Smlouva o dílo č. RCJ-2012-Z104

1. Smluvní strany

Jihomoravský kraj

Sídlo:	Žerotínovo nám. 3/5, 60182 Brno		
Jednající:	Michal Hašek, hejtman Jihomoravského kraje		
Bankovní spojení:	Komerční banka, a.s., pobočka Brno-město	číslo účtu: 35-1399230207/0100	
IČ:	70888337	DIČ:	CZ70888337

dále jen Objednatel na straně jedné

AutoCont CZ a.s.

Sídlo:	Hornopolní 3322/34, 702 00 Ostrava		
Jednající:	Ing. Jaroslav Biolek, ředitel společnosti a člen představenstva		
Bankovní spojení:	Citibank a.s.	číslo účtu:	2021301100 /2600
IČ:	47676795	DIČ:	CZ47676795
spisová značka OR:	Krajský soud v Ostravě, oddíl B, vložka 814		

dále jen Zhotovitel na straně druhé,

uzavírají níže psaného dne, měsíce a roku ve smyslu § 536 obchodního zákoníku tuto Smlouvu.

2. Předmět Plnění

2.1. Předmětem Plnění této Smlouvy je závazek Zhotovitele realizovat části projektového záměru Objednatele v oblasti eGovernmentu v rámci projektu „eGovernment v kraji, část výzvy I. - VI.“, registrační číslo projektu CZ.1.06/2.1.00/08.07386 v souladu s požadavky zadávací dokumentace Objednatele a nabídkou podanou Zhotovitelem (dále jen „Dílo“) a poskytnout níže uvedené služby navazující na toto Dílo (dále společně s Dílem také jako „Plnění“). Objednatel se zavazuje Dílo převzít a zaplatit Zhotoviteli v této smlouvě dále stanovenou cenu za poskytnuté Plnění. Veškeré podmínky a podrobnosti týkající se Předmětu Plnění jsou obsaženy v zadávací dokumentaci k veřejné zakázce, u níž je Objednatel zadavatelem, zejména v její příloze č. 1 s názvem „Technická specifikace předmětu plnění veřejné zakázky“ a v předmětu nabídky Zhotovitele, který je jako Příloha č. 1 nedílnou součástí této Smlouvy (dále také jako „Nabídka“).

2.2. Předmětem Díla je vytvoření komplexního řešení rozvoje e-Governmentu Objednatele dle specifikací obsažených v zadávací dokumentaci a nabídce Zhotovitele pro následující funkční oblasti:

a) technologické centrum Jihomoravského kraje
b) integrace vnitřního systému
c) elektronická spisová služba
d) datové sklady (DS), manažerské informační systémy a nástroje Business Intellligence (BI) Jihomoravského kraje
e) krajská digitální spisovna (KDS) a krajský digitální repozitář (KDR)

(společně dále také jako „realizační fáze“).

2.3. Zhotovitel se dále zavazuje poskytnout objednateli po předání Díla následující servisní služby:

a) odstraňování závad
b) provozní správu
c) expertní podporu
d) provádění změn provozní dokumentace
e) monitoring HW a základního SW

(dále také jako „provozní fáze“)

2.4. Provozní fáze navazuje na realizační fázi a bude realizována v období dle čl. 3. odst. 3.1 Smlouvy.

3. Termíny Plnění, harmonogram Projektu

3.1. Smluvní strany dohodly následující termíny zahájení a ukončení pro jednotlivé části Díla:

	Název fáze	**Datum/Termín Od - Do**
Realizační fáze	Zahájení Projektu	termín podpisu a nabytí účinnosti Smlouvy
	Dodávka a implementace Technologického centra Jihomoravského kraje	do 3 měsíců od podpisu a nabytí účinnosti Smlovy
	Dodávka a implementace Integrace vnitřního systému – *Analytická část*	do 2 měsíců od podpisu a nabytí účinnosti Smlovy
	Dodávka a implementace Integrace vnitřního systému – *Veškerá ostatní plnění v rámci této oblasti*	do 12 měsíců od podpisu a nabytí účinnosti Smlovy
	Dodávka a implementace Elektronická spisová služba	do 4 měsíců od podpisu a nabytí účinnosti Smlovy
	Dodávka a implementace Datových skladů, manažerských informačních systémů a nástrojů Business Intelligence – *Analytická část*	do 3 měsíců od podpisu a nabytí účinnosti Smlovy
	Dodávka a implementace Datových skladů, manažerských informačních systémů a nástrojů Business Intelligence – *Veškerá ostatní plnění v rámci této oblasti*	do 12 měsíců od podpisu a nabytí účinnosti Smlovy
	Dodávka a implementace Krajská digitální spisovna, Krajskrý digitální repozitář	do 6 měsíců od podpisu a nabytí účinnosti Smlovy
	Zkušební provoz všech oblastí plnění	Délka 2 měsíce od předání a převzetí všech oblastí plnění (nejpozději však do 30.10.2013)

	Předání a akceptace Díla	Po úspěšném předání všech oblastí plnění a zároveň úspěšném ukončení zkušebního provozu (nejpozději však 31.10.2013)
Provozní fáze	Servisní služby po dobu 5 let	Po dobu 5 let od úspěšného předání všech oblastí plnění a zároveň úspěšného ukončení zkušebního provozu (nejpozději však od 1.11.2013)

3.2. Smluvní strany berou na vědomí, že dodržení sjednaných termínů Plnění je podmíněno poskytnutím řádné součinnosti Objednatele.

4. Cena Plnění

4.1. Celková cena předmětu Plnění podle článku 2.1 je stanovena dohodou a činí

Cena bez DPH: 112.463.035,00 Kč
(slovy stodvanáctmiliónůčtyřistašedesáttřitisíctřicetpět korun českých)

Výše DPH (20%): 22.492.607,00 Kč
Cena s DPH: 134.955.642,00 Kč

4.2. Podrobná specifikace ceny předmětu Plnění je uvedena v příloze č.2 této Smlouvy.

4.3. Cena plnění je:

- je celkovou cenou za kompletní a řádné splnění předmětu Smlouvy,
- je maximální a její překročení je nepřípustné vyjma případu, kdy během realizace předmětu Plnění dojde ke změně výše sazby daně z přidané hodnoty, která se uplatňuje na předmět Plnění ke dni uskutečnění zdanitelného plnění
- obsahuje veškeré náklady Zhotovitele nezbytné pro řádnou a včasnou realizaci předmětu Plnění včetně nákladů souvisejících (např. vedlejší náklady, náklady na poskytnutí licencí, cestovní náklady, předpokládaná rizika spojená s realizací předmětu Plnění apod.). Zhotovitelem navržené ceny budou konstantní po celou dobu platnosti Smlouvy.

4.4. DPH se pro účely této Smlouvy rozumí peněžní částka, jejíž výše odpovídá výši daně z přidané hodnoty vypočtené dle zákona č. 235/2004 Sb., o dani z přidané hodnoty, ve znění pozdějších předpisů.

4.5. Cena Plnění zahrnuje nezbytné náklady, které Zhotoviteli vzniknou při poskytování sjednaných služeb.

5. Platební podmínky

5.1. Sjednaná cena za předmět Plnění, resp. za každou řádně předanou a převzatou dílčí část Plnění, je splatná na základě daňového dokladu – faktury vystavené Zhotovitelem v termínu nejpozději do 15 dnů od data převzetí Plnění, resp. jeho dílčí části. Podkladem pro vystavení faktury je vždy dílčí akceptační protokol (tj. protokol o předání a převzetí dílčí části Plnění).

5.2. Splatnost daňových dokladů – faktur se sjednává ve lhůtě 30 dnů ode dne jeho doručení Objednateli (stejná lhůta splatnosti se uplatní i při placení jiných plateb, smluvních pokut, úroků z prodlení, náhrady škody atd.), přičemž za den doručení faktury se pokládá den uvedený na otisku doručovacího razítka podatelny Objednatele. Faktura musí obsahovat veškeré náležitosti daňového a účetního dokladu dle zvláštních právních předpisů, a to zejména dle zákona o DPH.

5.3. Cena za poskytování servisních služeb bude Objednatelem uhrazena vždy předem na příslušné pololetí, a to na základě vystaveného daňového dokladu – faktury. První faktura může být Zhotovitelem vystavena po podpisu finálního předávacího protokolu (tj. převzetí Plnění do produkčního provozu).

5.4. Objednatel není vázán obsahem daňového dokladu vyhotoveným Zhotovitelem v případě, kdy tento daňový doklad nemá požadované náležitosti, resp. jsou v něm uvedeny nesprávné údaje, přičemž Objednatel je současně povinen zaslat takto neúčinný daňový doklad zpět Zhotoviteli a to nejpozději před uplynutím data splatnosti dotčeného daňového dokladu. Nová lhůta splatnosti začne běžet ode dne doručení bezvadného (opraveného či doplněného) daňového dokladu Objednateli.

5.5. Každý daňový doklad musí obsahovat informaci, že se jedná o veřejnou zakázku financovanou Evropskou unií z Evropského fondu pro regionální rozvoj v rámci IOP a musí být označen názvem a registračním číslem projektu eGovernment v kraji, část výzvy I.-VI., kofinancovaného z IOP.

5.6. Veškeré platby budou prováděny bezhotovostním převodem na účet uvedený v záhlaví Smlouvy, pokud na příslušné faktuře nebude výslovně specifikováno jinak.

6. Komunikace, pravomoci a odpovědnosti zástupců smluvních stran

6.1. Kontaktní osoby

6.1.1. Kontaktní osoba Zhotovitele:

Účel - provozní, finanční, … záležitosti
Jméno, Příjmení: Ing. Radim Frendl
e-mail: Radim.Frendl@autocont.cz
tel: +420 602 731 619
adresa: AutoCont CZ a.s.,Sochorova 23, 616 00 Brno

6.1.2. Kontaktní osoba Objednatele:

Účel - provozní, finanční, … záležitosti
Jméno, Příjmení: Ing. Roman VRBA
e-mail: vrba.roman@kr-jihomoravsky.cz
tel: 54165 8842
adresa: Jihomoravský kraj, Žerotínovo nám. 3/5, 60182 Brno

6.2. Oprávněné osoby

Jsou zplnomocněné osoby smluvních stran, které jsou oprávněny jednat jménem smluvních stran o všech smluvních a obchodních záležitostech týkajících se Smlouvy a souvisejících s jejím plněním.

6.2.1. Oprávněné osoby Zhotovitele:

Jméno, Příjmení: Ing. Jaroslav Biolek

e-mail: Jaroslav.Biolek@autocont.cz
tel: +420 596 254 442
adresa: AutoCont CZ a.s.,Sochorova 23, 616 00 Brno

6.2.2. Oprávněné osoby Objednatele:
Jméno, Příjmení: JUDr. Michal HAŠEK
e-mail: hejtman@kr-jihomoravsky.cz
tel: 54165 1501
adresa: Jihomoravský kraj, Žerotínovo nám. 3/5, 60182 Brno

6.3. Všechna oznámení mezi smluvními stranami, která se vztahují k této Smlouvě, nebo která mají být učiněna na základě této Smlouvy, musí být učiněna v písemné formě a doručeny opačné straně, nebude-li stanoveno, nebo mezi smluvními stranami dohodnuto jinak.

6.4. Oznámení se považují za doručená uplynutím třetího (3) dne po jejich prokazatelném odeslání.

6.5. Smluvní strany se zavazují, že v případě změny své adresy budou o této změně druhou smluvní stranu informovat nejpozději do tří (3) dnů.

6.6. Řídící výbor

6.6.1. Řídící výbor bude průběžně vyhodnocovat plnění této Smlouvy a bude sloužit k případné eskalaci problémů, pokud se smluvní strany nedohodnou ne jejich řešení nejpozději do 30 dnů od jejich vzniku.

6.6.2. Členové řídícího výboru:

Za Objednatele

Jméno a příjmení	*Pozice/funkce*	*E-mail*	*Telefon*
Ing. Jan Forbelský	*Vedoucí odboru informatiky JMK*	*forbelsky.jan@kr-jihomoravsky.cz*	*+420 606 768 015*

Za Zhotovitele

Jméno a příjmení	*Pozice/funkce*	*E-mail*	*Telefon*
Ing. Martin Stejskal	*ředitel divize ITI*	*Martin.Stejskal@autocont.cz*	*+420 602 771 942*

7. Místo a způsob Plnění

7.1. Místem Plnění předmětu Smlouvy je lokalita hlavního a záložního datového centra Objednatele v lokalitách:

- hlavní sídlo Objednatele na adrese Žerotínovo nám. 3/5, 601 82 Brno (hlavní datové centrum)
- budova Objednatele na adrese Cejl 73, 601 82 Brno (záložní datové centrum)

7.2. Dopravu zajišťuje Zhotovitel na své náklady.

8. Předání a Akceptace Díla

8.1. Smluvní strany sjednávají systém akceptační procedury, který zohledňuje základní požadavky Objednatele uvedené v následujících odstavcích. Akceptační procedura je zasazena do

harmonogramu plnění veřejné zakázky (tj. respektuje veškeré časové milníky stanovené touto Smlouvou.

8.2. Předání a převzetí Plnění proběhne prostřednictvím akceptační procedury, která zahrnuje porovnání skutečných vlastností Plnění se specifikací Plnění uvedenou v nabídce Zhotovitele a této Smlouvě na realizaci veřejné zakázky, a to za přítomnosti oprávněných osob obou smluvních stran.

8.3. Akceptační procedura bude zahrnovat dílčí akceptační testy, které budou probíhat na základě specifikace akceptačních testů obsahující popis testů, testovací data, příslušné prostředí, pořadí provádění testů a akceptační kritéria. Nedohodnou-li se smluvní strany jinak, vypracuje specifikaci akceptačních testů Zhotovitel a předá ji Objednateli k odsouhlasení. Odsouhlasení bude provedeno písemnou formou v termínu 10 pracovních dnů před zahájením akceptační procedury.

8.4. Objednatel je povinen převzít Plnění nebo jeho část dříve, než jak je sjednáno v harmonogramu plnění, vyzve-li jej Zhotovitel při respektování akceptačních kritérií k dřívější akceptaci.

8.5. Zhotovitel bude písemně informovat Objednatele, resp. jeho oprávněné osoby nejméně deset 10 dní předem o termínu zahájení akceptačních testů. Objednatel je oprávněn se těchto testů zúčastnit a osvědčit jejich konání, a to formou předávacího protokolu (resp. dílčích předávacích protokolů) podepsaného (podepsaných) oprávněnými osobami obou smluvních stran. Pokud se Objednatel nedostaví v termínu určeném pro provedení akceptačních testů, ačkoli byl s tímto termínem řádně seznámen, je Zhotovitel oprávněn provést příslušné akceptační testy bez jeho přítomnosti. Kopie veškerých dokumentů vypracovaných v souvislosti s provedením těchto akceptačních testů budou Objednateli poskytnuty 5 dnů před požadovaným termínem k odsouhlasení dokumentace akceptačních testů.

8.6. Základním předpokladem pro řádné předání dílčí části Plnění Zhotovitelem a jeho převzetí Objednatelem (formou předávacího protokolu podepsaného oprávněnými osobami obou smluvních stran), je skutečnost, že Plnění splní kritéria akceptačních testů.

8.7. Jestliže dílčí část Plnění splní akceptační kritéria akceptačních testů, Zhotovitel se zavazuje v den následující po ukončení akceptačních testů umožnit Objednateli Plnění v tomto rozsahu převzít a Obbjednatel se zavazuje v tomto termínu Plnění převzít. Pokud Objednatel v tomto termínu Plnění nepřevezme, má se za to, že takto provedená část Plnění byla řádně předána a Objednatelem převzata v den následující po ukončení akceptačních testů.

8.8. Jestliže Plnění (resp. jeho dílčí část) nesplňuje stanovená akceptační kritéria akceptačního testu, Zhotovitel bezodkladně po provedení takového testu sepíše akceptačním testem zjištěné nedostatky. Zhotovitel napraví tyto nedostatky a příslušné akceptační testy budou provedeny znovu. Tento proces testování a následných oprav se bude opakovat, dokud Zhotovitel nesplní veškerá akceptační kritéria pro příslušný akceptační test daný pro příslušnou část Plnění.

8.9. Při převzetí příslušné části Plnění se strany zaváží podepsat příslušný dílčí akceptační protokol.

8.10. Po akceptaci poslední dílčí části Plnění na základě shora uvedené akceptační procedury proběhne zkušební provoz po dobu 2 měsíců. Po jeho úspěšném dokončení bude do 14 dnů provedena akceptace Plnění jako celku na základě finálního předávacího protokolu podepsaného oprávněnými zástupci smluvních stran. Zkušební provoz nebude ukončen dříve, než bude provedena finální akceptace Plnění jako celku. Do okamžiku finální akceptace Plnění jako celku bude Zhotovitel poskytovat bezplatné servisní služby ve stejném rozsahu jako po akceptaci Plnění do produkčního provozu. Akceptačním protokolem musí být prokázána rovněž skutečnost, že Zhotovitel provedl nezbytné seznámení pracovníků Objednatele s obsluhou předaného Plnění, a to v rozsahu stanoveném v zadávací dokumentaci a této Smluvě.

8.11. Dokumenty, které budou zpracovány Zhotovitelem a které se poskytují Objednateli jako součást Plnění, budou nejdříve předloženy Objednateli ve formě návrhu k posouzení.

8.12. Objednatel je oprávněn ve lhůtě 10 dnů od doručení příslušného návrhu písemně předložit Zhotoviteli své připomínky k návrhu. Po diskusi o těchto připomínkách Zhotovitel upraví návrh v souladu s dohodnutými změnami a předá Objednateli konečnou verzi dokumentů se

zapracováním všech připomínek. V případě, že Objednatel připomínky ve shora uvedené lhůtě nepředloží, má se za to, že s předloženým dokumentem souhlasí.

8.13. Dokumenty se považují za předané doručením jejich konečné verze Objednateli.

9. Přechod vlastnického práva Díla a jeho částí, práva duševního vlastnictví

9.1. Vlastnické právo k předmětu Plnění nabývá Objednatel okamžikem akceptace Plnění; totožný okamžik platí i pro přechod nebezpečí škody.

9.2. Je-li součástí plnění Zhotovitele autorské dílo dodávané třetí stranou, je Zhotovitel povinen zajistit, aby Objednatel nabyl bezúplatně příslušná oprávnění z práv duševního vlastnictví, která se týkají takového autorského díla a která jsou nezbytná k jeho užívání Objednatelem (případně dalšími oprávněnými subjekty) a k jeho provozování, a zachování funkčnosti. Objednatel (případně další subjekty) je oprávněn taková autorská díla užívat v souladu s licenčními podmínkami třetích stran, přičemž Zhotovitel nese veškeré náklady s tímto oprávněním Objednatele spojené.

9.3. V případě, že při plnění veřejné zakázky vznikne dílo, které je chráněno předpisy o duševním vlastnictví, vzniká okamžikem vzniku takového díla právo Objednatele toto dílo užívat v rozsahu nezbytném pro naplnění účelu, ke kterému bylo vytvořeno, a to po dobu neomezenou (i po ukončení trvání této Smlouvy).

9.4. Dojde-li v rámci plnění předmětu této Smlouvy k pořízení databáze, pak je Objednatel od okamžiku pořízení databáze oprávněn databázi užívat.

10. Změnové řízení

10.1. Kterákoliv ze smluvních stran je oprávněna písemně navrhnout změny Plnění před jeho dokončením. Žádná ze smluvních stran však není povinna navrhovanou změnu Plnění akceptovat. Veškeré změny budou dohodnuty zejm. v souladu se zákonem o veřejných zakázkách. Zhotovitel bude povinen provést hodnocení dopadů Objednatelem navrhovaných změn Plnění na termíny a cenu Plnění.

10.2. Jakékoliv změny Plnění musí být sjednány písemně smluvním dodatkem. V závislosti na tom budou upraveny termíny Plnění, cena, platební podmínky a požadavky na součinnost Objednatele. Zhotovitel není povinen provést jakékoliv změny Plnění, dokud tyto nebudou písemně potvrzeny a dokud nebudou písemně dohodnuty příslušné změny týkající se ceny a harmonogramu Plnění.

11. Práva a povinnosti smluvních stran

11.1. Součinnost smluvních stran
Pro zajištění řádné realizace Díla požaduje Zhotovitel na Objednateli zejména následující součinnost:

11.1.1. Přístup k provoznímu prostředí, který je nezbytný pro Plnění Díla.

11.1.2. Určení Odpovědné osoby Objednatele, vyhrazení odpovídajících časových kapacit Odpovědné osoby Objednatele.

11.1.3. Poskytování požadovaných podkladů, informací, případně zajištění spolupráce s třetími stranami, jejichž řešení se může dotýkat předmětu Díla.

11.1.4. Smluvní strany se zavazují vzájemně spolupracovat a poskytovat si veškeré informace potřebné pro řádné plnění svých závazků z této Smlouvy.

11.1.5. Smluvní strany se zavazují informovat opačnou smluvní stranu o veškerých skutečnostech, které jsou, nebo by mohly být důležité pro řádné plnění této Smlouvy.

11.1.6. Smluvní strany se zavazují vytvářet předpoklady pro plnění závazků vyplývajících z této Smlouvy tak, aby nedocházelo k prodlení s plněním jednotlivých termínů pro poskytnutí věcného Plnění, ani k prodlení s úhradou jednotlivých finančních závazků.

11.2. Práva a povinnosti Zhotovitele:

- Zhotovitel spolupracuje s Odpovědnými osobami Objednatele při řízení postupu prací na Projektu, včetně organizace schůzek v rámci Projektu.
- Zhotovitel plánuje a koordinuje realizaci Projektu, navrhuje a vypracovává jeho harmonogram.
- Zhotovitel svolává ve spolupráci s Objednatelem schůzky k řešení sporných otázek.
- Zhotovitel konzultuje řešení v průběhu realizace předmětu Plnění na požádání Objednatele.
- Zhotovitel zajistí potřebný počet pracovníků s kvalifikací potřebnou pro realizaci předmětu Plnění.
- Zhotovitel řeší ve spolupráci s Objednatelem závady vzniklé při plnění této Smlouvy.

11.3. Účelem této Smlouvy je realizace části projektového záměru Objednatele v oblasti eGovernmentu v rámci projektu „eGovernment v kraji, část výzvy I. - VI.“, registrační číslo projektu CZ.1.06/2.1.00/08.07386

11.4. Zhotovitel prohlašuje, že si je plně vědom způsobu kofinancování ceny projektu z Evropského fondu pro regionální rozvoj EU v rámci Integrovaného operačního programu (IOP), přičemž se náležitě seznámil se všemi podmínkami stanovenými tímto operačním programem, které se zavazuje pro účely plnění Smlouvy a projektu dodržovat.

11.5. Zhotovitel se zavazuje učinit veškeré nezbytné úkony a opatření vedoucí ke splnění všech podmínek IOP v rámci plnění svých povinností vyplývajících ze Smlouvy, a to zejména:

11.5.1. umožnit zaměstnancům nebo zmocněncům Objednatele, oprávněným orgánům státní správy a poskytovateli příslušné dotace vstup do prostor dotčených projektem a dále umožnit fyzickou kontrolu realizace projektu, jakož i kontrolu veškerých dokladů souvisejících s projektem,

11.5.2. vytvořit podmínky k provedení kontroly vztahující se k realizaci projektu, poskytnout veškeré doklady vážící se k realizaci projektu, umožnit průběžné ověřování souladu údajů o realizaci projektu uváděných ve zprávách o realizaci projektu se skutečným stavem v místě jeho realizace a poskytnout součinnost všem shora uvedeným osobám oprávněným k provádění kontroly projektu,

11.5.3. uchovávat odpovídajícím způsobem v souladu se zákonem č. 499/2004 Sb., o archivnictví a spisové službě a o změně některých zákonů, ve znění pozdějších předpisů, a v souladu se zákonem č. 563/1991 Sb., o účetnictví, ve znění pozdějších předpisů, po dobu nejméně deseti let veškeré originály účetních dokladů, smlouvu včetně jejích dodatků a další originály dokumentů, vztahujících se k projektu, přičemž běh lhůty se začne počítat od 1. ledna následujícího kalendářního roku po roce, ve kterém byl projekt ukončen.

Splnění shora uvedených povinností je Zhotovitel povinen smluvně zajistit i u svých subdodavatelů tak, aby řídící orgán a další oprávněné osoby byly oprávněny obdobným způsobem provést kontrolu i u subdodavatele.

11.6. Zhotovitel se zavazuje dodržovat pravidla publicity dle Pravidel pro provádění informačních a propagačních opatření (Příloha č. 3 Příručky pro žadatele příjemce finanční podpory v rámci IOP – výzva 08)., resp. poskytnout nezbytnou součinnost Objednateli k jejich provádění, v rozsahu vyplývajícím z Nařízení komise (ES) č. 1828/2006, kterým se stanoví prováděcí pravidla k Nařízení Rady (ES) č. 1083/2006 o obecných ustanoveních.

11.7. Zhotovitel se zavazuje k veškeré nezbytné součinnosti pro výkon finanční kontroly ve smyslu ust. § 2 písm. e) zákona č. 320/2001 Sb., o finanční kontrole ve veřejné správě a o změně některých zákonů (zákon o finanční kontrole), ve znění pozdějších předpisů, a to v souvislosti s plněním veřejné zakázky.

11.8. Zhotovitel je oprávněn vstupovat do objektů Objednatele v souvislosti s Plněním smlouvy jen se souhlasem nebo v přítomnosti oprávněné osoby Objednatele.

11.9. Zhotovitel je povinen respektovat skutečnost, že Objednatel musí být oprávněn dle zákona č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů, zveřejnit určité informace. Ostatní informace uvedené ve Smlouvě či získané na základě Smlouvy budou stranami považovány za obchodní tajemství podle obchodního zákoníku, pokud je právně možné je jako obchodní tajemství kvalifikovat.

11.10. Práva a povinnosti Objednatele:

11.10.1. Objednatel se zavazuje poskytnout a vytvořit Zhotoviteli odpovídající pracovní podmínky pro realizaci předmětu této Smlouvy, a to v rozsahu specifikovaném tímto článkem Smlouvy. V této souvislosti Objednatel prohlašuje, že je srozuměn s tím, že dodržení termínů pro poskytnutí věcného Plnění Zhotovitelem závisí i na řádném a včasném plnění povinností stanovených touto Smlouvou pro Objednatele.

11.10.2. Objednatel k termínu zahájení Projektu jmenuje do všech úrovní řízení Projektu pracovníky s pravomocemi potřebnými pro výkon příslušné funkce.

11.10.3. Objednatel předává Zhotoviteli potřebné nebo vyžádané podklady a informace, související s realizací předmětu Plnění, nejpozději do tří (3) Pracovních dnů po jejich písemném či ústním vyžádání, pokud se o obě strany nedohodnou jinak.

11.10.4. Objednatel konzultuje řešení v průběhu realizace předmětu Plnění na požádání Zhotovitele. Nejpozději do tří (3) Pracovních dnů od písemného vyzvání k projednání řešení Objednatel zorganizuje toto projednání a zajistí účast Odpovědných osob Objednatele.

11.10.5. Objednatel je povinnen zajistit řádné a včasné předávání potřebných nebo Zhotovitelem vyžádaných dokumentů, předpisů, informací, rozhodnutí, specifikací požadavků a dalších podkladů souvisejících s realizací díla.

11.10.6. Objednatel je povinen v průběhu Zkušebního provozu neprodleně předávat Zhotoviteli informace o skutečnostech, které brání úspěšnému provádění Ověřovacího provozu.

11.10.7. Objednatel je povinen zajistit přístup Pracovníkům Zhotovitele do objektů a k pracovištím, v souvislosti s plněním Díla.

11.10.8. Objednatel se zavazuje poskytovat řádnou a včasnou součinnosti při předávání a akceptacích plnění díla, resp. jeho částí nebo etap, včetně písemného oznamování vad a nedodělků díla bránících akceptaci plnění.

12. Odpovědnost za škodu

12.1. Omezení výše odpovědnosti za škodu, jakož i sankcí uvedených v této Smlouvě se nepřipouští. Nepřipouští se omezení výše škody, kterou lze při porušení Smlouvy předvídat. Jakýmkoli ujednáním o smluvní pokutě není dotčen nárok Objednatele na náhradu škody.

13. Záruka

13.1. Na veškerá technická zařízení dodávaná v rámci Plnění poskytuje Zhotovitel záruku po dobu 5 let od doby finálního předání a akceptace Díla.

13.2. Zhotovitel odpovídá za zajištění technické podpory po celou dobu záruky v souladu s podmínkami a SLA, uvedenými v Příloze č. 5 Smlouvy.

13.3. Objednatel je oprávněn po Zhotoviteli požadovat úhradu smluvní pokuty při nedodržení následujících závazných parametrů SLA servisních služeb:

a) 1.200,- Kč za každou započatou půlhodinu při prodlení s dodržením doby reakce na kritickou vadu (vada kategorie A) či odstraněním kritické vady;

b) 1.000,- Kč za každou započatou hodinu při prodlení s dodržením doby reakce na střední vadu (vada kategorie B) či odstraněním střední vady;

c) 800,- Kč za každou započatou hodinu při prodlení s dodržením doby reakce na nízkou vadu (vada kategorie C) či odstraněním nízké vady.

13.4. V případě nedodržení stanovené doby reakce v souvislosti s požadavky na provozní správu, požadavky na expertní podporu a změny provozní dokumentace platí smluvní pokuta dle písm. c), a to za každou započatou hodinu při prodlení.

13.5. V případě nedodržení stanovené doby reakce v rámci monitoringu HW a základního SW v oblasti TCK bude Zhotovitel povinen zaplatit smluvní pokutu ve výši 500,- Kč za každých započatých 5 minut prodlení Zhotovitele.

13.6. Poskytovateli služeb Zhotovitele bude umožněn zabezpečený vzdálený přístup k servisovaným a spravovaným zařízením a SW.

13.7. Záruka se vztahuje na shodu funkčního chování a vlastností Plnění při Předání.

14. Další povinnosti Zhotovitele, prodlení, sankce

14.1. Zhotovitel prohlašuje, že poskytované Plnění odpovídá všem požadavkům vyplývajícím z právních předpisů či příslušných technických norem, které se na Plnění vztahují, přičemž výslovně prohlašuje a uznává závaznost technických norem aplikovatelných na předmět Plnění. V případě, že se toto prohlášení ukáže jako nepravdivé, má Objednatel vedle práva písemného odstoupení od Smlouvy právo na smluvní pokutu ve výši Kč 300.000,- Kč za každý jednotlivý případ, čímž není nijak dotčen nárok Objednatele na náhradu škody.

14.2. V případě, že se Zhotovitel při realizaci předmětu Plnění dle Smlouvy dostane do kontaktu s osobními údaji, je povinen o nich zachovávat mlčenlivost; to platí i po ukončení plnění Smlouvy i v případě výpovědi Smlouvy či odstoupení. V případě porušení tohoto ustanovení, jakož i v případě neoprávněného přístupu k osobním údajům, má Objednatel právo na smluvní pokutu ve výši 300.000,- Kč za každé jednotlivé porušení, čímž není dotčen nárok na náhradu škody. Objednatel je oprávněn požadovat, aby Zhotovitel uzavřel smlouvu o zpracování osobních údajů.

14.3. V případě prodlení Zhotovitele s předáním Plnění nebo jeho dílčí části (tj. jednotlivé oblasti Plnění specifikované v zadávací dokumentaci a této Smlouvě) má Objednatel právo na smluvní pokutu ve výši 0,5 % z příslušné ceny Plnění či jeho části (kalkulováno z ceny za příslušnou oblast Plnění vč. DPH), a to za každý i jen započatý den prodlení. V případě jakéhokoli prodlení

Zhotovitele po dobu delší než 14 dnů má Objednatel právo Smlouvu (či její část) písemně vypovědět s účinností k okamžiku doručení výpovědi Zhotoviteli.

14.4. V případě, že Zhotovitel neoprávněně zasáhne do práv duševního vlastnictví, má Objednatel právo vedle případné náhrady škody na smluvní pokutu ve výši 300.000,- Kč za každý jednotlivý neoprávněný zásah. Odpovědnost za neoprávněný zásah do autorských i jiných práv třetích osob nese výlučně Zhotovitel.

14.5. Zhotovitel je povinen pro plnění veřejné zakázky využívat kapacit, prostřednictvím kterých prokázal splnění kvalifikačních předpokladů; není-li to objektivně možné, je povinen o tom neprodleně písemně informovat Objednatele a navrhnout nejméně stejně kvalifikovanou náhradu. Nesplní-li kteroukoliv z uvedených povinností, má Objednatel právo na smluvní pokutu ve výši 300.000,- Kč za každé jednotlivé porušení.

14.6. Zhotovitel je povinen mít po celou dobu trvání Smlouvy sjednáno pojištění odpovědnosti za škodu způsobenou třetí osobě, a to s limitem pojistného plnění ve výši nejméně 50 mil. Kč na jednu škodnou událost. Zhotovitel je povinen na požádání tuto pojistnou smlouvu kdykoliv předložit v Objednatelem stanovené přiměřené lhůtě (nejdéle však do 7 dnů); v případě nepředložení pojistné smlouvy s požadovanými parametry je Objednatel oprávněn požadovat po Zhotoviteli smluvní pokutu ve výši 300.000,- Kč za každé porušení a rovněž písemně Smlouvu či její část vypovědět s účinností k okamžiku doručení výpovědi Zhotoviteli.

14.7. Zhotovitel se zavazuje uhradit Objednateli smluvní pokutu ve výši 5.000,- Kč za porušení jakékoli smluvní povinnosti Zhotovitele, na kterou není sjednána zvláštní smluvní pokuta, a to za každý jednotlivý případ.

14.8. Zhotovitel je oprávněn požadovat po Objednateli zaplacení úroku z prodlení nejvýše ve výši 0,05 % z částky, s jejíž úhradou je Objednatel v prodlení, a to za každý započatý den prodlení.

15. Platnost, odstoupení a zánik smlouvy

15.1. Pokud bude Zhotovitel opakovaně v prodlení s plněním jakékoli povinnosti, je Objednatel oprávněn Smlouvu vypovědět s účinností k poslednímu dni v kalendářním měsíci, v němž byla výpověď Zhotoviteli doručena. Není-li uvedeno jinak, za opakované prodlení se považuje prodlení Zhotovitele s plněním jakékoli povinnosti, které nastalo alespoň třikrát, a týkalo se totožné povinnosti. Objednatel je oprávněn vypovědět Smlouvu i jen z části, tj. jen ve vztahu k té části Smlouvy, která stanovuje povinnost, s jejímž splněním je Zhotovitel opakovaně v prodlení, jedná-li se o Plnění oddělitelné.

15.2. Objednatel je oprávněn ve vztahu k poskytování servisních služeb kdykoli Smlouvu písemně vypovědět i bez udání důvodu v šestiměsíční výpovědní lhůtě. Zhotovitel je oprávněn Smlouvu vypovědět ve vztahu k poskytování servisních služeb ve lhůtě šesti měsíců, přičemž tohoto oprávnění může využít nejdříve po uplynutí čtyř let od účinnosti Smlouvy. Výpovědní lhůta počíná běžet vždy prvním dnem kalendářního měsíce následujícího po doručení výpovědi druhé smluvní straně.

15.3. Tato Smlouva nabývá platnosti a účinnosti dnem podpisu zástupců obou smluvních stran.

15.4. Skončit platnost této Smlouvy lze dohodou smluvních stran, která musí mít písemnou formu.

15.5. Každá smluvní strana je oprávněna jednostranně odstoupit od Smlouvy, jestliže:

15.5.1. druhá smluvní strana neplní hrubě podmínky Smlouvy, byla na tuto skutečnost upozorněna, nesjednala nápravu ani v dodatečně poskytnuté přiměřené lhůtě

15.6. V případě skončení smluvního vztahu odstoupením, smluvní strany nebudou aplikovat ustanovení § 351 odst. 2 obchodního zákoníku v platném znění.

16. Řešení sporů

16.1. Veškeré spory vzniklé mezi smluvními stranami na základě této Smlouvy nebo v souvislosti s ní, které se nepodaří odstranit jednáním mezi stranami, budou s konečnou platností rozhodovány příslušným soudem. Rozhodčí řízení je vyloučeno.

17. Závěrečná ustanovení

17.1. Tato Smlouva respektuje ustanovení zákona o veřejných zakázkách a další právní předpisy, které se vztahují na provádění veřejné zakázky; do Smlouvy jsou začleněny veškeré požadavky Objednatele plynoucí ze zadávací dokumentace a její příloh.

17.2. Zhotovitel prohlašuje, že:

- nemá v úmyslu nezaplatit daň z přidané hodnoty u zdanitelného plnění podle této Smlouvy (dále jen „daň"),
- mu nejsou známy skutečnosti nasvědčující tomu, že se dostane do postavení, kdy nemůže daň zaplatit a ani se ke dni podpisu této Smlouvy v takovém postavení nenachází,
- nezkrátí daň nebo nevyláká daňovou výhodu.

17.3. Tato Smlouva nevylučuje ani žádným způsobem neomezuje oprávnění Objednatele uvedená v zadávací dokumentaci veřejné zakázky.

17.4. Vztahy mezi stranami se řídí ustanoveními této Smlouvy a obchodním zákoníkem. V částech vztahujících se k udělení práva užití programů splňujících znaky autorského díla se použije režim autorského zákona.

17.5. Obsah Smlouvy může být měněn jen dohodou stran smluvních a to vždy jen vzestupně číslovanými písemnými dodatky potvrzenými Oprávněnými osobami smluvních stran.

17.6. Smlouva je vyhotovena ve čtyřech stejnopisech, z nichž každý má platnost originálu. Dvě vyhotovení jsou určena pro Objednatele a zbývající dvě vyhotovení jsou určena pro Zhotovitele.

17.7. Nedílnou součástí Smlouvy jsou následující přílohy:
Příloha č.1 – Podrobný popis Plnění
Příloha č.2 – Členění ceny Plnění
Příloha č.3 – Část Díla, jejíž plnění je zajištěno prostřednictvím subdodavatele
Příloha č.4 – Projektová metodika
Příloha č. 5 – Technické parametry SLA
Příloha č. 6 – Výčet standardů

Doložka podle § 23 zákona č. 129/2000 Sb., o krajích (krajské zřízení), ve znění pozdějších předpisů:
Tato smlouva byla schválena Radou Jihomoravského kraje dne 30. 7. 2012 na schůzi 17.
usnesením č. 1280C/12/2173

V Brně dne 30. 7. 2012

Objednatel
JUDr. Michal Hašek,
hejtman Jihomoravského kraje

Jihomoravský kraj
Žerotínovo nám. 3/5
601 82 Brno

V Brně dne 10. 7. 2012

Zhotovitel
Ing. Jaroslav Biolek,
ředitel společnosti a člen představenstva
AutoCont CZ a.s.

AutoCont®
AutoCont CZ a.s., Brno
Sochorova 23, 616 00 Brno
Tel.: 596 254 444, fax: 596 254 400
DIČ: CZ47676795

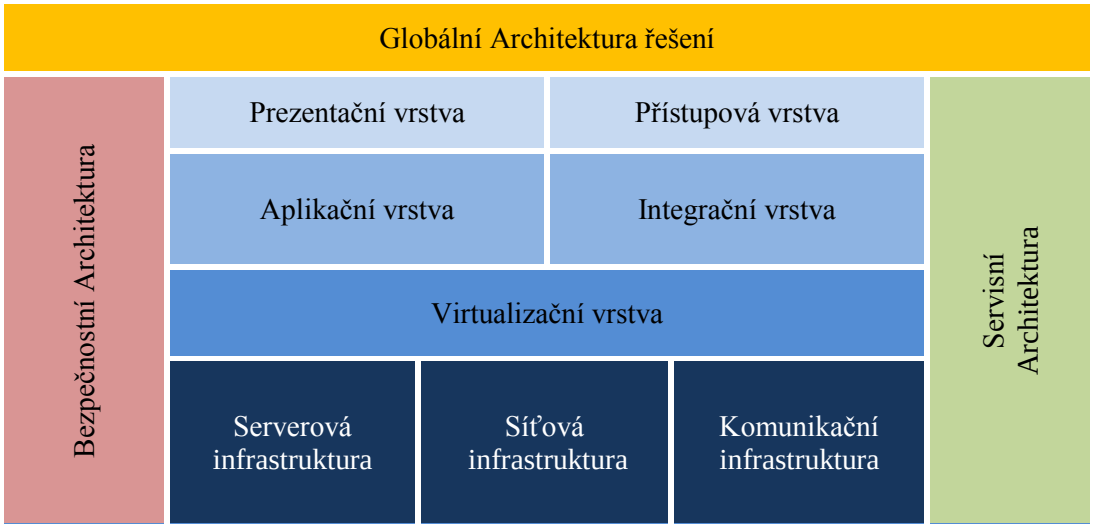
Příloha č.1 – Podrobný popis Plnění

Architektura a koncepce technického řešení

Zhotovitel navrhl celkovou architekturu řešení a její jednotlivé funkční celky s ohledem na informace uvedené v Zadávací dokumentaci a v dokumentaci Rozvoj eGovernmentu v rámci JMK (http://www.kr-jihomoravsky.cz/Default.aspx?PubID=151556&TypeID=2).

Celková struktura řešení je shrnuta do konceptu v kapitole Globální architektura. Zhotovitel dále člení vlastní koncept řešení podle logiky komunikace a toku informací na vrstvy:

- Prezentační vrstva
- Přístupová vrstva
- Aplikační vrstva
- Integrační vrstva
- Virtualizační vrstva
- Serverová infrastruktura
- Síťová infrastruktura
- Komunikační infrastruktura



Obrázek: Členění architektury do částí dekompozicí pro možnost rozdělení návrhu na menší části systému s definovanými vrstvami a hierarchií mezi nimi

Zhotovitel v rámci kapitoly Globální architektura přehledně objasňuje úlohu jednotlivých vrstev a vazby mezi nimi, kde návrh opírá o vlastní know-how a Best Practice, které získal při implementaci obdobných integračních řešení.

Zhotovitel popisuje architekturu řešení s důrazem na důležité komponenty integrace umístěné do aplikační a integrační vrstvy, kde se soustřeďuje na integraci aplikací dodávaných v rámci plnění pomocí Integrační platformy, která představuje sběrnici úřadu a po které dokácí ke komunikaci formou volání služeb. Úroveň propracovanosti integrační architektury dokládá i tím jak začleňuje stávající IS úřadu tak, aby byly schopny využívat služeb informační platformy ke sdílení služeb centrálních ISVS, které představují především Základní Registry a Informační systém Datových Schránek

Detailní technické parametry a vlastnosti jednotlivých komponent rozmístěných ve vrstvách globální architektury, splňující podmínky kladené na provoz a dlouhodobý rozvoj systému popisuje Zhotovitel v kapitole 6, kde jsou za všechny hlavní části předmětu plnění (tj. oblasti A - E) uvedeny a doplněny v souvislostech o popis procesů zajišťujících jejich dlouhodobou udržitelnost: částí plnění F- Servisní služby a H - Bezpečnost.

Vrcholová architektura je Architektura prezentační vrstvy, kde musí docházet k prolnutí všech informací v souvislostech tak, aby uživatelé úřadu, především role, které budou provádět vlastní výkon Agend OVM, dostaly do rukou přívětivý, komfortní, ale i robustní a hladce zaintegrovaný nástroj pro jejich práci. Zde Zhotovitel klade důraz na vizuální formu prezentace funkcionality řešení (Portál integrující aplikace) a procesní podporu výkonu agend (Workflow napojené na Integrační sběrnici)

Zhotovitel při koncipování architektury vzal na vědomí požadavek vysoké technické úrovně a volil jednotlivé komponenty všech vrstev tak, aby tento požadavek naplil co největší možnou měrou. Proto použil standardizované, osvědčené a moderní komponenty, které zajistí udržitelnost provozu celého řešení po dobu 5-ti let s ohledem na co nejmenší zátěž lidských zdrojů Objednatele.

Globální Architektura řešení

Aby Globální architektura řešení naplnila základní představy a cíle zákazníka, byly nutné vzít do úvahy při návrhu i informace o zdrojích, s kterými bude řešení realizováno a provozováno.

Vstupy:

- Finanční – zajištění zdrojů financování
- Lidské – stav lidských zdrojů a připravenost přijmout nové řešení
- Materiálové – prostory, stávající systémy
- Časové – představu posloupnosti a časovém naplnění realizace

Při koncipování technického návrhu bylo nutno uvažovat v výhledem do budoucna a s vědomím, že Zhotovitelem předložené řešení ve svém důsledku vždy ovlivní především procesy Objednatele, ale i pohled na užitnou hodnotu řešení a význam dá nový význam pojmům:

- Znalosti – co se musí stát v oblasti sdílení znalostí,
- Informace – co se musí stát v oblasti toku informací,
- Data – co se musí stát v oblasti zacházení a ukládaní s daty,

Aby byla implementace celého řešení a jeho následný provoz úspěšné, musí Globální architektura řešení splnit množinu základních předpokladů, které si Zhotovitel stanovil pro návrh, a které užívá jako neměnné axiomy na kterých pak staví svůj návrh architektury:

- ochrana stávajících investic,
- pružnost celkového návrhu,
- otevřenost řešení,
- schopnost realizace a uvedení do provozu,
- efektivnost navrhovaného řešení,

- nízké požadavky na interní zdroje.

Na takto definované axiomy Zhotovitel nasadil vlastní ověřený přístup k návrhu, založený na principech modelování Podnikové Architektury (Enterprise Architecture), jenž je perspektivním a moderním konceptem pro vytváření systému orientovaných na služby a které umožní začlenění řešení do již existujícího prostředí ICT na úřadě a ochrání tak stávající investice Objednatele. Rozložení do jednotlivých vrstev a dekompozice metamodelu EA do dílčích vrstev umožní úřadu efektivně řídit změny, reagovat pružně na nové požadavky a dovolí začleňovat budoucí IS úřadu. Objednatel si tak zajistí schopnost poskytovat stávající služby v požadovaných parametrech a kvalitě a zároveň reagovat na nové interní i externí požadavky a vytvářet služby nové.

LOGICKÉ VRSTVY ARCHITEKTURY

Logické vrstvení architektury je velmi podstatné a samo o sobě ovlivňuje celkovou správu, bezpečnost a flexibilitu infrastruktury. Je důležité, že každá logická vrstva je považována za oddělenou část architektury, která má vazby/rozhraní k dalším sousedním vrstvám a tato rozhraní respektuje v celém návrhu infrastruktury. Oddělení logických vrstev definovaným rozhraním umožňuje snadněji lokalizovat a opravit případný problém.
V návrhu systému Zhotovitel pracuje s následujícími logickými vrstvami architektury ICT. Je důležité poznamenat, že i jednotlivé logické vrstvy se následně dělí na samostatné části (komponenty vrstev) jak z technologického tak i z bezpečnostního důvodu.

Prezentační vrstva
Na prezentační vrstvě jsou provozovány aplikace/instance zajišťující odpovídající prezentaci výsledků předávaných aplikační vrstvou (přístup pro interní uživatele). V případě, že jsou výsledky prezentovány externímu subjektu, procházejí dále přístupovou vrstvou.

Přístupová vrstva
Tato vrstva je nositelem základních bezpečnostních technologií pro zajištění rozhraní Intranet/Extranet, přístup přes mobilní zařízení, synchronizace s plánováním a např. finančními operacemi. Z procesního pohledu jsou zde prováděny základní autentizační a autorizační činnosti nezbytné k povolení/zamítnutí přístupu k aplikacím a jejich službám. Vrstvu dělíme na dvě logické podvrstvy - externí a interní. Na externí jsou soustředěny základní bezpečnostní technologie a autentizace externích subjektů přistupujících k veřejným/externím službám (LDAP, AD).

Aplikační vrstva
Aplikační vrstva představuje logickou část informačního systému, ve které je zpracovávána aplikační logika implementovaných subsystémů a procesní logika obsluhovaných procesů. Aplikační vrstvy jednotlivých aplikací (služeb, subsystémů) mohou být hostovány na stejných serverech. Jejich činnost však vždy zajišťuje samostatná instance aplikačního serveru (nebo obecně samostatná instance aplikační vrstvy daného subsystému). To znamená, že jedna instance aplikačního serveru by neměla sloužit pro obsluhu více samostatných aplikačních vrstev. V případě integrační platformy (ESB), IDM aj. jsou pak všechny instance provozované ve virtuálním prostředí.

Integrační vrstva
Sestává z dvou základních komponent, které zajišťují integraci technologií a integraci procesů.

„Integrace pro Stroje“: bude realizována Integrační platformou / Podnikovou sběrnicí služeb (ESB), která spadá do oblasti návrhů systému typu Business Process Management System (BPMS) a je technicky realizována v Architektuře orientované na služby (Service Oriented Architecture).

„Integrace pro lidi“: bude realizován elektronickým Workflow, jakožto nástrojem pro organizaci toku práce, efektivní sdílení dokumentace a informací, hlídání zákonných lhůt, dodržování procesních pravidel a zákonných norem, spolupráci uživatelů a snazší řešení jejich zastupitelnosti.

Virtualizační vrstva
Vrstva, která pomocí postupů, technik a SW, umožní přistupovat k dostupným zdrojům Technologického Centra jiným způsobem, než jakým fyzicky existují a jakým jsou propojeny. Virtualizované prostředí může být mnohem snáze přizpůsobeno potřebám vyšších vrstev řešení, snáze se přizpůsobovat požadavkům, případně před vyššími vrstvami řešení zakrývat pro ně nepodstatné detaily (jako např. rozmístění hardwarových prostředků). Virtualizovat lze na různých úrovních. Návrh Zhotovitele v hrubých rysech počítá se serverovou a diskovou virtualizací.

Serverová, Síťová a Komunikační infrastruktura
Dostatečné robustní a bezpečná komunikační, serverová a síťová Infrastruktura významně snižuje především rizika výpadků celého řešení v provozu, dále zamezuje rozšiřování nebezpečných kódů, zabraňuje nedostupnosti a zcizení dat z informačních systémů a předchází tak ztrátám v produktivitě zaměstnanců. Konkrétní detaily návrhu těchto vrstev jsou uvedeny v následujících kapitolách.

KONCEPT ŘEŠENÍ INTEGRACE NA ÚŘADĚ

Základem architektonického konceptu je přiměřeně robustní HW a SW infrastruktura navržená s ohledem na předpokládanou zátěž a požadavky na dostupnost. Předpoklady pro pružné a efektivní využití technických (HW) prostředků jsou přitom vytvořeny využitím serverové virtualizace. Obdobná pružnost na straně SW prostředků je dosažena synergickou kombinací integrační platformy a platformy pro řízení pracovních procesů (workflow).

Architektonický koncept založený na současném využití serverové virtualizace, integrační platformy a workflow přináší **otevřenou a efektivní provozně-technologickou platformu připravenou pro budoucí rozvoj** (kapacitní, výkonový, technologický) při maximální ochraně investic do ICT úřadu. Stávající aplikace úřadu lze na takové platformě provozovat buď přímo, případně s úpravami – „obalení“ aplikace – rozhraním pro publikaci jeho WebServices.

Zásadní výhodou návrhu na bázi integrační platformy a workflow je vytvoření předpokladů pro **efektivní integraci dílčích IS a aplikací úřadu do jediného komplexního IS** - tj. vytvoření technických a technologických předpokladů pro realizaci integrace vnitřního chodu úřadu, jejíž provedení je v návrhu chápáno jako realizace zásadní části funkčnosti celého TC.

Integrovaný IS vytvořený na bázi integrační platformy a workflow umožňuje pružnou reakci prostředků ICT na organizační a procesní změny v rámci úřadu nebo i mimo něj.

Organizační a procesní změny jsou v takovém prostředí reflektovány na úrovni úpravy konfigurace, příp. změny procesního modelu, zatímco tradiční náročné programování je minimalizováno nebo dokonce zcela eliminováno. Dochází tak k úspoře času, kapacit, technických a finančních prostředků a v důsledku i k vyšší kvalitě a efektivitě ICT a IS úřadu. V takto koncipovaném systému se aplikace operativně přizpůsobují požadavkům procesů úřadu a nikoliv naopak.

ZAJIŠTĚNÍ VAZBY NA CENTRÁLNÍ PROJEKTY

Jedním z hlavních cílů integrace vnitřního chodu úřadu je vytvoření takového prostředí a přijetí takových opatření, které budou **garantovat schopnost úřadu připojit se k eGON službám**, a to včetně budoucích požadavků služeb, které nejsou v době návrhu k dispozici (viz např. Základní registry). Navržený koncept řeší tyto požadavky na přístup k eGON službám nasazením technických prostředků a technologií na bázi průmyslových standardů - tj. zejména prostřednictvím webových služeb (Web Services), integrační platformy a workflow.
Návrh je koncipován jako otevřený vůči stávajícím i budoucím eGON službám.
Aktuálně bude realizováno nebo připraveno připojení k následujícím eGON službám:

- Připojení k Informačnímu systému základních registrů (využití referenčních a informativních údajů pro potřeby agend úřadu, plnění katalogu služeb Registru práv a povinností údaji o službách a agendách poskytovaných úřadem, autorizace přístupu ke službám a agendám prostředky ISZR atp.).

- Připojení k Portálu veřejné správy, publikace informací o službách poskytovaných KÚ pro tento portál.

Jedním z nejdůležitějších aspektů napojení KÚ na systém Základních registrů je **zajištění výkonu role editora referenčních údajů o právech a povinnostech osob**. Výkon této role bude přednostně realizován na procesní úrovni (tj. s využitím prostředků workflow), čímž bude zaručena **vynutitelnost plnění referenčních údajů o vydaných rozhodnutích** (úředník je technickými prostředky veden k tomu, aby vydané rozhodnutí vložil přes centrální agendové systémy do Registru práv a povinností). Zároveň bude umožněno přizpůsobení vazeb rozhodovacích procesů úřadu na systém Základních registrů při organizačních či procesních změnách agend úřadu.

Návrh řešení integrační platformy s komunikačním adaptérem vně úřad zajišťuje požadavek na schopnost volání eGon služeb Základních registrů tím, že tyto služby zprostředkuje Aplikacím a nástrojům pro výkon agend (tj. modulům systému Ginis) právě Integrační platforma, která rovně zajistí jejich logování a auditovatelnost používání služeb. V pricipu tedy Integrační platforma nabídne lokálně dostupné centrální eGon služby ISZR

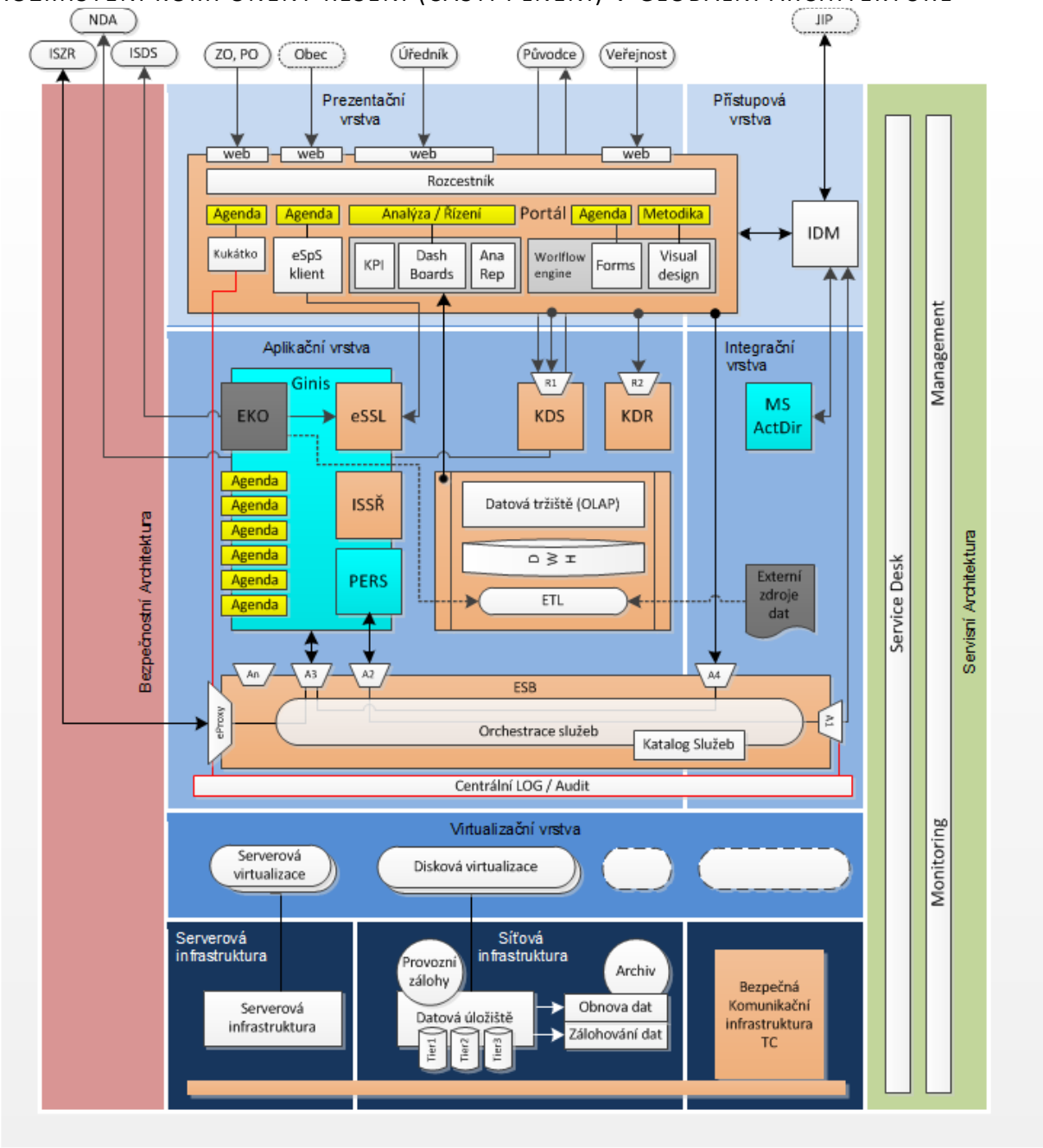
DOPLNĚNÍ GLOBÁLNÍ ARCHITEKTURY Z POHLEDU DLOUHODOBÉ UDRŽITELNOSTI

Hlavní vrstvy systému se v návrhu doplňují o **Bezpečnostní architektura** – která na základě ohodnocení aktiv organizace a doplní Globální architekturu o ošetření identifikovaných rizik, která tyto aktiva ohrožují (více v kapitole Bezpečnostní Architektura).

Obrázek: doplněná GA o Bezpečnostní a Servisní architekturu

Druhým pilířem pro zajištění dlouhodobé udržitelnosti projektu je **Servisní architektura**. Ta vzniká jasnými požadavky na provozování systému po jeho implementaci a akceptaci. Tato architektura se zaměřuje na vytvoření prostředí pro sledování a dohled provozu, poskytování služeb při vzniku nenadálých provozních situací a především poskytování služeb proaktivní podpory, které chybovým stavům předcházejí. Architekturu servisu doplňuje jasná metodika opírající se o standardy (výčet uveden v detailním popisu kapitoly Bezpečnost), bázi znalostí již vyřešených incidentů a spektrum kanálů pro příjem požadavků a v neposlední řadě o možnosti poskytování servisní podpory v místě nebo pomocí vzdáleného přístupu.

ROZMÍSTĚNÍ KOMPONENT ŘEŠENÍ (ČÁSTÍ PLNĚNÍ) V GLOBÁLNÍ ARCHITEKTUŘE

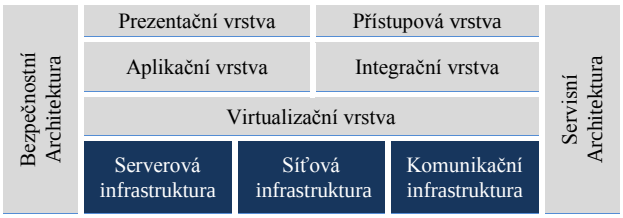


Význam barevného označení komponent, popis rozhraní a adaptérů

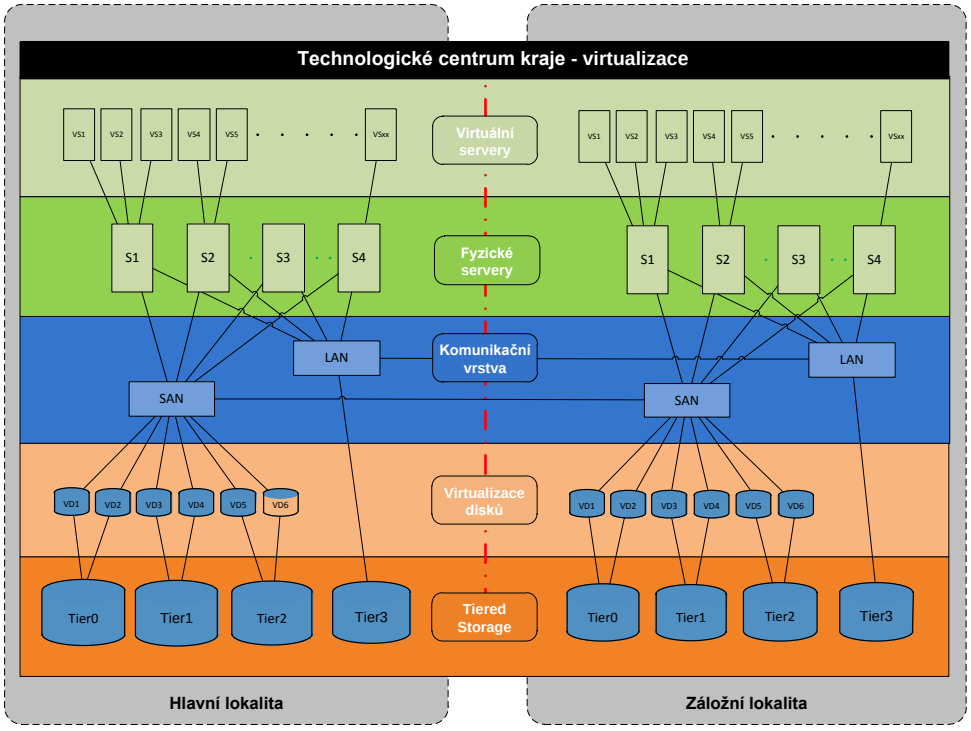
Oranžová barva onačuje komponenty, které jsou částmi plnění A-E (včetně bíle označených subčástí)
Tmavě šedá barva označuje existující IS na úřadě, nebo jejich části, které se neintegrují, ale podskytují data
Žlutá barva označuje procesy (především se jedná o výkon Agend)
Tyrkysová barva označuje IS nebo jejich části, které mají být v rámci plnění integrovány
R1, R2 – API rozhraní KDS, KDR
A1 – adaptér pro napojení IDM k ESB
A2 - adaptér pro integraci existujícího IS Personální
A3 – adaptér pro integraci IS Ginis (pro eGon služby a pro komunikaci s Portálem)
A4 – adaptér pro integraci Portálu a Workflow (An je adaptér pro možná připojení dalších IS úřadu)

Následují subkapitoly, které rozpracovávají v detailu jednotlivé architektury přičemž se postupuje jednotlivými vrstvami architektury odspodu nahoru tak jak se bude postupovat při realizaci projektu.

Virtualizace, Serverová, Síťová a Komunikační infrastruktura



Základní architektura vychází ze **studie proveditelnosti** a především ze **zadávací dokumentace** Objednatele. Předpokládá vybudování dvou nezávislých datových center s využitím HW osvědčených předních výrobců HP, Falcon Store, Hitachi atd. Infrastruktura bude vybudována s ohledem na vysoký výkon a vysokou dostupnost, odolnou proti výpadku libovolné komponenty i celého jednoho datového centra. TcK bude tvořeno dvěma rovnocennými datovými centry v uspořádání Active-Active, která budou umístěna ve dvou geograficky oddělených lokalitách.
Pro splnění náročných požadavků na dostupnost byl navržen robustní replikovaný hierarchický storage systém, který slouží jak pro provoz virtualizačních serverů, tak jako garantované úložiště. Pro serverovou virtualizaci byla zvolena platforma VMware vSphere 5.0. S touto platformou má Krajský úřad dlouhodobé pozitivní zkušenosti a budou tak minimalizovány nároky na přesun stávajících serverů a aplikací do TcK a také nároky na seznámení pracovníků Krajského úřadu. Celou filozofii TcK doplňuje zálohovací subsystém se škálovatelnou robotickou páskovou knihovnou, který umožňuje svojí licenční politikou zálohovat libovolné množství virtuálních serverů a aplikací. Podrobnější popisy jednotlivých částí a komponent TcK, jakož i způsobu jejich využití a konfigurace jsou rozvedeny v následujících kapitolách nabídky.
Primárně architektura řešení využívá virtualizace serverovou VMWARE a virtualizaci diskovou FalconSTOR. Celé řešení je budováno ve dvou datových centrech dle zadání.



SERVERY A STORAGE

Servery a storage (Tier_0 až Tier_2 jsou nabízeny na bázi produktů HP, virtualizace serverová je realizována technologií VMWARE , virtualizace disková je realizována technologií FalconSTOR. VMWARE je nabízen v nejvyšší možné edice EnterprisePlus. Pro VMWARE virtualizaci jsou nabízeny 4 hosty se čtyřmi CPU. Každé datové centrum bude osazeno jedním blade šasi HP BLc 7000, každé s 5 blade servery. Replikaci dat mezi lokalitami zajišťuje technologie FalconSTOR. Vrstva Tier3 je osazena magnetopáskovou knihovnou a garantovaným úložištěm.

DISKOVÁ VIRTUALIZACE A ZÁLOHOVÁNÍ DAT

Jako virtualizační řešení pro datová úložiště navrhujeme, instalovat plně redundantní systém spravovaný produktem FalconStor IPStor ve verzi NSS. NSS Appliance jsou vloženy do datové cesty mezi datová úložiště a servery a jsou nakonfigurovány v režimu storage clusteru, jako Active-Active módy. V případě výpadku jedné z těchto appliance, přebírá všechny její funkce zbylá appliance, aniž by došlo k výpadku aplikačních serverů.
Umístěním celé jedné poloviny tohoto Storage Clusteru do jedné serverovny a druhé polovinu do druhé, získáme DR řešení v rámci vzdálených serveroven a jsme tak chráněni i proti výpadku celé jedné lokality/serverovny. Zároveň jsou takto rozmístěna i veškerá datová úložiště a data mezi nimi jsou synchronně zrcadlena tak, aby byl zajištěn nepřetržitý chod aplikací i v případě výpadku celé jedné poloviny řešení.
Hlavní přínosy řešení jsou zejména tyto:

- **Maximální redundance všech prvků** – systém zajišťuje nepřetržitou funkčnost i v případě výpadku celého jednoho fyzického zařízení. Tzn. celý systém je navržen jako plně redundantní s možností instalace částí systému do různých serveroven tak, aby byla zajištěna funkčnost systému i v případě výpadku celé jedné serverovny. Např. u diskových polí je možno zajistit synchronní mirror mezi dvěma diskovými poli (i různých výrobců), kde v případě výpadku jednoho celého diskového pole takto zabezpečené aplikace vůbec nepoznají, že k tomuto výpadku došlo.
- **Transparentní použitelnost datových úložišť různých typů i výrobců** – systém zajišťuje možnost instalace v podstatě jakéhokoliv datového úložiště s možností budoucího rozšíření o další disky nebo externí diskové prostory, například technologie Flash disků apod.
- **Rozšiřitelnost** – jednoduchá rozšiřitelnost řešení, nejlépe pouhou instalací dodatečných disků se zachováním možnosti dalšího kapacitního rozšiřování včetně možnosti rozšíření i o další funkcionality. Další možnosti rozšiřování o další disková úložiště.
- **Možnost replikace do vzdálené lokality** – veškerá data spravovaná systémem mohou být replikována do vzdálené lokality prostřednictvím protokolu TCP/IP a to i po pomalejších linkách – volitelná součást, která není součástí nabídky.
- **Rozšířené služby zabezpečení dat** – data jsou zabezpečena pomocí synchronního zrcadlení do druhého diskového pole, aplikačně konzistentních snapshotů a CDP žurnálu, kdy je možný návrat do jakéhokoliv okamžiku v minulosti.
- **Nezávislost na výrobci hardware** – pomocí tohoto systému je možno spravovat různá datová úložiště, různých typů a výrobců.
- **Jednoduchá a jednotná správa** – konsolidovaná správa datových úložišť v rámci jedné konzole nebo webového rozhraní.

Navržené řešení je tak redundantní ve všech svých prvcích a fyzicky je představováno vždy dvěma nezávislými zařízeními, které vzájemně fungují v režimu tzv. storage clusteru. **Tento koncept zajistí nepřetržitou dostupnost diskových prostor i v případě výpadku celého jednoho zařízení nebo celé jedné poloviny řešení.**

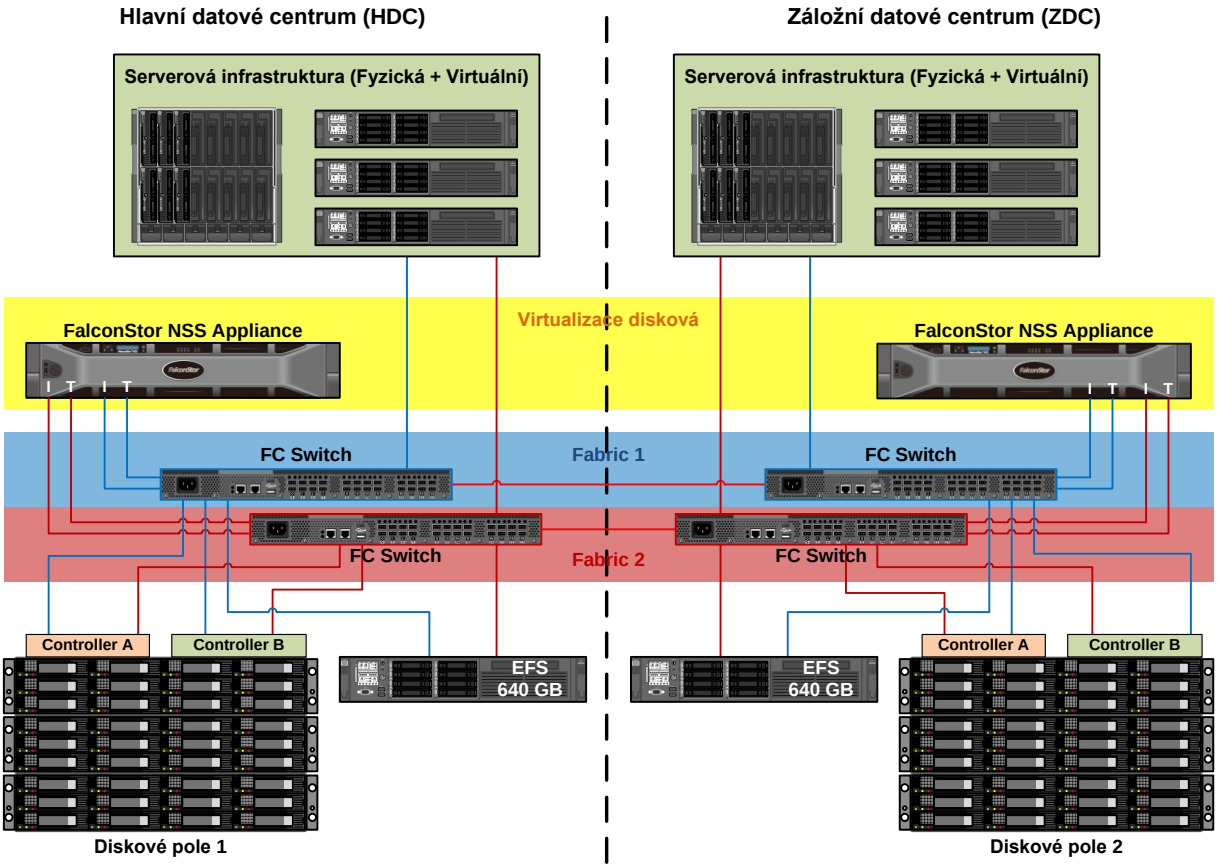
PRINCIP REDUNDANCE ŘEŠENÍ

Tato kapitola popisuje princip redundance celého řešení a jeho jednotlivých komponent:

- **Výpadek celé NSS Appliance** – v případě výpadku celého jednoho serveru s NSS Appliancí dojde k překlopení veškerých spravovaných datových služeb na druhý server s druhou NSS Appliancí, která převezme veškeré datové služby první appliance tak, že aplikační servery nezaznamenají žádný výpadek.
- **Výpadek jednotlivého disku** – disky jsou v každém diskovém poli konfigurovány v rámci svazků typu RAID, takže nedochází ke ztrátě dat.
- **Výpadek celého diskového pole** – v případě simultánního výpadku 3 nebo více disků v rámci jednoho diskového pole nebo výpadku celého diskového pole dochází k automatizovanému a transparentnímu přepnutí poskytovaných datových služeb na druhé diskové pole u všech datových prostor, které jsou zabezpečeny synchronním mirrorem. Aplikace a servery tak nepocítí výpadek diskového pole a data jsou neustále dostupná.

- **Výpadek napájení –** každý server nebo diskové pole jsou vybaveny dvěma nezávislými hot swap napájecími zdroji. V případě výpadku jednoho zdroje nebo jednoho napájení pracuje celé zařízení plnohodnotně pouze s jedním zdrojem.

Následující obrázek ukazuje zjednodušené schéma architektury řešení při rozdělení mezi dvě nezávislé serverovny a synchronní zrcadlení veškerých dat mezi těmito serverovnami:

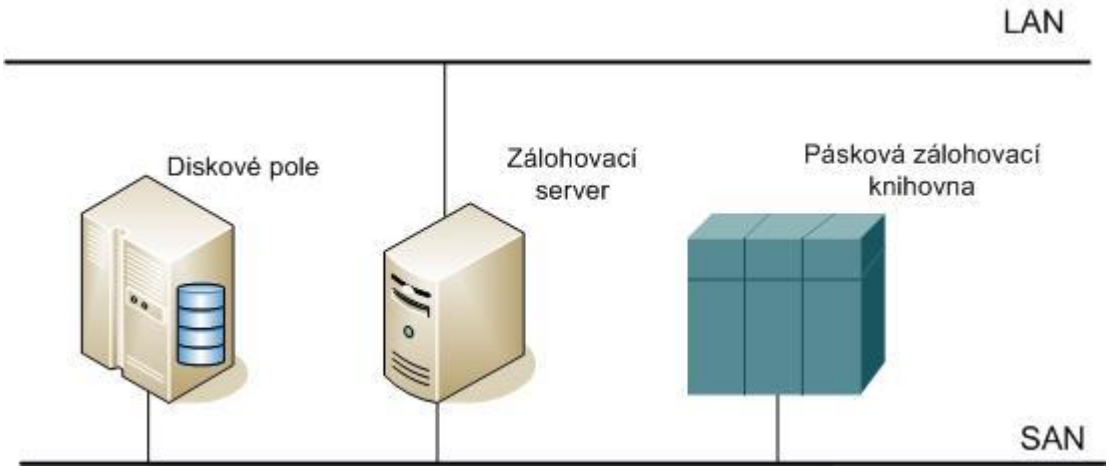


Obrázek 1: Zjednodušené schéma virtualizačního řešení

ZÁLOHOVÁNÍ

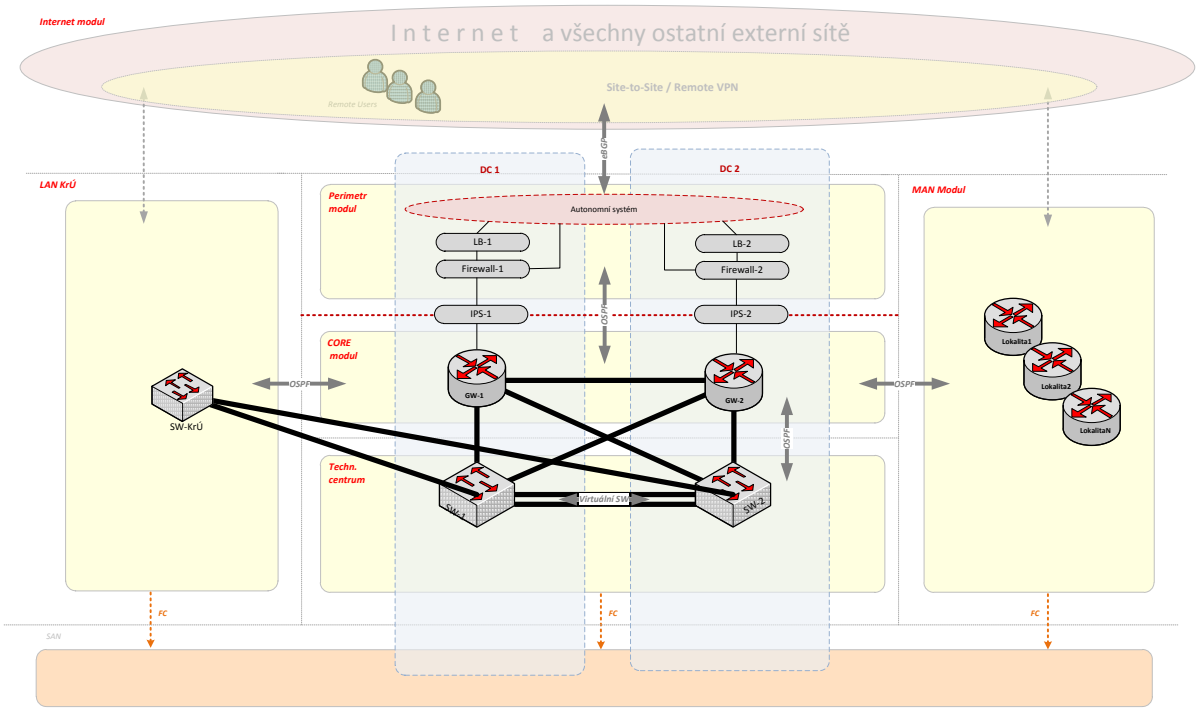
V rámci nabízeného řešení je zajištěna ochrana dat zálohováním. Kritická provozní a uživatelská data budou zálohována minimálně jednou denně, systémová data minimálně jednou měsíčně a to tak, aby byla na přijatelnou míru minimalizována možnost ztráty těchto dat i v případě zničení obou datových center.

Návrh zálohovací infrastruktury tvoří samostatnou funkční jednotku (zálohovací bod) skládající se ze zálohovacího serveru, vyhrazené části diskové kapacity na sdíleném úložišti a páskové knihovny.



TECHNICKÝ NÁVRH SÍŤOVÉ INFRASTRUKTURY

Technický návrh síťové infrastruktury je zpracován bez výjimky čistým modulárním přístupem od high-level až po low-level úroveň. V nejvyšší úrovni je definován celkový komunikační model, který definuje jednotlivé možné části inrastruktury JMK, které lze připojit do budovaného TCk pomocí dodaných komponent. Obecný model lze znázornit následujícím způsobem:



Obrázek 2: Model úrovní síťové infrastruktury

O úroveň níže, v high-level topologii TCk je design rozdělen do samostatných vrstev:

- Páteřní – páteřní přepínače,
- Agregační – agregační přepínače,
- Přístupová přístupové přepínače,
- Management LAN – management LAN přepínače,
- Servisní - loadbalancery,
- Perimetr – routery, firewally,
- Bezpečnostní – IPS,

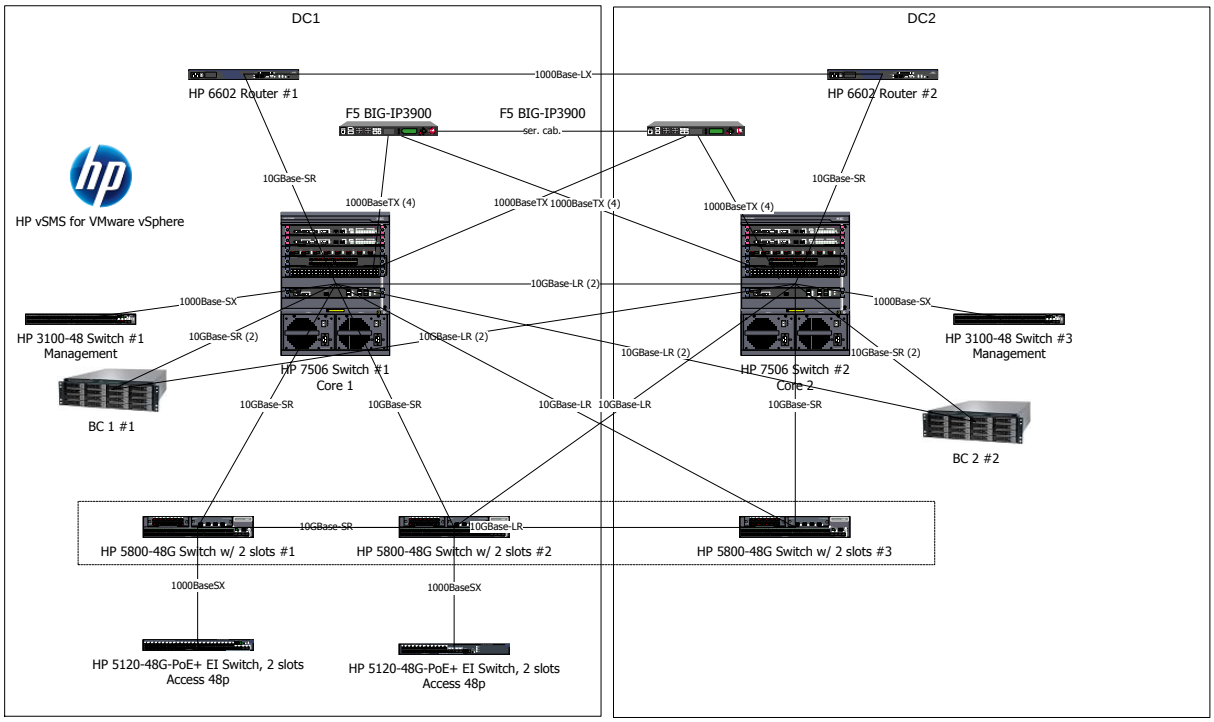
- Dohledová – síťový management systém,

kde je problematika služeb sítě dané vrstvy řešena samostatně s přesně definovanými rozhraními mezi jednotlivými vrstvami.
V low-level úrovni je design navržen jako modulární na úrovni samotného hardware a operačních systémů síťových prvků. Jednotlivé hardwarové prostředky jsou rozšiřitelné na úrovni kapacity fyzických přípojných míst k síti, jak co do jejich počtu, tak typu fyzického média podle požadavků připojovaných koncových uzlů. Zároveň je ve funkčních vlastnostech operačních systémů síťových prvků podporována škálovatelnost a rozšiřování fyzické i logické sítě.
Design komunikační infrastruktury klade důraz na:

- Splnění všech technických požadavků Objednatele,
- Integraci se současným ICT prostředím Objednatele,
- Zajištění vysoké dostupnosti komunikační infrastruktury,
- Bezpečnost komunikační infrastruktury,
- Rozšiřitelnost navrhované infrastruktury bez technických obtíží a s minimálními náklady,
- Volbu technologie vhodné do prostředí velkých organizací nároky na vysokou důvěrnost přenášených informací,
- Kvalitu servisní a technické podpory,
- Zajištění minimální ceny vzhledem ke splnění uvedených kritérií.

KOMUNIKAČNÍ INFRASTRUKTURA

Technická koncepce architektury sítě je postavena na výkonné vysoce dostupné infrastruktuře zajištěné zdvojením všech technických prostředků síťových prvků a fyzických přenosových tras. Všechny síťové prvky v jednotlivých vrstvách jsou v případě poruchy některého z prvků vzájemně zastupitelné. Samotné prvky jsou postaveny v redundantních sestavách (záložní řídící jednotky, záložní zdroje) a jsou v rámci své vrstvy i mezi vrstvami propojeny redundantními fyzickými přenosovými trasami. Propustnost sítě je dimenzována s dostatečnou rezervou a s ohledem na rozsah a povahu ICT prostředí Objednatele. Dostatečná propustnost sítě je zajištěna neblokovanou line rate architekturou přepínaných subsystémů jednotlivých vrstev s kapacitou od cca 300Gbps do 1,5Tbps v rámci vrstev (od přístupové po páteřní vrstvu). Propojení mezi síťovými prvky a samotných koncových serverových systémů jsou realizovány Nx1G a Nx10G redundantními propoji, které jsou agregovány do trunků, které zajišťují vysoce dostupnou topologii (802.3ad agregace) a rychlou konvergencí v případě poruch (max. 2ms) bez nutnosti vytváření smyček. V případě síťových prvků 3. vrstvy je vysoká dostupnost řešena pomocí router-redundancy protokolů (routery) a Active-Standby/Active-Active failover clusterů (IPS, firewally, loadbalancery).



Topologie komunikační infrastruktury

Management a dohled datového centra

Cílem je vybudování systému pro dohled a správu všech prvků datacentra. Systém bude schopen sledovat jak síťové prvky, tak i další moduly datového centra jako jsou disková úložiště, záložní zdroje napájení atd. Informace o jejich stavu budou zobrazeny přehlednou formou v centrální dohledové konzoli (management portálu). Při zjištění problému se objeví informace v centrální konzoli, díky využití řady metod pro izolaci zdroje problémů se pro správce výrazně zjednoduší nalezení primárního problémů, což vytváří dobré podmínky pro jeho rychlé vyřešení. Systém umožňuje správce také automaticky notifikovat pomocí emailu či SMS.
Kromě základní konzoly jsou součástí také moduly pro správu a sledování výkonnosti nejdůležitějších prvků datacentra. Sledování výkonnosti umožní detailnější analýzy zátěže a tím předcházet budoucím problémům, lépe plánovat případná rozšíření atd. Moduly pro správu pak zjednodušují správu síťových prvků, sledují verze firmwaru například z hlediska potřeb zabezpečení atd.

Integrační vrstva

INTEGRACE - VNITŘNÍ CHOD ÚŘADU

Integrační platforma

Integrační platforma je stěžejní částí technologického návrhu propojující nejen vnitřní chod úřadu, ale i úřad s okolním světem.

Tato platforma umožňuje asynchronní i synchronní komunikaci mezi SW komponentami. Asynchronní komunikaci, ke které je integrační platforma primárně určena, zajišťuje pomocí tzv. orchestrací, které lze v případě potřeby buď jednotlivě, nebo hromadně publikovat jako webovou službu, s automaticky generovanými veškerými náležitostmi jako je například WSDL definice, a tím umožnit jejich jednoduchou integraci s okolím úřadu. Tyto orchestrace představují předem definovaný tok a transformaci dat (zpráv) mezi několika stranami, kdy si integrační platforma sama řídí komunikaci podle předem definovaných pravidel.

Komunikace mezi jednotlivými aplikacemi probíhá pomocí vytvořených adaptérů. Tyto adaptéry definují způsob komunikace s daným rozhraním a sestávají s několika částí. Technologická část umožňuje flexibilní komunikaci s různými rozhraními, ať už se jedná o široké spektrum databázových adaptérů, komunikaci přes webové služby, adaptér pro souborový systém, nebo jiné specializované aplikační adaptéry. Dále tyto adaptéry mohou zajišťovat komunikaci s využitím šifrovaných zpráv. Další z mnoha možných funkcionalit adaptéru je validace dat zprávy. V neposlední řadě tyto adaptéry obsahují definici, jak se mezi sebou jednotlivé systémy mapují, a to hlavně na přesně definovanou strukturu interních zpráv.

V případě synchronní komunikace poskytuje integrační platforma možnost transakčního řízení, kdy pokud to podstata operace umožňuje, lze využít možnosti rollbacku atomické transakce. V případě asynchronní komunikace lze definovat rámce, ve kterých se aplikuje kompenzace dané operace.

Integrační platforma zajišťuje také management chybných zpráv, umožňuje manuální obnovení v případě nepředvídatelné chyby a tím navázání operace v místě kde, kdy byla přerušena. Je tedy stoprocentně zajištěno, že se žádná z příchozích nebo nově vytvořených zpráv neztratí.

Nedílnou součástí integrační platformy je Katalog služeb. Katalog služeb v zásadě plní 3 hlavní funkce:

- Eviduje jednotlivé základní služby (včetně popisných metadat) všech komponent a informačních systémů úřadu, které s integrační platformou mají komunikovat, využívání těchto služeb/funkcí je pouze pro vnitřní účely komunikace mezi aplikacemi, takto komunikace pomocí služeb je iniciovaná funkcemi orchestrace integrační platformy (BPEL Enginem),
- Eviduje (včetně jejich metadat) služby úřadu, které integrační platforma nabízí svému okolí, publikuje tyto služby na svém rozhraní – jedná se tedy o služby úřadu. Tyto služby mohou být složené z více základních služeb popsaných v prvním odstavci (tyto služby mohou být
- Eviduje vazby mezi vnitřními základními službami/funkcemi a vnějšími publikovanými službami (viz předchozí odrážky)

S integrační platformou je možné komunikovat výhradně prostřednictvím volání publikovaných služeb katalogu služeb. Tím je zajištěna vysoká flexibilita celého systému – volající aplikaci je v zásadě jedno kdo a jak službu provede – aplikace jen využije službu, zavolá jí s příslušnými parametry a přijme příslušnou odpověď.

Z pohledu architektury a standardů respektuje integrační platforma Business Process Management System (BPMS) a je navržena v architektuře orientované na služby (Service Oriented Architecture - SOA) a umožňuje procesní zpracování požadavků.

Cílová instalace ESB bude obsahovat logické funkční celky - služby. Ty spolu budou komunikovat přes definované rozhraní, které vychází z procesní analýzy a odpovídá business potřebám zákazníka.

Každý případ užití služby je iniciován definovaným aktérem, tím může být interní zaměstnanec přes AIS nebo jiný systém, případně nějaká automatizovaná činnost. Aktéři komunikují se službami přes definované rozhraní. Uživatelé jednotlivých IS přes grafické rozhraní, které nemusí být vázáno na stejnou technologickou platformu, jako je ESB.

K datům uloženým v úložišti budou služby vyšší než aplikační vrstvy přistupovat pouze přes aplikační Servery dále na ESB. Tím, že bude do úložiště vystaveno několik předem definovaných služeb, se zajistí jednotnost přístupu a stejná validace dat a stejná reprezentace chybových stavů v aplikaci. Zamezí se tak dvojím psaní stejných funkcionalit na jiných AIS či jiných systémů.

Workflow

Klíčovou komponentou úspěšné integrace vnitřního chodu úřadu je podpora pracovních postupů neboli Workflow. Workflow umožní zautomatizovat procesy popsané procesními modely a zároveň slouží pro efektivní elektronický oběh dokumentů na úřadě s využitím formulářů pro sběr dodatečných informací.

Tvorba workflow musí podporovat možnost flexibilního vytvoření modelů pracovních činností z předem definovaných kroků, které odpovídají částem jednotlivých procesů správního řádu, např. zahájení řízení, schválení, dožádání apod. Jednotlivé workflow jsou stavebnicí dílčích částí legislativních předpisů, které je možné v průběhu času aktualizovat, doplňovat a vzájemně zaměňovat. Při změně procesního modelu tak není nutné pracovníky přeškolovat, workflow po aktualizaci a novém spuštění bude automaticky respektovat novou verzi procesu.

Workflow podpoří i takové procesy na úřadě, které nejsou v současné době obsluhovány žádným agendovým systémem či jinou aplikací. Takové podpůrné procesy jako je např. svolávání jednání či schvalování různých dokumentů jsou tímto způsobem efektivně prováděny, řízeny a monitorovány.

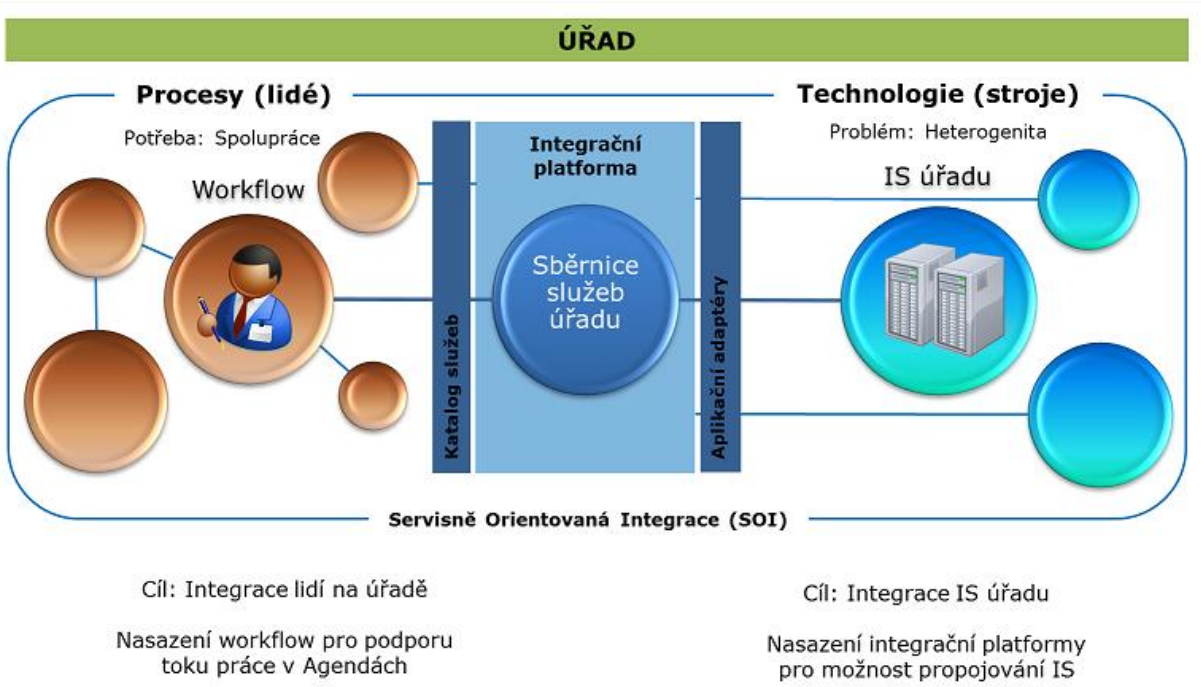
Vstupní dokumenty do workflow budou pocházet buď ze spisové služby nebo od jednotlivých pracovníků úřadu. Pokud budou účastníky prováděného procesu i subjekty mimo úřad, pak vstup i výstup musí být zaznamenáván spisovou službou a dokumenty jak vstupní tak výstupní budou uloženy v datovém úložišti spisové služby.

Portál je pak prostředek, kterým budou pracovníci úřadu komunikovat s jednotlivými kroky vyžadovanými workflow nástrojem. Uživatel tak bude vždy vědět, co a kdy má udělat, jaké kroky jednotlivých procesů na něj čekají a jaké již splnil.

Jednotlivé úlohy workflow nesmí být přiřazovány konkrétním uživatelům, ale musí být definovány na úrovni uživatelských rolí v Agendách KÚ JMK. Uživatelské role budou definovány a spravovány v modulu IDM. Teprve do takto definovaných rolí je možno přiřazovat konkrétní úředníky KÚ.

Automatická inicializace workflow a komunikace s externími aplikacemi (interními i externími) probíhá pomocí integrační platformy. Současně je zajištěno, aby u každé instance workflow bylo možné sledovat, v jakém stavu se nachází.

Propojení světa lidí a strojů v jeden harmonický celek
Integrace vnitřního chodu musí mít úzkou vazbu na procesy úřadu. Toho je dosaženo aplikováním procesního přístupu k zajištění SW nástrojů. Procesní přístup se skládá z navzájem propojených oblastí, které na sebe časově navazují a tvoří tak uzavřený celek.
Základní oblastí, které je nutné věnovat patřičnou pozornost je procesní pohled na výkon agend – zachycení všech důležitých činností, které úřad vykonává na základě zákonného zmocnění - pomocí vhodných h modelů ve vhodném nástroji, který umožní nejen proces zaznamenat, ale také s ním dále pracovat (elektronizovat jej). Nejde ale o to popsat současný stav, ale také navrhnout změny, které povedou k efektivnějšímu dosažení cíle činností v agendách. Nesmírně významné je, že moderní nástroje pro vizuální modelování nevytváří výstupy pouze v podobě papírových dokumentů, ale umožňují popis chování procesů ukládat a následně tohoto popisu využít k využít při elektronizaci - podpoře procesů IT prostředky integrační platformy a workflow.
Popisy procesů zachycené v procesních modelech slouží jako základ pro toky pracovních činností (workflow) – tedy předpis činností, jejich vazeb a časových souvislostí, které je třeba v procesu učinit.



Propojení lidí a IT prostředků mezi sebou zajišťuje Integrační platforma, jejímž axiomem je nabízení a využívání služeb zapojených informačních systémů bez ohledu na jejich lokalizaci. Workflow s její pomocí využívá konkrétní služby ostatních IS pro přímou podporu kroků/činností, které uživatel zrovna vykonává.
Posledním kamenem, který zajišťuje zpětnou vazbu reality a jejích procesních modelů je sběr údajů o provedených činnostech v rámci workflow, sběr údajů z integrační platformy, jejich statistické vyhodnocení. Měření se provádí online a výsledky zpracování úlohy mohou být znázorňovány formou grafů a tabulek. Na základě porovnání aktuálních údajů a sesbíraných agregovaných údajů za delší období z více instancí proběhlého procesu je možné vytvářet i rozdílové analýzy, jejichž výsledky zpětně ovlivňují oblast procesního modelování – přesněji: poskytují poklady pro optimalizaci procesů.
Definovaná struktura procesu v modelu a zřetelně popsané vazby na okolní procesy přináší výhody při provozu celého řešení – především objasňují rizika a dopady implementace změn v procesech, ke kterým v realitě často dochází a dává tak relevantní poklady pro rozhodnutí o provedení změn v procesu, které je v takto koncipované architektuře poskytování služeb velmi flexibilní.
Napojení Workflow systému na Integrační platformu vzniká unikátní řešení. Celé řešení dodává novou zcela funkcionalitu ale hlavně možnosti volného provázání jednotlivých dalších systémů.

INTEGRACE - VAZBA NA CENTRÁLNÍ PROJEKTY ISVS

Návrh je proveden s ohledem na budoucí připojení i takových projektů a záměr na jejich připojení reflektuje v následujících rovinách:

- Vytvoření robustní, otevřené a dostatečně pružné integrační infrastruktury na bázi průmyslových standardů tak, aby bylo umožněno bezproblémové napojení v na centrální projekty VS (především ISZR a ISDS).

- Zohlednění dostupných analytických podkladů (tj. zejména popis komunikačního rozhraní ISZR) a vytvoření funkčního adaptér pro volání eGon služeb.

Návrh předpokládá napojení úřadu na centrální projekty v rozsahu dle následujících odrážek.
Základní registry (integrační bod k ISZR) budou připojeny na úrovni:

- Vytvoření přístupového adaptéru k systému Základních registrů v rozsahu funkčních prototypů následujících rozhraní:

    - Možnost čtení referenčních a informativních údajů z dílčích registrů a jejich centrálních AIS, na základě oprávnění, které vzniklo přihlášením Agend OVM k jejich výkonu,

    - Editace referenčních údajů Registru práv a povinností v roli editora referenčních údajů o rozhodnutích OVM,

    - Autorizace přístupu ke službám a agendám prostředky JIP,

    - V budoucnu plnění AIS RPP Modelovacího údaji o modelech procesů úřadu, vazbách těchto modelů na agendové činnosti a Workflow,

- Modifikace Agend zahrnující vydání rozhodnutí tak, aby vložení uložených práv a povinností do RPP bylo jejich nepominutelnou součástí,

- Možné zpřístupnění centrálních AIS RPP v Portálu úředníka formou rozcestníku.

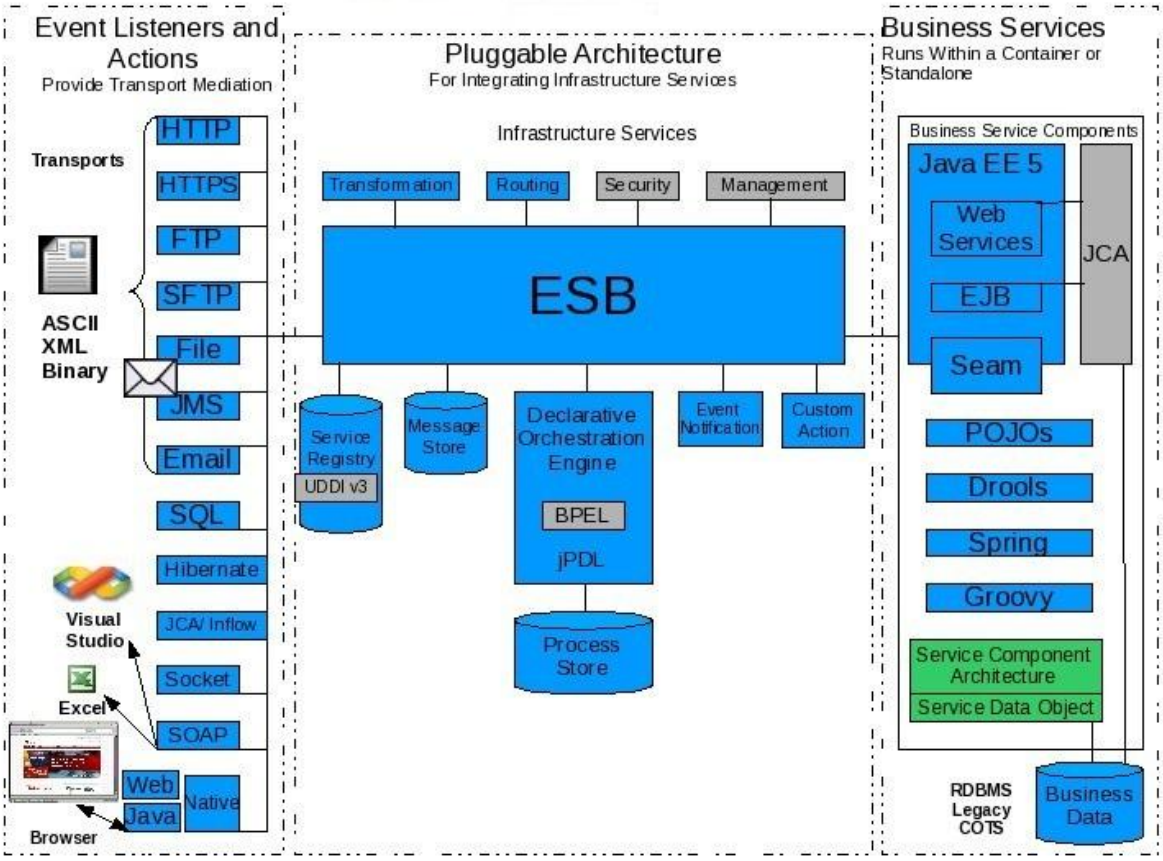
Datové schránky budou připojeny prostřednictvím Elektronické spisové služby. Integrace vnitřního chodu úřadu se problematika datových schránek dotýká pouze zprostředkovaně, vazbou přes Elektronickou spisovou službu:

- Automatizovaná distribuce podání osob, úřadů a organizací z Elektronické spisové služby do agend informačního systému.

- Odesílání agendových výstupů prostřednictvím Elektronické spisové služby, která zajistí jejich distribuci v souladu s platnou legislativou, tj. mj. doručením datové schránky, pokud ji má adresát zřízenou.

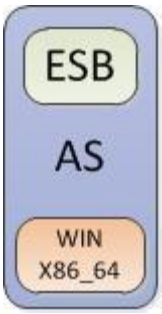
UNITŘ SBĚRNICE SLUŽEB ÚŘADU

Integrace systému bude tvořena jako aplikace na zakázku pomocí vlastního vývoje nad produktem JBoss Enterprise SOA Platform. Budou dodány nástroje a dokumentace pro snadné ovládání, konfiguraci a administraci systému, případně vytvoření funkcionality svépomocí.
Integrační platforma, kterou společnost AutoCont a.s. nabízí, je z pohledu architektury řešena jednotným a jednoduchým principem, kterým je integrace různých systému přes Enterprise Service Bus (dále jen ESB). Tento návrh vychází z uznávaného konceptu Service Oriented Architecture (dále jen SOA).



Obrázek - zobrazení obecného zapojení ESB v systému integrace.

Ve světě IT je SOA brána jako seznam metodik pro návrh a vývoj aplikací ve formě kompaktních služeb. Tyto služby jsou dobře definované business funkce, které jsou vybudovány jako jednotlivé komponenty, které mohou být znovu použity pro jiný účel. Principy návrhu SOA jsou použity jak ve fázi vývoje, tak u fáze integrace. Tyto principy jsou ověřeným standardem.



SOA obecně poskytuje způsob pro konzumenty služeb (např. portály, webové aplikace, tlustí klienti), aby měli přehled o poskytovaných službách. Například, několik různorodých oddělení v rámci společnosti, vyvine a nasadí několik služeb implementovaných v různých jazycích. Klienti je budou moci využívat ve svůj prospěch využívající přesně popsaného rozhraní služeb.

Servisní orientace vyžaduje volné spojení služeb s operačními systémy a dalšími technologiemi, které tvoří základ aplikace. SOA odděluje funkce do samostatných jednotek, nebo dalších služeb, které se vývojářům zpřístupňují přes síť s cílem umožnit uživatelům kombinovat a znovu je použít. Služby a spotřebitelé navzájem komunikují a předávají si data v přesně stanoveném formátu.

SOA může být viděna v kontinuu, ze starších konceptů pro distribuované výpočty a modulární programování. Dnešní trend chápání SOA je mashup mezi SaaS a cloud computing (který někteří vidí jako potomky SOA)

Návrh, analýza, nasazení systému vychází z předpokladu, že Enterprise Service Bus (dále jen ESB) je uzlem komunikačních cest v systému. Současně s ním je potřeba nasadit aplikační server, ve kterém dané ESB bude puštěno.

ESB v navrženém systému slouží pro definování jednotného stylu přístupu k informacím/datům k vytvoření jednotného procesu napříč různými informačními systémy s jednotnou správou jednoduchým konfigurováním cest a jednoduchou změnou pravidel směřování.

ESB podporuje celou škálu protokolu a je maximálně otevřená pro napojení různorodých systému. To, které protokoly budou využity, bude předmětem analýzy současného stavu a systémů, které bude

nutné integrovat. Již teď lez říci, že podporované protokoly ESB jsou http/https, ftp, sftp, file, jms, e-mail, sql, hibernate, JCA, SCA, SOAP.

Klíčové vlastnosti SOA:

- volné svázání systémů
- nezávislost na architektuře volaného a volajícího
- přesná definice zpráv
- využívání již jednou napsaných služeb
- snadné napojení dalších systému
- možnost orchestrace pomocí BPEL/BPMN2
- možnost vlastními silami měnit logiku volání služeb
- oddělení prezentační vrstvy od místa, kde jsou data uložena/zpracovávána

NAPLNĚNÍ ÚLOHY INTEGRACE

Hlavní úlohou integrační vrstvy je propojení nově dodaného IDM, některé vybrané systémy a jejich některé funkcionality, integrovat aplikace s Portálem úředníka/úřadu, IS pro podporu IT správních řízení, Elektronickou spisovou službou, systémem HR, Ekonomika a nově vytvořených systému dodaných v rámci této nabídky a integrací na ZR.

Cílem výběrového řízení je zvýšení transparentnosti veřejné správy, efektivnosti a snížení administrace pro občany a instituce. Tento cíl dosáhneme zavedení jednotné integrační vrstvy, která umožní napojení různorodých systémů a jejich vzájemnou komunikaci. Auditní činností integrační vrstvy dosáhneme transparentnosti a snadného dokazování nepochybení úřadu v jeho postupování. Integrováním jednotlivých systémů zmenšíme administrativní kolečko a ulehčíme komunikaci občanům s úřady. Úředník bude mít díky provázanosti systémů takřka všechny informace v jednom místě.

Navržený koncept splní následující cíle:

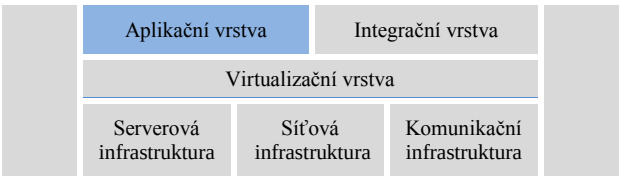
- Zajistí schopnost vzájemné komunikace mezi základními registry a agendovými informačními systémy (AIS) zajišťujícími vykonávání agend v působnosti Krajského úřadu Jihomoravského kraje vykonávaných dle platných právních předpisů
- Bude respektovat členění činnosti (agend, služeb) veřejné správy zajišťovaných Objednatelem s možností řešit lokální odlišnosti a jejich informační podporu
- Člení pracovní pozice a aplikační role ve vazbě na personalistiku, práva a povinnosti rolí a probíhající změny ve vztahu k základním registrům
- Zajistí kvalitní systém řízení uživatelských oprávnění k funkcím a datům používaných informačních systémů
- Realizuje integrační vazby mezi nově dodanými aplikacemi a systémy.

Dané cíle umožní řešit platforma SOA, která volně svazuje systémy – nejsou na sobě technologicky závislé. Volným svázáním jednotlivých systémů můžeme řešit lokální odlišnosti.

Provázáním nového IDM s jednotlivými AISy a ISZR bude systém schopen respektovat členění pracovní pozice a aplikační role v JMK a integrovaným aplikacím zprostředkuje eGon služby Nový IDM bude mít kvalitní webové rozhraní, kterým bude moci nastavit oprávnění uživatelům v kraji. Systém bude zohledňovat implementační a technologické standardy specifikované v zadávací dokumentaci pro oblast „Technologické centrum kraje“

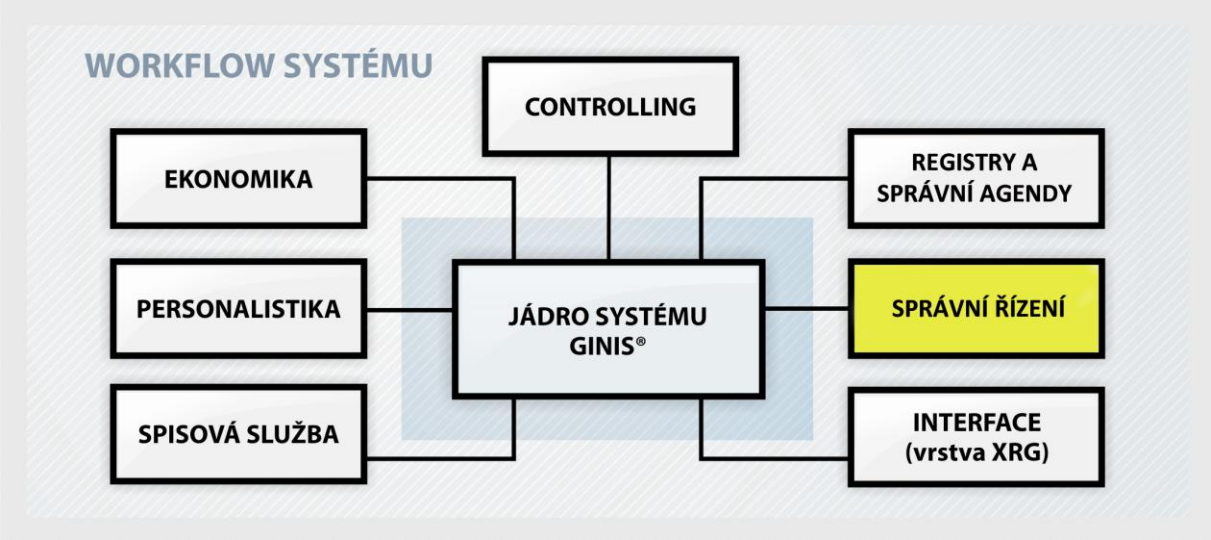
Aplikační vrstva

Globální Architektura řešení			
Prezentační vrstva	Přístupová vrstva		



STÁVAJÍCÍ A NOVÉ APLIKACE PRO PODPORU VÝKONU AGEND OD JEDNOHO VÝROBCE

Informační systém GINIS je tvořen jádrem s administračními moduly a dále pak subsystémy Ekonomika, Mzdy a personalistika, Controlling, Spisová služba, Registry a správní agendy. Jednotlivé agendy používají společnou vrstvu workflow. Agendy komunikují mezi sebou přes společnou vrstvu, na které jsou postaveny. Tím je zajištěna funkční a procesní propojenost všech agend, u kterých existuje nebo může existovat logická vazba.



Obrázek: Požadovaná funkcionalita jako jeden z modulů systému Ginis

Požadavek na dodávku funkcionality pro Evidenci správních řízení je vyřešen nejlepším možným způsobem – dodávkou modulu Správní řízení, od jednoho výrobce - Zhotovitele systému Ginis. **Takováto integrace na aplikační vrstvě se vyznačuje významnou ochranou investic do stávajícího IS Ginis, který je provozován na úřadě.**

Dalším nepominutelným faktem je, že systém Ginis bude komunikovat v jednom bodu s Integrační platformou a tedy jedním rozhraním (adaptérem) se zprostředkuje možnost používat eGon služby publikované na vnějším rozhraní ISZR. **Takováto integrace zajistí pracovníkům v Agendách OVM transparentní dostupnost služeb eGON Základních Registrů v jejich Lokálních AIS.**

Napojení subsystému IDM k integrační vrstvě, která je dále připojena na moduly systému Ginis zajistí funkcionalitu jednotného místa správy identity jednotně pro všechny moduly systému Ginis, jak nově dodávaných (Správní řízení), tak už existujících (Personalistika)

Tři výše uvedené funkce realizované zcela nezávisle prostřednictvím Integrační platformy považuje Zhotovitel za největší přidanou hodnotu řešení a významnou ochranu dosavadních investic Objednatele.

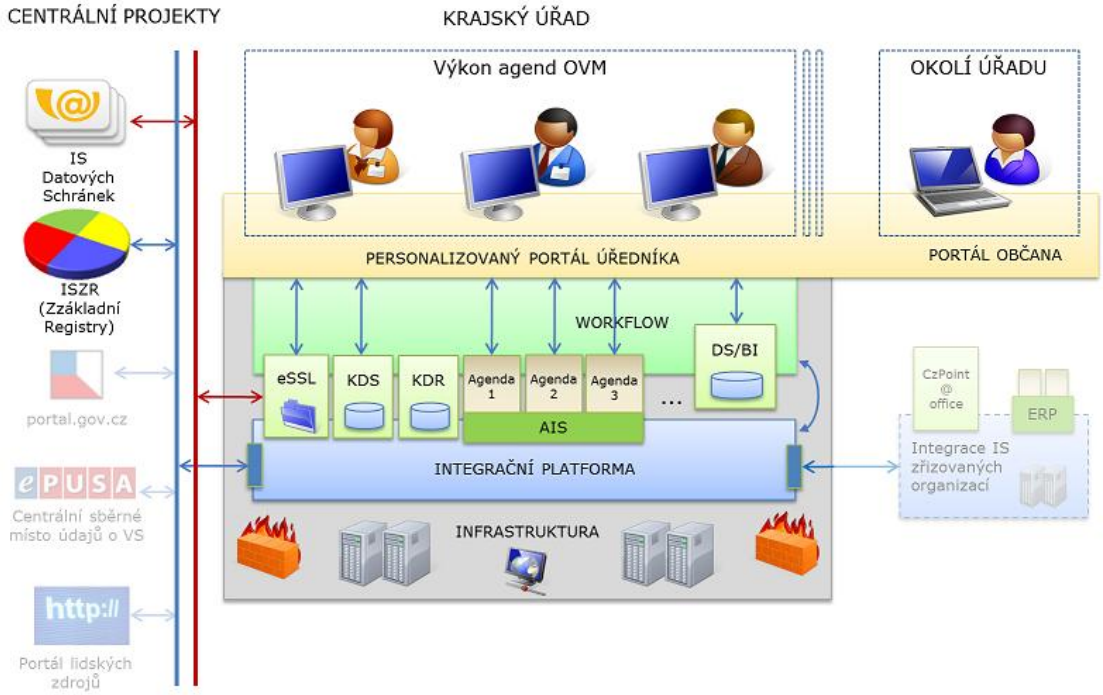
Prezentační a přístupová vrstva

PORTÁL ÚŘEDNÍKA

Cílem předloženo návrhu je vytvořit takové prostředí, které je možno dále rozvíjet vlastními silami pracovníků IT úřadu s podporou Zhotovitele formou servisních a rozvojových služeb, tedy bez nutnosti hlubokých programátorských zásahů Zhotovitele s těmito vlastnostmi:

- Uživatelé budou k systému přistupovat prostřednictvím webového prohlížeče,
- Bude realizována Integrace vybraných agend do jednoho uživatelského portálu, který umožní práci s různým webovým a aplikačním obsahem, dokumenty a formuláři,
- Návrh počítá s publikací informací z analytické části (DS/BI) v prostředí portálu,
- Díky navrženému vizuálnímu návrháři Workflow je možné definování a provoz různých typů workflow,
- Navržený systém je modulární a umožní značné rozšiřování funkcionality vlastními kapacitami úřadu, bez nutnosti externí dodávky dalších komponent.

Přístup pracovníků úřadu a občanů ke službám poskytovaných v rámci řešení je v maximální možné míře unifikován a centralizován do portálového prostředí, viz "Portál úředníka" a "Portál občana". Ve stejném portálovém prostředí se také odehrávají aktivity související s řízením interních procesů úřadu - tj. např. zadávání úkolů, příprava a zpracování podkladů, zpřístupnění podkladů z externích (typicky z centrálních projektů) a interních zdrojů (typicky z agend úřadu), komunikace mezi pracovníky úřadu, komunikace s občany, hlídání termínů atp.



Obrázek: Cílový koncept spolupráce komponent a začlenění jejich rozhraní do portálu

Portál slouží jako primární rozhraní mezi uživatelem a informačními systémy úřadu. Integruje do svého prostředí SW komponenty, se kterými uživatel pracuje. Cílovým stavem je sjednocení uživatelského vzhledu a stylu práce všech pracovníků začleněných do výkonu agend úřadu. Vytvoření jednotného uživatelského prostředí na bázi webového portálu je zvoleno z následujícího důvodu:

- klientem je webový prohlížeč (veškeré aplikační změny jsou realizovány výhradně na serveru)
- při použití portálového řešení je možné využít nativní služby portálu (rozcestník, vyhledávání, sdílené kalendáře, diskuze, pracovní weby) pro týmovou spolupráci uživatelů, čímž dojede ke zvýšení efektivita jejich práce

Portál dále umožní vytvoření struktury týmových webů určených pro sdílení informací v rámci jednotlivých odborů úřadu, návrh a nastavení oprávnění přístupu do jednotlivých částí portálu, dostupnost prostředí pro správu webového obsahu a dokumentů, které primárně neprocházejí přes spisovou službu (typicky pracovní dokumenty) včetně systému správy metadat těchto dokumentů.

PŘÍSTUPOVÁ VRSTVA

Systém IDM (na konceptu není zakreslen) bude tvořen jako aplikace na zakázku pomocí vlastního vývoje. Bude vytvořen jako tenký (webový) klient, pomocí kterého bude umožněna správa ostatních identit ostatních IS. Veškerá komunikace bude prostřednictvím služeb nad zabezpečeným protokolem https a bude plně integrován s prostředím Portálu úředníka.
Systém IDM, který Zhotovitel je z pohledu architektury a řešení založen na jednoduchém principu, kterým je integrace různých systémů, založená na obecném, moderním principu třívrstvé architektury, kde střední vrstva je řešena pomocí SOA (Service Oriented Architecture). Pro komunikaci IDM s jednotlivými systémy AD bude využito komunikace pomocí protokolu LDAP.
Toto řešení je efektivní, výkonná platforma vhodná jak pro IDM samotné, tak i pro integraci různých, na sobě nezávislých systémů. Pro komunikaci mezi IDM a jednotlivými Active directory bude využito nativní komunikace pomocí LDAP protokolu.

ZAČLENĚNÍ ANALYTICKÉ KOPONENTY DO PORTÁLU

Zhotovitel s výhodou použil prostředí portálu pro začlenění nástrojů dodávaných v části plnění: Datové sklady a nástroje Business Intelligence, které umožní zobrazování analytických výstupů, reportů a definovaných ukazatelů. Toto prostředí samozřejmě poslouží i pokročilým analytickým uživatelům, kteří potřebují disponovat nástroji typu OLAP (On Line Analytic Processing), tedy nástrojů pro interaktivní analýzy a získávání informací pro kvalifikované rozhodování.
(Pozn. Detailní informace o možnostech a principech funkce těchto nástrojů je uvedeno v kapitole 0 **Detailní popis řešení - Datové sklady, manažerské informační systémy a nástroje Business Inteligence JMK**).

Bezpečnostní a Servisní architektura

BEZPEČNOSTNÍ ARCHITEKTURA

je z hlediska požadavku na koordinaci bezpečnosti napříč jednotlivými částmi plnění řešena na společném a jednotném základě spojujícím technickou a procesní oblast řešení. Jedná se o komplex vzájemně provázaných aktivit, které vyžadují pokrytí identifikovaných rizik na všech úrovních, ať už se jedná o celý projekt, nebo o jednotlivé dílčí části.
Globálně aplikovatelné bezpečnostní požadavky vyplývající z uvedeného schématu celkové architektury a popsané v této kapitole budou závazné pro řešitele všech částí při zohlednění specifických potřeb té které části, a to zejména z důvodu zajištění vzájemné koordinace a kompatibility.
Z těchto důvodů navrhujeme řešení architektury bezpečnosti jako samostatnou kapitolu - bezpečnostní projekt. Výhodou tohoto přístupu je především celistvost a účinnost realizace činností, jako je analýza rizik, příprava projektové a provozní bezpečnostní dokumentace, zavádění procesů informační bezpečnosti, penetrační testování či havarijní plánování. Současně s tím bude zajištěna celková integrita bezpečnostní dokumentace vytvářené jednotlivými řešiteli prostřednictvím supervize jejího zpracování. Cíle vybudování jednotné bezpečnostní architektury byly stanoveny na základě potřeby:

- zajištění a prosazení bezpečnosti ve všech fázích životního cyklu informačních a komunikačních technologií;
- vybudování jednotného systému řízení bezpečnosti napříč všemi oblastmi ochrany informací;
- stanovení globální bezpečnostní politiky a uplatňování stejné metodiky a pravidel pro hodnocení bezpečnosti;
- zajištění efektivního způsobu dohledu na řešení bezpečnosti ve všech částech plnění projektu;

Primárním požadavkem je koordinace procesů řešení bezpečnosti prostřednictvím společné bezpečnostní základny. Ta zahrnuje globální část (platnou pro všechny oblasti plnění) a jednotlivé části týkajících se konkrétních oblastí z hlediska naplňování bezpečnostních požadavků.
Struktura rozdělení aktivit řešení bezpečnosti je znázorněna na schématu „Globální architektura řešení“, z níž je patrné, že se bezpečnost prolíná celou hierarchií a jsou do ní integrovány všechny popisované části infrastruktury.
Řešení bezpečnosti je založeno na definici bezpečnostních cílů a z nich vyplývajících bezpečnostních požadavků a mechanismů. Jejich úkolem je postihnout globální i specifické aspekty bezpečnosti nejen v případě analýzy rizik a v bezpečnostní dokumentaci, ale dále v rámci zavedení do praxe v běžném provozu, a následně v rámci bezpečnostního auditu, testování a vyhodnocování účinnosti celého systému.
Koordinace bezpečnosti se vztahuje jak k přípravě (návrhu), tak k vlastní realizaci částí plnění. Aby byla zajištěna v celém životním cyklu, měla by probíhat v následujících krocích:

- návrh bezpečnostního projektu zahrnujícího analýzu požadavků a bezpečnostních aspektů,
- stanovení bezpečnostních cílů,
- realizace analýzy rizik,
- návrh efektivních bezpečnostních opatření ve formě plánu bezpečnosti,
- návrh provozní bezpečnostní dokumentace pro všechny oblasti plnění
- závěrečný audit systému řízení bezpečnosti informací.

SERVISNÍ ARCHITEKTURA

Servisní architektura je souborem nástrojů a předem definovaných procesů pro zajištění dlouhodobé udržitelnosti projektu.

V rámci servisní architektury je Hlavní přístupovým a komunikačním bod této architektury (Single point of contact - „SPOC“). Pro zákazníky a smluvní partnery Objednatele je tento bod vybaven nástrojem Service Desk, zajišťující procesní komunikaci a následné řešení požadavků eskalací na řešitelské týmy a koordinaci s Zhotoviteli ICT třetích stran. Služby Service Desku Zhotovitele v současné době zajišťuje více jak 40 vyškolených zaměstnanců ve 4 lokalitách v České republice, kteří v současné době hladce řeší více jak 120.000 požadavků ročně. Toto centrální kontaktní místo je dostupné v režimu 24x7po celý rok.

Základním pojmem v této architektuře je z procesního úhlu prohledu Servisní služba. Tyto Servisní služby budou zahrnovat odstraňování závad, provozní správu, expertní podporu, provádění změn provozní dokumentace, monitoring HW a základního SW. Základními oblastmi pro poskytování jsou:

- oblast reaktivní podpory (řešení vzniklých problém)
- oblast proaktivní podpory (předcházení problémům)

Pro poskytování služeb v oblasti reaktivní podpory - řešení nenadálých událostí typu bezpečnostní incident má Zhotovitel zpracovány procesní schéma (uvedené v kapitole 6.7), které detailně popisují způsob řešení toho typu incidentů, jednotlivé kroky a ošetřeny možné stavy.

Pro poskytování služeb v oblasti proaktivní podpory – bude Zhotovitel poskytovat:

- **Výkon provozní správy a činností prováděných automaticky bez nutnosti jejich aktivace:**
  - pravidelné prohlídky
  - poskytovat informace o bezpečnostních rizicích
  - poskytovat informace o platnosti podpor
  - bude aplikovat bezpečnostní opravy komponent
  - bude instalovat nové verze SW podle předem stanoveného postupu stanoveného v provozním řádu
- **Služby obsahující činnosti prováděné na vyžádání pro provozní účely:**
  - Příjem požadavku na provedení provozní správy v režimu 7x24
  - Provedení zálohy konfigurací/nastavení před provedením požadované provozní činnosti
  - Ověření možných dopadů realizace požadavku na zachování funkcionality technologického celku
  - Upozorňovat na rizika Objednatele požadavku o možných důsledcích provedení požadavku
  - Posuzovat možný negativní dopad zadaného požadavku na infrastrukturu Objednatele
  - Provádět simulaci změny v testovacím prostředí

Dále bude poskytováno Provedení požadované činnosti provozního charakteru na vyžádání:

- změny konfigurace
- SW úprava funkčnosti menšího rozsahu
- Provedení požadavku otestování funkčnosti dotčeného technologického celku

Konečně doplňující třídou Servisních Služeb bude Expertní podpora v oblastech

- konzultační služby (telefonicky, emailovou komunikací, nebo v lokalitě Objednatele),
- řešení problémů (telefonicky, emailovou komunikací, nebo v lokalitě Objednatele),
- zajištění eskalace problémů na mezinárodní centra výrobců HW/SW,
- předkládání návrhů na rozvoj systémů - přidělení technického specialisty zhotovitele (systémového architekta), který bude mít přehled o provozovaných systémech, jejich architektuře a bude předkládat návrhy rozvoje a poskytovat konzultační služby související s provozem a rozvojem těchto technologií,
- zpracování oponentních posudků ke studiím, analýzám, technické dokumentaci předložených Objednatelem (nebo jeho partnerem) ovlivňujících provoz nebo rozvoj spravovaných technologií,
- možnost otestování nových technologií a technických řešení na prototypovém modelu,
- poskytování služeb v lokalitě Objednatele nebude mít dopad na cenu poskytované služby (cestovné a další náklady jsou zahrnuty v ceně služby),
- rozsah poskytovaných služeb 20 hodin měsíčně, nevyčerpané hodiny lze převádět neomezeně v rámci kalendářního roku,
- Součástí služby je i pravidelné reportování o poskytování služeb expertní podpory.

Všechny výše uvedené služby budou poskytovány na základě ujednání o SLA. Jejich detailní nastavení je popsáno v kapitole 6.7.3 Garantovaná úroveň podpory (SLA).

Nedílnou součástí poskytovaných služeb v rámci provozní správy bude:

- zaznamenání změn do technické provozní dokumentace,
- uložení informací o provedení provozního zásahu do elektronického systému pro příjem a evidenci požadavků na technickou (servisní) podporu

Součástí poskytování servisních služeb podpory bude:

- nepřetržitý 24x7 proaktivní monitoring dostupnosti servisovaných zařízení,
- reakce na vzniklý mezní stav v uvedené době od jeho vzniku,
- nahlášení vzniklého mezního stavu určenému zástupci Objednatele,
- v dohodnutých případech okamžité zahájení řešení vzniklého mezního stavu (seznam situací bude podléhat souhlasu Objednatele a bude stanoven a aktualizován na základě návrhu Zhotovitele),
- možnost změn některých parametrů monitoringu (změna intervalu zjišťování stavu zařízení, změna počtu zachycených událostí, po nichž je vyhodnoceno zařízení jako nedostupné apod.),
- poskytování reportů o zaznamenaných mezních stavech, úpravy reportů na základě požadavků Objednatele.

Kvalita návrhu nabízeného řešení s ohledem na možnosti jeho budoucího rozvoje a dlouhodobou udržitelnost systému, možnosti údržby, provozu a rozvoje Objednatelem

Udržitelnost systému v provozu a jeho rozvoj

Základním faktorem ovlivňujícím udržitelnost systému v provozu, je dle mínění Zhotovitele dostupnost celého řešení, tj. pokrytí rizik spojených především s **výpadky Technologického centra**. Proto se Zhotovitel soustředil oblasti, které tyto výpadky eliminují ve dvou základních rovinách:

V oblasti zabezpečení obsahu informačních systémů proto výpadkům, které mohou zapříčinit ztrátu dat, navrhuje Zhotovitel zajistit **efektivní údržbu a správu** celého systému dodanými prostředky pro robustní **provozní zálohování s možností obnovy systému.** Ochrana proti ztrátě dat je navrhována pro všechny důležité oblasti řešení:

- **Zálohování dat souborových systémů serverů** – v rámci návrhu řešení lze přidávat **neomezený počet dalších serverů**, není potřeba žádná dodatečná licence HP DataProtectoru. V reálném nasazení je doporučeno výrobcem počet zálohovaných serverů pro jeden řídící zálohovací server omezit na 100-150, toto omezení je směrováno k reálným možnostem přenosu dat z takového počtu serverů v požadované době, která je k dispozici pro provádění jejich záloh.
- **Zálohování dat databází** - v rámci návrhu řešení lze jednoduše přidat zálohování dat dalších databázových serverů, pro každý přidaný databázový server je nutno zajistit další licenci typu *HP DataProtector Online backup*.
- **Zálohování na úrovni virtualizační vrstvy** – v rámci návrhu řešení lze přidat zálohování dat dalších virtualizačních serverů, tedy zálohování obrazů virtuálních serverů na těchto virtualizačních serverech běžících. Pro každý přidaný virtualizační server je nutno zajistit další licenci typu *HP DataProtector Online backup*.
- **Vlastní prostory pro umisťování záloh** – jejich kapacitní rozšiřitelnost je neomezená. Omezením jsou pouze reálné propustnosti LAN a SAN infrastruktury a diskových polí pro provedení záloh rostoucích datových objemů v čase. Pro každé rozšíření na straně úložišť pro data záloh je nutno zajistit další licence a to typu *HP DataProtector Advanced Backup to Disk* pro diskový prostor a *HP DataProtector Drive Extension* pro zálohovací knihovny.

V oblasti **předcházení stavům**, které mohou způsobit výpadky systému

- nasazením prostředků pro **dohled nad chodem celého řešení** s možností včasného a proaktivního předcházení chybovým stavům
- nasazením nástrojů pro co **nejrychlejší lokalizaci problémů** síťového provozu a poruch v infrastruktuře, které představují základní stavební kameny celého systému.

Udržitelnost dodaného řešení v provozu je z pohledu vyšších vrstev systému vnímána Zhotovitelem **také jako schopnost realizovat změny funkcionality,** na které mají vliv změny v **organizaci úřadu** a změny, které jsou vyvolány vnějšími vlivy, především měnící se **legislativou**. Tyto vnitřní a vnější podněty, vedoucí k potřebám změnit funkcionalitu systému, jsou v předkládaném řešení schopny zajistit komponenty:

- **V oblasti podpory práce uživatelů je to především flexibilní Workflow** nástroj pro zajištění podpory pracovníků úřadu se schopností rychlé realizace změn vyplývajících z nových požadavků na změny v organizaci úřadu, efektivního řešení pro zastupitelnost osob a změn v řízení toku práce.
- **V oblasti schopnosti komunikovat s okolím a zapojovat další interní systémy do této komunikace je to Integrační platforma**, která svojí nativní architekturou orientovanou na služby (SOA) byla přímo **vytvořena pro to aby zvládala požadavky na rychlé změny** v nastavení komunikace mezi jednotlivými IS Objednatele formou volání služeb a proto je

koncipována jako „stavebnice“ umožňující doplňovat a rozšiřovat dílčí komponenty, rozhraní a aplikačními adaptéry, díky čemu může Objednatel udržovat řešení v chodu díky vlastnostem:

- Systém integrace je navržen s ohledem na jeho budoucí rozšíření, které je možné po analýze typu napojení, identifikaci seznamu potřebných operací, které je potřeba řešit v rámci integrace s následnou implementací změny,
- Integrační platforma (ESB) bude nainstalována v clusterovém prostředí tak, aby uspokojila potřebu práce v Agendových IS. Horizontální škálovatelnost bude dostupná díky principu SOA, který je základem definice ESB. Konfigurace a připojení další možné instance ESB je veřejně publikováno a detailně popsáno v dokumentaci.
- ESB ke svému běhu potřebuje transakční úložiště, pro zajištění perzistence komunikace prostřednictvím webových služeb. Otevřenost sběrnice je dána tím, že je možno použít většinu venderovských databází. Napojení ESB na DB je provedenou přes technologie aplikačního serveru „data source“. Tento „data source“ je registrován na aplikačním serveru a jeho konfigurace je popsána v dokumentaci. Pro rychlý běh integrační vrstvy je kritické, aby byla instalace DB na stejném segmentu sítě a zápisy/čtení do/z DB nebyly zpomalováni infrastrukturou sítě. Kvůli dostupnosti integrační vrstvy bude DB instalována v clusteru. Data ESB (systémová data) budou uložena odděleně od dat AIS (komunikační data) a jiných systémů krajského úřadu.

Detailní popis způsobu **dohledu nad chodem klíčových komponent systému** bude popsán v samostatné části dokumentace, kde budou popsány scénáře řešení možných problémů a postup jak se jim předcházet a jak vyřešit pokud nastanou. Již teď lze říci, že údržba systému se bude skládat z pravidelného monitoringu a kontroly dostupnosti jednotlivých služeb integrační platformy a napojených systémů.

Neposledním faktorem ovlivňujícím udržitelnost systému je dle mínění Zhotovitele **pokrytí rizik spojených s aktivy Objednatele**, které bude řešit Zhotovitelem navržená implementace **Komplexní Informační Bezpečnosti** pro oblasti plnění A-E, které se opírá o normu ISO 27001 a dále o postupy řešící kvalitativní a bezpečnostní požadavky dle zák. č. 365/2000 Sb., resp. související vyhlášky o dlouhodobém řízení ISVS a o referenčním rozhraní, které společně v požadavcích na systém řízení bezpečnosti informací vytváří rámec pro realizaci nezbytných opatření:

- vedoucích k definici pravidel a předpokladů pro budoucí rozvoj řešení v souladu s bezpečností celého systému,
- k dlouhodobé udržitelnosti z pohledu přístupu k datům systému a auditovatelnosti systému,
- pro definici podmínek bezpečné údržby a zajištění bezpečného provozu.

Přes to, že byly výše identifikovány negativní faktory ovlivňující dlouhodobou udržitelnost systému a navrženy způsoby jak tyto faktory eliminovat technickými prostředky, je stále nejdůležitější zajistit v provozu hladkou komunikaci mezi zaměstnanci Objednatele a osobami poskytujícími servisní služby Zhotovitele. Touto platformou pro komunikaci informací a požadavků koncových uživatelů systému, rovněž tak pro organizaci aktivit spojených s údržbou systému je poskytování servisních služeb s vlastnostmi:

- Pro zajištění maximální efektivity a rychlosti poskytování servisních služeb a provozní podpory je zajištěn centrální kontaktní bod pro příjem požadavků,
- Ke každé z požadovaných oblastí podpory je navrženo samostatné procesní eskalační schéma, popisující životní cyklus daného požadavku od fáze zadání po jeho vyřešení,
- Samotný Service Deskový systém je schopen vyhodnocovat kromě parametrů plnění SLA i další výkonové a kvalitativní metriky, sloužící ke zvyšování kvality poskytovaných služeb,

- Na garanci kvality dbají po celou dobu manažeři kvality, kteří pravidelně sledují, měří a vyhodnocují procesy a kvalitu poskytovaných služeb, zejména pak garantovanou úroveň podpory (dle SLA) a tvoří také statické výstupní informace (reporty pro Objednatele) dle nastaveného smluvního plnění a proaktivně identifikují možnosti zlepšení dodávky IT služeb. Řešitelské týmy jsou rozděleny do 3 úrovní, přičemž:
  - Řešitelé 1. úrovně řeší základní běžné incidenty a požadavky,
  - Řešitelé 2. úrovně představují řešitelské týmy s hlubší produktovou / technologickou znalostí dané oblasti a zajišťují podporu řešitelům 1. úrovně.
  - 3. úroveň představuje nejvyšší úroveň podpory, kompetenčně a kvalitativně schopnou řešit ty nejobtížnější incidenty, problémy a požadavky. Řešitelé na této úrovni podpory jsou špičkovými technologickými odborníky ve svém oboru, majícími hluboké znalosti a rozsáhlé zkušenosti. Součástí 3. úrovně podpory je i specializovaný bezpečnostní tým, připravený zajistit součinnost v oblasti řešení bezpečnostních incidentů a problémů.
- Do budoucna předpokládá Zhotovitel (například v rámci řešení nových, navazujících projektů) rozšiřování jak dodaných technologií v rámci plnění této zakázky, tak implementování nových v průběhu 5ti letého servisu. Díky širokému technologickému záběru a velkému množství certifikovaných specialistů předpokládáme (např. na základě samostatného smluvního kontraktu) možnost rozšíření naší servisní podpory o tyto nové technologie dodané mimo náš předmět plnění. Tuto svoji nabídku opíráme o existenci více jak 450 specialistů Zhotovitele, která má v současné době bezmála 900 jedinečných certifikačních titulů.

Zhotovitel se zavazuje sdělovat možné postupy a nápady, jak nejlépe využívat klíčové komponenty celé architektury řešení tj. **Workflow a Integrační platformu** ve světle nových informací v době běhu systému a bude Objednateli nápomocen v udržování platformy v chodu s podílem na návrhu zapracování nových požadavků tak, aby mohl Objednatel tuto klíčovou část řešení rozvíjet samostatně i za přispění Zhotovitelem poskytovaných servisních služeb s předem definovanými SLA.

Zhotovitel je pro tuto spolupráci (přenos Know-how), přesahující rámec smluvních podmínek, motivován především dlouhodobostí smluvního vztahu, jeho závazky a zájmem o rozvoj řešení v budoucnu, který pro něj bude představovat významnou referenci.

Nativní funkce a konfigurační parametry ovlivňující funkci řešení
V následujících subkapitolách jsou uvedeny tabulky s výčtem **nativních funkčností a konfiguračních parametrů** ovlivňujících funkce celého systému z pohledu jednotlivých části plnění.

TC

A - Technologické Centrum Jihomoravského kraje			
Oblast plnění	**Komponenta**	**Nativní funkce / Parametr**	**Ovlivněná funkce řešení**
Infrastruktura Datového centra	Zabezpečení výpadku el. energie - UPS	Modulární řešení UPS	Snadné uživatelské rozšiřování výkonu i doby zálohy
	Klimatizace	Hot-swap výkonové a bateriové moduly	Oprava, servis, rozšiřování výkonu/doby zálohy bez omezení provozu zálohovaných technologií
		Vysoká účinnost (až 98%)	Snížení provozních nákladů, snížení tepelných ztrát
		Technologie ABM	Většina UPS baterií, které jsou dnes na trhu je trvale dobíjena malým proudem „kapkovitě“. Tento způsob poškozuje vnitřní chemické uspořádání baterie a snižuje její potenciální životnost až o 50% Exkluzivní ABM technologie naproti tomu používá důmyslné detekční zapojení a pokrokové třístupňové dobíjení prodlužující praktickou životnost baterie při současné optimalizaci doby jejího dobíjení. ABM technologie též poskytuje v předstihu až 60 dnů upozornění, že končí praktická životnost baterie a tím dává dostatek času k výměně baterií za provozu, aniž by bylo nutné odstavovat připojená zařízení.
		Technologie Hot Sync	Tato technologie dovoluje, aby vícemodulová konfigurace pracovala v paralelním zapojení, aniž by bylo nutné zajišťovat komunikaci mezi moduly. Takové uspořádání zabraňuje vzniku nejslabších článků v řetězci, které jsou vlastní tradičním paralelním zapojením, a maximalizuje dostupnost.
		Digital scroll kompresory	Plynulá regulace výkonu klimatizačního systému, poskytován je výkon přesně dle aktuálních potřeb technologie
		EC ventilátory v jednotkách	Vyšší účinnost než klasické ventilátory, nižší ztráty a nižší spotřeba elektrické

			energie
		Komunikační propojení jednotek	Dohled a ovládání systému klimatizace z jednoho místa
		Přesné klimatizace určené pro DC s nepřetržitým provozem	Zajištění přesných parametrů vnitřního prostředí, schopnost chlazení i při nízkých venkovních teplotách až do -30 °C
		Zvlhčovač integrovaný v jednotce	Není nutný samostatný zvlhčovač, lepší distribuce upraveného vzduchu
Serverová infrastruktura	Blade system	Technologie HP Thermal Logic	Inteligentní řízení teploty snižuje potřebu napájení a chlazení Blade šasi.
		Hot-Swap moduly	Všechny prvky blade šasi jsou redundantní a umožňují výměnu za provozu (servery, ventilátory, napájecí zdroje, I/O moduly, management moduly). -> Oprava, servis bez omezení provozu produkčních systémů.
		Podpora různých procesorových platforem	Možnost osadit kromě standardních procesorů x86 (Intel, AMD) Blade šasi i servery s procesory Itanium (operační systém HP-UX).
	Blade servery	Management procesor iLO3	Kromě všech standardních funkcí disponuje iLO3 i funkcí zapamatování posledního děje a následného zopakování. Správce tak má možnost zpětně se podívat například na to, co se na serveru dělo těsně před výpadkem serveru. Úspora času při řešení problémů.
		Extrémní rozšiřitelnost paměti	Nabízené servery BL685c G7 mají možnost osazení až 1TB paměti RAM. -> Snadné rozšiřování serverů v případě potřeby
	Virtual Connect Flex-10	Serverové profily	Umožňuje všechny potřebné parametry serveru oddělit od fyzického HW a přidělovat je dle potřeby. Například při výměně serveru správce nemusí nic dělat všechny parametry server získá od Virtual Connect Flex10. Server stačí pouze zasunout a zapnout. -> Zjednodušení správy, úspora nákladů.
		FlexNIC adaptéry	Každý 10Gb/s adaptér je možné rozdělit až

			na 4 adaptéry FlexNIC a každému přidělit potřebné přenosové pásmo. -> Snížení počtu potřebných síťových karet, menší potřeba kabeláže.
Serverová virtualizace	Virtuální stroj	Rychlost nasazení	Nový virtuální server může být připraven k použití v rychlosti desítek minut a více (podmínkou pro takto rychlé navýšení HW kapacity o nový virtuální server je předpřipravená image nebo klon včetně OS)
		Flexibilita realizace	změnové požadavky aplikací na požadovaný výkon lze realizovat prakticky ihned
		Změna výkonu	Změnové požadavky na výkonové parametry virtuálního serveru budou řešeny ihned
		Vysoká dostupnost	Virtuální servery budou násobeny tak, aby byla zajištěna co nejvyšší dostupnost aplikací jako takových
		Automatizace	Systémové požadavky, které vzniknou za provozu aplikace, budou v maximálně možné míře uspokojovány automaticky bez nutnosti zásahu obsluhy
		Provozní úspory	nasazením nového serveru v rámci existující virtuální infrastruktury nevznikají nové požadavky na napájení a chlazení tohoto serveru
Datová úložiště	Disková pole Tier 0	Extrémní výkon	Výkon, pro který by „klasická“ disková pole potřebovala stovky disků. -> Úspora nákladů
		Rozšiřitelnost	Kapacita je možná jednoduše modulárně rozšiřovat dle potřeby -> Možnost růstu a přizpůsobení se potřebám uživatelů
	Disková pole Tier1	Režim řadičů Active-Active	Přístup k libovolnému svazku je možný přes oba řadiče. -> Zvýšení propustnosti.
		Rozšiřitelnost	Možnost přidání dalších disků až do celkového počtu 450. -> Možnost růstu a přizpůsobení se potřebám uživatelů bez nutnosti dalších investic.
	Disková pole	Režim řadičů Active-	Přístup k libovolnému svazku je možný

	Tier 2	Active	přes oba řadiče. -> Zvýšení propustnosti.
		Rozšiřitelnost	Možnost přidání dalších disků až do celkového počtu 450. -> Možnost růstu a přizpůsobení se potřebám uživatelů bez nutnosti dalších investic.
	Garantované uložiště Tier 3	Dlouhodobá časová kontinuita	Technologie archivního úložiště je připravená na to, aby v průběhu svého života a za provozu bez složitých migrací, bylo schopno přijímat nový hardware a případně vyřazovat morálně zastaralý hardware. -> úspora nákladů při provozu
		Deduplikace	Odstranění duplicit je založeno na nahrazení již existujícího objektu odkazem. -> Úspora alokovaného místa.
		Virtuální archivy	Fyzický archiv je možné dělit na logické oddělené virtuální archivy = tenanty. -> Snadnější správa archivů
Disková virtualizace	Virtuální stroj	Maximální dostupnost	Data jsou synchronně uchovávána ve dvou serverovnách (lokalitách) -> Diskový subsystém funguje i při výpadku celé jedné lokality.
		Nezávislost na výrobci hardware	Systém je otevřený pro datová úložiště různých výrobců -> Snazší rozšiřování kapacity v budoucnu
		Automatické umísťování dat do vrstev	Automatizovaná migrace nejčastěji používaných, diskových bloků na nejrychlejší, zpravidla SSD disky -> vyšší výkon
Zálohování a obnova dat	SW pro zálohování	Vnitřní systém práv uživatelů produktu s možností definování dalších vlastních uživatelských skupin.	Možnost definování a rozdělení rolí pro správu a provoz zálohovacího řešení a tím snížení kvalifikační náročnosti na obsluhu řešení.
		Přednastavené „spouštěče“ pro vytváření reportů a monitoring produktu s možností definovat další vlastní dle potřeb	Zvýšení dohledovatelnosti řešení, zjednodušení správy provozu produktu, pro standardní provoz není potřeba vysoce kvalifikovaná obsluha
		Globální konfigurační	Vysoká flexibilita řešení, možnost

		soubory s velkým množstvím konfiguračních parametrů	přizpůsobení konfigurace požadavkům prostředí a jejich změnám.
		„Plovoucí“ licence pro zálohovací mechaniky knihovny připojené přes FC konektivitu.	Možnost přímého zasílání dat (sdílení knihovny) z „neomezeného“ počtu serverů bez potřeby dalších licencí pro mechaniky knihovny.
Bezpečná komunikační infrastruktura TCK	Páteřní přepínače	Nativní funkce IRF Konfigurace IRF	Virtualizace přepínače, společně s active/active redundantními řídícími moduly v každém přepínači, zásadním způsobem zvyšuje dostupnost celého řešení a eliminuje potřeby využití specializovaných mechanismů pro zajištění redundance (HSRP, VRRP, Spanning-tree…). Konfigurace IRF má pozitivní dopad také na propustnost systému. V budoucnu bude možné sdružit až 4ks přepínačů
		Nativní funkce – licencování SW	Součástí dodávky přepínače je již v základu plná funkcionalita, žádné vlastnosti nejsou předmětem licenčních poplatků (BGP, MPLS, VPLS, …). V případě potřeby lze tyto vlastnosti začít využívat bez dodatečných nákladů
		Nativní funkce	Jednotný operační systém na všech dodaných přepínačích a směrovačích
	SAN přepínače	Rozšiřitelnost	Možnost rozšíření až na 40 portů s rychlostí 8Gb/s
		Výkonnost	Neblokující platforma bez over-subscription s celkovou šířkou pásma 680 Gb/s
	Systém pro dělení zátěže na servery (loadbalancery)	Nativní funkce – po aktivaci licence	Application Security Manager (ASM) – WEB Aplikační Firewall
		Nativní funkce	Application Visibility and Reporting – Sledování odezev serverů.
		Nativní funkce – po aktivaci licence	Access Policy Manager (APM) – řízení přístupu uživatelů, aplikací, síťových zařízení k síti .
		Nativní funkce – po aktivaci licence	Global Traffic Manager (GTM) Link Controller – rozklad zátěže mezi různé lokality prostřednictvím inteligentního DNS

			překladu.
		Nativní funkce – po aktivaci licence	WAN Optimization Manager (WOM)
		Nativní funkce – po aktivaci licence	WebAccelerator – akceleracere aplikací dat a aplikací mezi datovými centry.
		Konfigurační parametr	iRule - Možnost doplnění uživatelské funkcionality pomocí skriptů.
		Konfigurační parametr	Řízení procesu na základě obsahu komunikace na L2 až L7 vrstvě. Možnost změny obsahu přenášených dat až na L7 vrstvě.
		Nativní funkce	Filtrování provozu (packet filtering).
		Nativní funkce	Možnost řízení šířky pásna. Podpora ToS, QoS (marking/preservation/mimic)
		Nativní funkce	Vytvářet uživatelsky přizpůsobitelné statistiky.
		Konfigurační parametr	iControl - napojení na externí systémy prostřednictvím API. Možnost dynamického řízení konfigurace systému dělení zátěže na servery.
	Management síť	Nativní funkce	Jednotný operační systém na všech dodaných přepínačích a směrovačích
	Hraniční routery pro připojení do Internetu	Nativní funkce – licencování SW	Součástí dodávky směrovače je již v základu plná funkcionalita, žádné vlastnosti nejsou předmětem licenčních poplatků (BGP, MPLS, VPLS, …). V případě potřeby lze tyto vlastnosti začít využívat bez dodatečných nákladů
		Nativní funkce – OAA	Open aplication architecture – umožňuje upravovat definice L4-L7 služeb poskytovaných směrovačem
		Nativní funkce	Distribuovaná architektura a oddělený controlplane od dataplane má pozitivní vliv na propustnost celého řešení

	Systém IDS/IPS	Nativní funkce	Ochrana proti zero day útokům
		Nativní funkce	Modulární operační systém
		Nativní funkce	Optimalizace skenovacích pravidel a ochrana proti přetížení zařízení
	Systém firewallové ochrany	Lokálnost	specifikovat povolené a zakázané aplikace nehledě na čísla portů, rozeznává také skutečné uživatele, nikoliv pouze zdrojové IP adresy. Skupiny uživatelů pak mohou mít svá vlastní pravidla a nastavení komunikace na firewallu
		Interpretace chování uživatelů	umožňuje snadné, ale přesto velmi detailní nastavení bezpečnostní politiky v síti. Pravidla jsou snadno interpretovatelná – riziko chyby způsobené nesprávným pravidlem je téměř nulové
		Rozpoznání obsahu	Na základě skutečného obsahu a signatur dokumentu FW+ rozpozná, o jaký typ souboru se jedná., umožňuje i inspekci dat přenášených šifrovaně pomocí protokolu SSL
		Podpora virtualizace – energeticky úsporné řešení	lze provozovat i ve virtuálním prostředí (VMware, VirtualBox). Virtualizace je navíc šetrná i z pohledu spotřeby energie
		Bezpečnost celého řešení	Důsledně dodržujeme filozofii prosazovanou mimo jiné národním bezpečnostním úřadem ČR - posuzována je bezpečnost celého řešení nikoliv jednotlivých použitých produktů
Management a monitoring	Network management Systém	Lze vytvářet konfigurace/skripty pro prvky, které nejsou podporovány out-of-the-box s využitím běžných standardů správy.	Vzdálená konfigurace všech aktivních prvků, včetně automatického zálohování a obnovy této konfigurace
		Alarmy lze obsáhle konfigurovat podle řady kritérií. K dispozici je správce notifikací jako nativní funkce, možnosti konfigurací jsou ale	Možnost nastavení alarmů

		velmi obsáhlé.	
		Podpora SNMP včetně v3 je nativní funkcí. Správce systémů má možnost konfigurace – přidání MIB, správa trapů z ní	Podpora protokolu SNMP
		Sestavy lze v různé podobě získávat ze všech částí systému, publikace je do unifikované konzole. Sestavy lze podle potřeby upravovat, lze doplnit i data z dalších oblastí.	Sestavy a statistiky, podklad pro stanovení dostupnosti sítě a jejích částí
	Centrální management portál	Standardní součástí systému jsou možnosti řady úprav – jak prosté úpravy prvků podle potřeb uživatele, tak možnost publikace vlastních prvků do konzole	Zákaznické úpravy a rozšíření všech funkcí a prostředí aplikace
		Je možné definovat exporty podle požadavků správy	Export dat do aplikací třetích stran
		Zejména v rámci SNMP lze konfigurovat řadu pravidel pro sběr	Podpora tvorby vlastních definic sběru a nastavení konfiguračních dat
		K dispozici je jako nativní funkce řada předdefinovaných reportů, k dispozici jsou ale i funkce pro konfiguraci a tvorbu vlastních	Zpracování dat v historickém kontextu (reporty)
		V konzoli NNM lze zobrazovat sledované prvky řadou způsobů. Základní pohledy	Podpora tvorby grafických pohledů s prezentací stavu prvků a skupin

		jsou k dispozici jako nativní funkce (například zobrazení mapy sítě), kromě toho ale lze vytvářet i vlastní pohledy.	
		Lze vytvářet vlastní konfigurované reporty podle řady kritérií.	Tvorba vlastních reportů

VIU

B – Vnitřní integrace Krajského úřadu			
Oblast plnění	**Komponenta**	**Nativní funkce / Parametr**	**Ovlivněná funkce řešení**
Portál	Search	Oblast a metoda vyhledávání	Úspěch nalezené informace
	Kalendáře	Sdílení, komunikace aktivit	Plánování, informace ve správný čas a pro správné cílové skupiny
	Úkolovníky	Rozdělení rolí podle priorit, charakteru, závislostí	Snazší vyhledání osob pro Zastupitelnost
	Rozcestník	Nastavené různých úhlů pohledu na procesy a zdroje	Přehlednost, rychlost přístupu k aplikacím, informacím, službám a analytickým výstupům
	Vizuální nástroj pro modelování a následný běh aktivit Workflow	Nativní funkcí je Model pro podpůrné / sdílené procesy organizace a Model vlastního sledu činností při výkonu agend OVM	Funkce schválení a vyplnění formuláře, jasná pravidla a definice začátku a konce aktivity s kontrolou výstupů, efektivní využívání lidských zdrojů při organizaci toku práce, rychlejší podpora při rozhodování (samoobslužný a řízený oběh informací).
	Formuláře	Poskytuje formuláře pro další zpracování	Flexibilita při definici formulářů s možností začlenění kontrol.

	Katalog elektronizovaných služeb úřadu	Registruje a poskytuje seznam dostupných služeb integrační vrstvy pro napojení systémů a správnou komunikaci/dodávku dat	Flexibilní nastavení podpory procesů výkonu Agend OVM. Rychlejší modifikace a zavádění změn v množině užívaných služeb podpoře interních procesů
	Adaptéry napojení AIS	Vzájemné propojení systémů standardními postupy.	Schopnost integrovat standardizovaným způsobem IS úřadu.
Workflow	BPEL engine	Seznam seřazených funkcionalit za sebou pro agregování do jedné a poskytnutí správného vyhodnocení a upozornění na událost	Schopnost správně sekvenčně vyhodnotit jiné funkce z katalogu služeb. Schopnost orchestrovat jiné služby.
	JMS adaptér	Přijmutí, odeslání a persistentní uchování zpráv k vyhodnocení.	Schopnost integrace systému a komunikace technologií JMS s jinými systémy (Exchange, IDM, AIS aj.)
Integrační platforma	Souborový Adaptér	Uložení souboru a poskytnutí souboru integrovaným systémům	Schopnost uložit soubor z vybraných systémů nebo jejich načtení
	Persistentní úložiště	Ukládá a data, která vyhodnocuje pro bezpečný běh integrace	Schopnost běhu aplikace rychle v HA mode. Odolnost proti výpadku. Dostupnost integrovaných systémů a jejich rychlost.
	Notifikace událostí	Upozornění zainteresovaných aktérů na události, na které mají být podle procesu agendy upozorněni	Ovlivnění termínů, upozornění zaměstnanců na události ovlivňující běh zpracování agendy
	IDM Management konektor	Poskytuje připojení integrovaných systémů na centrální systém správy uživatelů a rolí.	Schopnost se přihlásit do systémů a ovlivnit práva na funkce.

	Založení správního řízení	Tvorba správního spisu, spisového přehledu a dokumentů v něm obsažených Vedení jednotlivých úkonů správního řízení	Profilová karta řízení Napojení na spisovou službu jedno řízení jeden spis Podnět jde přes Spisovou službu
	Registr účastníků řízení	Evidence účastníků řízení	Procesní způsobilost, postavení osoby v řízení
	Registr dotčených orgánů	Evidence dotčených orgánů	Stanovení typu dotčeného orgánu, vazba na registr externích subjektů
	Registr úkonů ve správním řízení	Evidence úkonů	Profil úkonu Nabídka možných vzorů a formulářů, Odeslání přes spisovou službu
IS Správních Řízení	Lhůtník	sledovaní a vyhodnocování lhůt v řízení	Výpočet lhůt
	Přehledy	Vedení přehledů o úkonech ve správním řízení	Statistiky, výběry

eSSL

C – Hostovaná elektronická spisová služba			
Oblast plnění	**Komponenta**	**Nativní funkce / Parametr**	**Ovlivněná funkce řešení**
eSSL	Podatelna	Napojení na datovou schránku a emailový účet el. podatelny	Přímá evidence elektronických podání, rovnocenný přístup k digitálním a analogovým podáním
	Hlavní evidence	Evidence dokumentů	Přidělování ČJ a vedení podacího deníku
	Hlavní evidence	Oběh dokumentů	Oběh a vyřizování dokumentů

	Výpravna	Odesílání datových zpráv, emailů, poštou, kurýrem	Odesílání a evidence jak listinných tak elektronických dokumentů
	Spisovna	Skartační řízení	Ukládání spisů a dokumentů, skartace
	Hlavní evidence	Práce s elektronickými dokumenty	Konverze mezi formáty, elektronický podpis a časové razítko

DS

D – Datové sklady, manažerské informační systémy a nástroje business Intelligence JMK			
Oblast plnění	Komponenta	Nativní funkce / Parametr	Ovlivněná funkce řešení
Úložiště Datového skladu	Microsoft SQL Server 2012 Database Engine	Základní služba pro ukládání, zpracování a zabezpečení dat. Poskytuje řízený přístup a rychlé zpracování transakcí pro splnění požadavků i těch nejnáročnějších aplikací. Poskytuje také bohatou podporu pro udržení vysoké dostupnosti.	Robustní datová základna strukturovaných údajů datového skladu. Je plněna prostřednictvím Integration Services.
	Microsoft SQL Server 2012 Integration Services	platforma pro budování vysoce výkonných řešení datové integrace, založené na ETL (Extract, Transformation, Loading) procesech, jejich monitorování, sdružování do balíčků atd. pro zpracování datových skladů.	Sběr dat pro datový sklad, transformační úlohy, procesování OLAP Databází a datových kostek, Kvalita dat
	Microsoft SQL Server 2012 Analysis Services	platforma a sada nástrojů pro provoz Business Intelligence založené na OLAP databázích a datových kostkách, které umožňují on-line multidimenzionální analýzu velkých dat. Zahrnuje i dolování dat (data mining), k odhalení zákonitostí a vztahů ukrytých uvnitř velkých objemů dat.	Analýza dat v analytických prostorech prostřednictvím různých klientských Business Intelligence nástrojů – typicky Excel, SharePoint prostředí, MDF – Manažerský datový fond
Business Intelligence	Microsoft SQL Server 2012 Reporting	Představuje Webově dostupné sestavy, reporty,	BI nástroj pro přednastavené

nástroje	Services	výstupy a analýzy, které čerpají z obsahu datového skladu a Analysis Services. Výstupy lze publikovat v různých formátech, a centrálně spravovat zabezpečení a doručování.	interaktivní výstupy pro zaměstnance krajského úřadu, managementu, analytikům, výkonným pracovníkům, veřejnosti, managementu zřizovaných organizací.
	Microsoft SharePoint Server 2010 Performance Point Services	Umožňuje ad-hoc analýzu, tvorbu KPI, uživatelské vyhledávání, organizace optimální podoby výstupů a jejich organizaci v tzv. dashboardech, neboli „palubní desce“, která uživatelům umožňuje zorganizovat výstupy např. jednoho tématu na jednu stránku.	BI nástroj pro ad-hoc analýzu pro management, analytikům a vybraným výkonným pracovníkům.
	Microsoft SharePoint Server 2010 Excel Services	Umožňuje velice jednoduše vytvořené sešity v Microsoft Excel a ty zobrazit ve webovém prohlížeči na portálu SharePoint, kde lze jednotlivé listy zobrazit a přepočítávat (zjednodušená tvorba analýz a reportů pro sdílení informaci s kolegy v týmu, případně publikování rychlých analýz pro mamagement)	BI nástroj pro management, analytikům a vybraným výkonným pracovníkům.
	MDF – Manažerský datový fond	Modul IS GINIS, umožňující multikriteriální analýzu z prostředí IS GINIS.	Rozpadové analytické stromy pro odhalování hlubších souvislostí a vyhledávání analytických workflow
Interní analytický portál /Interní manažerský informační systém	Microsoft SharePoint Server 2010	Integrace analytických, plánovacích, kontrolních a reportovacích funkcí s obsahem Business Intelligence – tzn. s výstupy a analýzami pro interní potřeby úřadu	„Přístupový bod“ z interní sítě úřadu, tedy předběžně pro zaměstnance krajského úřadu, management, analytiky, výkonné pracovníky.
Externí analytický portál /Externí manažerský informační systém	Microsoft SharePoint Server 2010	Integrace reportovacích funkcí s obsahem Business Intelligence – tzn. s výstupy a analýzami pro potřeby okolí úřadu	„Přístupový bod“ z internetu, tedy předběžně pro management zřizovaných organizací, veřejnost, ORP, obce,

			dalším institucím.
Metodika GORDIC	Analytická workflow	Možnost interaktivního procházení reportů skrze nejčastěji používanou „analytickou cestu“ od hrubých informací k detailním.	Best-practises, předpřipravené analýzy pro uživatele, optimalizace reportingu
	Účetní a rozpočtová metodika	Znalost účetní a rozpočtové metodiky úřadu v kombinaci se znalostí datového zdroje rozpočtu a účetnictví, umožňuje načtení kompletní obsažené historie od prvopočátku s ošetřením návazností v časových řadách i přes změny legislativy.	
	Znalost základních ekonomických zdrojů dat	Znalost základních ekonomických zdrojů dat.	Plné využití informačního potenciálu IS GINIS, umožnění analýzy až do konkrétního dokladu vč. jeho detailů.

KDS / KDR

E – Krajská digitální spisovna / Krajský digitální repozitář			
Oblast plnění	Komponenta	Nativní funkce / Parametr	Ovlivněná funkce řešení
Vstupní modul	Příjem dat	zajišťuje komunikaci s původcem, autentizaci, autorizaci a uložení přijatých balíčků SIP do pracovního úložiště	Bezpečnost komunikace s původci
	Kontrola kvality vstupních dat	kontroluje formální strukturu balíčků a přítomnost virů a jiného škodlivého obsahu balíčků. V rámci tohoto modulu je zřízena i tzv. karanténní zóna pro zajištění spolehlivosti kontrol	Možnost infikace dat, či přijetí chybného balíčku. To by mělo vliv na dlouhodobé uložení

	Řízení příjmu	kontrola popisných a technických metadat, kontrola přípustnosti souborových formátů, kontrola struktury balíčku SIP a vzájemného provázání balíčků	Chybějící metadata by mohla znamenat pozdější odmítnutí balíčku NDA
	Generování balíčků AIP	automatické doplnění zejména technických metadat, konverze formátů metadat, možnost manuálního doplnění metadat, vstupní migrace formátů včetně generování náhledů pro prezentaci dat archivu v určeném formátu	Chybějící metadata by mohla znamenat pozdější odmítnutí balíčku NDA
	Řízení ukládání	zajišťuje konzistentní uložení metadat a obsahu archivních balíčků současně do archivního systému, systému správy dat a systému pro přístup	Konzistence ukládaných dat
Modul správy dat	Evidenci číselníků	zajišťuje ukládání a přístup k číselníkům používaným v rámci vstupní kontroly a vyhledávání. Jedná se o tyto číselníky - původci, klasifikace, povolené souborové formáty, kategorizace dokumentů podle kritérií přístupnosti, požadavků na zachování důvěryhodnosti, doby uložení.	Informace o uložených entitách
	Evidence přijímaných a uložených balíčků	zajišťuje vedení a přístup ke katalogu uložených dokumentů včetně stavu příjmu a uložení.	Informace o uložených entitách
	Evidence periodické obnovy časových razítek	zajišťuje evidenci historie obnovy časových razítek pro jednotlivé balíčky pro trvalé zajištění důvěryhodnosti uloženého obsahu	Zajištění trvalé důvěryhodnosti

	Evidence kontroly konzistence	uložení kontrolních součtů jednotlivých uložených balíčků AIP na aplikační úrovni pro účely periodické kontroly konzistence uloženého obsahu nezávisle na vlastnostech použitého archivního úložiště	Neměnnost uložených dat
	Evidence procesů skartace a archivace	informace o stavu skartace a informace o stavu jednotlivých balíčků AIP zařazených do skartačního řízení	Skartace
Archivní systém	Archivní systém	Zajišťuje vlastní důvěryhodné uložení obsahu balíčků AIP. Je implementován primárně prostřednictvím technologie CAS.	Napojení na úložiště
Modul administrace	Řízení procesu příjmu	zajišťuje přehled pro administrátora o stavu příjmu balíčků SIP, umožňuje řešení problémů se strukturou a obsahem balíčků při příjmu	Chybějící metadata by mohla znamenat pozdější odmítnutí balíčku NDA
	Řízení procesů migrace	spouštění migrace souborových formátů v uložených balíčcích a přehled o provedených migracích	Vadný souborový formát by mohla znamenat pozdější odmítnutí balíčku NDA
	Řízení procesu časového razítkování	kontrola periodické obnovy časových razítek u uložených balíčků, případně i manuální spouštění obnovy razítek	Zajištění trvalé důvěryhodnosti
	Skartační řízení	příprava návrhu a jeho schvalování, provedení skartace, případně exportu do jiného archivu v definovaném formátu	Skartace
	Správa kontroly konzistence	přehled o průběhu ověřování kontrolních součtů a o nalezených problémech s uložením balíčků AIP	Konzistence ukládaných dat

	Správa číselníků	zajišťuje pro administrátory, původce a archiv aktualizaci a čtení číselníků používaných v rámci vstupní kontroly a vyhledávání	Administrace systému
	Ukládání transakčních záznamů	pro účely auditu zaznamenává veškeré provedené operace nad uloženými balíčky (příjem, kontrola, transformace, ukládání, čtení). Zaznamenané záznamy jsou zároveň ukládány do úložiště ve formě AIP	Průkaznost uložených balíčků
	Transakční záznamy	Přístup k transakčním záznamům	Průkaznost uložených balíčků
Přístupový modul	Zabezpečení přístupu a autentizace uživatelů	zajištění přístupu uživatelů k uloženým metadatům a dokumentům	Autentizace
	Autorizace	omezení přístupů na základě klasifikace dokumentu, původce, uživatelských skupin a rolí uživatelů. Modul povolí přístup ke čtení obsahu nebo metadat podle rolí přihlášeného uživatele a oprávnění příslušného balíčku	Autorizace a bezpečnost
	Vyhledání	Vyhledání uložených balíčků na základě zvolených metadat	Úspěch nalezeného balíčku
	Zobrazení náhledů a distribuce uložených dokumentů ve formě DIP	systém umožní výběr dokumentů a jejich zaslání oprávněnému uživateli ve standardizované podobě	Dostupnost balíčků
	Transakční záznamy	Provádění transakčních záznamů o přístupu k jednotlivým uloženým balíčkům	Průkaznost uložených balíčků
	Programové rozhraní API na externí portál pro přístup	systém eviduje veškeré přístupy k uloženým dokumentům a archivuje je	Integrace

Servisní služby, Projektové řízení a Bezpečnost

Zhotovitel dále uvádí seznam služeb/Aktivit a jejich Vlastností/Schopností, které jsou nedílnou součástí plnění a mají nepřímý vliv na funkčnost řešení i přes to, že se nejedná o technické komponenty řešení. Důvodem je na jednom místě podat komplexní náhled i na možnosti nastavení procesů, které významnou měrou vlastní implementaci a používání technických prostředků v provozu ovlivňují.

F – Úroveň poskytovaných služeb			
Oblast plnění	Služba / Aktivita	Vlastnost / Schopnost	Ovlivněný proces
Podpora uživatelů	ServiceDesk	Centralizovaný přístupový bod pro hlášení a příjem požadavků o podporu. přehled o stavu řešení jednotlivých požadavků. Historie zadaných požadavků.	Standardizovaný přístup a komunikační kanál. Přehled o stavu požadované podpory.
	HotLine	Rychlá telefonická podpora pro řešení požadavků a konzultací, které lze vyřešit telefonicky systémem tzv. „call back“ (požadavek je zaregistrován, a pokud nelze vyřešit přímo operátorem, je automaticky eskalován na řešitelský tým.)	Rychlá pomoc Kontaktním osobám Objednatele.
Zajištění kvality servisních služeb	Řízení kvality	Aktivní dohled nad plněním smluvních parametrů podpory.	Kontinuální odhled a vyhodnocování kvality poskytovaných služeb.
	Demingův cyklus PDCA	Model neustálého zlepšování procesů.	Kontinuální zlepšování a zdokonalování v oblasti servisních služeb.
	Víceúrovňové Řešitelské týmy	Efektivní eskalace mezi Level 1 až Level 3 řešitelskými týmy.	Rychlejší a efektivnější vyřešení reaktivních i proaktivních událostí.

	Monitoring SW a HW	Kontinuální sledování definovaných parametrů infrastruktury Objednatele. V případě detekce mezního stavu automatizované předání podle eskalačního scénáře.	Minimalizace vzniku nenadálých událostí typu incident.
G – Projektové řízení			
Oblast plnění	Služba / Aktivita	Vlastnost / Schopnost	Ovlivněný proces
Projektová metodika postavená na metodologii PRINCE2	Přizpůsobení témat	Politiky a standardy společnosti jsou aplikovány a použity při tvorbě projektových standardů v oblasti řízení **Rizik**, **Kvality**, **Komunikace** a **Konfigurace**.	Aplikace má za následek přiblížení se k prostředí, standardům a zvyklostem společnosti a nevnáší zavádějící přístup k řešení jednotlivých témat jinou, na první pohled nejasnou formou.
	Použití firemní terminologie	Byť metodologie pracuje s odbornými termíny, v rámci přizpůsobení projektu je počítáno s použitím terminologie zažité a používané v prostředí projektu.	Není nutné zavádět nové pojmy, pokud jsou stávající známé, zažité a nekonfliktní. Zvyšuje se míra pochopení projektu.
	Popis produktu	Stěžejní částí metodologie je detailní popis výsledného produktu projektu. Metodologie pracuje s rozsáhlými parametry popisu produkt, ale v rámci přizpůsobení je předpokládáno zohlednění specifik pro dané prostředí. Jinou míru a motivy sledování kvality produktu jsou např. ve sféře komerční a jiné ve sféře nekomerční.	Přínosem je možnost zaměřit se při dodávce produktu na parametry přinášející nejvyšší přínos uživateli v cílovém prostředí.
	Zahrnutí rolí	PRINCE2 pracuje s hierarchickou organizační strukturou, přesně definuje jednotlivé role a odpovědnosti, ale na druhou stranu opět otevírá možnost přizpůsobení jednotlivých rolí v závislosti na firemních standardech, způsobu řízení apod.	Tento přístup umožňuje maximálně efektivní využití konkrétních osob, jejich oprávnění a odpovědností.
	Zahrnutí procesů	Procesy aplikované v rámci PRINCE2 metodologie jsou přesně definovány a	Využití a zahrnutí stávajících procesů zjednodušuje a

		vyžadovány. Ovšem i zde v rámci přizpůsobení lze zahrnout možnosti, zvyklosti a způsob práce tak, aby byly maximálně přizpůsobeny prostředí uživatele.	zefektivňuje plnění aktivit v rámci těchto procesů a snižuje míru nejistoty a nejasnosti jako by to bylo při aplikaci zcela nových a nezaběhnutých postupů.
H - Bezpečnost			
Oblast plnění	Služba / Aktivita	Vlastnost / Schopnost	Ovlivněný proces
Metodika bezpečnosti	Demingův cyklus PDCA	Model neustálého zlepšování procesů.	Kontinuální zlepšování a zdokonalování v oblasti informační bezpečnosti.
Řízení bezpečnosti	Systém řízení bezpečnosti informací (ISMS)	Zajištění systematického řízení rizik a ochrany informací.	Měřitelná úroveň ochrany informací, efektivita bezpečnostních opatření eliminujících rizika, bezpečnost informací a ICT.

Míra požadavků na specializaci pracovníků IT oddělení Objednatele

Frontend / Klientské aplikace: poskytnuté běžné klientské **uživatelské rozhraní pro ovládání funkcionality aplikací** bude dle mínění Zhotovitele natolik intuitivní, že pro jeho ovládání a nastavení dostačuje běžná znalost na úrovni ovládání kancelářských aplikací a přístup k dokumentaci, kterou Zhotovitel dodá v rámci plnění.

Backend / Serverové systémy: rozsah očekávaných **dovedností pracovníků IT oddělení** u Objednatele je uveden v následující tabulce:

Komponenta	**Rámcový rozsahu očekávaných dovedností pracovníka IT oddělení**	**Požadovaná odbornost**
Hostovaná spisová služba	Cílově: schopnost dohlížet a monitorovat chod komponenty v provozu, Spolupracovat s Zhotovitelem při nasazení upgrade a update ASW, realizovat základní potřeby správy, tj. nastavovat a konfigurovat ASW s dohledem a podporou Zhotovitele podle dodané dokumentace, Spolupracovat při definování a schvalování požadavků na změny funkčnosti.	**SŠ technického zaměření** Zkušenosti s provozem spisové služby, administrací aplikací a schopnost zapojení do aktivit podléhajícím projektovému řízení
Datové sklady, Portál úředníka	Cílově: Schopnost analytického myšlení, Spolupráce při zajišťování implementace na úrovní pochopení základních entit a vazeb v datovém skladu a OLAPu, Schopnost spolupráce s Zhotovitelem při migrací dat, organizaci seznámení, zajišťování provozu, dohledu a monitoringu, Schopnost spolupracovat s Zhotovitelem při nasazení	**SŠ technického zaměření** Zkušenosti s administrací úloh a práce s Share Pointem, MS Excelem. Schopnost zapojení do aktivit podléhajícím projektovému řízení. Výhodou je znalost základních principů datového modelování pro

	upgrade a update ASW a DB, realizovat základní potřeby správy, tj. nastavovat a konfigurovat ASW s dohledem a podporou Zhotovitele podle dodané dokumentace, Spolupracovat při definování a schvalování požadavků na změny funkčnosti.	orientaci v datovém modelu.
Datová tržiště	Cílově: Spolupráce na tvorbě metodiky sběru dat a zajištění jejich validace, Koordinace postupů při zajištění konzistence celého systému BI a datového skladu s ekonomickým systémem, spolupráce s návrhy a schvalováním speciálních výstupů a rozborů z datové základny kraje ve stanovených oblastech datových tržišť dle ZD.	**VŠ či SŠ vzdělání** Znalost ekonomického systému kraje po stránce procesní, organizační s důrazem na metodiku a analytické potřeby koncových skupin uživatelů. Schopnost zapojení do aktivit podléhajícím projektovému řízení
KDS, KDR	Cílově: Spolupráce při zajišťování analýzy, provozu, dohledu, monitoringu, Schopnost spolupracovat s Zhotovitelem při nasazení upgrade a update ASW a DB, realizovat základní potřeby správy, tj. nastavovat a konfigurovat ASW s dohledem a podporou Zhotovitele podle dodané dokumentace, Spolupracovat při definování a schvalování požadavků na změny funkčnosti.	**VŠ či SŠ technického zaměření** Zkušenosti s archivním systém či minimálně systémem spisové služby, administrací aplikací obdobného charakteru. Schopnost zapojení do aktivit podléhajícím projektovému řízení.
IS Správních řízení	Cílově: Řeší centrální evidenci všech správních řízení, které příslušný orgán vede.	**VŠ či SŠ vzdělání** Zkušenosti s vedením a nastavováním procesů správního řízení. Znalost zákonů a předpisů ovlivňující procesy. Schopnost nastavit podle dokumentace chování aplikace.
ESB	Cílově: Schopnost řídit, směřovat a procesovat integrační dotazy mezi jednotlivými systémy. Sjednotit způsob komunikace a umožnit	**VŠ technického zaměření** Zkušenosti s platformou a filozofií SOA. Znalost BPEL a WS, Znalost business dopadů dané spravované agendy.
IDM	Cílově: Schopnost centralizovat správu uživatelských účtů a rolí. Mít jedno místo evidence a auditu nastavení oprávnění.	**VŠ či SŠ technického vzdělání** Schopnost nastavit podle příručky oprávnění a nastavení systému. Znalost prostředí, do kterého se IDM integruje.
WorkFlow	Cílově: Schopnost vytvářet uživatelsky zaměřené procesy zpracování například. Schválení cestovního příkazu s dynamickým přiřazením nadřízených případně jejich zástupců v době dovolených	**VŠ či SŠ technického vzdělání** Schopnost analytického vzdělání a míra abstrakce potřebná pro představení si pracovního postupu a jeho následné realizace pomocí grafických nástrojů pro modelování. Schopnost pochopit a realizovat postupy

		dodané Objednateli v rámci dodávky.
ServiceDesk Kontaktní osoby Objednatele oprávněné k eskalaci servisních požadavků na Service Desk Zhotovitele	Seznámení definovaných kontaktních osob Objednatele (tj. osob oprávněných zadávat u Zhotovitele servisní požadavky) s metodikou a procesy v oblasti eskalace servisních služeb, procesů podpory, incident managementu, využívání komunikačních kanálů (webového rozhraní, elektronické komunikace, telefonického / faxového zadávání požadavků) na Centrální komunikační bod zhotovitele.	Žádné specializované odbornosti nejsou vyžadovány.

Budoucí rozvoj systému - otevřenost
Zhotovitel v této nabídce předkládá řešení, které dle jeho mínění jednoznačně podporuje budoucí rozvoj systému, neboť se při výběru jednotlivých komponent komunikační infrastruktury, zaměřil na **eliminaci hlavního faktoru, který rozvoj systému výrazně negativně ovlivňuje**. Tímto faktorem je maximální **flexibilita při rozšiřování** kapacity a funkcionality pro potřeby pokrytí budoucích požadavků, kterou Zhotovitel ošetřuje

- v každé komunikační vrstvě sítě návrhem, který rozšiřitelnost po komponentách umožňuje,
- v oblasti zálohování schopností zařazovat do zálohy budoucí servery a pracovní stanice
- v oblasti rozšiřování prostor pro data záloh lze zálohovací řešení prakticky neomezeně rozvíjet a to jak možností rozšíření diskové kapacity přidáním dalších disků pro tato data, tak i připojením další zálohovací knihovny do SAN infrastruktury
- v oblasti virtualizace, jak na úrovni výpočetního výkonu, tak i na úrovni diskových úložišť, možností konfigurovat fyzické zdroje podle požadavků vyšších vrstev řešení,
- v oblasti aplikačních vazeb a komunikace celého řešení s okolím, nasazením škálovatelné integrační platformy, která je rovněž významným prvkem při ochraně budoucích investic Objednatele díky své schopnosti integrovat stávající heterogenní IS Objednatele,
- v oblasti procesní podpory výkonu agend nasazením flexibilního workflow, které bez „programování“ umožní rychlé změny v pracovních postupech, pravidlech a ošetření výjimek procesů,
- v oblasti prezentační vrstvy portálem, který umožní sjednocení nástrojů pro podporu pracovních činností, sdílení informací a integraci nástrojů pro podporu kvalifikovaného rozhodování označované v řešení jako analytické nástroje Business Intelligence.

Návrh opatření a přístup pro zajištění realizovatelnosti
Jako stěžejní opatření pro zajištění realizovatelnosti veřejné zakázky navrhujeme aplikovat projektovou metodiku PRINCE2 komplexně na celé prostředí projektu. V projektu se soustředit a nepodcenit zejména následující oblasti.

STRATEGIE ŘÍZENÍ RIZIK
V procesu iniciace projektu se zaměřit na strategii řízení rizik, aplikovat vnitřní systém pro řízení rizik (pokud je k dispozici), rizika náležitě vyhodnotit a evidovat formou Registru rizik v průběhu celého životního cyklu projektu.

ŘÍZENÍ ETAPY PROJEKTU
Jedná se o proces, jehož cílem je sledovat a vyhodnocovat dodávku produktů v požadované kvalitě, ceně, času, rozsahu, rizicích a benefitech. Sleduje výjimky od plánu, rizika a otevřené body.

PROJEKTOVÝ DOHLED
Z pozice Projektového výboru naplnit roli projektového dohledu a nezávisle sledovat součinnost a průběh projektu ze všech oblastí projektu. Jak za oblast vedení projektu, tak uživatelů, tak i Zhotovitele

Harmonogram projektu
Harmonogram projektu definuje základní časový rámec projektu a nastiňuje základní členění do etap s přihlédnutím na požadovanou délku trvání realizace jednotlivých produktů projektu.
Způsob zobrazení harmonogramu byl zvolen zejména s ohledem na jeho čitelnost a přehlednost.
V rámci projektu předpokládáme sledování času, závislostí a pracností formou Ganttova diagramu (MS Project).
Časový průběh projektu respektuje požadované plnění předepsaných etap harmonogramu, přičemž čas T je datum nabytí platnosti smlouvy. Nejzazší termín zahájení projektu (nabytí platnosti smlouvy) je 31.8.2012.

BLIŽŠÍ VYSVĚTLENÍ JEDNOTLIVÝCH ETAP PROJEKTU
Příprava projektu
Je z pohledu metodiky PRINCE2 stěžejní a nesmírně důležitá. Zahrnuje v sobě procesy přípravy/zahájení projektu a iniciaci projektu. Výstupem tohoto úkolu bude základní projektová dokumentace definující strategie řízení projektu v oblastech kvality, rizik, konfigurace a komunikace, bude popisovat dodávané jednotlivé produkty, zejména s ohledem na očekávané kvalitativní parametry, které budou sloužit jako podklad pro akceptaci produktů.

Řešení bezpečnosti
V rámci dodání jednotlivých výstupů/produktů bude řešen a zohledněn aspekt bezpečnosti, který prochází projektem napříč všemi produkty.

Výstavba technologického centra
V rámci této technologické etapy plánujeme vlastní vybudování technologického centra a záložního technologického centra.

Integrace vnitřního systému – analýza (Vnitřní integrace úřadu)
Výstupem této etapy je schválená analýza nutná pro realizaci vnitřní integrace úřadu.

Datové sklady, manažerské informační systému a nástroje BI – Analýza (Datové sklady, manažerské informační systémy a nástroje Business Intelligence)
Výstupem této etapy je schválená analýza výstavby datového skladu.

Hostovaná elektronická spisová služba
Výsledným produktem této etapy je systém hostované spisové služby.

Krajská digitální spisovna (KDS) a Krajský digitální repozitář (KDR)

Výstupem tohoto projektu jsou produkty KDS a KDR.

Integrace vnitřního systému - Vytvoření implementačního analytického manuálu a návrh integrace
V rámci této etapy se předpokládá dodání produktu Vnitřní integrace úřadu na základě dříve provedené analýzy. Proběhne návrh dané integrace, která bude vycházet z analýzy a potřeb zákazníka a rozsahu projektu. Po návrhu jednotlivých částí začne vývoj jednotlivých modulů (vystavení integračních rozhraní, vytvoření IDM, napojení na ISZR pomocí eProxy).

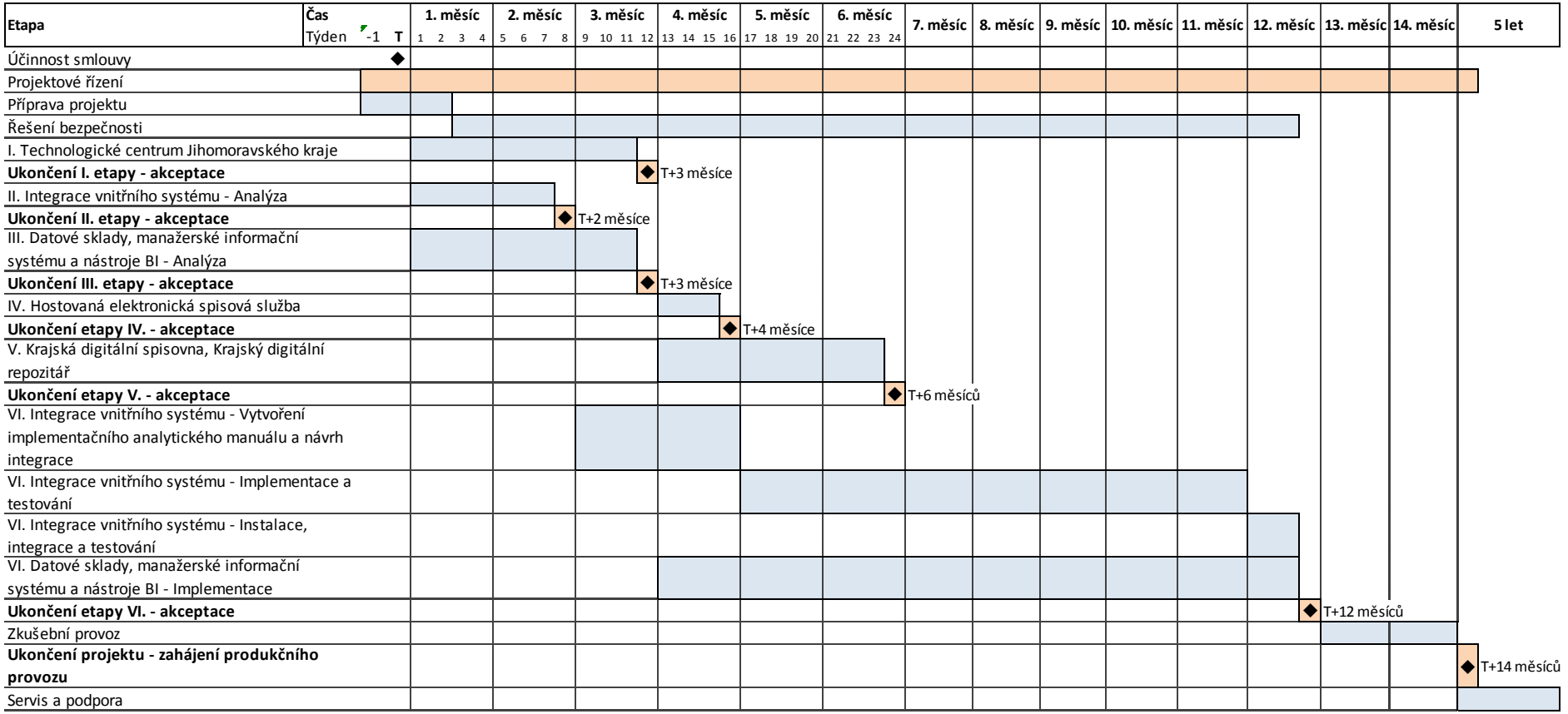
Integrace vnitřního systému - Implementace a testování
Vývoj jednotlivých částí bude probíhat iterativně a každá vydaná mini verze může být na přání Objednatele nainstalována na jeho prostředí. Plánujeme 4 iterace.

Integrace vnitřního systému - Instalace, integrace a testování
Po vytvoření finální verze se provede nasazení aplikací na test Objednatele a poté jeho testy Objednatelem. V průběhu vývoje, nasazení a testů se provede dokumentace. Poslední fází bude seznámení určených pracovníků Objednatele.

Datové sklady, manažerské informační systému a nástroje BI – Implementace (Datové sklady, manažerské informační systémy a nástroje Business Intelligence)
Produkt Datový sklad bude dodán na základě upřesnění z analýzy.

Zkušební provoz
Zkušební provoz je etapa, jejíž výsledkem je ověření korektní funkčnosti implementovaného řešení v rámci definovaných kritérií.

POPIS UKONČENÍ JEDNOTLIVÝCH ETAP
Ukončení jednotlivých etap v sobě zahrnuje nejen vlastní akt akceptace, ale celý proces dodání produktu, včetně času nutného na převzetí produktu, schválení kvalitativních parametrů, případně provedení testů a zapracování připomínek.


Etapa
Čas
Týden
-1
T
1. měsíc
2. měsíc
3. měsíc
4. měsíc
5. měsíc
6. měsíc
7. měsíc
8. měsíc
9. měsíc
10. měsíc
11. měsíc
12. měsíc
13. měsíc
14. měsíc
5 let
1 2 3 4
5 6 7 8
9 10 11 12
13 14 15 16
17 18 19 20
21 22 23 24
Účinnost smlouvy
Projektové řízení
Příprava projektu
Řešení bezpečnosti
I. Technologické centrum Jihomoravského kraje
Ukončení I. etapy - akceptace
T+3 měsíce
II. Integrace vnitřního systému - Analýza
Ukončení II. etapy - akceptace
T+2 měsíce
III. Datové sklady, manažerské informační systému a nástroje BI - Analýza
Ukončení III. etapy - akceptace
T+3 měsíce
IV. Hostovaná elektronická spisová služba
Ukončení etapy IV. - akceptace
T+4 měsíce
V. Krajská digitální spisovna, Krajský digitální repozitář
Ukončení etapy V. - akceptace
T+6 měsíců
VI. Integrace vnitřního systému - Vytvoření implementačního analytického manuálu a návrh integrace
VI. Integrace vnitřního systému - Implementace a testování
VI. Integrace vnitřního systému - Instalace, integrace a testování
VI. Datové sklady, manažerské informační systému a nástroje BI - Implementace
Ukončení etapy VI. - akceptace
T+12 měsíců
Zkušební provoz
Ukončení projektu - zahájení produkčního provozu
T+14 měsíců
Servis a podpora

Kvalita návrhu integrace nabízeného řešení do ICT prostředí Objednatele a garance dostupnosti

Zhotovitel si plně uvědomuje, že při uzavření smluvního závazku vstupuje do prostředí úřadu, kde jsou již používány ICT, uvědomuje si stejně jako Objednatel, že si realizace projektu vyžádá změny v technickém prostředí a změny v organizaci zaměstnanců Objednatele a to vše nejen bezprostředně po implementaci, ale i průběžně v následném servisu po dobu 5-ti let.

Aby byly eliminovány, v co největší možné míře rizika, vyplývající z těchto změn je třeba vložit do celého procesu vhodnou metodiku řízení, použít informace a dosavadní znalosti o funkcionalitě a architektuře stávajících IS úřadu, navrhnout vhodnou Globální Architekturu, která tyto existující IS hladce začlení a integruje. A to jak systémy interní - zajistí propojení mezi stávajícími a novými IS systémy, které jsou předmětem plnění v oblastech A-E dle zadávací dokumentace, ale i v oblasti integrace předmětu plnění na centrální IS VS a dále komunikaci mezi krajským úřadem a jeho zřizovanými organizacemi.

Předkládaný návrh řešení využívá plnohodnotných a standardních způsobů integrace pro začlenění stávajících aplikací Objednatele. Tvůrcem těchto aplikací je firma Gordic, která je současně subZhotovitelem Zhotovitele. Toto spojení znalostního potenciálu obou firem je dle mínění **hlavní přidaná hodnota** pro Objednatele. Výhody spojení jsou zřejmé:

- Významná úspora času ve všech fázích projektu, díky společným sehraným týmům řešitelů obsazeným zaměstnanci s vhodnou kompetencí, budou velmi rychle proudit potřebné znalosti a informace,
- Konzistentní komunikace mezi Zhotovitelem – SubZhotovitelem pomocí moderních nástrojů pro spolupráci a sdílení informací, jenž obě firmy využívají,
- Smluvně uzavřená motivace Zhotovitele a SubZhotovitele řešit vzniklé situace společně, operativně a efektivně.

Princip a metoda integrace
Zvolená metoda integrace pomocí Integrační platformy postavená na standardu SOA dává návrhu flexibilitu v možnostech realizace vnitřní integrace systému krajského úřadu.
Princip užitý pro integraci komponent je komunikace prostřednictvím webových služeb, jejichž zpracování řídí Sběrnice služeb úřadu (ESB adaptovaná pro potřeby úřadu), které zajistí nezávislost a vychází z nejmodernějších, ale již ověřených postupů například v segmentu výrova a logistika, kde se uvedené koncepty hojně využívají.
Navržený způsob integrace umožní připojit libovolný počet jiných systémů Objednatele s ohledem na výkonnost TC. V době analýzy budou upřesněny technologie, kterými bude možné propojit jednotlivé Agendové Informační Systémy. Již v této době víme, že protokoly budou technologie JMS, HTTP/HTTPS, WS, FILE, FTP, JCA. V té době také budou analyzovány business procesy a funkce, které budou nutné pro integraci jednotlivých systémů tak, aby ulehčili komunikaci v agendách úřadu a napříč podpůrnými procesy úřadu.
Integrace systému JMK bude vedena centrálně přes vrstvu ESB, která je pro integraci nejvhodnější.
Vrstva umožní úřadu následující funkce, které v budoucnu úřad využije:

- Monitorování a řízení výměny zpráv jednotlivých napojených systémů
- Vyřešit komunikační problémy jednotlivých systémů
- Dopsání adaptérů na systémy 3. stran
- Odstranit duplicitní služby
- Kontrolovat nasazení a verzování služeb
- Orchestrovat propojení a postup vyhodnocení a volání integračních služeb
- Mapovat zprávy na jiné
- Nastavit bezpečnost integrace
- Logování a audit provozu
- Efektivnější získávání dat
- Audit jednotlivých operací

- Centrální monitoring integrace
- Globální zpracování chybových stavů, skrz celý systém integrace

Potenciální rizika ohrožení nebo omezení funkcí systému
Kritické oblasti, kde bude systém nejvíce ohrožen, spatřuje Zhotovitel ve dvou rovinách:

- Lidské – selhání osob – tuto část ošetřuje samostatný návrh bezpečnostní architektury a implementace systému vlastního ISMS podle metodiky ISO 27001,

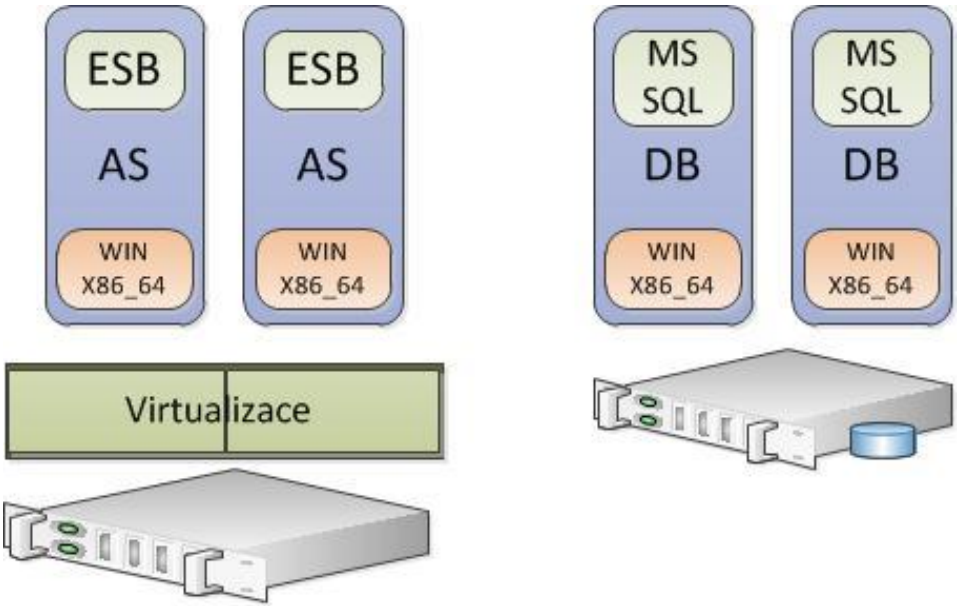
- Technické – tato část je detailněji popsána v následujícím textu.

TECHNICKÁ RIZKA OHROŽENÍ KLÍČOVÝCH ČÁSTI SYSTÉMU

Rizika ohrožení technické části mohou být z globálního pohledu výpadky v serverové, síťové či komunikační infrastruktury.
Proto je **sítová infrastruktura** navržena tak, aby bez jakýchkoliv omezení byla připojitelná na fyzické i logické úrovni **k náhradním komunikačním uzlům** a s rezervou dimenzovaná pro potřeby datových toků ICT prostředí Objednatele.
Design komunikační infrastruktury je **redundantní v každé své komponentě** – na úrovni zdvojení fyzického propojení, zdvojení jednotlivých hardwarových sestav (vzájemná zastupitelnost přepínačů, routerů, balancerů, firewallů, bezpečnostních systémů) i dílčích komponent uvnitř jednotlivých hardwarových sestav (redundantní řídící moduly, Ethernet moduly, zdroje). Výsledkem je zabezpečení ošetřující:

- **Výpadek kterékoliv komponenty nezpůsobí nedostupnost žádné provozované služby sítě**
- **Případná porucha v kterékoliv části sítě nezpůsobí uživateli v čase zřetelnou nedostupnost používané služby**
- **Použité síťové prvky jsou pod servisním kontraktem a technikou podporou jednoho ze dvou největších a nejvýznamnějších výrobců síťových technologií.**

Systémy dodávky technické části B budou využívat prostředků TC JMK. Architektura **hlavní integrační vrstvy je navržena jako samostatná a bude nasazena odděleně od ostatní informačních systémů, z důvodů kritičnosti celé aplikace.** Vlastní integrační platforma (ESB) bude permanentně ukládat svoje metadata data do své vlastní (dedikované) databáze. ESB i DB vrstva bude dostupná v clusteru pro zajištění HA a co možná největšího výkonu.
Řešením výše uvedených předpokladů je virtualizace. ESB bude přímo komunikovat s DB, kde bude perzistovat data. Load balancing předcházející přetěžování systému bude proveden na SW úrovni.



Obrázek – HW architektura ESB

Konfigurace jednoho AS bude 2x CPU Core 2, 4 GB RAM 100 GB HDD s gigovou sítí. Konfigurace jednoho DB bude 2x CPU Core 2, 4 GB RAM 1 TB HDD v RAID 10. Tato konfigurace se představuje dostatečně dimenzovaný výkon pro kritckou část řešení Integrační platformu.

Pro instalaci ESB bude použit hojně užívaný produkt JBoss Enterprise SOA Platform a to zejména JBoss EBS

Výpadky Aplikační vrstvy jsou ošetřeny jejich virtualizací, zálohováním dat s archivací

Garance dostupnosti v režimu 24/7

Zhotovitel garantuje Objednatelem požadovanou dostupnost ve smyslu Objednatelem požadované úrovně poskytovaných služeb servisní podpory (SLA) na úrovni **99,620%** v režimu 24/7, kterou zajišťuje službami podpory v profesionální kvalitě za:

- důsledného dodržování doporučení technologických standardů vyplývajících ze standardů ISO 9001, ISO 20000, ISO 27001, ISO 16001, ITIL a interní projektové metodiky,
- zajištění dostatečného počtu kvalifikovaného personálu,
- proaktivního používání nástrojů Service Desku pro měření a vyhodnocování kvality poskytovaných služeb.

I.A: Detailní popis řešení - TC Jihomoravského kraje

Infrastruktura datového centra

UPS

UPS pro hlavní i záložní lokalitu je nabízená ve stejné konfiguraci.
Jedná se o plně redundantní modulární řešení UPS Eaton BladeUPS o celkovém výkonu 24 kW (12 kW n+1). Jedná se o UPS určenou pro instalaci do standardního racku s možností dalšího rozšiřování výkonu i doby zálohy v budoucnu. Údržba, servis i rozšiřování výkonu je možné provádět za provozu bez výpadku napájení kritických IT technologií.
UPS pracuje s vysokou účinností, až 98%, a má proto minimální tepelné ztráty. Je vybavena technologií ABM zajišťující podstatné prodloužení životnosti baterie ve srovnání s tradiční metodou dobíjení, dále technologií Hot-Sync, která zajišťuje snadné modulární rozšiřování UPS systému o další kapacitu nebo redundanci, neobsahuje slabý článek (single point of failure).
Systém UPS bude vybaven SNMP kartou pro vzdálený dohled a správu, dodávaný SW PowerVision Network edition zajišťuje v součinnosti se SNMP kartou řízený shutdown všech běžných OS včetně integrace do virtualizovaných prostředí.

REDUNDANCE UPS

Potřebný elektrický příkon nabízených technologií v hlavní lokalitě je cca 9200W, v záložní lokalitě je to cca 8200W. V obou případech bude tedy nabízené řešení s redundantním výkonem 12 kW plně vyhovující potřebám s úrovní redundance n+1. V případě budoucího navýšení výkonu je možné zvýšení výkonu UPS pouhým dalším doplněním výkonového/bateriového modulu.

KLIMATIZACE

Pro obě lokality je nabízeno řešení přesné klimatizace výrobce Emerson Network Power. Nabízené řešení pro hlavní a záložní lokalitu se vzhledem k prostorovým možnostem daných místností liší způsobem distribuce chladicího vzduchu.
V obou případech jsou nabízeny moderní vysoce účinné přesné klimatizace, jednotky jsou vybaveny kompresory s plynule regulovatelným výkonem, EC ventilátory a venkovními kondenzátory s nízkou hlučností a nízkou spotřebou elektrické energie. Jednotky jsou nabízeny včetně integrovaných zvlhčovačů pro plné řízení prostředí (teplota i vlhkost) datového centra. Klimatizační jednotky jsou vybaveny LAN kartou pro vzdálený dohled. Jednotky budou provozovány tak, že v provozu bude vždy jedna klimatizační jednotka v dané lokalitě s automatickým střídáním po nastavené době, a v případě poruchy/servisu dojde k automatickému přepnutí na záložní jednotku.
Pro **hlavní lokalitu** je vzhledem k nízké zdvojené podlaze a nemožnosti umístění podstropních klimatizačních navrženo řešení postavené na mezirackových chladicích jednotkách s distribucí studeného vzduchu přímo před racky a nasáváním ohřátého vzduchu v zadní části jednotek. Jedná se tedy o horizontální proudění chladicího vzduchu. Konkrétně se jedná o n+1 redundantní řešení se dvěma jednotkami CRV20 s redundantním chladicím výkonem 23 kW.
Pro **záložní lokalitu** jsou vzhledem k možnosti využití zdvojené podlahy pro distribuci chladného vzduchu nabízeny jednotky s distribucí vzduchu do zdvojené podlahy a nasáváním ohřátého vzduchu vrchem. Konkrétně se jedná o n+1 redundantní řešení se dvěma jednotkami D2EUA s redundantním chladicím výkonem 23 kW.

REDUNDANCE KLIMATIZAČNÍHO SYSTÉMU

Celkové vyzářené teplo dodávaných technologií je v každé z lokalit je <10 kW. Redundantní výkon nabízeného klimatizačního systému je v obou případech 23 kW. Chladicí výkon je plně plynule regulovatelný v rozmezí 30-100%, tedy od cca 7 kW. Vzhledem k náročnějšímu eventuálnímu rozšiřování systému chlazení (stavební úpravy apod.) je zvoleno řešení s vyšším počátečním výkonem optimalizované z pohledu provozních nákladů, které pokryje i zvýšené potřeby technologií do budoucna. Je samozřejmě možné využití nabízeného systému chlazení i pro stávající technologie a snížení provozních nákladů spojených s provozováním stávajících klimatizačních jednotek.

Serverová infrastruktura

Serverová Infrastruktura je tvořena dvojicí Blade šasi HP c7000 (každé bude umístěno do jedné lokality). Každé šasi obsahuje 4 vysoce výkonné servery pro virtualizaci, jeden server pro backup či management a prvky připojující Blade šasi k LAN a SAN infrastruktuře.

BLADE ŠASI

Blade šasi HP c7000 pojme až 16 serverů a 8 propojovacích (I/O) modulů v redundantním uspořádání. Šasi je vybaveno pasivní, multi terabitovou vysoce výkonnou sběrnicí propojující servery s I/O moduly. Napájení je zajišťováno prostřednictvím sdružené napájecí sběrnice, která zajišťuje, že plná kapacita redundantních napájecích zdrojů je k dispozici všem serverům.

Každé Blade šasi HP c7000 je vybaveno následujícími funkcemi:

- velikost blade šasi je 10U (rack unit)
- pojme až 16 serverů poloviční velikosti
- umožnuje současné připojení až ke čtyřem různým propojovacím infrastrukturám (Ethernet, Fibre Channel, Infiniband, SAS)
- Redundantní připojení do LAN infrastruktury pomocí dvojici ethernet modulů Virtual Connect Flex-10
- Redundantní připojení do SAN infrastruktury pomocí dvojici fibre channel modulů Virtual Connect Fibre Channel
- umožňuje napájení z jedno-fázových, tří-fázových nebo 48V stejnosměrných napájecích rozvodů
- 6 napájecích zdrojů v konfiguraci N+N umožňující připojení dvou nezávislých napájecích větví (až polovina zdrojů může vypadnout bez omezení provozu). Zdroje jsou redundantní, za provozu vyměnitelné, s prediktivním rozpoznáváním poruch. Zdroje podporující řízení výkonu v závislosti na spotřebě CPU v instalovaných serverech
- 10 redundantních ventilátorů Active Cool 200 s prediktivním rozpoznáváním poruch zajišťuje nepřetržité chlazení blade šasi při zachování minimální hlučnosti (řízení rychlosti otáček dle aktuálního zatížení instalovaných komponent)
- Všechny prvky blade šasi jsou redundantní a umožňují výměnu za provozu (ventilátory, napájecí zdroje, redundantní I/O moduly, management moduly)

.

Management modul (BladeSystem Onboard Administrator) je vestavěný redundantní modul s následujícími funkcemi:

- dedikovaný ethernet port
- integrovaný KVM přepínač
- paralelní vzdálený přístup k více serverům
- reportování všech inventárních informací o nainstalovaných komponentách
- reportování teplotních informací a informací o spotřebě jednotlivých serverů i celého blade šasi
- zepředu blade šasi namontovaným informačním displejem s ovládáním
- poskytuje sigle sign-on přístup ke všem zařízením v blade šasi
- bezpečnostní model založený na rolích (Role-based security)
- Přístup ke všem iLO management rozhraním serverů přes jeden kabel
- Přístup ke všem management rozhraním I/O modulů přes jeden kabel

Obrázek – Blade šasi s reálným osazením serverů, I/O modulů a ostatních prvků

LAN PRVKY V BLADE ŠASI

HP Virtual Connect Flex-10 Ethernet modul

Každé Blade šasi je vybaveno dvojicí Ethernetových modulů Virtual Connect Flex-10, představující novou třídu propojení blade šasi, které zjednodušuje připojení serveru tím, že jasně odděluje skříň serveru od sítě LAN, zjednodušuje sítě redukcí kabeláže bez přidání dalších přepínačů a umožňuje změnit servery a doladit rychlosti sítě podle potřeb aplikace v pouhých minutách.
S modulem Virtual Connect Flex-10 lze zjednodušit propojení sítí LAN, konsolidovat a přesně řídit jejich síťová propojení a umožnit správcům rychle přidávat, nahrazovat a obnovovat serverové prostředky.
Modul Virtual Connect Flex-10 poskytuje optimalizaci sítě tím, že umožňuje správcům doladit šířku pásma sítě na straně připojení serverů. To se provádí rozdělením každého 10Gb síťového připojení na čtyři

nezávislá fyzická serverová připojení vNIC. Každé připojení vNIC lze nastavit vLAN a rychlost v rozsahu od 100 Mb do 10 Gb, takže můžete využívat správnou šířku pásma na základě potřeb aplikací.

Základní vlastnosti

- 8x 10Gb ethernetových portů SFP+ nabízí vysoce výkonné možnosti pro odchozí připojení s volitelnou podporou připojení pomocí optických kabelů nebo měděných kabelů
- Modul je vybaven 2x SFP+ 10Gb/s ethernet optickým modulem (1x ShortRange, 1x Long range). Celková konektivita Blade šasi do LAN je 4x 10Gb/s.
- 16x 10Gb příchozích připojení směrem od serverů podporuje 1Gb nebo 10Gb síťové porty nebo až 4 karty FlexNIC na jedno 10Gb připojení
- 2 x 10Gb cross connects pro redundanci a stohování
- 1 x 10Gb metalický odchozí CX-4 port pro stohování Virtual Connect modulů nebo pro odchozí připojení k centrálním LAN switchům
- Podpora pro všechny 1Gb a 10Gb síťové karty v serverech (integrované na základní desce i v rozšiřujících slotech)
- Přepínací kapacita - Line Rate, full-duplex 480 Gbps
- Latence 1.5 µs
- MTU až do 9216 Bytes - Jumbo Ethernet rámce
- Podpora vLAN (802.1Q), až 4,096 vLANs podporováno v tunelovacím režimu a 1000 vLANs v mapovacím režimu
- Možnost definice privátních VLAN
- Možnost nastavení Ethernet NIC MAC adres
- Možnost nastavení Boot parametrů serverů

Funkce dostupnosti:

- Protokol pro agregaci spojení (802.3ad)
- Automatická ochrana proti smyčce
- Podpora protokolu 802.1AB
- Podpora sdružování síťových karet na straně serverů NIC teaming/bonding
- Zrcadlená profilová databáze
- Přenášení prezenčních signálů mezi redundantními moduly několika cestami

Funkce správy:

- Jednoduché a intuitivní grafické uživatelské rozhraní a průvodce instalací dostupné přes protokol HTTP/S
- Bezpečné skriptovací rozhraní příkazového řádku CLI
- Integrovaný management systém podporující XML API
- Integrované rozhraní SNMP v1, v2
- „port mirroring“ pro porty serveru na libovolném portu pro odchozí připojení
- Bezpečnost založená na rolích (Role-based security) pro administraci kompatibilní s LDAP, TACACS+ and RADIUS
- Pro administrátory LAN infrastruktury se modul Virtual Connect Flex-10 jeví jako „Pass-Thru“ zařízení

SAN PRVKY V BLADE ŠASI

HP Virtual Connect Fibre Channel modul

Virtual Connect Fibre Channel modul pracuje jako agregátor několika FC host bus adaptérů přes jeden nebo několik odchozích „N-portů“ pomocí virtualizace N_port_ID (NPIV). Technologie NPIV umožňuje Fibre

Channel switchům aby rozpoznaly více identifikátorů WWNs za jedním N-portem. Tím je dosaženo bezproblémové integrace do SAN infrastruktury různých výrobců.

Konektivita k SAN infrastruktuře

- Podpora technologie NPIV
- Každý Virtual Connect Fibre Channel modul podporuje připojení až do osmi SAN „Fabric“ a je připojen do centrálních SAN prvků, které jsou nakonfigurovány pro podporu NPIV. Výsledkem je, že se jednotlivé host bus adaptéry v serverech chovají jako přímo připojené k centrálním FC switchům. Z pohledu SAN infrastruktury se Virtual Connect Fibre Channel Moduly jeví jako „pass-thru“ zařízení.
- Rychlost každého z osmi odchozích portů (uplinků) je volitelná z 2, 4 nebo 8 Gb/s.
- Modul je vybaven 4x Fibre Channel SFP+ 8Gb/s optickým modulem. Celková kapacita připojení Blade šasi do San je 8x 8GB/s

Funkce správy:

- Jednoduché a intuitivní grafické uživatelské rozhraní a průvodce instalací dostupné přes protokol HTTP/S
- Bezpečné skriptovací rozhraní příkazového řádku CLI
- Integrované rozhraní SNMP v1, v2
- „port mirroring“ pro porty serveru na libovolném portu pro odchozí připojení
- Bezpečnost založená na rolích (Role-based security) pro administraci kompatibilní s LDAP, TACACS+ and RADIUS
- Možnost přidělování vlastních předdefinovaných adres WWN serverům
- Není potřeba další doménové ID
- Každý server má nakonfigurovaný profil s potřebnými údaji, který je možno mezi servery libovolně přesouvat

Výkonnost

- 8x 2/4/8Gb Fibre Channel odchozích portů připojených do centrálních SAN switchů
- 16x 1/2/4/8Gb Fibre Channel příchozích portů směrem od serverů
- Agregace HBA na odchozích portech s použitím ANSI T11 standardu
- Extrémně nízká latence.

SERVERY

8 ks serverů

Nabízené servery pro virtualizaci jsou vysoce výkonné servery HP BL685c. Každý server je vybaven:

- čtyři 16jádrové procesory AMD Opteron 6276 2,3 GHz poskytují výjimečný výpočetní výkon (celkový počet výpočetních jader v serveru je 64)
- 128 GB registrované paměti DDR3 DIMM s pokročilou ochranou ECC, 1333 MHz
- Rozšiřitelnost paměti až na 1 TB
- Vysoce výkonný řadič Smart Array P410i polí RAID 0,1,5 s 1GB modulem mezipaměti se zálohováním pamětí flash
- dva disky SAS 72 GB 15k RPM v malém provedení (SFF) připojitelné za provozu (rychlost SAS rozhraní je 6Gbps)
- Interní port USB a slot na karty MicroSD
- Podpora technologie Integrated HP Virtual Connect Flex-10
- Dva vestavěné NC551i síť. Adaptéry, každý se 2 porty a propustností 10 Gb/s zaručují dostatečnou šířku pásma pro aplikace náročné na síťový provoz
- Celková šířka pásma v jednom serveru pro připojení do LAN je 40 Gb/s

- Každý 10Gb/s port je možno rozdělit na 4 nezávislé vNIC, celkem 16 vNIC
- Šířku pásma sítě lze rozdělit a vyladit tak, aby přesně vyhovovala požadavkům aplikací. Omezení šířky pásma je možno nastavit pro každý vNIC v rozsahu 100Mb/s – 10 Gb/s
- Optimalizace účinnosti serveru díky snižování zátěže protokolu TCP/IP
- Integrovaný nezávislý procesor pro vzdálenou správu iLO3
    - vzdálené vypínání a zapínání serveru
    - plně integrovanou grafickou konzoli s možností sdílení až čtyřmi uživateli současně
    - připojení virtuálních médií (FDD, DVD, ISO, USB klíče, 1GB adresáře pro čtení)
    - "Windows" konzole s rozlišením až 1600x1200
    - JAVA konsole
    - možnost přesměrování terminálových služeb Windows na dedikovaný management port
    - možnost záznamu a následného přehrání video záznamu chybové obrazovky a následného restartu
    - možnost využití běžných www prohlížečů integrovaných v desktopových OS
    - kódování AES a 3DES pro zabezpečení komunikace s běžnými www prohlížeči
    - CLP a XML rozhraní pro skriptování

Pro ověření výkonnosti nabízených serverů přikládáme odkaz na veřejně dostupné výsledky publikované na webu http://www.spec.org/
http://www.spec.org/cpu2006/results/res2011q4/cpu2006-20111025-18740.html
http://www.spec.org/cpu2006/results/res2011q4/cpu2006-20111025-18742.html

SERVERY

2 ks serverů

Nabízené servery pro účely zálohování a správy celého prostředí jsou servery HP BL465c. Každý server je vybaven:

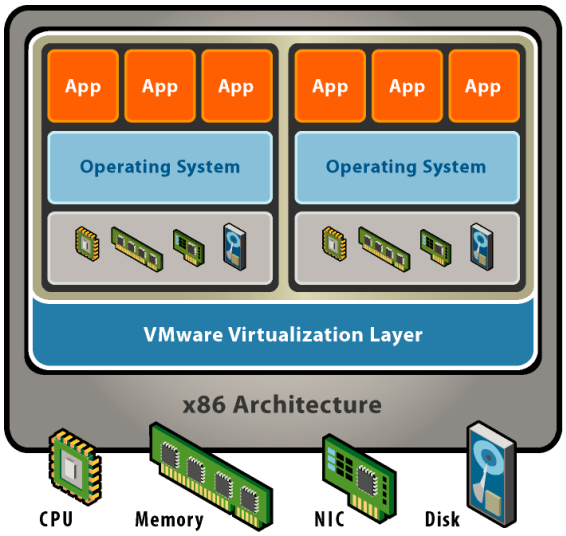
- jeden 16jádrový procesory AMD Opteron 6276 2,3 GHz (celkový počet výpočetních jader v serveru je 16)
- Možnost rozšíření na dva procesory
- 16 GB registrované paměti DDR3 DIMM s pokročilou ochranou ECC, 1333 MHz
- Rozšiřitelnost paměti až na 512 GB
- Vysoce výkonný řadič Smart Array P410i polí RAID 0,1,5 s 1GB modulem mezipaměti se zálohováním pamětí flash
- dva disky SAS 142 GB 15k RPM v malém provedení (SFF) připojitelné za provozu (rychlost SAS rozhraní je 6Gbps)
- Interní port USB a slot na karty MicroSD
- Podpora technologie Integrated HP Virtual Connect Flex-10
- Jeden vestavěný NC551i síť. Adaptér, se 2 porty a propustností 10 Gb/s
- Celková šířka pásma v jednom serveru pro připojení do LAN je 20 Gb/s
- Každý 10Gb/s port je možno rozdělit na 4 nezávislé vNIC, celkem 8 vNIC
- Šířku pásma sítě lze rozdělit a vyladit tak, aby přesně vyhovovala požadavkům aplikací. Omezení šířky pásma je možno nastavit pro každý vNIC v rozsahu 100Mb/s – 10 Gb/s
- Optimalizace účinnosti serveru díky snižování zátěže protokolu TCP/IP
- Integrovaný nezávislý procesor pro vzdálenou správu iLO3
    - vzdálené vypínání a zapínání serveru
    - plně integrovanou grafickou konzoli s možností sdílení až čtyřmi uživateli současně
    - připojení virtuálních médií (FDD, DVD, ISO, USB klíče, 1GB adresáře pro čtení)
    - "Windows" konzole s rozlišením až 1600x1200
    - JAVA konsole

- možnost přesměrování terminálových služeb Windows na dedikovaný management port
- možnost záznamu a následného přehrání video záznamu chybové obrazovky a následného restartu
- možnost využití běžných www prohlížečů integrovaných v desktopových OS
- kódování AES a 3DES pro zabezpečení komunikace s běžnými www prohlížeči
- CLP a XML rozhraní pro skriptování

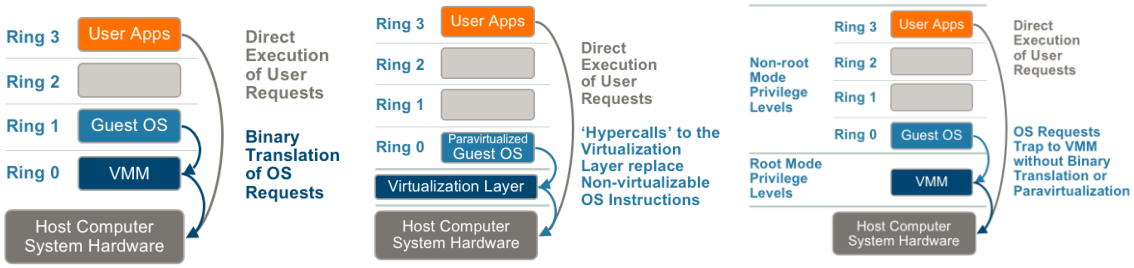
Serverová virtualizace

VIRTUALIZACE V HLAVNÍM A ZÁLOŽNÍM DATOVÉM CENTRU

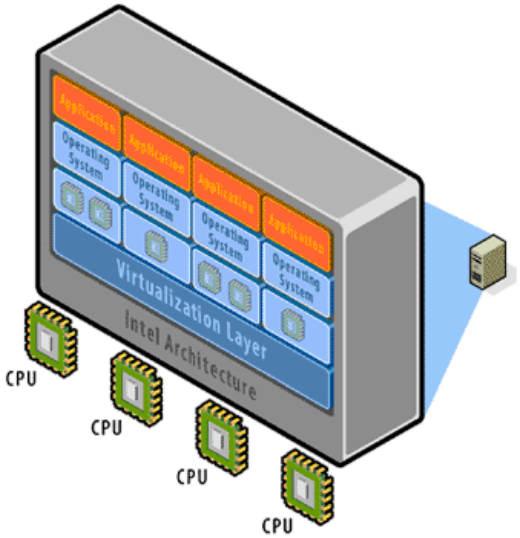
V každém datovém centru instalováno jedno blade šasi se 4 blade servery. Celkem tedy budou pro virtualizaci použita2 šasi a 8 blade serverů. Pro serverovou virtualizaci x86 výpočetního výkonu v hlavním a záložním datovém centru je použit produkt VMware vSphere 5.0. Tento ESXi hypervizor je instalován přímo na hardware serveru a umožňuje plnou virtualizaci x86 strojů.



Mezi virtualizační technologie, které tento hypervizor podporuje, patří paravirtualization, binary translation a hardware assist. Produkt podporuje umístění kompletního prostředí včetně OS a aplikací do virtuálních strojů bez závislosti na provozovaném hardware. Virtualizace a agregace x86 strojů a k nim připojených síťových a datových úložišť do unifikovaných souborů zdrojů je funkcionalitou tohoto produktu. Je možná škálovatelnost pro možnost podpory IT prostředí jakékoliv velikosti. Vlastností produktu je symetrický multiprocesing zlepšující výkonnost virtuálního stroje a umožňující, aby jediný virtuální stroj využíval několik fyzických procesorů současně. Součástí je centralizované řízení umožňující nastavení jednoduchého a plně automatického disasterrecovery řešení (konfigurace, testování, výpadek, obnova).



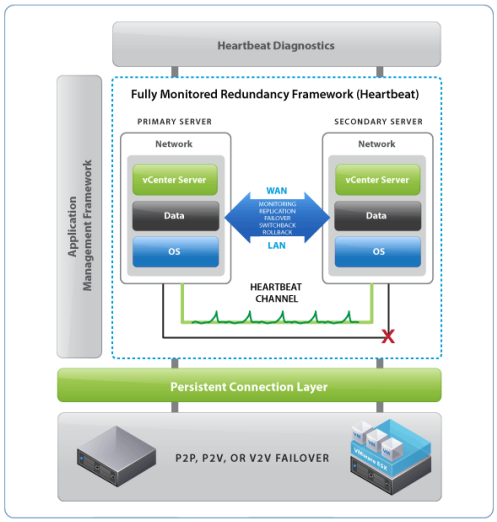
ESXi hypervizor umožňuje vytvářet výkonné virtuální stroje až s 32 vCPU (licence vSphere Enterprise Plus), kdy jsou využity všechna jádra fyzického CPU. Hypervizor periodicky cykluje mezi fyzickými jádry, čímž je zajištěno rozložení zátěže mezi jednotlivé CPU.



Ve vSphere vCenter bude vytvořeno jedno virtuální datacentrum obsahující všech 8 vSphere ESXi 5.0 serverů. Tato infrastruktura umožňuje kompletní virtualizaci prostředí, ovšem je vysoce doporučeno, aby alespoň jeden doménový řadič běžel mimo virtuální farmu. Výhodou virtualizace strojů je mimo jiné i kompletní hardwarová nezávislost, kdy je pro celé prostředí použit jednotný virtuální hardware poskytnutý hypervizorem ESXi. Pro účely správy a provozu budou vytvořeny role s granulárními oprávněními na jednotlivé části vSphere vCenter serveru. Jedná se například o roli operátora, která umožňuje provádět standardní úkony správy virtuálních serverů, jako například, vypnutí a zapnutí, ale již neumožňuje vytváření nových virtuálních severů, nebo změnu parametrů existujících serverů. Definice rolí budou stanoveny na základě analýzy požadavků zákazníka a pomohou vymezit oprávnění nad virtualizačním řešením např. mezi správci systému, operátory nebo Zhotovitelem poskytující support.
Primárním datovým úložištěm bude řešení FalconStor NSS, které vytvoří pro vSphere servery vizualizovaný úložný prostor tvořený synchronními replikami v hlavním a záložním datovém centru. Umístění primárních a replikovaných LUN bude pro vSphere servery transparentní, servery v obou datových centrech budou mít prezentovány stejné LUN, ke kterým budou přistupovat transparentně do jednoho z datových center.
V případě výpadku jednoho z nodu diskového pole v jednom z datových center budou LUNy z padlého nodu automaticky přesunuty do druhého datového centra a vSphere servery k nim budou mít zachovány přístup bez nutnosti rekonfigurace. Na sdíleném datovém úložišti budou ležet všechny virtuální stroje, které mají jednotnou formu pro celé prostředí. Tato datová struktura se sestává z adresářů na VMFS filesystemu, které mají stejný název jako virtuální stroje a ve kterých jsou uloženy soubory konfigurace virtuálního stroje, virtuální disky, soubory snapshotů, stránkovací soubor apod. Každý virtuální stroj se nachází v jednom adresáři, tudíž je snadná identifikace souborů patřících danému stroji.

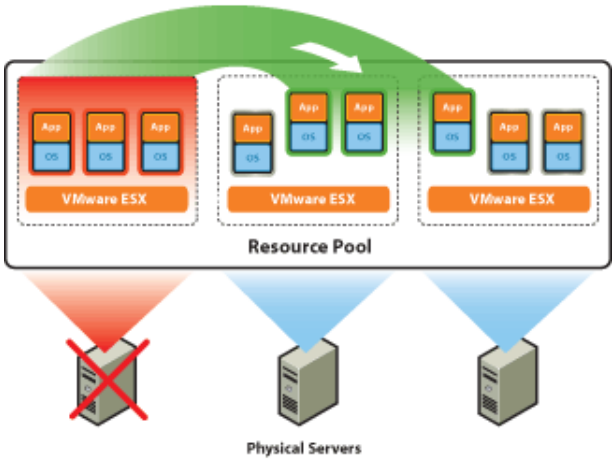
VYSOKÁ DOSTUPNOST VCENTER SERVERU V HLAVNÍM A ZÁLOŽNÍM DATOVÉM CENTRU

Řešení obsahuje centralizované řízení zajišťující automatický provoz, optimalizaci zdrojů a vysokou dostupnost IT prostředí. vCenter Server je software pro management farmy vSphere serverů, který běží jako služba na OS Windows 2008 R2. Při jeho nedostupnosti je správa vSphere serverů značně omezená, kdy je nutno se hlásit na každý ESXi server jednotlivě. Vysoká dostupnost vCenter serveru bude zajištěna vytvořením jedné instance serveru v každém datovém centru a jejich propojením do clusteru pomocí software vCenter Server HeartBeat. Takto vybudovaná virtuální infrastruktura umožní snadnou správu robustního prostředí až do velikosti 1000 ESXi hostů a rozběhnout současně až 10000 virtuálních strojů. Při linkovaném propojení až 10-ti vCenter serverů je možné toto prostředí až třikrát zvětšit. Jestliže uvážíme, že lze takováto prostředí budovat opakovaně vedle sebe, jsou možnosti škálování v podstatě neomezené.



VYSOKÁ DOSTUPNOST VIRTUÁLNÍCH SERVERŮ V HLAVNÍM A ZÁLOŽNÍM DATOVÉM CENTRU

Dostupnost virtuálních serverů mezi hlavním a záložním datovým centrem bude zajištěna pomocí VMware High Availability (VMware HA). Funkce VMware HA sdružuje vSphere servery do clusteru. V tomto clusteru jednotlivé vSphere servery navzájem komunikují a při zjištění nedostupnosti některého člena clusteru zajistí restartování virtuálních severů, které na něm běžely, na zbylých serverech clusteru.



VMware HA je určena primárně pro nasazení v rámci jednoho datového centra, ale díky virtualizaci datového úložiště mezi datovými centry pomocí FalconStor NSS můžeme na obě datová centra nahlížet jako na jedno. Nasazení VMware HA ve dvou datových centrech při existenci FalconStor NSS je podporováno firmou VMware.

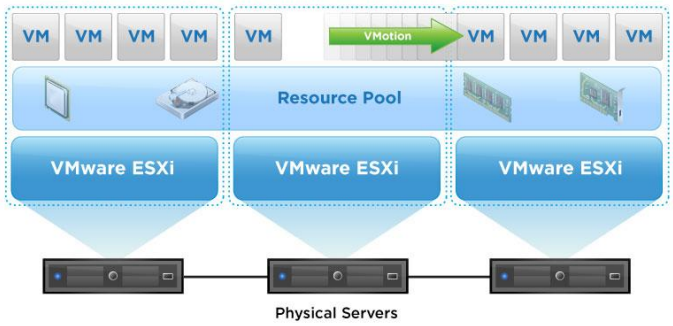
Bude tedy vytvořen HA cluster, který bude obsahovat vSphere servery z obou datových center a v případě výpadku jednoho nebo i všech serverů v jednom datovém centru zajistí VMware HA restart virtuálních serverů na funkčních vSphere serverech.

Vytvoření HA clusteru v obou datových centrech má jedno technické omezení. V každém HA clusteru je 5 serverů tzv. primárních a ostatní jsou sekundární. Primární servery jsou řídící severy HA clusteru, které rozhodují a řídí fail-over akce v případě výpadku některých serverů. Primární servery jsou vybírány náhodně a při každé rekonfiguraci HA clusteru se primární servery určují náhodně znovu. Pro funkčnost HA clusteru musí fungovat alespoň 1 primární server. Tuto podmínku zajistíme tak, že při vytváření HA clusteru budou jeho členem v jednom datovém centru maximálně 4 vSphere servery.

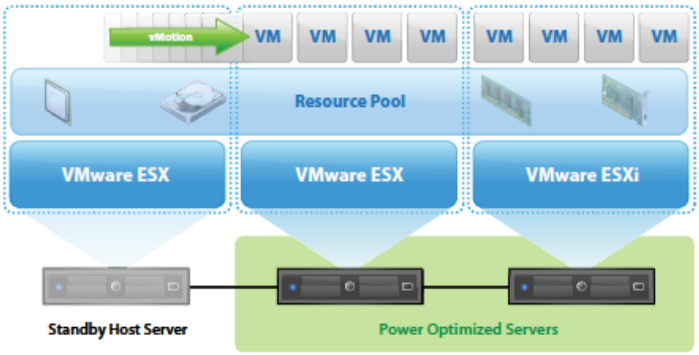
Při 8 ESXi serverech tuto podmínku splníme, tudíž můžeme vytvořit pouze 1 HA cluster. Aby HA cluster poskytoval ochranu při havárii všech vSphere severů v jednom datovém centru, je nutno, aby bylo vyhrazeno 50% výpočetní kapacity serveru jako rezerva (pro fail-over jedné z lokalit).

Nepřetržitý monitoring všech host serverů ve zdrojovém poolu zajišťuje v případě detekce selhání host serverů automatické iniciování procesu restartování všech dotčených virtuálních strojů na zbývajících host serverech.

V rámci HA clusterů je použita funkce DRS (Dynamic Resource Scheduler), která zajišťuje plně automatizovaný load balancing zdrojů. Tím bude zajištěno rovnoměrné rozložení výkonu mezi všechny ESXi server v HA clusteru a nedojde k přetížení jednoho ESXi server na úkor jiného. Pro funkci DRS je využita technologie vMotion, která umožňuje migraci virtuálního stroje z jednoho ESXi server na jiný ESXi server v HA clusteru bez výpadku. Jedná se tedy o migraci virtuálních strojů za provozu zajišťující tak plynulou správu a údržbu IT. Součástí je inteligentní alokace zdrojů na základě předdefinovaných pravidel.



Naopak jestliže nejsou prostředky ESXi server využity (mimopracovní doba, víkendy, svátky…), technologie DPM (Distributed Power Management) umožní online migraci (konsolidaci) virtuálních strojů na tolik ESXi serverů, které jsou nezbytné pro běh virtuálních strojů a nevyužité ESXi server přepne do standby modu (snížení nákladů na el. energii, klimatizaci…). Při potřebě zvýšení výpočetního výkonu jsou opět ESXi server probuzeny ze standby modu a stroje automaticky migrovány dle potřeby zdrojů. Je tedy zajišťena konsolidace zátěže a potřeb virtuálních strojů na menší počet fyzických serverů v případě nižších požadavků na výkon včetně jejich přenosu bez ztráty spojení a jejich následný pohyb zpět na základě změny požadavků.



VMware DPM automatically powers off physical servers to reduce power consumption in datacenters.

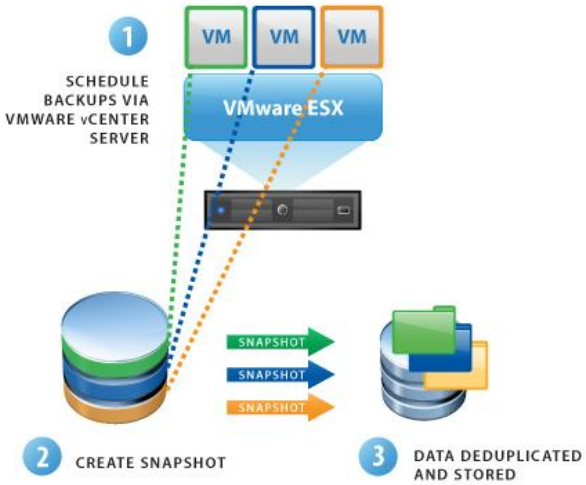
Pro hromadnou správu výpočetního výkonu jsou použity resource pooly, pomocí kterých můžeme rezervovat a omezovat výpočetní výkon HA clusteru pro skupiny virtuálních serverů nebo pouze pro jednotlivé stroje. Tyto zdroje lze za provozu dynamicky měnit či ladit. Je tedy možný kontinuální dynamický balancing aplikačního výkonu nad dostupnými HW zdroji.

MIGRACE STÁVAJÍCÍHO VIRTUALIZAČNÍHO ŘEŠENÍ

Stávající virtualizační severy mohou propojením SAN fabricu a připojením LUNů k novému diskovému subsystému FalconStor NSS migrovány na novou storage a nové ESXi servery. Pokud je stávající edice vSphere serveru Enterprise, lze tuto migraci provést bez výpadku.

VMWARE ZÁLOHOVÁNÍ VDR (VMWARE DATA RECOVERY)

Jako jednoduché a centralizované LAN zálohovací řešení v prostředí VMware vSphere je použit zálohovací systém VMware Data Recovery. Toto řešení se sestává z řídící backup appliance, ke které se připojí disk pro ukládání záloh (vmdk, CIFS, RAW) a zde jsou uloženy jednotlivé zálohy virtuálních strojů včetně katalogu. Ovládání záloh se provádí jednoduše přes konzoli vCenter serveru, stejně tak obnova záloh. Při spuštění zálohovacího plánu je vytvořen snapshot, do kterého se zapisují změny dat během zálohování. Změny ze snapshotů jsou po záloze propsány na virtuální disky. Data jsou na cílových discích deduplikována.



Datová úložiště

Nabízená datová úložiště umožní vybudování vysoce dostupného a škálovatelného prostředí pro ukládání aplikačních a uživatelských dat v prostředí Objednatele. Základní vlastností datových úložišť je jejich vysoká modularita jak v oblasti výkonu, tak v oblasti kapacity. Datová úložiště jsou rozdělena do celkem čtyř vrstev (Tier). Tři vrstvy (Tier0, Tier1 a Tier 2) jsou součástí diskové virtualizace, Tier 3 pak plní funkci dlouhodobého archivního úložiště.

Tier 0 Storage - Enterprise Flash Storage (EFS)

Enterprise Flash Storage (EFS) představuje novou generaci zařízení pro ukládání dat s extrémně vysokou propustností při sekvenčním i transakčním zpracování. EFS je založeno na technologii FusionIO ioDrive nebo ioDrive Duo (NAND Flash paměti) a instaluje se přímo do podnikových SAN pro využití aplikacemi s vysokými požadavky na transakční výkonnost, nebo jako zařízení s nejvyšším výkonem pod správu "virtualizačních" systémů. Řešení s využitím EFS je možné snadno škálovat a dosáhnout tak transakčního výkonu vyššího než 1 milion IOPS.

TECHNICKÝ POPIS

Dodávané EFS je založeno na 2U serveru HP DL 385 G7 v provedení se dvěma 8Gb/s FC porty a kapacitou 640 GB, kterou zajišťuje integrovaná NAND Flash FusionIO ioDrive Duo. Do prostředí SAN je možno exportovat až 256 logických svazků. Zápis do flash paměti je trvalý a nehrozí tak nebezpečí ztráty dat při výpadku napájení. EFS se také vyznačuje velmi nízkou energetickou náročností, takže je vhodná pro budování pokročilých systémů Enterprise Storage, které disponují vysokým výkonem a nízkou spotřebou. Zařízení je dále rozšiřitelné o další FusionIO NAND Flash karty, čímž je možno dosáhnout nejen vyšší kapacity (až 3,5 TB), ale i několikanásobně vyššího výkonu.
Navrhované zařízení je vybaveno EFS softwarem, který zajišťuje komunikaci přímo se prostředky diskové virtualizace FalconStor NSS a je tak možno využít veškerých funkcí virtualizační vrstvy pro výraznou akceleraci I/O operací prostřednictvím automatického tieringu SafeCache nebo HotZone, případné přímým připojením, jako produkčního svazku pro velmi náročné aplikační systémy.

VÝKONNOSTNÍ CHARAKTERISTIKA

Read Bandwidth (64KB)	1,5 GBps
Write Bandwidth (64KB)	1,0 GBps
Sequential Read IOPS (512 Bytes)	196 000

Sequential Write IOPS (512 Bytes)	285 000
Mixed IOPS (75/25 R/W)	138 000
Access Latency (512 Bytes)	29 µs

Tier 1, Tier2
Nabízená disková pole HP P6500 Enterprise Disk Array (jedno do každé lokality) jsou disková pole modulárního designu třídy Enterprise. Každé z polí disponuje těmito vlastnostmi:

- Redundantní napájení
- 2x řadič v režimu Active-Active (přístup k libovolnému svazku je možný přes oba řadiče pro zvýšení propustnosti)
- 8x 8Gb/s FC host porty (čtyři 8 Gb/s FC host porty na řadič)
- 8GB cache (4GB na řadič), baterie zálohující cache v nezávislém, samostatně vyměnitelném modulu pro každý kontrolér
- možnost kombinovat HDD technologie SAS a Mid-line SAS v jedné diskové polici
- možnost přidání dalších disků až do celkového počtu 450
- možnost připojení dalších rozšiřujících diskových polic až do celkového počtu 20, způsob propojení diskových polic umožňuje fungování zbylých diskových polic i při výpadku jedné police
- velikost diskových řadičů 2U (každý), celková velikost nabízeného diskového pole je 14U
- podpora RAID typu 0, 1, 5, 6, 1+0, 5+0, 6+0
- podpora několika různých RAID uspořádání na stejných fyzických discích
- podpora velikosti LUN až 32TB
- automatický loadbalancing a rozmístění dat na všechny disky v okamžiku přidání nových disků
- podpora funkcí Thin Provisioning, s možností automatického zvětšování a zmenšování svazků podle datového obsahu pro OS MS Windows
- možnost rozšíření o funkce lokálních kopií typu Snapshot (bez nutnosti rezervace kapacity), Clone, kombinace snapshot a clone a podpora technologie split-mirror
- možnost rozšíření o funkce replikace a synchronního mirroru mezi dvěma HP EVA diskovými poli na úrovni pole
- součástí dodávky je licence managementu a základního provozu diskového pole na neomezenou diskovou kapacitu a neomezený počet připojených hostů (serverů) včetně softwaru pro MultiPathing
- Součástí nabídky vzdálený je vzdálený dohled support centrem výrobce
- Diskové pole je certifikováno pro použití s nabízenou diskovou virtualizací IPStor NSS a serverovou virtualizací VMware vSphere 5.0.

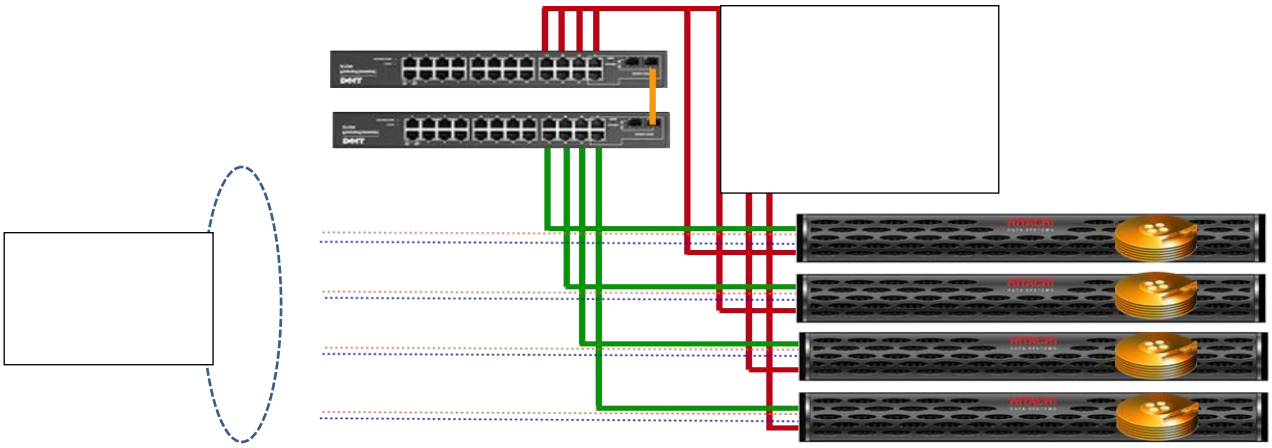
Disky pro Tier 1

- Každé diskové pole obsahuje 36 ks 600GB 6G SAS 15K 3.5in hard disků, které poskytují čistou kapacitu 10,2 TB při uspořádání RAID 10

Disky pro Tier 2

- Každé diskové pole obsahuje 20 ks 2TB 6G SAS 7.2K 3.5in NL-SAS hard disků, které poskytují čistou kapacitu 32 TB při uspořádání RAID 6

TIER 3 - Garantované úložiště Hitachi content platform – archivní úložiště HCP 300
Hitachi Content Platform (HCP) je vysoce škálovatelné, otevřené a spolehlivé řešení pro aktivní digitální archiv pro datová centra všech velikostí. Je navrženo tak, aby mohlo být velmi jednoduše integrováno do existující infrastruktury.
Systém je založen na skupině společně fungujících archivních nodů s jasně definovaným a neměnným rozhraním, jak pro vnitřní, tak pro externí komunikaci (přes kterou je možné definovat metadata k uloženým digitálním archiváliím).



Technologie archivního úložiště je tak připravené na to, aby v průběhu svého života a za provozu bez složitých datových migrací, bylo schopno přijímat nový hardware (archivní nody) a případně vyřazovat morálně zastaralý hardware. Tímto je zajištěna průběžná kontinuita dat a tedy splnění základní podmínky = dlouhodobé časové kontinuity digitálního archivního úložiště.
HCP společnosti HITACHI je v oblasti archivačních řešení ověřeným standardem a jedná se o robustní archivní řešení, které umožňuje **uložení a autentifikaci neměnných dat pomocí digitálního podpisu i možnost ověření, že data jsou od doby uložení beze změny, a to po celou dobu uložení (tzv. retenční doba).** Po uplynutí této retenční doby je možné data průkazně skartovat tak, jak je definováno pravidly organizace.

HCP a přístupové protokoly

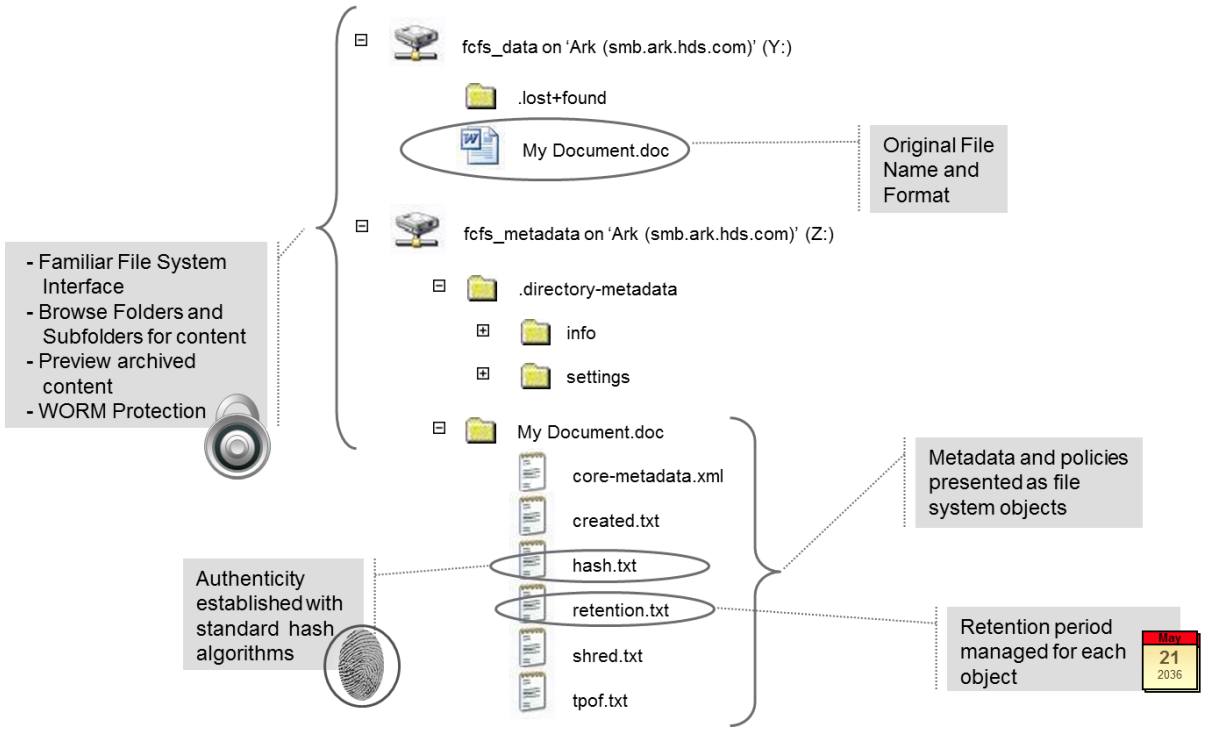
Hitachi Content Platform podporuje standardizované protokoly pro komunikaci a to zejména:

- CIFS/SMB, NFS, HTTP, HTTPS, WebDAV, XAM, SMTP, NDMP a REST

Tzn. přístup je možný přes standardní protokoly pro sdílení (CIFS) a lze v nejjednodušším možném případě přistupovat k HCP jako síťovému disku. Preferovaný protokol pro komunikaci je pak HTTP/HTTPS.
Poznámka:
Fyzický archiv je možné dělit na logické, izolované archivy (tenanty, viz dále) dle potřeb. Prioritní a doporučovaný mechanismus komunikace s archivem je přes protokol http/ https (Tento mechanismus využívá i řada konektorů, které HCP má pro SharePoint, OpenText, Documentum, a desítky dalších). Některé protokoly, jsou podporovány pouze pro první defaultní tenant.

HCP a struktura uloženého objektu

Ke každému uloženému archivnímu objektu vytváří HCP adresář s metadaty. Tímto vzniká objekt o následující struktuře:



Metadata
Metadata asociována s archivovaným obsahem, umožňující definování pravidel pro nakládání s těmito daty. Pro každý vložený objekt si archiv vytváří automaticky metadata, přičemž rozpoznává a dokáže extrahovat metadata z 370 typů datových formátů. Prostor je věnován i uživatelským metadatům, které mohou být přes aplikační interface vloženy nebo modifikovány.

Politiky
Správa objektů je založená na pravidlech garantujících autentičnost archivovaných dat, dostupnost a bezpečnost použitím volitelných hash algoritmů.
WORM: WORM formát zajišťuje ochranu proti korupci dat nebo falšování dat.
DPL: Úrovně zajištění dat (DPL = Data Protection Level) umožňují uložení daného počtu kopií objektů v archivu a ochranu proti případnému výpadku.
Retence: Retenční pravidla zajišťují definovanou dobu retence dat – ochrana proti předčasnému smazání archivovaných objektů na úrovni nastavení parametrů souboru.

Enkrypce
Vícenásobné úrovně enkrypce dat jak pro přenos, tak i pro ukládání dat.

Replikace
Objektově založená replikace umožňuje replikovat archivované objekty mezi jednotlivými systémy HCP pro off-site disaster recovery

Deduplikace
Odstranění duplicit je založeno na nahrazení již existujícího objektu odkazem. Zjištění duplicit je založeno na porovnání jak generovaných hash příznaků, tak i binárním porovnáním obsahu objektů.

Komprese
Snižuje fyzickou velikost dat uložených v systému HCP, umožňuje dosažení vyšší efektivity při ukládání dat, větší škálovatelnosti a snižuje celkové TCO.

Bezpečnost digitálního archivu – Data Protection Level
Primárním požadavkem archivu je jeho bezpečnost. Za tímto účelem obsahuje nabízené archivační řešení HCP300 další funkce a mechanismy ochraňující archivovaná data. **Jednou z těchto funkci je funkce DPL**

(Data Protection Level). DPL určuje počet interních bezpečnostních kopií archivovaných souborů a model HCP300 může pracovat:

- DPL=1 (každý objekt je uložen v HCP pouze jednou), nebo:
- s úrovní bezpečnosti DPL=2, tedy automatickým vytvářením druhé kopie k uloženému originálu. Jednotlivé DPL kopie jsou rozmístěny a udržovány na různém hardwaru tak, aby v případě výpadku jednoho hardwaru byla vždy dostupná jiná kopie. Počet funkčních DPL kopií je neustále monitorován. V případě, že je interních kopií nedostatek (vlivem poruchy), je automaticky vytvořena další interní kopie tak, aby počet odpovídal nastavení DPL. V opačném případě (odstranění poruchy), kdy je počet internách kopií větší než nastavení DPL, dojde k redukci na správný počet.

Výrobce doporučuje používat úroveň DPL=2. Použití DPL=1 je možné při požadavku zákazníka s akceptací menší bezpečnosti řešení a rizika možné ztráty dat.

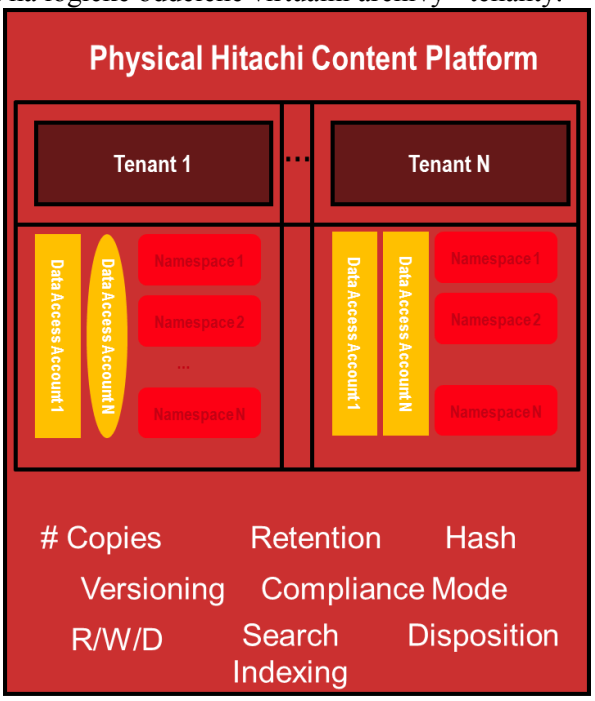
Digitální archiv – garance neměnnosti dat
HCP archiv garantuje neměnnost dokumentu po určitou dobu - tzv. retenční perioda. Lze nastavit takzvanou absolutní retenci, tedy explicitní nastavení data a času, do kdy nebude možné archivovaná data měnit nebo smazat (například 6. 10. 2077). Nebo může být retence nastavena relativně, například 20 let, 5 dnů, 6 hodin a 23 minut od data archivace. Retenční periodu nelze zkrátit nebo odstranit. Retenční periodu lze pouze prodloužit. HCP také podporuje šifrování dat.

Replikační mechanismus
Služba replikace vytvoří replikační linku mezi primárním HCP systémem a replikou (záložním HCP systémem). Replikace je zabezpečené spojení mezi těmito dvěma systémy. To určuje, co je replikováno, jak jsou data přenášena mezi primárním systémem a replikou, zda jsou data komprimována a/nebo zašifrované před jejich odesláním.

Linka vytvořená na primárním systému musí být přijata replikou před začátkem replikací. V primárním systému je linka označena jako odchozí spojení. Na replice je linka označena jako příchozí spojení. Replikace se opírá o SSL zabezpečení pro zajištění integrity a bezpečnosti přenášených dat. Před implementací replikačního mechanismu musí mít primární systém a replika platný SSL certifikát. Replikace je asynchronní s ostatními tenant a namespace aktivitami.

Virtuální archivy = tenants

Fyzický archiv je možné dělit na logické oddělené virtuální archivy= tenanty.



Monitoring "Call Home" funkce
Hi-Track – je monitorovací systém, který 24 hodin denně, 7 dní v týdnu neustále monitoruje HCP systém a v případě jakéhokoliv výpadku neprodleně informuje servisní organizaci. Forma komunikace monitorovací aplikace HiTrack se servisním organizací je dána modemový připojením (dialup) nebo internetem (HTTPS, SFTP, FTP). Aplikace HiTrack neumožňuje vzdálený přístup k diskovému systému a nemá přístup k datům uloženým na diskovém systému. Ze strany uživatele je třeba pro tuto aplikaci umožnit spuštění této služby na WIN nebo Linux systému.
Nabízené řešení HCP 300 a splnění zadávací dokumentace

V rámci nabídky se jedná o 2 stejné systémy HCP 300 splňující všechny body dle zadávací dokumentace:

- je otevřený systém podporující minimálně tyto protokoly - CIFS, NFS, HTTP, HTTPS, WEBDAV, XAM, SMTP, NDMP a REST,
- garantuje škálovatelnost archivní nodů i storage kapacity,
- přístup k datům je možný prostřednictvím protokolů NFS v3, CIFS,
- na data je možno přistupovat prostřednictvím integrace aplikací přes API úložiště a standardu XAM,
- garantuje možnost jednoznačné autentifikace na vstupu pro všechny objekty,
- garantuje systém jedinečných identifikátorů archivních objektů,
- čistá kapacita každého úložiště je 8,5 TB
- garantované úložiště je rozšiřitelné minimálně na 84TB v DPL 2 nebo 140TB v DPL1,
- garantuje neměnnost uložených dat a metadat (WORM úložiště),
- garantuje jedinečnost dat (podpora HASH algoritmů minimálně MD5, SHA-2, SHA-256), jsou-li ukládána shodná data, pak jsou uložena pouze jednou,
- garantuje autentičnost a nepodvržitelnost obsahu archivu (certifikace US SEC 17 CFR 240.17a-4 popř. certifikáty EU dle OAIS - ISO 14721:2003),
- je certifikován na soulad s požadavky zákona č. 499/2004 Sb., o archivnictví a spisové službě ve znění pozdějších předpisů pro úlohy elektronické spisovny (požadavky NSESSS) a § 16 vyhlášky č. 191/2009 Sb. Dále obsahuje mechanismy, které zajistí uložení dat ve shodě se SEC Rule 17a-4, 21CFR Part 11, HIPAA, Sarbanes-Oxley, GoBs, DoD 5015.2, Moreq II,
- garantuje nesmazatelnost uložených dat – možnost nastavení selektivně pro každý objekt příznak nesmazatelnosti na definovanou libovolně dlouhou dobu (i nekonečno),
- garantuje podporu úloh dle standardu ISO 15489,
- garantuje skartační algoritmus a elektronickou skartaci,
- garantuje dlouhodobé uchování – nastavení politiky pro uchování dat (různé doby skartace až po neomezenou dobu uchování dat),
- garantuje skartační algoritmus podle NSA – objekt, jenž byl aplikací vymazán, je nejenom logicky odstraněn z disků, ale zároveň je proveden vícenásobný přepis diskových sektorů tak, aby nebylo možné objekt obnovit ani v případě získání fyzických disků,
- garantuje možnost definice retenčních politik, umožňuje vynucení retenční doby pro ukládaná data, umožňuje konfiguraci výchozí retenční periody,
- systém umožňuje definici min. a max. retence,
- garantuje vysokou bezpečnost (neexistuje nikdy natolik privilegovaný administrátor, který by mohl získat přístup k obsahu objektů, případně objekty mazat nebo manipulovat s podpisy a obsahem),
- garantuje neměnnost systémového času popř. garance neměnnosti retenční doby,
- umožňuje replikace dat na stejné nebo nadřazené (podřízené) úložiště prostřednictvím TCP/IP protokolu do vzdálené lokality při garanci konzistence a zabezpečení stejných politik ukládání i v replikovaném archivu ve vzdálené lokalitě,
- garantuje automatické vytváření 4 identických kopií objektů (2 v jedné lokalitě, 2 v jiné lokalitě),
- podporuje virtuální resp. logicky oddělená úložiště – podpora modelu využití a správy více organizacemi a úlohami,

- obsahuje nástroje pro dohled, management a audit stavu celého systému (Hi-Track), podporuje SNMP,
- jedná se 2 shodné garantovaná úložiště s redundantním řešením,
- diskový systém je postaven na zabudované architektuře Contentaddressedstorage (uložení objektů je závislé na jejich obsahu). Není přípustná externí emulace této architektury SW,
- systém garantuje nativní auditované smazání obsahu s důkazem uloženým přímo na úložišti,
- možnost asynchronní replikace celého zařízení nebo pouze vybraných částí zařízení do vzdálené lokality,
- možnost virtuálního rozdělení zařízení na více logických celků pro využití různými organizačními jednotkami či subjekty se zachováním autenticity dat a možností definice vlastních politik,
- diskové úložiště je nezávislé na použitém zdrojovém filesystému nebo aplikaci,
- systém je založen na tzv. RAIN architektuře. Tedy nezávislých modulů, které jsou schopny v případě výpadku některého z nich převzít jeho roli bez přerušení dostupnosti systému, - SLA 99,999 %
- garantované úložiště má zabudován vysoký stupeň ochrany formou zrcadlení (DPL 2 nebo více – automaticky vytvářená kopie v garantovaném úložišti přes node, paritní kopie – RAID 5),
- garantované úložiště má zabudován samo-zotavovací mechanismus, který bez zásahu administrátora je schopen při selhání některé z komponent obnovit nebo zpřístupnit dotčená data bez přerušení dostupnosti systému,
- součástí je i software pro asynchronní replikaci do vzdálené lokality,
- umožňuje klastrování více systému do jednoho virtuálního archivu,
- má konektivitu 1Gb ethernet,
- obsahuje podporu protokolů TCP/IP,
- umožňuje průběžnou kontrolu dat na pozadí prostřednictvím nástrojů pro správu,
- umožňuje vzdálenou správu, diagnostiku a reportování do servisního centra (Hi-Track),
- umožňuje aktualizaci SW a údržbu bez výpadku provozu,
- umožňuje automatizaci správy,

Disková virtualizace
Jako virtualizační řešení pro datová úložiště navrhujeme, instalovat plně redundantní systém spravovaný produktem **FalconStor IPStor** ve verzi **NSS**. NSS Appliance jsou vloženy do datové cesty mezi datová úložiště a servery a jsou nakonfigurovány v režimu storage clusteru, jako Active-Active nody. V případě výpadku jedné z těchto appliancí, přebírá všechny její funkce zbylá appliance, aniž by došlo k výpadku aplikačních serverů.
Umístěním celé jedné poloviny tohoto Storage Clusteru do jedné serverovny a druhé polovinu do druhé, získáme DR řešení v rámci vzdálených serveroven a jsme tak chráněni i proti výpadku celé jedné lokality/serverovny. Zároveň jsou takto rozmístěna i veškerá spravovaná datová úložiště a data mezi nimi jsou synchronně zrcadlena tak, aby byl zajištěn nepřetržitý chod aplikací i v případě výpadku celé jedné poloviny řešení.

Hlavní přínosy řešení jsou zejména tyto:

- **Maximální redundance všech prvků** – systém zajišťuje nepřetržitou funkčnost i v případě výpadku celého jednoho fyzického zařízení. Tzn. celý systém je navržen jako plně redundantní s možností instalace částí systému do různých serveroven tak, aby byla zajištěna funkčnost systému i v případě výpadku celé jedné serverovny. Např. u diskových polí je možno zajistit synchronní mirror mezi dvěma diskovými poli (i různých výrobců), kde v případě výpadku jednoho celého diskového pole takto zabezpečené aplikace vůbec nepoznají, že k tomuto výpadku došlo.
- **Transparentní použitelnost datových úložišť různých typů i výrobců** – systém zajišťuje možnost instalace v podstatě jakéhokoliv FC nebo iSCSI datového úložiště s možností

budoucího rozšíření o další disky nebo externí diskové prostory, například technologie Flash disků apod.

- **Rozšiřitelnost** – jednoduchá rozšiřitelnost řešení, nejlépe pouhou instalací dodatečných disků se zachováním možnosti dalšího kapacitního rozšiřování včetně možnosti rozšíření i o další funkcionality. Další možnosti rozšiřování o další disková úložiště.
- **Možnost replikace do vzdálené lokality** – veškerá data spravovaná systémem mohou být replikována do vzdálené lokality prostřednictvím protokolu TCP/IP a to i po pomalejších linkách – volitelná součást, která není součástí nabídky.
- **Rozšířené služby zabezpečení dat** – data jsou zabezpečena pomocí synchronního zrcadlení do druhého diskového pole, aplikačně konzistentních snapshotů a CDP žurnálu, kdy je možný návrat do jakéhokoliv okamžiku v minulosti.
- **Nezávislost na výrobci hardware** – pomocí tohoto systému je možno spravovat různá datová úložiště, různých typů a výrobců.
- **Jednoduchá a jednotná správa** – konsolidovaná správa datových úložišť v rámci jedné konzole nebo webového rozhraní.

Navržené řešení je tak redundantní ve všech svých prvcích a fyzicky je představováno vždy dvěma nezávislými zařízeními, které vzájemně fungují v režimu tzv. storage clusteru. Tento koncept zajistí nepřetržitou dostupnost diskových prostor i v případě výpadku celého jednoho zařízení nebo celé jedné poloviny řešení.

Princip redundance řešení

Tato kapitola popisuje princip redundance celého řešení a jeho jednotlivých komponent:

- **Výpadek celé NSS Appliance** – v případě výpadku celého jednoho serveru s NSS Appliancí dojde k překlopení veškerých spravovaných datových služeb na druhý server s druhou NSS Appliancí, která převezme veškeré datové služby první appliance tak, že aplikační servery nezaznamenají žádný výpadek.
- **Výpadek jednotlivého disku** – disky jsou v každém diskovém poli konfigurovány v rámci svazků typu RAID, takže nedochází ke ztrátě dat.
- **Výpadek celého diskového pole** – v případě simultánního výpadku 3 nebo více disků v rámci jednoho diskového pole nebo výpadku celého diskového pole dochází k automatizovanému a transparentnímu přepnutí poskytovaných datových služeb na druhé diskové pole u všech datových prostor, které jsou zabezpečeny synchronním mirrorem. Aplikace a servery tak nepocítí výpadek diskového pole a data jsou neustále dostupná.
- **Výpadek napájení** – každý server nebo diskové pole jsou vybaveny dvěma nezávislými hot swap napájecími zdroji. V případě výpadku jednoho zdroje nebo jednoho napájení pracuje celé zařízení plnohodnotně pouze s jedním zdrojem.

Architektura řešení

Pro zajištění veškerých výše popsaných funkcí navrhujeme tedy instalovat dvě FalconStor NSS appliance, z nichž každá je vybavena 6 x 8 Gbps FC porty a 4 x 1 Gbps LAN porty. Celé řešení je připojeno do dvou zcela nezávislých SAN sítí a poskytuje celkově 12 x 8 Gbps FC portů a 8 x 1 Gbps LAN portů. Pro připojení diskových polí a aplikačních serverů jsou k dispozici protokoly Fibre Channel a iSCSI.
Navrhované řešení zahrnuje veškeré poptávané funkcionality včetně možnosti manuální nebo automatizované migrace dat mezi jednotlivými tiery datového úložiště. Pro zajištění těchto funkčních vlastní implementuje řešení tři konkrétní funkce:

- **Migrace dat za plného provozu** – tato funkce umožňuje migraci celých datových svazků mezi jednotlivými tiery diskových polí z plného chodu aplikací.
- **HotZone** – tato funkce umožňuje automatizovanou migraci nejčastěji používaných, tj. nejčastěji čtených diskových bloků do cache prostoru umístěného na rychlejších, zpravidla FC nebo SSD discích. Tím je zajištěno pro kritické svazky výrazné navýšení výkonnosti celého řešení.

- **SafeCache** – tato funkce je alternativou funkce HotZone pro zápisové operace. Funkce umožňuje vytvoření zápisové cache paměti na rychlých diskových prostorech, zpravidla na FC nebo SSD discích v rychlých RAID konfiguracích. Využití této funkce významně přispívá k navýšení průchodnosti systému v případě náročných nárazových write operací.
-

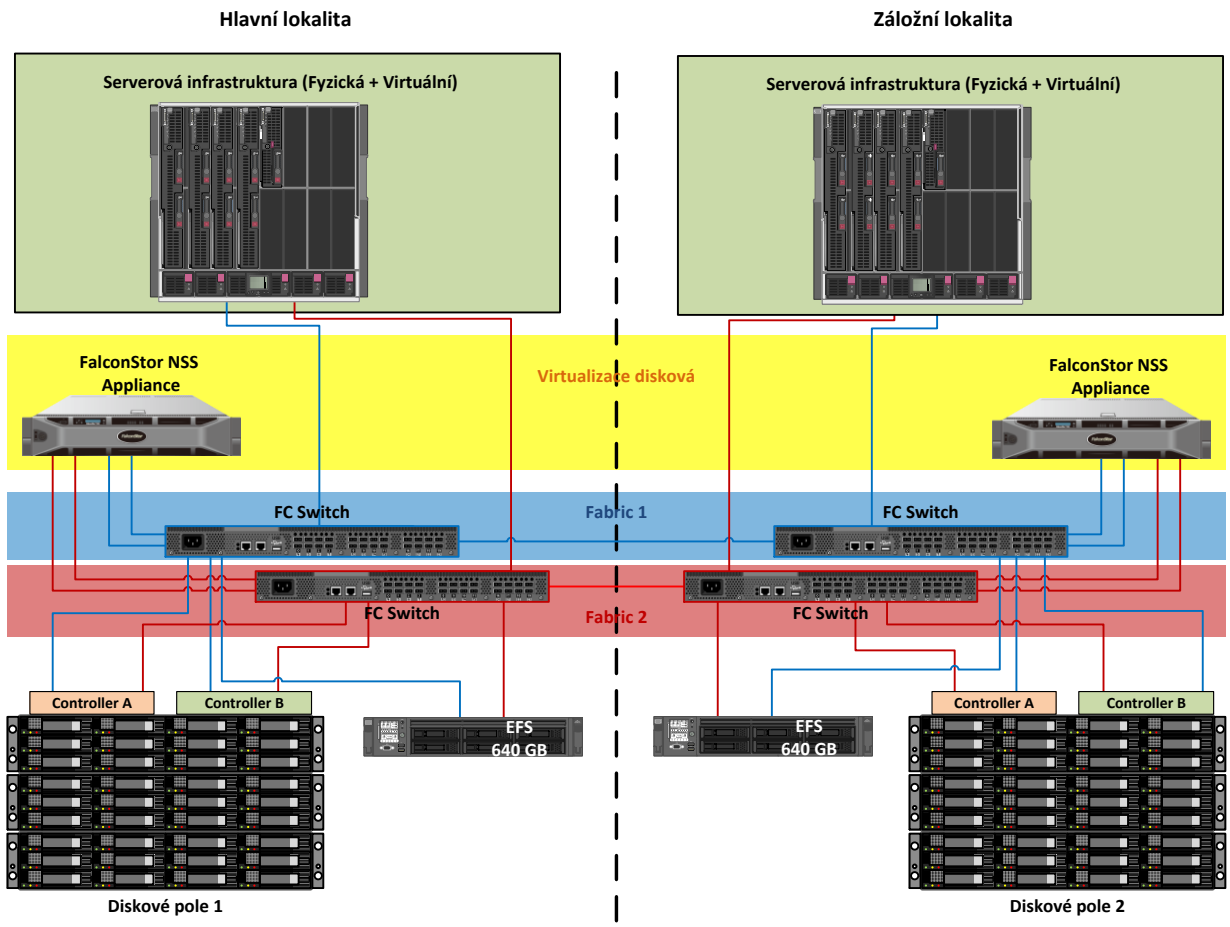
Pro využití výše uvedených možností akcelerace diskových operací je součástí řešení **Tier 0** storage ve formě **Enterprise Flash Storage (EFS)**, která je založena na úložné kapacitě typu NAND Flash, a která umožňuje výrazné zvýšení zápisových a čtecích operací v rámci redundantního datového úložiště. Velikost tohoto prostoru není nijak omezena.
Tak jako i ostatní diskové kapacity Tier 1 a Tier 2, jsou i tyto EFS instalovány v obou lokalitách a jsou vzájemně mirrorovány tak, aby ani v případě výpadku jedné z nich nedošlo k výpadku aplikací nebo ke ztrátě dat.

Dále systém FalconStor NSS poskytuje následující požadované funkce:

Aplikačně konzistentní snapshoty a CDP žurnál
Produkt FalconStor NSS umožňuje na úrovni jednotlivých kopií svazků vytváření logických snapshotů. Ke každému virtuálnímu svazku je možné vytvořit až 1 000 snapshotů. Pro vytváření snapshotů využívá NSS mechanismus „copy on write“ a tudíž vyžaduje pouze tolik diskového prostoru, kolik reálně činí objem změn v datech. Tento diskový prostor může NSS ze svěřeného objemu diskových prostor dynamicky rozšiřovat dle potřeby až do výše kvóty stanovené pro daný virtuální svazek. Administrativně lze tento diskový prostor i zmenšit.
Vytvořené snapshoty lze prostřednictvím tzv. views zpřístupnit libovolnému serveru v prostředí. Jeden snapshot lze v jednom čase zpřístupnit zároveň více serverům v režimu read/write. Zápisy do „view“ jsou pro každý server poté spravovány zvlášť. Z jakéhokoli snapshotů je také možné provést rollback příslušného virtuálního svazku. Data jsou do původního svazku kopírována na pozadí, zatímco svazek je možné již plně využívat.
Pomocí agentů nainstalovaných na jednotlivých klientských serverech lze takto provádět plně aplikačně konzistentní snapshoty pro tyto systémy: IBM DB2 UDB, Informix, Microsoft SQL Server, Oracle, Pervasive, SQL, Sybase, SAP, IBM Lotus Notes/Domino, Microsoft Exchange, Microsoft VSS, Novell GroupWise, MySQL, Ingres a souborové systémy (AIX, HP UX, Linux, NetWare, Solaris a Windows).
Snapshoty je možno vytvářet jednorázově i periodicky. Nastavení se provádí pomocí centrální konzole nebo pomocí příkazového řádku, takže je možno využít i metod „skriptování“.
Součástí licence je i možnost využívání **CDP žurnálu**, kdy je možné vrátit se do jakéhokoliv okamžiku v minulosti (Any Time Point In Time Recovery). Zpřístupnění dat z tohoto CDP žurnálu se provádí stejně jako u snapshotů.

Synchronní mirror
Každý diskový svazek zpřístupněný koncovému serveru (virtuální svazek) bude fyzicky umístěn na dvou diskových subsystémech. V případě požadavku na provedení operace typu write zajistí NSS synchronní zápis dat do obou diskových systémů. Požadavky na operace typu read jsou vyřizovány s využitím diskového systému, který je pro daný virtuální svazek definován jako primární. V případě výpadku jednoho z diskových systémů NSS pracuje pouze s druhým diskovým systémem. Ten pak využívá pro vyřízení požadavků na operace typu read i write. Vzhledem ke koncovému klientskému serveru je tento přechod plně transparentní a koncový server tuto situaci vůbec nezaznamená. Po opětovném obnovení funkčnosti havarovaného systému zajistí NSS na pozadí re-synchronizaci dat. Synchronní zrcadlení se nastavuje na úrovni virtuálního svazku.
Vedle této možnosti synchronního zrcadlení diskových prostor existuje i možnost nastavit near-line mirror, asynchronní mirror nebo periodický mirror s předem definovanými konzistentními stavy (např. pro databáze).

Následující obrázek ukazuje zjednodušené schéma architektury řešení při rozdělení mezi dvě nezávislé serverovny a synchronní zrcadlení veškerých dat mezi těmito serverovnami:



Obrázek - Zjednodušené schéma virtualizačního řešení

Integrace snapshotů se systémem zálohování na pásku

Pro integraci existujícího systému zálohování dat s NSS je součástí nabízeného řešení modul **FalconStor HyperTrac**, který se instaluje na zálohovací server. Tento modul zajišťuje automatizaci migrace dat prostřednictvím zálohovacího softwaru na zálohovací zařízení.

Programové vybavení HyperTrac zajišťuje automatizaci procesu zpřístupnění již existujícího aktuálního snapshotů, případně nově vytvořeného snapshotů, backup serveru. Backup server provede z tohoto snapshotů zálohu na pásku a po dokončení, opět prostřednictvím produktu HyperTrac, tento snapshot odpojí. Díky tomu je možno zálohovat kdykoliv, protože zálohování se již vůbec netýká primární infrastruktury.

Vzhledem k tomu, že snapshoty jsou již zcela aplikačně konzistentní, není nutno instalovat žádné další agenty a data jsou tak použitelná i pro plnou obnovu dat databází nebo messagingových systémů.

Možnost vybudování DR lokality pomocí replikace dat s využitím TCP/IP linek

Replikační modul je součástí licence a je tedy zahrnut v ceně řešení. Replikace se dodává jako softwarový modul, který zajistí replikaci dat do vzdálené lokality, prostřednictvím protokolu TCP/IP nebo RUDP. Do této vzdálené lokality je jen třeba umístit FalconStor NSS nebo CDP Applianci, která bude tato data přijímat. Replikace je zajišťována pro vybrané diskové prostory kontinuálně nebo jako tzv. delta schedulovaná replikace prostřednictvím snapshotů, takže je zajištěna konzistence replikovaných dat i pro databáze a messagingové systémy.

Replikaci je možno provádět i po pomalejších linkách a je možno nastavit její omezení v případě, že je to požadováno nebo je linka využívána i pro jiné aplikace tak, aby nedocházelo k jejímu přetěžování. Vzdálenost, na kterou je možno tuto replikaci provádět, není nijak omezena. Replikaci je možno provádět v režimu M:N, což v praxi znamená, že lze provádět replikaci do více lokalita a zároveň přijímat replikaci z více lokalit najednou. Replikační algoritmus provádí prostřednictvím funkce microscan rozklad nově vzniklých dat až na bloky o velikosti 512 B, čímž zajistí, že se přenáší opravdu pouze změněná data.

Integrace na úrovni ukládaných dat je zajištěna prostřednictvím funkce replikace dat. Nově vznikající data lze do DR lokality replikovat ve dvou možných režimech:

- **Kontinuální replikace** – data jsou odesílána ihned po jejich vytvoření. Je tak garantováno, že veškerá nově vznikající data jsou k dispozici v DR lokalitě v nejkratším možném čase. Pro zajištění konzistentní podoby od replikovaných dat je tento typ replikace doplňován vytvářením aplikačně konzistentních snapshotů, které jsou na replikované kopii udržovány.
- **Periodická replikace** – data jsou odesílána v pravidelných intervalech v tzv. garantovaně aplikačně konzistentní podobě. Díky tomuto přístupu je zajištěno, že od replikovaná data mohou být garantově použita k obnově provozu, tj. že jsou v tzv. konzistentních stavu. Zároveň je v průběhu replikace využita reduplikace, která umožňuje replikaci i po relativně pomalých datových linkách.

Integraci na úrovni provozu virtuálních serverů je možno zajistit prostřednictvím produktu VMware Site Recovery Manager (SRM). Tento produkt umožňuje prostřednictvím předem definovaných disaster recovery plánů snadnou obnovu provozu v DR lokalitě v případě potřeby.
Pomocí replikačního modulu a jediného serveru ve vzdálené lokalitě je tak možné dosáhnout komplexního DR řešení umožňující restart celého výpočetního prostředí v DR lokalitě prostřednictvím pouhého stisku jednoho tlačítka.

Zálohování a obnova dat

Zálohovací bod
Návrh zálohovací infrastruktury tvoří samostatnou funkční jednotku (zálohovací bod) skládající se ze zálohovacího serveru, vyhrazené části diskové kapacity na sdíleném úložišti a páskové knihovny.
Vyhrazený prostor bude představovat definovanou kapacitu diskového pole umístěnou na velkokapacitních discích (Tier 2 - SATA disky), které jsou součástí diskového pole v rámci SAN infrastruktury v prostředí záložního datového centra.
Pro roli zálohovacího serveru bude dedikován jeden z fyzických serverů v rámci blade centra záložního datového centra.
Tento zálohovací bod je schopen v provozním stavu zajistit z jednoho místa zálohování systémových, aplikačních i provozních dat celé infrastruktury v rámci obou datových center.

Detailní specifikace komponent zálohovacího bodu
Zálohovací server
- 1x server HP BL465c
- 1x AMD Opteron 6276 (16C)
- 16 GB paměti RAM
- 2x 142GB disky
- 2x 10Gb/s LAN, 2 x 8GB/s SAN

Diskové pole (vyhrazený prostor pro zálohy)
- Počítáme s využitím stávajících diskových polí ve vlastnictví Objednatele (např. HP EVA), na nichž bude po zmigrování provozních dat do nového prostředí vyhrazen prostor o kapacitě 5TB.

Pásková zálohovací knihovna
- 1x HP MSL 4048
- 2x LTO-5 Ultrium 3000 mechanika
- 2x 8Gb/s nativní Fibre Channel připojení
- Celková kapacita 144 TB (při obvyklém kompresním poměru 2:1)
- Možnost rozšíření až na 6 mechanik přidáním další knihovny a jejích propojením
- 48 slotů pro media
- Možnost rozšíření až na 144 slotů pro media přidáním další knihovny a jejích propojením
- Redundantní napájení
- Snímač čárových kódů pro rychlou identifikaci používaných medií

Zálohovací SW
V rámci nabízeného řešení bude zajištěna ochrana dat zálohováním. Pro zajištění této ochrany bude použito SW řešení DataProtector společnosti Hewlett-Packard.

Instalované komponenty

Na jednotlivých serverech v rámci infrastruktury jsou nainstalovány komponenty produktu HP DataProtector podle toho, jaká data tohoto serveru budou zálohována a jakým způsobem budou zálohy prováděny.

Komponenta HP DataProtector	Cíl instalace
DataProtector Core	Zálohovací server, všechny zálohované fyzické i virtuální servery
DataProtector Disk Agent	Zálohovací server, všechny zálohované fyzické i virtuální servery
DataProtector Media Agent	Zálohovací server
DataProtector Cell Server	Zálohovací server
DataProtector Cell Manager	Zálohovací server
DataProtector Online Extension for Windows – Exchange Server	1 poštovní server MS Exchange
DataProtector Online Extension for Windows – MS SQL	2 nody databázového clusteru MS SQL
DataProtector Online Extension for Windows – Oracle DB	1 databázový server s Oracle db
DataProtector Online Extension for Windows – Virtual Enviromnent Integration	Zálohovací server

Ukládání dat záloh

Data záloh budou ukládána:

- pouze na pásková média (zálohy typu D2T) – bude se jednat o zálohy, u kterých lze zajistit vysoký datový tok pro maximalizaci využití zálohovacích mechanik, hlavně se bude jednat o zálohy obrazů celých virtuálních strojů, které není nutné zálohovat s velkou frekvencí a data těchto záloh se použijí pouze pro případ celkové obnovy těchto serverů (Disaster Recovery)
- pouze do diskového prostoru (zálohy typu D2D) – bude se jednat o zálohy mimo pořadí, testovací zálohy, zálohy při migraci provozních systémů, tedy o takové, u kterých není nutné požadovat dlouhou dobu jejich dostupnosti pro případnou obnovu dat.
- zálohy do diskového prostoru a následně na pásková média (záloha typu D2D2T) – bude se jednat o většinu standardních provozních záloh, data budou primárně ukládána do diskového prostoru, následně bude z nich vytvořená kopie (klon) na páskové médium. Data záloh v diskovém prostoru budou určena pro rychlou dostupnost v případě potřeby obnovy, kopie dat na páskových médiích bude sloužit hlavně pro zvýšení bezpečnosti dat záloh (tato média s daty záloh budou ukládána do trezoru fyzicky umístěného mimo datová centra).

Záloha dat podle typů serverů

Zálohování dat bude probíhat stejným způsobem pro stejné typy dat na stejných typech serverů.

Virtuální servery běžící na ESX/vSphere serverech

Záloha obrazů celých virtuálních serverů

Záloha obrazů celých virtuálních serverů bude prováděna pomocí komponent HP DataProtecotru přes VMware vStorage API rozhraní přímo na páskové médium a to přímo po SAN síti (LAN-free zálohy).

Frekvence zálohování tohoto typu dat se předpokládá jednou měsíčně nebo vynuceně po aplikaci opravných fixů na operačním systému nebo provozovaných aplikacích, instalaci nové verze aplikací, apod.

Záloha dat uvnitř virtuálních serverů

Ve všech virtuálních serverech budou nainstalováni HP DataProtector disk agenti, pomocí kterých bude možno provádět zálohování dat zevnitř virtuálních strojů, tedy převážně dat souborových systémů, případně aplikací na daných virtuálních serverech provozovaných. K ukládání dat záloh bude primárně použit diskový prostor spravovaný zálohovacím serverem (DataProtector File System Library), sekundární záloha (klon) těchto dat bude následně uložena

na pásková média. Tato data budou na zálohovací server přenášena po provozní LAN síti, vzhledem k jejich objemům a propustnosti LAN sítě není nutno budovat speciální LAN infrastrukturu pro zálohování.

U těchto dat bude prováděno zálohování plnou zálohou jednou denně, případně dle individuálních potřeb konkrétních dat umístěných na konkrétním virtuálním serveru.

Záloha dat databázových serverů

Na hlavních databázových serverech budou nainstalováni HP DataProtector Online Extenze pro zálohování těchto databázových serverů.

K ukládání dat záloh bude primárně použit diskový prostor spravovaný zálohovacím serverem (DataProtector File System Library), sekundární záloha (klon) těchto dat bude následně uložena na pásková média. Tato data budou na zálohovací server přenášena po provozní LAN síti, vzhledem k jejich objemům a propustnosti LAN sítě není nutno budovat speciální LAN infrastrukturu pro zálohování.

U těchto dat bude prováděno zálohování plnou zálohou jednou denně, v průběhu dne budou několikrát zálohovány transakční logy databází, aby se minimalizovala možná ztráta dat v případě celkového zhroucení infrastruktury a bylo možno provádět obnovy dat typu „point-in-time“, tedy návrat databáze do předem zvoleného času.

Fyzické servery

Jedná se o nově dodané fyzické servery (zálohovací server, management server, vCenter servery) a původní fyzické servery do okamžiku, kdy budou zvirtualizovány.

Zálohování dat těchto serverů bude prováděno pomocí lokálně nainstalovaného HP DataProtector Disk Agenta. Zálohovaná data budou primárně ukládána do diskového prostoru a sekundárně na pásková média.

Předpokládá se provádění záloh pouze na úrovni souborového systému a operačních systému. V případě potřeby provádění záloh malých databází provozovaných na některých z těchto serverů, se tyto budou zálohovat nativními prostředky do souborů na lokální disky daného serveru a následně popsaným způsobem dále.

Tato data budou na zálohovací server přenášena po provozní LAN síti (mimo zálohovacího serveru), vzhledem k jejich objemům a propustnosti této LAN sítě není nutno budovat speciální LAN infrastrukturu pro zálohování.

Požadované funkcionality zálohovacího SW:

Zálohování požadovaného počtu serverů a stanic – základní dodávaná licence (HP DataProtector Starter Pack) obsahuje právo instalace a využívání NEOMEZENÉHO počtu zálohovacích agentů pro zálohování dat souborových systémů serverů a stanic (Disk Agent) v rámci daného zálohovacího bodu. Je tedy zajištěna možnost zálohování souborových dat jak stávajícího počtu serverů, tak i případných dalších serverů a stanic.

Podpora zálohování na nabízenou páskovou mechaniku – dle matice kompatibility dostupné v dokumentu *HP DataProtector 6.20 Device Support Matrix* jsou nabízené páskové mechaniky plně kompatibilní s jejich řízením, zápisem a čtením dat na platformách Windows, Linux, HP-UX a IBM AIX, celá zálohovací knihovna je kompatibilní s provozováním na shodných platformách jako mechaniky plus platformy Sun Solaris a Novell Netware.
Nabízený zálohovací server, který zajišťuje řízení zálohovací knihovny a datových toků do ní směrovaných bude provozován na platformě Microsoft Windows, dodávané zařízení je tedy kompatibilní.
Pro zajištění podpory dodávaných zálohovacích mechanik jsou vyžadovány speciální licence (HP DataProtector Drive Extension for SAN). Tato licence je vyžadována pro každou zálohovací mechaniku, v počtu 2 kusů jsou součástí nabízeného řešení.

Podpora zálohování na disk v režimu D2D2T – HP DataProtector v nabízené konfiguraci umožňuje ukládat data primárních záloh přímo na páskové médium nebo do dedikovaného diskového prostoru. Data záloh z diskového prostoru lze následně přenést na páskové médium tzv. Copy Jobem, vytvoří se plnohodnotný klon zálohovaných dat pro danou zálohovací úlohu.
Tyto sekundární zálohovací úlohy lze spouštět následovně:

- ihned po dokončení primární zálohy dat (Post Backup Copy Job)
- v požadovaném čase (Scheduled Copy Job)
- interaktivně (Manual Copy Job)

Pro zajištění podpory zálohování do diskového prostoru jsou vyžadovány speciální licence (HP DataProtector Advanced Backup to Disk). Tato licence je vyžadována pro každý TB diskového prostoru pro ukládání dat záloh, pro diskovou kapacitu 5 TB jsou součástí nabízeného řešení. Výsledný objem

uložitelných dat záloh je však několikanásobně větší, jelikož součástí těchto licencí je i deduplikační mechanismus, který umožňuje optimalizovat uložená data záloh.

Podpora pro online zálohování aplikací (MS Exchange, MS SQL, Oracle DB) – dle matice kompatibility dostupné v dokumentu *HP DataProtector 6.20 Platform and Integration Support Matrix* je nabízené zálohovací řešení schopno zajišťovat zálohování a obnovu dat databázových platforem MS SQL a Oracle DB stejně jako groupwarové platformy MS Exchange pro všechny jejich verze a jejich kombinace s platformou, na které jsou tyto aplikace provozovány, které jsou podporovány výrobcem dané aplikace.
Pro zajištění podpory online zálohování těchto aplikací jsou vyžadovány speciální licence (HP DataProtector Online Extension). Tato licence je vyžadována pro každý zálohovaný databázový server, v počtu 4 kusů pro platformu MS Windows jsou součástí nabízeného řešení.

Podpora pro online zálohování „Image" virtuální serverů z VMware/vSphere. Zálohování musí probíhat „LAN-free" pouze pomocí FC SAN – HP DataProtector umožňuje řídit a provádět zálohování a obnovu dat obrazů virtuálních serverů v rámci VMware/vSphere infrastruktury. K vlastnímu zálohování a obnově se využívá rozhraní vStorage API VMware/vSphere infrastruktury, které umožňuje provádět zálohování a obnovu z centrálního bodu v rámci celé infrastruktury nezávisle na tom, na kterém konkrétním ESX serveru se zálohovaný virtuální server v okamžiku zálohy nachází.
Vlastní přenos dat obrazů virtuálních serverů je možno provádět v rámci LAN nebo SAN infrastruktury. Námi nabízené řešení bude provádět přenos dat v rámci SAN infrastruktury (LAN-free), podmínkou této varianty je nutnost mít tzv. Backup Host (centrální bod, přes který tečou data ze VMware infrastruktury na zálohovací zařízení) připojen do SAN infrastruktury - musí se tedy jednat o fyzický server v rámci celé infrastruktury. V rámci našeho řešení bude role Backup Host jednou z rolí zálohovacího serveru, pro zvýšení efektivity řešení se využije faktu, že tento server je připojen do SAN infrastruktury z důvodu jeho komunikace a přenosu dat na páskovou zálohovací knihovnu připojenou do této infrastruktury a přístupu k diskům na sdíleném diskovém poli pro ukládání dat záloh.
Pro zajištění podpory zálohování na úrovni VMware infrastruktury jsou vyžadovány speciální licence (HP DataProtector Online Extension). Tato licence je vyžadována pro každý zálohovaný ESX/vSphere server, v počtu 8 kusů jsou součástí nabízeného řešení.

Podpora pro centralizovanou správu patchů zálohovacího SW, která umožní jednotnou distribuci a vzdálenou instalaci nových klientů zálohovacího SW, stejně tak jejich patchování, reinstalaci či přidání /odebrání komponent – součástí základní instalace produktu HP DataProtector na zálohovací server je tzv. instalační server (Installation Server), tedy součást produktu, která obsahuje instalační balíčky pro všechny komponenty produktu na příslušné platformě (Windows/Linux/Unix). Tento instalační server je v rámci jeho instalace zaregistrován do řídící konzoly HP DataProtectoru.
Z řídící konzoly pak lze centrálně přidávat zálohovací agenty v požadované konfiguraci komponent na další servery nebo stanice, odebírat je jako celek nebo pouze některé z komponent, případně provádět upgrade těchto komponent.
Prováděním upgrade je chápan stav, kdy se na instalační server (zálohovací server) nainstaluje patch produktu a tento se následně z řídící konzoly pomocí volby „Upgrade" distribuuje na všechny zvolené klientské servery. Patch produktu se tedy jako instalační balíček výrobce instaluje pouze jednou, následná distribuce je zajištěna pomocí řídící konzoly HP DataProtectoru.
Řídící konzola taktéž umožňuje z centrálního místa kontrolu verzí produktu na jednotlivých registrovaných klientských serverech a to včetně verzí patchů.
Tato funkcionalita je součástí základní licence HP DataProtector Starter Pack, k jejímu využívání není vyžadována žádná další licence.
Počet DisasterRecovery Agentů dle aktuálního stavu – základní dodávaná licence (HP DataProtector Starter Pack) obsahuje právo instalace a využívání NEOMEZENÉHO počtu disaster recovery agentů pro úplnou obnovu serverů ze zálohy. Tito agenti budou využiti pro zajištění disaster recovery obnovy fyzických serverů v rámci nabízeného řešení, úplná obnova virtuálních serverů provozovaných v rámci VMware infrastruktury bude řešena obnovou obrazu virtuálního serveru zálohovaného na úrovní této virtuální infrastruktury.

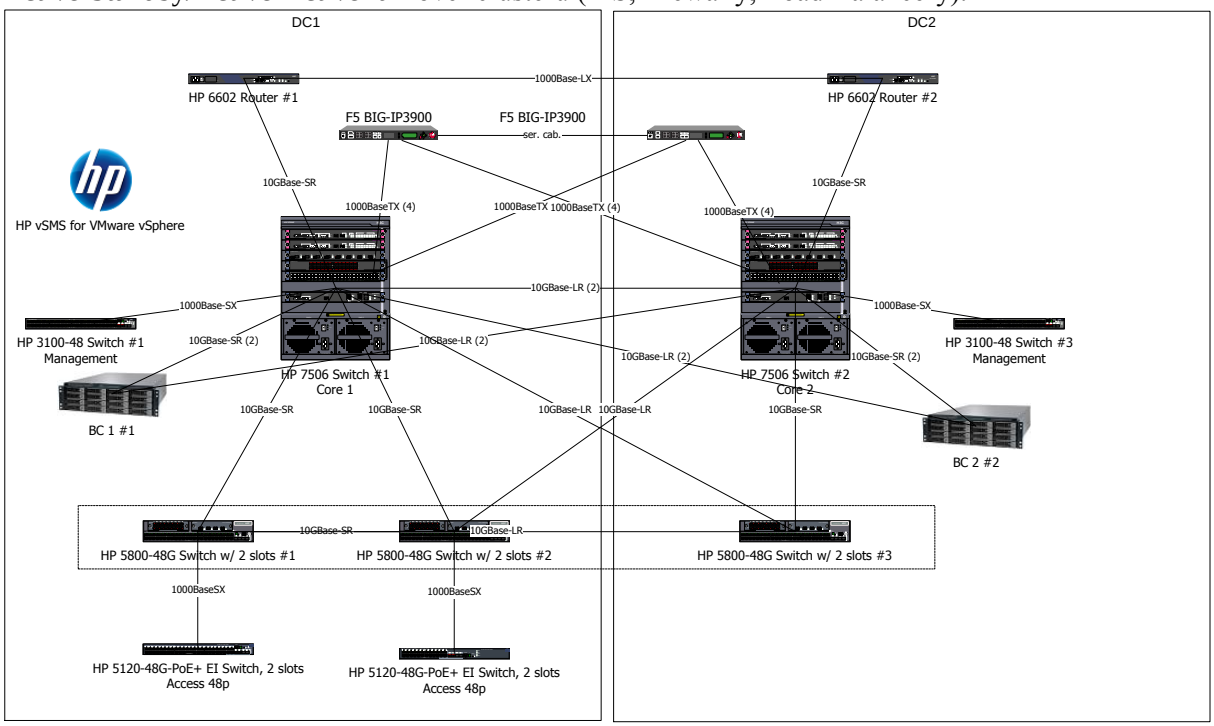
Licence na Monitoring a Reporting, možnost zasílat SMTP zprávy a generovat SNMP trapy založené na konci zálohovací úlohy nebo naplánované pravidelně – komponenta HP DataProtector Cell Manager, která je součástí základní licence produktu, v sobě obsahuje funkcionality typu „Monitoring" a „Reporting".

Monitoring dokáže reagovat na události podle jejich typu, informace o nich předává ať už ve formě mailových zpráv nebo SNMP trapů. Umožňuje nastavení určitého typu události jako tzv. spouštěče, který v případě, že nastane, spustí generování a zasílání určeného reportu nebo skupiny reportů.
Reporting umožňuje připravit reporty nebo jejich skupiny na základě nastavení požadovaných parametrů a tyto po jejich vygenerování ukládat do souborů nebo zasílat formou mailů. Vytváření těchto reportů se pak provádí buď v nastavenou dobu, nebo po aktivaci spouštěče, který je vytvořen v rámci monitoringu produktu.

Bezpečná komunikační infrastruktura TCK
Komunikační infrastruktura je navržena v architektuře dělené do vrstev:

- Páteřní,
- Agregační,
- Přístupové,
- Samostatné management LAN vrstvy,
- Servisní,
- Vrstvy perimetru sítě,
- Dohledové vrstvy

Technická koncepce architektury sítě je postavena na výkonné vysoce dostupné infrastruktuře zajištěné zdvojením všech technických prostředků síťových prvků a fyzických přenosových tras. Všechny síťové prvky v jednotlivých vrstvách jsou v případě poruchy některého z prvků vzájemně zastupitelné. Samotné prvky jsou postaveny v redundantních sestavách (záložní řídící jednotky, záložní zdroje) a jsou v rámci své vrstvy i mezi vrstvami propojeny redundantními fyzickými přenosovými trasami. Propustnost sítě je dimenzována s dostatečnou rezervou a s ohledem na rozsah a povahu ICT prostředí Objednatele. Dostatečná propustnost sítě je zajištěna neblokovanou line rate architekturou přepínaných subsystémů jednotlivých vrstev s kapacitou od cca 300Gbps do 1,5Tbps v rámci vrstev (od přístupové po páteřní vrstvu). Propojení mezi síťovými prvky a samotných koncových serverových systémů jsou realizovány Nx1G a Nx10G redundantními propoji, které jsou agregovány do trunků, které zajišťují vysoce dostupnou topologii (802.3ad agregace) a rychlou konvergencí v případě poruch (max. 2ms) bez nutnosti vytváření smyček. V případě síťových prvků 3. vrstvy je vysoká dostupnost řešena pomocí router-redundancy protokolů (routery) a Active-Standby/Active-Active fail-over clusterů (IPS, firewally, Load Balancery).



Topologie komunikační infrastruktury

Základní vlastnosti
Páteřní vrstva

Páteřní vrstva je tvořena modulárním L3 přepínačem HP 7506, který disponuje 6-ti sloty pro line Ethernetové moduly a 2-mi sloty pro řídící moduly.

Páteřní L3 přepínač je instalován po 1ks do každé lokality (DC1 a DC2). Pro zajištění redundance řídících modulů jsou oba sloty pro řídící moduly osazeny moduly HP 7500 Fabric Module. Každý řídící modul disponuje propustností 384Gbps, což poskytuje celkovou propustnost páteřního přepínače HP7506 760Gbps. Oba řídící moduly jsou dohromady osazeny 4x 10Gb XFP (HP X130 10G XFP Transceiver). Společně s Ethernet line modulem HP 7500 8-port 10G SFP+ osazeným 8x SFP+ (HP X130 10G SFP+ Transceiver) je páteřní přepínač vybaven 12x 10Gb Ethernet porty (4x XFP + 8x SFP+). Páteřní L3 přepínač je dále vybaven Ethernet line modulem HP 7500 48-port Gig-T, tzn. 48x 10/100/1000 BaseT Ethernet portů a Ethernet line modulem HP 7500 24-port GbE SFP, který je osazen 24x 1G SFP FO/LC porty.
HW konfigurace 1 sestavy páteřního L3 přepínače HP7506 (po 1 sestavě do obou DC):

- Výška 13RU
- 2x řídící modul HP 7500 Fabric Module (dohromady propustnost 760Gbps)
- 12x 10GE porty
- 48x 10/100/1000 BaseT Ethernet porty
- 24x 1G SFP porty
- 3x volný slot pro line moduly (6 slotů celkem)

Architektura páteřního přepínače HP 7506 je plně distribuovaná, kdy veškeré přepínání probíhá v rámci line přepínacích modulů. Modularita HP7506 spočívá ve škálovatelnosti hardwarových prostředků systémů a zároveň ve škálovatelnosti modulárního operačního systému. Řešení páteřního přepínače poskytuje vysokou dostupnost páteřní sítě s možností současné funkce obou řídících přepínacích matic v režimu Active-Active. Další vlastností, která je klíčová pro funkcionalitu TCk je podpora tvorby virtuálního přepínače (technologie IRF) z více fyzických jednotek. IRF umožní sloučení fyzických přepínačů do jednoho celku (vznikne jedno šasi s celkem 12ti sloty a 4mi fabric moduly). Virtuální přepínač vystupuje v síti jako jedna entita, má jeden IP stack, jeden management s výhodou lze konfigurovat distribuované LACP mezi více fyzickýma jednotkami (rychlá konvergence, eliminace STP).

Podporované servisní karty
HP 7500 NetStream Monitoring Module pro sběr informací o síťovém provozu, monitoring a jejich následnou analýzu.
HP TippingPoint S1200N IPS A7500 Module pro hloubkovou analýzu síťového provozu za účelem prevence nežádoucího průniku – Intrusion Prevention Systém (IPS).
HP 7500 Access Controller Module sloužící jako Wireless LAN kontrolér pro řízení bezdrátových sítí.
HP 7500 Advanced VPN Firewall Module pro rozšíření páteřní vrstvy o vysoce výkonný centrální stavový firewall určený pro technologická centra.
HP 7500 SSL VPN Module sloužící jako SSL VPN koncentrátor.

Agregační vrstva
Agregační vrstva je v lokalitě technologického centra DC1 tvořena 2ks přepínačů HP5800-48G a v lokalitě DC2 1ks přepínače HP5800-48G.
Každý z těchto přepínačů disponuje 2-mi sloty pro line Ethernet moduly, osazenými modulem (HP 5800 16-port SFP) pro 16x SFP porty a modulem (HP 5800 4-port 10GbE SFP+) pro 4x SFP+ porty. Dále je agregační přepínač vybaven, integrovanými 48x 10/100/1000TX porty a integrovanými 4x SFP sloty pro 1G porty. Každý agregační přepínač je osazen 20x 1000BaseSX (SFP) porty (HP X120 1G SFP LC Transceiver) a 4x 10GE (SFP+) porty (HP X130 10G SFP+ LC Transceiver).
Výkonnostní parametry agregačního přepínače jsou:

- Výška 1RU
- Přepínací kapacita centrálních řídících modulů: 284Gbps
- Propustnost: 211Mpps
- Velikost směrovací tabulky IPv4 unicast: 16 000
- Velikost MAC adresní tabulky: 32 000
- Počet bezpečnostních a QoS záznamů v hardware: 12 000

- Všechny fyzické porty pracují v neblokovaném režimu – line rate.
- Podpora směrování IPv4/IPv4 v hardware

HW konfigurace 1 sestavy agregačního L3 přepínače HP5800-48G (2 sestavy v DC1 a 1 sestava v DC2):

- 4x 10GE porty
- 48x 10/100/1000 BaseT Ethernet porty
- 20x 1000BaseSX SFP porty
- 2x napájecí zdroj
- Podpora CWDM/DWDM SFP

Přístupová vrstva

Přístupová vrstva je pouze v lokalitě technologického centra DC1 a je tvořena 20ks L2 přepínačů HP 5120-48G-PoE+ EI.
Každý z těchto přepínačů disponuje 2-mi rozšiřujícími sloty a 4-mi sloty pro SFP/SFP+/CX4 porty.
Přístupový přepínač je vybaven, integrovanými 48x 10/100/1000TX porty a SFP sloty, které jsou osazeny 2x 1G porty (HP X120 1G SFP LC Transceiver).
Výkonnostní parametry přístupového přepínačů HP 5120-48G-PoE+ EI jsou:

- Výška 1RU
- Přepínací kapacita centrálních řídících modulů: 192Gbps
- Propustnost: 142.9Mpps
- Výkon PoE 370W
- Podpora PoE na přístupových portech
- Podpora CWDM SFP

HW konfigurace 1 sestavy přístupového L2 přepínače HP 5120-48G-PoE+ EI (20 sestav v DC1):

- 4x slot pro 1GE nebo 10GE porty
- 48x 10/100/1000 BaseT Ethernet porty
- 2x 1000BaseSX SFP porty
- Podpora CWDM/DWDM SFP

Samostatné management LAN vrstvy

Management LAN vrstva je tvořena 1ks L2 přepínače HP 3100-48 v2 v obou lokalitách.
Každý z těchto přepínačů disponuje 4-mi sloty pro SFP porty. Přístupový přepínač je vybaven integrovanými 48x 10/100/1000TX porty.
Výkonnostní parametry přístupového přepínače HP 3100-48 v2 jsou:

- Výška 1RU
- Přepínací kapacita centrálních řídících modulů: 17.6 Gbps
- Propustnost: 11.7Mpps

HW konfigurace 1 sestavy přístupového L2 přepínače HP 3100-48 v2 (po 1 sestavě v obou lokalitách):

- 4x slot pro 1GE porty
- 48x 10/100/1000 BaseT Ethernet porty

Protokoly fyzické vrstvy

Přepínače podporují vzájemné propojování, případně propojování serverů prostřednictvím agregace portů protokolem Link Aggregation Control Protocol (LACP) dle standardu 802.3ad. Páteřní L3 přepínače HP 7506 a agregační přepínače HP5800-48G podporují konfiguraci 802.3ad přes více Ethernet modulů. Na páteřním přepínači je podporováno až 128 agregací současně, přičemž v každé agregaci lze použít až 8 fyzických portů.

Pro potřeby napájení koncových zařízení prostřednictvím sítě Ethernet (Power over Ethernet –PoE) jsou podporovány protokoly standardu 802.3 revidovaných dle 802.3-2005, tzn. protokoly 802.3af/at (15,4W/port a 30W/port). Revize dle 802.3-2005 zároveň zahrnuje podporu 10G Ethernetu.
Pro zajištění vysoké propustnosti a snížení zatížení CPU páteřního, agregačního a přístupového přepínače jsou podporovány Jumbo rámce až do velikosti 9216 bajtů.
Pro zabezpečení ochrany sítě před zahlcením multicasty a broadcasty jsou k dispozici mechanismy Packet Storm Protection s možností nastavení úrovně akceptovatelného limitu broadcastů a unicastů.

Protokoly 2. vrstvy

Pro zajištění flexibility a škálovatelnosti designu přepínané sítě jsou podporovány protokoly a funkce:

- konvergence sítě 802.1D Spanning Tree Protocol (SPT) - 802.1w Rapid SPT, 802.1s Multiple SPT mechanismy STP rootguard , STP loopguard,
- detekce jednosměrné optické linky (UDLD) a autorecovery po chybovém stavu (UDLD, rootguard, loopguard),
- segmentace sítě do VLAN podsítí 802.1.Q (až 4096 aktivních VLAN na páteřní a agregační vrstvě, 250 na přístupové a 64 aktivních VLAN na management přepínači), vč. Podpory VLAN na základě MAC adres, protokolů a IP podsítí a automatické dynamické registrace VLAN prostřednictvím VLAN Registration protokolu (GVRP). Na agregační vrstvě je zároveň podpora Q-in-Q a selective Q-in-Q,
- prioritizace provozu 802.1p minimálně do 8 vnitřních front (na přístupové a management vrstvě do 4 front),
- uživatelské autentizace prostřednictvím 802.1x suplikantu proti RADIUS serveru (AAA klient),
- detekce protilehlého zařízení IEEE 802.1AB Link Layer Discovery Protocol (LLDP),
- vynucování autonegociace 10/100 pro 10/100/1000BaseT porty.

Protokoly 3. Vrstvy

Součástí funkce páteřní a agregační vrstvy jsou služby směrování IP provozu. Tyto služby jsou podporovány protokoly a funkcemi:

- směrovací RIPv1/v2, RIPng, OSPFv2 a OSPFv3 včetně podpory NSSA a autentizace MD5, BGP-4, BGP-4+ ,
- pro podporu konvergence na 3. vrstvě: MSDP, PIM a PIMv6. Na agregační a přístupové vrstvě také podpora IPv6 MLDv1 & v2 snooping,
- pro podporu real-time aplikací, která je zajištěna prostřednictvím komunikačního protokolu IGMP verze 2 a verze 3 (resp. funkcí IGMP snooping, podporované rovněž na přepínačích přístupové vrstvy),
- směrování podle ACL - Policy-based routing,
- vysoké dostupnosti fyzických směrovačů – VRRP.
- Předávání dhcp požadavků mezi L3 sítěmi – DHCP relay.

Na agregační vrstvě jsou k dispozici služby kvality služeb QoS mapováním do front na základě nastavení DSCP bitů.

Základní bezpečnostní mechanismy

Řízení datového provozu po úroveň 4. vrstvy lze účinně provádět filtrováním provozu. Filtrování provozu je prováděno prostřednictví Access Control Lists (ACL). Pomocí ACL lze definovat pravidlo (s podporou čítače paketů) filtru na rozhraní v příchozím (IN) i odchozím (OUT) směru na základě kombinace:

- Zdrojové/cílové IP adresy a zdrojového/cílového UDP/TCP portu (na přepínačích přístupové vrstvy včetně virtuálních - VLAN, loopback, 802.1ad).
- Zdrojové/cílové MAC adresy

Pravidlo může být aplikováno trvale nebo v konkrétních dnech či časech.
Další významnou bezpečnostní vlastností jsou funkce port security, která umožňuje na portech páteřního a agregačního L3 přepínače:

- Definovat povolené MAC adresy.
- Provést akci (blokování portu, blokování MAC adresy) v případě komunikace z nepovolených MAC adres.

Ochrana před útoky na páteřní a agregační přepínač:
- Ochrana před neplatnými ARP dotazy - Dynamic ARP Inspection (DAI)
- DHCP looping.

Pro detekci nežádoucího provozu (např. spoofing):
- Unicast Revers Path Check (uRPF).

Ochrana před útoky na přístupový přepínač:
- DHCP snooping

Administrace přepínačů
Administrace je typicky prováděna prostřednictvím rozhraní Command Line Interface (CLI), které kromě samotných konfiguračních příkazů umožňuje provádět diagnostické příkazy, jako jsou debbug a show příkazy, jejichž výstupem je řada statistik a informací o stavech fyzických a logických rozhraní. Dále informací o síťovém provozu a komunikačních protokolů apod. Do prostředí CLI je možné se připojit bezpečným protokolem SSHv2, přičemž oprávnění přístupu lze řídit pomocí ACL, zmiňovaných v předchozím odstavci.
Pro účely dohledu a správy je používán protokol Simple Network Management Protocol verze 1, 2. A také SNMP verze3, který umožňuje šifrování přenášených SNMP informací. Přístup přes protokoly SNMPv2 a v3 je možné rovněž omezovat prostřednictvím ACL. Další možností dohledu je využití protokolu sFlow (dle RFC3176), který nabízí sofistikované výstupy pro účely monitorování síťového provozu bez ovlivňování zatížení sítě.
Události zaznamenávané prostřednictvím logových zpráv jsou přenášeny do Syslog serveru pomocí standartního syslog protokolu.
Přesný čas nezbytný pro potřeby dohledu je synchronizován ntp protokolem s NTP serverem. Ochrana před podvrženým NTP serverem je zajištěna MD5 autentizací.
Ověřování oprávnění administrátorských přístup je prováděno proti lokální uživatelské databázi nebo přes RADIUS protokol proti databázi na autentizační RADIUS serveru.
Přepínače podporují DNS klienta pro integraci do domény.
Pro potřeby monitorování nebo diagnostiku síťového provozu je k dispozici funkce kopírování síťového provozu mezi porty – Port mirroring (SPAN).

Servisní vrstva
Servisní vrstva - **Systém pro rozdílení zátěže na servery** (Load Balancery)
Systém dělení datové zátěže je navržen na platformě F5 BIG-IP Local Taraffic Manager (LTM).
Celý systém je řešen v plně redundantním fail-over clusteru 2x F5-BIG-LTM-3900-8G-R s propustností 4Gbps.
Local Taraffic Manager (LTM) je základní komponenta systému F5-BIG-LTM-3900-8G-R, která zajišťuje směrování požadavků od uživatelů na aplikační servery v technologickém centru podle aktuálního zatížení serveru a stavu služeb provozovaných na těchto serverech. Tím je zajištěno rovnoměrné dělení zátěže mezi jednotlivé servery, které jsou takto chráněny před přetížením. Rozklad zátěže je zajišťován volitelnými kombinacemi algoritmů a mechanismů:
- Rozkládání zátěže jednotlivých relací (persistence) na základě Cookies, HTTP hlaviček, zdrojová a cílová IP adresa a SSL v3 session ID
- Round Robin, WeightedRound Robin, Least Connections

Zdraví serverů a aplikací je monitorován prostřednictvím protokolů:
- ICMP
- HTTP/HTTP
- TCP/UDP

HW konfigurace 1 sestavy F5-BIG-LTM-3900-8G-R:

- Výška 1U
- redundantní napájení 2x 300 W AC Power Supply
- CPU Quad Core CPU
- RAM 8 GB
- Compact Flash 8 GB
- Hard Drive 300 GB
- 4x volitelné SX/LX SFP
- 8x Port 10/100/1000
- Port SFP 1 Gbps Fiber

Součástí LTM je SSL akcelerace, což znamená, že přístup k aplikačním systémům je chráněn šifrováním na protokolu HTTPS (SSL relace). Klient komunikuje s LTM šifrovaným spojením a naopak komunikace LTM s aplikačními servery je dekryptována. Přesunutí SSL terminace na předřazená zařízení F5 BIG-IP zároveň umožní centrální management a úložiště SSL klíčů a certifikátů a především odlehčení systémovým prostředkům aplikačních serverů.
Výkonnostní parametry systému rozdílení zátěže na servery:

- Propustnost 4 Gbps
- Max. počet současných spojení 8 000 000
- L7 propustnost 4 Gbps
- L2/L3 Switch Backplane 34 Gbps
- Počet SSL transakcí/s 15 000 tps
- Max. počet současných SSL spojení 1 000 000
- Podporovaný počet nově otevřených spojení min. 175 000/s
- Počet NAT záznamů 1 000 000
- Max. SSL Bulk Crypto 2.4 Gbps
- Max. komprese 3.8 Gbps

Ostatní vlastnosti:

- Podpora statického a dynamického překladu adres NAT/PAT
- Fast Cache
- Rate Shaping
- Podpora IPv4/IPv6 Gateway
- RAM CACHE (cache statických modulů dle URL a min/max velikostí objektů)
- Podpora TCP offloading

Systém rozdílení datové zátěže na servery je možné nasadit do prostředí síťové infrastruktury v L3 (Routed) režimu nebo L2 (bridged) v režimu bez potřeby zásahu do topologie síťové infrastruktury

Vrstvy perimetru sítě

Hraniční routery pro připojení do internetu

Pro zajištění připojení TCk do sítě internet navrhujeme směrovač HP 6602 (JC176A). Tato rodina směrovačů disponuje multicore distribuovanou architekturou, která odděluje zpracování směrovacích a forwardovacích funkcí.
Směrovač je ve variantě rackmount (výška 1U) a je rozšiřitelný o dva interface moduly. V nabízené variantě disponuje směrovač následujícími ethernet rozhraními:

- 4x 10/100/1000Base-T nebo GigabitEthernet SFP combo porty (funguje buďto metalický nebo SFP port) – porty osazeny 3x SFP 1000Base-LX a 1x SFP 1000Base-SX
- 1x 10Gbit XFP (na rozšiřujícím HIM modulu JC168A) – osazen modulem 10GBase-SR

Směrovač je doplněn o přídavný redundantní napájecí zdroj.

Výkonnostní parametry

Přepínač disponuje výkonu při forwardování více než 4,91Mpps (backplane propustnost 48Gbps), při zapnutí běžných funkcí (QoS, ACL, …) neklesá výkon pod 0,5Mpps. Při použití šifrování IPSec neklesá výkon pod 3,8Gbps (3DES/SHA1,1400B packets), při použití IMIX skladby provozu neklesne výkon pod 0,5Gbps.
Při využití firewallovacích funkcionalit je propustnost směrovače nad 2Gbps a při použití NAT překladu adres, je propustnost více než 2,3Gbps.
Vhodnost využití tohoto směrovače pro peering do internetu potvrzuje schopnost akceptovat plnou internetovou směrovací tabulku (full BGP) – směrovač podporuje 1mil. směrovacích záznamů pro IPv4 a 100tis pro IPv6.

Protokol IP
Směrovač umožňuje na jednom L3 rozhraní definovat více IP adres (IP alias), umožňuje také použití protokolu VRRP pro zajištění redundance IP adres mezi několika HW jednotkami.
Směrovač podporuje následující techniky zajištění kvality služby:

- Traffic classification: based on port, MAC address, IP address, IP priority, DSCP priority, TCP/UDP port number, and protocol type
- Traffic policing: CAR rate limiting, granularity configurable
- Rate limiting based on source/destination address (supporting subnet-based rate limiting)
- GTS
- Priority Mark/Remark
- Queue scheduling mechanism: FIFO, PQ, CQ, WFQ, RTPQ, CBWFQ
- Congestion avoidance algorithm: Tail-Drop, WRED
- MPLS QoS
- IPv6 QoS

Díky zmíněným algoritmům lze zajistit požadovanou funkcionalitu dvouúrovňového QoS.
Výběr dalších podporovaných funkcionalit směrovačů:

- DHCP Server/Relay/Client
- DNS Client
- NTP Server/Client
- Telnet Server/Client
- TFTP Client
- FTP Server/Client
- UDP Helper

MPLS
Směrovače také podporují budování MPLS VPN sítí. Mezi podporované mechanismy MPLS patří:

- L3VPN: Inter-domain MPLS VPN (OptionA/B/C), nested MPLS VPN, Hierarchy PE (HoPE), CE dual homing, MCE, multi-role host, GRE tunnel
- L2VPN: Martini, Kompella, CCC, and SVC
- MPLS TE, RSVP TE
- Multicast VPN
- MPLS label inposition a label disposion
- Label swapping
- QoS s využitím MPLS EXP bitů

Směrovací protokoly

- Směrovače podporují následující způsobu směrování:
- Static routing
- Dynamic routing protocols: RIPv1/v2, OSPFv2 s MD5 autentizací a podporou NSSA, BGP, IS-IS
- Route recursion
- Routing policy

A následující protokoly pro podporu IPv6

- Basic functions: IPv6 ND, IPv6 PMTU, dual-stack forwarding, IPv6 ACL
- IPv6 tunnel: manually configured IPv6 tunnel, configured IPv6 over IPv4 tunnel, automatic IPv6 over IPv4 tunnel, 6to4 tunnel, ISATAP tunnel
- Static routing
- Dynamic routing protocols: RIPng, OSPFv3, IS-ISv6, BGP4+

Směrování multicastu
Pro šíření multicastu skrz hraniční směrovač lze využít následující protokoly:

- IGMP (Internet Group Management Protocol) v1/v2/v3
- IGMP snooping
- PIM (Protocol Independent Multicast) DM/SM
- MSDP (Multicast Source Discovery Protocol)
- MBGP
- Multicast static routing
- IPv6 multicast:MLDv1/v2,PIM-DM,PIM-SM,PIM-SSM

Bezpečnost
Směrovač podporuje následující bezpečnostní mechanismy:

- ACL jak IN, tak také OUT směr
- L2 ACL
- ACL acceleration
- Time-based access control
- Packet filter firewall
- Stateful firewall ASPF
- TCP attack prevention on local host
- Control panel rate limiting
- Virtual fragment reassembly
- URPF
- Web filtering
- Hierarchical user management and password protection

Management
Pro management přístup ke směrovači lze využít následující mechanismy:

1. AAA
2. RADIUS klient
3. HW TACACS+
4. směrování log záznamů na syslog server
5. Portal
6. PKI Certification
7. SSH v1.5/2.0
8. podpora ACL pro omezení management přístupu
9. Configuration through the CLI
10. Configuration through the console port
11. Telnet for configuration and remote maintenance through Ethernet port
12. Dialing up for configuration and remote maintenance via Modem through AUX port
13. SNMP (v1, v2c, v3)
14. RMON (group 1, 2, 3 and 9 MIB)
15. System logs
16. Hierarchical alarms
17. Ping and Tracert

18. NQA: Network Quality Analysis, supporting collaboration with VRRP, policy-based routing, and static routing
19. Fan detection, maintenance, and alarm
20. Power supply detection, maintenance, and alarm
21. CF card detection, maintenance, and alarm
22. Temperature detection, alarm
23. NetStream (support v5/v8/v9 packet frames; support IPv4,IPv6 and MPLS packets), což je funkčně plně ekvivalentní technologie, jako je NetFlow v9¨
24. port mirroring

Systém detekce průniku IDS/IPS
Pro detekci/prevenci útoků a bezpečnostních incident nabízíme IPS HP Tippingpoint S1200N (JC527A). Zařízení je formě zásuvného modulu do páteřního přepínače, na jehož interní sběrnici je připojeno interním 10Gb portem. Rovněž disponuje dvěma páry 1Gb Ethernet portů pro online zapojení dvou segment sítě. Pro zvýšení dostupnosti síťového prostředí, podporuje zařízení update operačního systému za běhu a bez dopadu na inspekční schopnosti.
Výkonnostní parametry zařízení
1. Dle údajů výrobce, ale stejně tak dle nezávislého měření společnosti NCSA, je propustnosti IPS modulu 1,3Gb/s a maximální zpoždění menší než 100ms.
2. Počet nově otevíraných spojení za sekundu – 80 tis.
3. Celkové množství současně otevřených a inspektovaných spojení 6,5 mil.
4. Zařízení podporuje transparentní zapojení
5. Optimalizace signatur, včetně adaptivní konfigurace a ochraně proti zahlcení zařízení

Inspekční parametry
IPS sonda podporuje inspekci velkého množství specifických protokolů. Kromě klasického IP provozu se jedná o inspekci 802.1q trunků, QinQ trunků, GRE tunelů, MPLS provozu a také sonda podporuje inspekci IPv6 protokolu a 802.1q VLAN mapping.
Inspekce je založena na existence bezpečnostních signatur, které specifikují jednotlivé případné útoky. Součástí jsou signatury výrobce (digitální vakcína), je však možné importovat z externích nástrojů (SNORT), či vytvořit zákaznické definice. Samotné IPS disponuje schopností odhalit také zero-day útoky, pro které ještě nebyly vytvořeny signatury (pomocí detekce anomálií). Navíc jsou signatury doplněny o databázi reputace jednotlivých IP zdrojů (adresy, DNS jména, domény) v internetu. Díky tomu mohou být některé nebezpečné části internet prohlášeny za nedůvěryhodné a sonda je znepřístupní na úrovni IP a nemusí již nahlížet do obsahu takovéhoto IP provozu. To se jeví jako velmi přínosné pro využití výpočetního výkonu sondy. Aktualizace všech těchto databází se děje v intervalech minimálně 2x týdně, v nutných případech I častěji.
Sonda podporuje následující skupiny signatur:
1. exploit
2. zranitelnosti
3. krádeže identity
4. spyware
5. viry
6. vynucování bezpečnostních politik
7. filtry proti průzkumným aktivitám
8. filtry proti síťové infrastructure
9. IM aplikace (instantní messengery)
10. filtry proti P2P sítím
11. nástroje na kontrolu toku multimédia
12. DoS útoky (např. ICMP floods, UDP floods, SYN floods a TCPEstablishConnectionfloods), sonda zvládne zachytit vice než 100tis takovýchto útoků za vteřinu a to bez vlivu na inspeci dalšího provozu

Po identifikaci hrozby může sonda provést následující akce:

1. Block,
2. Block + Notify
3. Block + Notify + Trace
4. Permit
5. Permit + Notify
6. Permit + Notify + Trace
7. Rate Limit
8. Network and Web Quarantine

Pro případ zapojení sondy do LACP trunků (nebo podobných asymetrických toků), podporuje sonda asymetrickou inspekci . Tato vlastnost je klíčová v plánované topologii TCk, hlavně díky využití virtualizace přepínačů a požití distribuovaných LACP linek.
Zařízení navrhujeme společně s management nástrojem HP vSMS, který umožňuje globální správu vice IPS sond a tvorbu meta pravidel. Jednotlivé IPS sondy jsou však spravovatelné také samostatně, pomocí vestavěných HTTPS management nástrojů.

Firewall
Kernun Firewall+ je prvním českým **next generation firewallem**. Výjimečný je především svým zaměřením na specifika a zvláštnosti českého prostředí, které je v mnohém velice odlišné od zbytku celého světa. Zná jak aplikace mezinárodního formátu, tak čistě lokální aplikace jako jsou například Datové schránky, formuláře správy sociálního zabezpečení, či internetové bankovnictví českých bank.
Firewall+ je vyvíjen s velkým důrazem na aktuální trendy v oblasti síťové bezpečnosti, které neustále sledujeme a zohledňujeme ve všech svých produktech. Díky pravidelným aktualizacím je Kernun Firewall+ schopen se pružně přizpůsobovat neustálým změnám podmínek a prostředí, je tak stále spolehlivý stejně, jako při jeho pořízení.

Hlavní výhody řešení:

- Díky použité technologii je možné specifikovat jednotlivé aplikace (např. Datové schránky, Facebook, Skype, Google Docs, P2P sítě apod.) a to nehledě na čísla portů. Je tedy možné velice jemně nastavit bezpečnostní politiku v síti.
- Podporované aplikace jsou charakteristické pro české prostředí, které dobře známe, což nám umožňuje nabídnout vyšší efektivitu, než konkurenční produkty.
- Kernun Firewall+ navíc rozeznává jednotlivé uživatele, nikoli pouze IP adresy. Jednotliví uživatelé jsou rozpoznáni podle přihlášení do domény v LDAP adresáři nebo na základě autentizace přímo na firewallu. Skupiny uživatelů pak mohou mít svá vlastní pravidla a nastavení komunikace na firewallu.
- Podpora široké škály autentizačních mechanizmů s návazností na MS Active Directory, Kerberos, Radius nebo LDAP. Možnost definice politiky na základě uživatelů, skupin, IP adres a data/času. Definice výjimek, vyhodnocování kombinací a nadřazenosti umožní vytvořit bezpečnostní politiku bez jakýchkoliv omezení.
- Možnost logování lokálně nebo vzdáleně, včetně logování do jednoho místa. Logy ze zařízení mohou být chráněny pomocí podepisování a šifrování. Kromě interní struktury logů jsou k dispozici také konvertory do formátu Apache, Squid a syslog.
- Správce má k dispozici záznamy o veškerých činnostech. Všechny logy jsou ve strukturovaném formátu a lze je libovolně analyzovat a dohledávat konkrétní záznamy, archivace veškeré komunikace není časově nijak omezena.
- Rozpoznávání typu souboru na základě skutečného obsahu a signatur dokumentu (PDF, Flash, spustitelná aplikace, video …). Nezáleží přitom na použitém protokolu, možná je i inspekce dat přenášených šifrovaně pomocí protokolu SSL.

- Možnost blokování služeb instant messaging (ICQ, SKYPE….) a služeb remote desktop (LogMeIn, TeamViewer…). IM nástroje mohou v současném konkurenčním prostředí znamenat ohrožení citlivých interních informací.
- Integrovaný VPN server s podporou IP Sec i SSL/TLS. Ukončení VPN spojení na FW s možností provádění veškerých bezpečnostních kontrol provozu.
- Řízení sítové komunikace na úrovni paketového filtru i jednotlivých aplikačních protokolů v rámci aplikačních proxy pro HTTP, FTP, SMTP, POP3, IMAP4, DNS, SIP, H.323 i SQL*Net. Součástí řešení jsou i generické TCP a UDP proxy.
- Umožnuje zakončit šifrovanou TLS/SSL komunikaci a provádět aplikační a bezpečnostní kontrolu v šifrovaném provozu pomocí aplikačních proxy.
- Plná podpora IPv6 včetně Dual- Stack, IPv6/IPv4 brána, TRT, IPv6 multicast.
- Blokování panelů a dynamického obsahu na základě zdroje informací. Filtrování Web 2.0 pro eliminaci hrozeb souvisejících s anonymním obsahem sociálních sítí a „user customized“ webovými portály.
- Kernun Firewall+ se vyznačuje modulární architekturou s možností dalších úprav podle požadavků cílového nasazení. Samozřejmostí je vysoká úroveň lokalizace uživatelského rozhraní nejen do českého jazyka.
- Jedinečná záruka odstranění bezpečnostní chyby do 10 pracovních dnů s okamžitým work around zásahem.

Kernun FW+ je rozšířen o modul pro filtraci webového provozu Kernun Clear Web. Jedná je webový filtr nové generace orientovaný primárně na webové stránky navštěvované uživateli v ČR. Hlavním cílem Clear Webu je maximální úspěšnost kategorizace použitých webových odkazů u konkrétního zákazníka. Vysoká úroveň kategorizace je garantována lidskou obsluhou a také zaměřením na uživatele z ČR a Střední Evropy. Kromě standardního web filtru používá Kernun Clear Web navíc modul analýzy uživatelských URL, který zajišťuje minimální velikost databáze, maximální rychlost filtrace a maximální úspěšnost kategorizace, vždy na míru konkrétní instalace.

Hlavní výhody řešení:

- Vysoká úspěšnost kategorizace webových stránek navštívených českými uživateli (98% provozu). Znalost stereotypů místních uživatelů a jazyka zaručuje vysokou kvalitu a nízkou chybovost kategorizace.
- Kategorizace stránek se provádí podle celé URL, nejen podle domény druhého, či třetího řádu včetně možnosti zařazení stránek do více kategorií.
- Databáze kategorií je neustále doplňována a průběžně aktualizována. 99 % neznámých stránek navštívených našimi zákazníky je zatřízeno do následujícího dne.
- Blokování panelů a dynamického obsahu na základě zdroje informací. Filtrování Web 2.0 pro eliminaci hrozeb souvisejících s anonymním obsahem sociálních sítí a „user customized“ webovými portály.
- Filtrování aktivních elementů webových stránek (ActiveX, JavaScript, Java Applety, …). Možnost nastavení této filtrace pouze na vybrané kategorie stránek.
- Filtrace stahovaných dokumentů podle kategorie stránek, na základě black/white list, dle definičních pravidel, velikosti souboru, přípony souboru nebo ověřeného typu souboru (true-type file detection).

Kernun FW+ s modulem Clear Web popsaný výše bude nasazena jako HW appliance v režimu cluster active/active tj. v každé z lokalit bude jedna HW appliance Kernun FW+. Clusterového řešení je dosaženo pomocí load balanceru, který zajištuje nejenom zachování plné funkčnosti v případě výpadku jednoho z uzlů, ale i rozkládání zátěže na jednotlivé uzly clusteru. Z důvodu vysoké dostupnosti bude každý z uzlů clusteru naddimenzované tak, aby v případě výpadku jednoho z nich druhý převzal veškerý provoz bez omezení. Samotné HW appliance clusteru obsahují redundantní prvky jako RAID disku, Hot-Swap zdroj napájení, agregované sítové rozhraní. HW appliance obsahují management porty, které budou zapojeny do

management sítě. Pomocí nich je možné i v případě kritického výpadku provádět vzdálenou analýzu a recovery obnovu.
Otevřenost nabízeného řešení pro další úpravy a případné budoucí připojení dalších systémů a zároveň s ohledem na zachování stávající investice je zaručeno dodáním zdrojového kódu FW Kernun + oproti NDA, s možností a právem modifikace tohoto systému. Tím je zaručena maximální možná otevřenost systému pro další úpravy a zachování investice. Měnit funkce a vlastnosti řešení skrze jeho nativní funkčnost je možné přeinstalováním libovolného balíku, který je kompatibilní s OS Kernun (FreeBSD) včetně pokročilého nastavení jemného ladění výkonnostních parametrů. Měnit funkce a vlastnosti skrze jeho konfigurační parametry je možné pro veškerou funkcionalitu FW Kernun + s modulem webové filtrace a VPN řešení. Jednotlivé parametry je možné měnit pomocí grafického rozhraní a to jak u paketového filtru, tak jednotlivých aplikačních proxy HTTP, FTP, SMTP, POP3, IMAP4, DNS, SIP, H.323 i SQL*Net i generické TCP, UDP a VPN. Jednotlivé konfigurační parametry jsou součástí veřejné dokumentace http://download.kernun.com/doc/handbook.pdf a jedná se o nepřeberné množství parametrů, cca 800 stránek textu. Pro příklad je možné uvést http proxy s clear webem, kde je možné nastavovat politiku pravidel řídící přístup uživatelů k webovým stránkám na základě IP adresy, portů, doménových jmen, skupin, uživatelů, regulárních výrazů, kategorií, názvů serverů, času, šířky pásma, typu souboru, typů aplikace. Tuto komunikaci lze povolit, zakázat, omezit či modifikovat. Také je možné nastavit různé parametry pro dosažení nejvyšší výkonnosti v daném prostředí a další.

SAN přepínače
Součástí nabízeného řešení je čtveřice SAN přepínačů HP 8/40 Base SAN Switch. V každé lokalitě bude umístěna dvojice SAN přepínačů, které budou tvořit dva redundantní SAN Fabric, aby při výpadku jakékoli komponenty nebyla narušena funkčnost celého systému.

Vlastnosti nabízených SAN přepínačů:

- Neblokující platforma bez přetížení (over-subscription) s celkovou šířkou pásma 680 Gb/s v provedení 1U
- 24 portů aktivních portů s rychlostí 8Gb/s
- Autodetekce rychlosti portů 8Gb/s, 4Gb/s, 2Gb/s, 1Gb/s
- Možnost rozšíření až na 40 portů s rychlostí 8Gb/s
- Obsahuje port USB, který usnadňuje obsluhu a protokolování chyb pomocí upgradů firmwaru a stažených souborů systémového protokolu.
- Využívá grafické rozhraní Brocade Fabric Manager dostupné přes webové rozhraní
- Redundantní napájení
- Podpora technologie NPIV (N-Port ID Virtualization)
- Součástí SAN switchů je licence ISL Trunking, která umožňuje vysokorychlostní propojení switchů (trunking) až na rychlost 8x 8Gb/s, celkem 64Gb/s
- Součástí SAN switchů je licence Full Fabric, která odstraňuje omezení počtu FC switchů v SAN
- Součástí dodávky jsou SFP moduly do FC switchů (duplexní LC konektory) pro připojení všech dodaných zařízení s rozhraním do SAN i na propojení mezi Hlavním a Záložním datovým centrem včetně potřebných optických propojovacích kabelů
- Všechna zařízení připojované do SAN jsou kompatibilní s nabízenou diskovou virtualizací a s nabízeným zálohovacím systémem
- SAN switche jsou certifikovány pro serverovou virtualizaci VMware vSphere 5.

Management a monitoring

Síťový management systém a centrální management portál
Cílem realizace je získání systému pro dohled a správu všech prvků datacentra. Systém bude schopen sledovat jak síťové prvky, tak i další moduly datového centra jako jsou disková úložiště, záložní zdroje napájení atd. Informace o jejich stavu budou zobrazeny přehlednou formou v centrální dohledové konzoli (management portálu). Při zjištění problému se objeví informace v centrální konzoli, díky využití řady metod pro izolaci zdroje problémů se pro správce výrazně zjednoduší nalezení primárního problémů, což vytváří dobré podmínky pro jeho rychlé vyřešení. Systém umožňuje správce také automaticky notifikovat pomocí emailu či SMS.

Kromě základní konzoly jsou součástí také moduly pro správu a sledování výkonnosti nejdůležitějších prvků datacentra. Sledování výkonnosti umožní detailnější analýzy zátěže a tím předcházet budoucím problémům, lépe plánovat případná rozšíření atd. Moduly pro správu pak zjednodušují správu síťových prvků, sledují verze firmwaru například z hlediska potřeb zabezpečení atd.

Jako konkrétní řešení byly zvoleny produkty firmy HP - HP Network Node Manager (i) pro dohled prvků a centrální konzoli, HP Network Automation pro funkce správy konfigurací a HP iSPI Performance Metric pro výkonnostní dohled. Ve všech případech jde o ověřené systémy s dlouhou historií, což dává předpoklad stabilního provozu. Systémy podporují fault tolerant nastavení a podporují více platforem, v rámci nabídky předpokládáme nasazení na Windows Server 2008 64bit.
K dispozici je i řada dalších modulů od firmy HP, které lze plně integrovat s navrženým řešením. Týká se to například modulů pro MPLS VPN a NetFlow performance, zmíněných jako možné budoucí doplňky v rámci poptávky.

Konkrétní technické řešení

Úvodní předpoklady

Pro splnění požadavků zadání navrhujeme využití a integraci dvou produktů firmy HP - HP Network Node Manager(i), (dále HP NNMi) a HP Network Automation (dále HP NA). Produkty se z hlediska zadání do jisté míry prolínají - HP NNMi spadá z větší části do oblasti management portálu, HP NA do oblasti síťového managementu. Rozdělení ale není úplně přesné a zejména HP NNMi zasahuje i do řady funkcí, které byly v zadání uvedeny v oblasti síťového managementu, proto popisujeme tyto kapitoly společně. Kromě těchto základních modulů je vhodné i nasazení moduly HP iSPI Performace for Metrics pro detailnější sledování výkonnostních dat kritických prvků.

Stručná charakteristika HP Network Node Manager (i)

HP NNMi (aktuálně ve verzi 9.1) je řešením firmy HP pro síťový management. Pro nasazení v rámci JMK je zásadní to, že slouží jako centrální konzola, do které se integrují další moduly od HP i třetích stran a proto může posloužit i jako centrální management portál. NNMi ale poskytuje i řadu funkcí pro monitoring sítě (Network Fault Management), stejně jako sledování prakticky jakéhokoli prvku, založeném na SNMP.
Vlastnosti důležité pro nabídku:

- Kvalitní konzole založená na webovém rozhraní (WebGUI)
- Možnost customizace konzole, přístup podle rolí
- Obsáhlé možnosti pro discovery síťových i jiných prvků
- Funkce pro potlačování duplicitních událostí (Event flood) pomocí propracované Casual engine
- Funkce pro rychlé nalezení primární příčiny problému (root cause analysis)
- Téměř neomezené možnosti pro práci se SNMP zařízeními - import MIB, zpracování trapů na události atd. Podporováno je i SNMP v3.
- Možnosti exportů do jiných systémů
- Podpora fault tolerance - založen na kombinaci primárního a backup systému, mezi kterými probíhá replikace
- Možnost integrace s řadou dalších produktů HP:
    - V rámci základní implementace bude do konzole integrován modul HP NA a iSPI Performance for metrics
    - Možná nativní integrace s moduly pro budoucí rozšíření - MPLS, NetFlow performance a další
- Podpora performance managementu
    - Základní je přímou součástí NNM
    - Rozšířené možnosti pomocí iSPI se objeví přímo v konzoli jako její nedílná součást
- Alarm Point Express - modul pro notifikaci při alertech s podporou plánovacích kalendářů pro hotovostní skupiny

HP NNMi lze provozovat na řadě platforem, pro prostředí JMK předpokládáme instalaci na platformě Windows 2008 Server Standard 64bit.

Stručná charakteristika HP Network Automation

Řešení HP Network Automation (aktuální verze 9.1) lze popsat jako "Management konfigurací a změn". HP NA provede discovery síťových zařízení, na rozdíl od NNMi se ale zaměřuje na konfigurace - verze

firmware, konfigurační soubory switchů a routerů, atd. Konfigurace jsou uloženy na servery HP NA (včetně verzování).
Pro tuto nabídku pokládáme za zásadní následující funkce:

- Snadná distribuce (obnova) konfigurací na všechna zařízení v síti
- Možnost vynucování politik, kontroly souladu se standardy
- Diagnostika problému s možností porovnání s baseline - HP NA ukáže, kde se odlišuje aktuální konfigurace od uložené starší
- Vynikající integrace s HP NNMi - sdílení discovery, možnost volání NA přímo z centrální konzoly atd.
    - Administrátor proto v praxi bude většinu času pracovat pouze s konzolí NNMi, kde uvidí všechny alerty, při diagnostice si zavolá kontextově NA.
    - Naopak při potřeba administrovat nový prvek je možné jeho discovery pomocí NNMi, z jeho konzole se pak zavolá NA, které provede jeho standardizovanou konfiguraci atd.
    - Mezi NNMi a NA probíhá rovněž synchronizace SNMP komunit - pokud NNMi objeví prvek s implicitní komunitou a NA provede změnu nastavení včetně volby bezpečnější komunity, tak se tato změna zpětně promítne do NNMi
    - Mezi konzolemi NNMi a NA je možné sjednocené přihlášení (SSO)

HP NA lze provozovat na řadě platforem, pro prostředí JMK předpokládáme instalaci na platformě Windows 2008 Server Standard 64bit (shodnou s HP NNMi).

Architektura nasazení
Doporučujeme provést základní nasazení systému na dva servery - jeden pro HP NNMi, druhý pro HP NA a performance DB pro HP iSPI.
Při požadavku na fault tolerance přibydou dva další servery jako záložní - aplikační cluster.

HW nároky:

Server	Účel	CPU	RAM	HDD
SRV1	HP NNMi	4xCore	16GB	min 72GB
SRV2	HP NA, iSPI	4xCore	16GB	min 200GB

Licencování produktu
V rámci nabídky je nutno zalicencovat tři moduly:

- HP NNMi
- HP NA
- HP iSPI for Performance Metric

Všechny moduly se licencují "per node", tedy podle počtu sledovaných objektů.

V případě HP NNMi je nutné licencovat vlastně všechny SNMP sledované objekty v síti, včetně například čidel teploty, UPS, atd. Ze zadání vyplývá požadavek na minimum 100 nodů, doporučujeme ale zakoupit licenci na 250 node, s ohledem na cenovou politiku je totiž cena za 250 node totožná, či spíše nižší, než za 100 node. Stejným způsobem je licencován i výkonnostní dohled iSPI, sice by postačoval pro menší počet nodů, jednotková cena ale pro 250 mode poklesne o tolik, že se menší počet licencí nevyplatí.
Situace u modulu HP NA je mírně odlišná, zde má cenu licencovat pouze klíčové prvky návrhu, u kterých má smysl řešit verzování konfigurací atd. V nabídce proto u tohoto modulu uvádíme licenci pro 50 nodů.

Pro případ nasazení fault tolerant řešení jsou pro všechny moduly součástí nabídky i tzv. NP (non productive) licence za výrazně nižší cenu, které se použijí pro záložní nody.

Možný budoucí rozvoj a škálování
Na navržených serverech je reálně možné provozovat minimálně dvojnásobný počet prvků, než na kolik je navržena licence. V případě přidání dalšího hardware je ale možno škálovat téměř neomezeně - například u HP NNMi jsou uvažovány konfigurace v desítkách tisíc nodů a stovkách tisíc objektů v nich.
Druhou možností rozvoje je doplnění dalších funkcí přidáním dalších plně integrovatelných modulů.
Jde například o tyto produkty:

- HP iSPI for MPLS pro dohled MPLS VPN

- HP iSPI Performance for Traffic pro výkonnostní reporty pomocí NetFlow a podobnými nástroji
- HP Operations Manager pro detailní dohled operačních systémů a aplikací na serverech
- HP BSM pro monitoring z pohledu služeb

Kromě toho je možná integrace i se řadou dalších nástrojů třetích stran (např. Ciscoworks, IBM Netcool).

Projektová dokumentace
Součástí nabídky je zpracování projektové dokumentace a dokumentace výsledného provedení plnění a její předání Objednateli.
Projektová dokumentace bude min. obsahovat:

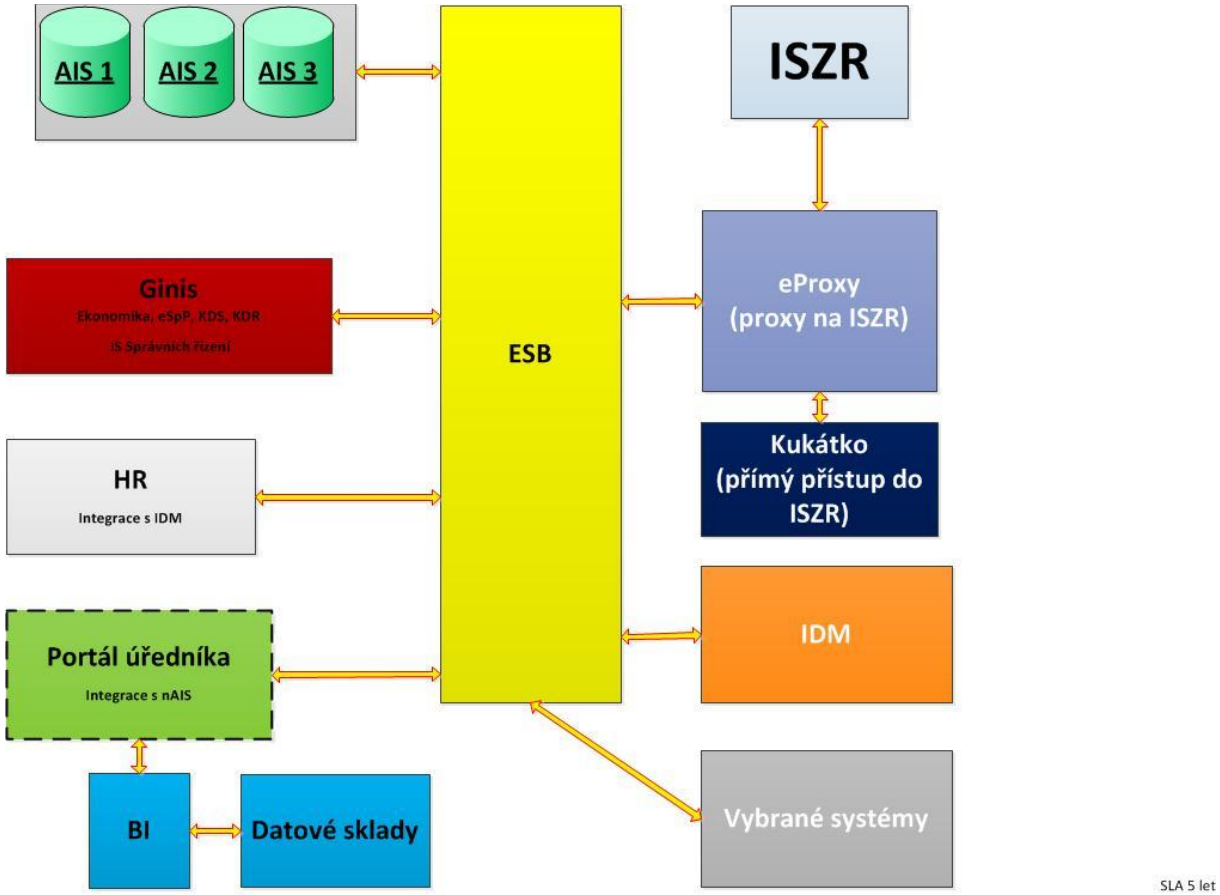
Projektová dokumentace musí min. obsahovat:

- Detailní popis technického řešení infrastruktury TCK
- Nákresy zapojení prvků
- Jmenné konvence a adresní plány
- Pracovní postup implementace a migrační plán
- Testovací postupy ověření vysoké dostupnosti redundantních subsystémů TCK
- Testovací scénáře pro ověření funkční implementace dílčích systémů, aplikací a služeb
- Uživatelskou dokumentaci pro nově dodávané aplikace v českém jazyce
- Administrátorskou dokumentaci pro správu a instalaci nově dodávaných komponent systému

Dokumentace výsledného provedení plnění bude realizována formou aktualizace dodané projektové dokumentace po úspěšném dokončení implementačních prací a odrazí finální stav plnění. Součástí dokumentace budou také konfigurace jednotlivých prvků KI.

Implementace
Součástí nabídky je kompletní instalace, funkční konfigurace dodaných prvků a subsystémů, integrace se stávající ICT infrastrukturou, migrační práce související s přechodem na virtuální serverovou infrastrukturu. Jednotlivé kroky implementace a také funkčnost dodaného plnění jako celku bude ověřena akceptačními testy, které Zhotovitel navrhne ve fázi tvorby projektové dokumentace.

I.B: Detailní popis řešení - Vnitřní integrace Krajského úřadu
Systém bude řešit integraci v rozsahu požadovaném v dokumentu Rozvoj eGovermentu v Jihomoravském kraji. Návrh integrace je zobrazen na následujícím schématu. Před provedením vlastním integrace bude provedena analýza. Tento návrh je řešen pomocí *„best practices“* návrhu integrace SOA.



Obrázek –Integrace app

Integrace různých systémů je složitým odvětvím, kde výsledkem musí být komunikace zdánlivě nesourodých systémů. Předmětem analýzy bude vybrat takové systémy, aby byly splněny cíle Objednatele.
Z obrázku je patrné, že Datové sklady budou integrovány přímo do Portálu úředníka. Toto řešení jsme zvolili proto, že jde o zprostředkování dat a různých reportů. Nejedná se o funkce potřebné v jiných systémech. Pracovník KÚ data najde na jednom místě v Portálu úředníka.
Analyzovány budou Agendové informační systémy za účelem vybrání funkcionality potřebné pro integraci. Aplikace GINIS je již na úřadě nainstalována a je psána tak, že je schopna se integrovat na jiné systémy. Systém bude integrovat i aplikace HR. Její hlavní integrační aplikací bude nově dodávané IDM. Další z předmětu analýzy bude navržení integrace a využití dat ze systému HR. Stěžejní aplikací pracovníka KÚ je Portál úředníka. V rámci analýzy bude vybrán seznam aplikací vhodných pro zobrazení v portálu úředníka. Již teď lze říci, že v portálu bude možné zobrazit informace z Datových skladů a přihlášení do tohoto portálu proběhne přes centrální IDM. Dále pak aplikace jako je modul eSpS aplikace GINIS.
Na obrázku je zobrazeno eProxy. Jde o aplikaci, která poskytuje rozhraní ISZR dále do systému. Navíc provádí audit dotazů do ISZR. Výstupem analytické části bude seznam atributů a dotazů, které se budou logovat a auditovat.

Analýza stávajícího stavu a návrh integrace Identity Management (IDM)

Zavedení Identity Management (IDM) do systému

Návrh, analýza, nasazení systému vychází z předpokladu, že samotný IDM je středem správy identit. Pro jeho smysl je potřeba současně s ním nasadit minimálně jeden AD systém a ten pomocí konfiguračního formuláře propojit s IDM.

Další integrované systémy budou zahrnuty do systému IDM tak, aby se z pohledu uživatele jednalo pouze o konfigurační ukazatele. Je nutno podotknout, že pro tyto systémy bude před samotnou konfigurací nutno řešit rozhraní tak, aby odpovídalo oběma stranám spravujících identity Objednatele (IDM i IS třetí strany, tj. integrované rozhraní).

Seznam protokolů a služeb vznikne až v průběhu analýzy integrovaných systémů, ale již v této části je zřejmé, že bude minimálně v rozsahu: LDAP, HTTPS, SOAP a případně protokol pro zabezpečený přenos souborů SFTP, které jsou standardem pro komunikaci

INTEGRACE IDM S PERSONÁLNÍM SYSTÉMEM OBJEDNATELE

Systém je navržen jako tenký, webový klient. Pro práci s IDM budou navrženy formuláře, pomocí kterých bude umožněno provádět požadované akce. Po odeslání údajů formulář předá data webové službě, která bude mít za cíl propagaci dat jak do samotného systému IDM, tak do MS AD a zároveň i do ostatních systémů. Výhodou tohoto řešení je modularita systému a zároveň maximální re-use již vyvinutých služeb.

Zhotovitel předpokládá v první etapě provést podrobnou analýzu požadavků na IDM s tím, že součástí tohoto postupu je i analýza požadavků na systémy třetích stran:

Personální systém Objednatele

Elektronická spisová služba

Ekonomika

Celkový seznam integrovaných systémů bude vznikat na základě podrobné analýzy tak, aby v co největší míře využíval již existující služby IDM, které vznikly v průběhu předchozího vývoje.

Pro navržené IDM bude použito vytvoření vlastní struktury v SQL databázi pro potřeby autentizace externích IS. Tento přístup bude reflektovat bezpečnostní politiku úřadu, která může být rozšířena pro potřeby dohledu aktuálnosti.

Obvykle je pro určenou skupinu externistů delegován interní zaměstnanec v roli garanta, jehož úkolem je periodicky aktualizovat svěřené identity. Procesní zajištění je vhodné doplnit technickými prostředky jako je dočasná (například dvouměsíční) platnost účtů, prodloužení jejich platnosti je v takových případech delegováno právě na garanta.
Pro zjednodušení práce garanta (administrátora externích systémů) lze povolit nastavení neomezené platnosti účtu s omezenou platností hesla.

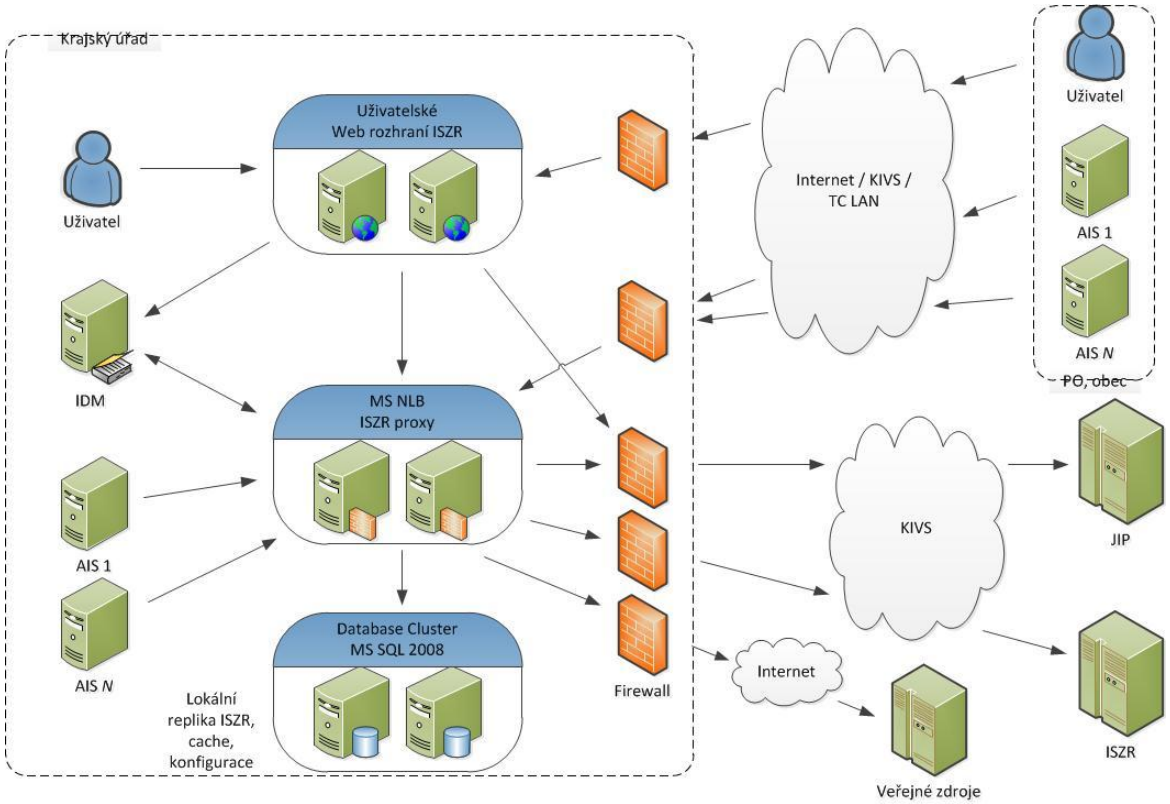
Integrační bod vůči veřejným registrům
Úlohou této části bude zprostředkovat data z veřejných registrů Agendovým informačním systémům (AIS). Komunikace bude procházet přes Informační systém základních registrů (ISZR). Veškerá komunikace AIS a ZR tak bude procházet jediným bodem. Tím se dá zajistit vysoká míra zabezpečení:

- AIS nebudou mít přímý přístup do ISZR
- Bude možné autorizovat každý požadavek směřující do ISZR
- Bude možné omezit dotazy dle pravidel ISZR (hodnot, objektů, počtu dotazů atd.)
- Bude možné vytvářet centrální log o komunikaci s ISZR

To řešení dále přinese možnosti rozšířené funkcionality

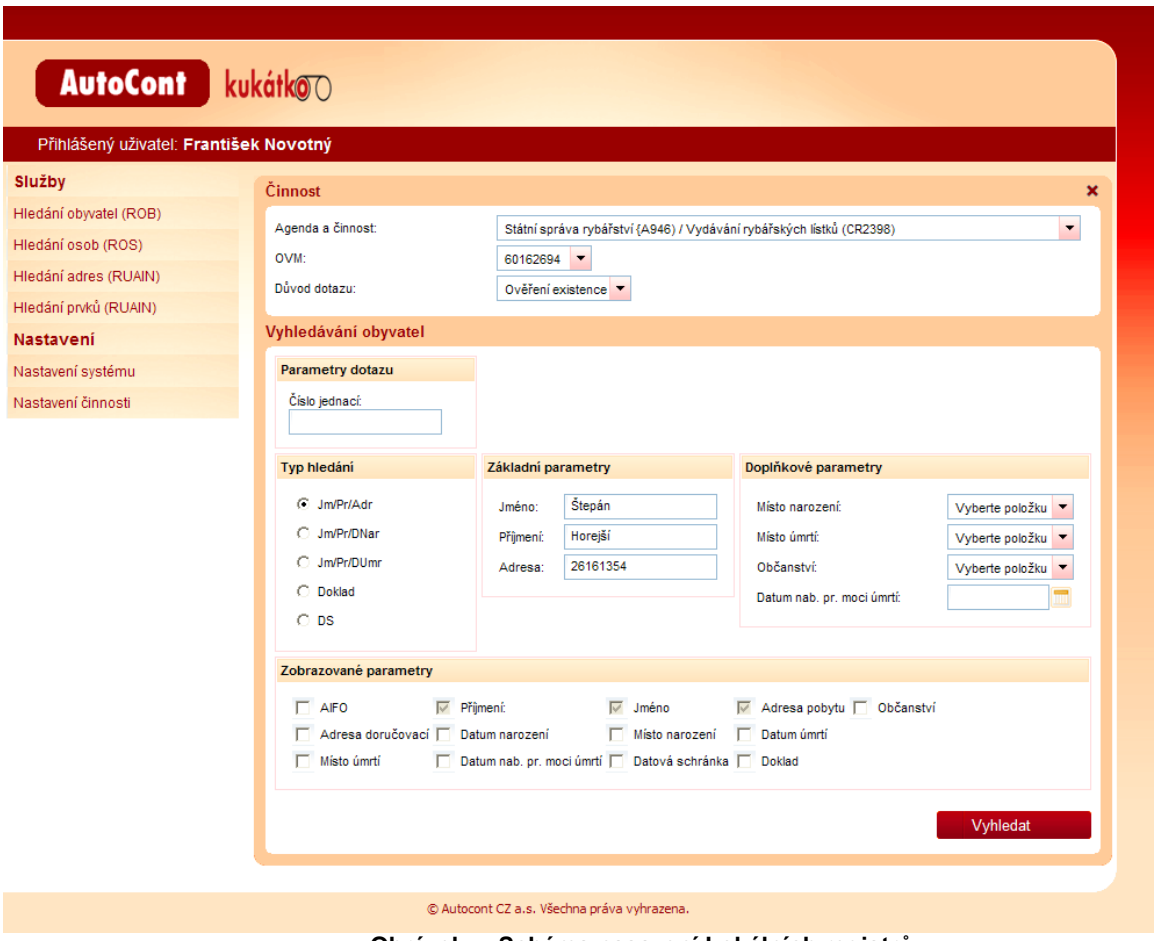
- Zajištění opakovaného volání ISZR u odpovědí rozdělení do několika částí
- Natavení priorit volání jednotlivých AISů
- Serializace sekvence požadavků
- Vytvoření krátkodobé cache výsledků
- Centrální hlášení chybových stavů administrátorům
- Vytvoření Lokální repliky ISZR z výsledků realizovaných dotazů
- V případě nutnosti vytvořit nestandardní rozhraní ISZR (TXT soubor, ODBC)

eProxy (ISZR proxy) bude mít stejné rozhraní jako ISZR. AIS budou pro práci s eProxy používat stejná volání jako při práci s ISZR – pouze budou přesměrovány na adresu serveru eProxy. Bude třeba dát eProxy k dispozici certifikáty jednotlivých AIS nutné pro komunikaci s ISZR.



Obrázek – Integrace Základních Registrů – rozhraní ISZR

Uživatelské Web rozhraní ISZR
Tato komponenta bude určena pro práci uživatele s daty ISZR. Jejím úkolem je vyřešit absenci uživatelského rozhraní ISZR. Uživatelské Web rozhraní ISZR bude možné používat především pro ty agendy krajského úřadu, které nemají informační systém napojený na ISZR.
Protože je nutné vyřešit autentizaci a autorizaci uživatele na úrovni úřadu, bude Uživatelské Web rozhraní ISZR napojeno na IDM, případně na JIP. Předpokládá se napojení Uživatelského Web rozhraní k ISZR přes komponentu eProxy.
Uživatelské Web rozhraní bude komunikovat s ISZR přes eProxy. Rozhraní bude možné využívat pro všechny zaregistrované agendy úřadu, podmínkou je instalace potřebného certifikátu AIS.
Bude sloužit jak interním uživatelům krajského úřadu, tak externím uživatelům využívajícím služeb hostingu (PO, obce). Pokud z analýzy vyplyne potřeba oddělit prostředí určené interním uživatelům od prostředí určeného externím uživatelům, bude pro externí uživatele rozběhnuta další instance eProxy na zvláštních virtuálních serverech. V opačném případě bude využita možnost provozovat obě instance na stejných virtuálních serverech. Na následujícím obrázku je ukázka návrhu uživatelského rozhraní:



Obrázek – Schéma nasazení Lokálních registrů

Pro uložení konfiguračních parametrů, rozpracovaných reklamací a případně dalších dat bude použita SQL databáze.
Autentizace a autorizace uživatelů bude možná díky napojení na AD a IDM, dále bude možné (především pro externí uživatele) využít napojení na JIP.
Nasazení se bude dále řídit postupy, normami a metodikami Autocont uvedenými v následující kapitole.

Aplikace eProxy je v souladu s požadavky Objednatele a to v těchto bodech:

- Ohlášení Agendy a Rolí pro výkon v Agendě u správce Registru Práv a Povinností (RPP),
- Povinnosti zaregistrovaných Rolí v Agendě provádět změny referenčních údajů v ostatních Základních Registrech (ROS, ROB, RUIAN) po vlastních rozhodnutích, které tyto referenční údaje mění (Role Editor v Agendě),
- Povinnosti Agendových informačních systémů ukládat vlastní Akt rozhodnutí a odkaz na právní předpis, podle kterého bylo rozhodnutí učiněno, do RPP (Role Editor v Agendě),
- Povinnosti provést ověření a aktualizaci referenčních dat základních registrů, pokud jiná Agenda zpochybní jejich hodnoty (referenční záznamy základních registrů ve stavu „zpochybněno“)
- Vedení Katalogu služeb úřadu, které musí Agendy publikovat do RPP, aby je mohly využívat subjekty (fyzické a právnické osoby) a ostatní Agendy při součinnosti
- Potřeba zajištění požadovaných referenčních dat Základních registrů do prostředí krajského úřadu k využití v AIS a pro podporu kvalifikovaného rozhodování v souladu se zákonem č. 111/2009 Sb., o základních registrech, ve znění pozdějších předpisů.

eProxy bude splňovat následující:

- Implementovat přístupový adaptér pro čtení informativních údajů ze základních registrů
- Implementovat systémy pro shromažďování, vyhodnocování a archivaci logovaných informací
- Implementovat systém umožňující provádět audit a sledovat činnost a aktivity uživatelů AISu na základě oprávnění k jednotlivým činnostem v rámci agend.

eProxy bude splňovat tyto funkční požadavky:

- Auditní činnost systému jednotlivých přístupů uživatelů k agendám v souladu s paragrafem 57 zákona č. 111/2009 Sb. o základních registrech ve znění pozdějších předpisů a uchovávání po dobu minimálně jednoho roku
    - Identifikaci volajícího uživatele – přímo či nepřímo inicioval
    - Důvod a konkrétní účel využití služby
    - Subjekt, pro jehož účel se údaje využívají nebo poskytují
    - OVM, pro které je služba vykonávána
    - Identifikace agendy, na základě které volání probíhá
    - Agendová role, která službu využívá
- Systém bude navíc dostatečně robustní a bude mít tyto vlastnosti
    - Uložení jednotlivých údajů bude zabezpečeno a šifrováno
    - Uložení bude snadno zálohovatelné.

Katalog služeb integrace bude plněn v rámci administrativního rozhraní. Přístup k KS bude definován v centrálním IDM. Seznam atributů uchovávaných v katalogu služeb bude předmětem analýzy. Již teď lez ale identifikovat tyto atributy: Jméno služby identifikátor, adresa, popis služby, definované sla služby. Funkce katalogu služeb budou: vypiš seznam, vypiš detail služby, vlož službu, uprav službu, smaž službu.

Nad rámec dodávky Zhotovitel dodá aplikaci Kukátko
Jde o pomocný informační systém, který se uplatní tam, kde kraj nemá vhodný agendový systém, ale potřebuje získat informace z registrů. Tento systém bude dále rozvíjen o další funkce na požádání Objednatele. Předmětem analýzy bude seznam těchto nových dotazů do ISZR.

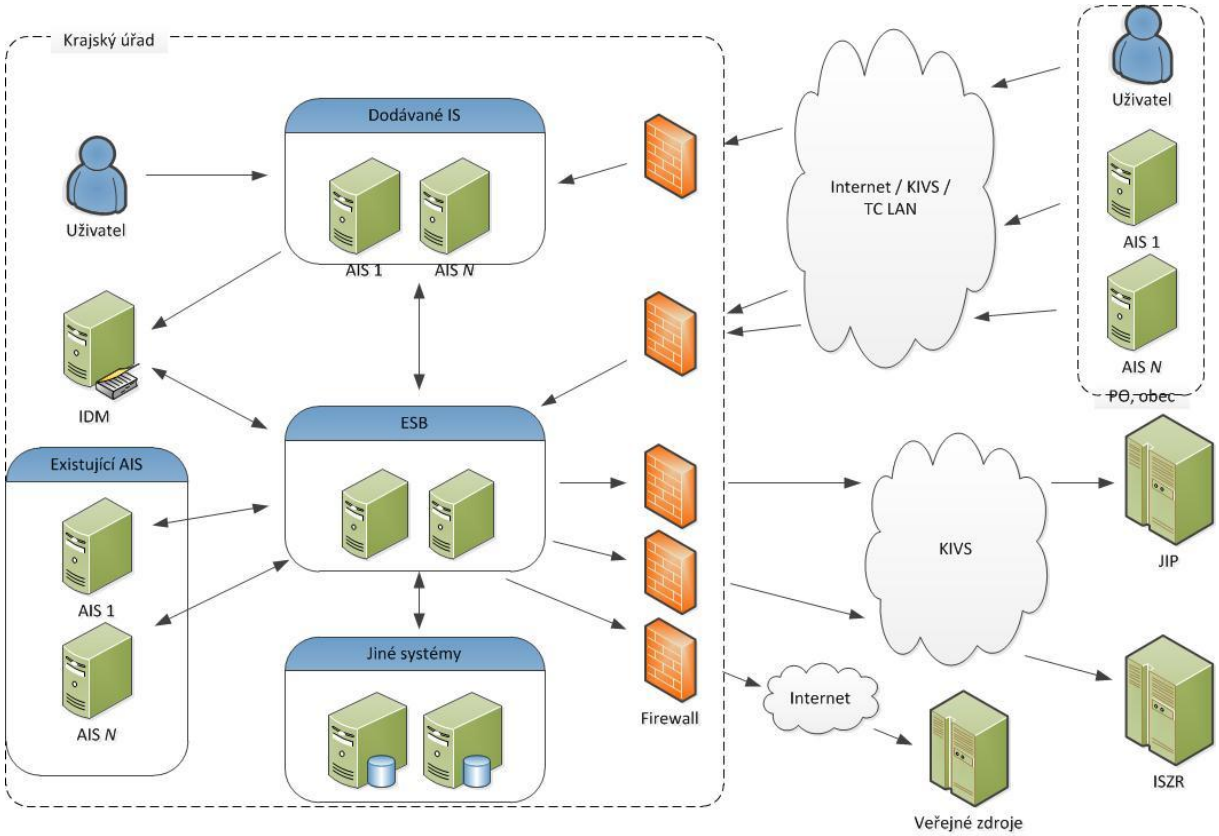
DETAIL NASAZENÍ

Aplikace eProxy bude dodána v rámci ESB jako přidaná funkcionalita. Vytvoří se tak jedno centrální místo pro přístup k ISZR pro celý systém JMK.

VYTVOŘENÍ INTEGRAČNÍCH BODŮ VŮČI STÁVAJÍCÍMU SYSTÉMU OBJEDNATELE

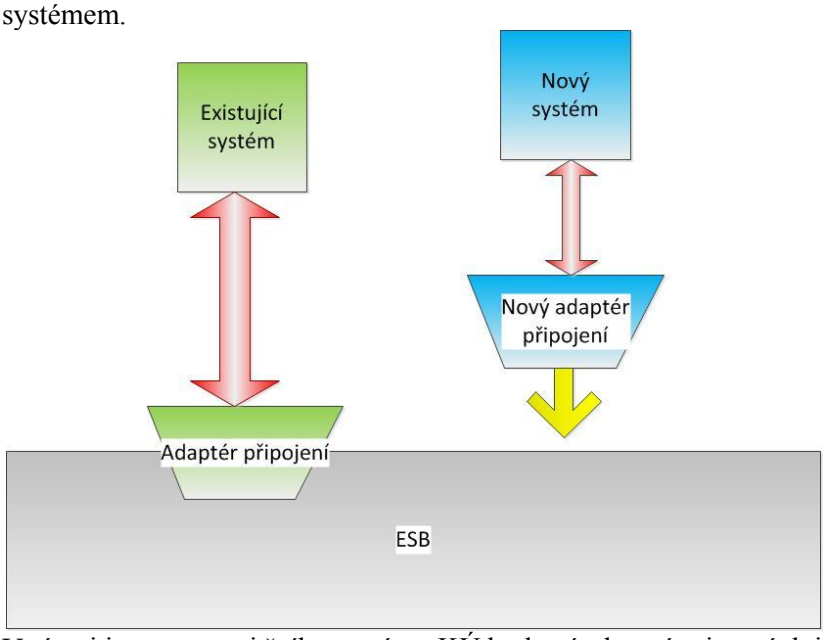
Vnitřní integrace systému krajského úřadu je navržena podle moderních postupů. Navržený způsob integrace umožní připojit libovolný počet jiných systémů Objednatele s ohledem na výkonnost TC. V době analýzy budou upřesněny technologie, kterými bude možné propojit jednotlivé Agendové systémy. Již v této době víme, že protokoly budou technologie JMS, HTTP/HTTPS, WS, FILE, FTP, JCA. V té době také budou analyzovány business procesy a funkce, které budou nutné pro integraci jednotlivých systémů tak, aby ulehčili agendu úřadu.
Integrace systému JMK bude vedena centrálně přes vrstvu ESB, která je pro integraci nejvhodnější. Vrstva umožní úřadu následující funkce, které v budoucnu úřad využije:

- Monitorování a řízení výměny zpráv jednotlivých napojených systémů
- Vyřešit komunikační problémy jednotlivých systémů
- Dopsání adaptérů na systémy 3. stran
- Odstranit duplicitní služby
- Kontrolovat nasazení a verzování služeb
- Orchestrovat propojení a postup vyhodnocení a volání integračních služeb
- Mapovat zprávy na jiné
- Nastavit bezpečnost integrace
- Logování a audit provozu
- Efektivnější získávání dat
- Audit jednotlivých operací
- Centrální monitoring integrace
- Globální zpracování chybových stavů, skrz celý systém integrace



Obrázek – Návrh integrace systému Objednatele

Integrace nově implementovaných systémů v rámci plnění veřejné zakázky
Integrační platforma ESB je navržena tak, aby bylo možné dopsání nového adaptéru a připojení nových systémů do integrovaného systému Objednatele. Postup připojení bude probíhat prvně analytickou fází a pak implementační a zakončí testovací fází. Integrace nových systémů se nebude lišit od integrace stávajících systémů. Výhodou ovšem bude lepší provázanost a využití již existujících služeb na integrační vrstvě. U nově dodávaných systému nebude nutné dopisovat speciální adaptéry na napojení. Při vývoji nových systému se zohlední to, že budou připojeny na integrační vrstvu. Tím se těsněji sváže adaptér připojení se systémem.

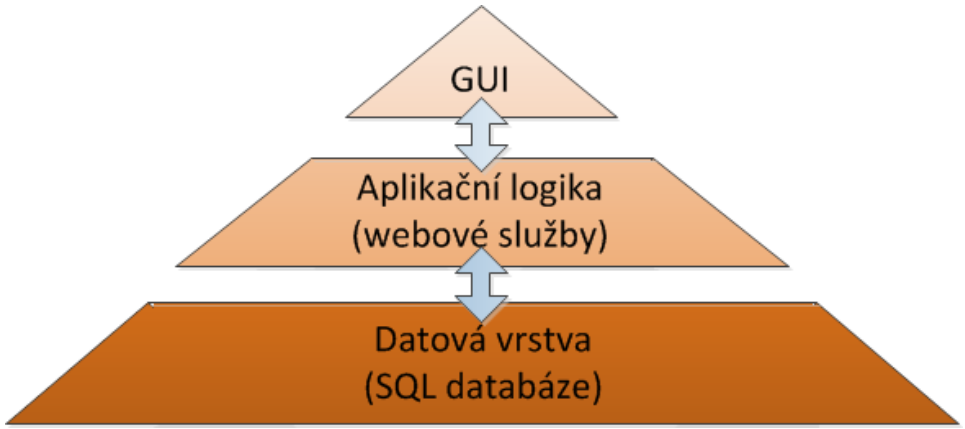


V rámci integrace vnitřního systému KÚ bude návrh a vývoj nových informačních systémů veden s ohledem na integraci do celkového systému. Bude se postupovat tak, aby byl problém řešen v rámci celého systému a nebyl řešen pouze pro danou malou oblast.

Integrace vnitřního systému krajského úřadu

Systém správy identit (Identity and Access Management)
Systém IDM je navržen a bude tvořen jako aplikace na zakázku pomocí vlastního vývoje. Bude vytvořen jako tenký (webový) klient, pomocí kterého bude umožněna správa ostatních identit ostatních IS. Veškerá komunikace bude prostřednictvím služeb nad zabezpečeným protokolem https.
Systém IDM, který nabízí společnost AutoCont a.s., je z pohledu architektury a řešení založen na jednoduchém principu, kterým je integrace různých systémů, založená na obecném, moderním principu třívrstvé architektury, kde střední vrstva je řešena pomocí SOA (Service Oriented Architecture). Pro komunikaci IDM s jednotlivými systémy AD bude využito komunikace pomocí protokolu LDAP.
Toto řešení je efektivní, výkonná platforma vhodná jak pro IDM samotné, tak i pro integraci různých, na sobě nezávislých systémů. Pro komunikaci mezi IDM a jednotlivými Active directory bude využito nativní komunikace pomocí LDAP protokolu.
Tomuto řešení se říká třívrstvá architektura, kde jednotlivé vrstvy jsou definovány svou funkcionalitou a zodpovědností:

- Prezentační vrstva – GUI rozhraní pro uživatele nejčastěji tvořené formuláři. V systému IDM bude tvořeno jako webový klient.
- Aplikační vrstva – obsahuje logiku aplikace, webové služby, komunikace IDM a AD, IDM a ostatních IS
- Datová vrstva – databáze, AD úložiště. Zodpovídá za konzistenci dat.

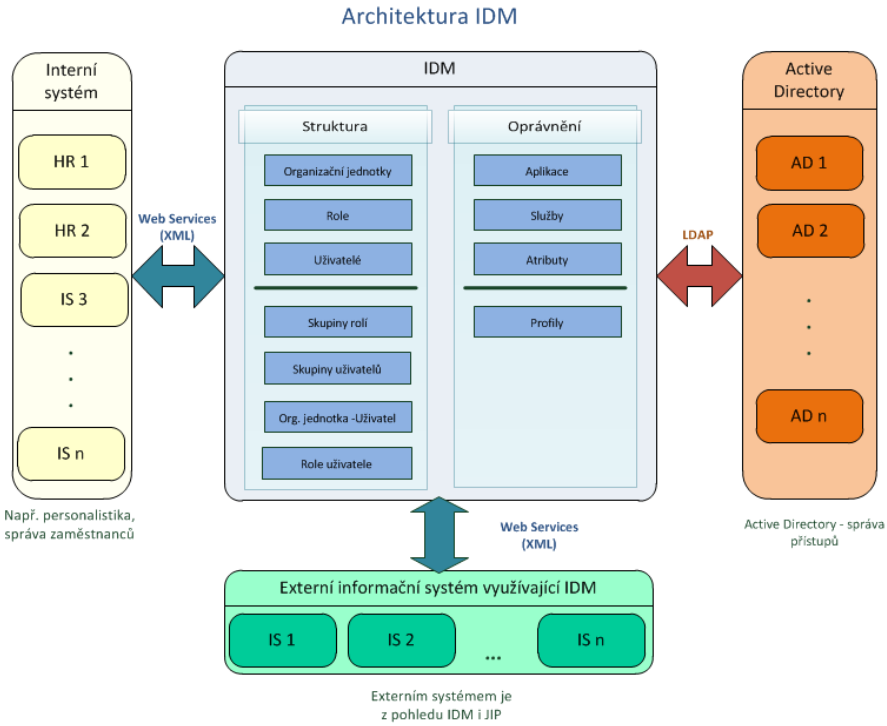


Obrázek 1 - Schéma třívrstvé architektury

Touto architekturou řešení bude dosaženo následujících funkcionalit a cílů:

- Uživatelské rozhraní, sloužící pro usnadnění správy IDM, AD a pro definované výstupy. Nejčastěji je tvořeno formuláři.
- Snadná a jednoznačně definovaná správa dat pomocí přesně popsaných služeb a struktur.
- Využití existujících služeb (znovu použitelnost – re use).
- Sdílení a kompozice existujících služeb do různých skupin, celků (agregace služeb).
- Otevřenost pro nové aplikace snadným doplněním potřebných rozhraní bez nutnosti testování již existujících částí
- Možnost sdílení stejných dat v celém systému (např. správa zaměstnanců, uživatelů, organizačních jednotek).
- Nastavení oprávnění přístupu k jednotlivým službám v katalogu služeb

IDM bude vytvořeno jako webové rozhraní, které bude integrovat informační systémy, které jsou z pohledu Objednatele interními, externími. Umístění IDM je znázorněno v následujícím schématu.



Obrázek 2 – Schéma nasazení systému IDM

NÁVRH ZPŮSOBU POUŽÍVÁNÍ IDM:

a) návrh jmenné konvence uživatelských jmen pro interní i externí uživatele a zajištění jejich unikátnosti (i s ohledem na identitní prostor veřejné správy - JIP)

Návrh jmenné konvence uživatelských jmen bude řešen v průběhu analýzy. Pro toto řešení bude vytvořeno doporučení, které bude využito v rámci jejich generování. Tyto uživatelská jména (loginy) bude systém IDM umožňovat změnit na jinou hodnotu. Konečný algoritmus generování bude potvrzen Objednatelem jako primární požadavek na analýzu správy uživatelů. Jednou z možností je například generovat uživatelské jméno jako Příjmení s prefixem E, I, J (uživatel externí, interní, JIP).

b) stanovení principu zajištění jednoznačných identifikátorů identit pro replikace s ostatními IS (včetně centrálního JIPu)

Tento bod souvisí s předchozím odstavcem. Zhotovitel provede analýzu požadavků jak vzhledem k interním a externím uživatelům, tak i k jejich jednoznačnosti v rámci JIPu. Zhotovitel po analýze provede detailní návrh GUI a případně algoritmu pro generování identifikátorů identit tak, aby byl pro administrátory co nejvíce uživatelsky přívětivý. Zhotovitel předpokládá součinnost s Objednatelem.

c) mechanizmus přidělení hesla identitě (nově vytvořené, při ztrátě hesla)

Postup při vytvoření nového hesla je shodný s přidělením hesla identitě po jeho ztrátě.

Založení identity:
IDM provede vytvoření identity a vygenerování prvotního hesla. Prvotní heslo bude nastaveno na default hodnotu, kterou může administrátor změnit. Po potvrzení administrátorem služba pro založení nové identity nastaví příznak pro povinnou změnu hesla při prvním přihlášení do systému. V rámci založení nové identity bude povinně vyplněna i e-mailová adresa identity. Po uložení identity systém odešle podle definovaného workflow přihlašovací údaje Login + Heslo.

Změna při ztrátě hesla:

Postup je shodný s tím, že administrátor obdrží žádost od uživatele pro nastavení nového hesla. Administrátor IDM bude mít v rámci svých oprávnění možnost nastavit systém tak, že může provádět generování nového hesla a jeho odesílání uživateli automaticky, okamžitě po odeslání žádosti uživatelem.

Akce bude logována.

d) mechanizmus změny hesla uživatelem

Změnu hesla smí provést pouze přihlášený uživatel. Tím je zajištěno, že své staré, původní, heslo zná. Pro změnu bude přesto vyžadováno staré, původní heslo, nové heslo a jeho verifikace. Systém provede změnu hesla a potvrdí tuto akci výpisem „Vaše heslo bylo úspěšně změněno.“. Další přihlášení k systému bude již pod novým heslem.

Akce bude logována.

e) stanovení atributů identit, které si může identita popř. pověřená osoba či organizace měnit sama

V rámci nastavení IDM bude mít administrátor právo nastavit jednotlivé atributy identity pro zápis, nebo čtení, případně lze provést jejich úplné skrytí pro uživatele. Systém provede u nové identity nastavení defaultních oprávnění.

NÁVRH PROCESŮ SPRÁVY UŽIVATELŮ (ZAVÁDĚNÍ, ZMĚNY, RUŠENÍ, NASTAVOVANÍ PRÁV, …) A ZPŮSOB INTEGRACE IDM

Proces správy uživatelů je z velké části v kompetenci administrátora. Uvedená funkcionalita a její popis, je v následující tabulce.

Služba	Popis	Povoleno pro roli
Nový uživatel	Založení záznamu uživatele v systému. Uživateli je přidělen mimo jiné i Login, Heslo, E-mail a příznak prvotního hesla	Administrátor
Změna uživatelů	Změna atributů libovolného uživatele v rámci své a podřízených domén.	Administrátor
Změna svého záznamu	Změna atributů aktuálně přihlášeného uživatele (heslo, jméno, příjmení).	Uživatel
Nastavení přístupných aplikací	Výběr aplikací ze seznamu.	Administrátor
Nastavení práv / rolí	Výběr role ze seznamu rolí	Administrátor
Pozastavení uživatele	Nastavení příznaku pozastaven pro vybraného uživatele (stav x datum od-do)	Administrátor
Zrušení uživatele	Logické zrušení uživatele. Uživatel se chová, jako by v systému nebyl.	Administrátor
Odstranění uživatele	Fyzický výmaz záznamu uživatele z AD	Administrátor
Odeslání žádosti o zpřístupnění nové role, aplikace	Odeslání žádosti o změnu mailem na administrátora IDM	Uživatel

Tabulka 3 - Správa uživatelů - služby IDM

Integrace IDM do systémů kraje Liberec předpokládáme jako postupné začleňování dalších externích systémů, které se budou postupně integrovat. IDM umožní integraci s více AD, pomocí konfiguračních dat, které bude moct nastavit oprávněný uživatel. Tím bude umožněna práce nad interními i externími AD (po provedení bezpečnostní studie a potřebných zabezpečených prostupech).

NÁVRH ČLENĚNÍ OBJEKTŮ V RÁMCI IDM PRO INTERNÍ I EXTERNÍ SUBJEKTY

Struktura IDM a AD bude z pohledu dodávaného systému navržena tak, aby umožňovala logicky stejnou funkcionalitu jak v IDM tak i v AD. Tím bude zajištěna replikace dat z IDM do AD, ale i naopak. Struktury služeb IDM pak budou vyhovovat jednak strukturám používaným v AD, tak i v IDM.
IDM bude respektovat požadavky na organizační strukturu a role, uživatele apod. Návrh členění objektů, jmenné konvence, struktury a vazby budou předmětem analýzy. Již nyní je ale zřejmé, že systém IDM bude z velké části omezen strukturou a požadavky zejména na AD.

Jelikož jedním z hlavních přínosů IDM je integrace různých AD (interní, externí) bude IDM navržen tak, aby plně pokryl požadavky na jednoduchou správu identit v rámci AD s tím, že IDM bude sloužit jako uživatelsky přívětivé rozhraní s poměrně širokými možnostmi pro správu všech integrovaných systémů Objednatele (HR, systémy třetích stran, AD,…).
Z pohledu členění struktur na externí a interní se v současné fázi návrhu jeví IDM řešit jako dva stromy, kde jeden root objekt je pro interní objekty a druhý pro externí. Konečné řešení bude ale navrženo po důkladné analýze současného nasazení informačních systémů v prostředí Objednatele s ohledem na požadavky integrací externích IS do IDM.

NÁVRH NEJVHODNĚJŠÍHO ZPŮSOBU IDENTIFIKACE, AUTENTIZACE A AUTORIZACE INTERNÍCH I EXTERNÍCH UŽIVATELŮ DO IS

Autentizace bude opět předmětem analýzy požadavků Objednatele. Z pohledu správy a požadavků bude minimálně v kombinaci uživatelské jméno + heslo. Pro některé aplikace lze zvolit ještě možnost autentizace pomocí certifikátu. Z tohoto požadavku a je zřejmé, že IDM umožní vést seznam certifikátů ke každému uživateli. Další možnost je přihlášení se do systému pomocí identifikační karty.
Vhodnost použití typu autentizace bude analyzována a navržena pro každý integrovaný systém a bude součástí dílčí akceptace dané etapy, případně zahájení vývoje dané integrační platformy, systému.
Identifikace bude nejčastěji prostřednictvím uživatelského jména. Pomocí tohoto jedinečného klíče, který bude použit k vyhledání reference na identitu zaměstnance, budou doplněny nacionále (Jméno + příjmení, případně další) ze systémů HR.
Autorizace je krok, který následuje bezprostředně po autentizaci. Autorizace slouží k získání přístupových práv k určitým funkcionalitám. V systémech AD je autorizace vyjádřena pomocí rolí a jejich přiřazení autentizovanému uživateli.

NÁVRH VHODNÝCH UŽIVATELSKÝCH ROLÍ PRO PŘÍSTUP DO JEDNOTLIVÝCH IS A SPECIFIKACE JEJICH OPRÁVNĚNÍ

Seznam rolí bude jednoznačně definován až v průběhu analýzy integrovaných systému (AD - interní, externí, systémy třetích stran…). Ve většině systémů ale platí, že obsahují minimálně následující role:

- Čtenář – uživatel s právem pouze číst vybrané data
- Editor – uživatel s právem měnit vybrané údaje. Editor dědí od role Čtenář.
- Administrátor – uživatel s právem administrovat systém. Administrátor nemá defaultně role čtenář, nebo editor.

Návrh integrace IDM s jednotným identitním prostorem veřejné správy (JIP)
Pro integraci JIPu do IDM bude využito služeb JIPu, které jsou popsány v dané dokumentaci. Zhotovitel bude poskytovat integraci JIPu v rozsahu aktualizace identit jak v rámci IDM, tak jejich následného promítnutí do JIPu samotného.
Samotná struktura ukládaných dat, způsob integrace (struktura rozhraní) bude součástí analýzy tohoto požadavku, který úzce souvisí s předpokládanou integrací základních registrů včetně registru práv a povinností RPP.

NÁVRH INTEGRACE IDM SE INFORMAČNÍM SYSTÉMEM ZÁKLADNÍCH REGISTRŮ (ISZR), ZEJMÉNA S REGISTREM PRÁV A POVINNOSTÍ (RPP)

Integrace s RPP bude provedena pomocí služeb, které registr RPP nabízí. Zhotovitel, je tvůrcem IS ISZR a proto je v této oblasti schopen poskytnou patřičné znalosti a doporučení jednak jak tento požadavek řešit s ohledem na jeho důležitost pro celkovou bezpečnost přístupu k datům základních registrů.

Správa uživatelů a řízení oprávnění v IS

IDM umožní udržovat identity a organizační strukturu ve své vnitřní databázi. Tyto identity ve vnitřní databázi budou sloužit jako referenční data/identity pro ostatní vnitřní i vnější informační systémy, se kterými komunikuje KÚ

Pro perzistenci dat vlastního IDM bude použita SQL databáze. IDM bude sloužit jako rozhraní pro možnou integraci systémů třetích stran do prostředí kraje JMK. Každý záznam bude obsahovat jedinečný GUID v rámci celého IDM, který bude integrovaným systémům sloužit jako referenční odkaz. Tím bude omezena duplicita dat. Ostatní systémy si mohou, pomocí služeb poskytnutých IDM, požadované údaje stáhnout k sobě, přesto bude za primární zdroj dat považována DB IDM, případně AD.

IDM UMOŽNÍ UDRŽOVAT A SPRAVOVAT KOMPLETNÍ ŽIVOTNÍ CYKLUS IDENTITY ZAMĚSTNANCE

IS IDM bude jednak udržovat kompletní životní cyklus identity uživatele, od založení až do jeho zrušení a to včetně jeho plné historizace změn. Systém IDM umožní prohlížení této historie změn včetně uživatele, který změnu provedl a času, kdy byla změna provedena (více v popisu historie záznamů).

IDM umožní práci s min. 5000 identitami na úrovni fyzických osob, s min. 4000 identitami (min 3000 aktivních a 1000 neaktivních), na úrovni funkcí (funkčních míst, rolí), min. 1000 identitami na úrovni organizací a min. 20ti připojenými informačními systémy

5000 identitami na úrovni fyzických osob
4000 identitami (min 3000 aktivních a 1000 neaktivních), na úrovni funkcí (funkčních míst, rolí)
1000 identitami na úrovni organizací
20 připojených informačních systémů

Pro systém IDM nebude omezující množství záznamů pro jednotlivé požadavky. Systém umožní správu osob (uživatelů), rolí (role, činnosti), organizace a funkční místa (organizační struktura) a externí IS (integrované systémy) tak, aby jejich správa z pohledu odpovědných uživatelů IDM (AD) byla co nejjednodušší. Pro cílový stav není důležité, zda bude například organizací 1000 nebo 2000, ale to, zda bude správně navržena struktura uložení dat (organizační strom) a způsob navržení operací nad touto množinou záznamů. Tyto funkcionality jsou zcela zásadní a budou podrobeny důkladné analýze jak z pohledu množství záznamů, tak především z pohledu vnitřních vazeb (kdo, kde, co).

V rámci IDM bude správa výše uvedených entit provedena jako samostatná část správy systému IDM. Pro tuto část bude potřeba oprávnění na úrovni Administrátor IDM. Bude vytvořena možnost importu rolí, funkci a organizaci z jiných (externích systémů) pomocí definovaných rozhraní. Struktura rozhraní bude předmětem analýzy požadovaných struktur systému IDM ale i ostatních integrovaných systémů. Systém IDM umožní plnění jednotlivých entit pomocí webových služeb, ale i souborů různých struktur a typů (txt, csv).

IDM UMOŽNÍ ZOBRAZENÍ IDENTIT VE STROMOVÉ (ORGANIZAČNÍ) STRUKTUŘE

Pro správu vybraných identit bude systém IDM umožňovat správu v rámci stromové struktury, která je z pohledu integrace do AD stěžejní. Systém, v případě, že bude analýzou požadováno, umožní zařadit nové nadřízené uzly a to včetně top-level úrovně (root - nemá nadřízený uzel), tak i přesun celých uzlů pod jiný rodičovský záznam (externí organizace se stane interní a naopak).

Seznam předpokládaných služeb pro správu stromové struktury je obsažen v následující tabulce. Veškeré služby budou přístupné pouze pro privilegované uživatele. Pro tuto část IDM předpokládáme roli administrátor, ale lze definovat i speciální roli administrátor organizační struktury:

Služba	Popis
Založení nového root záznamu	Založení organizační složky, která je root identitou.
Založení nového podřízeného záznamu	Založení organizační složky, která je podřízeným záznamem.
Změna záznamu	Změna vybraných atributů identity, nastavení globálních pravidel pro daný záznam. Tato pravidla jsou platná pro všechny podřízené, pokud u nich není uvedeno jinak.
Odstranění záznamu	Odstranění vybrané identity. Lze definovat například, že odstranit lze pouze záznam, který nemá podřízené záznamy. Pravidlo bude specifikováno po analýze požadavků Objednatele.
Přesun záznamu	Přesun záznamu a jeho podřízené struktury pod jiný rodičovský záznam. Spolu s tímto záznamem se provede přesun všech podřízených záznamů.

Tabulka 4 - Služby pro správu stromové struktury

IDM UMOŽNÍ PRÁCI S VÍCE STROMOVÝMI STRUKTURAMI (NAPŘ. INTERNÍ, EXTERNÍ, PŘÍSPĚVKOVÉ ORGANIZACE, OBCE) A VZÁJEMNÝMI RELACEMI OBJEKTŮ

Jak bylo uvedeno v předchozím bodě, bude umožněno v rámci správy organizační struktury vytvořit libovolný počet root záznamů. Relace mezi jednotlivými objekty budou opět umožněny pomocí administrátorských nástrojů. Touto funkcionalitou bude pokryt i požadavek na práci s více stromovými strukturami, kde v každém stromu lze definovat různou část IDM a například i vazbu této části (stromu) na jiné AD tak, jak bude požadováno administrátorem. Seznam služeb pro správu struktur je uveden v tabulce Tabulka 4 - Služby pro správu stromové struktury.
Vzájemné relace mezi různými strukturami (stromy) budou předmětem analýzy požadavků Objednatele. Tato funkcionalita totiž umožní z oddělených stromových struktur získat vazbu m:n, tedy obecně možnost mapovat každý záznam stromu A na jakýkoli jiný záznam ostatních stromů. Pro tuto funkcionalitu je vhodné důkladně zvážit, kde ji použít. Například lze ji využít u mapování uživatele do různých organizací a jejich rolí (zaměstnanec úřadu má roli admin v n externích organizacích), ale již nemusí být vhodná pro mapování různých organizačních struktur.

IDM UMOŽNÍ SPRÁVU UŽIVATELSKÝCH CERTIFIKÁTŮ V MS ACTIVE DIRECTORY (AD)

IDM povede pro uživatele seznam jeho certifikátů a příznak platnosti certifikátu, případně i datum platnosti Od-Do, které je uvedeno v daném certifikátu. Systém umožní validaci uživatele na jeho seznam certifikátů a provede kontrolu, zda je jeho certifikát, pomocí kterého přistupuje k vybrané části platný.

IDM UMOŽNÍ SPRÁVU UŽIVATELSKÝCH ROLÍ (ZAŘAZENÍ UŽIVATELE DO ODPOVÍDAJÍCÍ ROLE V DANÉM IS)

IDM umožní v rámci správy uživatelů jeho přiřazení administrátorem do vybraných rolí. Role samotné budou do IDM importovány spolu s novým systémem, který bude doplněn mezi již existující. Pořizování a změnu rolí v rámci samotného IDM nepředpokládáme, pokud nebude analýzou požadováno jinak. Role budou často řešeny jako enumerace, pokud nebude analýzou zjištěna potřeba správy rolí, pro každý IS. Rolím v IDM budou přidělována práva. Jaká práva bude předmětem analýzy v závislosti na cílové aplikaci. Administrátor IDM pak pouze přidělí uživatele k jednotlivým rolím.

IDM UMOŽNÍ IMPORT ROLÍ Z JIP/KAAS A ZPĚTNÝ EXPORT PŘIDĚLENÝCH VAZEB DO JIP/KAAS

IDM umožní import a export rolí z a do JIP / KAAS pomocí webových služeb. Struktura předávaných dat a bude předmětem analýzy a bude vycházet z předpisů JIPu. Stejné omezující podmínky struktur budou jak pro import z JIPu, tak i pro export IDM do JIPu.

IDM UMOŽNÍ REGISTRACI APLIKACÍ A JEJICH ROLÍ

IDM pomocí svého rozhraní umožní registraci jak jednotlivých aplikací, tak i jejich rolí. Zároveň bude umožněna aktualizace těchto rolí ve smyslu dohrání nových rolí. Role budou řešeny jako enumerace. Pro tuto službu bude možnost jak pořízení nové aplikace a jejich služeb pomocí rozhraní IDM pro správu této části, tak i možnost nahrát dané záznamy z vyexportovaných souborů. Typ a struktura souborů budou předmětem analýzy, ale předpokládáme import z txt, csv, xml struktur.

IDM UMOŽNÍ DYNAMICKOU AKTUALIZACI ROLÍ, TZN. NAČTENÍ ROLÍ Z IS, KTERÉ BUDOU NABÍZET NA VÝSTUPU SVÉ ROLE (NAPŘ. POMOCÍ DB VIEW, TABULKY, WS)

IDM umožní aktualizaci rolí z IS, které má již ve své správě. Tento požadavek je částečně zodpovězen v předchozím bodu. IDM umožní pomocí svého rozhraní import rolí do své databáze.
V průběhu analýzy bude definován seznam integrovaných IS třetích stran. Pokud bude Objednatel požadovat, může IDM poskytnou rozhraní pro správu rolí pro každý IS samostatně. Tento postup ale nedoporučujeme. IDM by mělo ve vztahu k ostatním IS vystupovat jako centrální uzel zodpovědný za správu identit, které jsou z pohledu chodu aplikací jednou z nejdůležitějších částí. Z tohoto důvodu by IDM mělo poskytovat jedno univerzální, kompaktní, rozhraní pro import rolí napříč všemi systémy.
Každý systém, který bude do IDM připojen, musí toto rozhraní implementovat. Tím bude dosaženo vysoké odolnosti proti případným atakům. Pokud bude pro každý systém různé rozhraní, vzroste složitost údržby a tím i případná možnost chyb.
Nové role budou importovány z třetích systémů a IDM bude pouze v roli pasivního systému.

IDM UMOŽNÍ SPRÁVU ČLENSTVÍ V AD SKUPINÁCH (STATICKÉ I DYNAMICKÉ ZAČLEŇOVÁNÍ DO SKUPIN PODLE RŮZNÝCH HODNOT ATRIBUTŮ NAPŘ. ODBOR UŽIVATELE NEBO ZAŘAZENÍ DO VEDOUCÍCH FUNKCÍ)

IDM umožní správu v rámci jednotlivých skupin. V rámci IDM bude povolena správa členství ve skupině jak pomocí ručního vkládání do skupiny, kterou si můžete vybrat, tak i dynamické začlenění do skupiny podle atributů definujících danou skupiny. Systém IDM, jeho vstupní služby, podle těchto atributů rozpozná cílovou skupinu a do této skupiny daného uživatele automaticky přiřadí.

IDM UMOŽNÍ OBOUSMĚRNOU SYNCHRONIZACI DAT TZN. JAK Z IDM DO IS (NAPŘ. UŽIVATELE A JEJICH ATRIBUTY), TAK Z IS DO IDM (NAPŘ. ROLE IS, DO KTERÝCH JE MOŽNÉ UŽIVATELE ZAŘAZOVAT)

IDM poskytne služby jak pro naplnění vlastních struktur, tak i pro jejich poskytnutí třetím stranám. Pro tyto služby bude vyžadován zabezpečený přístup ověřených uživatelů. Předpokládáme, že služba IDM pro export bude nabízet jak plný seznam, tak i přírůstek od zadaného data. Seznam služeb bude dán analýzou požadavků, ale pro naplnění tohoto bodu bude obsahovat minimálně služby pro:

- Role
- Organizační strukturu
- Uživatele včetně povolených rolí a zařazení do organizačních struktur

IDM UMOŽNÍ VSTUPNĚ/VÝSTUPNÍ OPERACE POMOCÍ VŠECH TĚCHTO ROZHRANÍ:

- databázová tabulka, view (MS SQL, Oracle)
- webová služba SOAP
- CSV textový soubor
- XML struktura (soubor)
- LDAP v3

Pro veškeré přístupy k datům bude vyžadován zabezpečený SSL přístup. Veškeré operace budou logovány minimálně v rozsahu kdo, kdy a co. IDM bude umožňovat vstupně / výstupní operace pomocí těchto rozhraní:

- Databázová tabulka, view (MS SQL, Oracle) – tyto operace budou povoleny v minimální míře. Naprostá většina přístupu k datům IDM bude řešena jiným typem přenosu dat. Pro externí subjekty (IS, Agendy) bude tato možnost povolena pouze po důkladné analýze požadavků a pod DB uživatelem s právem SELECT, EXECUTION (GRANT SELECT, EXECUTION …), kde procedury budou umístěny v samostatném package.
- Webová služba WS pod protokolem SOAP – standartní rozhraní IDM pro přenos dat mezi IDM a jinými IS. Pro volání této služby bude vyžadována šifrovaná komunikace a autentizace uživatele.
- CSV textový soubor – IDM umožní import / export dat z csv souborů. Soubor bude uložen na předem daný adresář pomocí zabezpečených protokolů. Pro import dat z těchto zdrojů bude vytvořena služba. Pro volání této služby bude vyžadována šifrovaná komunikace a autentizace uživatele.
- XML struktura – IDM umožní stejnou funkcionalitu jako v předchozím bodě
- LDAP v3 – umožní přístup k datům uloženým v AD a jejich přenos do IDM.

IDM UMOŽNÍ DEFINOVÁNÍ VLASTNÍCH ATRIBUTŮ K IDENTITÁM A JEJICH PUBLIKACI EXTERNÍM APLIKACÍM PŘES DATOVÉ ROZHRANÍ

Pomocí uživatelského rozhraní bude umožněno definovat vlastní atributy, typ atributu a jejich hodnoty. Jejich export (publikace) bude umožněn pomocí webových služeb ve formátu XML.

IDM UMOŽNÍ AUTONOMNÍ SPRÁVU HESEL FORMOU ROZHRANÍ NAD AD

IDM umožní pomocí rozhraní autonomní správu hesel a jejich propagaci do AD včetně příznaku prvotního nastavení a délky platnosti hesla. Správu hesel bude mít umožněnu uživatel s rolí Administrátor. Běžný uživatel si může změnit pouze vlastní heslo. Pro změnu bude použit standartní formulář, kde musí zadat Původní heslo, Nové heslo a Verifikaci nového hesla.

PODPORA SPRÁVY ROLÍ A OPRÁVNĚNÍ NEZBYTNÝCH PRO KOMUNIKACI S RPP (MATICE AGEND, ČINNOSTÍ, FUNKČNÍCH MÍST A OSOB)

Integrace s RPP bude provedena pomocí služeb, které registr RPP nabízí. Zhotovitel, je tvůrcem IS ISZR a proto je v této oblasti schopen poskytnou patřičné znalosti a doporučení jednak jak tento požadavek řešit s ohledem na jeho důležitost pro celkovou bezpečnost přístupu k datům základních registrů. Systém IDM bude podporovat správu agend, činností a osob tak, aby byla pokryta komunikace s RPP.

Přehled povinných úloh, jejichž realizace bude předmětem implementace řešení
Celková funkcionalita, struktury dat a rozsah poskytnutých služeb bude dán analýzou požadavků Objednatele. Pro veškeré povinné úlohy v IDM se předpokládá historie změn záznamů v rozsahu kdo, kdy a co změnil (stará a nová hodnota), mimo hodnot hesel. Seznam služeb, pokud je uveden v tabulkách, je pouze orientační a vychází ze zkušeností Zhotovitele, které má z dřívějších návrhů již dodaných IS. Popis funkcionalit je pouze informativní a opět bude nutné projít analýzou požadavků na každý konkrétní systém (bod nabídky).

IDM UMOŽNÍ SPRÁVU UŽIVATELŮ V MS ACTIVE DIRECTORY 2008 A TO PŘEDEVŠÍM:

- založení uživatele
- změnu atributů u uživatele
- zrušení uživatele
- správu certifikátů uživatele

V rámci IDM budou k dispozici funkcionality, které se pomocí uživatelského rozhraní a volání střední vrstvy služeb zpropagují jednak do IDM (databáze SQL), tak i do daného AD.

IDM UMOŽNÍ SPRÁVU MAILBOXŮ V MS EXCHANGE 2010 A TO PŘEDEVŠÍM:

- založení mailboxu uživatele
- zrušení mailboxu uživatele

Služba	Popis	Povoleno pro roli
Založení uživatele	Založení záznamu uživatele v systému. Uživateli je přidělen mimo jiné i Login, Heslo, E-Mail a příznak prvotního hesla	Administrátor
Změna uživatele	Změna atributů libovolného uživatele.	Administrátor
Zneplatnění uživatele	Zneplatní uživatele v AD	Administrátor
Zrušení uživatele	Zrušení uživatele v AD. Přesun jeho zodpovědností na jiného uživatele.	Administrátor
Správa certifikátů	Správa certifikátů a jejich přiřazení uživateli.	Administrátor
Změna hesla uživatele	Nastavení prvotního hesla a příznaku pro vynucenou změnu. Nastavení datumu expirace hesla.	Administrátor
Změna hesla uživatelem	Změna vlastního hesla	Uživatel
Odeslání žádosti o změnu zapomenutého hesla	Žádost a notifikace o změně hesla administrátorem	Administrátor/Uživatel
Založení mailboxu uživatele	Založení mailboxu uživatele – výběr DB, velikost mail boxu	Administrátor
Zrušení mailboxu uživatele	Zrušení mailboxu uživatele – výběr DB, velikost mail boxu.	Administrátor

Tabulka 5 - seznam funkcí pro správu uživatelů a jejich mail boxů

Systému IDM bude primárně tvořen na základě webových služeb. Pro správu uživatelů budou jednotlivé služby a jejich vstupně / výstupní struktury definovány tak, aby poskytly možnost opakovaného použití (re-use). Tím bude pokryt i požadavek na propagaci uživatelských změn do systémů třetích stran.

IDM UMOŽNÍ SPRÁVU UŽIVATELŮ V ERP GINIS VČETNĚ PŘÍPADNÝCH SUBZHOTOVITELSKÝCH ÚPRAV NA STRANĚ ERP SYSTÉMU GINIS (WEBOVÉ SLUŽBY PRO SPRÁVU UŽIVATELŮ)

- založení uživatele
- založení funkčního místa a nadefinování konkrétní konfigurační skupiny
- změna atributů u uživatele (např. změna odboru a z toho odpovídající změny v IS Ginis)
- zrušení uživatele včetně přesunu veškerých dokumentů, které jsou na daného uživatele navěšeny

Pro požadavek na tuto funkcionalitu bylo odpovězeno v předchozím bodu – znovu použitelnost služeb. Pro integraci ERP Ginis do IDM bude potřeba spolupráce třetí strany. Z pohledu vlastního IDM se nejedná o nový požadavek. Ten je již popsán v předchozím bodu. Pro požadavek v bodu d) bude využita funkcionalita systému Ginic, která umožňuje předání dokladů a zároveň eviduje historii vlastníků dokladu.

Portál IDM

Tato kapitola má za cíl navázat na předchozí části a doplnit je popis návrhu řešení IDM jako webového portálu pomocí tenkého klienta. Veškerý přístup bude pomocí zabezpečeného protokolu https.

WEBOVÝ PORTÁL, KTERÝ UMOŽNÍ SPRÁVU IDENTIT UŽIVATELŮ (INTERNÍCH I EXTERNÍCH) A JEJICH PŘÍPADNOU ŘÍZENOU NEBO NEŘÍZENOU ÚPRAVU, ZALOŽENÍ NEBO ZNEAKTIVNĚNÍ/SMAZÁNÍ

Pro správu jednotlivých identit uživatelů bude využito webových služeb a jejich mapování na navržené formuláře (dále GUI), které vzniknou pro aplikaci IDM. Návrh změn z pohledu toho, zda jde o změnu řízenou (schválená oprávněnou osobou), případně neřízenou změnu bude navržen po analýze požadavků Objednatele a jejich schválení Objednatelem. Řízená změna bude doplněna minimálně o stav schváleno k provedení (kdo a kdy schválil požadavek). Návrh workflow bude předmětem další analýzy. Jelikož se jedné o správu identit uživatelů, bude jeden administrátor požadavek zadávat a jiný, případně superadmin, schvalovat.

MOŽNOST DEFINOVÁNÍ WORKFLOW PRO UŽIVATELSKÉ ZMĚNY

Jedná se o požadavek, který duplikuje v logice předchozí odstavec. Rozdíl je pouze v tom, že zde se jedná o tok akcí uživatele. Na rozdíl od předchozího požadavku může jít o žádost běžným uživatelem (např. změna příjmení) a schválení adminem.

MOŽNOST ZMĚNY HESLA PRO EXTERNÍHO UŽIVATELE

mající účet v AD KrÚJMK (řízená změna tj. s povolením administrátora v rámci workflow nebo neřízená změna, kterou si uživatele provede kdykoliv samostatně). Pro provedení změny hesla externím uživatelem, bude Portál IDM umožňovat změnu ve dvou režimech. V prvním se provede změna hesla okamžitě po odeslání žádosti o změnu hesla a uživatel dostane on-line zprávu a výsledku změny „Heslo bylo x nebylo úspěšně změněno.“. V potvrzovacím režimu se tento požadavek rozpadne na dílčí části:

- Uživatel volá stránku pro změnu hesla
- Uživatel vyplní požadované údaje pro změnu hesla: současné heslo, nové heslo, verifikace nového hesla
- Uživatel odešle požadavek na změnu hesla
- Služba pro změnu hesla provede kontrolu, zda je Uživatel + Současné heslo platná kombinace a zda se nové heslo rovná verifikaci a současně odpovídá požadavkům na bezpečnost hesla (min. délka, obsah povolených znaků, apod.)
- Pokud bod 4 neprojde kontrolou, Portál IDM na chybu upozorní a opakuje od bodu 2
- Pokud bod 4 projde kontrolou, Portál IDM zapíše požadavek do databáze a zároveň zašle mail jak administrátorovi, tak potvrzující mail uživateli
- Administrátor se přihlásí na stránku Požadavky. Vybere požadavky na změnu hesla a požadavek Potvrdí x Zamítne. Systém provede požadovanou akci a odešle mail žádajícímu uživateli (Vaše heslo bylo změněno. Vaše heslo nebylo změněno – zamítnuto administrátorem.).
- Uživatel má, pokud je změna schválena, povolen přístup pod novým heslem.

VEŠKERÉ POŽADAVKY, KTERÉ PROVEDOU UŽIVATELÉ NA PORTÁLU IDM BUDOU HISTORIZOVÁNY A LOGOVÁNY, TAK, ABY BYLO MOŽNÉ ZPĚTNĚ PROKÁZAT KDO, KDY A CO ZMĚNIL V IDM IDENTITÁCH A ORGANIZAČNÍ STRUKTUŘE

Pro veškerou práci se záznamy v Portálu IDM se povede následující logování minimálně v tomto rozsahu:

- Plná historie změn záznamu
- Historie pokusů přihlášení uživatele na Portál IDM – kdo, kdy, odkud (IP adresa), stav (OK x ERR)
- Seznam navštívených stránek uživatelem – kdy, URL, odkud (systém), status (OK x ERR)

PODPORA FUNKCE SAMOOBSLUŽNÉ REGISTRACE NOVÝCH UŽIVATELŮ VČETNĚ MOŽNOSTI VÝBĚRU NÁVRHU OPRÁVNĚNÍ, NASTAVENÍ SCHVALOVACÍHO WORKFLOW VČETNĚ EMAILOVÝCH NOTIFIKACÍ A POTVRZOVÁNÍ (OCHRANA PROTI EXTERNÍM ÚTOKŮM)

Pro možnost žádosti nového uživatele o přístup do dané části IS bude mít Portál IDM možnost samoobslužné registrace uživatelů. Tato žádost bude pouze připravena pro následující odsouhlasení oprávněným uživatel (Administrátor IDM). Režim žádosti je popsán níže:

- Nový žadatel volá stránku pro přidání do IS IDM, AD
- Žadatel vyplní povinné údaje (Jméno, Příjmení, Osobní číslo, Telefon, soukromý E-mail Funkce, Adresa, Seznam požadovaných oprávnění, atd. - plný seznam bude předmětem podrobné analýzy)
- Žadatel odešle požadavek na registraci do systému
- Portál IDM provede kontrolu formuláře na úplnost a formální správnost nové žádosti
- Pokud bod 4 neprojde kontrolou Portál IDM na chyby upozorní a opakuje se od bodu 2 (údaje zůstávají vyplněny)
- Pokud bod 4 projde kontrolou, Portál IDM zapíše požadavek do databáze a zároveň zašle mail jak administrátorovi, tak potvrzující mail žadateli

- Administrátor se přihlásí na stránku Požadavky. Vybere požadavky na založení uživatele a požadavek doplní služební E-mail, upraví + Potvrdí x Zamítne. Systém provede, v případě Potvrzení, založení uživatele do AD.
- Systém odešle mail žádajícímu (Byl jste zaregistrován spolu s Otiskem nastavených hodnot Loginem a prvotním heslem x Nebyl jste zaregistrován).
- Uživatel má, pokud je žádost schválena, povolen přístup do daného systému.

Ochrana proti externím útokům bude řešena na více úrovních a bude řešena v rámci bezpečnostního auditu Portálu IDM. V nabídce je popsána pouze část z těchto kroků:

- Dotazy, data pro přístup do DB budou ošetřeny kontrolou na nebezpečné znaky, řetězce a to pomocí funkcí na odstranění, překlad těchto znaků
- Nastavením práv DB uživatelů pro přístup k záznamům. Služba bude přistupovat pod určitým uživatelem, který bude mít pouze omezená práva. Nebude mít např. práva na odstranění, založení tabulky, sloupce, indexu apod.
- Zabránění přímých dotazů do DB. Portál IDM bude navržen jako třívrstvá architektura a bude v maximální možné míře komunikovat prostřednictvím webových služeb
- Překlad nebezpečných slov v požadavcích na data – ve filtrech (insert, update, delete, drop, …)
- Portál IDM bude mít nastaven maximální počet dotazů za danou časovou jednotku (např. 5 dotazů z portálu za sekundu. Dotaz je ve smyslu volání URL stránky)
- Rozhraní na zařazení podezřelé IP adresy na černou listinu. Pokud bude IP adresa na tomto seznamu, budou veškeré přístupy z ní odmítány.
- Veškeré požadavky se budou logovat

PLNÁ LOKALIZACE PORTÁLU DO ČESKÉHO JAZYKA

Portál IDM dodávaný firmou AutoCont a.s. bude vyvíjen plně v českém jazyku. Veškerá dokumentace, popisy, nápověda, příručky se předpokládají v češtině.

Administrace IDM

MOŽNOST DEFINOVÁNÍ JEDNOTLIVÝCH ÚROVNÍ ADMINISTRÁTORSKÝCH OPRÁVNĚNÍ K IDENTITÁM A STROMOVÉ STRUKTUŘE.

IDM umožní definici oprávnění jak k identitám (objektům) tak i k různým úrovním organizační struktury. Tato funkcionalita bude poplatná v rámci celé aplikace IDM.

MOŽNOST KROKOVAT JEDNOTLIVÉ ÚLOHY IDM VČETNĚ ZOBRAZENÍ NÁHLEDU ZMĚN

Umožnění krokování úloh bude spojeno s některými dalšími funkcionalitami. Mezi těmito požadavky je:

- Vedení historie změn záznamu
- Umožnění work flow schvalování x zamítnutí
- Náhled neuložených změn

První bod může sloužit k náhledu na původní hodnoty. Work flow umožní některé změny zastavit, respektive zrušit. Náhled změn je z pohledu uložení dat do DB zcela jiný případ. V této fázi data ještě nejsou odeslána do DB. Tato funkcionalita bude doplněna tam, kde bude nezbytně nutná a po důkladné analýze požadavků.

IDM umožní nastavení, které zabrání hromadným změnám např. z důvodu chybných dat na vstupu (z personálního systému), tak aby nedošlo k hromadným nežádoucím změnám (např. smazání objektů v Active Directory). Tato funkcionalita umožní při větším počtu změn zastavit frontu změn a upozornit administrátora IDM mailem a zapsat tuto informaci do aplikačního logu serveru i do interního logu IDM. Tato vlastnost je poplatná pro všechny vstupně/výstupní konektory.

Pro nahrání dat pomocí batch dávek, případně spuštění hromadných importů administrátorem bude v rámci IDM defaultně postupováno v souladu s přístupem všechno nebo nic. Administrátor může změnit tento status na hodnotu pouze OK záznamy. V obou případech bude zapsána v případě zjištění chyby tato událost do

logů. Pouze v rámci prvního nastavení bude zápis pouze první chyby a dávka, zpracování, bude ukončeno. V druhém dojede zpracování do konce a OK záznamy budou uloženy. Chybné záznamy se odmítnou a v rámci logu budou reportovány k další analýze. Jelikož systémy podobné navrženému IDM jsou často IS, které musí být plně autonomní a data v nich konzistentní, bude ze strany Zhotovitele na požadavek ve smyslu jen OK požadován vždy potvrdit formou zápisu. Může se stát, že např. role se budou nahrávat ve smyslu jen OK a následně, v případě nenahraní role ABC všechny záznamy, které na ni vážou (např. uživatel, skupina uživatelů) budou systémem odmítnuty z důvodu neexistující role.

IDM UMOŽNÍ ALERTOVAT KONFLIKTNÍ STAVY POMOCÍ MAILU NA ADMINISTRÁTORY IDM A ZAPISOVAT DO APLIKAČNÍHO LOGU NA SERVERU I DO INTERNÍHO LOGU IDM.

Pro konfliktní stavy (chyby při ukládání dat, vytvoření účtu, který neodpovídá žádné roli) bude tato informace jednak logována a zároveň bude odeslán mail na definované adresy. Současně s tím bude v rámci Portálu IDM zobrazeno upozornění, například formou ikony v dané části obrazovky o tom, že v IDM došlo ke konfliktnímu stavu. Detailní popis bude zobrazen až v obrazovce k tomu určené.

IDM UMOŽNÍ LOGOVÁNÍ VEŠKERÝCH OPERACÍ NA VSTUPU A VÝSTUPU A UCHOVÁVÁ IMPORTNÍ DATA (DÁVKY) V ARCHIVU.

Pro zpracování vstupně výstupních operací (import x export dat) bude IDM poskytovat následující funkcionality:

- Archivace veškerých IN x OUT souborů s daty (název souboru, velikost souboru, datum a čas vytvoření souboru, zdrojový systém)
- Logování jednotlivých řádků souboru před vlastním importem do daného systému (např. AD)
- Logování veškerých WS a jejich struktur s daty, které budou určeny pro zápis do systému IDM, AD. Každý záznam, který bude importován do IS IDM bude mít jedinečný identifikátor z primárního systému (ID, Kód, GUID), který se v primárním systému nemění.
- Logování výstupních dat na úrovni kdo, komu (pokud je uvedeno), kdy a co (pokud jsou data exportována do externího souboru, je ukládán tento soubor před odesláním)

Pomocí těchto pravidel systém IDM neprovede automatické duplicitní nahrání dat. Data se stejným identifikátorem budou buď odmítnuta, nebo pouze změněna na nové hodnoty. Shodné soubory budou v případě opakovaného požadavku na zpracování odmítnuty.

IDM BUDE PODPOROVAT OCHRANU VYBRANÝCH KONTEJNERŮ AD (ZÁKAZ ZMĚN)

Systém IDM bude respektovat role a práva nastavená roli/uživateli v daném AD. Pokud tedy bude nastaveno omezení na daném AD například zákaz zápisu do vybraného kontejneru, bude toto nastavení propagováno až do IDM. Pokud přihlášený uživatel provede akci, která bude na AD zakázána, dostane zprávu o nepovoleném přístupu. V ostrém provozu by tuto akci vůbec neměl mít povolenu na IDM (např. neuvidí tlačítko Odeslat, nezobrazí se formulář apod.).

IDM UMOŽNÍ SLEDOVAT JEDNOTLIVÉ STAVY V PRŮBĚHU SYNCHRONIZACE

Synchronizace dat s ostatními systémy, které budou integrovány do IDM, bude probíhat jak pomocí dávkových služeb, tak v požadovaných oblastech v on-line režimu. Pro tyto služby budou využívány stavy záznamů, které budou popisovat synchronizaci – Běžící, Dokončená, Čekající na spuštění.
Flow jednotlivých synchronizací bude předmětem analýzy požadavků. V rámci této analýzy vznikne jak popis v BPM diagramu (pokud bude požadováno) tak i stavový diagram, pomocí kterého bude popsán přechod stavů synchronizací. Z tohoto diagramu pak bude provedeno mapování do samotné aplikace IDM, která umožní procházet, sledovat, synchronizace jak podle stavů, tak i podle časů spuštění, dokončení.

IDM BUDE UMOŽŇOVAT DATABÁZOVOU HISTORIZACI

Pro návrh IS IDM předpokládáme ukládání dat do SQL databáze. IDM bude pro vlastní běh využívat třívrstvou architekturu, kde veškeré logické operace budou provedeny na střední vrstvě. Tyto služby pak budou zapisovat jak nové, případně změněné údaje všech vybraných identit. Samotná historizace dat bude provedena pomocí dvou rozdílných způsobů:

- Historizace pomocí samotných WS – zápis dat z datových struktur
- Historizace pomocí databázových operací – triggerů

Rozhodnutí, kdy bude která možnost využita, bude vydáno až v průběhu tvorby vlastní aplikace IDM. Obě varianty ale provedou z pohledu historie dat, shodnou operaci, pomocí které uloží nové hodnoty záznamu do historické tabulky. V rámci procházení historie záznamu pak bude umožněno postupně procházet změny záznamu + kdo a kdy změnu provedl. Změněné hodnoty lze zobrazit například výrazně.
Jelikož bude IDM spolupracovat s aplikacemi třetích stran, bude muset s vysokou pravděpodobností řešit tzv. dvoufázový commit. Pro správnou funkcionalitu je potřeba provést úpravu i v rámci třetích stran. V prvním kroku je proveden tzv. "PREPARE COMMIT". Tím je uložena nová hodnota ve smyslu nepotvrzeno v cílovém IS (např. AD). Následně se volá služba třetího systému, která propaguje data do svého datového úložiště. Tato služba vrací status. Pokud je OK, pak se nastaví „PREPARE COMMIT" na "COMMIT". Pokud je ERR, pak se nastaví na "ROLLBACK", případně se data odstraní.
Je nutné poznamenat, že dvoufázový commit je časově náročnější operace.

Reporty a datové výstupy

Auditní reporty – přehled uživatelů a jejich rolí v IS napojených na IDM
Rozdílové reporty – atributové rozdíly mezi identitami uloženými v IDM a jednotlivých IS
ISZR reporty – identity synchronizované do JIP, KAAS a RPP.

Seznam reportů a jejich struktura budou součástí detailní analýzy požadavků zákazníka. V rámci Portálu IDM bude vytvořena speciální část pro přehledy s možností výstupu do souborů, případně k tisku. Tato oblast bude přístupná pro uživatele s danou rolí – Čtenář reportů.
Každý report bude mít vlastní možnost filtrování – například audit uživatelů za organizační strukturu, podle role, podle vybraného IS apod. Filtry budou opět analyzovány a nastaveny podle potřeb zákazníků.
Auditní reporty budou umožňovat pro jednotlivý IS integrované do IDM provést výpis všech identit (podle filtrů) a to jak z IDM, tak i z Integrovaného systému. To umožní provést kontrolu integrity dat mezi IDM (AD), a cílovým systémem (například HR). K této funkcionalitě bude potřeba na straně integrovaných systémů doplnit rozhraní pro získání dat z patřičných objektů. Pro tento požadavek bude nutné posoudit, zda je potřeba mít tuto možnost v on-line režimu, nebo stačí export dat z třetích systémů pouze 1x za 24 hodin.
Pro rozdílový report předpokládáme opět spolupráci třetích stran a to v rozsahu sjednocení vstupně výstupních struktur a shodné funkcionality dané služby.
ISZR reporty budou sloužit primárně k ověření aktuálního stavu v JIP, KAAS a RPP a jeho porovnání proti IDM.

Metodika vývoje v oblasti IDM

ETAPY VÝVOJE APLIKACE

Vývoj jednotlivých etap, jejich postupný vývoj a implementace, bude proveden v následujících krocích:

Sběr a analýza požadavků Objednatele

V této části provádí Zhotovitel zakázky sběr a analýzu požadavků Objednatele v rozsahu nutném k vybudování aplikace (IDM, Lokální registry). Seznam požadavků bude veden v analytickém nástroji Enterprise Architect, kde budou požadavky rozděleny na funkční a nefunkční a zároveň k nim bude doplněn návrh jejich řešení.

Analýza a návrh řešení požadavků pomocí případů užití

Návrh řešení požadavků je dalším krokem, který povede k sjednocení představy Objednatele a návrhu řešení. Cílem této části je zamezit chybnému řešení jednotlivých požadavků a dále provést sjednocení duplicitních, případně odstranění (po konzultaci) protichůdných požadavků na vyvíjenou aplikaci. Po této fázi bude zřejmé, co Objednatel konkrétně od aplikace očekává a zároveň mu bude předveden první návrh řešení systému.

Vznik modelu tříd, Model aktivit

Po prezentaci jednotlivých případů užití navrhované aplikace, která povede k odsouhlasení analyzovaných funkcionalit a uchovávaných údajů, bude provedena další etapa analýzy – návrh modelu tříd. V této části vznikne jak samotný diagram tříd, který je z pohledu konečného řešení stěžejní, ale v souvislosti s ním bude

vznikat i diagram stavů a pro vybrané části i diagram toku aktivit (požadavků na work flow vybraných činností). Po této části již bude jednoznačně definováno chování systému tak, aby mohl začít vývoj aplikace.

Návrh datového modelu

Na základě odsouhlasení této části vznikne návrh databázových struktur SQL databáze a to jednak tabulek a jejich polí, ale i návrh jejich vazeb, omezení a indexů. Zároveň bude provedena kontrola na integritu datových struktur a bezpečnosti dat v databázi uložených (šifrování na úrovni databáze).

Návrh služeb, GUI – zahájení vývoje

Jako další následuje návrh jednotlivých obrazovek pro vlastní práci s aplikací. Bude provedeno mapování jednotlivých tříd, jejich atributů na obrazovky (vstupně výstupní pole, seznamy) a přechody mezi obrazovkami navzájem. Objednateli bude před samotným vývojem předvedena část, která mu umožní aktivně vstoupit do připomínkování požadavků na funkcionalitu jednotlivých formulářů a flow mezi nimi. Tím budou minimalizovány pozdější požadavky na změny, které přináší navyšování pracností. Po akceptaci dílčích částí bude zahájeno samotné programování.

Testování etapy

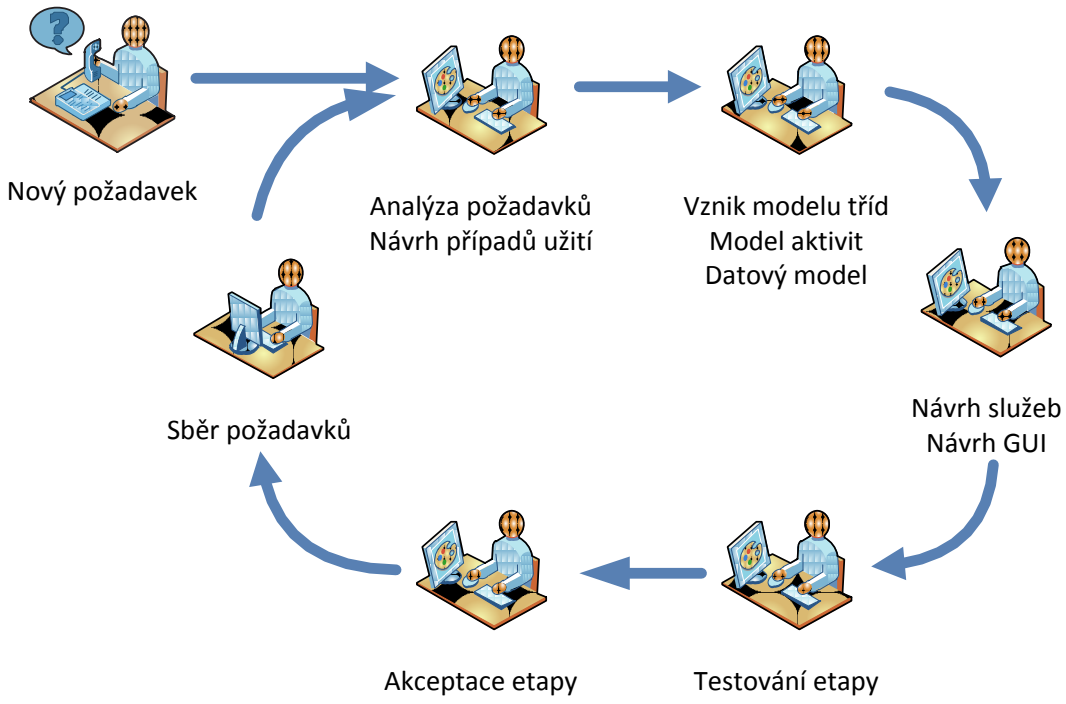
Po ukončení jednotlivých etap vývoje proběhne jednak zátěžový test, ale i test dílčích částí, který bude v případě, že se změní, případně doplní i již dříve akceptované části proveden i nad těmito, v minulosti již testovanými moduly.

Akceptace etapy

Po úspěšném otestování předávané fáze proběhne její akceptace ze strany Objednatele.

Životní cyklus vývoje systému

Pro samotnou tvorbu aplikace, stejně tak jako u každého projektu, předpokládáme, že jednotlivé fáze nejsou striktně odděleny a uzavřeny pro případné dílčí změny. Je pochopitelné, že Objednatel může vznést doplňující požadavky v případě, že již probíhá vývoj aplikace samotné. Požadavek bude zanesen do modelu, analyzován a zapracován stejně, jako by byl vznesen na počátku. Výše popsaný postup má pouze zabránit zbytečné a chaotické práci na vývoji dodávaného systému.



Obrázek - Životní cyklus projektu

INTERNÍ DOKUMENTACE PRO VEDENÍ, ANALÝZU A DESIGN PROJEKTŮ.

Podrobněji je tento postup rozveden v popisech metodiky firmy AutoCont a.s. sloužících k jednotnému vedení zakázek. Jednotlivé dokumenty nejsou součástí této nabídky, mohou být ale na vyžádání propůjčeny.

Dokumentace projektového řízení

Zhotovitel využívá vlastní projektové metodiky. Metodika je přizpůsobena vnitřním potřebám společnosti a projektům v oblasti implementace IT.

Metodika klade důraz zejména na kvalitu Návrhu a jeho přenesení a kontrolu do Vývojových a Testových fází projektu, čímž je zajištěna kvalita a zaručeno plnění požadavků Objednatele.

Analýza, design projektu

Zhotovitel postupuje v souladu s popisem, který je uveden v interní dokumentaci. Tato dokumentace vychází z ověřených postupů, které odpovídají UP a RUP požadavkům na tyto části. Pro každou část je samostatný popis, co je obsahem dané části (Analýza, design) a doporučení postupu.

Metodika vychází ze zkušeností pracovníků, kteří již pracovali na různých projektech a obsahuje jejich Best Practices z těchto činností.

Testování projektu

Zhotovitel bude opět postupovat v souladu s popisem, který je uveden v interní dokumentaci pro oblast testování. Pro vedení jednotlivých problémů bude použit nástroj pro vedení zjištěných chyb BugNet, který je v rámci firmy AutoCont již dlouhodobě používán a zcela pokrývá požadavky na vedení a odstraňování chyb.

METODIKA TESTOVÁNÍ

Část 1 – Identity Management Systém

Testování je plánováno a provedeno s ohledem na potřeby projektu, tak aby byla zajištěna maximální kvalita předávané aplikace. Pro projekt IDM bude důraz kladen zejména na funkční, integrační testování a zátěžové testování a bude zahrnovat jak testování v prostředí Zhotovitele, tak v prostředí Objednatele. Testování je obvykle prováděno po definovaných přírůstcích aplikace s následným testováním aplikace jako celku. Velikost testovacího týmu je stanovena dle rozsahu projektu a aktuálních požadavků na provedení testování (rozsah, rychlost, typy testů). Role, které se účastní testování:

- test manažer - řídí přípravu a provedení testování
- test analytik - připravuje testování a jednotlivé testy jako logické celky
- tester – provádí testování a vyhodnocuje výsledky testů
- zástupce zákazníka – zajišťuje potřebnou součinnost na straně zákazníka a dle potřeby provádí i testování aplikace ať už jako celku z pohledu zákazníka nebo částí které nemůže otestovat Zhotovitel (např. kvůli bezpečnostním omezením).

Zhotovitel předpokládá opakování testů vždy po dokončení etapy IDM, případně po integraci dalších informačních systémů di IDM, bez ohledu na typ integrace (Interní x Externí x AD).

Část 2 – Lokální registry a analýza BackOffice

Přístup k testování je shodný s předcházející části. Pro část lokální registry a analýzy BackOffice nebude testována samotná analýza BackOffice, ale implementovaná Proxy aplikace. Z povahy aplikace bude důraz kladen na integrační testování, zátěžové testování a dle potřeby bude provedeno také testování bezpečnosti daného systému.

DEFINICE RIZIK

Tato kapitola má za cíl definovat rizika, které mohou nastat v průběhu analýzy a vývoje IDM a navrhnou takové řešení, které povede k minimalizaci jejich dopadů. Dá se očekávat, že v průběhu analýzy a především vlastního vývoje a implementace do prostředí zákazníka ještě další rizika vzniknou. To je ale zcela běžný jev a nelze v této chvíli přesně specifikovat veškeré překážky, které mohou před úplným předáním systému do ostrého provozu nastat. Následující tabulka tedy obsahuje ty rizika, které jsou z pohledu Zhotovitele známá již v průběhu tvorby nabídky.

Číslo	Oblast	Popis rizika	Návrh způsobu řešení
1.	Analýza	Nedostupná dokumentace integrovaných systémů k jednotlivým rozhraním. Neexistující dokumentace datové struktury.	Provedení analýzy ve spolupráci s pověřenou osobou Objednatele, které je specialistou na danou problematiku (AD, integrované systémy).
2.	Spolupráce třetích stran	Nutnost úzké spolupráce s Zhotoviteli systémů třetích stran. Bude potřeba doplnit nové funkcionality pro úspěšnou implementaci nových služeb.	Delegování pracovníka třetí strany pro konzultaci v části analýzy i tvorby systému.
3.	Integrace	Nebezpečí časového nesouladu mezi dokončením IDM a ZR	IDM provádět přírůstkově. Před zahájením ověřit funkčnost ZR. Využít znalostí Zhotovitele, který je tvůrcem ISZR.
4.	Nárůst práce	S postupným budováním IDM, může dojít k neočekávanému nárůstu požadavků a tím i k celkovému nárůstu práce.	Důkladná analýza požadavků. Nové požadavky řešit s ohledem na jejich prioritu. Nezahltit pracovníky nefunkčními požadavky.
5.	Konektivita ZR	Je potřeba projít konektivitu na základní registry a JIP.	Využít znalostí Objednatele jako tvůrce ISZR, kde je konektivita již vyřešena.
6.	Testy výkonnost	Provedení zátěžových testů u vícevrstvých technologií nemusí vždy odhalit výkonnostní problémy testovaných systémů (na rozdíl od zátěžových testů HW prvků infrastruktury, které lze jednoznačně nakonfigurovat).	Provést testy i v součinnosti s ostatními systémy.
7.	Certifikáty AIS	ISZR Proxy potřebuje pro komunikaci s ISZR využívat certifikáty volajících AIS. Může nastat problém s poskytnutím těchto certifikátů (zvlášť u certifikátů externích AIS).	Smluvní ošetření, informovat zainteresované
8.	TXT a ODBC rozhraní ISZR – kompatibilita	XML dotaz a XML odpověď je třeba převést na TXT, ODBC formát. Protože XML dává širší možnosti definování struktury, může nastávat problém s konverzí.	Eliminovat použití těchto rozhraní
9.	TXT a ODBC rozhraní ISZR – rozsah	Rozsah použití těchto rozhraní vyplyne až z analýzy. Zároveň se jedná o poměrně pracný vývoj.	Nabídka předpokládá určitý rozsah (10x3 čd vývoj + odpovídající implementace, test, dokumentace). Být připraven na úpravu požadavků, přesun zdrojů.
10.	Uživatelské Web rozhraní ISZR - rozsah	Požadavek na počet potřebných služeb a požadavek na provedení vyplyne až z analýzy. Zároveň se jedná o poměrně pracný vývoj.	Nabídka předpokládá určitý rozsah (50x3 čd vývoj + odpovídající implementace, test, dokumentace). Být připraven na úpravu požadavků, přesun zdrojů.

Ostatní

KOMPLETNÍ PODPORA ČESKÉHO JAZYKA Z HLEDISKA DAT, SE KTERÝMI PRACUJE IDM VČETNĚ MOŽNOSTI PŘÍPADNÉHO OŘEZÁNÍ DIAKRITIKY

Systém IDM bude tvořen od počátku v češtině. Pro vybrané funkcionality budou české znaky s diakritikou nahrazeny znaky bez diakritiky (např. tvorba mailové adresy uživatele z kombinace jméno.příjmení). Části IDM, kde bude tato funkcionalita použita, budou tvořeny na základě analýzy IDM, požadavků Objednatele ale i na základě zkušeností pracovníku Zhotovitele.

V RÁMCI IMPLEMENTACE MUSÍ BÝT ZAJIŠTĚNO SEZNÁMENÍ APLIKAČNÍCH SPRÁVCŮ (MIN. 2)

Pro samotné ovládání IDM bude probíhat pravidelné seznámení vybraných zaměstnanců, administrátorů. Pro tyto uživatele bude vytvořena uživatelská příručka IDM, kde bude podrobně vysvětlena veškerá funkcionalita Portálu IDM.

Termín seznámení bude domluven v rámci nasazení IS na provozní prostředí tak, aby nové funkcionality byly probrány před nasazením této verze na ostré prostředí. Předpokládáme, že školícím prostředím bude testovací server, v rámci kterého bude proveden jak test nových funkcionalit, tak i seznámení uživatelů. Zároveň po provedení testů a akceptace dílčího plnění bude tato nová verze IDM nasazena na provozní prostředí. Seznámení tedy poběží nad novou verzí, která je zároveň připravena k nasazení. Počet osob a frekvence seznámení se předpokládá pololetně v požadovaném rozsahu, případně na vyžádání.

Integrační body a propojení vybraných systémů

Integrační body pro napojení vybraných systémů budou možné vystavit v katalogu služeb pomocí technologie UDDIv3. Integračním bodem bude každá nově vystavená funkce/operace v jakémkoli systému Objednatele. Body spolu vytvoří síť služeb vhodné pro řešení několika problémů.

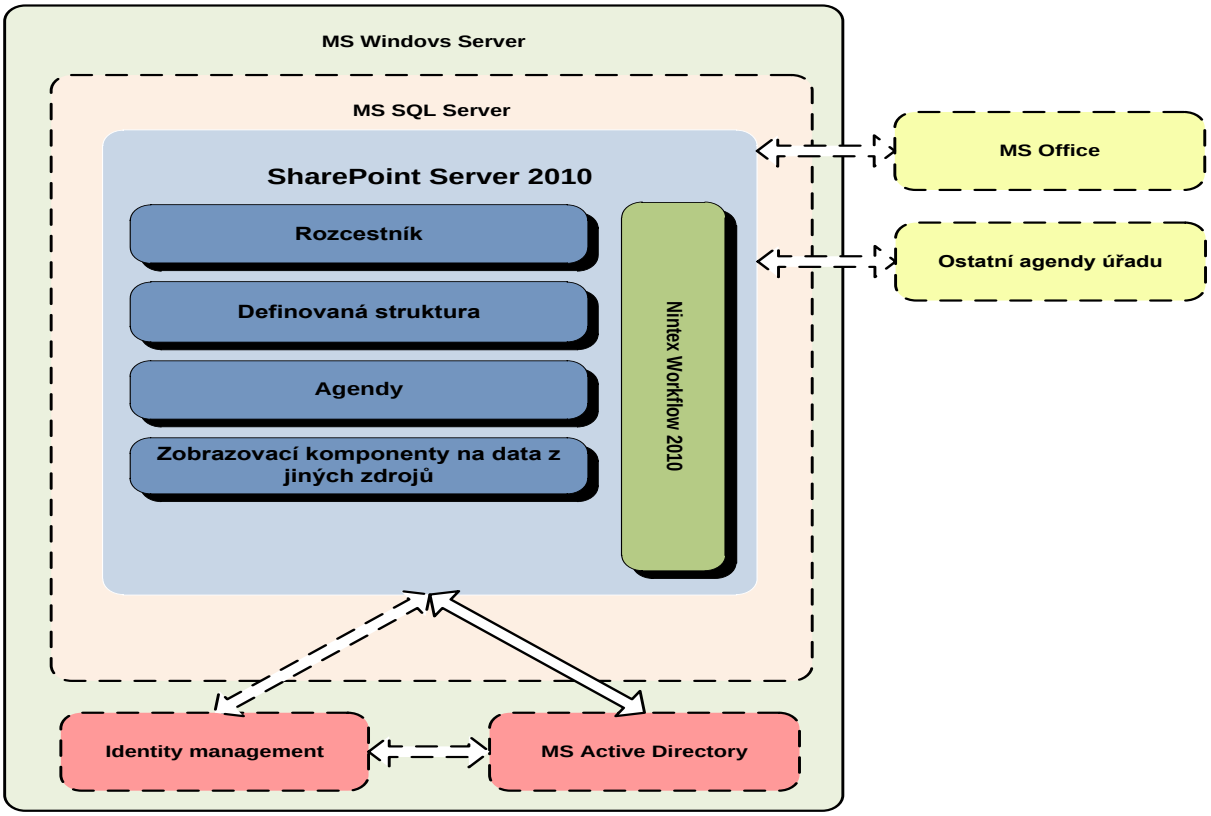
Seznam služeb a komunikující technologie bude předmětem analýzy a technického návrhu v době realizace. Již teď můžeme říci, že podporované technologie jsou HTTP/HTTPS, JCA, JDBC, WS, Hibernate, FTP, SFTP.

Na sběrnici ESB budou vystaveny integrační body. Tyto budou zabezpečeny a využívat je budou pouze autorizované systémy a uživatelé. Autorizace/autentizace bude probíhat vůči centrální správě účtu IDM. Vystavením integračních bodů jako business služeb, definováním, popsáním a registrováním do katalogu služeb docílíme jednoho registračního místa (podobný záměr jako mají Základní Registry). Integrace systémů bude probíhat tak, že se prvně bude prověřovat, že daná služba již neexistuje. Pokud bude existovat, odpadne složité programování a testování. To se omezí jen na testy u nové integrovaného systému. Složité business funkce bude možné nastavit na ESB tak, aby zde probíhal časové upomínky, opakované dotazování na služby, které selhaly z důvodů nedostupnosti na straně poskytovatele.

Technologie Portálového řešení

Základem nabízeného řešení je implementace SW prvků v podobě platforem, které jsou podle požadavku Objednatele schopny „pokrýt funkční oblasti uvedené v zadávací dokumentaci a to buď samostatně, nebo zprostředkovaně ve spolupráci s některými integrovanými systémy“. Řešení je otevřené, je možno jej dále rozšiřovat o další agendy a procesy úřadů a upravovat podle potřeby úřadu a to jeho vlastními silami.

V rámci zpracování Implementační studie (analýzy a prováděcí studie) bude navrženo jejich optimální využití, odpovídající vlastnostem instalovaných platforem a na úřadě již existujících – provozovaných - systémů.



Obrázek 3 *Dodávané SW komponenty*

Dodávané komponenty a jejich postavení v řešení
Celkové funkčnosti dodaného řešení, dosáhneme instalací následujících platforem.

Microsoft SharePoint Server 2010 - včetně Enterprise CAL licencí pro uživatele, jako standardní produkt firmy Microsoft – obsahuje standardní funkční výbavu pro přípravu aplikací, evidencí správu dokumentů atd. Předpokládáme, že Objednatel tuto technologii již vlastní a proto není součástí dodávaného SW, nicméně je nezbytná pro navrhované řešení.

NINTEX WORKFLOW – na základě zkušeností Zhotovitele bude dodána tato platforma, která rozšíří nativní prostředí workflow, které je součástí SharePointu. Tato komponenta podstatně zkvalitní a rozšíří možnosti ovládání celého systému, práce s daty, jejich zabezpečení a variabilitu pořizování. Dodávkou Nintex získává Objednatel silný prostředek modelování procesů vnitřního chodu úřadu i ostatních klíčových procesů správy města. Tyto procesy je možné spouštět z jiných AISů. Výhodou Nintexu je tedy ušetření nákladů na budování nových IS s vazbou na procesní zpracování úloh. Objednateli postačí pouze dodat funkci do již existujícího systému a vhodně propojit aplikaci přes integrační platformu s Nintex Workflow a to díky publikovanému rozhraní Nintex přes webové služby, které jsou standardem.

MS SQL SERVER REPORTING SERVICES – komponenta umožňující na portále zobrazovat definované reporty z různých zdrojů. Výhodou tohoto řešení je, že uživatele nenutí přistupovat přímo do jednotlivých aplikací, které obsahují zdrojová data. Ale naopak umožňují autorizované zobrazení dat v jednotném prostředí. Pro plnou funkcionalitu je však potřeba implementovat protokol Kerberos, který zajistí přenos jednotlivých přístupových oprávnění napříč systémy.

VZOROVÉ APLIKACE BACK OFFICE připravené na platformě SharePoint pod názvem aMOSS.gov. Viz. popis Portálu úředníka.

Microsoft SharePoint Server 2010
Rozhodujícími přínosy plynoucími z nasazení Microsoft SharePoint Server 2010 (SharePoint nebo SPS) budou zejména:

- **Sdílení informací** - snadný přístup k informacím. Informace budou dostupné oprávněným uživatelům z prostředí webového prohlížeče na centrálním místě vždy v aktuální verzi.

- **Odstranění duplicit** – vytvořením a sjednocením platformy pro sdílení informací dojde k odstranění duplicitního uložení informací (veřejné složky, lokální disky uživatelů, sdílené složky na serverech, poštovní schránky uživatelů, atd.). Uživatelé si již nebudou muset zasílat dokumenty elektronickou poštou, ale mohou zasílat pouze odkazy na úložiště těchto dokumentů, která jsou dostupná všem uživatelům s potřebnými právy. Vytvořením jednotného intranetu v celé Allianz nebudou muset uživatelé procházet několik různých webů, aby našli potřebnou informaci.

- **Integrace s ostatními aplikacemi** s webovým uživatelským GUI. Uživatelé nebudou nuceni zadávat opakovaně své uživatelské jméno a heslo. Je rovněž možné využít Single Sign-on pro přístup k aplikacím, které nevyužívají k autentizaci uživatele doménové účty.

- **Další rozvoj řešení** – SharePoint je otevřené řešení, které je možné do budoucna dále rozšiřovat za použití vlastních zdrojů bez nutnosti větších zásahů ze strany externích Zhotovitelů. SharePoint není jen „hotovým řešením“, ale může také sloužit jako platforma pro tvorbu specifických aplikací.

MS SharePoint v kombinaci s aplikací MS SharePoint Designer umožňují vytváření jednoduchých schvalovacích postupů. Z naší zkušenosti, ale vyplývá, že tyto nejsou velmi často dostačující a proto doplňujeme SharePoint o nástroj Nintex Workflow 2010, který rozšiřuje možnosti SharePointu právě o vytváření pracovních postupů přímo ve webovém prohlížeči. Uživatelé, po krátkém seznámení s produktem, budou schopni vytvářet složité pracovní postupy bez znalosti jakéhokoliv programování. Výhodou Nintex Workflow 2010 je také to, že poskytuje "platformu" pro další vývoj systému v budoucnu (nejste v té chvíli závislí na externím Zhotoviteli v případě, že potřebujete provést úpravy nebo vytvořit další pracovní postup). Pomocí tohoto produktu získává organizace nástroj pro modelování a řízení procesů.

APLIKACE ROZŠIŘUJÍCÍ SHAREPOINT FUNKCE (PORTÁL ÚŘEDNÍKA)

Řešení Portál úředníka (dále PU) nazvané ***aMOSS.gov*** je navrženo jako webový prostor (intranet) pro interní využití v organizacích veřejné správy, s důrazem na jednoduchost, rychlost nasazení a s možností dále toto řešení rozvíjet a dotvářet. Jako základ jsou použity aplikace (samostatné agendy typu dokumentové úložiště, žádosti apod.), řešící dílčí oblasti a procesy v organizaci uspořádané do logického celku, který je dále rozšiřován o další aplikace.

Řešení aMOSS.gov vytváří podmínky pro zavedení automatizovaného zpracování podpůrných, vnitřních, i vnějších služeb veřejné správy a připravuje kvalitní data o práci úřadu pro jejich další použití, například zpracováním analýz prostřednictvím manažerských nástrojů, controlling a benchmarkingu poskytovaných služeb. Aplikace a jejich Workflow požadované Objednatelem obsahují základní sadu aplikací, které jsou popsány v dalším textu. Zhotovitel předpokládá nastavení jejich funkcí dle výsledků úvodní implementační analýzy. Přirozenou vlastností našeho řešení je možnost úpravy vlastními silami Objednatele v oblastech:

- Úprava datové struktury evidencí.
- Přípravu potřebných pohledů na data pro případ podání žádosti, změny, schvalování atd.
- Vytvoření evidencí (formulářů žádostí, automobilů, kurzů, školitelů atd.) v plochém datovém modelu s jednoduchým popisem.
- Workflow – automatizace průběhu procesů.
- Práci s dokumenty souvisejícími s řešenými procesy.
- Indexování obsahu vložených informací.
- Vytváření exportních souborů.
- Výběr dat podle definovaných kritérií.

Nintex Workflow 2010

Pro vytváření pracovních postupů v prostředí webového prohlížeče tak, aby byly uživatelsky snadno konfigurovatelné, využijeme produktu Nintex Workflow 2010. Nintex Workflow umožňuje vytvářet pokročilé schvalovací procesy, včetně nastavení rolí dle jednotlivých workflow a významně tak rozšiřuje standardní vlastnosti SharePointu. Nintex Workflow poskytuje:

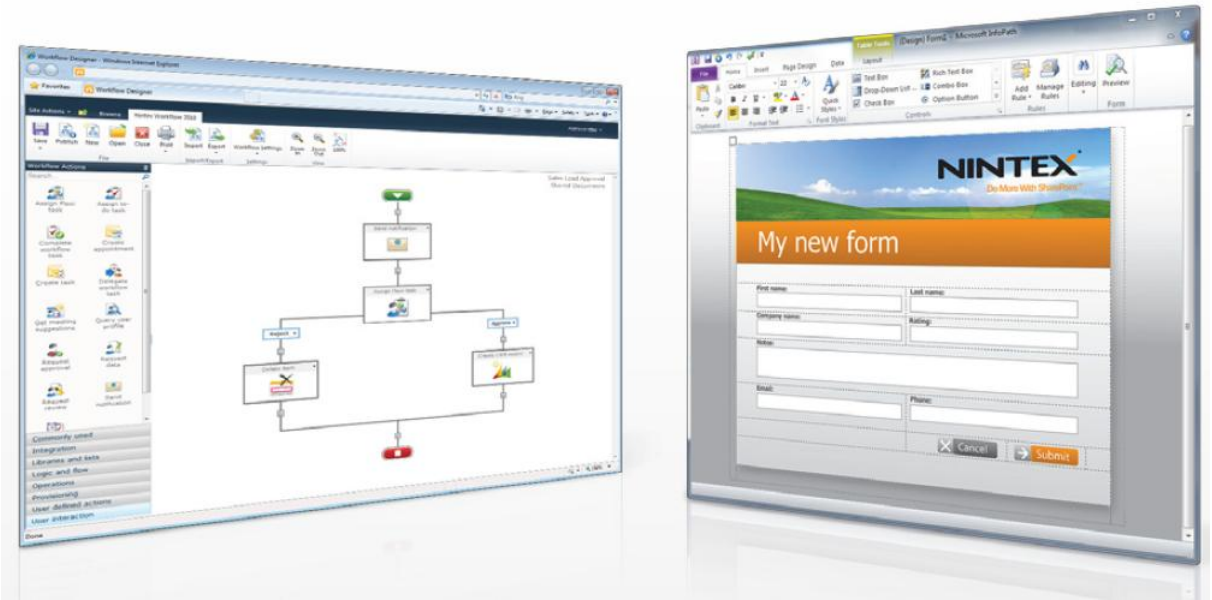
- Grafické rozhraní pro definování procesu.
- Vlastní modelování procesů.
- Podporu „sériových“, „paralelních“ nebo kombinovaných procesů.

- Emailové notifikace, ukládání komentářů jednotlivých kroků „schvalovacího procesu“.
- Monitorování a reporting všech aktivit realizovaných v rámci knihoven dokumentů.
- Monitorování stavu „schvalovacího procesu“.
- Automatická notifikace a eskalační mechanismy.
- Logování událostí.
- Možnost publikace dokumentů do jiných složek v rámci SharePoint systému nebo do systémů třetích stran.
- Integrace se systémy třetích stran prostřednictvím webových služeb.

POPIS ŘEŠENÍ

Jako nástroj pro modelování a řízení procesů bude dodán **Nintex Workflow 2010**, komponenta která podstatným způsobem rozšíří funkčnost portálu. Objednatel získá silný prostředek modelování procesů vnitřního chodu úřadu a jejich výkonu v rámci provádění různých agend. Získá tak možnost rychle a snadno automatizovat procesy počínaje od jednoduchého zpracování žádosti o schválení dovolené až po složitou integraci napříč externími aplikacemi a různými datovými zdroji. Za použití Nintex Workflow 2010 budou vytvořeny požadované vzorové pracovní postupy Objednatele.

Nintex Workflow 2010 je produkt australské společnosti Nintex, která je certifikovaným zlatým partnerem společnosti Microsoft. Produkt je plně integrován s produkty společnosti Microsoft a vhodně doplňuje portálovou platformu Microsoft SharePoint 2010. Nintex Workflow 2010 je lokalizován do českého jazyka. Jedná se o prověřený a stabilní produkt, který prošel rozvojem v několika verzích, přičemž jeho další rozvoj je připravován ve vztahu k rozvoji nástrojů společnosti Microsoft.



Komponenta Nintex Workflow 2010 rozšíří nativní workflow prostředí, které je součástí platformy MS SharePoint a podstatně zkvalitní a rozšíří možnosti ovládání celého informačního systému úřadu, práci s daty, jejich zabezpečení a jejich pořizování.

MS SharePoint se svou základní funkcionalitou MS SharePoint Designer nativně umožňuje vytváření jednoduchých schvalovacích postupů. Z našich zkušeností však vyplývá, že tyto nejsou velmi často pro organizace obdobného typu dostačující a proto doplníme MS SharePoint o nástroj Nintex Workflow 2010, který rozšíří funkcionality SharePointu v oblasti modelování a provádění procesů. Nintex Workflow pak mimo jiné přináší vizualizaci procesu i možnost sledování průběhu workflow.
Uživatelé budou po seznámení s produktem schopni vytvářet pracovní postupy bez znalosti jakéhokoliv programování. Výhodou nástroje Nintex Workflow 2010 je také to, že poskytuje flexibilní platformu pro

další rozvoj systému v budoucnu, přičemž organizace není v té chvíli závislá na externím Zhotoviteli v případě, že potřebujete provést úpravy nebo vytvořit další pracovní postup nebo proces.

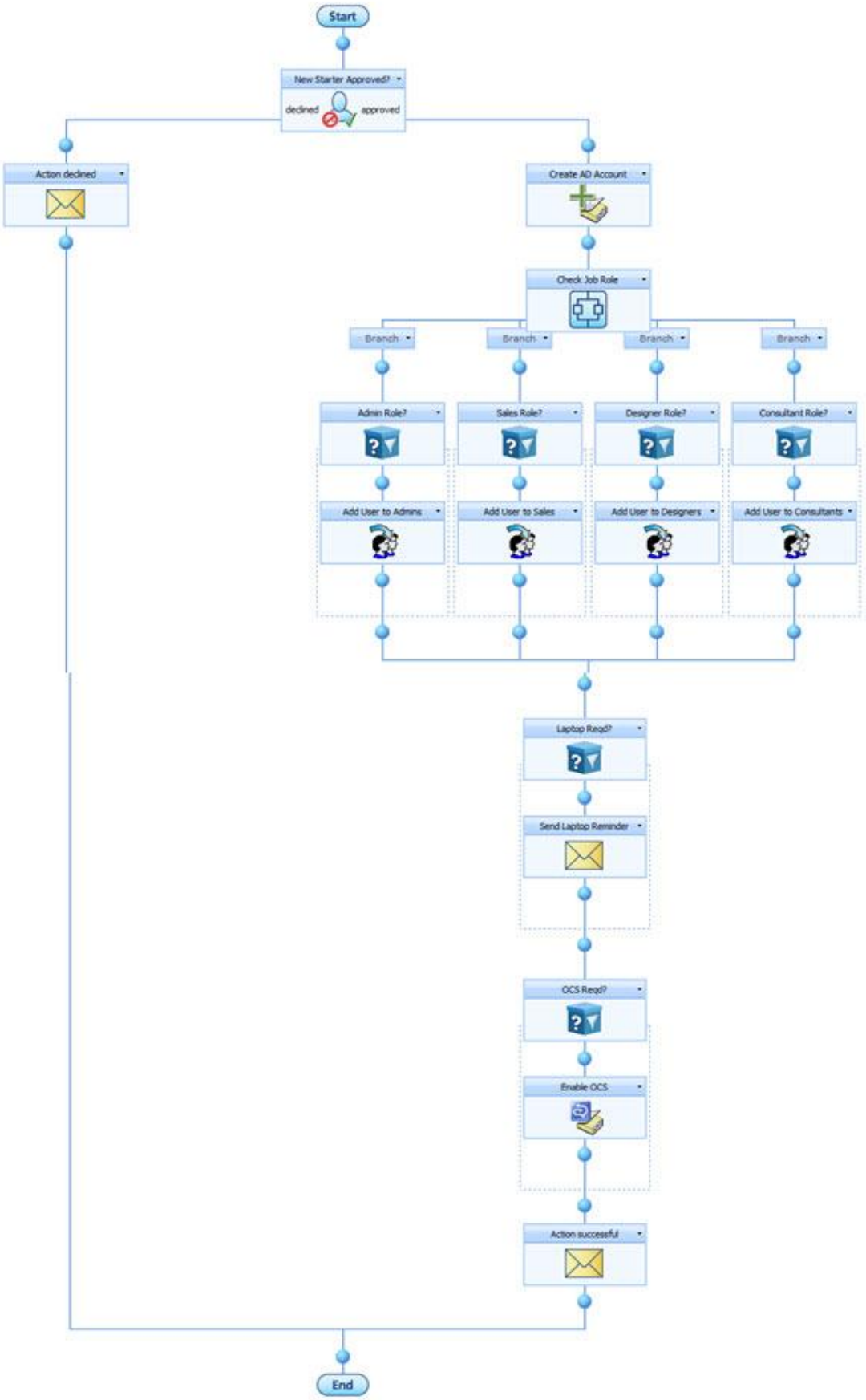
Za použití Nintex Workflow 2010 budou vytvořeny požadované vzorové pracovní postupy:

- 3 interní žádosti s workflow
  - žádost o povolení služební cesty
  - žádost o materiál
  - žádost o udělení přístupu k agendě-aplikaci
- 1 vzorová agenda s workflow
  - nástup nového zaměstnance

Za tímto účelem budou ve vhodné míře využity následující služby Nintex Workflow 2010:

- Grafické rozhraní pro definování procesu.
- Vlastní modelování procesů.
- Podpora „sériových“, „paralelních“ nebo kombinovaných procesů.
- Emailové notifikace, ukládání komentářů jednotlivých kroků „schvalovacího procesu“.
- Monitorování a reporting aktivit realizovaných v rámci knihoven dokumentů.
- Monitorování stavu „schvalovacího procesu“.
- Automatická notifikace a eskalační mechanismy.
- Logování událostí.
- Publikace dokumentů do jiných složek v rámci SharePoint systému nebo do systémů třetích stran.
- Integrační vazby se systémy třetích stran prostřednictvím webových služeb.

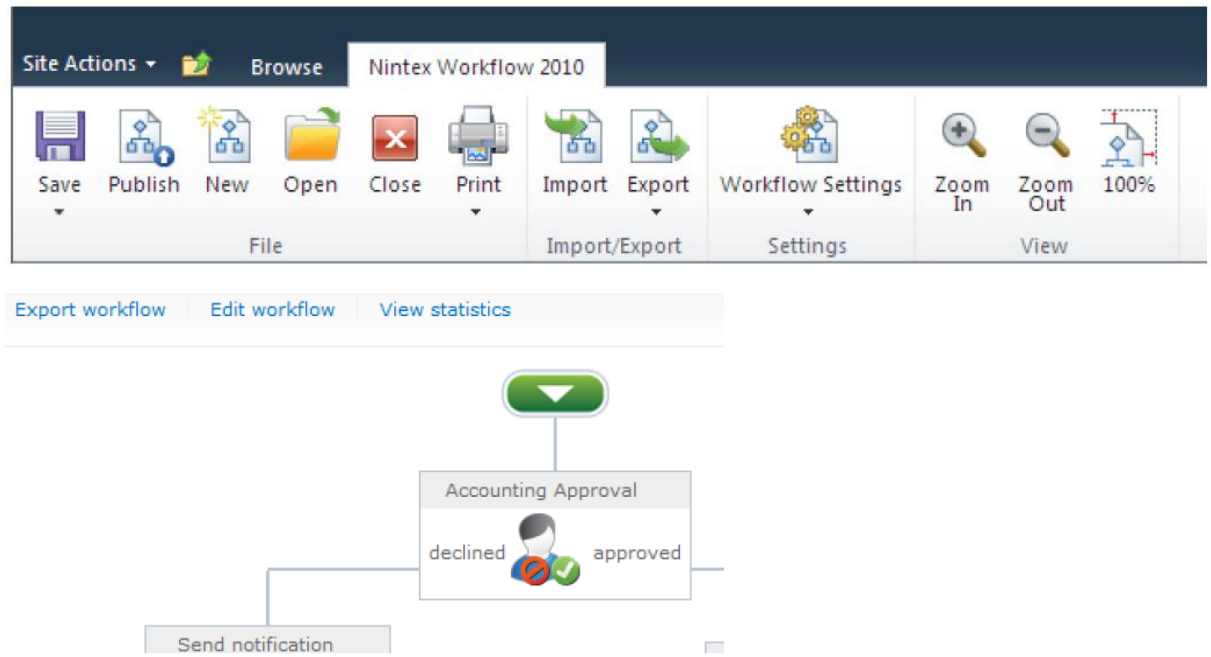
Následující schéma ukazuje vzorový model workflow pro nástup nového zaměstnance jako příklad.



FUNKCIONALITY NINTEX WORKFLOW 2010

Kreslení namísto psaní kódu

- Intuitivní, snadno použitelný nástroj pro navrhování pracovních postupů založený na internetovém prohlížeči a používající funkci „táhni a pusť“
- Umožňuje všem uživatelům platformy SharePoint během několika málo minut zautomatizovat jejich procesy

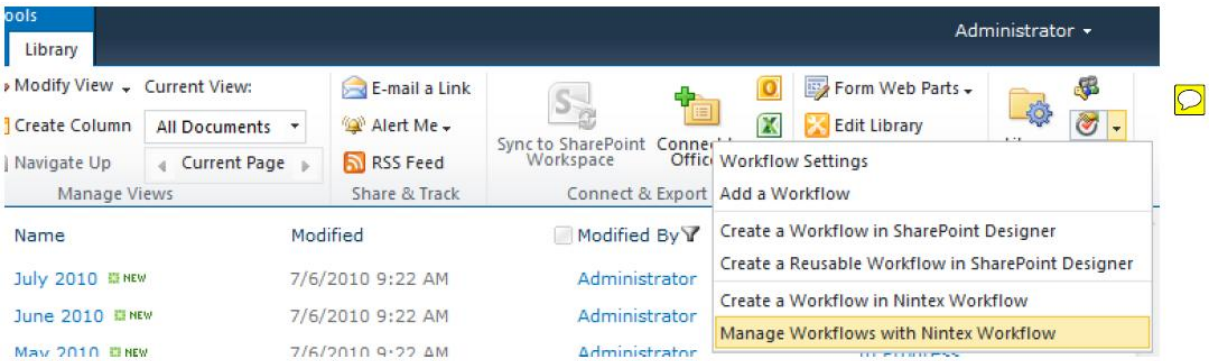


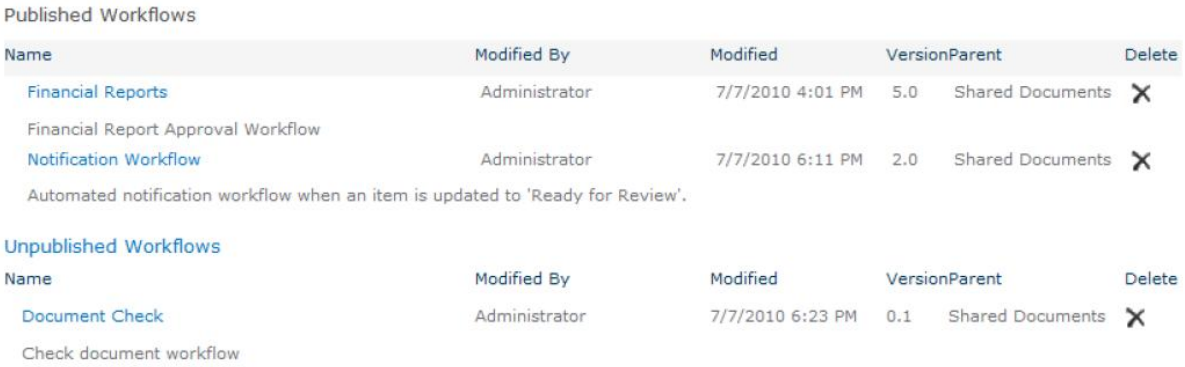
Návrh workflow procesů probíhá přímo na portále v grafickém návrháři a to bez programování. Po uložení návrhu lze workflow přímo aplikovat. K dispozici je velké množství různých funkcí (podmínky, schvalování, změna položky, atd.), které se do diagramu vkládají jednoduše přetažením myši a následně se ve webovém prohlížeči konfigurují.

Měření a řízení

- Sleduje stav vašich pracovních postupů v reálném čase
- Měří a zlepšujte výkonnostní parametry vašich procesů

Administrátor má prostřednictvím webového rozhraní přehled o životním cyklu pracovních postupů s možností jeho řízení.

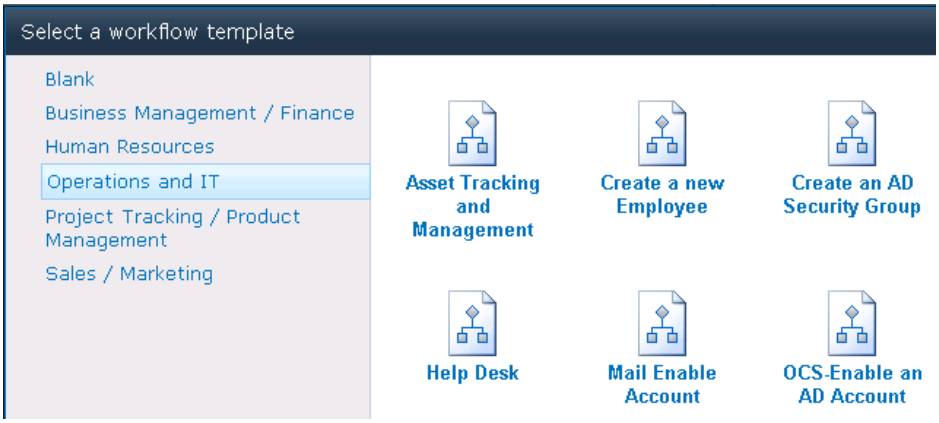




Dvě webové části, které jsou k dispozici hned po instalaci („Moje úkoly pracovních postupů“ a „Pracovní postupy iniciované mnou“), lze konfigurovat na úrovni farmy, takže uživatelé mohou sledovat veškeré pracovní postupy, které se jich týkají, na jednom místě.
Statistiky pracovních postupů nabízejí celkový náhled na výsledky pracovních postupů a jsou k dispozici pro každý pracovní postup. Zahrnují informace o průměrné době spuštění, celkovém počtu spuštění, počtu probíhajících pracovních postupů a dále také o výsledcích uživatele, což je důležitá funkce pro zjištění úzkých míst v obchodních procesech.
Funkce vytváření sestav jsou dále rozšířeny o grafické webové části podle dat, včetně sestav jako např. ‘průměrná doba dokončení pracovního postupu‘, ‘standardní odchylky‘, ‘minimální a maximální doba dokončení‘ a ‘doba odpovědi uživatele‘.

Opakované využití jednou vytvořeného návrhu

- Opakovaně použitelné šablony a moduly
- Sdílené a sjednocené pracovní postupy napříč týmy



Postaveno na platformě SharePoint a pro ni

- Jednoduché nasazení a řízení, není zapotřebí žádný klientský software
- Chrání vaši investici do platformy SharePoint
- Eliminuje dodatečné investice do infrastruktury

Rychlá návratnost vynaložené investice

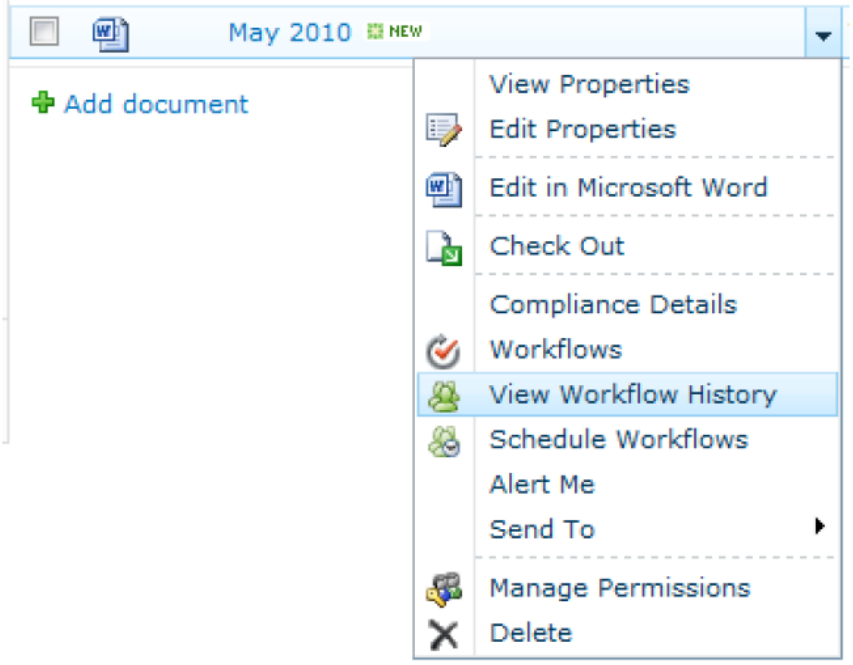
- Větší efektivita a menší náklady na zpracování
- Menší zátěž rozpočtu na IT

Integrované funkce SharePoint 2010

- Plovoucí pás karet
- Služby podnikové konektivity

- Služby Excel
- Formuláře InfoPath
- Opakovaně použitelné pracovní postupy
- Pracovní postupy webu
- Pracovní postupy typu obsahu
- Sady dokumentů

Vlastností Nintexu je jeho plná integrace do systému SharePoint. Ihned po instalaci jsou z adekvátních menu a kontextových nabídek přítomné možnosti nastavení i práce se samotným workflow. Také tvorba workflow je plně integrována a probíhá, stejně jako práce v celém prostření SharePointu, prostřednictvím webového prohlížeče. Prvky v diagramu i prvky z galerie je možné přenášet prostřednictvím funkcionality „táhni a pusť“. Samozřejmostí je také verzování jednotlivých workflow.
Pracovní postupy mohou odesílat dokumenty na weby center záznamů serveru SharePoint a mohou tak prostřednictvím jednoduchého uživatelského rozhraní s minimálními nároky na uživatele pomoci spravovat přípravu obsahu v průběhu celého jeho životního cyklu.



Akce pracovního postupu pro vytváření úkolů a schůzek v Outlooku a pro načítání návrhů časů schůzek. Například pracovní postup pro schválení dovolené by mohl přidat schválenou dovolenou do kalendáře žadatele i jeho nadřízeného. Jelikož se využívají rozhraní APIwebové služby Exchange Server, hodí se tato metoda také pro nejrůznější on-premises (ve vlastní budově umístěné), hostované a hybridní architektury.
Pracovní postupy mohou vytvářet a využívat modely excelového listu. Služby Excel Services pro server SharePoint mohou využívat výpočetní modely a data tabulky prostřednictvím služby SOAPWeb. Díky této akci pracovního postupu mohou uživatelé snadno poskytovat vstupy a načítat výsledky z listů tabulky.
Akce pracovního postupu ke zpracování dokumentů Word prostřednictvím služeb Word Services. Umožňují tvorbu dokumentů, aktualizaci formulářových polí a převod dokumentu do PDF-ka jiných formátů prostřednictvím serverové aplikace

Můžete spouštět dotazy na podnikové vyhledávání ve vyhledávacím modulu serveru SharePoint a výsledky zařádit do pracovních postupů. Tento postup funguje jak pro fulltextové dotazy, tak i pro dotazy založené na vlastnostech.

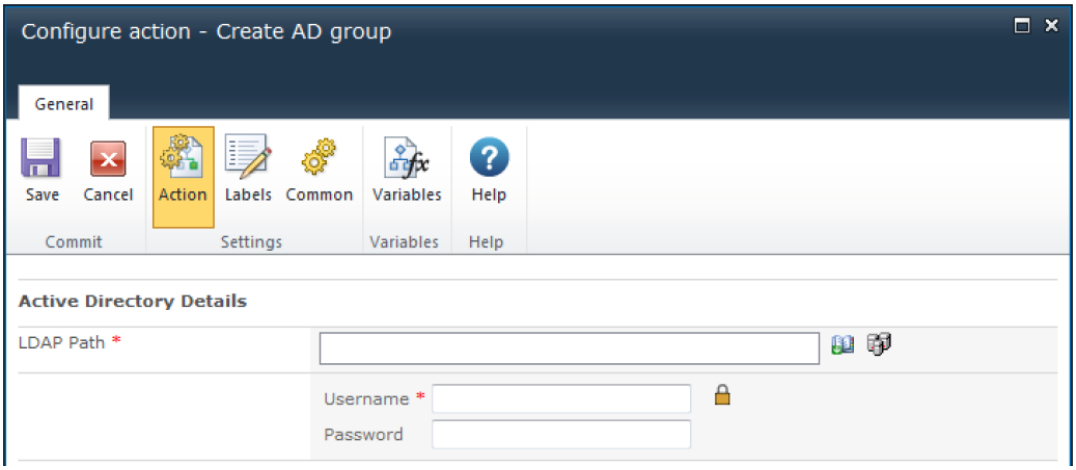
UŽIVATELSKÉ ÚČTY, PROFILY UŽIVATELE A CÍLOVÉ SKUPINY

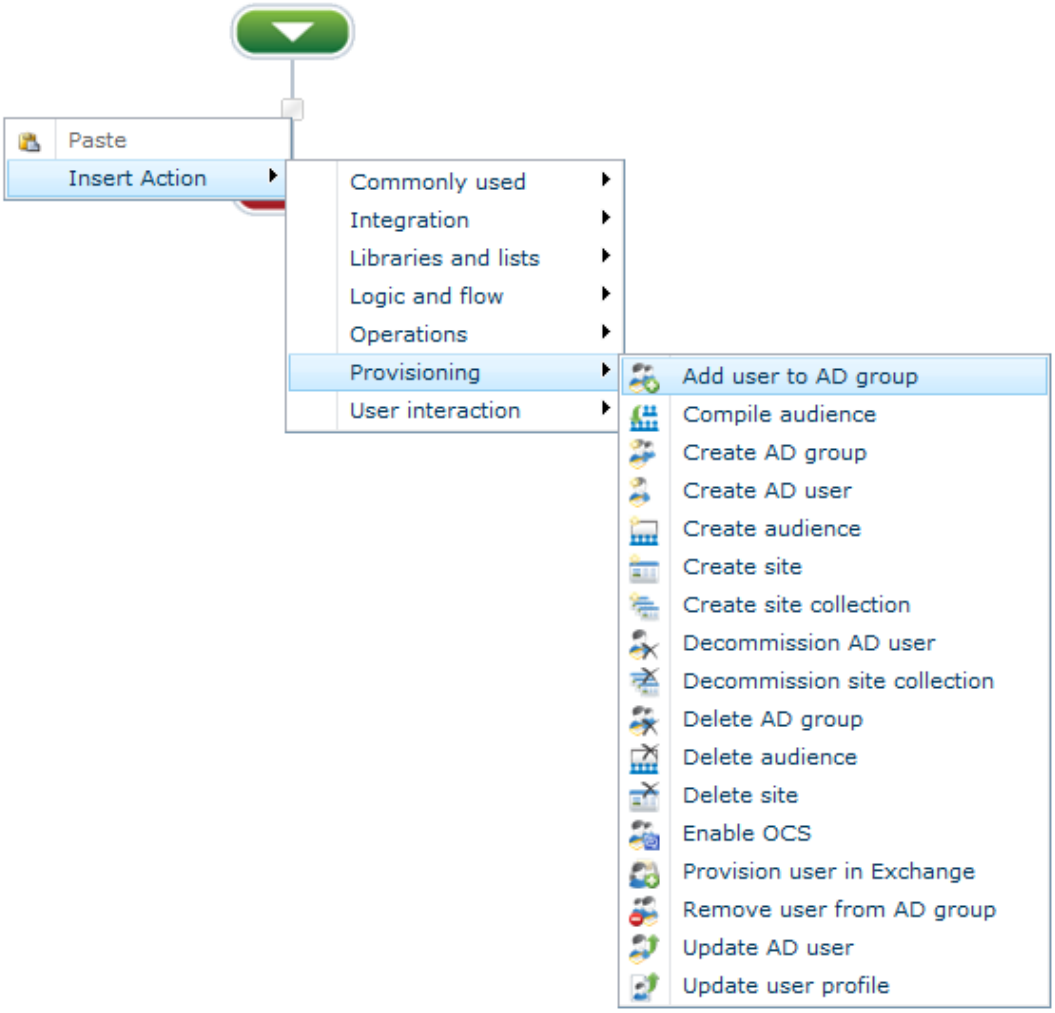
Nintex Workflow umožňuje nativně převzít uživatelská oprávnění ze systému SharePoint. Při integraci systému SharePoint s LDAP/Active Directory jsou tak zároveň integrovány uživatelské účty Ninntex Workflow a tím je zjednodušena autentizace uživatelů Nintex Workflow.

Akce pracovních postupů podporují přidávání/aktualizaci/odstraňování v úložišti profilů uživatele na serveru SharePoint, včetně vlastností, skupiny členů a členství. Cílové skupiny lze vytvářet, odstraňovat, měnit a přepočítávat.

Akce pracovního postupu podporují také automatické zpracování následujících úkolů: přidání/odstranění uživatelů ze skupin Active Directory (AD); vytváření, aktualizování a mazání účtů Active Directory.
Je možné vytváření a odstraňování oprávnění pro e-mailové účty Exchange Server (2003, 2007 a 2010) u účtů Active Directory.

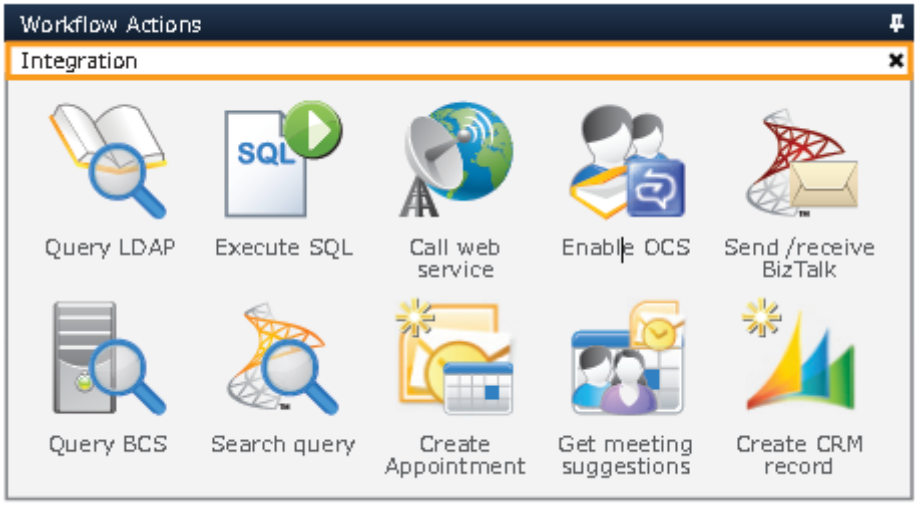
Dále je možné povolování a zakazování oprávnění pro Office Communication Server (2007 a 2010 a také Live Communication Server 2005) (OCS / LCS) u účtů Active Directory.




Paste
Insert Action
Commonly used
Integration
Libraries and lists
Logic and flow
Operations
Provisioning
User interaction
Add user to AD group
Compile audience
Create AD group
Create AD user
Create audience
Create site
Create site collection
Decommission AD user
Decommission site collection
Delete AD group
Delete audience
Delete site
Enable OCS
Provision user in Exchange
Remove user from AD group
Update AD user
Update user profile

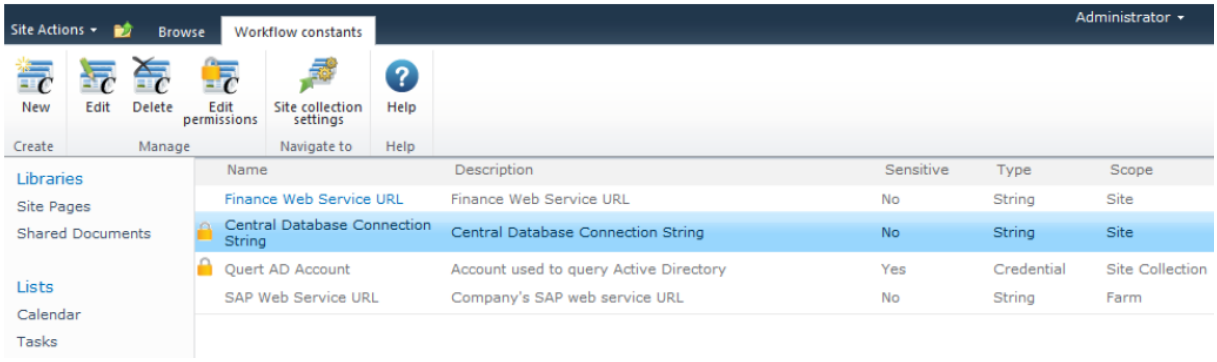
MOŽNOSTI NAPOJENÍ NA OSTATNÍ SYSTÉMY

- Vytváření uživatelských účtů ve službách Active Directory, Exchange Server a Office Communications Server
- Načítání a zápis dat z Microsoft CRM
- Nastavení položek kalendáře a úkolů ve službě Exchange Server
- Snadný přístup k datům a procesům z podnikových a externích systémů za pomoci webových služeb, SQL, LDAP, XML , BizTalk a jiných běžných aplikačních programů a otevřených rozhraní



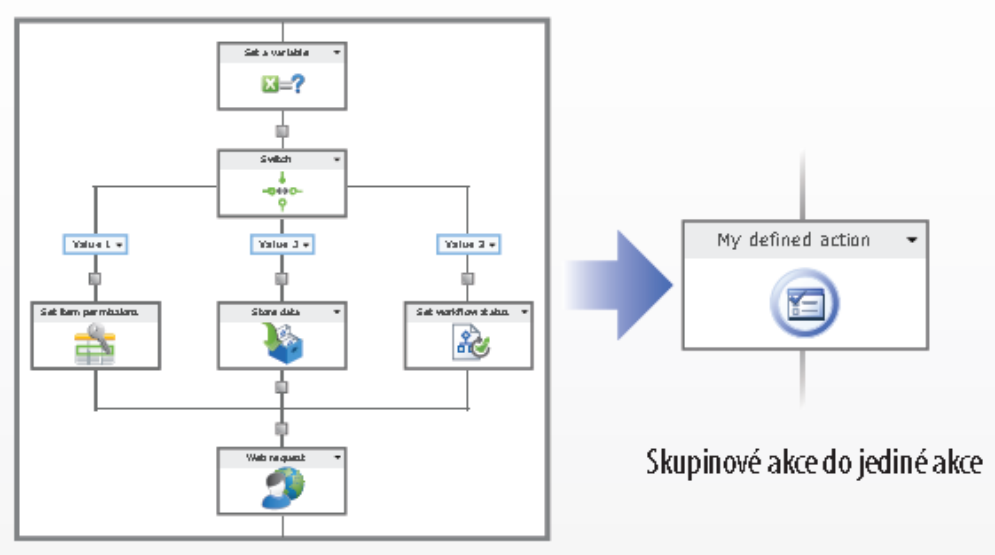
Umožňuje například interakci se serverem BizTalk. Tato akce dokáže posílat zprávy do orchestrace BizTalk, případně počkat na zprávu ze serveru BizTalk. Tato akce umožňuje, aby probíhala interakce mezi pracovním postupem a libovolným externím systémem, se kterým spolupracuje server BizTalk.

Nintex Workflow 2010 se dokáže připojit k SharePoint 2010 Business Connectivity Services (BCS) a načítat a zapisovat data z nebo do externích datových zdrojů.



ROZŠIŘITELNOST A INDIVIDUALIZACE

- Vytváření „User Defined Actions“ pomocí návrháře pracovních postupů s podporou funkce „táhni a pusť“
- Vytváření vlastních akcí pomocí aplikace Visual Studio
- Export pracovních postupů do aplikace Visual Studio
- K dispozici je celá řada doplňků, rozšíření a konektorů nezávislých výrobců



DALŠÍ FUNKCE

- Exkluzivní systém LazyApproval®, odpovědi na požadavky v reálném jazyce, i když jste v pohybu a nemáte přístup k portálu SharePoint
- Delegování umožňuje ad hoc delegování úkolů pracovního postupu, nebo lze úkoly na stanovenou dobu předelegovat na jiného uživatele
- Plánované a časově vymezené pracovní postupy pro opakované procesy
- Bohaté možnosti upozorňování na pracovní postupy prostřednictvím elektronické pošty, instant messagingu a SMS
- Řízení přístupu uživatelů k akcím
- Anotace procesního diagramu a náhled pro tisk
- Proces schvalování změn pro publikované pracovní postupy
- Individuálně upravitelný panel nástrojů s funkcemi hledání a změny velikosti
- Možnost změny velikosti pohledu návrháře

Obecné minimální Systémové požadavky:

Nintex Workflow 2010 vyžaduje instalaci následujícího software a jeho korektní konfiguraci:

- Nintex Workflow 2010 musí být inslalován na Microsoft Windows Server 2008 nebo 2008 R2
- Internetový prohlížeč Microsoft Internet Explorer 7.x, doporučován je Microsoft Internet Explorer 8 nebo vyšší
- Microsoft SharePoint Foundation 2010 a/nebo Microsoft SharePoint Server 2010
- SQL Server 2012 nebo SQL Server 2008 nebo SQL Server 2005

Portál úředníka – popis funkcionalit
Portál bude zaměřen na všeobecné použití pro každého úředníka. Jednotlivé aplikace budou umístěny na PU v horizontální navigaci (menu). Návrh portálu také předpokládá budoucí vytvoření vlastních webových prostorů pro jednotlivé odbory, případně pracovní skupiny na podporu vnitřního chodu úřadu. Tyto „podweby“ mohou obsahovat stejné aplikace s „lokální působností“ nebo s modifikovanou konfigurací, případně jsou využitelné pro podporu spolupráce v rámci odborů.

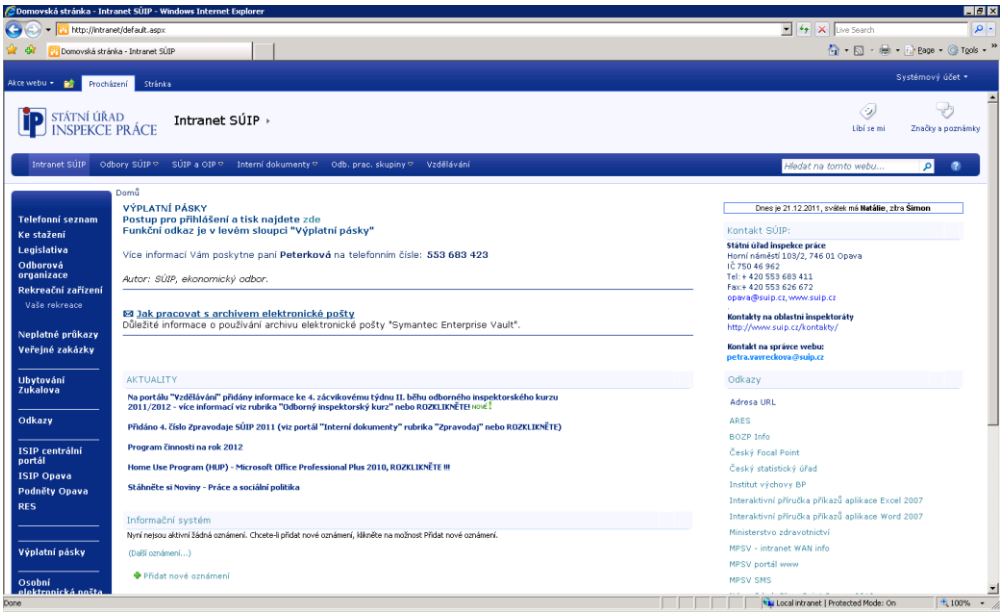
Vlastní realizace portálu bude zahrnovat:

- detailní analýzu a návrh řešení, vč. vypracování detailního harmonogramu nasazení,
- navržení oblastí řešení a možného budoucího rozvoje
- instalaci serverové části portálu
- vytvoření vzorových agend a workflow dle návrhu řešení v minimálním rozsahu:
- 3 interní žádosti s workflow (žádost o povolení služební cesty, žádost o
- materiál, žádost o udělení přístupu k agendě-aplikaci apod.)
- 1 vzorová agenda s workflow (nástup nového zaměstnance apod.)
- zpracování dokumentace konfigurace a instalace systému
- návrh disaster recovery plánu
- popis údržby systému

Oblast portál bude zahrnovat vytvoření následující části:

NÁVRH DESIGNU PORTÁLU A JEHO REALIZACE

SharePoint 2010 umožňuje upravit grafickou podobu a ovládací prvky portálu tak, aby odpovídala požadavkům nebo grafickému manuálu organizace. Pro tyto úpravy je možné využít jak již předdefinovaných šablon SharePointu a upravit jeho podobu pomocí barevných motivů, nebo navrhnout celé grafické rozhraní. Rozsah pracnosti úprav grafického rozhraní se tak může pohybovat v rozmezí jednoho dne až po desítky hodin specialisty na grafiku. Rozhodnutí o finální podobě použité grafiky bude doplněno před zahájením implementace, jako výstup analytické části.
Dále uvádíme příklad takové úpravy:



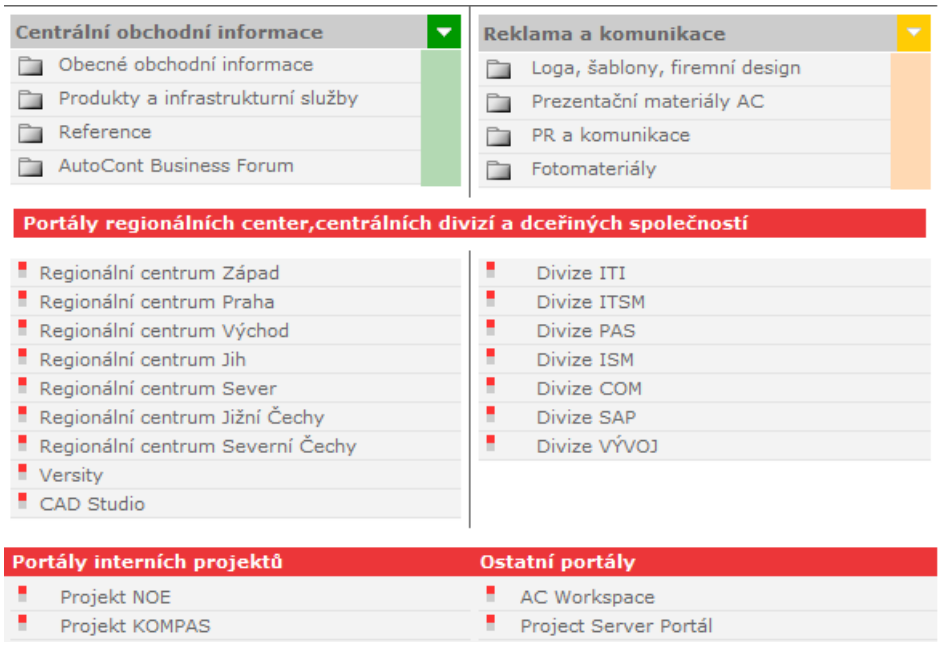
VYTVOŘENÍ PORTÁLOVÉHO ROZCESTNÍKU

Na hlavní stránce předpokládáme vytvoření tzv. portálového rozcestníku, který zjednoduší uživatelům orientaci na portále. Portálový rozcestník bude tvořen sadou objektů tvořících obsah úvodní stránky portálu, které zobrazují důležité informace jako například:

- Novinky organizace,

- Důležité odkazy a odkazy do jednotlivých částí portálu
- Moje naposledy navštívená místa na portále
- Atd.

Příklad rozcestníku je na následujícím obrázku:



VYTVOŘENÍ ZÁKLADNÍ STRUKTURY PORTÁLU, DO KTERÉ BUDE MOŽNÉ INTEGROVAT VYBRANÉ AGENDY

Bude vytvořena základní struktura portálu dle následujících pravidel:

a) ***Oblast týmových webů dle organizačního členění*** - každá organizační jednotka bude mít svůj vlastní prostor v rámci portálu (týmový web), určený pro sdílení informací a dokumentů v rámci jednotky,
b) ***Oblast sdílených prostorů pro informace a dokumenty všeobecného charakteru***,
c) ***Oblast pro sdílení informací projektového typu***, které sdílí uživatelé napříč organizací,
d) **Oblast pro agendy** – zde budou publikovány jednotlivé agendy portálu (žádosti apod.).

Definitivní návrh struktury portálu bude detailně rozpracován v rámci analýzy a návrhu řešení. Odkazy do jednotlivých částí portálu budou reprezentovány v rámci rozcestníku portálu.

NÁVRH A NASTAVENÍ OPRÁVNĚNÍ PŘÍSTUPU DO JEDNOTLIVÝCH ČÁSTÍ PORTÁLU

Součástí návrhu struktury portálu bude i definice distribučních skupin zajišťujících přístupy do jednotlivých částí portálu. Členění těchto skupin se bude odvíjet od rolí uživatelů v jednotlivých částech portálu.

Příklad:

1. Návštěvníci webu XY – právo pouze pro čtení
2. Přispěvatelé webu XY – právo pro čtení a zápis
3. Vlastníci webu XY – pro modifikace a administraci webu

Do těchto skupin budou následně mapovány AD skupiny uživatelů. Tím vznikne matice přístupových oprávnění uživatelů v závislosti na roli uživatele v dané části. Tento princip zároveň zajistí, že nastavení přístupu uživatele na portál bude řešenou pouze začleněním uživatele do patřičných AD skupin, bez

nutnosti definovat přístup pro uživatele přímo na portále. Tento mechanismus zároveň umožní, že případný identity systém, který bude řídit změny v Active directory bude zároveň řídit i přístupy uživatelů na portále.

PROSTŘEDÍ PRO SPRÁVU WEBOVÉHO OBSAHU A DOKUMENTŮ, KTERÉ PRIMÁRNĚ NEPROCHÁZEJÍ PŘES SPISOVOU SLUŽBU A SYSTÉM SPRÁVY METADAT K JEDNOTLIVÝM DOKUMENTŮM

Bude vytvořena agenda „a.Dokumenty“ určená pro sdílení dokumentů, které primárně neprocházejí spisovou službou, přesto je potřeba tyto dokumenty sdílet. Dokumenty budou rozděleny na typy, dle kterých budou definovány metadata k tento typům a principy práce s těmito dokumenty jako je např. sledování změn – verzování, definice pravidel platnosti dokumentů, požadavky na revize a schvalování atd. V rámci implementace bude provedena definice a nastavení vybraných typů dokumentů v jednotlivých dokumentových knihovnách. Součástí dodávky není migrace těchto dokumentů na portál.

NÁVRH PROPOJENÍ PORTÁLU A SPISOVÉ SLUŽBY

V rámci analýzy bude zpracován návrh propojení portálu se spisovou službou, aby např. spisová služba mohla v určité fázi zpracování dokumentu využít např. možnost publikace na portál. Tato komunikace bude řešená prostřednictvím webových služeb nebo specifických konektorů, které budou zajišťovat vzájemnou komunikaci mezi portálem a spisovou službou.

SYSTÉM NA GRAFICKOU TVORBU WORKFLOW A DALŠÍCH POKROČILÝCH VLASTNOSTÍ OBĚHU DOKUMENTŮ, JEJICH NÁVRH A ZOBRAZENÍ

Součástí dodávky portálu bude komponenta pro grafickou tvorbu Workflow – Nintex Workflow 2010 (popis vlastností je uveden výše), která umožní definovat procesy organizace v grafické podobě.
Agenda „a.Žádosti“ v principu umožní připravit formulář žádosti a řídit průběh jejího schvalování prostřednictvím workflow, které po vložení nové žádosti informuje emailem příslušného schvalovatele. Po schválení/zamítnutí žádosti bude žadatel zpětně informován emailem o výsledku. Následně žádost vytváří úkol pro řešitele, aby ji zpracoval. V systému dále jednotlivé žádosti s patřičným stavem (povoleno, zamítnuto) pro evidenci zůstávají. V rámci funkcionality formulářů bude možné využít elektronický podpis, pomocí kterého budou uživatelé autorizovat jednotlivé části formuláře nebo formulář celý. Takto podepsaný formulář potom zajišťuje jednoznačnou identifikaci pravosti vložených dat. Pozn. Funkcionalita elektronického podpisu je podmíněna funkčním systémem správy a evidence el. Certifikátů.
V rámci analýzy bude posouzen současný způsob řešení formulářů a procesů s tím spojených a navrženo využití instalované funkcionality. Budou vytipovány 3 interní žádosti s workflow a 1 vzorová agenda s workflow, které budou v rámci implementace komplexně zpracovány jako vzorové vč. vytvoření formulářů k danému procesu. Typickým příkladem takového procesu může být např. „Žádost o povolení služební cesty“, „Žádanka o materiál“, „Žádost o udělení přístupu k agendě-aplikaci“ a proces „Nástup nového zaměstnance“. Vybrané žádosti-procesy budou v rámci analýzy posouzeny a u vybraných bude navrženo jejich řešení i s ohledem na časovou náročnost řešení.

SYSTÉM PRO ZOBRAZOVÁNÍ DAT A REPORTŮ IMPLEMENTOVANÝCH V OBLASTI ŘEŠENÍ PROJEKTU DATOVÝ SKLAD A BI, PŘÍPADNĚ I REPORTŮ Z DALŠÍCH ZDROJŮ

Součástí dodávky bude i konfigurace služeb SharePoint serveru (Excel services a performance services) a instalace MS SQL server reporting services, pomocí kterých umožníme na portále zobrazovat data z různých zdrojů podporujících napojení přes standardní rozhraní.
Tyto služby umožňují zobrazování informací ve formě tabulek, reportů apod. z různých zdrojů jako jsou např. datové sklady a BI přímo na portále bez nutnosti spouštět zdrojové aplikace.

NÁVAZNOSTI NA OSTATNÍ PRODUKTY A SLUŽBY

Portálové řešení postavené na MS SharePoint serveru umožňuje:

- spolupracovat s identitním systémem, aby přístup uživatelů na portál byl řiditelný prostřednictvím IDM systému resp. prostřednictvím skupin uživatelů viz „*Návrh a nastavení oprávnění přístupu do jednotlivých částí portálu*“;
- integraci aplikací a systémů prostřednictvím definovaného API rozhraní viz. *http://msdn.microsoft.com/en-us/library/dd776256(v=office.12)* ;

- integraci s výstupy části DS a BI – zakomponování reportů/BI výstupů do portálu;

Portál úředníka - Architektura řešení
Cílovým stavem v projektu je provozování portálu včetně integrace GUI se stávajícími intranetovými aplikacemi využívanými v rámci úřadu. Pro řešení bude použito prostředí SharePoint Server 2010. Za tímto účelem bude potřeba naplnit následující infrastrukturní kroky:

- Nainstalovat MS SQL Server.
- Nainstalovat SharePoint 2010 farmu a produkty potřebné pro řešení (Nintex workflow,…).
- Vytvořit Definovat a zprovoznit základní logické členění portálu v rámci SharePoint.
- Zprovoznit základní technologické vlastnosti systému: základní vyhledávání nad daty uloženými ve farmě SharePoint 2010.

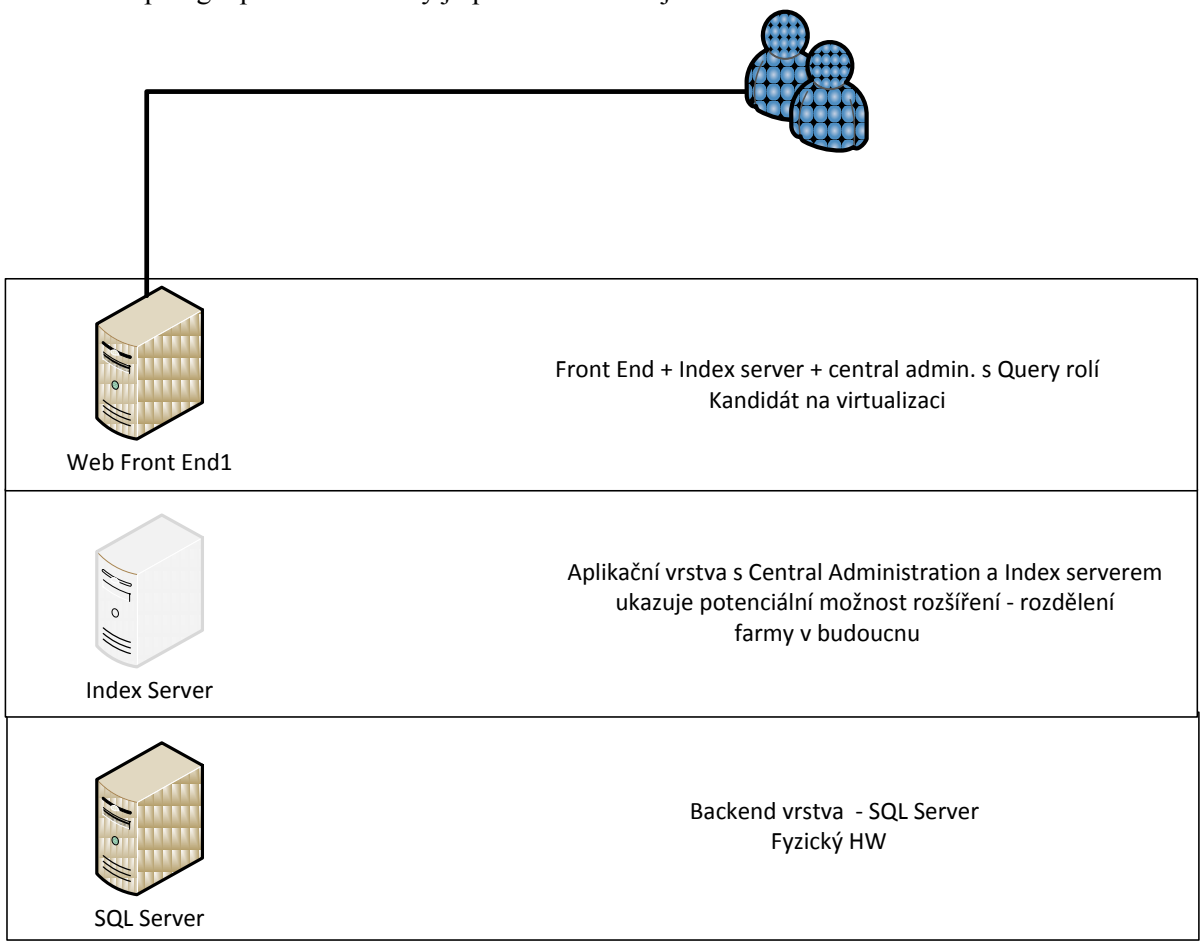
Pro implementaci a následný provoz systému doporučujeme vybudovat 3 prostředí:

1. **Produkční** – určené pro provozování ostré verze portálu. Portál bude publikován na portu 80 na URL http://portal.domena.cz . Detailní adresa vyplyne až z provedené analýzy. V rámci analýzy mohou být specifikovány i další požadavky (např. přístupy, porty,…).
2. **Testovací** – určené pro seznamování a testování uživatelů. Pro tento účel není bezpodmínečně nezbytné budovat samostatnou farmu. Je možné zvláště pro účely testování vytvořit v produkční farmě pouze testovací webovou aplikaci. Nicméně z našich zkušeností doporučujeme takové prostředí vybudovat, protože zvláště při instalaci updatů systému a aplikací provozovaných na portále, je nutné ověřit funkčnost nejprve na testovacím prostředí, jehož konfigurace odpovídá produkčnímu. Pro vybudování takového prostředí je možné využít zvýhodněných licencí v rámci MSDN balíčku aplikací. Testovací prostředí bude obsahovat kopii aplikací provozovaných v produkčním prostředí.
3. **Vývojové** – určené pro vývoj aplikací. Z hlediska tohoto projektu, předpokládáme, že bude pro případný vývoj aplikací použito interní vývojové prostředí AutoContu.

Produkční SharePoint farma bude postavena jako farmové řešení v jedné lokalitě v této topologii:

- Frontend server, Index (Search) server a web centrální administrace v jednom serveru. Instalace typu farma.
- Backend SQL Server

Navržená topologie produkční farmy je patrná z následujícího schématu:



Zálohování farmy bude řešeno nativními nástroji SharePointu popř. SQL serveru, pokud z analýzy nevyplyne možnost použití specializovaného nástroje např. SC DPM 2010 apod. Antivirová ochrana SharePoint farmy bude řešena stávajícím antivirovým produktem úřadu.
Produkční farma bude dostupná uživatelům v interních sítích zákazníka.
Vedle produkčního prostředí bude vybudováno také testovací prostředí pro vývoj aplikací, které bude sloužit k testování a akceptaci aplikací a jejich aktualizací před tím, než budou schváleny pro nasazení v produkčním prostředí. Pro účely vývoje aplikací (napojení na stávající specifické aplikace apod.) bude vybudováno další virtualizované prostředí.
Pro testovací prostředí a prostředí pro vývoj aplikací je doporučena následující konfigurace:

- 1 SharePoint server obsahující všechny role
- 1 SQL server

Analýza vnitřního prostředí a implementace portálu, včetně zajištění zkušebního provozu
Základem našeho řešení je vypracování analýzy oblastí, dle požadavků uvedených v zadávací dokumentaci. Cílem je optimální využití vlastností instalovaných SW komponent vzhledem k současnému stavu informačního systému Objednatele, předpokladům jeho dalšího rozvoje v těchto oblastech, časovým a finančním možnostem projektu. Projekt předpokládá, že infrastruktura pro jeho realizaci je připravena.

ANALÝZA VNITŘNÍHO PROSTŘEDÍ, IMPLEMENTAČNÍ STUDIE

Prvním krokem je zpracování požadované implementační studie. Výsledky studie budou následující:

- Návrh architektury portálu
- Návrh členění portálu.
- Návrh řešení jednotlivých požadovaných oblastí (formulářový systém, …).
- Návrh prováděcího projektu.

- Specifikace úzkých míst a rozsahu řešení.
- Detailní návrh průběhu, jednotlivých kroků implementace, definice zodpovědností a termínů realizace.
- Návrh disaster recovery plánu.

VÝVOJ A IMPLEMENTACE POŽADOVANÝCH APLIKACÍ A FUNKCIONALIT

Tato část je rozdělena na následující kroky:

- **Vývoj funkcionalit a aplikací**.

Autocont má připravené šablonovité řešení jednotlivých požadovaných funkcionalit, které mohou být uzpůsobeny požadavkům vyplývajícím z analýzy. Pro vývoj aplikací máme vytvořené vlastní vývojové prostředí a nástroje, které umožňují sledovat stav řešení jednotlivých požadavků. Ať už vznikají podkladem z analýzy tak i případných bugů. Pro tento účel využíváme produkt *Team foundation server*. Klasický způsob vývoje našich aplikací probíhá prakticky ve sledu:

analýza a návrh –> programování –> testování –> nasazení u zákazníka (údržba).

S důrazem na to, že vývoj jednotlivých oddělených komponent aplikací může probíhat paralelně.

- **Implementace portálu.**

Konfigurace systému a vytvoření základní struktury portálu, využití možností aplikací v oblasti formulářů, rezervací apod. včetně nastavení vybraných schvalovacích postupů a přístupových práv. V analýze bude uveden detailní rozsah nasazených řešení.

- **Seznámení uživatelů a správců**

Pro správce bude obsahovat:

- administrace a údržby portálu
- tvorba a práce s workflow v produktu Nintex
- na tvorbu e-Learning obsahu

Pro uživatele bude obsahovat:

- používání portálu
- práce v dodaných aplikacích

ZKUŠEBNÍ PROVOZ

V rámci zkušebního provozu dojde k ověření funkčnosti VIÚ, případně doladění systému na základě výstupů ze zkušebního provozu.

Během zkušebního provozu je uživatelům poskytována metodická a technická podpora tak, aby zkušební provoz probíhal hladce a úspěšně.

Na konci zkušebního provozu bude provedeno zdokumentování konfigurace a úprav nabízeného řešení a následné předání do ostrého provozu.

TECHNICKÁ PODPORA

V rámci technické podpory po dobu implementačních prací předpokládáme:

- průběžné provádění inovace produktů definovaných v nabídce, zejména legislativního update, legislativního upgrade ve vazbě na vždy aktuálně platné právní předpisy,
- distribuce produktů definovaných v nabídce upraveného za účelem legislativního update nebo legislativního upgrade bude provedena před termínem účinnosti změn právních předpisů,
- poskytování update produktů definovaných v nabídce dle potřeby vzniklé legislativními změnami a požadavky Objednatele či samostatnou, nevynucenou inovační činností Zhotovitele,
- provádění obecných změn produktů definovaných v nabídce v důsledku vývoje HW a SW prostředků.

Portálová řešení bude vytvořeno na technologiích s vysokou mírou standardizace a bude možno jej dále rozvíjet schopnostmi Objednatele. Zhotovitel se zavazuje vyškolit vybrané pracovníky KÚ pro správu a vývoj nových funkcionalit portálu. Portál bude pro pracovníky KÚ přístupný pomocí internetového prohlížeče.
Portálové řešení bude plnit tyto cíle:

- Integrovat vybrané agendy do jednoho uživatelského portálu, který umožní práci s různými webovým a aplikačním obsahem, dokumenty a formuláři.
- Publikovat informace z ostatních aplikací resp. Zdrojů (BI) v prostředí portálu
- Definovat a provozovat různé typy workflow včetně jejich návrhu a zobrazení v systému

Systém bude modulární a umožní další rozšiřování funkcionality vlastními kapacitami úřadu bez nutnosti externí dodávky.
Implementace portálu se bude skládat z:

- Návrhu a designu portálu a jeho realizace
- Vytvoření portálového rozcestníku
- Vytvoření základní struktury portálu, do které bude možné integrovat vybrané agendy
- Vytvoření struktury týmových webů určených pro sdílení informací v rámci jednotlivých odborů úřadu
- Návrh a nastavení oprávnění přístupu do jednotlivých částí portálu
- Prostředí pro správu webového obsahu a dokumentů, které primárně neprocházejí přes spisovou službu.
- Systém správy metadat k jednotlivým dokumentům
- Návrh propojení portálu a spisové služby
- Systém na grafickou tvorbu workflow a dalších pokročilých vlastností oběhu dokumentů, jejich návrh a zobrazení
- Systém pro zobrazení dat a reportů implementovaných v oblasti řešení projektu Datový sklad a BI, případně i reportů z dalších zdrojů

Realizace portálu bude probíhat podle následujícího postupu.
a, Vlastní realizace portálu bude zahrnovat

- Detailní analýzu a návrh řešení, vč. Vypracování detailního harmonogramu nasazení, navržení oblastí řešení a možného budoucího rozvoje
- Instalaci serverové části portálu
- Vytvoření vzorových agend a workflow dle návrhu řešení v minimálním rozsahu
    - 3 interní žádosti s workflow (žádost o povolení služeb cesty, žádost o materiál, žádost o udělení přístupu k agendě-aplikaci)
    - 1 vzorová agenda s workflow (nástup nového zaměstnance)
- Dokumentaci, která je popsána v samostatné kapitole 6.7.1
- Disaster recovery, který je popsán v samostatné kapitole a je řešen standardně přes celý systém integrace.
- Popis údržby systému se bude skládat
    - Backup systému prováděn 1x týden
    - Backup DB prováděn 1x týdně
    - Archivace záloh bude prováděna v rámci TC JMK.
    - *„best practices“* navržené vendorem systému Portálu úředníka

b,Návaznosti na ostatní produkty a služby

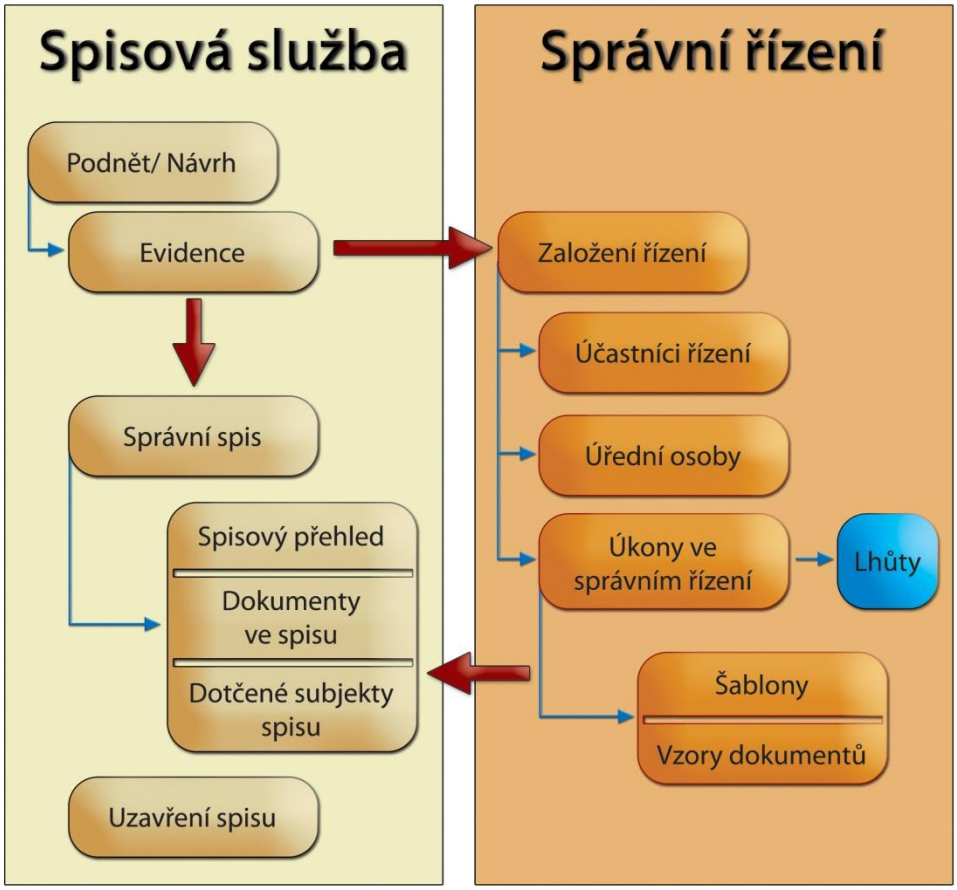
- Portálové řešení bude spolupracovat s IDM systémem. Autentizace do portálu bude probíhat pomocí IDM a jím vystavených služeb. Autentizace a Autorizace k jednotlivým aplikacím bude výsledek kombinací práv na IDM.
- Portálové řešení umožní integraci aplikací a systémů prostřednictvím definovaného API rozhraní
- Portálové řešení umožní integraci s výstupy části DS a BI. Budou zakomponovány reporty a výstupy z BI.

Informační systém pro IT podporu správních řízení na krajském úřadu
Integrace tohoto systému bude probíhat standardním způsobem jako u ostatních integrovaných systémů. Sjednocením postupu integrace a způsobu zacházení se všemi systémy stejně docílíme minimální chybovosti při správě systému a instalování nových verzí/bezpečnostních patchů.

Celková filozofie řešení

Program Správní řízení (SPR) bude společně s programy specializovaných agend nástrojem pro vedení, evidenci, metodickou podporu správního řízení krajského úřadu. V navržené koncepci je program SPR určen k centrální evidenci všech správních řízení, která příslušný správní úřad vede.
Od 1. ledna 2006 probíhají všechna správní řízení probíhat v souladu s tímto zákonem. Novelizovaný správní řád upravuje postup orgánů moci výkonné, orgánů územních samosprávných celků a jiných orgánů, právnických a fyzických osob, pokud vykonávají působnost v oblasti veřejné správy (správních orgánů). Vedle zavedení relativně složitého systému účastenství ve správním řízení, správních lhůt, systému rozhodnutí a usnesení vázaných jak na typ procesního úkonu, tak na osobu adresáta, jakož i dalších podstatných změn, je další novinkou zřízení institutu správního spisu jako součásti systému spisové služby správního úřadu.
Modul GINIS SPR je navržen je v tenké (.NET) technologii. Orientace na tuto platformu byla zvolena zejména pro moderní pojetí její technologie a architektury, která umožňuje okamžitě řešit většinu v současnosti požadavků. Největší předností je nenáročnost aplikace na vybavení pracovní stanice. Může se jednat o počítač s nainstalovaným operačním systémem MS Windows a internetovým prohlížečem MS Internet Explorer (Mozilla Firefox). Toto řešení nenutí uživatelské organizace (příspěvkové organizace) k pořízení nového hardwarového vybavení.

Modul SPR je určen k centrální evidenci všech správních řízení, která příslušný správní úřad vede. Nedílnou součástí navržené koncepce je integrace se subsystémem SSL – spisová služba (komplexní správa dokumentů a spisů). Návrh struktury subsystému SPR umožňuje doplnění (resp. rozšíření) dalších modulů specializovaných agend pro jednotlivé oblasti veřejné správy dle potřeb správního úřadu.



Obr. Schéma vazby spisové služby krajského úřadu a správního řízení

Návrh struktury subsystému SPR umožňuje doplnění (resp. rozšíření) dalších modulů specializovaných agend pro jednotlivé oblasti veřejné správy dle potřeb správního úřadu.

Základními komponenty správního řízení:
- profil správního řízení s napojením na spis;
- registr úředních osob, včetně organizační struktury (pověřená úřední osoba, oprávněná úřední osoba, …);
- registr účastníků řízení s určením jejich postavení v řízení;
- registr dotčených orgánů a jejich vztahu k řízení;
- registr úkonů ve správním řízení včetně vzájemných vazeb, včetně vzorů a formulářů pro jednotlivé úkony;
- lhůtník, ke sledování a vyhodnocování termínů jednotlivých úkonů;
- spisový přehled;
- statistiky, výběry.

Základní funkčnost modulu
- sledovaní, výpočet a vyhodnocování lhůt v řízení;
- nabídka možných procesních postupů v dané fázi správního řízení;
- nabídka možných vzorů a formulářů pro jednotlivé úkony správního řízení;
- tvorba správního spisu, spisového přehledu a dokumentů v něm obsažených;
- integrace se subsystémem spisové služby (SSL);
- integrace se subsystémem ekonomika (EKO).

Moduly specializovaných agend (MSA) generují ať už automaticky nebo za interakce uživatele do subsystému SPR příslušné záznamy, případně umožňují tyto záznamy editovat. Např. při pořizování nového případu do agendy STU – stavební úřad, se nejprve vytvoří spis do subsystému SSL – spisová služba, následně je založen záznam o správním řízení do subsystému SPR – správní řízení a nakonec se provede pořízení nového případu do agendy STU bez nutnosti opakovaně zadávat stejné údaje.

Výstupy
Výstupy z programu jsou především dokumenty formátu MS Word, určené pro zpracování správního řízení. Modul obsahuje sadu formulářů a vzorů pro jednotlivé typy správních řízení, dále pak tiskové sestavy pro vytváření přehledů správních řízení, osob, plateb a dalších evidovaných údajů. Tiskové sestavy lze ukládat v různých formátech pro další využití v rámci správního úřadu.
Moduly jednotlivých specializovaných agend pak obsahují sestavy pro statistická hlášení.
Pro integraci s externími informačními systémy je v systému vytvořeno rozhraní pro webové služby.

Modul SPR – komponenty
Základem řešení je elektronický spis s vazbou na elektronickou spisovou službu. Elektronický spis umožňuje podrobnou chronologickou evidenci správních úkonů a pomáhá logicky a uspořádaně evidovat všechny potřebné údaje týkající se řízení, čímž zlepšuje proces jeho vedení.

Základní komponenty správního řízení v řešení GORDIC®
- profil správního řízení s napojením na spis
- registr oprávněných úředních osob, včetně organizační struktury
- registr účastníků řízení s určením jejich postavení v řízení
- registr dotčených orgánů a jejich vztahu k řízení
- registr úkonů ve správním řízení včetně vzájemných vazeb, včetně vzorů a formulářů pro jednotlivé úkony
- lhůtník, ke sledování a vyhodnocování termínů jednotlivých úkonů
- spisový přehled
- statistiky, výběry

Profilová karta správního řízení
Profil správního řízení s napojením na spis (jedno řízení = jeden spis).

Speciální profilová záložka
- slouží k evidenci položek vztahujících se k příslušnému typu řízení
- je navrhována individuálně pro každý úřad nebo typ řízení

Záložka Oprávněné úřední osoby
- slouží k evidenci oprávněných úředních osob, které mají vazbu na dané řízení
- uvádí postavení OÚO v řízení

Záložky Účastníci řízení
- lze zaznamenat údaje: jazyková práva, znalost jazyka, procesní způsobilost, místo pobytu

Záložka Dotčené orgány
- výběr z kartotéky ESU jednotlivě nebo lze přebírat celé připravené skupiny subjektů
- lze stanovit typ dotčeného orgánu (např. DO – stanovený zákonem).
- viditelnost záložky „Dotčené org.“ lze v administraci zakázat

Záložka Ostatní
- evidence ostatních účastníků (znalec, svědek,….).
- výběr z kartotéky ESU, případně lze založit nový subjekt

Záložka Zástupci
- evidence zástupců účastníků (plná moc, opatrovník,…)

Záložka Spisový přehled

- čerpá data ze spisové služby
- všechny dokumenty (došlé i odeslané), které se vztahují k danému řízení.

Záložka Úkony
- evidence provedených úkonů v rámci daného řízení
- každý úkon má svůj profil

Záložka Dotčené subjekty (vztahují se k úkonu)
- definování subjektů, které se vztahují k úkonu
- výběr z evidovaných subjektů na jednotlivých záložkách – Účastníci, Dotčené subjekty

Tvorba dokumentů
- generování dokumentu výběrem šablony
- automatické doplnění údajů do šablony
- Výsledný dokument je vytvořen dotažením položek do připravené šablony.
- Dokument je vytvořen v MS Word nebo Open Office a lze jej dále upravovat.
- Je uložen do el. úložiště.
- Je připojen k profilu dokumentu jako jeho elektronický obraz.

Odeslání dokumentu
- lze realizovat z detailu úkonu (využívá se služeb SSL)

Záložka Platby
- evidence jednotlivých předpisů a plateb uskutečněných v rámci řízení (pokuty, náklady řízení apod.)

Manažerské sestavy
- tiskové sestavy přehled SŘ dle typu, lhůt, za spisový uzel, oprávněnou úřední osobu
- speciální sestavy – přehled správních poplatků, pokut, nákladů řízení, dle typu rozhodnutí apod.
- tvoří se dle konkrétních požadavků zákazníka

Dokumentace v rámci plnění Integrace
Žadatel předá veškerou technickou, administrátorskou a instalační dokumentaci Objednateli jako podklad pro akceptaci. Dokumentace bude obsahovat popis implementace a způsob provázání systémů, popis

jednotlivých technických detailů k pochopení funkcionality systému. Objednateli bude dodána i dokumentace JBoss Enterprise SOA Platform k dané nainstalované verzi u Objednatele. Administrační dokumentace bude obsahovat postupy jak správně administrovat systém. Bude dále obsahovat seznam vybraných možných technických problémů a návod jak tyto problémy vyřešit. Instalační dokumentace bude obsahovat návod jak správně instalovat systém do ICT Objednatele. Bude obsahovat přesné formulace a proměnné potřebné pro nainstalování v systému Objednatele.

C: Detailní popis řešení - Elektronická spisová služba JMK

Popis funkcionality elektronické spisové služby

Splnění požadavků řešení dle studie proveditelnosti
Splnění požadavků dle Přílohy č. 4 zadávací dokumentace „Technické požadavky a minimální požadované funkce pro část B veřejné zakázky“.
Tabulkový přehled obsahuje výčet požadavků, které má splňovat řešení hostované elektronické spisové služby Královéhradeckého kraje podle studie proveditelnosti. Vedle každého požadavku je uvedeno buď ANO, v případě, že nabízené řešení danému požadavku vyhovuje, či NE, v případě, že nikoli.

OBECNÉ POŽADAVKY

Požadavek	**Řešení splňuje**
Nabídka a řešení plně vyhovuje výzvě č. 8 Integrovaného operačního programu na Rozvoj eGovermentu v krajích	ANO
Soulad s platnou legislativou pro oblast archivnictví a spisové služby, zejména s těmito předpisy:	ANO
Zákon č. 499/2004 Sb., o archivnictví a spisové službě, ve znění pozdějších předpisů	ANO
Vyhláška MV č. 191/2009 Sb., o podrobnostech výkonu spisové služby	ANO
Zákon č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů, ve znění pozdějších předpisů	ANO
Vyhláška MV č. 193/2009 Sb., o stanovení podrobností provádění autorizované konverze dokumentů	ANO
Vyhláška MV č. 194/2009 Sb., o stanovení podrobností užívání a provozování informačního systému datových schránek	ANO
Národní standard pro elektronické systémy spisové služby	ANO
Zákon č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů (zákon o elektronickém podpisu), ve znění pozdějších předpisů	ANO
Vyhláška MI č. 496/2004 Sb., o elektronických podatelnách	ANO
Shoda spisové služby s mezinárodním standardem ISO 15489	ANO
Objednatel má právo udělit podlicenci zřizovaným organizacím Královéhradeckého kraje nebo obcím I. a II. typu	ANO
Podpora bude dostupná v rámci Královéhradeckého kraje	ANO

ORGANIZAČNÍ POŽADAVKY

Požadavek	Řešení splňuje
Návrh modelů migrace spisové služby z centrálního hostingu do lokálního prostředí organizace včetně metodiky pro administrátory	ANO součástí nabídky, kapitola 5.3.1
Návrh typové metodiky implementace	ANO, součástí nabídky, kapitola 5.3.2
Návrh struktury a organizace seznámení uživatelů	ANO, součástí nabídky, kapitola 5.3.3

TECHNICKÉ POŽADAVKY

Požadavek	Řešení splňuje
Rovnocenný přístup k analogovým a digitálním dokumentům	ANO
Modulárnost a škálovatelnost systému	ANO
Použití jednoznačných identifikátorů dokumentů	ANO

Plnohodnotná podpora komunikace dodaného řešení s informačním systémem datových schránek	ANO
Přihlášení do datové schránky organizace pomocí spisové služby jménem a heslem a systémovým certifikátem	ANO
Příjem, uložení a evidence došlých datových zpráv	ANO
Odesílání datových zpráv a jejich uložení	ANO
Příjem oznámení o dodání datové zprávy do datové schránky adresáta	ANO
Příjem a uložení doručenky odeslané datové zprávy	ANO

Možnost integrace s DMS	ANO
Zabezpečený přenos dat	ANO
Otevřené komunikační rozhraní pro externí systémy (na principu webových služeb)	ANO
Podpora migrace popř. oddělení jednotlivých organizací (např. do lokální instance)	ANO
Možnost centrální i delegované administrace	ANO
Podpora předávání dokumentů a spisů dle modelu OAIS (rozhraní Národního digitálního archivu)	ANO
Zajištění kompletního životního cyklu dokumentů (viz 5.1.4 Minimální požadované funkce systému elektronické spisové služby)	ANO
Řešení el. podatelny, el. spisovny a el. výpravny	ANO
Podepisování elektronických dokumentů zaručeným elektronickým podpisem založeným na kvalifikovaném certifikátu včetně možnosti vícenásobného podepisování	ANO
Elektronická podpisová kniha	ANO
Používání kvalifikovaných časových razítek	ANO
Oddělitelnost archivu dokumentů od databáze	ANO
Podpora plnohodnotné historizace a logování přístupů	ANO
Podpora provozu serverové části ve virtuálním prostředí	ANO
Možnost uživatelských změn (zejména sestavy a šablony)	ANO
Rozhraní na systém Czech POINT	ANO
Zabezpečení komunikace s krajskou digitální spisovnou, která bude definována a zprovozněna v rámci jiných projektů IOP (Zhotovitel se zavazuje ke zprovoznění komunikace s krajskou digitální spisovnou)	ANO

Možnost integrace s Active Directory	ANO
Implementace produktu v třívrstvé architektuře klient, aplikační server, databázový server. Jednotlivé vrstvy musí splňovat kritéria zajišťující kompatibilitu se současnou architekturou IS KU: Vrstva klienta	ANO
V případě přístupu přes běžný webový prohlížeč je vyžadována podpora min. IE, FireFox a Opera v posledních verzích	ANO Opera-ne

V případě, že navrhované řešení vyžaduje instalaci klienta spouštěného na koncové stanici, musí tento vyhovovat následujícím požadavkům:	
Kompatibilita s OS Windows XP a vyšší ve verzi x32 i x64	ANO
Klienta bude možné spouštět z lokálního disku i ze sdíleného prostoru organizace	ANO
Pro plnou funkci klienta bude postačovat přístupové oprávnění k instalovaným souborům pro čtení bez možnosti zápisu. Pokud bude klient vyžadovat zápis na klientské PC, bude využita pouze složka v uživatelském profilu.	ANO
Klient bude při spuštění automaticky kontrolovat aktuálnost proti příslušnému aplikačnímu serveru. Pokud nebude možné provést při spuštění klienta automatickou aktualizaci, bude uživatel upozorněn na nutnost aktualizovat. Další možností bude centrální aktualizace prostřednictvím naplánované úlohy na místním serveru organizace a manuální aktualizace stažením souborů z centrálního distribučního místa. Aktualizace musí být funkční i při přístupu k Internetu prostřednictvím libovolného proxy serveru.	ANO

Přístup k aplikačnímu serveru pomocí zabezpečeného protokolu HTTPS případně VPN, funkční i při přístupu k Internetu prostřednictvím libovolného proxy serveru	ANO

Vrstva aplikačního serveru	
Podporován bude aplikační server implementovaný na fyzickém HW i ve virtualizovaném prostředí VMware a Hyper-V, s možností využití funkcí automatizovaného či manuálního přenosu spuštěného virtualizovaného serveru v rámci virtuální farmy	ANO
Předpokládané parametry aplikačního serveru v cílové virtualizované infrastruktuře (TC K): CPU min. 2x2.0GHz 64 bit, min. 64GB RAM, SAS disky připojené prostřednictvím SAN. Server provozovaný v režimu vysoké dostupnosti. Pro provoz aplikačního serveru se předpokládá využití maximálně jednoho virtuálního serveru. HW omezení dle využitého hypervizoru (VMware, Hyper-V). Přidělená dynamická paměť pro server max. 8GB, virtualizované disky, síťový provoz na virtualizovaném síťovém rozhraní.	ANO
Parametry aplikačního serveru pro dočasné řešení v případě, že v době implementace nebude k dispozici cílová virtualizovaná infrastruktura TCK: Microsoft Windows Server 2008 R2 Standard Edition; 1x CPU 4Core Xeon E5530, 2,39 GHz/1333 MHz FSB, podpora EM64T; 2x 146GB SAS 15k HDD; RAM 8GB.	ANO
Aplikačním serverem bude služba IIS provozovaná v operačním systému Windows 2008R2 s technologií .NET Framework. Přístup k aplikačnímu serveru bude pouze prostřednictvím HTTPS protokolu a to buď k webovým stránkám, nebo k webovým službám.	ANO
Aplikace nebude chráněna HW klíčem či jiným mechanizmem, který by znemožňoval přenos serverových instancí v rámci virtuálního uzlu se zachováním funkčnosti aplikace (např. vázán na konkrétní HW apod.)	ANO
Aplikace musí umožňovat logovaní přidělených uživatelských oprávnění, logování svého provozu a debug log	ANO
V oblasti zpracování osobních údajů bude aplikace vyhovovat požadavkům	ANO

zákona č. 101/2000 Sb., o ochraně osobních údajů	
Aktualizace serverových komponent bude probíhat centrálně	ANO

Vrstva databázového serveru	
Podporován bude databázový server implementovaný na fyzickém HW i ve virtualizovaném prostředí VMware a Hyper-V, s možností využití funkcí automatizovaného či manuálního přenosu spuštěného virtualizovaného serveru v rámci virtuální farmy	ANO
Předpokládané parametry databázového serveru v cílové virtualizované infrastruktuře (TC K): CPU 2x2.2GHz 64 bit, min. 64GB RAM, SAS disky připojené prostřednictvím SAN. Server provozovaný v režimu vysoké dostupnosti. Virtuálnímu serveru budou přidělené HW prostředky dle možností hypervizoru (VMware, Hyper-V), maximálně 8 vCPU, dynamická paměť max. 16GB, virtualizované disky, síťový provoz na virtualizovaném síťovém rozhraní. Virtuální server bude provozován v Microsoft 2008R2 clusteru. Databázový server bude MS SQL 2008 per CPU, provozován v režimu aktive-pasive cluster.	ANO
Parametry databázového serveru pro dočasné řešení v případě, že v době implementace nebude k dispozici cílová virtualizovaná infrastruktura TCK: Microsoft Windows Server 2008 R2 Standard Edition; 1x CPU 4Core Xeon E5530, 2,39 GHz/1333 MHz FSB, podpora EM64T; 2 x 146GB SAS 15k HDD; RAM 8GB	ANO
Bude implementována na OS Windows 2008R2 a databázovým serverem bude MS SQL 2008 a vyšší licencován na CPU	ANO
Přístup k databázovému serveru bude realizován pomocí TCP/IP protokolu a ověřování bude podporováno jak na úrovni SQL serveru, tak na úrovni Windows ověření. Účet bude mít k dispozici pouze přístup do vytvořené databáze, vlastníky objektů bude DBO. Jméno databáze a vytvoření a případná změna připojovacího řetězce k databázi bude v kompetenci Objednatele.	ANO
Pokud v průběhu provozu produktu bude třeba z důvodu zálohování zajistit zmenšení velikosti databáze produktu, zavazuje se Zhotovitel dodat v rámci poskytované technické podpory a údržby takovou úpravu produktu, která umožní rozdělení databáze na archívní databázi přístupnou pouze pro čtení a produkční databázi	ANO
Zálohování a údržba bude prováděna pouze prostředky databázového serveru	ANO
Aktualizace databází bude řešena centrálně	ANO

MINIMÁLNÍ POŽADOVANÉ FUNKCE SYSTÉMU ELEKTRONICKÉ SPISOVÉ SLUŽBY

Požadavek	**Řešení splňuje**

Příjem a evidence doručených i vlastních dokumentů	ANO
Evidence doručených i vlastních listinných dokumentů	ANO
Zobrazení a uschování zpráv doručených do datové schránky a elektronické podatelny	ANO
Označení dokumentů evidenčním číslem a číslem jednacím	ANO
Vedení podacího deníku	ANO

Oběh a vyřizování dokumentů – evidence předání a převzetí	ANO
Sledování stavu vyřízení a uzavření dokumentů	ANO
Práce se spisy a uzavírání spisů	ANO

Práce s elektronickými dokumenty – vložení, zobrazení a editace elektronických dokumentů	ANO
Ukládání elektronických dokumentů způsobem zaručujícím věrohodnost	ANO

původu dokumentu, neporušitelnost jeho obsahu a čitelnost dokumentu	
Automatická kontrola a doplňování časových razítek a elektronických značek dle požadavků zákona	ANO
Elektronické podpisy (podepsání souboru, ověření podpisu)	ANO
Převádění dokumentu v analogové podobě na dokument v digitální podobě a naopak (neautorizovaná konverze dokumentů)	ANO
Integrovaná konverze dokumentů do ukládacího nebo výstupního datového formátu	ANO

Odesílání listinných i elektronických dokumentů	ANO
Odesílání dokumentů v listinné podobě (pošta, kurýr aj.)	ANO
Odesílání dokumentů v elektronické formě elektronickou podatelnou a do datové schránky	ANO
Evidence doručení dokumentu v listinné podobě	ANO
Evidence doručení a data dodání datovou schránkou	ANO

Vyřízení a uzavření	ANO
Vyřízení a uzavření spisů a dokumentů	ANO

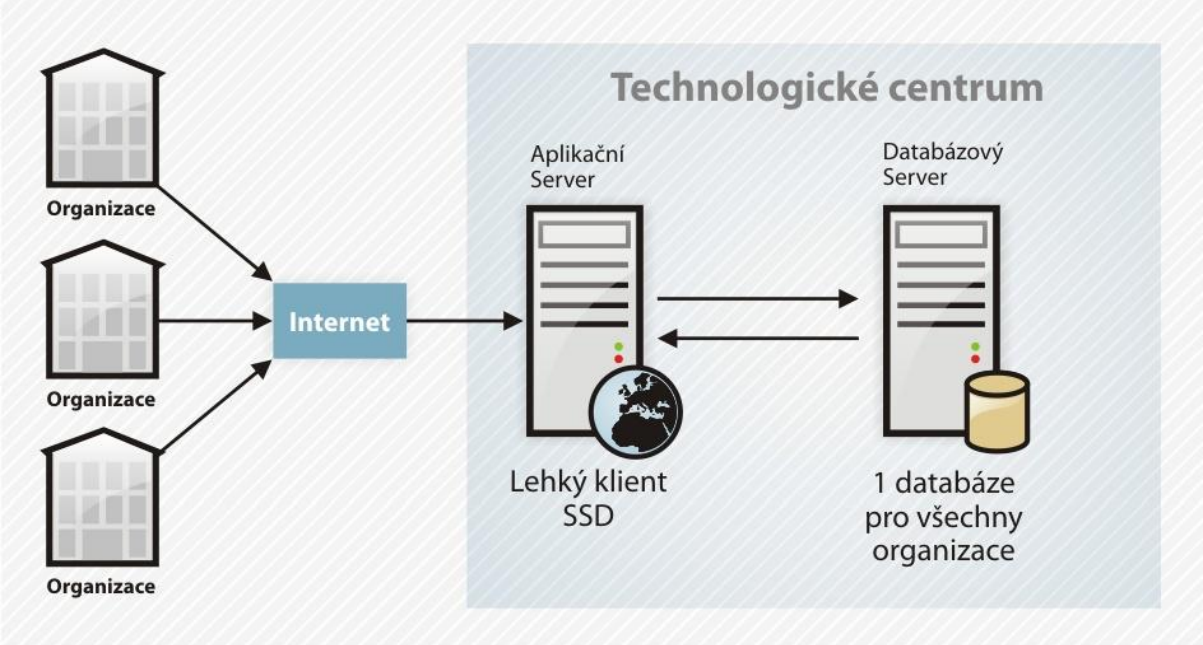
Ukládání a skartace – evidence skartačních znaků a lhůt	ANO
Ukládání spisů a dokumentů	ANO
Podpora skartačního řízení pro listinné i elektronické dokumenty	ANO
Předávání spisů a uzavřených dokumentů do krajské digitální spisovny	ANO

Požadavky na integraci s datovými schránkami	ANO
Plná integrace s datovými schránkami (dopad implementace datových schránek do chodu organizace, tj. dopad zákona č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů, a zákona č. 301/2008 Sb., kterým se mění některé zákony v souvislosti s přijetím zákona o elektronických úkonech a autorizované konverzi dokumentů - projekt MV ČR „Datové schránky“)	ANO
Shoda s platnou legislativou, nároky kladené na systémy Objednatele, a její současná i budoucí údržba, zejména respektování vydaných národních standardů a rozhraní za účelem ukládání dokumentů	ANO
Součástí dodaného řešení musí být i dokumentace a kompletní popis API rozhraní dodávaného produktu pro budoucí integraci s dalšími systémy	ANO

Popis řešení hostované spisové služby
Nejvhodnější variantou řešení je hostování služeb spisové služby pro organizace centrálně v technologickém centru.
Licence pro zakládané, zřizované organizace a obce ve správním obvodu jsou pořízeny úřadem, který může udělit jednotlivým organizacím podlicenci. Tyto organizace jsou pak klienty systému, kdy podlicence a služba zajištění provozu po dobu udržitelnosti projektu jsou organizacím zajištěny centrálně.

Jako navrhovaný a ideální je způsob administrace spisové služby pro organizace variantou jedné databáze pro příspěvkové organizace s vnitřním dělením podle IČ. Pokud bude požadavek na samostatné databáze pro jednotlivá IČ, je možno toto nastavení taktéž realizovat.

Obr.: Konfigurace komunikace organizací se spisovou službou umístěnou v rámci technologického centra



Návrh řešení vychází z využití softwarového vybavení systému GINIS® SSD, jehož jednoduchost a srozumitelnost pomůže organizacím splnit zákonnou povinnost vedení spisové služby včetně nároků kladených v dalších fázích elektronizace veřejné správy.

DETAILNÍ POPIS ŘEŠENÍ

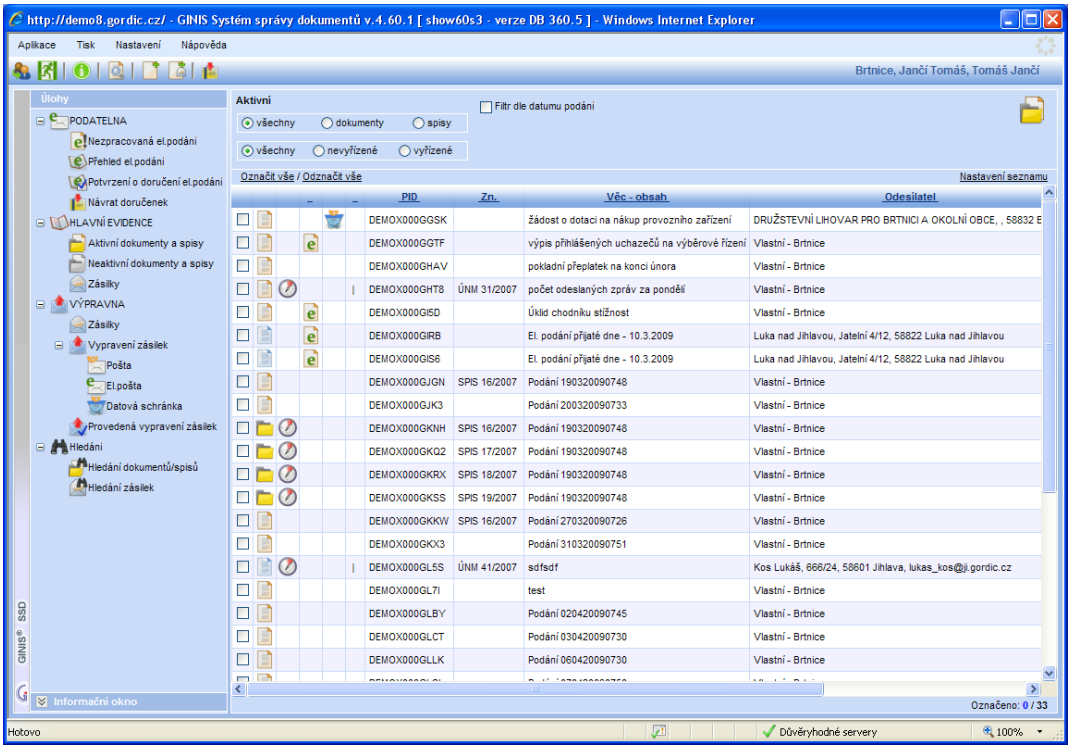
Navrhovaný systém GINIS® SSD umožňuje práci jak s fyzickými (např. papírovými) dokumenty, tak i s elektronickými (eDMS). Integrace s běžným kancelářským prostředím (MS Office, OpenOffice) umožňuje uživateli rychlou evidenci datové zprávy z DS i odeslání dokumentu do DS, automatický export dat do formulářů, např. MS Word, možnost vstupu a evidence digitalizovaných dokumentů ze skenovací linky atp.

Systém správy dokumentů umožňuje evidenci veškerých údajů o písemnostech i spisech včetně sledování pohybu dokumentů v organizaci. Je určen pro **kompletní správu dokumentů** v organizaci. Systém činnosti spisové služby firmy GORDIC® plně vyhovuje aktuálně platným legislativním normám.
Údaje o jednotlivých dokumentech se do systému pořizují ručním zadáváním nebo lze načíst data z jiných programů (systémů). Oběh jednotlivých dokumentů mezi moduly spisové služby je závislý na vykonávaném procesu (předání k vyřízení, stornování, vrácení k doplnění, předání do před archivní péče…), který je řízen **metodikou spisové služby a interními normami organizace** (zejména spisovým a skartačním řádem). Každý dokument je při počáteční evidenci označen prvotním identifikátorem (čárový kód), pod kterým lze následně vysledovat oběh dokumentu v organizaci. Dokument lze tímto identifikátorem označit fyzicky (nalepením kódu samolepky na dopis, fakturu…) nebo se kód vygeneruje a k dokumentu je přiřazen v elektronické podobě (např. evidence elektronických dokumentů, dokumenty z datových schránek, skenované dokumenty).

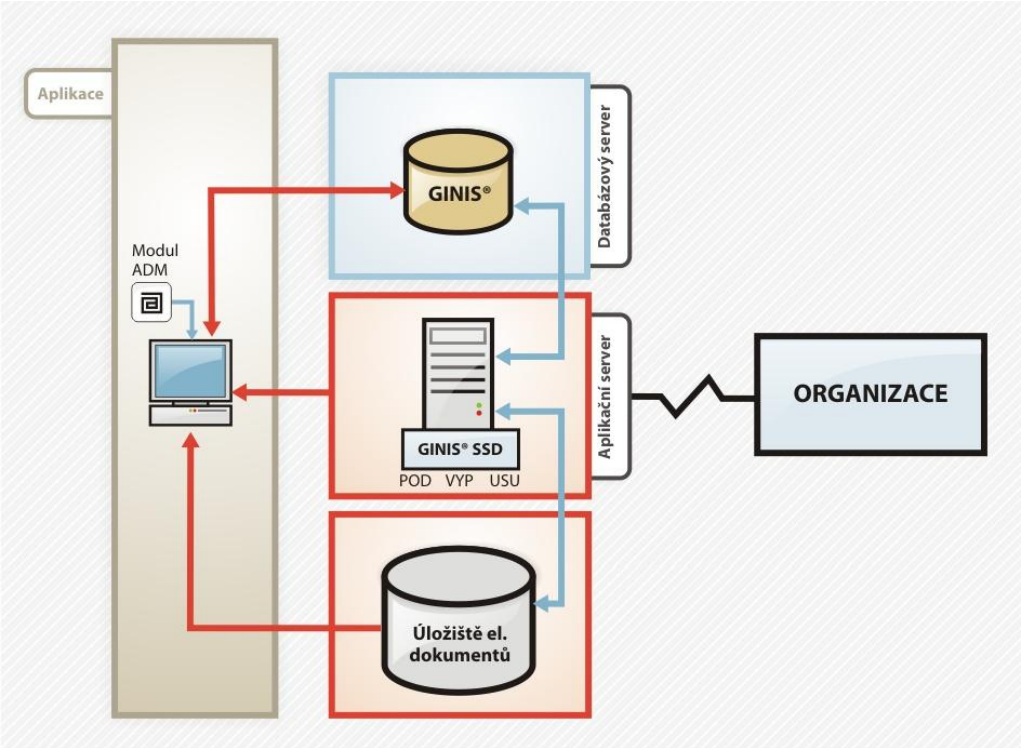
Rozsah modulu GINIS® SSD sdružuje 4 moduly spisové služby do jednoho řešení:
USU – Univerzální spisový uzel (vyřizování dokumentů, tvorba spisů, odesílání, redistribuce…)
POD – Podatelna (příjem podání, evidence a předávání dokumentů směrem do organizace…)
VYP – Výpravna (příjem a vypravení zásilek, tisk předávacích protokolů…)
SPI – Spisovna (ukládání dokumentů, spisů, skartační návrhy…)

Základem řešení je formalizovaná konfigurace organizací v jedné databázi ORACLE nebo MS SQL umístěné na HW vybavení úřadu. Každá organizace bude přistupovat k této centrální databázi pomocí lite klientů umístěných na aplikačních serverech úřadu. Konfigurace těchto klientů bude nastavena pro každou organizaci zvlášť a to zejména s ohledem na rozložení.

Hlavní evidence


http://demo8.gordic.cz/ - GINIS Systém správy dokumentů v.4.60.1 [show60s3 - verze DB 360.5] - Windows Internet Explorer
Aplikace
Tisk
Nastavení
Nápověda
Brtnice, Jančí Tomáš, Tomáš Jančí
Úlohy
PODATELNA
Nezpracovaná el.podání
Přehled el.podání
Potvrzení o doručení el.podání
Návrat doručenek
HLAVNÍ EVIDENCE
Aktivní dokumenty a spisy
Neaktivní dokumenty a spisy
Zásilky
VÝPRAVNA
Zásilky
Vypravení zásilek
Pošta
El.pošta
Datová schránka
Provedená vypravení zásilek
Hledání
Hledání dokumentů/spisů
Hledání zásilek
GINIS® SSD
Informační okno
Aktivní
všechny
dokumenty
spisy
všechny
nevyřízené
vyřízené
Filtr dle datumu podání
Označit vše / Odznačit vše
Nastavení seznamu
PID
Zn.
Věc - obsah
Odesílatel
DEMOX000GGSK
žádost o dotaci na nákup provozního zařízení
DRUŽSTEVNÍ LIHOVAR PRO BRTNICI A OKOLNÍ OBCE, , 58832 E
DEMOX000GGTF
výpis přihlášených uchazečů na výběrové řízení
Vlastní - Brtnice
DEMOX000GHAV
pokladní přeplatek na konci února
Vlastní - Brtnice
DEMOX000GHT8
ÚNM 31/2007
počet odeslaných zpráv za pondělí
Vlastní - Brtnice
DEMOX000GI5D
Úklid chodníku stížnost
Vlastní - Brtnice
DEMOX000GIRB
El. podání přijaté dne - 10.3.2009
Luka nad Jihlavou, Jatelní 4/12, 58822 Luka nad Jihlavou
DEMOX000GIS6
El. podání přijaté dne - 10.3.2009
Luka nad Jihlavou, Jatelní 4/12, 58822 Luka nad Jihlavou
DEMOX000GJGN
SPIS 16/2007
Podání 190320090748
Vlastní - Brtnice
DEMOX000GJK3
Podání 200320090733
Vlastní - Brtnice
DEMOX000GKNH
SPIS 16/2007
Podání 190320090748
Vlastní - Brtnice
DEMOX000GKQ2
SPIS 17/2007
Podání 190320090748
Vlastní - Brtnice
DEMOX000GKRX
SPIS 18/2007
Podání 190320090748
Vlastní - Brtnice
DEMOX000GKSS
SPIS 19/2007
Podání 190320090748
Vlastní - Brtnice
DEMOX000GKKW
SPIS 16/2007
Podání 270320090726
Vlastní - Brtnice
DEMOX000GKX3
Podání 310320090751
Vlastní - Brtnice
DEMOX000GL5S
ÚNM 41/2007
sdfsdf
Kos Lukáš, 666/24, 58601 Jihlava, lukas_kos@ji.gordic.cz
DEMOX000GL7I
test
Vlastní - Brtnice
DEMOX000GLBY
Podání 020420090745
Vlastní - Brtnice
DEMOX000GLCT
Podání 030420090730
Vlastní - Brtnice
DEMOX000GLLK
Podání 060420090730
Vlastní - Brtnice
Označeno: 0 / 33
Hotovo
Důvěryhodné servery
100%

Obr.: Konfigurace komunikace DB s úložištěm a aplikačním serverem



Modul SSD je v tenké (.NET) technologii
Orientace na platformu .NET byla zvolena zejména pro moderní pojetí její technologie a architektury, která umožňuje okamžitě řešit většinu požadavků kladených v současnosti na produkty GINIS®. **Největší předností je nenáročnost na vybavení pracovní stanice.** Může se jednat o počítač s nainstalovaným operačním systémem MS Windows a internetovým prohlížečem MS Internet Explorer (Mozilla FireFox). Toto řešení nenutí uživatelské organizace (příspěvkové organizace) k pořízení nového hardwarového vybavení.

Základní funkce systému GINIS® SSD
Systém GINIS® SSD vyhovuje aktuální novele zákona č. 499/2004 Sb., o archivnictví a spisové službě, včetně prováděcích vyhlášek a zákona č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů.

Mezi klíčové vlastnosti modulu patří:
Plná integrace s datovými schránkami (dopad zákona č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů, a zákona č. 301/2008 Sb., kterým se mění některé zákony v souvislosti s přijetím zákona o elektronických úkonech a autorizované konverzi dokumentů – projekt MV ČR „Datové schránky“)

Příjem a evidence listinných i elektronických dokumentů, vlastních i doručených
Zobrazení zpráv doručených do datové schránky a elektronické podatelny
Vytvoření dokumentu ze zprávy doručené do datové schránky nebo elektronické podatelny
Označení dokumentů evidenčním číslem a číslem jednacím
Vedení podacího deníku

Oběh a vyřizování dokumentů – evidence předání a převzetí
Sledování stavu vyřízení dokumentů
Práce se spisy a uzavírání spisů

Práce s elektronickými dokumenty – vložení, zobrazení a editace elektronických dokumentů
Ukládání elektronických dokumentů způsobem zaručujícím věrohodnost původu dokumentu, neporušitelnost jeho obsahu a čitelnost dokumentu

Automatická kontrola a doplňování časových razítek a elektronických značek dle požadavků zákona
Elektronické podpisy (podepsání souboru, ověření podpisu)
Převádění dokumentu v analogové podobě na dokument v digitální podobě a naopak

Odesílání listinných i elektronických dokumentů
Odesílání dokumentů poštou, elektronickou poštou a datovou schránkou
Evidence doručení dokumentu
Automatická evidence dodejky z datové schránky

Vyřízení a uzavření
Ukládání a skartace – evidence skartačních znaků a lhůt
Ukládání spisů a dokumentů
Podpora skartačního řízení pro papírové i elektronické dokumenty

Předávání spisů a uzavřených dokumentů do e-spisovny
Převod elektronického dokumentu do formátu PDF/A za použití externího konvertoru (PDF Creator, ADOBE Lifecycle, Print2PDF atp.)
Podepisování elektronických dokumentů PDF/A zaručeným elektronickým podpisem založeným na kvalifikovaném certifikátu
Používání kvalifikovaných časových razítek

Další vlastnosti:
Dokumentace a kompletní popis dodaných API rozhraní pro integraci s dalšími systémy
Možnost provozu serverové části ve virtuálním prostředí
Otevřené komunikační rozhraní pro externí informační systémy (webové služby)
Přístup prostřednictvím webového rozhraní
Podpora logického oddělení jednotlivých organizací v rámci databáze i samostatných databází pro jednotlivé organizace (každá organizace vlastní databázi)
Provádění autorizované konverze z moci úřední (z datové zprávy do listinné podoby i naopak)
Shoda s platnou legislativou, nároky kladené na systémy Objednatele a její současná i budoucí údržba, zejména respektování vydaných národních standardů a rozhraní za účelem ukládání dokumentů

ÚLOŽIŠTĚ ELEKTRONICKÝCH DOKUMENTŮ

Všechna data systému GINIS® SSD jsou ukládána do jedné databáze typu SQL. Jedinou výjimkou je ukládání elektronických dokumentů ve formě počítačových souborů. Tyto elektronické dokumenty jsou v systému GINIS® SSD užity jako elektronické obrazy evidovaných dokumentů nebo jako elektronické přílohy těchto dokumentů.

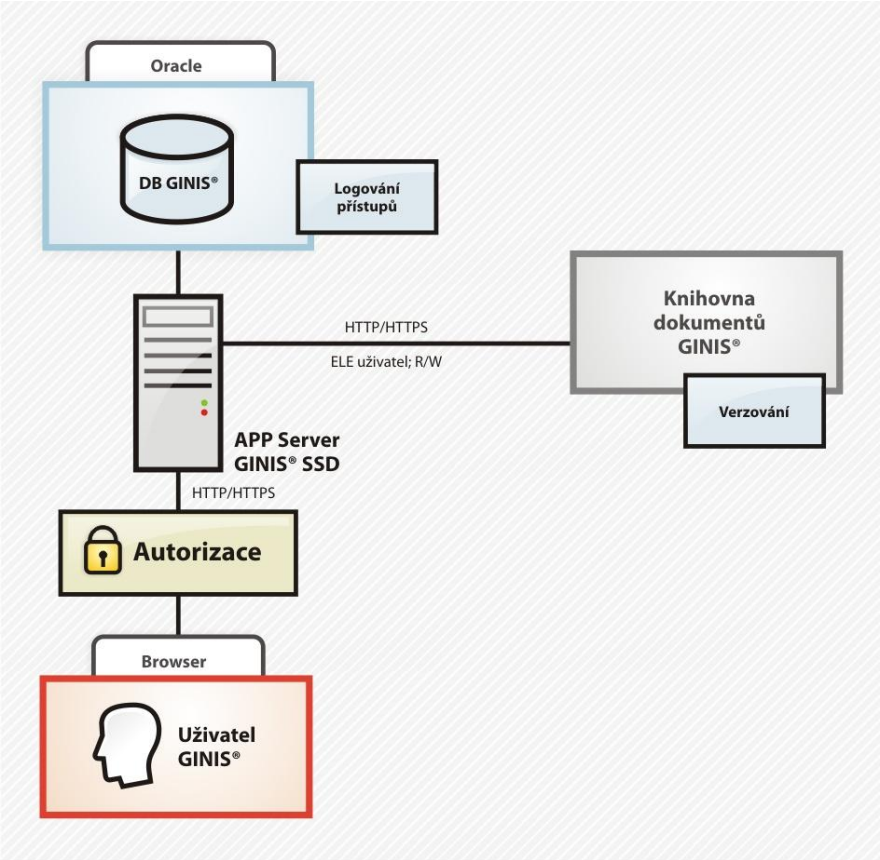
Protože se může v průběhu času jednat o velmi značné objemy dat, jsou tyto soubory ukládány mimo SQL databázi, a to do elektronického úložiště FTP (SFTP), FileNet, Microsoft SharePoint.

Hlavním důvodem tohoto řešení je eliminace případných rizik při provozním zálohování a obnově SQL databáze. Při objemech dokumentů, které mohou být časem uloženy do elektronického úložiště, by mohl čas potřebný k obnově databáze ze zálohy obsahující i elektronické dokumenty přesáhnout přijatelnou mez nutnou pro znovuuvedení informačního systému do provozuschopného stavu např. po případné havárii hardware.

Fyzické oddělení strukturovaných dat popisujících dokumenty uložených v SQL databázi a elektronických obrazů těchto dokumentů ale klade určité nároky na organizaci bezpečného provozování systému jako celku.

Klíčovou otázkou bezpečnosti je spolehlivé zálohování obsahu elektronických úložišť.

Obr.: Vazba úložiště elektronických dokumentů



Administrace – jádro systému GINIS®

ADM – Administrace základní

Administrace (společná pro celý systém GINIS®) je určena k nastavení a průběžné aktualizaci celého systému i jednotlivých subsystémů dle požadavků uživatele.

V rámci administrace systému se provádí evidence několika základních oblastí dat, která jsou ukládána do systému v rámci jednotlivých administračních úkonů:

- definice organizační struktury uživatele až do úrovně funkcí včetně osob na daných funkcích a vstupních práv do systému
- definice fází modulů nastavením jednotlivých parametrů a uživatelských práv pro každý modul, seskupení modulů do konfiguračních skupin a přiřazení jednotlivých funkcí do definovaných konfiguračních skupin
- definice zodpovědností a přístupových práv
- předplnění systémových číselníků pošt, bank, konstantních symbolů, bankovních spojení, typů písemností atp.
- definice číselníku spisových znaků
- definice evidenčních knih pro agendy, přiřazení přístupu jednotlivých funkcí (uživatelů) ke knihám
- definice spustitelných výstupních sestav
- definice spisových uzlů a středisek spisových uzlů (vhodné pro využití více organizací v jedné DB)
- naplnění dalších údajů potřebných pro správnou funkci subsystému GINIS®

ADK – Administrace kartotéky externích subjektů

Ve všech modulech s přístupnou kartotékou externích subjektů systém GINIS® umožňuje **využívat a nově vytvářet adresář externích subjektů.** Modul ADK slouží především k opravám chybných, neúplných a opakujících se záznamů externích subjektů, sdružování souvisejících externích subjektů, změnám jejich aktivity atp.

ADS – Administrace sestav

Firmou GORDIC®, spol. s r. o. jsou dodávány kompletní distribuční balíky sestav, obsahující řídící soubory tiskových sestav, které jsou přiřazeny do pevně definovaných distribučních stromů sestav pro každé tiskové téma. Ke každému tiskovému tématu může existovat libovolné množství sestav.

Administrace
V rámci efektivnosti správy a provozu aplikace hostované spisové služby je možné povolit konkrétní osobě správu uživatelských účtů a uživatelsky definovaných číselníků přímo z prostředí aplikace SSD.

Webové služby rozhraní XRG
Integrační platforma **GINIS® disponuje desítkami hotových webových služeb**, které jsou kategorizovány a dodávány ve skupinách podle okruhu zaměření jejich činnosti. Tímto okruhem se zpravidla rozumí vazba rozhraní na konkrétní agendu informačního systému GINIS®. I zde ovšem platí, že prezentovaný výčet kategorií webových služeb XRG, jakož i jím reprezentované penzum funkčnosti umístěné v jednotlivých interně zakomponovaných webových metodách, jsou neustále aktualizovány a rozšiřovány tak, aby reagovaly na okamžité požadavky měnících se integračních potřeb provozující organizace.

Životaschopnost a efektivita této koncepce rozhraní byla ověřena v řadě integračních projektů při propojení systému GINIS® s dalšími informačními systémy jiných Zhotovitelů. Webové služby XRG prokázaly, že výraznou měrou usnadňují sdílení dat mezi uživateli i integraci informačních procesů v organizacích, a to skutečně bez ohledu na jejich topologické uspořádání nebo existující technologická omezení.

Detailní popis řešení - Datové sklady, manažerské informační systémy a nástroje Business Inteligence JMK

Nabídka reflektuje hluboké a dlouholetou praxí ověřené znalosti a zkušenosti společnosti GORDIC, spol. s r.o. v technologické i metodické oblasti datových skladů (DS) a Business Intelligence (BI) v oblasti veřejné správy, zvláště u územních samosprávných celků.

Nabídka pokrývá veškeré požadavky vyplývající ze zadávací dokumentace ohledně datových skladů a Business Intelligence:

- vytvoření jednotné robustní datové základny strukturovaných údajů pro potřeby hlubší analýzy a hledání vzájemných souvislostí v získaných datech,
- provedení Analýzy a návrhu datového skladu a realizace datových tržišť a BI aplikací využívajících data z těchto tržišť, tj. vytvoření a udržování datového skladu kraje jako veřejné informační služby, určené organizacím, městům a obcím kraje i veřejnosti v definovaném rozsahu,
- provedení implementace nástrojů BI, vytvoření požadovaných datových tržišť a tvorba základních analytických výstupů (reportů, přehledů), které budou zpřístupněny jednotlivým cílovým skupinám uživatelů,
- vytvoření jednotného referenčního podkladu a zdroje analytických informací pro agendy územních samospráv, mezi které patří finance a rozpočet kraje, správa a rozvoj a služby.

Předmět dodávky

Předmětem dodávky bude:

- Analýza a návrh datového skladu (DS),
  - Datová tržiště (analytické prostory)
  - Analytické výstupy (klíčové ukazatele výkonnosti - KPI, dashboardy, reporty)
  - Analýza dostupnosti datových zdrojů
  - Návrh získávání dat z těchto zdrojů,
  - Návrh potřebných SW technologií nad rámec stávajících ve vlastnictví krajského úřadu.
  - Součástí bude definice potřebných rozhraní informačních systémů zřizovaných organizací Jihomoravského kraje.
- Implementace DS a BI zahrnující:
  - vývoj a realizaci relační datové vrstvy základního datového skladu,
  - vývoj a realizaci analytických prostorů (dalších datových tržišť),
  - vývoj programových nástrojů pro datové pumpy (ETL),
  - ověření způsobů získávání dat z rozhraní informačních systémů podřízených organizací,
  - vývoj uživatelských výstupů BI řešení,
  - nasazení jednotlivých vrstev a komponent řešení DS a BI do zkušebního provozu,
  - integrační a funkční testování,
  - projektové řízení, dokumentace, seznámení uživatelů a správců,
  - předání do rutinního provozu.

Cílové skupiny

Výstupy předmětu plnění této oblasti budou určeny níže uvedeným subjektům:

Na úrovni kraje

- Veřejnost - prostřednictvím publikace vybraných statických reportů zveřejněných na webových stránkách kraje (v souladu s platným legislativním rámcem pro zpřístupňování dat),
- Zaměstnanci a volení zástupci Jihomoravského kraje:
    - management - podklady pro rozhodování v podobě dashboardů reportingu pro sledování klíčových ukazatelů výkonnosti kraje,
    - analytici krajského úřadu – definice reportů a datových modelů, analýzy a tvorbu datových výstupů, statistické vytěžování dat, ad hoc analýzy a také pro administraci a údržbu celého BI řešení),
    - výkonní pracovníci krajského úřadu pro využití přehledů a zvýšení informovanosti o fungování příspěvkových organizací Jihomoravského kraje.

Na úrovni partnerů projektu

- Obcím s rozšířenou působností (ORP)
    - předpokládá se běžný veřejný přístup
    - pro vybrané výstupy bude možné v rámci partnerství obdržet autorizovaný přístup k neveřejným datům či analýzám týkajících se dané ORP
    - krajský DS nebude využíván pro zpracování dílčích provozních agend jednotlivých ORP

- Obcím
    - předpokládá se běžný veřejný přístup
    - mohou v rámci partnerství obdržet autorizovaný přístup k neveřejným datům či analýzám, případně analýze nestrukturovaných dat, týkajících se dané obce.

- Příspěvkovým organizacím
    - předpokládá se běžný veřejný přístup,
    - pro vybrané výstupy bude možné v rámci partnerství obdržet autorizovaný přístup k neveřejným datům či analýzám, týkajících se dané organizace či srovnání v rámci odvětví,
    - předpokládá se vzájemná výměna datových sad mezi krajem a informačními systémy příspěvkových organizací pro podporu a zajištění ekonomicko-provozních zřizovatelských funkcí. (data výkazů PO apod.)

- Dalším institucím a organizacím v kraji (např. vysoké školy)
    - předpokládá se běžný veřejný přístup,
    - mohou v rámci partnerství obdržet autorizovaný přístup k neveřejným datům či analýzám pro výukové a výzkumné činnosti, které jsou v souladu s potřebami kraje.

V rámci řešení bude zpracováno 8 základních věcných oblastí (datových tržišť) a k nim požadované výstupy:

EKONOMICKÁ TRŽIŠTĚ

(analýzy nákladů, výnosů, rozpočtů a zdrojů financování):

1. **Ekonomika zdravotnických zařízení** (přímo řízená zdravotnická zařízení Jihomoravského kraje) – účetnické a rozpočtové výstupy (tržby, závazky, rozpočty, fondy, zisky a ztráty, dotace, nákladovost). Datové tržiště bude čerpat z datových zdrojů data sumarizovaných výkazů GORDIC VYK, tabulky MS Excel, dávky CSV, databázové soubory. Datové tržiště umožní výstupy:
   - Plnění sestaveného, případně upraveného rozpočtu, v rozdílových ukazatelích absolutních a procentních hodnot
   - Přehled o tvorbě a čerpání peněžních fondů v absolutních a rozdílových ukazatelích
   - Výkaz zisku a ztráty
   - Rozvaha
   - Stav podrozvahových účtů
   - Zůstatky a obraty účtů účtového rozvrhu včetně podrozvahových účtů
   - Stav pohledávek po lhůtě splatnosti celkem (do 30 dnů, do 90 dnů, do 180 dnů, do 1 roku, nad 1 rok)
   - Stav závazků po lhůtě splatnosti celkem (do 30 dnů, do 90 dnů, do 180 dnů, do 1 roku, nad 1 rok)
   - Členění tržeb od zdravotních pojišťoven na jednotlivé pojišťovny
   - Členění poskytnutých dotací na provozní a investiční a dále dle jednotlivých poskytovatelů
2. **Ekonomika školských zařízení** (školská zařízení zřizovaná Jihomoravského kraje) Datové tržiště bude čerpat z datových zdrojů data sumarizovaných výkazů GORDIC VYK, datové dávky dle struktury „Rezortního výkazu MŠMT", tabulky MS Excel, dávky CSV, databázové soubory. Datové tržiště umožní výstupy:
   - Plnění rozpočtu
   - Výkaz zisku a ztrát
   - Rozvaha
   - Stav pohledávek po lhůtě splatnosti celkem (do 30 dnů, do 90 dnů, do 180 dnů, do 1 roku, nad 1 rok)
   - Stav závazků po lhůtě splatnosti celkem (do 30 dnů, do 90 dnů, do 180 dnů, do 1 roku, nad 1 rok)
   - Členění poskytnutých dotací na provozní a investiční a dále dle jednotlivých poskytovatelů
3. **Ekonomika ostatních neškolských zařízení** (ostatní zařízení zřizovaná Jihomoravského kraje) Datové tržiště bude čerpat z datových zdrojů data sumarizovaných výkazů GORDIC VYK, tabulky MS Excel, dávky CSV, databázové soubory. Datové tržiště umožní výstupy:

- Plnění rozpočtu
- Výkaz zisku a ztrát
- Rozvaha

- Stav pohledávek po lhůtě splatnosti celkem (do 30 dnů, do 90 dnů, do 180 dnů, do 1 roku, nad 1 rok)
- Stav závazků po lhůtě splatnosti celkem (do 30 dnů, do 90 dnů, do 180 dnů, do 1 roku, nad 1 rok)
- Členění poskytnutých dotací na provozní a investiční a dále dle jednotlivých poskytovatelů

4. **Ekonomika Krajského úřadu Jihomoravského kraje** Datové tržiště bude plně využívat dat z datového zdroje IS GINIS. Bude umožňovat analyzovat a distribuovat výstupy o interním hospodaření Objednatele, z hlediska rozpočtového a účetního. Analytický pohled na čerpání rozpočtu bude umožněn až do úrovně jednotlivých rozpočtových a účetních dokladů. Tržiště umožní vytvářet časové řady. Datové tržiště umožní analyzovat data v datových kostkách Obraty, Doklady, Hlavní kniha (účetnictví), Pohledávky a závazky, Rozvaha, Výsledovka) To umožní výstupy:
    - Plánovací funkce
        - Příprava podkladů pro střednědobý výhled rozpočtu, řešení musí poskytnout potřebná základní data o aktuálním stavu i historickém vývoji.
        - Sledování významných ukazatelů výdajové i příjmové stránky rozpočtu, možnost základních predikcí těchto ukazatelů pro následující období.
    - Plnění sestaveného, případně upraveného rozpočtu, v rozdílových ukazatelích absolutních a procentních hodnot
    - Přehled o tvorbě a čerpání peněžních fondů v absolutních a rozdílových ukazatelích
    - Výkazy kraje – rozvaha a výsledovka krajského úřadu
    - Hlavní kniha
    - Stav podrozvahových účtů
    - Zůstatky a obraty účtů účtového rozvrhu včetně podrozvahových účtů
    - Analýza stavů a obratů nákladových účtů v čase
    - Analýza příjmů rozpočtu
    - Analýza výdajů dle rozpočtové skladby
    - Stav pohledávek po lhůtě splatnosti celkem (do 30 dnů, do 90 dnů, do 180 dnů, do 1 roku, nad 1 rok)
    - Stav závazků po lhůtě splatnosti celkem (do 30 dnů, do 90 dnů, do 180 dnů, do 1 roku, nad 1 rok)
    - Členění poskytnutých dotací na provozní a investiční a dále dle jednotlivých poskytovatelů
    - A mnoho dalších.

STATISTICKÉ TRŽIŠTĚ

(demografie, organizace, vytížení, provoz):

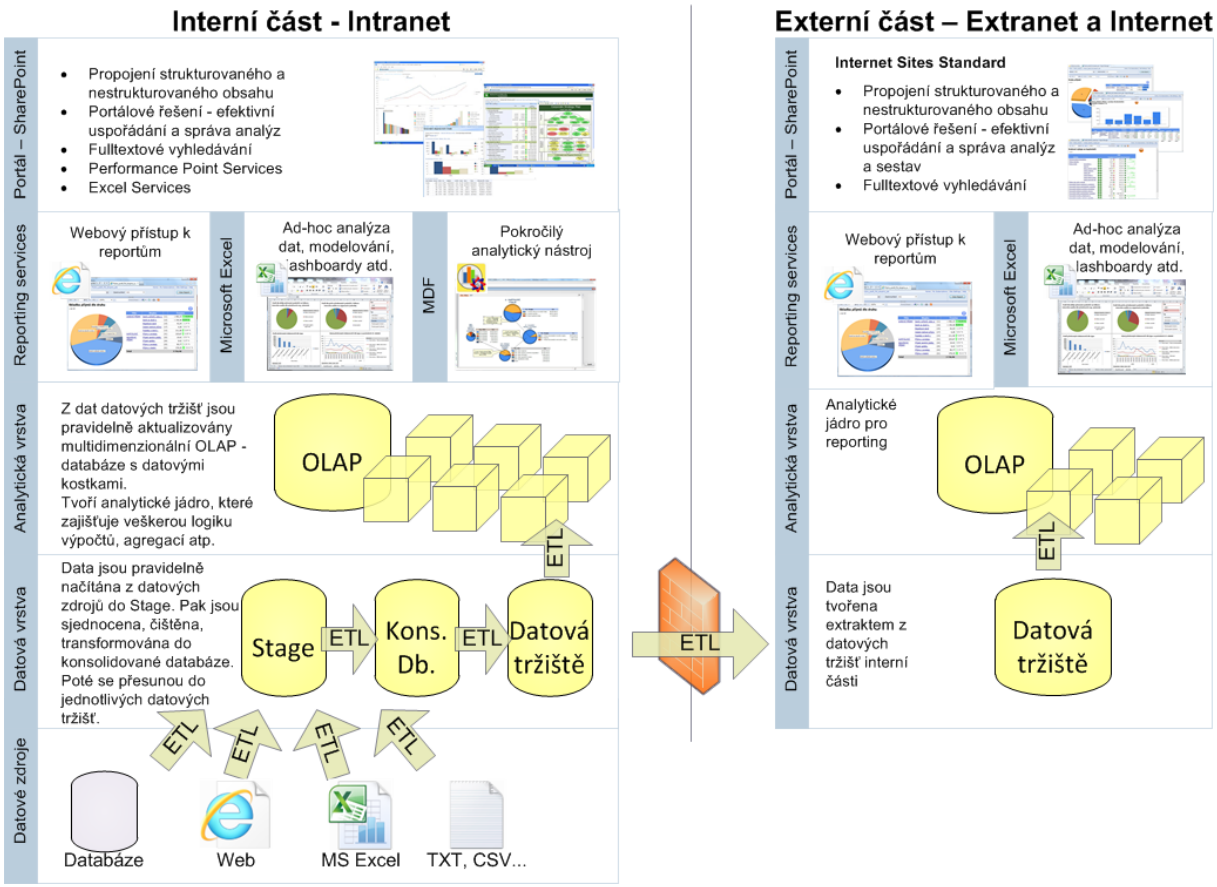
5. **Základní přehledové údaje příspěvkových organizací.** Datové tržiště bude čerpat z datových zdrojů tabulky MS Excel, dávky CSV, databázové soubory, může využívat externí zdroje dat (např. data sběru dat regionálního školství MŠMT (počty žáků) atp. Datové tržiště umožní výstupy:
    - Počty zaměstnanců

- Počty klientů (počty žáků, studentů, návštěvníků)
- Základní statutární údaje

6. **Statistika a výkony zdravotní péče** (přímo řízená zdravotnická zařízení Jihomoravského kraje) Datové tržiště bude čerpat z datových zdrojů tabulky MS Excel, dávky CSV, databázové soubory. Datové tržiště umožní výstupy:
   - Počet pacientů/klientů, struktura dle pohlaví, věku
   - Počet zaměstnanců dle kategorií
   - Struktura platů dle kategorií zaměstnanců (tarify, příplatky atd.)
   - Průměrné platy dle kategorií zaměstnanců a jejich vývoj
   - Počet lůžek
   - Počet pacientů/klientů na 1 zaměstnance
   - Náklady na 1 pacienta/klienta
   - Využití lůžek v %
   - Průměrná ošetřovací doba
   - Náklady na 1 ošetřovací den
   - Roční výkony vybraného přístrojového vybavení
   - Počet ošetřených osob v rámci LSPP
   - Náklady na LSPP
   - Výjezdy ZZS JMK
7. **Data ČSÚ** (demografická data získaná od ČSÚ) Datové tržiště bude čerpat z datových zdrojů poskytovatele dat Českého statistického úřadu (ČSÚ) tzn. dávky CSV, databázové soubory. Datové tržiště umožní výstupy:
   - Dostupné údaje z databází ČSÚ – KROK, MOS, Demografie, RES, Data předávána v xls, dbf z ČSÚ
   - Dostupná data Ministerstva práce a sociálních věcí - Nezaměstnanost, dávky státní sociální podpory, průměrná mzda, nezaměstnanost absolventů
   - Dostupná data EUROSTATU, OECD a další vybraná mezinárodní data na úrovni regionů pro potřeby srovnávání.
8. **Metadata** Datové tržiště bude čerpat jednak z aplikace pro správu metadat a z technologie datového skladu a Business Intelligence. Datové tržiště umožní výstupy:
   - Přehledové reporty nad logy procesů aktualizujících data
   - Přehledové reporty nad využitím reportů

Celková architektura DS a BI

Schéma architektury datových skladů a Business Intelligence:



Architektura Datového skladu, reportovacích a analytických služeb plně vyhovuje „best practices“, které se dnes při budování obdobných systémů využívají.

Logické rozdělení vrstev databáze datového skladu bude zahrnovat následující vrstvy:

- **„Nultá“ vrstva (Stage)** - pro dočasné uložení vstupních dat z externích systémů. Oblast umožní oddělit proces extrakce a přenos dat od procesu zpracování dat a uložení v dalších vrstvách.
- „První“ vrstva (konsolidovaná databáze) – pro uložení historických dat v potřebné míře detailu a zajišťující dlouhodobou správu dat.
- Datová tržiště (Performance layer) – pro zajištění poskytování dat uživatelům a aplikacím v podobě optimalizované pro jejich potřeby.

Datová integrace – vrstva transformačních mechanismů – ETL procesy, preferovány budou:

- deklarativní návrh a vývoj ETL modulů – pro zajištění snadné správy a údržby – oproti „ručně“ psanému programovému kódu ETL rutin;
- podpora extrakce dat z heterogenních datových zdrojů (relační databáze, soubory – XML, TXT, CSV, webové služby);

Analytická vrstva – analytický server a prezentační vrstva:

- přístup prostřednictvím klientských nástrojů pro analytiky i přes webové rozhraní;
- interaktivita analytických výstupů – možnost „slicingu“/dicingu“, drillování z agregovaných informací na detailní, parametrizace/filtrování výstupů;

- možnosti grafické prezentace informací – prezentace dat v podobě tabulek, křížových tabulek, grafů, „budíků“, statických textů;
- možnost exportu výstupů do standardních formátů (PDF, HTML, Excel, CSV, PowerPoint);
- možnost proaktivního monitoringu a upozorňování na nestandardní situace/hodnoty metrik (alerty s flexibilními možnostmi doručení informací);
- možnost periodické distribuce výstupů vybraných skupinám uživatelů s podporou různých typů koncových zařízení (email, mobilní telefon);
- bezpečnost a řízení přístupu na každou datovou položku, report a analýzu, možnost napojení na nově budovaný Identity management;
- možnost monitorování přístupů uživatelů k sestavám/analytickým výstupům pro následnou analýzu využití systému;

Další vlastnosti řešení:

- Aplikace pro správu metadat popisujících datové zdroje, strukturu datového skladu i realizovaných výstupů. Součástí řešení je též logování procesů aktualizujících data, včetně realizace přehledových reportů nad těmito logy.
- Celé řešení respektuje a v maximální možné míře zachovává již realizované investice do technologií a infrastruktury Krajského úřadu Jihomoravského kraje.
- Za účelem provádění dalších nestandardních analýz či datových exportů bude umožněn přístup do datové vrstvy pomocí obecného databázového rozhraní.
- K poskytovaným službám řešení budou mít přístup jak interní uživatelé Krajského úřadu, tak i uživatelé ze zřizovaných PO a veřejnost. Architektura a vlastnosti jednotlivých vrstev umožňují dostatečně robustní zabezpečení přístupů jednotlivých skupin pouze k informačním zdrojům, na které mají nárok.
- Řešení správy uživatelů a jejich přístupových oprávnění je kompatibilní se systémem pro správu identit, který je součástí plnění dle bodu B této nabídky.
- Bude dodána dokumentace k jednotlivým fázím projektu a systémová specifikace implementovaných částí včetně specifikace všech používaných rozhraní.
- Řešení umožňuje jeho budoucí úpravy a rozšiřování přímo vybranými pracovníky Objednatele. Tato možnost úprav je požadována na všech vrstvách řešení (uživatelské výstupy, datová tržiště, relační vrstva, plnění dat).

Přístupy uživatelů:

Externí část

- Veřejnost (anonymní přístup)
- ORP – Obce s rozšířenou působností (anonymní přístup, nebo autorizovaný přístup)
- Obce (anonymní přístup, nebo autorizovaný přístup)
- Příspěvkové organizace (anonymní přístup, nebo autorizovaný přístup)
- Další instituce a organizace v kraji např. vysoké školy atd. (anonymní přístup, nebo autorizovaný přístup)

Interní část

- Zaměstnanci a volení zástupci

- management
- analytici krajského úřadu
- výkonní pracovníci

Popis technologie

Řešení bude postaveno na platformě Microsoft Business Intelligence.

17.7.1.1. Technologie pro interní část – Intranet

Provoz v rámci interní sítě krajského úřadu – zaměstnanci a samospráva kraje (management, odborní pracovníci, analytici):

- **Microsoft SQL Server 2012** - Technologie datového skladu. Při implementaci bude využito níže uvedených součástí (viz jednotlivé bloky výše uvedeného schéma):
  - Datová integrace (ETL procesy) – SQL Server Integration Services (SSIS)
  - Datová vrstva – Database Engine
  - Analytická vrstva – SQL Server Analysis Services (SSAS)
  - Reportovací služby – SQL Server Reporting Services (SSRS)
- **Microsoft SharePoint 2010 –** analytický portál – integrace výstupů a jejich zpřístupnění pro uživatele. Další možnosti – Data Alerting – odesílání reportů emailem, Excel Services – tvorba reportů do portálu skrze MS Excel 2010, Performance Point Services – Dashboardy atd.
- **Další nástroje a komponenty:**
- **Pro analýzu dat z analytických databází:**
  - **Microsoft Excel** – (mimo dodávku, předpoklad využití stávajících licencí krajského úřadu) nástroj pro přímý přístup k multidimenzionálním datům, tvorbu ad-hoc analýz i jejich publikování. Díky pestré škále svých možností je vhodný zejména pro pokročilé uživatele - odvětvové analytiky. (doporučené verze: MS Excel 2007, lépe však 2010)
  - **MDF – Manažerský datový fond** – pokročilý analytický nástroj pro ad-hoc analýzu dat. Modul doplňuje možnosti analýzy o další zajímavé funkce, jako např. rozpadový graf.
- **Pro administraci datových struktur budou dále využity komponenty a nástroje:**
  - **ADR –** Administrace rozvrhu – nástroj pro administraci ekonomických dimenzí, díky čemuž odpovědní a seznámení uživatelé doplní stávající položky a číselníky rozvrhu o rozšiřující atributy, které se budou využívat při konstrukci a aktualizacích ekonomického datového tržiště.

17.7.1.2. Technologie pro externí část – Extranet (autorizovaný přístup), Internet (anonymní přístup)

Provoz v rámci externí sítě krajského úřadu, integrace s webovými stránkami kraje – určeno pro prezentaci dat občanům, zřizovaným organizacím, městům a dalším zainteresovaným skupinám:

- **Microsoft SQL Server 2012** - Technologie datového skladu. Při implementaci bude využito níže uvedených součástí (viz jednotlivé bloky výše uvedeného schéma):
  - Datová integrace (ETL procesy) – SQL Server Integration Services (SSIS)
  - Datová vrstva – Database Engine
  - Analytická vrstva – SQL Server Analysis Services (SSAS)
  - Reportovací služby – SQL Server Reporting Services (SSRS)
- **Microsoft SharePoint Foundation nebo Microsoft SharePoint 2010** Internet Sites Standard – analytický portál – integrace výstupů a jejich zpřístupnění pro uživatele.

Popis vrstvy transformačních mechanismů – procesy ETL

Vrstva odpovědná za datovou integraci. Datová integrace probíhá prostřednictvím „datových pump“, přesněji tzv. **procesů ETL** (Extract, transform and load. Jedním z jejich významných znaků je jejich **univerzálnost na vstupu**, kde je možno zpracovávat téměř jakýkoliv formát vstupních strukturovaných dat.

Datové pumpy načítají ve stanovených intervalech data do datové vrstvy – do relačního datového skladu. V rámci relačního datového skladu jsou nejdříve data uložena do **„Stage“ (též nazývané „nulté“ vrstvy),** kde se ukládají v původní kvalitě. Následně jsou na data aplikovány čistící, validační i kontrolní mechanismy tak, aby byla zajištěna jejich správnost a jednotný formát. Vyčištěná, transformovaná a zkontrolovaná data jsou pak uložena do tzv. Datových tržišť. Datová tržiště slouží pro uložení historických dat na nejnižší úrovni podrobnosti a jsou odpovědné za dlouhodobou správu dat.

17.7.1.3. SQL Server 2012 Integration Services

V rámci této služby zajišťuje následující funkcionality:

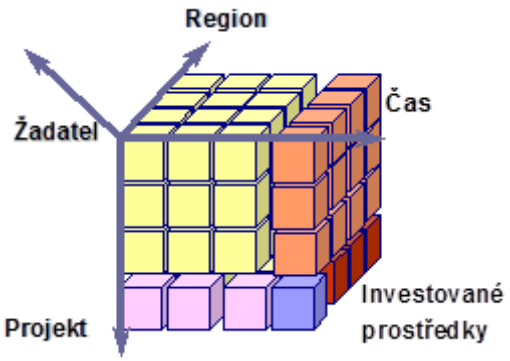
- **ETL** - Základní prvek datové integrace reprezentující řešení pro extrakci dat ze zdrojových systémů, jejich transformaci a jejich následné ukládání do cílového úložiště. Vzhledem k tomu, že komplexní datový sklad nemá jednolitou strukturu, používá se ETL i na „dopravu“ dat mezi jeho jednotlivými komponentami (staging area, konsolidovaná databáze, datová tržiště)

Popis analytické vrstvy

Konsolidovaná data jsou z relačního datového skladu prostřednictvím ETL pravidelně přepočítávána a ukládána do analytické vrstvy – OLAP databází, která je základem pro všechny typy výstupů z datových skladů. Data jsou zde uložena v tzv. multidimenzionálních objektech – tzv. datových kostkách, které umožňují rychlou analýzu dat, tvorbu multidimenzionálních dotazů, různé pohledy na data a především rapidní zrychlení jak analytické práce s daty, tak běžné rutinní práce např. s tabulkovým kalkulátorem. Tato vrstva je základem pro „prezentační vrstvu“ a veškeré analytické nástroje v ní obsažené.

Každá kostka obsahuje sledované ukazatele jim příslušné rozměry pohledu. Přesněji - jednotlivé „atomy“ relací dat jsou rozčleněny na tzv. fakta a dimenze.

- **Fakta** (měřítka atp.) jsou konkrétní hodnotová data vyjádřena číslem, nad nímž lze aplikovat agregační operace jako součet, průměr, atd..
- **Dimenze** jsou popisnými médii pro faktické informace, např. kdy byl faktický údaj pořízen, do jaké kategorie spadá, atd.



Pozn.: Buňky uchovávají hodnoty ukazatelů. Hrany krychle představují dimenze (úhly pohledu). Seskupení buněk představuje agregaci hodnot ukazatelů.

Kostky je vhodné vytvářet na míru požadovaným výstupům a vyhnout se tvorbě „super kostek“, které by v sobě agregovaly obrovské množství dat a jejich reakční doby na dotazy se tím výrazně zvýšily. Kostky představují základní datový zdroj datového skladu z pohledu uživatele stejně, jako jsou tabulky v klasické relační databázi.

Analytická vrstva tak pro všechna datová tržiště zajišťuje mimo jiné následující funkce:

- základní přehledy hodnot vybraných ukazatelů podle specifikovaných dimenzí a jejich vzájemných kombinací,
- operativní určování aktuálně požadované úrovně agregace, resp. úrovně detailu pro vybrané ukazatele,
- výpočty a sledování podílových hodnot ukazatelů,
- výpočty dalších odvozených ukazatelů ze základních podle okamžité potřeby pracovníků
- časový vývoj hodnoty vybraných ukazatelů, tzn. podle jednotlivých let, kvartálů, měsíců, výpočty a sledování různých typů indexů, např. řetězových nebo bazických,
- porovnávání plánovaných a skutečně dosahovaných hodnot ukazatelů s podporou pro výpočty plnění plánu,
- vizuální identifikace problémových hodnot ukazatelů nebo naopak vysoce pozitivních hodnot podle aktuálně stanovených pravidel pracovníky.

17.7.1.4. Prohlížení dat z analytické vrstvy

Pro prohlížení dat uložených v OLAP databázích (datových kostkách) lze používat reporty uložené na prezentačním serveru nebo nástroje jako MS Excel nebo MDF – Manažerský datový fond. Úzce spolupracují s analytickou vrstvou a starají se o správné zobrazení dat – předávají požadavky uživatelů analytické vrstvě a vrací výsledky ve vizualizované formě.

17.7.1.5. Zabezpečení oprávněných přístupů uživatelů k jednotlivým faktům a dimenzím datového skladu

Na úrovni analytické vrstvy je řešeno i zabezpečení přístupu k datům. V rámci definovaných dimenzí a faktů, které popisují logickou strukturu dat, lze zabezpečit přístupy uživatelům pouze k odpovídajícím množinám dat. Lze tak zabezpečit např. pro měřítko rozpočet upravený z ekonomického tržiště uživatel z odboru Zdravotnictví nebude mít přístupná data z ostatních odborů, aniž by byl jinak omezen v možnostech analýz.

Prezentační vrstva a nástroje Business Inteligence

Představuje z hlediska uživatelů nejdůležitější prvek celého řešení a jde o souhrn analytických, reportovacích, vizualizačních a interaktivních nástrojů pro analýzu, vizualizaci a reportování dat. Na výstupu může datový sklad poskytovat data pro další (i provozní) aplikace, kooperující datové sklady či interaktivní webové prezentace dat (včetně dávkového předání dat či webové služby). Prezentační vrstva zajišťuje funkce mimo jiné v následujících oblastech:

Reporting - Typické reporty (analytické výstupy), které budou zobrazovat data v definované podobě (statické či dynamické výstupy, jejichž zobrazení může být upraveno na základě zvolených parametrů).

- přístup k reportům přes webové rozhraní
- export reportů do různých formátů (xls, pdf, obrázek, text, xml …)
- automatická distribuce reportů (například emailem)
- pokročilé řízení přístupu uživatelů k reportům i vlastnímu obsahu reportů
- umožnění generování reportů z více datových oblastí

Multidimenzionální analýza - Obecné dotazovací prostory („analytické prostory“) umožňující tvorbu dalších ad-hoc výstupů s využitím všech atributů (dimenzí, ukazatelů) uchovávaných v rámci datové základny.

- pokročilá analýza za pomoci klientských nástrojů přístupu (webový portál, speciální aplikace)
- uložení vytvořeného pohledu na data a jeho exportu do dalších formátů

Ostatní analýzy

- pokročilá analýza za pomoci klientských nástrojů přístupu (webový portál, speciální aplikace)

- uložení vytvořeného pohledu na data a jeho exportu do dalších formátů

Ostatní

- personalizovaný prostor pro konkrétní skupiny uživatelů s různými potřebami
- Data alerting – Možnost specifikace pravidel pro vyhodnocování sledovaných ukazatelů a na jejich základě identifikace skutečných nebo potenciálních problémů. (Kontrolní funkce)

17.7.1.6. SQL Server Reporting Services

Všestranné řešení, které uživatelům jednoduše zpřístupní k prohlížení data z datového skladu pomocí předpřipravených výstupů. Řešení je určeno jednak pro vytváření a publikaci výstupů, ale také umožňuje řízení přístupu k nim nebo jejich distribuci (na portál, web, nebo emailem). Obecně je nabízeno řešení s funkcionalitou pokročilého reportingu, multidimenzionálních analýz a správy událostí.

Možností Reportingu bude plně využito při vytváření interního, externího analytického portálu a externího přístupu. Konkrétní způsob aplikace a implementace jeho vlastností v řešení vyplynou z detailní analýzy.

17.7.1.7. MDF – Manažerský datový fond

MDF – Manažerský datový fond – nástroj pro pokročilou analýzu ad-hoc s možnostmi exportů. Aplikace je modulem ekonomického informačního systému GINIS z portfolia společnosti GORDIC spol. s.r.o. Modul je určen právě pro prohlížení multidimenzionálních OLAP databází (datových kostek) a nabízí možnost tvorby libovolného (ad-hoc) dotazu. Výsledný pohled lze uložit pro daného uživatele modulu, exportovat do Microsoft Excelu atp.

17.7.1.8. Microsoft Excel

Standardní tabulkový procesor disponuje možnostmi, jak analyzovat data uložená v OLAP databázi. Microsoft Excel si přitom zachovává své všechny další výhody, jako podmíněné formátování, upozornění na anomálie v datech atp.

Možností Microsoft Excelu mohou využívat zejména odvětvoví analytici, kteří mohou výsledné analýzy publikovat na interním, případně i na externím analytickém portálu.

Detailní popis části řešení - Krajská digitální spisovna (KDS) a Krajský digitální repozitář (KDR)

Úvod

Lidstvo se potýká s problémem archivnictví od pradávna. Již v období, kdy se objevily první písemné záznamy, řešilo lidstvo problém jak uchovat dokumenty pro další generace. Tato iniciativa je zcela pochopitelná, pokud nezůstanou po civilizaci, národu či regionu žádné písemné záznamy stane se pro budoucí generace zcela neviditelným, tak upadnou v zapomnění i životy mnoha lidí, kteří se na budování civilizace, národu či regionu podíleli.

Po tisíce let existovaly jen analogové záznamy, za tu dobu se vyvinuly techniky na jejich uchování pro budoucí generace. Mezi výhody analogového záznamu patří to, že je možné jej uchovat po dlouhou dobu a zejména se nemusí řešit jeho čitelnost, analogový záznam je sám o sobě čitelný pro každého člověka. Hlavní nevýhodou analogového záznamu je to, že každým jeho použitím (přečtením či zhlédnutím) jej poškozujeme.

S příchodem digitálního věku se situace zcela změnila, digitální záznamy lze zcela bez poškození originálu používat dokola a není problém vytvořit neomezené množství kopií se stejnou kvalitou záznamu. Problém ovšem nastává s uchováním takové informace pro budoucí generace a zejména s jeho budoucí čitelností. Pokud nyní uložíme fotografii z digitálního fotoaparátu ve formátu JPEG na DVD disk, je zde 90% riziko, že fotografii za 10let z DVD disku nedokážeme přečíst. Buď bude poškozen DVD disk, nebo nebude existovat program, který by obrázek otevřel a zobrazil uživateli.

Nyní se tedy nacházíme na jednom z historických milníků archivnictví. Pokud přijmeme špatné či krátkozraké opatření, riskujeme tím, že náš historický odkaz nebude pro budoucí generace čitelný a tím pádem upadnou v zapomnění i naše životy a práce.

Krajská digitální spisovna (KDS)

Krajská digitální spisovna je aplikace, která se primárně stará o uchování dat pro dlouhé časové období (5 – 100 let). To klada na aplikace a její budoucí rozvoj nemalé nároky a výběr vhodného Zhotovitele musí být velice pečlivý. Aplikace by měla mít i početnou komunitu uživatelů z řad archivů, univerzit a jiných organizací zabývajících se archivací elektronických dokumentů, to zajistí, že Zhotovitel bude touto početnou komunitou tlačen k neustálému vývoji a zdokonalování aplikace.

Neustálá údržba (vývoj) KDS je pro archivované dokumenty životně důležitý

Současná média pro uchovávání dat mají omezenou životnost (cca 8 – 10 let). To znamená, že KDS bude muset každých 8 let provádět migrace dat z jednoho typu úložiště na jiný typ úložiště, které v dnešní době neexistuje. To znamená, že aplikace KDS musí být neustále udržována, aby dokázala držet krok s vývojem HW.

Dnes používané a schválené formáty jako jsou např. PDF/A, PNG, atd... budou za několik let nečitelné. Nebudou jednoduše existovat programy, které by uměly takto starý formát souborů přečíst. Pokud aplikace KDS nebude držet krok s aktuálními formáty, které jsou určené pro archivnictví, stane se to, že data budou z médií čitelná strojově, ale nikdo je nedokáže prezentovat do podoby pochopitelné pro člověka, což je defakto to samé jako by data byla poškozená.

Jak již bylo zmíněno v úvodu, dlouhodobé ukládání dat je vědní disciplína, která se neustále vyvíjí. To znamená, že modul KDS musí s těmito novými trendy držet krok, aby nedošlo ke kompromitaci nebo poškození archivovaných dat.

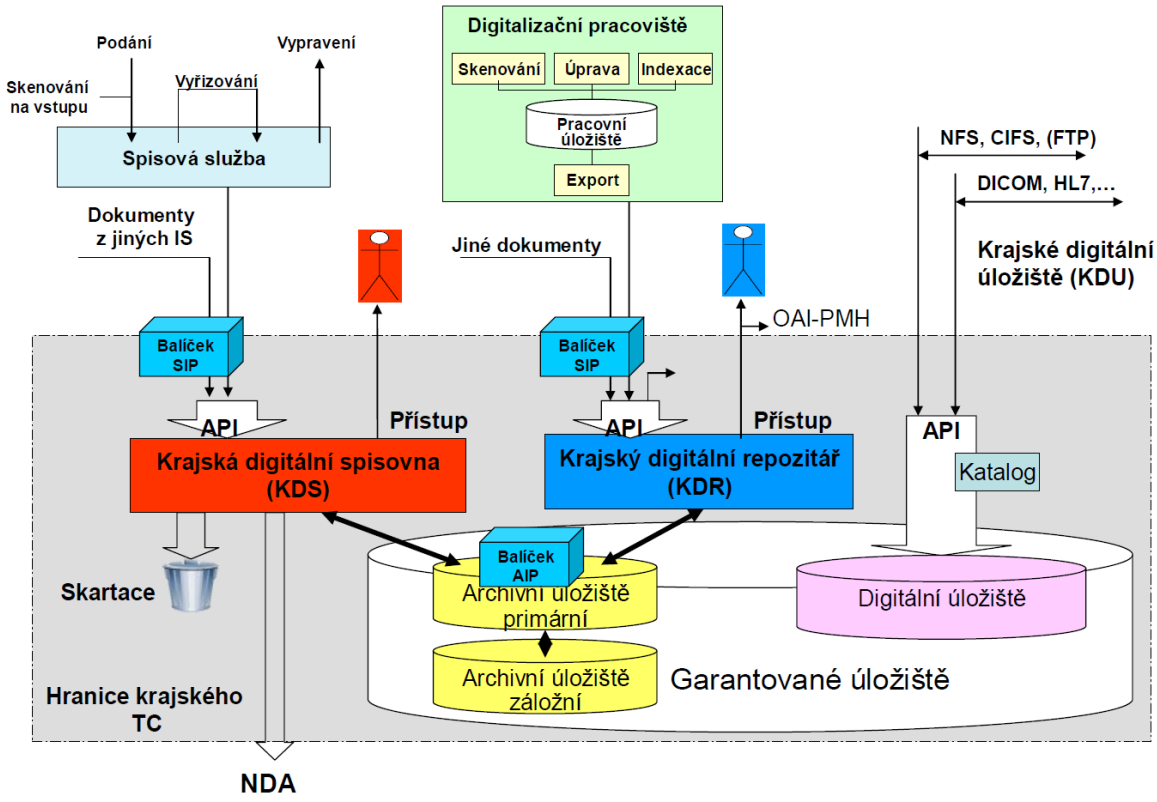
Krajský digitální repositář (KDR)

Krajský digitální repositář je aplikace, která má jiný legislativní základ než KDS, ale nároky na dlouhodobou archivaci jsou na ni kladené stejné ne-li vyšší (doba archivace zde není limitována). **Proto je životně důležité neustále udržovat (vyvíjet) modul KDR dle posledních trendů v archivaci a dlouhodobém uchovávání dat**.

Koncept řešení

Předmětem dílčího plnění oblasti E je dodávka integrovaného řešení pro krajskou digitální spisovnu (dále také jako „KDS“) a krajský digitální repozitář (dále také jako „KDR“). V KDS a KDR budou implementovány funkce podle příslušných národních a mezinárodních standardů, zejména OAIS, a platné legislativy ČR pro oblast dlouhodobé důvěryhodné archivace (zejména zákon č. 499/2004 Sb., o archivnictví a spisové službě, ve znění pozdějších předpisů, a ve znění prováděcích vyhlášek a nařízení Vlády ČR, Národní standard pro elektronické systémy spisové služby, připravovaný zákon o Národním digitálním archivu ČR a další).

KDS a KDR budou implementovány nad garantovaným úložištěm dokumentů v rámci Technologického centra Kraje. KDS a KDR budou dále využity k řešení dalších potřeb souvisejících se správou a dlouhodobou archivací dokumentů jednotlivých původců.



Popis produktu

ŘEŠENÍ KDS A KDR

Jak již bylo řečeno v úvodu, KDS a KDR jsou po technické stránce velice podobné systémy, které kladou vysoké nároky na systém pro dlouhodobé ukládání dat (LTP systém) a proto se o jejich bezpečnost a konzistenci stará navrhované řešení KDS/KDR.
V rámci ochrany dokumentů v KDS i KDR jsou data oddělena a mohou být uložena na fyzicky oddělených úložištích. S uživatelským rozhraním KDS přichází do styku jen seznámená obsluha (**správce archivu**).
Původce (Spisová služba) má do KDS přístup pomocí API rozhraní KDS.
Pomocí uživatelského rozhraní případně API může mimo jiné

- ukládat data do KDS ve formě SIP balíčků
- provádět skartace
- předávat spisy (dokumenty) do NDA
- zjišťovat stav podání
- atd ...

API je založeno na návrhu obecného formátu pro předávání dokumentů a jejich metadat do archivu viz příloha č. 2 k Národnímu standardu pro elektronické systémy spisové služby.
Původce tedy ovládá KDS pomocí své spisové služby nebo spisovny. Díky tomu může dělat všechny běžné úkony tak jak je zvyklí, ale změny se projevují přímo v KDS.
KDS a KDR budou využívat specifické softwarové vybavení implementující příjem a správu dokumentů v intencích modelu OAIS. Tento software bude instalovaný na aplikačních serverech TCK, přičemž bude možné využít i virtualizace těchto serverů.
K obslužným aplikacím KDS a KDR umístěným na aplikačních serverech bude možný vnější přístup pro jednotlivé původce dokumentů, kteří budou komunikovat prostřednictvím zabezpečeného kanálu (https) v rámci klientských aplikací a poskytovaných webových služeb.
Pro správu obslužných dat a metadat uložených balíčků subsystémů KDS a KDR bude využit databázový server a záložní databázový server podle potřeb těchto aplikací.
Pro účely důvěryhodného uložení balíčků AIP subsystémů KDS a KDR, obsahujících dokumenty a jejich metadata, bude obslužnou aplikací použito úložiště Technologického centra Jihomoravského kraje. Obslužná aplikace pracuje s daty uloženými v úložišti (CAS atd.) i po jejich uložení (čtení obsahu po vyžádání, procesy pro zajištění důvěryhodnosti a konzistence).

Základní scénáře použití KDS

PODÁNÍ DO KDS

Elektronický dokument, který je určen pro uložení do KDS, musí být nejprve připraven do vhodné podoby pro předání. Tuto přípravu zajistí buď určený uživatel původce manuálně, ve speciálním nástroji, nebo je příprava provedena automatickou službou zajišťující integraci spisové služby (či jiné aplikace, ve které dokumenty vznikají) s KDS. Připravené dokumenty v podobě informačních balíčků SIP jsou přes aplikační rozhraní přeneseny do KDS. Balíčky SIP obsahují kromě souborů s dokumenty také určená popisná metadata.

Dokumenty převzaté k archivaci v KDS jsou zkontrolovány dle stanovených pravidel (na integritu, neškodnost, validitu, kvalitu apod.). Elektronické dokumenty jsou dále doplněny technickými metadaty podporujícími procesy řízení, uchovávání a zpřístupňování. Každému dokumentu je přidělena jednoznačná identifikace a vše je zabaleno do archivního informačního balíčku AIP (všechna metadata a elektronické soubory). Archivní balíček je poté uložen do archivního úložiště.

KDS pak zajišťuje bezpečné uložení archivních balíčků. Na základě uchovávací strategie provádí činnosti pro udržení čitelnosti, důvěryhodnosti a životaschopnosti elektronických dokumentů.

SKARTAČNÍ ŘÍZENÍ

Dle zákona 499/2004 Sb., ve znění pozdějších předpisů a prováděcí vyhlášky, je původce stále zodpovědný za dokumenty uložené v KDS a tedy i za provedení skartačního řízení, KDS mu pouze poskytuje technické prostředky, ale veškeré úkony musí být provedeny na povel původce.

Po vypršení skartační, nebo archivační lhůty může být dokument ze systému vyřazen. Proces Skartačního řízení je několikafázový proces, který zahrnuje výběr dokumentů k vyřazení, sestavení skartačního návrhu, schválení skartačního návrhu a vlastní vyřazení.

Vyřazením se rozumí zničení obsahu skartovaných dokumentů, resp. export dokumentů a jejich metadat do formátu vhodného pro přenos do nadřazeného archivu. Podle nastavení systému se dokumenty předané prokazatelně do nadřazeného archivu také zničí, nebo zůstávají jako kopie nadále v systému. O vyřazení se pořizuje skartační, resp. předávací protokol.

Základní scénáře použití KDR

Krajský digitální repozitář je dlouhodobé úložiště digitalizovaných dokumentů, které nemají úřední charakter. Jedná se převážně o digitalizované knihy a regionální periodika. Do KDR se mohou dále ukládat např. digitalizované monografie, historické mapy, a mnohé další zdroje kulturního dědictví. Podle způsobu vzniku se může jednat o výstupy např. z krajské digitalizační jednotky (KDJ) případně dokumenty digitalizované třetí stranou jako služba pro Jihomoravský kraj, či o dokumenty vzniklé již v digitální podobě, což mohou být fotografie, audio a video záznamy apod.

Jelikož může být objem dat, ukládaných do KDR, veliký je doporučené provádět podání prostřednictvím disku. Technika tohoto podání je velice jednoduchá a umožňuje vytvoření podání do KDR i méně sofistikovaným zařízením.

Na sdíleném disku bude vytvořena složka, která bude obsahovat SIP balíček. Slovo balíček je v souvislosti se SIP nepřesné, jedná se totiž o XML soubor obsahující seznam souborů v SIP balíčku, jejich HASH a další náležitosti jako jsou metadata či digitální podpis. Do této složky (dle standardu METS) se nakopírují seskenované dokumenty a jako poslední se uloží zmíněný XML sobor popisující SIP. Tím je tvorba balíčku zakončena a systém KDR dostane signál, že může zpracovat balíček SIP. Dále se pokračuje dle nastavených procedur, SIP balíček může projít karanténou či jinými druhy kontrol. Výsledkem je opět AIP balíček uložený v archivním úložišti.

ZÁKLADNÍ CHARAKTERISTIKA KDR

Důvěryhodnost dokumentů či dat	Důvěryhodnost zajištěna postačujícím způsobem politikami KDR v rámci TC, právní prokazatelnost nemá u archivních dokumentů význam.

Přístupová práva k dokumentům či datům	Přístup je řízen systémem elektronického repozitáře, přístup je možno definovat podle nastavitelných politik na skupiny a role uživatelů. • některé dokumenty mohou být i obecně přístupné (veřejné) • nebo přístup k nim je řízen - autorskými právy - ochranou osobních údajů - komerčními hledisky (zhodnocení nákladů na pořízení dokumentů) Mimo přímý přístup do repozitáře existuje možnost exportu vybraných digitálních objektů (uživatelských kopií včetně vybrané podmnožiny metadat) do Systému zpřístupnění, jehož webové rozhraní je vytvořeno pro potřeby přístupu široké veřejnosti.
Metadatové standardy	• standard metadat stanovený Národní knihovnou pro knihovní systémy (probíhá jeho příprava a schvalování) • možné vazby na číselníky stanovené Národní knihovnou (např. Celostátní databáze národních autorit vedená Národní knihovnou) • základní archivní metadata používaná při budování archivních fondů a sbírek
Způsob získávání metadat	Metadata předávána spolu s dokumenty na vstupu do repozitáře. Podle typu ukládaných dokumentů se získávají většinou ruční indexací. Při digitalizaci je indexace jednou z činností digitalizačního pracoviště. Při digitalizaci knižních fondů se mohou s výhodou využívat existující elektronické knižní katalogy a čárové kódy nalepené na knihách. U archivních fondů je nutno metadata pořizovat až při ukládání do repozitáře – ruční práce odborných pracovníků.
Požadavky na vyhledávání a komfort pro konzumenty	Specializované uživatelské rozhraní pro - administrátory repozitáře (kontrola vstupu dat, definice oprávnění, správa číselníků, apod.). - odborné pracovníky (kontrola vstupu dat, doplnění metadat a pod.) - badatele a širokou veřejnost - řešeno exportem do Systému zpřístupnění
Existence vnitřních řídících procesů	Vnitřní skartace, rejstříkování, zpřístupňování, zajištění čitelnosti.
Spektrum technických formátů ukládaných dokumentů či dat	Úzké, definováno standardy a metodikou repozitáře.
Spektrum technických formátů ukládaných dokumentů či dat	Úzké, definováno standardy a metodikou repozitáře.
Způsob akvizice dokumentů či dat	"pull" – digitální archiv sám získává pro své fondy nové přírůstky vyhledáváním v různých zdrojích (fyzické a právnické osoby, jiné digitální archivy, knihovny) i "push" – výstupy z digitalizace.
Doba uložení	Dlouhodobá – trvale.
Zdroje dokumentů či dat	Neomezený počet původců včetně náhodných nebo neznámých zdrojů. Ukládání na základě smluvního vztahu.
Frekvence přístupů k dokumentům či datům	Nízká u přímého přístupu ke KDR Vysoká u Systému zpřístupnění, kam byly vybrané dokumenty z KDR exportovány - dokumenty kulturního dědictví regionálního významu.
Počet současně pracujících konzumentů	V některých časových úsecích vysoký zájem jak o vyhledávání, tak pro získávání dokumentů kulturního dědictví regionálního významu.

HW A SW POŽADAVKY KDS/KDR

Celé řešení je postaveno na moderních technologiích a je jej tedy možné provozovat na různých HW a SW platformách.
Předpokládáme, že provoz nabízeného řešení bude postaven na architektuře tvořené dvojicí virtuálních serverů, kde jeden z nich bude fungovat jako databázový a druhý bude určen jako server aplikační. Oba servery budou zapojeny přímo do sítě dané organizace. Pro komunikaci budou využívat běžného TCP/IP protokolu.
Dalším důležitým parametrem navrženého hardware je odhad potřebné diskové kapacity. Jako primární fyzické úložiště pro KDS, KDR předpokládáme implementaci prostřednictvím technologie CAS.
Pro režijní informace dokumentového úložiště, které jsou tvořeny především metadaty, nesmíme zapomenout připočítat dalších zhruba 10 – 20% kapacity navíc oproti objemu uložených dokumentů.
Z hlediska standardního software je potřeba mít k dispozici na databázovém serveru vhodnou verzi operačního systému a dále pak licenci relačního databázového stroje, který má v sobě integrovánu podporu pro fulltextové vyhledávání.

- Nabízené řešení lze provozovat v prostředí virtuálních serverů VMWare.

KDS/KDR komunikuje s uživatelem prostřednictvím webového rozhraní. Je tedy třeba funkční běžný internetový prohlížeče splňujícího standardy HTML 4.0 a CSS2 (MS Internet Explorer 7 a vyšší, Firefox 3.x a vyšší). Je-li tedy na koncové stanici nainstalován operační systém s funkčním internetovým prohlížečem, lze říci, že daná specifikace softwarového vybavení na straně koncového uživatele je splněna. Požadavky na nestandardní (potlačenou) funkčnost prohlížečů (např. nepoužívání CSS, JavaScriptu, apod.) bude nutné specifikovat během analýzy. V takovém případě by bylo nutné řešení příslušně modifikovat.
K provozu KDS/KDR je možné využití databáze Oracle (10g a vyšší) nebo MS SQL Server (2005 a vyšší).
Pro provoz nabízeného řešení předpokládáme využití vyhrazeného aplikačního serveru a databázového serveru.

Záruka, úroveň poskytovaných služeb (SLA), požadavky na podporu pro oblasti A-E

ZÁRUKA

Zhotovitel bude poskytovat **záruku na technické komponenty** dle specifiace uvedené na straně **Chyba! Záložka není definována.**v Kapitole **Chyba! Nenalezen zdroj odkazů. Chyba! Nenalezen zdroj odkazů.. Záruka na služby** je Zhotovitelem vnímána jako definice Úrovně Poskytovaných Služeb (SLA), která je definována v kapitole **Chyba! Nenalezen zdroj odkazů. Chyba! Nenalezen zdroj odkazů.**

Zhotovitel bude za podmínek vymezených dle zadávací dokumentace povinen poskytovat servisní služby po dobu 5 let od finální akceptace kompletního plnění dle odst. 2.4.1. bodu I. zadávací dokumentace

Servisní služby budou zahrnovat odstraňování závad, provozní správu, expertní podporu, provádění změn provozní dokumentace, monitoring HW a základního SW. Servisní služby budou poskytovány v rámci režimů SLA definovaných v příloze č. 1zadávací dokumentace.
Navržené servisní služby celého projektu korespondují v odpovídající kvalitě s požadavky Objednatele.
Poskytování služeb technické (servisní) podpory **předpokládáme po dobu pěti let od předání díla do provozu.**

STANDARDY

V oblasti poskytování služeb dbáme doporučení z technologických standardů, vyplývajících **z ISO 9001, ISO 20000, ISO 27001, ISO 16001**, dále využíváme doporučených standardů dle **ITIL** a interní projektové metodiky.
Hlavní přístupový a komunikační bod (Single point of contact - „SPOC“) pro zákazníky a smluvní partnery Objednatele je **Service Desk spol. AutoCont**, zajišťující procesní komunikaci a zajištění řešení požadavků eskalací na řešitelské týmy a koordinaci třetích stran. Služby Service Desku v současné době zajišťuje více jak 40 vyškolených zaměstnanců ve 4 lokalitách v České republice, kteří v současné době hladce řeší více jak 120.000 požadavků ročně. Toto centrální kontaktní místo je dostupné v režimu 24x7po celý rok.

ŘÍZENÍ SERVISNÍCH SLUŽEB

Na garanci kvality dbají po celou dobu manažeři kvality, kteří pravidelně sledují, měří a vyhodnocují procesy a kvalitu poskytovaných služeb, zejména pak garantovanou úroveň podpory (dle SLA) a zajišťují také statické výstupní informace (reporty) dle nastaveného smluvního plnění a proaktivně identifikují možnosti zlepšení dodávky IT služeb.
Požadavky lze zadávat přes webové rozhraní, telefonicky, prostřednictvím emailu a/nebo faxem.

ŽIVONÍ CYKLUS POSKYTOVÁNÍ SERVISNÍ PODPORY

Operátoři Service Desku v první fázi zalogují nahlášený požadavek a po provedení prvotní analýzy požadavku jej eskalují na kompetentní víceúrovňové řešitelské týmy, sleduje životní cyklus požadavku po dobu řešení (zejména plnění smluvních SLA parametrů a procesů) a po akceptaci vyřešení požadavek uzavírají a zajistí administrativu s tím spojenou.
jsou rozděleny do 3 úrovní, přičemž řešitelé 1. úrovně řeší základní běžné incidenty a požadavky, řešitelé 2. úrovně představují řešitelské týmy s hlubší produktovou / technologickou znalostí dané oblasti a zajišťují podporu řešitelům 1. úrovně. 3. úroveň představuje nejvyšší úroveň podpory, kompetenčně a kvalitativně schopnou řešit ty nejobtížnější incidenty, problémy a požadavky. Řešitelé na této úrovni podpory jsou špičkovými technologickými odborníky ve svém oboru, majícími hluboké znalosti a rozsáhlé zkušenosti. Součástí 3. úrovně podpory je i specializovaný bezpečnostní tým, připravený zajistit součinnost v oblasti řešení bezpečnostních incidentů a problémů.
Ke každé z požadovaných oblastí podpory je navrženo eskalační schéma, popisující životní cyklus daného požadavku od fáze zadání po jeho vyřešení.
Do budoucna předpokládáme (například v rámci řešení nových, navazujících projektů) rozšiřování jak stávajících technologií, tak implementování nových. Díky širokému technologickému záběru a velkému množství certifikovaných specialistů je samozřejmostí (např. na základě smluvního kontraktu) rozšíření servisní podpory o tyto nové technologie.
Zhotovitel disponuje více jak 450 specialisty, kteří jsou nositeli bezmála 900 jedinečných certifikačních titulů.
Na základě našich dlouholetých zkušeností z obdobných projektů jsme přesvědčeni, že naše nabídka přináší jednoznačné strategické a ekonomické přínosy v oblastech snížení provozních nákladů IT. Jsou definované

SLA pro všechny požadované služby, což vede k neustálému zvyšování efektivity poskytovaných služeb, ale i vyšší pružnosti v poskytování IT služeb.

Obecný popis poskytování servisních služeb

Tato kapitola popisuje rozsah služeb, vycházejících s požadavků Objednatele. Služby fakticky představují standardizované služby zajišťované Service Deskem společnosti AutoCont, který představuje pro smluvní zákazníky a partnery tzv. **SPOC** (hlavní kontaktní místo pro hlášení požadavků). Jedná se o tyto Objednatelem požadované služby:

- Telefonické zadání požadavku na technickou podporu je zajištěno lidskou obsluhou.
- Komunikace s dispečinkem technické podpory, stejně tak komunikace s řešiteli požadavků na technickou podporu je zajištěna v českém (případně slovenském) jazyce.
- Příjem požadavku je umožněn několika nezávislými komunikačními cestami:
    - prostřednictvím internetu (webové rozhraní, autentifikace pro oprávněné osoby na základě jména a hesla) - přímý přístup z Internetu pro zákazníka do SD systému Siebel. Možnost zadávání, okamžitého zjištění stavu požadavku a kontroly plnění jednotlivých požadavků,
        - http://sd.autocont.cz/ecustomer_csy
    - telefonicky - pro obsluhu tel. hovorů je použit systém callcentra (AVAVYa), který dovoluje vyhradit tel. číslo pro každého zákazníka, nastavit logiku toku jednotlivých hovorů směrem k operátorům/řešitelům, využít DTMF provolby, uvítací hlášky, IVR, nahrávání, atd.
        - 00420 251 022 564
        - 00420 723 465 409
    - e-mailem - virtuální mailové schránky pro daného zákazníka, projekt či oblast problémů,
        - zc.dispečink@autocont.cz
    - faxem - využití faxové brány směřující jednotlivé faxy do virtuálních mail.schránek, popř. použití standardního stolního faxu.
        - 00420 420 251 022 586
- Prostřednictvím internetu nebo e-mailu může být požadavek zadán i mimo stanovenou dobu (dle konkrétního parametru SLA) pro příjem požadavku, lhůta pro reakci na něj se však v této době počítat nebude.
- Služba obsahuje zajištění nepřetržitého přístupu do systému pro evidenci požadavků pro oprávněné osoby Objednatele pro možnost upřesnění požadavku v průběhu jeho řešení.
- Služba umožňuje přístup k historickým datům o řešení požadavků na technickou podporu (2 roky zpětně online, další roky na vyžádání).

Rozsah nabízených služeb v rámci podpory

Následující kapitola zahrnuje výčet reaktivních a proaktivních služeb na základě požadavků Objednatele, řešených certifikovanými pracovníky zhotovitele, případně přímo technikem výrobce.

Servisní služby

Služby požadované Objednatelem v rámci této kapitoly se zaměřují primárně na oblast reaktivní podpory – tedy na oblast řešení vzniku nenadálých událostí typu (bezpečnostní) incident.

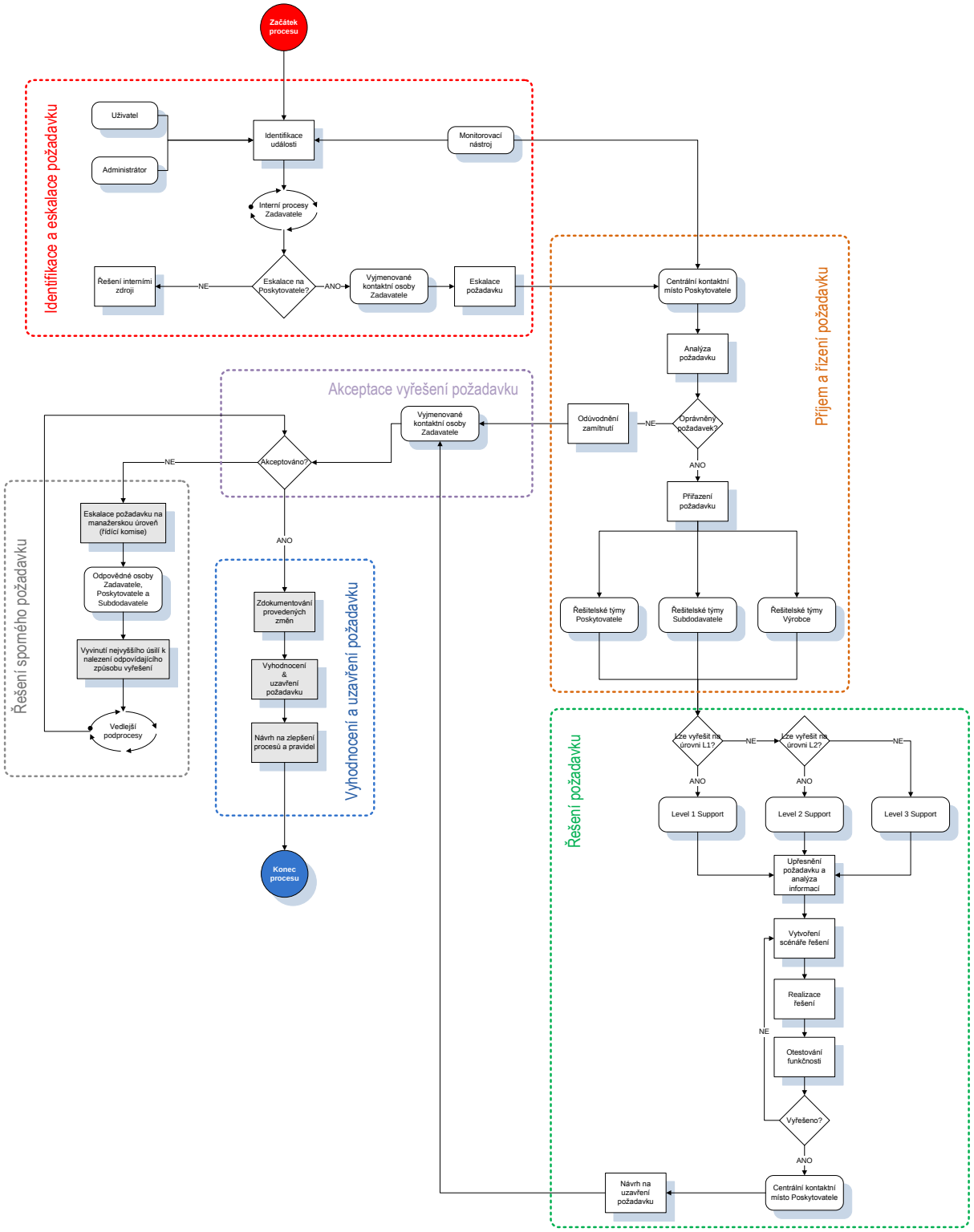
Mezi požadované Servisní služby patří:

- Příjem servisního požadavku v režimu 7x24 – zajištěno centrálním Service Deskem společnosti AutoCont CZ a.s.
- Diagnostika závady – dle povahy a charakteru incidentu (analýza logů, informace z monitorovacích systémů, printscreen obrazovky, využití sofistikovaných skenerů a analyzátorů atd.)
- Odstraňování HW i SW závad ve lhůtách uvedených v části SLA – dle sjednaných scénářů pro konkrétní technologickou oblast eskalují pracovníci Service Desku požadavek dle parametrů SLA na konkrétní řešitelský tým (v případě řešení softwarové závady), nebo v případě hardwarové závady požadavek přímo eskalují na výrobce.

  Na garanci kvality dbají po celou dobu manažeři kvality, kteří pravidelně sledují, měří a vyhodnocují procesy a kvalitu poskytovaných služeb, zejména pak garantovanou úroveň podpory (dle SLA) a

zajišťují také statické výstupní informace (reporty) dle nastaveného smluvního plnění a proaktivně identifikují možnosti zlepšení dodávky IT služeb.
Řešitelské týmy jsou rozděleny do 3 úrovní, přičemž řešitelé 1. úrovně řeší základní běžné incidenty a požadavky, řešitelé 2. úrovně představují řešitelské týmy s hlubší produktovou / technologickou znalostí dané oblasti a zajišťují podporu řešitelům 1. úrovně. 3. úroveň představuje nejvyšší úroveň podpory, kompetenčně a kvalitativně schopnou řešit ty nejobtížnější incidenty, problémy a požadavky. Řešitelé na této úrovni podpory jsou špičkovými technologickými odborníky ve svém oboru, majícími hluboké znalosti a rozsáhlé zkušenosti. Součástí 3. úrovně podpory je i specializovaný bezpečnostní tým, připravený zajistit součinnost v oblasti řešení bezpečnostních incidentů a problémů.
    - na odstraňování závad v rámci servisních služeb nebudou použity předplacené hodiny expertní podpory
    - náklady související s poskytnutím servisního zásahu jsou zahrnuty v ceně služby, žádné další náklady (cestovné, příp. nocležné apod.) nebudou fakturovány,
- Instalace náhradního zařízení/dílu do původního umístění (ve velké většině případů) – využití služby podpory garantované výrobcem dle služby zakoupené na konkrétní produkt a technologii, nebo nahrazení stejným dílem ze servisního skladu. Zhotovitel garantuje výměnu vadného zařízení nebo dílu totožným zařízením nebo dílem.
- Obnovení funkčnosti ze zálohy nebo reinstalací SW – v případě prokázání vady díla bude tato služba poskytnuta bezplatně, v opačném případě bude zpoplatněna.
- Otestování funkčnosti nejen měněného zařízení, ale celého celku, které zařízení nebo díl ovlivňuje – primární test funkčnosti měněného hardware fyzicky provádí standardně pracovník zhotovitele, nebo výrobce. Jako sekundární potvrzení může být v konkrétních případech (zejména u kritických incidentů) využito zpětné vazby monitorovacího systému.
- Uzavření servisního požadavku po akceptaci Objednatele a zhotovení servisního protokolu – servisní požadavek uzavírá standardně pracovník Service Desku zhotovitele a to buď po akceptaci Objednatele, nebo do 5ti kalendářních dnů, pokud pověřený pracovník zhotovitele nereaguje na doručený písemný návrh k uzavření požadavku.
- Zaznamenání změn do technické provozní dokumentace – je součástí životního cyklu řešení požadavku, nebo jako samostatný požadavek. V případě akceptace vyřešení vzneseného požadavku (na které se vztahuje SLA doby vyřešení) se za dobu vyřešení počítá doba prokazatelného odstranění hlášené vady, nikoliv doba zaznamenání provedené změny do provozní dokumentace (termín provedení změny ale musí být stanoven).
- Držení náhradních dílů skladem u Zhotovitele (některé servisní služby mohou být zajištěny formou podpory výrobce zařízení nebo software) – Eskalaci na výrobce provádí Service Desk zhotovitele přímo na technickou podporu výrobce (dle typu technologie a zakoupené záruky) a nebo (v případě držení náhradních dílů ve skladu zhotovitele) na interní podporu 1. úrovně, kde je podle SLA dojednán výjezd servisního technika s předmětným náhradním dílem.
- Uložení informací o provedení servisního zásahu do elektronického systému pro příjem a evidenci požadavků na technickou (servisní) podporu – provádí pracovník Service Desku zhotovitele. Každému požadavku je přiděleno jedinečné ID, pod kterým lze přes webové rozhraní sledovat jeho aktuální stav od založení až po dobu vyřešení.

V rámci poskytování servisních služeb pro oblast reaktivní podpory - tj. v rámci **řešení nenadálých událostí typu** (bezpečnostní) incident navrhujeme následující procesně eskalační schéma:



Jedním z významných zdrojů údajů a informací, sloužících jako zpětná vazba k vybudovanému systému efektivního řízení IS/ICT v organizaci, je zpracovávání podnětů, které s sebou přinášejí incidenty a zkušenosti získané jejich řešením. Spolu s tím, jak roste naše závislost na informačních technologiích, roste i význam informačních systémů a tedy i důležitost efektivního řešení incidentů.

IDENTIFIKACE A ESKALACE POŽADAVKU

Rozpoznání nestandardní události koncovým uživatelem / pracovníkem IT nebo detekovaný automatizovaným monitorovacím nástrojem, nahlášení události na HelpDesk Objednatele a poskytnutí primárních informací o povaze události (incidentu) a případně prvotní zařazení dle povahy dopadu události a dalších interně nastavených procesů.
Další navazující fází řešení incidentu je rozhodnutí, jedná-li se o událost, která musí být řešena nasazením externího poskytovatele služeb podpory – tedy podporou zhotovitele podporovaného díla. Tuto část procesu obvykle zajišťují v prvním okamžiku pracovníci Help Desku Objednatele v rámci služeb interní podpory podporu. Pracovníci zhotovitele přebírají od uživatelů, nebo na základě notifikace z automatizovaného monitorovacího nástroje hlášení o incidentu a provádějí jeho první identifikaci. Hlavním úkolem pracovníků podpory provozu je:

- zjistit od uživatelů / z monitorovacího systému co nejvíce informací o incidentu,
- provést primární identifikaci incidentu,
- přesně zdokumentovat zjištěná data,
- eskalovat incident na interní řešitelskou skupinu, nebo
- zjištěná data eskalovat na centrální kontaktní bod zhotovitele.

Při primární identifikaci incidentu používají pracovníci Objednatele obvykle, na základě analýzy bezpečnostních rizik, speciálně připravený seznam potenciálních incidentů spolu s pravděpodobnými důsledky jejich dopadu pro jednotlivé části organizace nebo pro organizaci jako celek.

PŘÍJEM A ŘÍZENÍ POŽADAVKU

Pracovníci zhotovitele na Centrálním kontaktním bodě provedou analýzu vzneseného požadavku ve smyslu souladu s poskytovanými službami na podporované technologie pod požadovaným SLA.
Primárním cílem Centrálního kontaktního bodu je:

- zaznamenat požadavek do informačního systému
- analyzovat soulad požadované kategorie a SLA požadavku a
- odmítnout s patřičným odůvodněním každý požadavek, jehož zadání bude v rozporu se smluvním plněním, nebo
- v případě akceptace požadavku zajistit eskalaci na řešitelskou skupinu v daném SLA a zajistit řešitele,
- průběžně sledovat plnění parametrů SLA

ŘEŠENÍ POŽADAVKU

Základní zjištěné informace o incidentu spolu s jeho primární identifikací jsou předány patřičnému řešitelskému týmu, který má za úkol dostat incident nejprve pod kontrolu a ve finále vyřešit. Řešitelský tým provede konečnou klasifikaci incidentu. De facto ověří platnost původní identifikace incidentu nebo jej překvalifikuje. Další náplní práce řešitelského týmu je získat všechny informace potřebné k vyřešení vzniklého incidentu. To znamená zjistit další data od Objednatele, vyhodnotit data z počítačové sítě (auditní záznamy, logy a další relevantní parametry a informace) a všechny zjištěné podklady důkladně, ale hlavně rychle, analyzovat.
Dle charakteru náročnosti incidentu je požadavek předán na odpovídající servisní řešitelskou úroveň:

- Level 1 Support - Jedná se o počáteční úroveň podpory, která je odpovědná za řešení základních a běžných incidentů a požadavků organizace a další služby vyžadující základní úroveň technické podpory. Primární funkcí podpory 1. stupně je shromáždit informace, provést základní analýzu a určit příčinu problému a základní klasifikaci. Podle povahy požadavku / incidentu zahájí řešitel 1. stupně podpory řešení s možností další eskalace. Technická podpora specialistů v této skupině typicky řeší přímočaré a jednoduché problémy a základní diagnostiky, provádí ověření dostupnosti jednotlivých vrstev infrastruktury (síťová, operační, vizualizační aplikační atd.), řeší základní uživatelské problémy (typicky zapomenutí hesla), odinstalace / reinstalace základních softwarových

aplikací, ověřování nastavení SW a HW atd. Řešitelé na této úrovni mají základní technické znalosti a nemusí být vždy zcela kompetentní pro řešení složitých incidentů, problémů a dalších požadavků. Nicméně, cílem této skupiny je zvládnout 70% -80% uživatelských problémů předtím, než dojde k eskalaci na vyšší úroveň podpory – Level 2 support.

- Level 2 support - Podpora 2. stupně představuje řešitelské týmy s hlubší produktovou / technologickou znalostí dané oblasti. Řešitelé na úrovni Level 2 Supportu jsou zodpovědní za poskytování součinnosti řešitelům 1. úrovně podpory při řešení eskalovaného incidentu / požadavku, což mimo jiné obsahuje i zpětnou kontrolu a podrobnější analýzu zjištěných dat předaných řešitelem 1. úrovně podpory, přičemž výstupem takové kontroly může být její potvrzení, upřesnění, nebo přehodnocení v závislosti na obchodních potřebách společnosti. Primárním cílem řešitelů na úrovni Level 2 Supportu je dostat incident co nejdříve pod kontrolu (např. formou workaround řešení) a ve finále jej vyřešit – s možností na eskalaci na vyšší úroveň podpory – Level 3 Support.
- Level 3 Support - Podpora 3. stupně představuje nejvyšší úroveň podpory, kompetenčně a kvalitativně schopným řešit ty nejobtížnější incidenty, problémy a požadavky. Řešitelé na této úrovni podpory jsou špičkovými technologickými odborníky ve svém oboru, majícími hluboké znalosti a rozsáhlé zkušenosti. Jednou z činností těchto expertních řešitelů je zajištění součinnosti řešitelům z 1-2. úrovně podpory při řešení nových, neznámých nebo příliš komplikovaných incidentů, problémů a ostatních požadavků, včetně provádění hloubkových analýz a řešení extrémních případů, kdy je ohrožena produktivita celé organizace a je potřeba rychle a efektivně incident vyřešit, nebo zajistit náhradní způsob řešení (workaroud) s maximálním ohledem na produktivitu, provozuschopnost a kontinuitu činnosti Objednatele. Další, podstatnou činností těchto expertních řešitelů je poskytovat specifickou strategickou a procesní podporu, zaměřenou na oblast strategie, bezpečnosti a procesů ICT, které se přímým způsobem podílejí na zvyšování konkurenceschopnosti, zefektivňování produktivity a zkvalitňování informační bezpečnosti. Součástí podpory 3. stupně je i zkušený a vysoce specializovaný bezpečnostní tým, který se orientuje na odhalování nedostatků, hrozeb, zranitelných míst a rizik, ať už ohrožují samotný informační systém, nebo jím zpracovávaná data. Důvody jsou zřejmé, neboť činnost organizací je stále více závislá na provozuschopnosti informačních systémů tvořených nejen technikou a technologiemi, ale také prostředím, obsluhujícím personálem a s tím vším souvisejícími procesy.

AKCEPTACE VYŘEŠENÍ POŽADAVKU

V této fázi je vyřešený požadavek / incident předán Objednateli do akceptace. Objednatel v této fázi:

- V případě spokojenosti akceptovat vyřešení požadavku, nebo
- v případě nespokojenosti eskalovat požadavek na řídící komisi k tomuto určenou a stávající se z oprávněných zástupců všech smluvních stran.

Akceptační proces musí mít vždy písemnou formu.

ŘEŠENÍ SPORŮ

V případě neshody v řešení jsou obě strany oprávněny vyeskalovat požadavek na manažerskou úroveň (řídící komisi), skládající se z odpovědných zástupců všech smluvních stran.
Mezi hlavní priority této komise patří vyvinutí nejvyššího úsilí k nalezení oboustranně akceptovatelného řešení.

VYHODNOCENÍ A UZAVŘENÍ POŽADAVKU

Vyřešením incidentu jsou zažehnány aktuální potíže organizace. Následná analýza a rozbor incidentu přináší poučení z příčin vzniku incidentu, vedoucí k následné aktualizaci analýzy (bezpečnostních) rizik. Na jejím základě jsou pak rizika přehodnocena. Obsahem etapy vyhodnocování incidentu jsou zejména:

- hlubší analýza incidentu a její závěry,
- aktualizace dat o vyřešených incidentech,
- poučení z incidentu pro potřeby zvyšování povědomí v organizaci,
- dopady incidentu na proces i obsah řízení incidentů.

V této etapě jsou dále zkušenosti získané při řešení incidentu zahrnuty do celého systému organizace.
Cílem této poslední etapy je zejména zobecnit z incidentu získané poznatky. Hlavními výstupy jsou:

- zobecnit závěry z incidentu směrem k analýze rizik, jejímu provedení a řízení,
- zobecnit dopady incidentu na řízení (bezpečnosti) IS/ICT organizace - aktualizace obsahu bezpečnostní / provozní dokumentace apod.,
- identifikovat a zavést případné změny do systému, upravit, zlepšit, nebo stanovit nové procesy a pravidla.

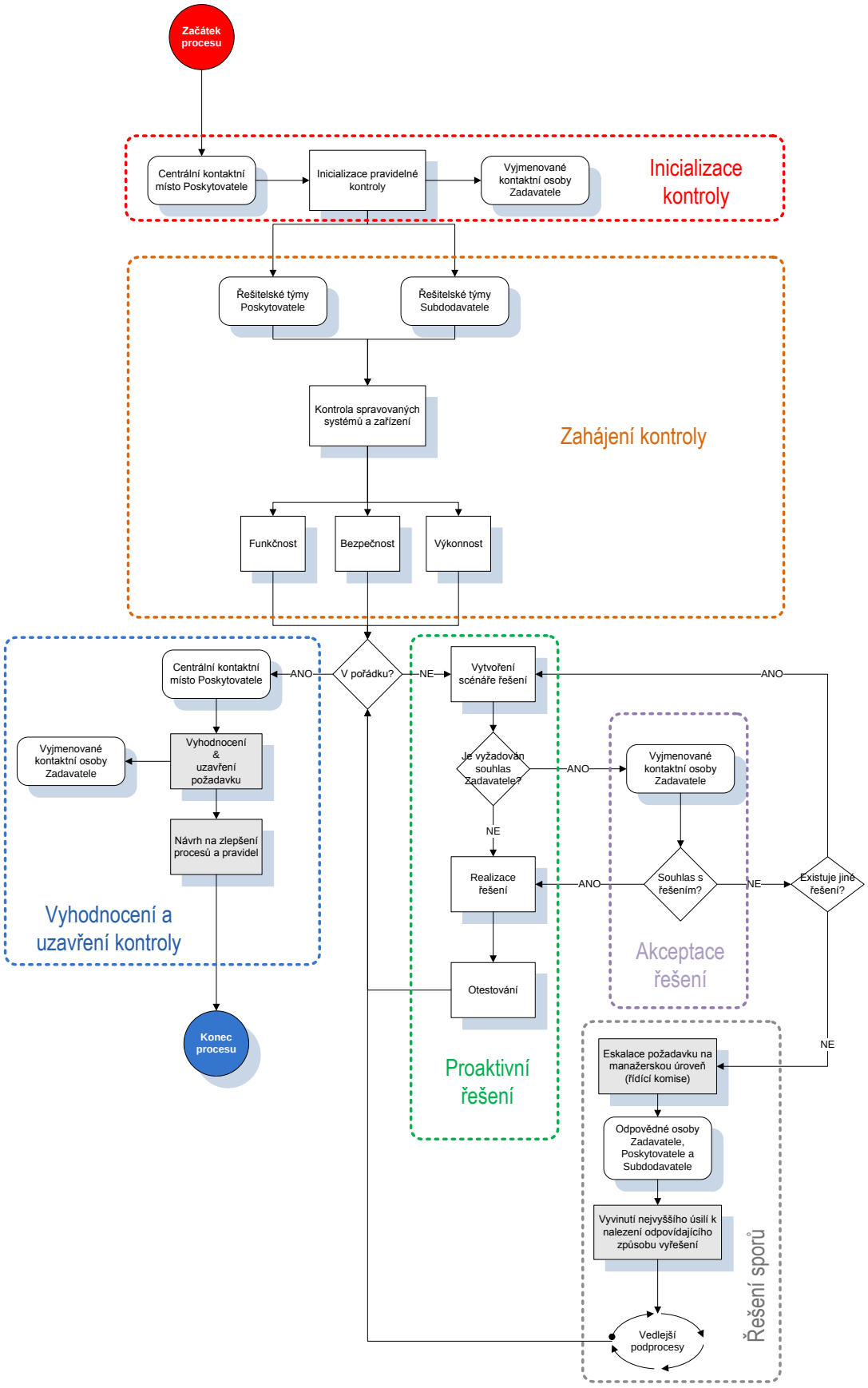
Etapa představuje finální zpětnou vazbu, kdy jsou zkušenosti, dovednosti a znalosti získané při řešení incidentu v oblasti IS/ICT promítnuty do strategické úrovně řízení informačního systému resp. celé organizace.

Provozní správa a činnosti prováděné automaticky – bez nutnosti jejich aktivace
Spektrum služeb požadované Objednatelem v rámci této kapitoly se zaměřuje primárně na oblast proaktivní podpory – tedy na oblast pravidelné správy podporovaných technologií a provádění činností vedoucí k zajištění stability řešení a eliminaci vzniku nenadálých událostí (incidentů).

Mezi činnosti (v souladu s požadavky Objednatele) pro tuto oblast podpory patří:

- **Pravidelné prohlídky** správné funkce spravovaných systémů a zařízení – pravidelné funkční kontroly podporovaných zařízení a technologií, prováděných vzdálenou formou – pokud to bude možné (např. kontrola logů, chybových hlášení a dalších informací ze systémů, revize výstupů z monitorovacího systému, kontroly spuštěných služeb apod.) a na místě (zejména mechanické profylaxe hardware – odsátí prachu, odstranění nečistot, kontrola kabeláže, výměna prachových filtrů, zvlhčovačů apod.)
- **Poskytování** informací o bezpečnostních rizicích – v této proaktivní oblasti využívá bezpečnostní tým Objednatele kombinaci vlastních zkušeností a know-how s konkrétními informačními zdroji. Bezpečnostní tým Objednatele pravidelně kontroluje a vyhodnocuje nově vzniklé bezpečnostní hrozby, a díky znalosti infrastruktury Objednatele dokáže porovnat tato potencionální bezpečnostní rizika a kvalifikovaně odhadnout, zda tato nová bezpečnostní hrozba může mít reální dopad na infrastrukturu Objednatele – pokud ano, s jakou pravděpodobností a s jakým možným důsledkem a jak toto riziko eliminovat, nebo alespoň co nejvíce snížit.
- **Poskytování informací o platnosti podpor** výrobce pro jednotlivé zařízení/SW, upozorňování na případné ukončení doby podpory zařízení/SW ze strany výrobce.
- **Aplikace bezpečnostních oprav** (vždy s předchozím souhlasem Objednatele) – v případě vzniku bezpečnostní opravy (např. patchů) bude tato skutečnost posouzena zhotovitelem s následným doporučením Objednateli na nutnost / doporučení jeho instalace (nebo otestování a instalace v případě, že Objednatel zajistí odpovídající testovací prostředí).
- **Reinstalace nových verzí SW** (vždy s předchozím souhlasem Objednatele) - v případě vzniku nové verze SW bude tato skutečnost posouzena zhotovitelem s následným doporučením Objednateli na nutnost /doporučení její instalace (nebo otestování a instalace v případě, že Objednatel zajistí odpovídající testovací prostředí).

V rámci zajištění provozní správy navrhujeme **u činností prováděných automaticky** následující procesně eskalační schéma:



INICIALIZACE KONTROLY

Inicializaci kontroly provádí pracovníci zhotovitele v rámci centralizovaného kontaktního místa.

Pracovníci Objednatele jsou v předstihu informování o této činnosti dle sjednaného kalendáře profylaktických služeb. Hlavní náplní této fáze je:

- Inicializovat a zaznamenat požadavek na automatickou kontrolu do informačního systému
- Eskalovat incident na odpovědnou řešitelskou skupinu
- Průběžně hlídat a vyhodnocovat plnění dle SLA parametrů dané služby

ZAHÁJENÍ KONTROLY

V okamžiku, kdy je požadavek předán na konkrétní řešitelský tým, provádí se standardně proces kontroly ze 3 rozdílných úhlů pohledu:

- Kontrola funkčnosti podporovaných systémů a zařízení
- Pátrání po nových bezpečnostních hrozbách
- Pátrání po zvýšení výkonnosti a zlepšení funkcionality

PROAKTIVNÍ ŘEŠENÍ

V případě detekce provozního nesouladu je řešitelským týmem navrhnut scénář nápravy. Zhotovitel je povinen informovat a vyžádat si souhlas navrženého řešení od Objednatele, zejména v případě aplikace bezpečnostních oprav (pro snížení bezpečnostní hrozby), nebo reinstalací nových verzí podporovaného software (pro zvýšení výkonnosti, zlepšení funkcionality apod.).

AKCEPTACE ŘEŠENÍ

V případě aplikace bezpečnostních oprav, nebo reinstalací nových verzí podporovaného software je Objednatel oprávněn před samotným zahájením řešení:

- Akceptovat navržené řešení
- Neakceptovat navržené řešení

V případě, že existuje další (náhradní) způsob řešení, je zhotovitel povinen tuto informaci předat bez zbytečného odkladu Objednateli. Pokud náhradní řešení neexistuje,

ŘEŠENÍ SPORŮ

V případě neshody v řešení jsou obě strany oprávněny vyeskalovat požadavek na manažerskou úroveň (řídící komisi), skládající se z odpovědných zástupců všech smluvních stran.
Mezi hlavní priority této komise patří vyvinutí nejvyššího úsilí k nalezení oboustranně akceptovatelného řešení.

VYHODNOCENÍ A UZAVŘENÍ KONTROLY

Detekce a eliminace nových bezpečnostních hrozeb přináší zejména zamezení vzniku nenadálých reaktivních událostí, a slouží také jako možný podklad vedoucí k následné aktualizaci analýzy (bezpečnostních) rizik.
V této etapě jsou dále zkušenosti získané při proaktivním řešení této události zahrnuty do celého systému organizace. Cílem této poslední etapy je zejména zobecnit získané poznatky. Hlavními činnostmi jsou:

- zobecnit závěry směrem k analýze rizik, jejímu provedení a řízení,
- zobecnit dopady incidentu na řízení (bezpečnosti) IS/ICT organizace - aktualizace obsahu bezpečnostní / provozní dokumentace apod.,
- identifikovat a zavést případné změny do systému, upravit, zlepšit, nebo stanovit nové procesy a pravidla.

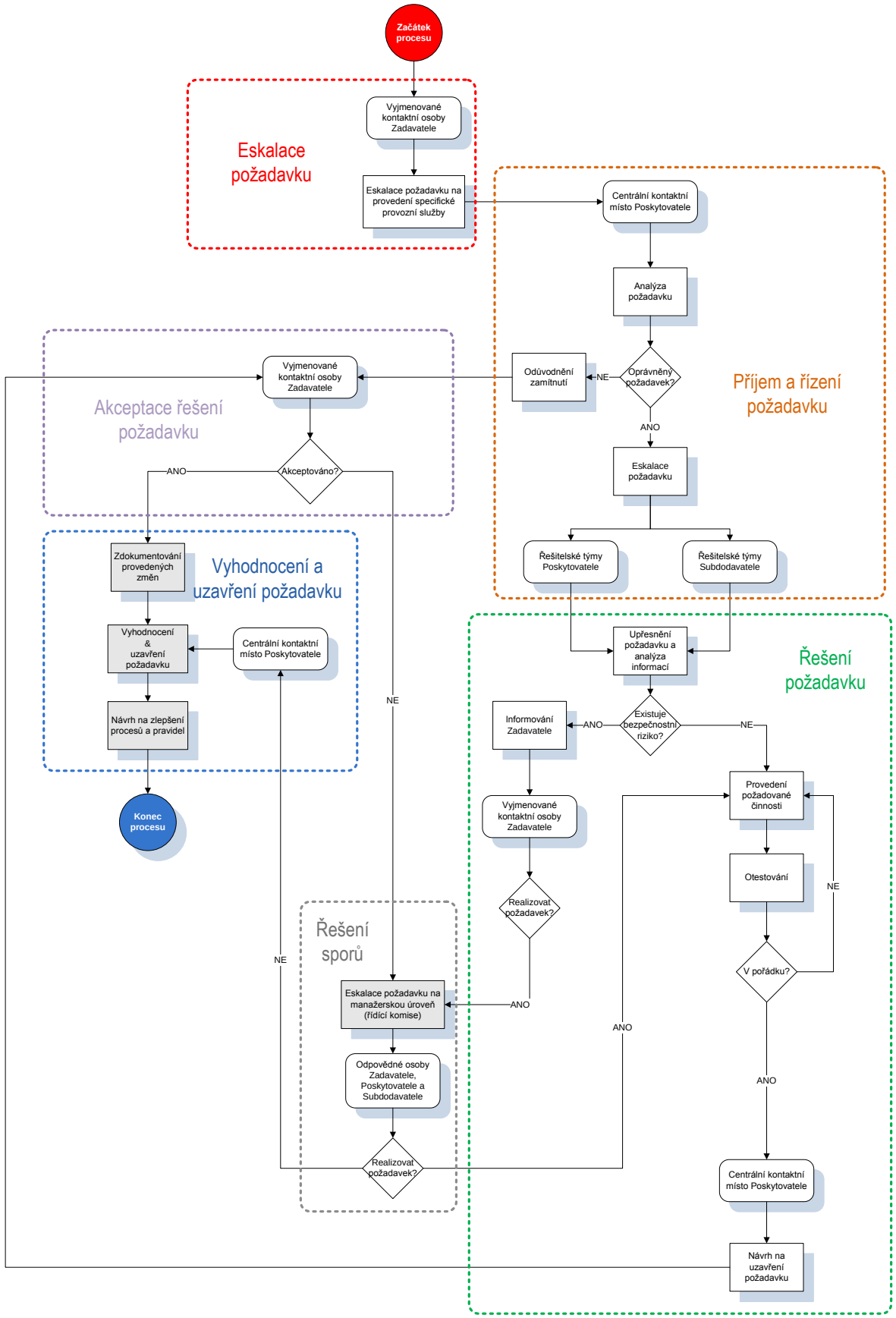
Etapa představuje finální zpětnou vazbu, kdy jsou zkušenosti, dovednosti a znalosti získané při řešení incidentu v oblasti IS/ICT promítnuty do strategické úrovně řízení informačního systému resp. celé organizace.

Provozní správa a činnosti prováděné na vyžádání
Spektrum služeb požadované Objednatelem v této oblasti se zaměřuje primárně na oblast proaktivní podpory – tedy na oblast pravidelné právy podporovaných technologií a provádění činností vedoucí k zajištění stability řešení a eliminaci vzniku nenadálých událostí (incidentů).

- **Příjem požadavku na provedení provozní správy** v režimu 7x24 - zajištěno centrálním Service Deskem společnosti AutoCont CZ a.s.

- **Provedení zálohy** konfigurací/nastavení před provedením požadované provozní činnosti – dle technologie bude provádět řešitel s adekvátní znalostí a certifikací.
- **Ověření možných dopadů realizace požadavku** na zachování funkcionality technologického celku, v případě existence rizik informování Objednatele požadavku o možných důsledcích provedení požadavku – řešitelský tým Objednatele s využitím kombinace vlastních zkušeností a technologického know-how s konkrétními informačními zdroji, posoudí možný negativní dopad zadaného požadavku na infrastrukturu Objednatele a v případě pojmutí podezření navrhne jiné řešení (pokud bude existovat), simulaci změny v testovacím prostředí, nebo doporučení k neprovádění požadované činnosti.
- **Provedení požadované činnosti provozního charakteru** na vyžádání (např. požadavku na změnu konfigurace, SW úpravu funkčnosti menšího rozsahu apod.) – tento typ služby se poskytuje primárně formou vzdáleného připojení, pokud se obě strany nedohodnou na jiném způsobu řešení.
- **Provedení požadavku** otestování funkčnosti dotčeného technologického celku – způsob, rozsah a hloubku testování dotčeného technologického celku předpokládáme dohodnout vždy ke konkrétnímu požadavku.

V rámci zajištění provozní správy u činností prováděných na vyžádání navrhujeme následující procesně eskalační schéma:



ESKALACE POŽADAVKU

Inicializaci požadavku na provedení specifické provozní služby hlásí pověřené kontaktní osoby zhotovitele na centralizované kontaktní místo zhotovitele.
Hlavní náplní této fáze je:

- Jasně popsat požadavek na provedení provozní služby
- Navrhnout předpokládaný termín pro zahájení řešení
- Stanovit kontaktní osoby ve vztahu k řešenému požadavku na straně pracovníků Objednatele

PŘÍJEM A ŘÍZENÍ POŽADAVKU

Pracovníci zhotovitele na Centrálním kontaktním bodě provedou analýzu vzneseného požadavku ve smyslu souladu s poskytovanými službami na podporované technologie pod požadovaným SLA.
Primárním cílem Centrálního kontaktního bodu je:

- zaznamenat požadavek do informačního systému
- analyzovat soulad požadované kategorie a SLA požadavku
- odmítnout s patřičným odůvodněním každý požadavek, jehož zadání bude v rozporu se smluvním plněním,
- v případě akceptace požadavku zajistit eskalaci na řešitelskou skupinu v daném SLA a zajistit řešitele,
- průběžně sledovat plnění parametrů SLA

ŘEŠENÍ POŽADAVKU

Řešitelský tým zhotovitele nejprve analyzuje požadavek na provedení provozní služby, zejména ověření možných dopadů realizace požadavku na zachování funkcionality technologického celku, v případě existence rizik informuje Objednatele požadavku o možných důsledcích provedení požadavku.
Pokud se jedná o reálnou hrozbu a řešitelský tým zhotovitele výslovně nedoporučí Objednateli provedení požadované provozní činnosti, avšak zhotovitel bude na provedení požadované činnosti trvat bez ohledu na rizika, je povinností tento požadavek eskalovat na manažerskou úroveň. V případě nenalezení žádného rizika následuje (pokud Objednatel požaduje) zálohování daného technologického prostředí, provedení poptávané provozní činnosti pod SLA, včetně otestování po provedené úpravě / změně (pokud Objednatel požaduje, nebo zhotovitel doporučuje).

AKCEPTACE VYŘEŠENÍ POŽADAVKU

V této fázi je vyřešený požadavek předán Objednateli do akceptace. Objednatel v této fázi může:

- V případě spokojenosti akceptovat vyřešení požadavku, nebo
- v případě nespokojenosti eskalovat požadavek na řídící komisi k tomuto určenou a stávající se z oprávněných zástupců všech smluvních stran.

Akceptační proces musí mít vždy písemnou formu.

ŘEŠENÍ SPORŮ

V případě neshody v řešení, nebo trvání na provedení provozního požadavku bez ohledu na doporučení zhotovitele, jsou obě strany oprávněny vyeskalovat požadavek na manažerskou úroveň (řídící komisi), skládající se z odpovědných zástupců všech smluvních stran.
Mezi hlavní priority této komise patří vyvinutí nejvyššího úsilí k nalezení oboustranně akceptovatelného řešení – v tomto případě k odsouhlasení provedení požadované provozní činnosti a vědomě akceptovat rizika, která mohou ovlivnit plnění ostatních služeb dle SLA, případně dostupnosti podporovaného řešení, nebo požadavek zrušit.

VYHODNOCENÍ A UZAVŘENÍ POŽADAVKU

V této etapě jsou řešené změny zahrnuty a popsány. Jsou vyhodnoceny parametry plnění dle příslušných SLA a po provedení a akceptaci řešení je vystaven protokol o provedení požadované činnosti. Dále může být předmětem (dle povahy řešené provozní činnosti) i úprava, zlepšení, nebo stanovení nových procesů a pravidla pro zvýšení efektivity poskytovaných servisních a provozních služeb.

Provozní správa – obecně zajišťované služby
Standardní součástí poskytovaných služeb v rámci provozní správy je:

- zaznamenání změn do technické provozní dokumentace,

- uložení informací o provedení provozního zásahu do elektronického systému pro příjem a evidenci požadavků na technickou (servisní) podporu

Další ustanovení na základě požadavků Objednatele:

- náklady související s poskytnutím služeb provozní správy jsou zahrnuty v ceně služby, žádné další náklady (cestovné, příp. nocležné apod.) související s poskytnutím služby, nebudou fakturovány,
- formou této služby nebudou řešeny požadavky na servisní zásahy (viz výše),
- čas na realizaci požadavků na provozní správu nebude snižovat předplacené hodiny expertní podpory,

Monitoring HW a základního SW

Součástí poskytování servisních služeb podpory je:

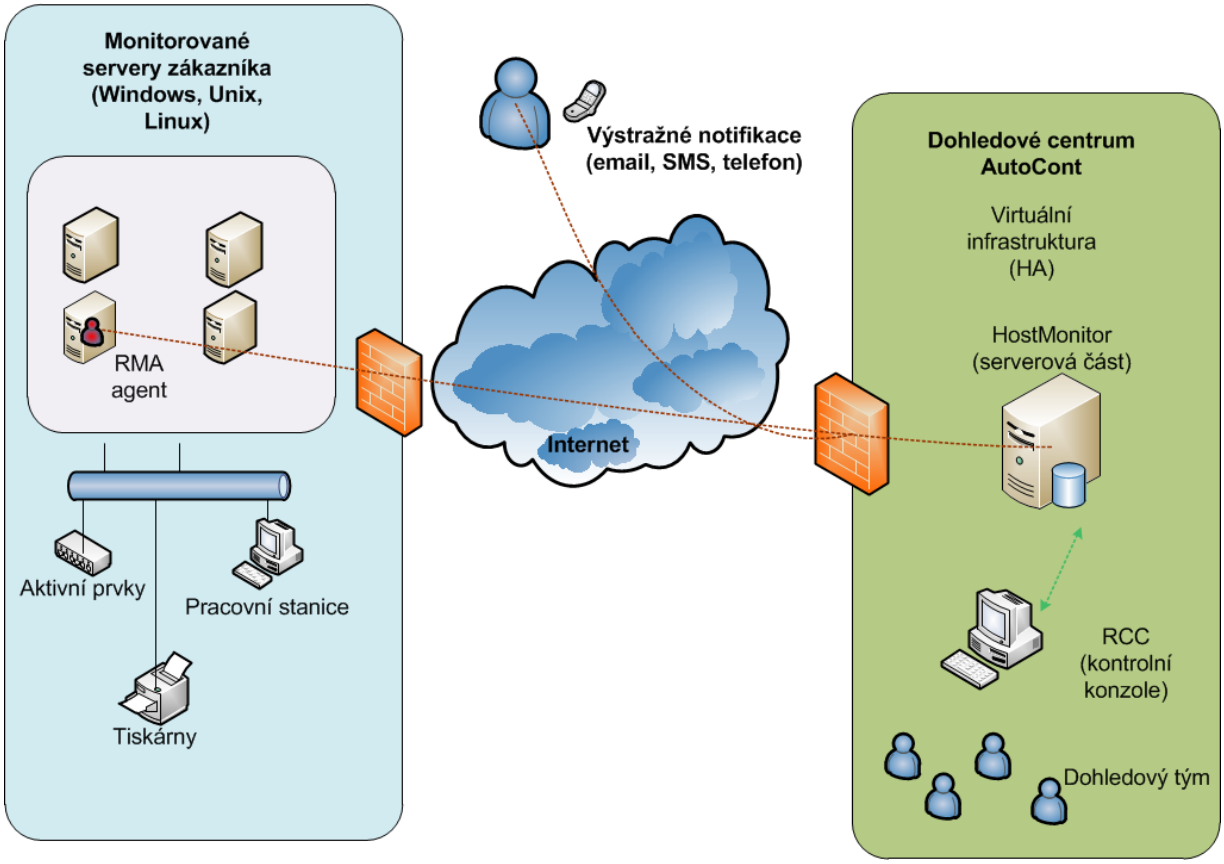
- nepřetržitý 24x7 proaktivní monitoring dostupnosti servisovaných zařízení,
- reakce do 30 minut na vzniklý mezní stav v uvedené době od jeho vzniku,
- nahlášení vzniklého mezního stavu určenému zástupci Objednatele,
- v dohodnutých případech okamžité zahájení řešení vzniklého mezního stavu (seznam situací bude podléhat souhlasu Objednatele a bude stanoven a aktualizován na základě návrhu zhotovitele),
- možnosti změn některých parametrů monitoringu (změna intervalu zjišťování stavu zařízení, změna počtu zachycených událostí, po nichž je vyhodnoceno zařízení jako nedostupné apod.),
- poskytování reportů o zaznamenaných mezních stavech, úpravy reportů na základě požadavků Objednatele.

Monitoring jako služba je koncipována jako řešení široce škálovatelné a je tedy vhodná jak pro malé firmy, které nemají vlastního IT správce, tak pro firmy střední velikosti, jejichž správci IT jsou vytíženi péčí o uživatele a provozované aplikace a monitorování serverové a síťové infrastruktury mohou bezpečně řešit prostřednictvím služby monitoringu společnosti AutoCont.

Monitoring přináší tyto hlavní výhody:

- vysoce škálovatelný software pro monitorování sítě
- proaktivní přístup k problémům v síti
- okamžitá informovanost o dění v síti
- šetří čas interních zdrojů společnosti
- nabízí různé způsoby reakcí na mezní hodnoty monitorovaných parametrů (telefonicky, e-mail a SMS).

Struktura je navržena s ohledem na bezpečnost a vysokou dostupnost. Služba je vybudována na systému Hostmonitor. Prostřednictvím sítě internet je tento systém připojen k serverům zákazníka pomocí RMA agenta.
HostMonitor je otevřený nástroj pro správu, který nepřetržitě monitoruje dostupnost serverů a výkonu. V případě chyby testovaného parametru HostMonitor upozorní správce sítě (nebo i opraví problém, když je to možné). To pomáhá chránit vaše firemní data a snižuje pravděpodobnost nákladných selhání sítě.
Za použití 62 zkušebních metod může HostMonitor zkontrolovat téměř libovolný parametr z vašich serverů. HostMonitor může kontrolovat veškeré služby TCP, ping, zkontroluje trasu, kontrola služeb, sledovat web, FTP, Mail, DNS servery. Také lze zkontrolovat volné místo na disku, velikost souboru nebo složky, kontrolu integrity souborů a webové stránky, testuje SQL servery, monitoruje síťový provoz a mnohem, mnohem víc.



Zkoušky lze provádět v pravidelných intervalech (např. každých 5 minut), nebo podle plánu (např. každý pátek osmnáct hodin až dvacet jedna hodin).
Služba monitoringu podporuje akce, které jsou navrženy tak, aby se systém zotavil z výpadku automaticky bez zásahu člověka (např. "restart služby", "restart počítače" atd.).
Služba potřebuje jen jeden TCP port pro komunikaci s agentem RMA (ve výchozím nastavení Pasivní RMA využívá TCP port 1055, Active RMA používá port 5056, ale lze použít jakýkoliv jiný port). Veškerý provoz mezi RMA a HostMonitorem je šifrovaný.

ZÁKLADNÍ TYPICKY SLEDOVANÉ PARAMETRY:
Windows platforma

- Výkonové parametry serverů: CPU, RAM
- Disková kapacita
- Logy: aplikační, systémový, DNS
- Služby: záloh, MS Exchange, služby informačních systémů (např. účetnictví, atd..), print spooler, SQL, Citrix, anti-x, ISA – je možno nastavit restart služeb
- Up Time
- NTP
- DNS, DHCP
- Velikost specifikovaných složek, souborů
- Definované porty – např. dostupnost portálů (CAG, OWA, Web portálů, ..)
- Poštovní servery - monitoring poštovního sytému kruhovým mailem (testuje se příjem pošty až do schránky a odeslání zpět na dohledový server)
- Exchange – fronta, velikost databází, velikost složky
- Kerio – velikost DB, velikost složky

VMware

- Logy: vmkernel, messages,
- Volné místo na vmfs svazcích
- Snapshoty

Ostatní

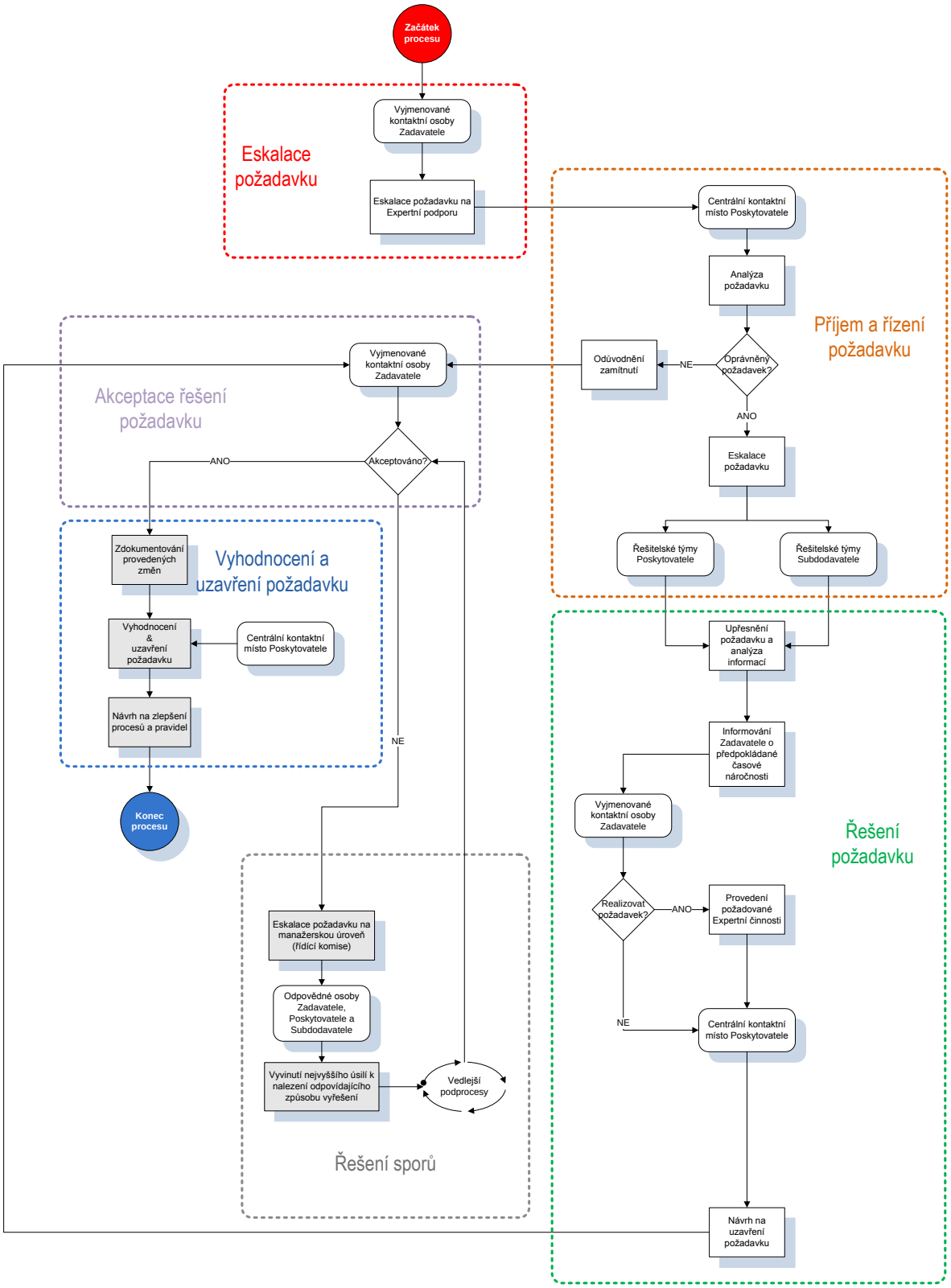
- Kontrola dostupnosti síťových prvků a konektivity – aktivních prvků, serverů, kritických PC,UPS, tiskáren, NAS
- Cisco – monitoring průtoku dat, vytížení CPU, teplota CPU
- HW: IBM a HP servery (omezeno generací serverů a funkčností managementu)
    - stav ventilátorů,
    - teplota komponent,
    - funkčnost zdroje,
    - stav disků

Expertní podpora

Obsahem expertní podpory jsou reaktivní i proaktivní služby poskytované nad rámec záruky. Podstatou činností expertní podpory je poskytovat specifickou strategickou a procesní podporu, zaměřenou na oblast strategie, bezpečnosti a procesů ICT, které se přímým způsobem podílejí na zvyšování konkurenceschopnosti, zefektivňování produktivity a zkvalitňování informační bezpečnosti.
Předmětem nabízených služeb zejména jsou:

- konzultační služby (telefonicky, emailovou komunikací, nebo v lokalitě Objednatele),
- řešení problémů (telefonicky, emailovou komunikací, nebo v lokalitě Objednatele),
- zajištění eskalace problémů na mezinárodní centra výrobců HW/SW,
- předkládání návrhů na rozvoj systémů - přidělení technického specialisty zhotovitele (systémového architekta), který bude mít přehled o provozovaných systémech, jejich architektuře a bude předkládat návrhy rozvoje a poskytovat konzultační služby související s provozem a rozvojem těchto technologií,
- zpracování oponentních posudků ke studiím, analýzám, technické dokumentaci předložených Objednatelem (nebo jeho partnerem) ovlivňujících provoz nebo rozvoj spravovaných technologií,
- možnost otestování nových technologií a technických řešení na prototypovém modelu,
- poskytování služeb v lokalitě Objednatele nebude mít dopad na cenu poskytované služby (cestovné a další náklady jsou zahrnuty v ceně služby),
- rozsah poskytovaných služeb 20 hodin měsíčně, nevyčerpané hodiny lze převádět neomezeně v rámci kalendářního roku,
- Součástí služby je i pravidelné reportování o poskytování služeb expertní podpory.

V rámci zajištění dodávky expertních služeb navrhujeme následující procesně eskalační schéma:



ESKALACE POŽADAVKU

Inicializaci požadavku na provedení expertní služby hlásí pověřené kontaktní osoby zhotovitele na centralizované kontaktní místo zhotovitele.
Hlavní náplní této fáze je:

- Jasně popsat požadavek na provedení provozní služby
- Navrhnout předpokládaný termín pro zahájení řešení
- Stanovit kontaktní osoby ve vztahu k řešenému požadavku na straně pracovníků Objednatele

PŘÍJEM A ŘÍZENÍ POŽADAVKU

Pracovníci zhotovitele na Centrálním kontaktním bodě provedou analýzu vzneseného požadavku ve smyslu souladu s poskytovanými službami na podporované technologie pod požadovaným SLA.
Primárním cílem Centrálního kontaktního bodu je:

- zaznamenat požadavek do informačního systému
- analyzovat soulad požadované kategorie a SLA požadavku a
- odmítnout s patřičným odůvodněním každý požadavek, jehož zadání bude v rozporu se smluvním plněním, nebo
- v případě akceptace požadavku zajistit eskalaci na řešitelskou skupinu v daném SLA a zajistit řešitele,
- průběžně sledovat plnění parametrů SLA

ŘEŠENÍ POŽADAVKU

Řešitelský tým zhotovitele nejprve analyzuje požadavek na provedení expertní služby, kvalifikovaně odhadne časovou náročnost na vyřešení poptávané expertní služby a tuto informaci bez zbytečného odkladu předá zpět Objednateli. V případě akceptace rozsahu plnění následuje realizace dodání expertní služby v dohodnutém termínu, pracnosti a pod SLA.

AKCEPTACE VYŘEŠENÍ POŽADAVKU

V této fázi je vyřešený požadavek předán Objednateli do akceptace. Objednatel v této fázi může:

- V případě spokojenosti akceptovat vyřešení požadavku, nebo
- v případě nespokojenosti eskalovat požadavek na manažerskou úroveň, stávající se z oprávněných zástupců všech smluvních stran.

Akceptační proces musí mít vždy písemnou formu.

ŘEŠENÍ SPORŮ

V případě neshody v řešení jsou obě strany oprávněny vyeskalovat požadavek na manažerskou úroveň (řídící komisi), skládající se z odpovědných zástupců všech smluvních stran.
Mezi hlavní priority této komise patří vyvinutí nejvyššího úsilí k nalezení oboustranně akceptovatelného řešení.

Provozní dokumentace

Součástí poskytování servisních služeb podpory je:

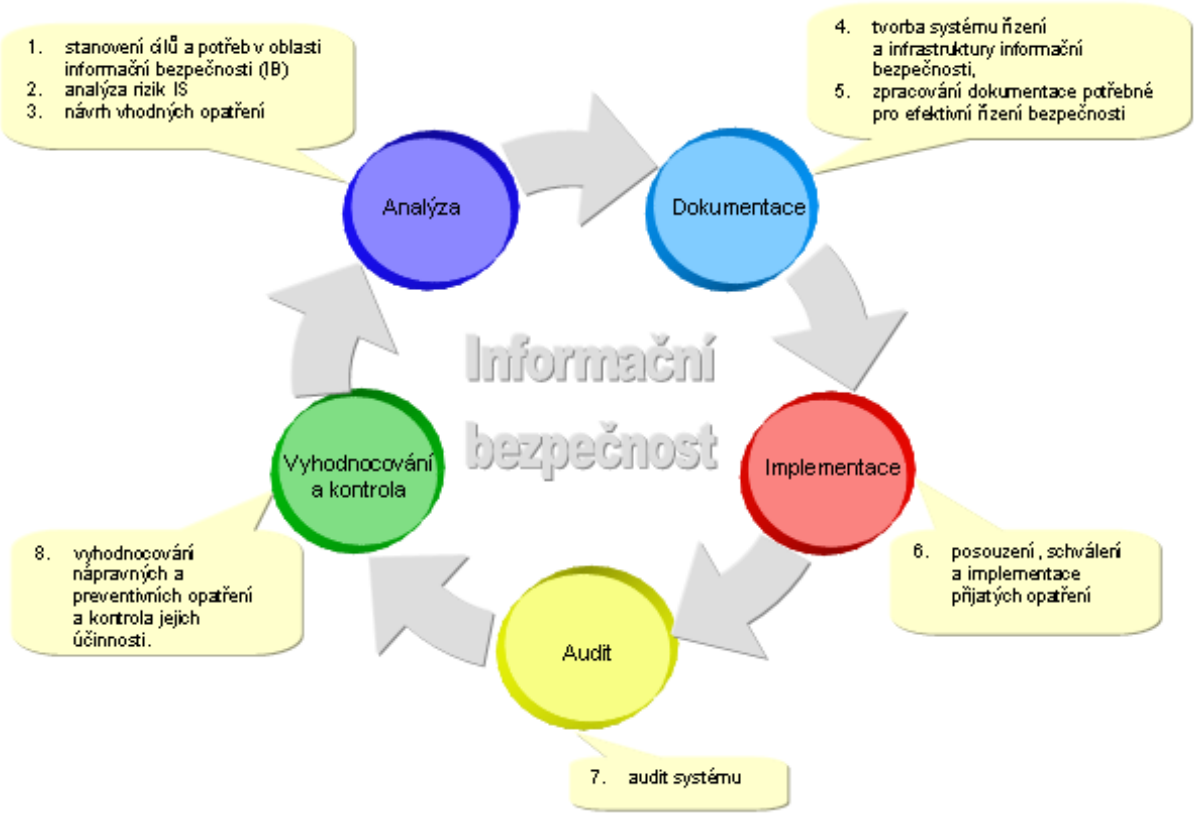
- vedení technické provozní dokumentace v elektronické podobě,

Další ustanovení na základě požadavků Objednatele:

- technická provozní dokumentace bude obsahovat strukturované základní technické a topologické údaje spravované infrastruktury, zejména základní evidenční údaje spravovaných zařízení a SW, jejich umístění, grafická schémata propojení včetně vazeb, platnosti podpor výrobců …),
- bude zajištěna pravidelná aktualizace technické provozní dokumentace po provedených změnách,
- bude zajištěno poskytování výstupů z technické provozní dokumentace oprávněným zástupcům Objednatele.

Řešení bezpečnosti pro oblasti A-E

Zhotovitel navrhuje využít ke komplexnímu řešení bezpečnosti TCK obecně doporučovaný a osvědčený procesní přístup k systému řízení bezpečnosti informací, tzv. ISMS (Information Security Management System, viz obrázek).



Systém řízení bezpečnosti informací TCK je založen na mezinárodně uznávaných ISO normách, konkrétně ČSN ISO/IEC 27001 (požadavky) a ČSN ISO/IEC 27002 (cíle a opatření). Pojem bezpečnost informací je v těchto normách definován jako zachování důvěrnosti, integrity a dostupnosti informací, a dalších vlastností jako např. autentičnost, odpovědnost, nepopiratelnost a spolehlivost.
Zavedení modelu PDCA známého jako „Plánuj-Dělej-Kontroluj-Jednej“ (Plan-Do-Check-Act) může být aplikováno na všechny procesy ISMS, které budou v souladu s uvedenými normami v TCK zavedeny.
Tento postup je možné použít pro budování ochrany dat a bezpečnosti ICT bez ohledu na potenciální zájem JMK získat certifikát dle normy 27001.

Bezpečnostní projekt TCK

Námi navrhovaná implementace bezpečnosti informací (nebo také informační bezpečnosti) v rámci plnění zakázky umožní, díky použitým metodikám a v návaznosti na nové požadavky v oblasti rozvoje řešení, zajistit i v budoucnu požadovanou bezpečnost definovanou v Bezpečnostním projektu TCK. Jednotlivé aspekty bezpečnosti informací se dotýkají a budou promítnuty do návrhu všech oblastí plnění této zakázky, tzn., že bezpečnostní požadavky vyplývající z této kapitoly budou zohledněny jak v návrzích konkrétního řešení architektury, infrastruktury či dodávaných aplikací, tak obecně v řešení celého životního cyklu dat a informací, včetně zabezpečení fyzického i logického přístupu k nim skrze jednotný systém IDM a zajištění dalších ochranných prvků.

Při řešení komplexní bezpečnosti je třeba zdůraznit potřebu koordinace činností všech subjektů podílejících se na realizaci jednotlivých oblastí plnění. Tuto koordinaci navrhujeme řešit vytvořením společného bezpečnostního týmu, v němž budou mít své zastoupení jak zástupci Objednatele, tak zástupci řešitelů jednotlivých subjektů. Bezpečnostní tým společně stanoví bezpečnostní rámec pro řízení a integraci bezpečnosti v průběhu plnění této zakázky.
Východiskem pro návrh celkové bezpečnosti provozu ICT a ochrany informací bude stávající bezpečnostní předpisová základna JMK (bezpečnostní politika a provozní řád).
Komplexní Bezpečnostní projekt TCK bude zahrnovat následující etapy, v nichž budou zohledněny všechny oblasti informační bezpečnosti, uváděné v zadání:

POČÍTAČOVÁ A KOMUNIKAČNÍ BEZPEČNOST TCK

Ochrana technické a technologické infrastruktury zahrnující zejména:

- řízení logického přístupu k počítačové síti, informačním systémům a informacím v nich zpracovávaným a ukládaným, (autentizace, autorizace, auditovatelnost), IdM,
- zajištění ochrany před škodlivým SW (antivir, antispyware, antispam apod.),
- opatření zajišťující bezpečnost počítačové sítě a komunikací (poskytovatelé připojení, aktivní prvky, bezdrátové připojení),
- kontrolu vzdáleného přístupu,

- firewally,
- systémy IDS/IPS, bezpečnostní dohled/monitoring,
- ochranu dat šifrováním (PKI),
- bezpečnou skartaci dat,
- update/upgrade SW (patch-management),
- systém zálohování, archivace,
- tvorbu a správu auditních záznamů a jejich vyhodnocování.

ORGANIZAČNÍ (A ADMINISTRATIVNÍ) BEZPEČNOST TCK

Požadovaná bezpečnostní opatření zahrnující:

- strukturu řízení (bezpečnostní role, funkce, kompetence),
- definici odpovědností a povinností,
- interní klasifikaci a vlastnictví aktiv,
- zajištění analýzy rizik, příp. její revize,
- přehled bezpečnostní předpisové základny,
- řízení přístupu třetích stran, outsourcing, servis (SLA),
- řízení incidentů,
- tvorbu, testování a aktualizaci havarijních plánů, řešení havárií,
- nezávislý audit a zajištění shody.

PERSONÁLNÍ BEZPEČNOST TCK

Týkající se bezpečnostních aspektů v oblasti zaměstnanců (personálu) a uživatelů:

- bezpečnostní požadavky na obsluhující personál,
- procesy náboru/změn/ukončení pracovního poměru zaměstnanců,
- systém bezpečnostního seznámení a vzdělávání,
- převzetí odpovědnosti, vymahatelnost, nepopiratelnost,
- systém hlášení, řešení a vyhodnocování incidentů.

FYZICKÁ BEZPEČNOST TCK

Objektová bezpečnost zahrnující:

- bezpečnost prostředí a ochranu objektu (bezpečnostní perimetr, ostraha),
- řízení fyzického přístupu ke klíčovým komponentám ICT,
- bezpečnostní prvky a opatření proti ztrátě, poškození či zničení fyzických (HW) aktiv a proti působení přírodních živlů,
- ochranu kabeláže, rozvodů a komunikačních kanálů,
- zásobování energií (vč. alternativních zdrojů), zajištění klimatizace (chlazení, vytápění),
- EZS a EPS atd.

Požadavky na bezpečnost informací jsou v normě ISO 27002 rozpracovány do celkem 11 detailně popsaných oblastí:

- Bezpečnostní politika (Security Policy)
- Organizace bezpečnosti informací (Organization of Information Security)
- Řízení aktiv (Asset Management)
- Bezpečnost lidských zdrojů (Human Resources Security)
- Fyzická bezpečnost a bezpečnost prostředí (Physical Security)
- Řízení komunikací a provozu (Communications and Ops Management)
- Řízení přístupu (Access Control)
- Akvizice, vývoj a údržba informačních systémů (Information Systems Acquisition, Development, Maintenance)
- Zvládání bezpečnostních incidentů (Information Security Incident Management)
- Řízení kontinuity činností organizace (Business Continuity)

- Soulad s požadavky (Compliance)

Analýza řešení
Cílem této etapy bude identifikace a analýza bezpečnostních požadavků týkajících se všech oblastí plnění (A-E) v rámci informační bezpečnosti.
V každé z oblastí plnění budou identifikovány a dále analyzovány bezpečnostní požadavky z hlediska:

- zákonných, regulatorních a jiných závazných předpisů, nadřízených orgánů apod.,
- technického řešení technologického centra Jihomoravského kraje, integrace vnitřního systému krajského úřadu, elektronické spisové služby, datových skladů, manažerských informačních systémů a nástrojů Business Intelligence a krajské digitální spisovny a krajského digitálního repositáře,
- norem, standardů a „best practices“.

Tato kapitola se v některých aspektech prolíná s kapitolami popisujícími technické řešení všech oblastí plnění, jež lze samo o sobě považovat za dílčí řešení bezpečnosti. Výstupem této etapy bude souhrn a analýza bezpečnostních požadavků ve všech oblastech plnění z výše uvedených hledisek.

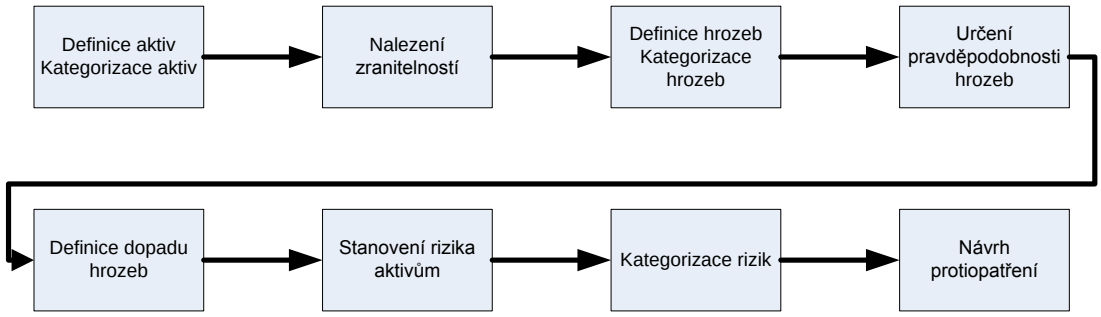
Analýza rizik
Cílem této etapy bude identifikovat a analyzovat rizika týkající se informační bezpečnosti pro každou z oblastí plnění (A-E), a dále navrhnout opatření k odstranění či eliminaci zjištěných rizik. Pod pojmem efektivní opatření rozumíme taková opatření, která zohledňují hodnotu daného aktiva, pravděpodobnost realizace hrozby, dopad uskutečnění hrozby na kontinuitu činnosti organizace a hodnotu (cenu) realizovaných protiopatření. To umožní přistupovat k řešení bezpečnosti diferencovaně podle důležitosti a požadavků na zabezpečení a dostupnost dat, a tak zabránit neefektivní paušální aplikaci relativně nákladných nebo naopak nedostatečně účinných bezpečnostních technologií na celý systém.
Analýzu rizik chápeme jako zahájení komplexního procesu, jehož výsledkem bude trvalé zajištění požadované úrovně bezpečnosti aktiv organizace, která jsou uložena a spravována pomocí informačních systémů a technologií. Analýza rizik představuje dále podklad pro vytvoření, případně revizi plánu zvládání rizik (tzv. Plánu bezpečnosti), z jehož změn je následně možné odvozovat i nutné změny metrik bezpečnosti.
Rozsah analýzy odráží požadavky Objednatele a pokrývá tedy všechny definované oblasti:

- bezpečnost informačních a komunikačních technologií (dále jen ICT),
- fyzická (objektová) bezpečnost,
- personální bezpečnost,
- administrativně-organizační bezpečnost.

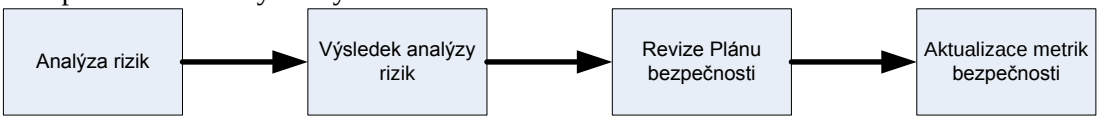
METODIKA
Analýza rizik bude realizována na základě doporučení mezinárodních norem řady ISO 2700x, konkrétně ČSN ISO/IEC 27005:2009.
Realizace analýzy rizik bude probíhat v souladu s přijatou a Objednatelem schválenou metodikou, v jejímž rámci bude stanoven:

- způsob hodnocení aktiv, pravděpodobností, zranitelností a dopadů uskutečnění hrozeb,
- způsob stanovení míry a akceptovatelnosti rizik,
- způsob měření účinnosti implementovaných opatření,
- způsob určování priorit pro navrhovaná opatření.

Metoda provedení analýzy rizik je zřejmá z jejího cíle – nejprve jsou definována aktiva organizace, následně jsou určeny veškeré hrozby těmto aktivům a ty jsou analyzovány z hlediska zranitelnosti. Z výsledné zprávy (analýzy) vyplývají navrhovaná bezpečnostní opatření.
Pod pojmem analýza je možné si představit posouzení pravděpodobnosti realizace jednotlivých hrozeb vůči jednotlivým aktivům či skupinám aktiv z hlediska jejich hodnoty a dopadu případného uskutečnění jednotlivých hrozeb na jednotlivá aktiva.
Pokud jsou definována aktiva i hrozby, je možné začít posuzovat pravděpodobnost jejich realizace.
Z pravděpodobnosti realizace hrozby s definovaným dopadem je potom možné stanovit míru rizika.
Jednotlivá rizika jsou následně kategorizována a na základě stanovených kategorií je navrženo protiopatření.
Průběh analýzy rizik je možné schematicky zobrazit takto:



Samotná analýza je ještě rozdělena do organizačních celků souvisejících s jejím vlastním průběhem – přípravné práce (návštěva specialisty nebo specialistů, kteří pomocí interview nebo dotazníkovou metodou získají informace nezbytné pro definici aktiv organizace, definici hrozeb, pravděpodobnost jejich realizace a jejich dopad na funkčnost IS, posouzení organizačních opatření ochrany aktiv a v neposlední řadě informace potřebné pro posouzení technické části opatření), a následná samotná analytická část zpracování informací a výsledků, jejímž výstupem je zpráva o bezpečnosti a navrhovaná bezpečnostní opatření.
Aby bylo možné posuzovat dosažení jednotlivých cílů v oblasti informační bezpečnosti, jsou stanoveny jejich metriky. Metrika je konkrétně definované kritérium, které slouží k měření a hodnocení dosažené úrovně stavu zabezpečení ICT.
Postup lze schematicky zachytit takto:



V okamžiku, kdy jsou známa rizika a tato jsou kategorizována, a je známo i jakým způsobem jim lze čelit, je možné vytvořit nebo provést revizi stávajícího plánu zvládání rizik (dále také Plánu bezpečnosti). Plán bezpečnosti definuje postup realizace jednotlivých bezpečnostních projektů, a je tedy zřejmé, že případná změna rizik nutně vyvolává potřebu revize Plánu bezpečnosti.

POSTUP NAPLNĚNÍ ETAPY

Jak je uvedeno v předchozí obecné části, základním úkolem je definování aktiv organizace, tj. té části, na kterou je třeba se při analýze zaměřit, dále jejich ohodnocení, následně určení jejich zranitelností a jim odpovídajících hrozeb, a poté z nich vyplývající ohodnocení pravděpodobnosti a dopadů hrozeb. V daném okamžiku je také potřeba seznámit se s bezpečnostní dokumentací, systémem řízení bezpečnosti a procesy řízení bezpečnosti, jsou-li nastaveny a dokumentovány.
Pro zpracování analýzy rizik bezpečnosti informací bude použita jednotná metodika, vycházející z normy ČSN ISO/IEC TR 13335 v oblasti přístupu k analýze rizik, a dále z normy ISO 27005 v oblasti realizace a managementu rizik, související s požadavky systému řízení bezpečnosti informací (dále jen ISMS) dle normy ISO 27001.
Analýzu rizik lze realizovat výběrem vhodného přístupu, tj. od základního přes neformální až k detailnímu přístupu, nebo využít kombinovaného způsobu, při kterém lze uplatnit výhody jednotlivých přístupů pro konkrétní potřeby. V případě JMK byl zvolen jako nejvhodnější kombinovaný přístup umožňující po zjištění základních informací a požadavků definovat klíčové rizikové oblasti a poté přistoupit k jejich detailní analýze. Analýza rizik pak posuzuje aktiva zejména s přihlédnutím k důsledkům hrozeb.
Navrhovaný kombinovaný přístup k analýze rizik zahrnuje následující:

- zjištění (analýzu) požadavků na bezpečnost (organizačních, legislativních, technologických, personálních);
- vlastní analýzu rizik (v závislosti na aktivech, hrozbách, zranitelnosti, pravděpodobnosti a dopadech) obsahující:
    - identifikaci aktiv, tj. zjištění hmotných a nehmotných hodnot, jakými jsou např. HW-aktiva, SW-aktiva, informační aktiva, tj. data, případně služby, fyzické prostředí, tj. budovy, ostatní zařízení a vybavení;
    - definici hrozeb, tj. stavů a situací s negativním dopadem na činnost JMK, jakými jsou např. úmyslné a neúmyslné působení lidského faktoru, živelní katastrofy, havárie, technické poruchy, závady apod.;
    - identifikaci zranitelných míst, tzn. zjištění slabin a bezpečnostních děr posuzovaného systému;
    - identifikaci pravděpodobnosti uskutečnění hrozby a dopadů, neboli kvalitativní posouzení míry konkrétního rizika, že se uskuteční určitá hrozba, jež využije daného zranitelného

místa, ohodnocení bezpečnostních rizik a postup jejich zvládání, stanovení kritérií pro akceptaci rizik a určení odpovědností. Míra rizika je definována v několika úrovních, které mj. dovolují stanovit hranici pro akceptovatelná rizika;
    - identifikaci stávajících bezpečnostních opatření v závislosti na procesech;
    - srovnání a zhodnocení dostatečnosti a účinnosti stávajících bezpečnostních opatření s definovanými cíli, požadavky a identifikovanými riziky a posouzení reálné pravděpodobnosti selhání přijatých opatření;
    - návrh a specifikaci vhodných opatření a kontrol na eliminaci rizik a implementace vhodných prostředků a technologií k zajištění navrhovaných opatření, včetně stanovení priorit k řešení zjištěných neshod;
    - ohodnocení důležitosti jednotlivých opatření a přínosů.

V základním zjednodušeném členění pro lepší přehlednost a porozumění posuzujeme rizika v následujících oblastech:

- organizační (a administrativní) bezpečnost tj. např. struktura a hierarchie řízení, odpovědností, pravomocí, kompetencí, povinností, interní předpisy atd.;
- personální bezpečnost tj. nábor/ukončení pracovního poměru uživatelů, seznámení uživatelů, bezpečnostní vzdělávání, vymahatelnost odpovědnosti, prověřování, povinnosti týkající se důvěrnosti/mlčenlivosti, dodržování předpisů, řešení incidentů, autorských práv, legálnosti SW apod.;
- fyzická (objektová) bezpečnost tj. ochrana objektu/lokality, bezpečnostní perimetry, zajištění infrastruktury (zdroj energie, telekomunikační služby, klimatizace/vytápění), fyzický přístup ke klíčovým komponentám prostředí JMK, opatření proti ztrátě, poškození či zničení fyzických aktiv;
- počítačová a komunikační bezpečnost tj. ochrana logického přístupu do prostředí JMK – zabezpečení komunikace, access/identity management (uživatelské účty, přístupová práva), ochrana před škodlivým SW, šifrování, bezpečná skartace dat, zálohování, atd.

Na základě interview a dotazníků vyplněných s odpovědnými zástupci prostředí ICT JMK, požadavků (globálních a specifických pro dané prostředí), identifikace aktiv, hrozeb, zranitelných míst, posouzení pravděpodobnosti, dopadů, analýzy existující dokumentace, případně doplňujících konzultací, bude zpracována výsledná zpráva podrobně definující veškerá zjištěná rizika a navrhovaná opatření.

VÝSTUPY Z ANALÝZY RIZIK

Výstup z analýzy rizik bude mj. obsahovat:

- identifikaci a ohodnocení aktiv,
- identifikaci a určení pravděpodobnosti výskytu a dopadů hrozeb,
- identifikaci a ohodnocení zranitelností aktiv,
- určení míry rizik,
- interpretaci výsledků analýzy rizik,
- návrh rozhodnutí o řízení rizik a stanovení postupů pro pokrytí rizik.

Součást výsledné zprávy budou tvořit podle potřeby a účelnosti samostatně zpracované přílohy např. z technické/technologické části analýzy, přehledové tabulky, případně další specifické výstupy z detailní analýzy rizik.

Penetrační testy

Penetrační testování bezpečnosti IS je jednou z častí komplexního procesu řízení informační bezpečnosti, který má podobu Demingova procesního cyklu PDCA (kontinuální vylepšování). Penetrační testování tedy primárně zkoumá stávající stav zabezpečení informačního systému a jeho výstupy jsou zpravidla podkladem pro opakovanou analýzu rizik.

Jedním ze základních přínosů této služby je zjištění, jakou míru proniknutelnosti mají aktuálně přijatá opatření ochraňující klíčová aktiva společnosti. Penetrační testy následně umožní:

- správně a účinně investovat do opatření,
- neplýtvat prostředky, ochránit bezpečnostní investice,
- cíleně plánovat zvýšení úrovně zabezpečení,
- implementovat technologie, které poskytnou požadovanou ochranu.

Běžný postup při penetračních testech:

- seznámení s prostředím,

- plánování útoku,
- útok a jeho vyhodnocení,
- dokumentace a interpretace výsledků.

VYSLOVENÍ SOUHLASU S TESTOVÁNÍM

V současné době nám není znám normativ, který výslovně upravuje aktivity penetračního testování. Nicméně při používání testů může dojít k situacím, u kterých je sporné, zda nedochází k omezování vlastnických práv osob, případně se nejedná o zlý úmysl. Z těchto důvodů je nutné vyslovení souhlasu s testováním – testovací mandát. Tento souhlas opravňuje testovací tým k vykonávání jednotlivých testů.

MAPOVÁNÍ

Tato kapitola zahrne ve zvolené tvrdosti, viditelnosti, čase, rozsahu a znalosti prostředí aktivity, které útočníka informačně obohatí. Mapování slouží k simulaci toho, jaké informace je schopen potenciální útočník získat o prostředí Objednatele. Za informační zdroje pro tento krok budou použity veřejné i neveřejné zdroje, invazivní i neinvazivní techniky. Zjištěné informace budou následně využity pro stanovení ideálního postupu útoku. Mezi tyto informace patří např. adresní prostory, otevřené porty, identifikace operačního systému, jmenné konvence apod.

STANOVENÍ POSTUPU

Stanovení postupu bude probíhat na základě zjištění získaných v předchozím bodě, bude vytvořen plán, podle kterého se bude realizovat vlastní útok/y, zejména ve vztahu k parametru času. Zajistí/připraví se např. vhodné body sloužící pro útok(y), stanoví se priority a provázanost jednotlivých kroků, připraví se nezbytné technické vybavení.

HLEDÁNÍ SLABIN A ZRANITELNOSTÍ

Tato činnost bude realizována automatizovaně i ručně, zejména ve vztahu k parametru času. Automatická kontrola slouží k objevení chyb, které jsou většinou jednoduše zneužitelné, a jejichž potenciál je již dokumentován. Manuální testy kladou maximální důraz na kreativitu a kombinatoriku simulovaného útočníka a zpravidla odhalují chyby, které nejsou jednoduše zneužitelné, ale mohou být velmi nebezpečné. Ručně budou prověřeny především chyby a komentáře v případně nalezeném kódu www stránek a aplikační logika, vstupy ve formulářích, Session Management, Cookie Management, Directory Traversal, Hidden Directory, Track a případně jiné chyby, které vyplynou z předchozích kroků.

POKUS O PRŮNIK

V této fázi je realizován pokus o průnik s využitím zjištěných slabin a zranitelností, zejména ve vztahu k parametru času. Konkrétní způsob útoku bude stanoven v předchozím bodě, předpokládáme i kombinaci různých technik. Cílem útoku je prokázat nebo vyvrátit existenci slabin nalezených v předchozím kroku, které lze potenciálním útočníkem zneužít a uskutečnit tak průnik do interní sítě Objednatele. Jde například o hádání hesel, DoS, SQL Injection, Content Injection, Cross Site Scripting, Web Cache Poinsoning, Buffer Overflow.

KOREKCE

Korekce v průběhu útoku slouží pro vyhodnocení zjištěných faktů ke zmírnění či rozšíření daného útoku, případně k rozvinutí nového typu útoku. Tento bod se v průběhu testu opakovaně aplikuje na základě výsledků jiných útoků nebo zjištění.
V tomto kroku dojde k vyhodnocení získaných informací a identifikaci rizikových oblastí. Výstupem z celého procesu je popisný dokument zjištěných faktů a jednotlivých pokusů o průnik, včetně doporučení jak řešit problematická místa.
Na základě výše popsaných parametrů je pro související vrstvy použito technik a nástrojů z následujícího výčtu:

- pro fyzické prostředí – místní obhlídka, prostupy do areálů, budov, kanceláří, překonání bariér této vrstvy ať již silou nebo logickými manipulacemi.
- pro boxy, hardware a fyzická propojení – testy manipulace, znefunkčnění propojení, manipulace s boxy, kabely, zásuvkami.
- pro aktivní propojení, připojení – testy manipulace a zmatení a znefunkčnění komponent účastnících se na aktivním propojení systémů, ARP, IP Spoofing, Squatting…

- pro aplikace a data – testy publikovaných zranitelností, například Remote Executing, Script a Code Injection, Cross Site Scripting, Parameter Manipulation.
- pro procesy osoby a role – možnosti průzkumu, manipulace, matení, cyklení, smyčkování.

Volba rozsahu není pro případ nabízeného typu testu stanovena pevně předem a dle zjištěných okolností bude přizpůsobena tak, aby byl maximalizován užitečný výstup.
Výstupem je vždy zpráva – forma sdělení, která je maximálně srozumitelná, odpovídá potřebám zákazníka a zahrnuje:

- Podrobný report, tj. zdokumentování použitých technik a jejich výstupů;
- Manažerské shrnutí, tj. zkrácená forma zaměřená na klíčové nálezy a jejich interpretaci;
- Prezentace výsledků – osobní interaktivní konzultace nad výsledky.

Plán bezpečnosti
Zpracování plánu bezpečnosti chápeme jako vytvoření návrhu harmonogramu realizace přijatých bezpečnostních opatření vyplývajících z předchozí realizace analýzy rizik. Návrh opatření bude konfrontován s hrozícími riziky identifikovanými v etapě Analýza rizik. U každého navrhovaného opatření bude v závislosti na stanovené míře takto eliminovaného rizika možno určit, do jaké míry bude toto riziko zmírněno nebo odstraněno. Tímto způsobem bude možné genericky analyzovat rizika, sledovat účinnost navrhovaných opatření a zvyšovat úroveň zabezpečení.
Plán bezpečnosti bude obsahovat nároky a požadavky na implementaci navrhovaných opatření, tj. zejména:

- kapacity,
- čas,
- personál,
- zdroje,
- finanční náklady,
- požadované priority.

Tento dokument bude mít za cíl definovat veškeré koordinované akce, které mají být realizovány pro zajištění implementace navrhovaných a posléze schválených bezpečnostních opatření v krátkodobém, střednědobém a dlouhodobém horizontu.
V rámci této etapy bude realizováno zpracování Plánu bezpečnosti s ohledem na výsledky analýzy rizik, a to v rozsahu potřebném pro splnění požadavků normy ISO 27005. Plán bezpečnosti stanoví opatření a postupy na straně Objednatele, které povedou ke splnění požadavků platné legislativy, zejména zákona č. 111/2009 Sb., o základních registrech, v platném znění a ke splnění požadavků daných normou ISO 27002.
Na základě zpracované analýzy rizik je možné rozhodnout o dalším postupu, který povede k odstranění zjištěných nedostatků v organizační (procesní) oblasti. V daném okamžiku je i v tomto případě velmi předběžné předjímat výsledek a tudíž stanovovat i další opatření, ale mezi taková opatření zařazená do Plánu bezpečnosti může typicky patřit:

- zavedení bezpečnostní politiky organizace pro oblast řízení/organizace bezpečnosti (vedení, vyhodnocování, kompetence, odpovědnost),
- řízení aktiv,
- klasifikace dat,
- personální bezpečnost (řízení lidských zdrojů, požadavky na personál),
- fyzická (objektová bezpečnost),
- přidělování přístupů a přístupových oprávnění,
- audit a zajištění shody,
- řízení komunikací a provozu,
- akvizice, vývoj a údržba informačních systémů,
- vytvoření plánu zvládání rizik a metrik bezpečnosti,
- řešení bezpečnostních incidentů,
- vytvoření systému bezpečnostních směrnic a pracovních postupů,
- zpracování havarijních plánů, plánů obnovy a zajištění kontinuity a konkrétních postupů,
- testování bezpečnosti – vytvoření testovacího plánu (testování systémů zevnitř, zvenčí, vlastními prostředky a nezávislými externími testery atd.),

Na základě analýzy rizik je dále možné rozhodnout o dalším postupu, který povede k odstranění případně zjištěných nedostatků v technologické oblasti. Mezi technická opatření může patřit:

- návrh a implementace zabezpečení prostředí, tj. např. fyzického perimetru a opatření objektové/fyzické bezpečnosti,
- řešení v oblasti přístupu (fyzického i logického),
- řešení autentizace a autorizace,
- kontrola obsahu,
- IPS/IDS,
- antivirová ochrana vč. antispyware a antispamu,
- šifrování, integrita (PKI),
- systémy patch-managementu,
- systémy identity-managementu,
- řešení zálohování,
- systémy řízení bezpečnosti a incidentů,
- monitoring,
- sledování aktivit serverové a síťové infrastruktury,

Pro výběr opatření eliminujících zjištěná rizika v souladu s jejich kategorizací navrhujeme využít soubor postupů a doporučení z takových zdrojů, jako jsou např. TR 13335, potažmo ISO 27002 apod. Podrobný návrh opatření pro zajištění informační bezpečnosti, optimalizaci procesů a přiřazení bezpečnostních prvků, včetně podrobného harmonogramu implementace navržených opatření, postupů a nástrojů, bude obsahovat:

1. Technologická opatření, která jsou založena na použití konkrétních technik, technických prvků či zařízení, dostupných technologií, bezpečnostních komponent, funkcí a prvků, vč. specializovaného SW apod., a vztahují se na následující oblasti (dle ČSN ISO/IEC 27001):
    - řízení komunikací a provozu,
    - řízení přístupu,
    - akvizice, vývoj a údržba informačních systémů,
    - zvládání bezpečnostních incidentů.
2. Procesní opatření, jež jsou určena k zavedení, prosazování a kontrole dodržování potřebných bezpečnostních politik, procesů, metod, postupů, aktivit a chování zajišťujících bezpečnost prostředí JMK, potažmo dat v něm zpracovávaných jak zvenčí (vnějšími uživateli), tak zevnitř (provozovatelem a správcem systému v chráněném prostředí počítačové sítě), která se vztahují na následující oblasti (dle ČSN ISO/IEC 27001):
    - politika bezpečnosti,
    - organizace bezpečnosti informací,
    - řízení aktiv,
    - bezpečnost lidských zdrojů,
    - fyzická bezpečnost a bezpečnost prostředí,
    - řízení kontinuity činnosti,
    - soulad s požadavky.

Výstupem z této etapy bude:

- podrobně zpracovaný implementační manuál popisující všechna doporučení a kroky k realizaci nápravných opatření vzešlých z analýzy rizik, dopadů a penetračních testů,
- rozpracování bezpečnostních cílů jednotlivých činností dle plánu zvládání rizik, harmonogramu a způsobů realizace.

Vytvoření interních předpisů TCK

V rámci této etapy bude realizováno vytvoření, případně aktualizace bezpečnostní předpisové základny Objednatele, a to v rozsahu potřebném pro splnění požadavků systému řízení bezpečnosti informací (ISMS), při zohlednění stávající interní předpisové základny a související dokumentace s vazbou na systémy řízení kvality a procesů souvisejících s provozováním ICT a dlouhodobého řízení informačních systémů veřejné správy (normy ISO 9001, ISO 20000, ISO 27001 a zákon č. 365/2000 Sb., o ISVS).

Vytvoření potřebné dokumentace představuje stanovení a zpracování jednoznačných předpisů pro řízení informační bezpečnosti organizace obsahujících pravidla, povinnosti a zodpovědnosti pro každou definovanou skupinu uživatelů.
V rámci této etapy bude zpracována potřebná bezpečnostní projektová, řídicí a provozní dokumentace, vyhovující jak legislativním požadavkům, tak potřebám systému řízení bezpečnosti informací a interním potřebám organizace. Soulad interních předpisů informační bezpečnosti s legislativou chápeme jako shodu se zákonnými předpisy, které upravují řízení a vykonávání určitých procesů JMK pomocí, prostřednictvím nebo za podpory informačních a komunikačních technologií zpracovávajících data, na základě výsledků z analýzy rizik.
K zajištění požadovaného souladu zrealizujeme v prvním kroku analýzu veškerých platných právních předpisů (zákony, vyhlášky, nařízení a předpisy), norem a standardů (např. normy ČSN ISO/IEC, případně doporučení NIST, ISACA, ITIL apod.).
Úkolem druhého kroku bude revidovat stávající předpisovou základnu JMK (minimálně v rozsahu stávající bezpečnostní politiky a provozního řádu) ze dvou hledisek:

- prvním z nich je analyzovat její rozsah, určení, obsahovou náplň, citlivost, stanovení odpovědností, úroveň podrobností, správnost a přehlednost, včetně formálních náležitostí a aktuálnosti jednotlivých dokumentů,
- druhým hlediskem je procesní stránka životního cyklu dokumentace, tzn. tvorby, změn, aktualizací, ukládání, evidence, správy, zálohování, archivace a likvidace dokumentů.

V rámci tohoto kroku budou realizovány následující činnosti:

- identifikace dokumentace k informační bezpečnosti,
- analýza obsahu, aktuálnosti, dostatečnosti a správnosti dokumentace,
- analýza souladu dokumentace s legislativou, vnějšími a vnitřními požadavky,
- identifikace neshod,
- obecný návrh opatření a doporučení týkajících se aktualizace dokumentů, tvorby či dopracování specifických, příp. povinně předkládaných dokumentů např. v rámci atestací,
- konkrétní doporučení rozsahu a obsahu potřebné dokumentace, případně vzorových šablon dokumentů s vyžadovanými náležitostmi.

Audit dokumentace se bude týkat následujícího výčtu typických interních dokumentů, jakými mohou být např.:

- informační strategie,
- informační koncepce,
- bezpečnostní politika ICT/IS,
- bezpečnostní směrnice a příručky,
- metodické materiály a pokyny (metodika analýzy rizik, katalog hrozeb),
- bezpečnostní plán (seznam schválených/neschválených opatření, stav implementace, akceptace rizik),
- havarijní plány, plány kontinuity a obnovy,
- a další.

Zaměříme se mj. také na procesy související s posuzovanou dokumentací, které se týkají:

- tvorby,
- schvalování,
- změnového řízení a aktualizace,
- publikování a evidence,
- ověřování správnosti, dostatečnosti, srozumitelnosti a přehlednosti,
- vyhodnocování dodržování dokumentovaných předpisů, stanovených kompetencí a zodpovědností.

Rozsah a objem návrhu vytvoření či aktualizace stávající interní dokumentace bude záviset na aktuálním stavu dokumentace, který bude podroben revizi, jejíž výsledky doplní či upřesní celkový souhrn požadavků identifikovaných z analýzy rizik. Minimální rozsah dokumentace musí odpovídat všem těmto požadavkům a zároveň zaručovat dostatečnou míru přehlednosti a jednotnosti, s vyloučením duplicitní dokumentace a za dodržení diferencovaného přístupu k jednotlivým dokumentům dle oprávnění a citlivosti obsahu.
Z pohledu legislativního se jedná o soubor dokumentů týkajících se utajovaných informací, ochrany osobních údajů nebo ISVS, jako jsou např.:

- bezpečnostní politika, informační koncepce, příp. návrh (plán) bezpečnosti a testy bezpečnosti;
- provozní dokumentace typu bezpečnostní směrnice;
- příručky (pro uživatele a pro bezpečnostního správce).

Z pohledu bezpečnostního se jedná o dokumentaci doporučovanou v normě ČSN ISO/IEC TR 13335 n. ISO 27001, např.:

- strategie bezpečnosti resp. celková bezpečnostní politika ICT;
- politika bezpečnosti systému;
- plán zvládání rizik, n. plán bezpečnosti ICT.

Do provozní dokumentace dále budou spadat např. provozní řády organizace v oblasti ICT, plány pro případ havárií a mimořádných událostí, provozní deníky, evidence a přílohy k těmto řádům či směrnicím, a také veškeré záznamy dokládající výkon popsaných procesů a činností.
Z procesně orientovaných dokumentů jsou to např.:

- popisy bezpečnostních mechanizmů,
- popisy nastavení přístupových oprávnění,
- popisy nastavení technických a programových parametrů,
- způsoby nastavení komunikace jak uvnitř organizace, tak i mimo ni,
- způsob práce s mobilní výpočetní technikou a její připojování do počítačové sítě,
- apod.

Z věcně orientovaných dokumentů je to např.:

- dodatek pracovní smlouvy, ve kterém se zaměstnanci zavazují dodržovat zásady bezpečné práce s ICT a informacemi,
- postup a procedury auditu IS/ICT/ISMS,
- apod.

Z dokumentace orientované na role jsou to např.:

- příručky bezpečnostních manažerů a správců, správců aplikací,
- příručka správce systému,
- příručka pro práci uživatele IS/ICT v organizaci,
- apod.

Samostatnou provozní dokumentaci mohou vyžadovat i některé specifické systémy či aplikace, pokud bude její tvorba účelná a potřebná pro zajištění jejich bezpečného provozu.
V rámci tvorby bezpečnostní dokumentace bude dle potřeby realizována či revidována také stávající Informační koncepce, včetně aktualizace souvisejících dokumentů pro potřeby splnění požadavků zákona o ISVS a prováděcích právních předpisů k tomuto zákonu, v případech, kdy se bude jednat o dodávku nových ISVS.
Informační koncepce je dokument, který je nezbytné vytvořit, revidovat, případně aktualizovat s ohledem na vývoj v uplynulém období, a měnící se zákonné, interní a jiné požadavky tak, aby byly zohledněny veškeré stávající, aktuální i budoucí dlouhodobé kvalitativní a bezpečnostní cíle a požadavky.
Účelem zpracování či revize Informační koncepce ISVS organizace je identifikovat změny, posoudit aktuálnost, zhodnotit provádění činností dle této koncepce, ověřit stav realizace cílů a požadavků bezpečnosti a kvality, a vyhodnotit, do jaké míry je zajištěna shoda se stanovenými požadavky a povinnostmi, které z tohoto dokumentu vyplývají.
Námi navrhovaná revize Informační koncepce v požadovaném rozsahu bude zahrnovat následující činnosti:

- identifikaci změn ISVS od data poslední revize IK (n. jejího vytvoření),
- aktualizaci dokumentovaných ISVS, tj.:
  - přehledu ISVS,
  - popisu jednotlivých ISVS,
  - záměrů na pořízení nebo vytvoření ISVS,
- aktualizaci plánu řízení kvality ISVS,
- aktualizaci plánu řízení bezpečnosti ISVS,
- ověření dodržování pravidel pro správu všech ISVS, tj. pro:

- pořizování a vytváření,
- provozování a údržbu,
- změnové řízení a ukončení činnosti,
- ověření pravidel financování ISVS v souladu s obecnými předpisy, podmínkami zadávání veřejných zakázek a zakázek malého rozsahu, pro:
- vytvoření či pořízení ISVS,
- financování dlouhodobých cílů (realizace cílů a požadavků kvality a bezpečnosti),
- financování správy (provozu a údržby),

- ověření pravidel pro realizaci IK.

Výstupy – Dokumentace

Z dokumentů odpovídajících kategorii bezpečnostní dokumentace budou zpracovány (příp. aktualizovány) následující dokumenty:

Projektová bezpečnostní dokumentace

- Bezpečnostní politika TCK zaměřená na specifická opatření pro všechny uvedené oblasti bezpečnosti;
- Informační koncepce.

Provozní bezpečnostní dokumentace

- Bezpečnostní směrnice pro bezpečnostní správce;
- Bezpečnostní směrnice pro správce systémů;
- Bezpečnostní směrnice pro uživatele;
- Specifické bezpečnostní metodiky, manuály a příručky ;
- Havarijní plány (řešení havárií, kontinuity a obnovy) obsahující:
  - definici kritických procesů,
  - identifikaci uvažovaných typů havárií,
  - definici postupu a koordinace činností při řešení havárie a obnově provozu,
  - definici testování postupů a plánů,
  - definici zodpovědností za jednotlivé činnosti.

Ostatní požadavky pro oblasti A-E

Dodávka veškerých potřebných licencí

Zhotovitel, v rámci úspěšné akceptace všech částí plnění, poskytne licence ke všem částem aplikačního programového vybavení, jehož je nebo bude po implementaci tvůrcem, včetně částí kterých je nebo bude po implementaci tvůrcem jeho subZhotovitel, a udělí oprávnění Objednateli k jejich nevýhradnímu užití, a to všemi způsoby uvedenými v ust. § 12 odst. 4 zákona č. 121/2000 Sb., autorského zákona, ve znění pozdějších předpisů, v rozsahu nutném pro naplnění účelu plnění veřejné zakázky a řádné užití předmětu plnění.

Soulad plnění s obecně platnými a účinnými právními předpisy ČR

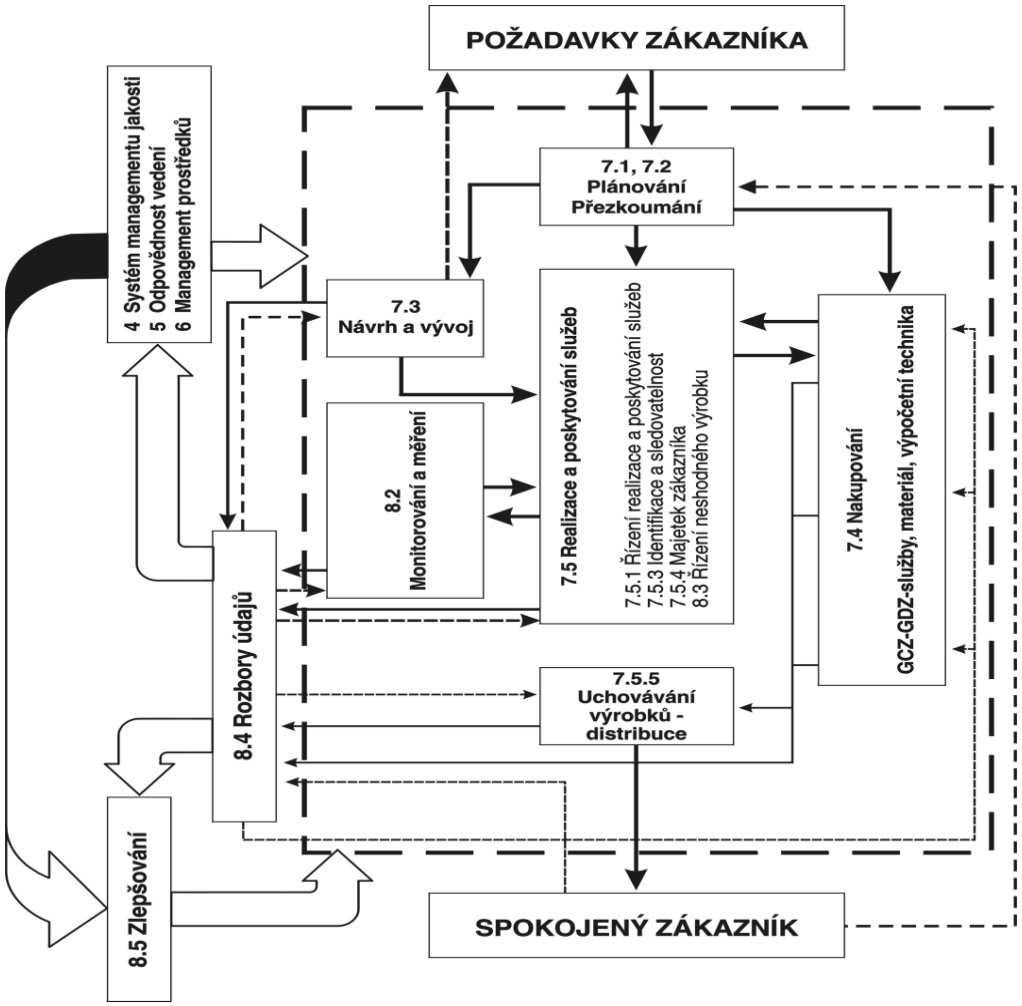
Zhotovitel zajistí, že veškeré vlastnosti plnění, včetně jeho update, legislativní kompatibility a legislativního update, upgrade a legislativního upgrade budou po celou dobu účinnosti smlouvy odpovídat vždy aktuálním obecně platným a účinným právním předpisům ČR při uplatnění nezbytné součinnosti Objednatele na identifikaci, návrhu, schvalování a akceptaci změn ve funkčnosti řešení, které budou procesy změn pro zajištění souladu vyžadovat.

Soulad s obecně platnými a účinnými právními předpisy ČR bude realizován v souladu s managementem jakosti podle norem **ISO 9001:2000**.

Na základě tohoto rámce je zabezpečeno vypracování a schválení procesu změnového řízení v souladu s odpovídající legislativou. Vzhledem k rozsahu této dokumentace ji Zhotovitel neuvádí v nabídce, ale garantuje její existenci. Tato úplná dokumentace je kdykoliv k nahlédnutí Objednateli.

Tento definovaný postup schematicky popsaný níže v souladu s firemními Směrnicemi a procesním řízením zajistí maximální pružnost schvalování nezbytných organizačních a legislativních změn (interní legislativa), které vyplynou z požadavků na implementaci projektu, reingeneeringu procesu apod.

Mapa procesů



Legislativní podpora projektu

- Legislativní dohled nad prováděnou implementací bude realizován v souladu s náležitostmi životního cyklu informačního systému a při ověřování účinnosti jednotlivých procesů bude využito metodik vyplývajících ze standardů zejména Prince II, metodologie LBMS a dalších norem. Účelem dohledu je zejména zabránění realizace legislativně nepřípustných řešení a schvalování přípustnosti navrhovaného řešení.
- Při provádění nezbytných legislativních úkonů (např. v případě schválení oprávněného požadavku vyžadujícího legislativní změnu jde o přípravu patřičných legislativních norem, klientských smluv, oznamovací povinnosti vůči např. Úřadu na ochranu osobních údajů apod.).
- Požadavky na odsouhlasení navrhovaného postupu, resp. požadavky na případnou legislativní změnu řešiteli této úlohy bude předkládat projektový manažer Objednatele nebo jím pověřená osoba.

Jednotlivé požadavky a jejich řešení jsou protokolovány a jsou součástí dokumentace projektu. Zhotovitel informuje o tom, že jeho subZhotovitel vyvíjí software jako legislativně závislý SW se silnou metodickou podporou a garantuje Objednateli soulad s příslušnou legislativou. K tomuto se zavazuje všem svým uživatelům a za součinnosti Objednatele se zavazuje na tomto úseku zejména k tomu, že bude:

- provádět legislativní úpravy *produktů GINIS a ASW*, vytvářet a dodávat Objednateli aktualizované verze *produktů GINIS* a ASW včetně uživatelské dokumentace k nim,
- na základě požadavků a specifikací Objednatele odsouhlasených Zhotovitelem provádět drobné úpravy *Produktů,*

- provádět takové úpravy i významné úpravy Produktu, které po dohodě Smluvních stran povedou ke zlepšení funkcionality Produktu a stanou se součástí další aktualizované verze Produktu
- vytvářet a dodávat Objednateli aktualizované verze *produktů GINIS* a ASW včetně uživatelské, technické dokumentace k nim, vést v aktuálním stavu provozní dokumentaci odrážející reálný stav implementace podporovaných systémů v místě Objednatele,
- na základě legislativních změn, které vyvolávají potřebu změny funkčnosti již dodaných programových produktů, vytvářet a dodávat nové verze těchto produktů, které svým rozsahem jsou:
    - buď "legislativním updatem",
    - nebo "legislativním upgradem",
    - na základě legislativních změn, které vyvolávají potřebu doplnění funkčnosti již dodaných programových produktů, vytvářet a dodávat nové programové produkty

Výsledkem procesu inovace Produktů budou nové verze Produktů a to buď jako update nebo jako upgrade:

- pod pojmem update aplikačního programového produktu se rozumí taková verze aplikačního programového produktu, u které se oproti předcházející verzi tohoto produktu mění jeho funkčnost, a to na základě změny jakékoliv skutečnosti, podle které byla celá funkčnost tohoto aplikačního programového produktu vytvořena, ale nemění se struktura dat datového fondu, s kterým tato verze aplikačního programového produktu pracuje. V případě, že změna funkčnosti tohoto produktu byla provedena pouze na základě legislativních změn, je nová verze tohoto produktu jeho "legislativním updatem",
- pod pojmem upgrade aplikačního programového produktu se rozumí taková verze aplikačního programového produktu, u které se oproti předcházející verzi tohoto produktu mění jeho funkčnost, a to na základě změny jakékoliv skutečnosti, podle které byla celá funkčnost tohoto aplikačního programového produktu vytvořena, a zároveň se mění struktura vět datového fondu, s kterým tato verze aplikačního programového produktu pracuje. V případě, že změna funkčnosti tohoto produktu a změna struktury dat datového fondu, s kterým tento produkt pracuje, byla provedena pouze na základě legislativních změn, je nová verze tohoto produktu jeho "legislativním upgradem".

Požadavky na součinnost Objednatele pro fázi I. – Realizace a zkušební provoz
Součinnost Objednatele, nezbytně nutná pro realizaci jednotlivých dílčích plnění, je uvedena v následujících kapitolách. Požadavky na součinnost ve Zkušebním provozu jsou uvedeny v samostatné kapitole níže.

Detaily požadované součinnosti v oblasti I.A – TC Jihomoravského kraje

Předimplementační fáze

- stanovení komunikační matice (kontaktních osob Objednatele)
- informace o fyzickém umístění jednotlivých komponent, včetně řešení jejich napájení, dostupnost pro management apod.
- informace o adresním plánu pro zařízení, propojovací sítě, klientské sítě a sítě externích subjektů
- informace o konkrétním způsobu propojení interních a externích sítí (médium, rychlost, požadavky na spolehlivost, kontaktní osoby, …)
- požadavky pro konfiguraci služeb na aktivních prvcích (pakliže budou)
- průběžné připomínkování prováděcího projektu
- závěrečná akceptace prováděcího projektu, který se následně stává závazným dokumentem pro implementační fázi

Implementační fáze

- potvrzení funkčnosti jednotlivých komponent a celků
- potvrzení splnění požadavků na časy konvergence a dalších parametrů uvedených v prováděcím projektu
- umožnění přístupu ke všem prvkům řešení v požadovanou dobu
- poskytnutí a zajištění konkrétních termínů a časů pro migraci infrastruktury (doplnění do relativního plánu v prováděcím projektu)
- průběžné vedení připomínek k instalovanému stavu – forma bude stanovena v prováděcím projektu

Poimplementační fáze

- potvrzení funkčnosti při finálních testech
- součinnost při řešení servisních zásahů (typicky umožnění přístupu instalovaným zařízením v požadovaném čase)

Detaily požadované součinnosti v oblasti I.B – Vnitřní integrace Krajského úřadu

Pro implementaci integrační platformy požaduje Zhotovitel nezbytnou součinnost Objednatele při získání popisu rozhraní a přesné technické specifikace napojovaných existujících systémů úřadu včetně popisu případných budoucích úprav těchto napojovaných systémů na integrační vrstvu od třetích stran. Obecně nezbytnou součinnost při napojování v dodání definic uživatelů spravovaných v IDM a jejich rolí v jednotlivých provázaných systémech.

Pro subsystém workflow požaduje Zhotovitel nezbytnou součinnost v oponentuře a při schvalování navržených workflow pro podporu práce v agendách a podpůrných procesech úřadu.

Pro subsystém portálu nezbytnou součinnost s klíčovými zástupci Objednatele z agend úřadu, kteří budou systém po jeho implementaci užívat, při schvalování návrhu grafického rozhraní.

Pro subsystém IS Správních řízení nezbytnou součinnost v rozsahu:

- Distribuce dotazníků a šablon pro administraci správního řízení
- Zpřístupnění dokumentů (nařízení, metodiky, vnitřní předpisy) souvisejících s výkonem správního řízení na krajském úřadu
- Zajištění přístupu pracovníků Zhotovitele na jednotlivá pracoviště úřadu za účelem analýzy, administrace a implementace
- Umožnění a součinnost při kontrole technické připravenosti hardware a software – konektivita, aktualizované operační systémy, prohlížeče a doplňky
- Kooperace při stanovení uživatelů využívajících aplikaci Správní řízení

- Spolupráce v oblasti analýzy a projektování (podklady, schválení výstupů) a dále pak při akceptaci jednotlivých etap řešení
- Spolupráce v oblasti nastavení systému
    - Stanovení pevného neměnného obecného rámce nastavení aplikace pro všechny
    - Stanovení rámce pro výjimky (pravidla pro změny, údržba specifického nastavení)
- Spolupráce specialistů úřadu při tvorbě univerzálně použitelných vzorů správních rozhodnutí
- Spolupráce při organizaci seznámení uživatelů, pokyny k organizaci práce za účelem účasti na seznámení uživatelů, přítomnosti v době analýzy a při akceptaci, reakce na písemné požadavky

Detaily požadované součinnosti v oblasti I.C - Elektronická spisová služba JMK
Tato součinnost s Objednatelem vyplývá z požadavku zajistit pro organizace hostovanou spisovou službu TC JMK:

- Zajištění jednotného komunikačního kanálu
    - Směrem k organizacím informace o novinkách, nastavení, odstávkách systému apod.
    - Směrem od organizací hlášení nesrovnalostí, nefunkčností, námětů…
- Distribuce dotazníků a šablon pro administraci spisové služby
- Zpřístupnění dokumentů (nařízení, metodiky, vnitřní předpisy) souvisejících se spisovou službou
- Zajištění přístupu pracovníků Zhotovitele za účelem analýzy, administrace a implementace
- Kontrola technické připravenosti hardware a software – konektivita, aktualizované operační systémy, prohlížeče a doplňky
- Rozdělení organizací do skupin dle velikosti, významu, priority nasazení, počtu uživatelů
- Spolupráce v oblasti analýzy
- Spolupráce v oblasti nastavení systému
    - Stanovení pevného neměnného obecného rámce nastavení pro všechny
    - Stanovení rámce pro výjimky (pravidla pro změny, údržba specifického nastavení)
- Spolupráce na univerzálně použitelném (elektronickém) spisovém plánu
- Spolupráce na úpravu Spisového a skartačního řádu – doplnění pasáží o elektronické spisové službě a pokynu k upravení
- Spolupráce při organizaci seznámení uživatelů, pokyny k organizaci práce za účelem účasti na seznámení uživatelů, přítomnosti v době analýzy, reakce na písemné požadavky
- V případě používání dočasné aplikace pro spisovou službu spolupráce se stanovením podmínek přechodu na hostovanou aplikaci

Detaily požadované součinnosti v oblasti I.D - Datové sklady, manažerské informační systémy a nástroje Business Intelligence Jihomoravského kraje

V průběhu projektu výstavby této části projektu je vyžadována následující součinnost Objednatele:

- účast managementu Objednatele a organizační podpora;
- stanovení komunikace (komunikační strategie ze strany Objednatele)
- zabezpečení striktního projektového řízení
- stanovení pravomocí a odpovědností (stanovení pozic a definice jejich kompetencí)
- stanovení kompetencí odpovídajících řešitelských týmů;
- zajištění součinnosti dalších Zhotovitelů

- zajištění dostatečných kapacit pracovníků řešitelských týmů
- dodržování harmonogramu projektu
- striktní řízení změn
- zajištění telekomunikačních služeb (hlasové i datové služby v místě plnění),
- zajištění pracovního zázemí pro Zhotovitele (místnost/ místnosti/ pracoviště)
- stanovení oponentů a principů oponentního řízení Implementační studie
- zajištění oponentního řízení a akceptace Implementační studie
- účast pracovníků Objednatele na schůzkách řešitelských týmů
- zajištění kvalifikovaných pracovníků v jednotlivých řešitelských týmech
- umožnění odborných konzultací řešitelských týmů
- aktivní účast při testovacím poloprovozu a testovacím provozu
- aktivní zapojení do ověřovacího provozu
- zabezpečení akceptačního řízení převzetí plnění jednotlivých fází projektu výstavby datového skladu, MIS a nástrojů Business Inteligence
- Jmenovat odpovědné osoby za jednotlivé řešené datové tržiště, poskytnutí rozhodovací pravomoci těchto osob v předmětu řešených datových tržišť k níže uvedeným součinnostem, a zajistit uvolnění jednotlivých členů týmu pro práci na projektu
    - Objednatel umožní v průběhu realizace projektu pro osoby realizačního týmu Zhotovitele zajištění přístupu k infrastruktuře, kde bude vybudováno testovací a provozní prostředí předmětu díla v pracovní dny v době (ideálně od 8.00 – 18.00)
    - Poskytnutí pracovníkům Zhotovitele vzdálený přístup do informačního systému úřadu k technologiím realizovaným Zhotovitelem po dobu nezbytně nutnou k plnění závazků vyplývající z této Smlouvy.
    - poskytnut řádně vyžádané dokumenty Objednatele vztahující se k plnění díla v dohodnutých termínech a dohodnutým způsobem
    - Zajištění přístupu k datům a příslušné dokumentace vytvářených softwarem třetích stran nebo zajištění dat v domluveném formátu (např. Flat File) za účelem zajištění dat z provozních systémů a aplikací a z externích zdrojů, které mají být načteny do datových skladů, v oboustranně dohodnutých termínech, nejpozději však do 15 pracovních dnů po předání žádosti.
    - Poskytnutí součinnosti směřující k zabezpečení požadované konektivity na datové zdroje prostřednictvím ETL procesů, jež jsou předmětem plnění díla a to jak pro provozní prostředí tak pro testovací prostředí
    - Poskytnutí specifikace vstupních a výstupních datových rozhraní mezi KÚ a jednotlivými poskytovateli externích dat.

Detaily požadované součinnosti v oblasti I.E - Krajská digitální spisovna (KDS) a Krajský digitální repositář (KDR)

V průběhu projektu výstavby KDS/KDR je vyžadována následující součinnost Objednatele

- účast managementu Objednatele a organizační podpora pro nasazení KDS/KDR;
- stanovení komunikace (komunikační strategie ze strany Objednatele)
- zabezpečení striktního projektového řízení
- stanovení pravomocí a odpovědností (stanovení pozic a definice jejich kompetencí)

- stanovení kompetencí odpovídajících řešitelských týmů;
- zajištění součinnosti dalších Zhotovitelů
- zajištění dostatečných kapacit pracovníků řešitelských týmů
- dodržování harmonogramu projektu
- striktní řízení změn
- poskytnutí dokumentace např. stavební dokumentace, řídící dokumentace, atp.
- zajištění přístupu Zhotovitele do budov
- zajištění telekomunikačních služeb (hlasové i datové služby v místě plnění),
- zajištění pracovního zázemí pro Zhotovitele (místnost/ místnosti/ pracoviště)
- stanovení oponentů a principů oponentního řízení Implementační studie
- zajištění oponentního řízení a akceptace Implementační studie
- účast pracovníků Objednatele na schůzkách řešitelských týmů
- zajištění kvalifikovaných pracovníků v jednotlivých řešitelských týmech
- umožnění odborných konzultací řešitelských týmů
- aktivní účast při testovacím poloprovozu a testovacím provozu
- aktivní zapojení do ověřovacího provozu
- zabezpečení akceptačního řízení převzetí plnění jednotlivých fází projektu výstavby KDS/KDR

Model spolupráce Zhotovitele se Objednatelem bude založen na vybudování komunikačních kanálů, které mohou být specifické pro jednotlivé řešitelské týmy. Od počátku přistupujeme k tomuto projektu se vší vážností a se snahou vybudovat v těsné spolupráci se Objednatelem špičkové pracoviště KDS/KDR. Jsme si vědomi, že je nutné KDS/KDR nejen vybudovat a zprovoznit, ale také zajistit jeho trvale udržitelný provoz a rozvoj. Z tohoto důvodu bude naší snahou maximálně zúročit know-how Objednatele i Zhotovitele a toto promítnout i do velmi těsné spolupráce během celého projektu.

Detaily požadované součinnosti v oblasti I.G – Projektové řízení pro oblasti A-E
Pro zdárný průběh řízení realizace projektu předpokládáme spoluúčast Objednatele na přizpůsobení projektové metodologie konkrétním podmínkám projektu a procesům Objednatele. Dále očekáváme součinnost v níže popsaných kapitolách.

METODIKY A STANDARDY ŘÍZENÍ NA ÚŘADĚ

Pro uplatnění principu nastavení projektu očekáváme dodání metodik a standardů, pokud jsou aplikovány v prostředí Objednatele, v oblastech:

- procesního řízení
- řízení a sledování kvality
- konfiguračního managementu
- komunikace a výměny informací
- řízení rizik

Uplatnění již použitých a aplikovaných standardů v rámci projektu zvýší efektivitu projektu a zjednoduší chápání fungování projektu.

VLASTNÍ ORGANIZACE A ŘÍZENÍ PROJEKTU

Projektová metodika pracuje s hierarchickou strukturou řízení projektu a v etapě startu projektu očekáváme společné naplnění jednotlivých rolí. Detailní popis rolí bude předmětem startovní etapy, nicméně níže uvádíme obecné předpoklady pro naplnění požadované struktury projektu. Vycházíme z předpokladu zapojení do projektu tří zájmových oblastí, vedení, uživatelů a Zhotovitele. Ze strany Objednatele očekáváme zajištění zejména rolí:

- Ředitel projektu
- Hlavní uživatel
- Projektový dohled

Tyto role musí být naplněny tak, aby byla pokryta schopnost:

- přijímat rozhodnutí v rámci projektu, zejména v oblasti řízení rizik, změnových požadavků, zpracování problémů a výjimek
- zajistit spolupráci na přípravě a plánování jednotlivých etap projektu
- zajistit spolupráci při přípravě a schválení základní projektové dokumentace
- zajistit nezbytnou součinnost pro realizaci jednotlivých úkolů
- přebírat a akceptovat jednotlivé úkoly, etapy a celý projekt
- zajistit nezbytně nutnou součinnost uživatelů/odběratelů jednotlivých produktů, a to zejména v oblasti specifikace a popisu vlastností produktu a pak následné akceptace
- dozorovat a kontrolovat jednotlivé projektové činnosti
- zajistit požadovanou míru komunikace a informovanosti na straně Objednatele na všechny participující subjekty
- poskytovat podporu projektovému managementu
- aktivně se podílet na procesu řízení projektu
- převzít dokončené produkty do standardního procesu podpory a provozu
- účastnit se kontrolních činností (hodnocení reportů a průběhu projektu)
- oponentura návrhů

Pro zdárnou implementaci nástrojů (částmi plnění A-E) pro podporu práce jednotlivých agend úřadu bude nutno zapojit do procesu spolupráce na řízení projektu tyto pracovníky nebo jejich kvalifikované zástupce:

- vedoucí odboru informatiky (technologické procesy)
- vedoucí ekonomického odboru (analytické procesy)
- vedoucí odboru vnitřních věcí (podpůrné procesy úřadu)

Detaily požadované součinnosti v oblasti I.H – Řešení bezpečnosti pro oblasti A-E

ANALÝZA ŘEŠENÍ

Pro analýzu řešení (požadavků vyplývajících z legislativy, norem a standardů, a technického řešení) je požadována součinnost v oblasti poskytování podkladových informací, a dostupnosti stávajících závazných předpisů (interních, nadřízených orgánů apod.).

ANALÝZA RIZIK

Pro zpracování analýzy rizik a následného návrhu opatření ve výše uvedeném rozsahu požadujeme součinnost Objednatele minimálně v rozsahu:

- určení zástupce Objednatele pro sběr podkladů k analýze rizik,
- poskytnutí potřebných vstupních informací formou osobní, telefonické nebo elektronické komunikace (kapacity respondentů v rozsahu min. 5 člověkodní pro každou oblast plnění),
- konzultačně-prezentační schůzky pro etapu návrhu bezpečnostních opatření,
- konzultačně-prezentační schůzky pro oponenturu vytvářené dokumentace,
- konzultačně-prezentační schůzky pro předání a prezentaci výsledků, a pro zajištění schvalovacího procesu výstupů.

PENETRAČNÍ TESTY

Požadovaná součinnost v rámci realizace penetračních testů spočívá v:

- odpovědném vyslovení souhlasu s testováním – projektový zápis, samostatný dokument,

- volbě parametrů testování – tvrdosti, viditelnosti, rozsahu, příbuzných systémů – formou projektového zápisu, nebo samostatný dokument.

BEZPEČNOSTNÍ SEZNÁMENÍ

Ze strany Objednatele je pro bezpečnostní seznámení požadována součinnost v oblasti konzultací k náplni, rozsahu a obsahu seznámení pro jednotlivé skupiny účastníků.

VYTVOŘENÍ INTERNÍCH PŘEDPISŮ

Pro úspěšnou realizaci fáze tvorby dokumentace a metodických materiálů a je klíčová úzká spolupráce a součinnost se Objednatelem zejména ve fázi zjišťování, poskytování informací a podkladů pro analýzu požadavků a potřeb. Předpokládáme zajištění nezbytné součinnosti pověřených respondentů ze strany Objednatele v rozsahu:

- minimálně 2 dny na každý zpracovávaný/aktualizovaný výstupní dokument ve fázi sběru podkladových informací,
- minimálně 2 dny na projednání připomínek a související konzultace k vytvořenému/aktualizovanému návrhu každého z dokumentů.

Rozsah seznámení pracovníků Objednatele s dodaným plněním pro oblasti A-E
Zhotovitel provede nezbytné seznámení pracovníků Objednatele s dodaným plněním v následujícím rozsahu pro oblasti předmětu plnění A-E (uvedené bude osvědčeno podpisem akceptačního protokolu v rámci akceptační procedury).
Zhotovitel dále navrhuje nezbytné seznámení pracovníků Objednatele s dodaným plněním v uvedeném rozsahu **i pro oblasti F a H**, neboť se domnívá, že jsou důležitou a nedílnou součástí plnění pro zajištění udržitelnosti projektu v oblastech Bezpečnost a Servis.
Navržené počty osob pro seznámení za části plnění F a H lze upravit (navýšit či snížit) podle potřeb zadá.

Seznámení s částí plnění A - TC Jihomoravského kraje

Uživatelská role	**Obsah**	**Počet osob**	**Rozsah**
Správci a administrátoři TCK	Podrobné seznámení správců s architekturou TCK a poskytnutí informací nutných pro rutinní provoz a údržbu TCK	4	10 dnů

Seznámení s částí plnění B – Vnitřní integrace Krajského úřadu

Uživatelská role	**Obsah**	**Počet osob**	**Rozsah**
Správci a administrátoři IDM	Podrobné seznámení správců s architekturou IdM a poskytnutí informací nutných pro rutinní provoz a údržbu systému IdM	5	3 dny
Ostatní zaměstnanci	Seznámení se samoobslužnými vlastnostmi řešení IDM z pohledu uživatele	Dle potřeby (max. 30)	Není nutná prezenční forma, možno zvolit jinou vhodnou (např. videokurz, e-learning apod.)
Správci a administrátoři	Podrobné seznámení správců s architekturou	5	3 dny

Uživatelská role	Obsah	Počet osob	Rozsah
	Logovacího a auditního systému a poskytnutí informací nutných pro rutinní provoz a údržbu systému Logovacího a auditního. Minimálně podrobné seznámení s jednotlivými funkčními bloky a jejich stavebními prvky a seznámení se základními administrátorskými postupy za účelem dohledu a lokalizace případných provozních problémů.		
Administrátoři technologie portálu	Podrobné seznámení administrátorů s technologií portálu a poskytnutí informací nutných pro rutinní provoz a údržbu portálu (serverové i klientské části) Seznámení musí obsahovat minimálně tyto části: • podrobné seznámení s jednotlivými funkčními bloky a jejich stavebními prvky; • seznámení se základními administrátorskými postupy za účelem dohledu a lokalizace případných provozních problémů. V rámci seznámení obdrží administrátor provozní dokumentaci portálu	3	5 dní
Správci obsahu portálu a klíčoví uživatelé.	Podrobné seznámení správců obsahu a uživatelů se způsobem a postupy zadávání, aktualizace a publikace informací různého typu (soubory, seznamy, diskusní příspěvky apod.) na portálu a s jejich užíváním.	3	3 dny

Uživatelská role	Obsah	Počet osob	Rozsah
	V rámci seznámení obdrží administrátor provozní dokumentaci portálu		

Žadatel nad rámec požadavků nabízí seznámení dvěma administrátorům Objednatele pro základní sledování chodu a ovládání celé integrační vrstvy v délce 1 den.

Seznámení s částí plnění C - Elektronická spisová služba JMK

Uživatelská role	Obsah	Počet osob	Rozsah
Správci a administrátoři IS	Podrobné seznámení správců s IS a poskytnutí informací nutných pro rutinní provoz a údržbu systému.	3	2 dny
Uživatelé IS	Seznámení s webovým klientem a spisovým a skartačním řádem	Dle potřeby (max. 500)	Není nutná prezenční forma, možno zvolit jinou vhodnou (např. videokurz, e-learning apod.)

Seznámení s částí plnění D - Datové sklady, manažerské informační systémy a nástroje Business Intelligence Jihomoravského kraje

Uživatelská role	Obsah	Počet osob	Rozsah
Správci a administrátoři datového skladu	Analytici a vybraní zaměstnanci odboru informatiky. Řeší požadavky všech ostatních uživatelů, administrují všechny softwarové nástroje i vrstvy datového skladu. Poskytují služby ostatním uživatelům systému a jsou odpovědní za chod řešení jako celku včetně jeho rozvoje.	5	8 dnů
Pokročilí uživatelé - analytici	Klíčoví uživatelé, kteří se budou podílet na rozvoji obsahu i funkčností řešení.	5	4 dny
Základní uživatelé	Zaměstnanci, kteří aktivně, ale nepravidelně, zpracovávají data ve formě tabulek či grafů, většinou se jedná o statické reporty včetně možností jejich parametrizace. Seznámení Objednatele musí být	40	2 dny

Uživatelská role	Obsah	Počet osob	Rozsah
	zaměřeno na detailní pochopení možností řešení BI a schopnost je aktivně využívat.		
Ostatní zaměstnanci	Půjde o pasivní příjemce informací řešení, u nichž se předpokládá zejména potenciál definice informačního požadavku a znalost možností řešení k jejich uspokojení.	max. 200	Není nutná prezenční forma, možno zvolit jinou vhodnou (např. e-learning).

Seznámení s částí plnění E - Krajská digitální spisovna (KDS) a Krajský digitální repositář (KDR)

Uživatelská role	Obsah	Počet osob	Rozsah
Správci a administrátoři KDS, KDR	Podrobné seznámení správců s IS a poskytnutí informací nutných pro rutinní provoz a údržbu systému.	3	2 dny
Uživatelé KDS, KDR	Seznámení s IS	Dle potřeby (max. 500)	Není nutná prezenční forma, možno zvolit jinou vhodnou (např. videokurz, e-learning apod.)

Seznámení s částí plnění F – Oblast servisních služeb

V této kapitole navrhuje Zhotovitel, **nad rámec požadavků** na seznámení pracovníků s částmi základního plnění A – E, **i seznámení v oblasti F – Záruka**, **úroveň poskytovaných služeb (SLA), požadavky na podporu**

Seznámení vyjmenovaných kontaktních osob Objednatele (tj. osob oprávněných zadávat u Zhotovitele servisní požadavky) v oblasti eskalace servisních služeb, procesů podpory, incident managementu, využívání komunikačních kanálů (webového rozhraní, elektronické komunikace, telefonického / faxového zadávání požadavků) na Centrální komunikační bod zhotovitele (tzv. „Single Point of Contact – SPoC“ v rozsahu 8 člověkohodin jednorázově. Zhotovitel předpokládá seznámení v místě Objednatele, pokud se obě strany nedohodnou jinak.

Seznámení s částí plnění H - Oblast bezpečnosti

Zhotovitel navrhuje, nad rámec požadavků na seznámení pracovníků s částmi plnění A–E**, i seznámení v oblasti H – Bezpečnost**. Zhotovitel se domnívá, že je bezpečnost nedílnou součástí celého řešení. Proto navrhuje provést seznámení pro níže uvedené zástupce cílových skupin tak, aby mohli následně provádět samostatná interní seznámení zaměstnanců či doplnit stávající obsah osnov seznámení pro zaměstnance Krajského úřadu Jihomoravského kraje a jím zřizovaných organizací v oblasti informační bezpečnosti, zejména s ohledem na výstupy a doporučení bezpečnostního projektu, který bude nedílnou součástí dokumentace implementace technického řešení v rámci této zakázky.

Cílem seznámení je zajistit informovanost a povědomí všech důležitých zástupců skupin zaměstnanců (uživatelů ICT) o nezbytných opatřeních pro zajištění informační bezpečnosti na úřadě. Návrh seznámení

těchto cílových skupin bude pokrývat potřeby bezpečnostního vzdělávání jak nových, tak stávajících zaměstnanců v rámci vstupního seznámení a následného pravidelného vzdělávání.

Pro potřeby JMK bude dále vypracována osnova a náplň seznámení na základě individuálních potřeb cílových skupin v celkovém rozsahu 4 dny:

- seznámení pro bezpečnostní management,
- seznámení pro vedoucí zaměstnance,
- seznámení pro správce systémů,
- seznámení pro uživatele.

Předmětem naplnění našeho návrhu tedy bude (bezpečnostního seznámení) jednak vytvoření osnovy a samostatné náplně školicího kurzu pro každou ze čtyř uvedených cílových skupin účastníků, a k realizace vždy jednoho ukázkového kurzu pro každou z těchto čtyř cílových skupin, určeného jako vzor pro zaučení budoucích školitelů z interních zdrojů Objednatele. Detaily námi navrhovaného seznámení jsou uvedeny v tabulce níže.

Uživatelská role	**Obsah**	**Počet osob**	**Rozsah**
vedení, pracovníci v manažerských pozicích	představení systému řízení bezpečnosti informací (ISMS); hierarchie bezpečnostních rolí; stanovení odpovědností, práv a povinností při zajištění ochrany informací; důvěrnost, dostupnost a integrita informací; hrozby a zranitelnosti; vypořádání rizik a jejich akceptace; bezpečnostní opatření; ověřování a vyhodnocování úrovně bezpečnosti; interní předpisová základna - bezpečnostní politika a související dokumentace (směrnice, metodiky, příručky).	5	1 den
bezpečnostní management (např. bezpečnostní manažer, bezpečnostní správce)	představení ISMS; metody a způsoby zavádění systému informační bezpečnosti; bezpečnostní role a funkce, jejich náplň činností; interní předpisová základna – bezpečnostní dokumentace pro bezpečnostní správce; způsoby a možnosti realizace analýzy rizik, související	5	1 den

Uživatelská role	Obsah	Počet osob	Rozsah
	metodiky, normy a standardy; kompetence, pravomoci a povinnosti bezpečnostního managementu; způsoby sledování, kontroly a ověřování systému řízení bezpečnosti.		
správci systémů (administrátoři)	představení ISMS; interní předpisová základna – provozní bezpečnostní dokumentace (pro správce); povinnosti, odpovědnosti a náplň činností správců v oblasti zajišťování bezpečnosti informací.	5	1 den
uživatelé (řadoví zaměstnanci)	představení ISMS; seznámení s interní předpisovou základnou – bezpečnostní dokumentace pro uživatele; nejdůležitější pravidla a zásady bezpečnosti při práci s informacemi; práva, povinnosti a odpovědnost uživatelů při používání ICT a práci s informacemi.	10	1 den

Příloha č. 2 – Členění ceny Plnění

Realizační fáze a zkušební provoz (Tabulka č. 1)

Dílčí plnění		Nabídková cena		
		Cena v Kč bez DPH	**Sazba DPH v %**	**Cena celkem v Kč s DPH**
A)	**Celková cena za plnění oblasti Technologické centrum Jihomoravského kraje**	43 403 620 Kč	20%	52 084 344 Kč
B)	**Celková cena za plnění oblasti Integrace vnitřního systému**	18 384 133 Kč	20%	22 060 960 Kč
C)	**Celková cena za plnění oblasti Elektronická spisová služba**	2 008 850 Kč	20%	2 410 620 Kč
D)	**Celková cena za plnění oblasti Datové sklady, manažerské informační systémy a nástroje Business Intelligence**	9 846 714 Kč	20%	11 816 057 Kč
E)	**Celková cena za plnění oblasti Krajská digitální spisovna, Krajský digitální repozitář**	7 999 998 Kč	20%	9 599 998 Kč
Cena za plnění veřejné zakázky dle odst. 2.4.1. bodu I. zadávací dokumentace (*Σ řádků A) – E) této tabulky*)		81 643 315 Kč	20%	97 971 978 Kč

Servisní služby v rutinním provozu (Tabulka č. 2)

Servisní služby/5 let	Cena v Kč bez DPH	Výše DPH v %	Výše DPH v Kč	Cena v Kč s DPH
Plnění dle odst. 2.4.1. bodu II. zadávací dokumentace	30 819 720 Kč	20%	6 163 944 Kč	36 983 664 Kč

Celková nabídková cena (Tabulka č. 3)

	Cena v Kč bez DPH	Výše DPH v %	Výše DPH v Kč	Cena v Kč s DPH
Celková nabídková cena za plnění veřejné zakázky (součet sum dle tabulky č. 1 a č. 2)	112 463 035 Kč	20%	22 492 607 Kč	134 955 642 Kč

Cena za poskytování servisních služeb za období 1 pololetí

Servisní služby/1 pololetí	Cena v Kč bez DPH	Výše DPH v %	Výše DPH v Kč	Cena v Kč s DPH
Cena za poskytování servisních služeb za období 1 pololetí	3 081 972 Kč	20%	616 394 Kč	3 698 366 Kč

Cena servisních služeb na 5 let – podrobná kalkulace

Servisní služby na 5 let (+ carepack a záruky 4. a 5. rok) OD okamžiku řádného ukončení zkušebního provozu - Akceptace					
počet let podpory	Položka	Cena v Kč bez DPH	Cena Celkem v Kč bez DPH	Cena DPH (DPH 20 %)	Cena celkem v Kč s DPH
5	**Oblast (A) Technologické centrum Jihomoravského kraje**	**2 781 374 Kč**	**13 906 870 Kč**	**2 781 374 Kč**	**16 688 244 Kč**
5	*Síťová a komunikační infrastruktura*	*964 580 Kč*	*4 822 900 Kč*	*964 580 Kč*	*5 787 480 Kč*
5	*Serverová infrastruktura*	*951 620 Kč*	*4 758 100 Kč*	*951 620 Kč*	*5 709 720 Kč*
5	*Zálohování a disková virtualizace*	*865 174 Kč*	*4 325 870 Kč*	*865 174 Kč*	*5 191 044 Kč*
5	**Oblast (B) Integrace vnitřního systému**	**768 000 Kč**	**3 840 000 Kč**	**768 000 Kč**	**4 608 000 Kč**
5	**Oblast (C) Elektronická spisová služba**	**200 000 Kč**	**1 000 000 Kč**	**200 000 Kč**	**1 200 000 Kč**
5	**Oblast (D) Datové sklady, manažerské informační systémy a nástroje Business Intelligence**	**890 000 Kč**	**4 450 000 Kč**	**890 000 Kč**	**5 340 000 Kč**
5	**Oblast (E) Krajská digitální spisovna, Krajský digitální repozitář**	**600 000 Kč**	**3 000 000 Kč**	**600 000 Kč**	**3 600 000 Kč**
5	**Společné náklady pro všechny oblasti (A-E) za poskytování servisní podpory**	**924 570 Kč**	**4 622 850 Kč**	**924 570 Kč**	**5 547 420 Kč**
5	*24x7 Service Desk, 24x7 Centrální dispečink, 24x7 Monitoring SW a HW*	*498 570 Kč*	*2 492 850 Kč*	*498 570 Kč*	*2 991 420 Kč*
5	*Expertní podpora*	*426 000 Kč*	*2 130 000 Kč*	*426 000 Kč*	*2 556 000 Kč*
			30 819 720 Kč	**6 163 944 Kč**	**36 983 664 Kč**

Část A. – Technologické centrum Jihomoravského kraje

Specifikace HW a SW Technologické centrum Jihomoravského kraje					
Cena za plnění oblasti Technologické centrum Jihomoravského kraje		Nabídková cena			
Infrastruktura Datového centra					
počet	Položka	Kusová cena v Kč bez DPH	Cena Celkem v Kč bez DPH	Cena DPH (DPH 20 %)	Cena celkem v Kč s DPH
2	**UPS PW Eaton Blade UPS 12kW N+1** plus příslušenství ,SNMP karta, SW PowerVision Network, EMP sonda	376 772 Kč	753 545 Kč	150 709 Kč	904 254 Kč
2	**HDC - CRV20 In the row chladící jednotka**, výkon dle přiložené selekce, regulace chladícího výkonu 30 - 100 %, EC ventilátory, elektrodový parní zvlhčovač, iCOM large display, čerpadlo kondenzátu	527 247 Kč	1 054 494 Kč	210 899 Kč	1 265 393 Kč
1	**ZDC -Sálová jednotka 23,3kW Sálová chladící**, výkon dle přiložené selekce, regulace chladícího výkonu 30 - 100 %, EC ventilátory, elektrodový parní zvlhčovač, iCOM large display, čidlo dodávané teploty, Itellislot pro dvě karty	235 430 Kč	235 430 Kč	47 086 Kč	282 516 Kč
1	**ZDC - Sálová jednotka 23,3kW - Sálová chladící**, výkon dle přiložené selekce, regulace chladícího výkonu 30 - 100 %, EC ventilátory, elektrodový parní zvlhčovač, čidlo dodávané teploty, Itellislot pro dvě karty	217 391 Kč	217 391 Kč	43 478 Kč	260 869 Kč
2	**Vzduchem chlazený kondensátor,LAN karta**	79 402 Kč	158 805 Kč	31 761 Kč	190 566 Kč
4	**HP 642 1075mm Shock Intelligent Rack - HP 642 Intelligent Series Rack (Shock Pallet) –** 42U racková skříň včetně předních a zadních dveří; výška 200 cm; hloubka 108 cm; statická nosnost 1360 kg (dodaný na palatě s vysokou nosností) ,2x HP 42U 1075mm Side Panel Kit, 2x HP 32A HV Core Only Corded PDU , 2x HP 2, 7X C-13 Stk Intl Modular PDU	32 533 Kč	130 132 Kč	26 026 Kč	156 158 Kč
6	**HP 642 1075mm Shock Intelligent Rack - HP 642 Intelligent Series Rack (Shock Pallet)** – 42U racková skříň včetně předních a zadních dveří; výška 200 cm; hloubka 108 cm; statická nosnost 1360 kg (dodaný na palatě s vysokou nosností),HP 42U 1075mm Side Panel Kit, 2x HP 32A High Voltage Modular PDU	35 781 Kč	214 687 Kč	42 937 Kč	257 624 Kč
			2 764 483 Kč	**552 897 Kč**	**3 317 380 Kč**

Serverová infrastruktura					
počet	Položka	Cena v Kč bez DPH	Cena Celkem v Kč bez DPH	Cena DPH (DPH 20 %)	Cena celkem v Kč s DPH
2	**HP BladeSystem c7000 Enclosure -**HP BLc7000 CTO 3 IN LCD ROHS Encl, Virtual Connect 2x - HP BLc VC Flex-10 Enet Module Opt, HP BLc VC-FC 8Gb 24-Port Opt Kit, Napájecí zdroje 6X HP BLc7000 1 PH FIO Power Module Opt,2400W Gold Ht Plg FIO Pwr Sply Kit, Napájecí modul HP BLc7000 1 PH FIO Power Module Opt ,Větráky HP BLc 6X Active Cool 200 FIO Fan Opt, **Blade police 2x HP BLc 10Gb SR SFP+ Opt.**	876 741 Kč	1 753 483 Kč	350 697 Kč	2 104 179 Kč
8	**HP ProLiant BL685c Server Blade min:** 2x 2 CPU HP BL685c G7 6276 2.30GHz 16c 2P FIO Kit, 1 x řadič HP Smart Array BL465c/685c G7 Cntrlr, 16 x HP 8GB 2Rx4 PC3-10600R-9 Kit ,2xHP 72GB 6G SAS 15K 2.5in DP ENT HDD, 1x HP BLc QLogic QMH2562 8Gb FC HBA Opt	109 449 Kč	875 595 Kč	175 119 Kč	1 050 714 Kč
2	**HP ProLiant BL465c Server Blade,min :** 1x CPU HP BL465c G7 6276 2.3Ghz 16c FIO Kit, řadič HP Smart Array BL465c/685c G7 Cntrlr, 2x HP 8GB 2Rx4 PC3-10600R-9 Kit, 2x HP 146GB 6G SAS 15K 2.5in DP ENT HDD , HP BLc QLogic QMH2562 8Gb FC HBA Opt	42 851 Kč	85 702 Kč	17 140 Kč	102 843 Kč
10	**HP MS WS08 R2 DataCnt2CPU ROK Eng SW**	73 083 Kč	730 826 Kč	146 165 Kč	876 992 Kč
			3 445 606 Kč	689 121 Kč	4 134 727 Kč

Serverová virtualizace

počet	Položka	Cena v Kč bez DPH	Cena Celkem v Kč bez DPH	Cena DPH (DPH 20 %)	Cena celkem v Kč s DPH
32	**VPP L4 VMware vSphere 5 Enterprise Plus for 1 processor** (with 96 GB vRAM entitlement per processor) SNS is Required. Each VS5 enterprise Plus edition license contributes 1 CPU and 96 GB of vRAM entitlement towards total available vRAM pool	57 885 Kč	1 852 319 Kč	370 464 Kč	2 222 783 Kč
1	**VPP L4 VMware vCenter Server Heartbeat 6 for 1 vCenter Server VMware vCenter Server Heartbeat for 1 vCenter Server ;**1 license is required for each vCenter Server that is protected. SnS Required	148 991 Kč	148 991 Kč	29 798 Kč	178 790 Kč
1	**Upgrade: VMware vCenter Server 5 Foundation to vCenter Server 5 Standard vCenter** Server Standard SNS is Required. Original FAC or Serial Number w/active SnS required.	82 678 Kč	82 678 Kč	16 536 Kč	99 214 Kč
			2 083 989 Kč	416 798 Kč	2 500 787 Kč

Datová úložiště

počet	Položka	Cena v Kč bez DPH	Cena Celkem v Kč bez DPH	Cena DPH (DPH 20 %)	Cena celkem v Kč s DPH
2	**Tier 0 - HP ProLiant DL385 G7 ,**HP DL385G7 6212 FIO Kit, 4x 8GB 1Rx4 PC3-12800R-11 Kit, 2x 300GB 6G SAS 15K 3.5in Dp ENT HDD, 82Q 8Gb Dual Port PCI-e FC HBA, 640GB MLC PCIe IO , IC ML/DL/BL 1-Svr FIO 24x7 SW	224 054 Kč	448 109 Kč	89 622 Kč	537 731 Kč
2	**Tier 1 ,Tier 2 - HP Enterprise Virtual Array P6500 , 3**6x M6612 600GB 6G SAS 15K 3.5in HDD, 20 x M6612 2TB 6G SAS 7.2K 3.5in MDL HDD , P6500 EVA Dual Controller FC Array ,P6500 Command View SW E-LTU	1 198 841 Kč	2 397 682 Kč	479 536 Kč	2 877 219 Kč
2	**Tier 3 - Hitachi HCP 300 ,** HCAP 300 - 8.5TB, 4- node storage module, CR220 - 1 ks, HCAP 300 1TB License - 9 ks , HCA v2.0 Software Media Kit , HCA Object Replication License	697 340 Kč	1 394 679 Kč	278 936 Kč	1 673 615 Kč
			4 240 471 Kč	848 094 Kč	5 088 565 Kč

Disková virtualizace

počet	Položka	Cena v Kč bez DPH	Cena Celkem v Kč bez DPH	Cena DPH (DPH 20 %)	Cena celkem v Kč s DPH
2	**FalconStor Software - Licence NSS GA710 , 2x** NSS GA Storage Capacity - 102 x 1TB ,3xClient Package for Backup Server	1 335 471 Kč	2 670 942 Kč	534 188 Kč	3 205 131 Kč
1	**Software pro EFS - License -**Software EFS pro 2 nody á 640GB	176 277 Kč	176 277 Kč	35 255 Kč	211 532 Kč
			2 847 219 Kč	569 444 Kč	3 416 663 Kč

Zálohování a obnova dat

počet	Položka	Cena v Kč bez DPH	Cena Celkem v Kč bez DPH	Cena DPH (DPH 20 %)	Cena celkem v Kč s DPH
1	**MSL4048 Tape Library** - MSL4048 2 LTO-5 3000 FC Tape Lbry , 2x LTO5 Ultrium Non Custom Label 20 Pk	300 011 Kč	300 011 Kč	60 002 Kč	360 014 Kč
2	**HP Data Protector Softwar**e -Drive Extension Data Prt drive ext UNIX/NAS/SAN E-LTU	267 415 Kč	534 829 Kč	106 966 Kč	641 795 Kč
1	**Starter Pack | pouze licence / Data Prot Stater Pack Windows E-LTU**	27 051 Kč	27 051 Kč	5 410 Kč	32 461 Kč
13	**HP DP On-line Backup for Windows**	29 018 Kč	377 230 Kč	75 446 Kč	452 676 Kč
5	**HP DP Advanced Backup to Disk 1TB E-LTU**	26 396 Kč	131 980 Kč	26 396 Kč	158 376 Kč
1	**HP Data Protector 6.20 English SW Media**	3 169 Kč	3 169 Kč	634 Kč	3 802 Kč
			1 374 270 Kč	274 854 Kč	1 649 124 Kč

Bezpečná komunikační infrastruktura TCK					
počet	Položka	Cena v Kč bez DPH	Cena Celkem v Kč bez DPH	Cena DPH (DPH 20 %)	Cena celkem v Kč s DPH
2	**HP 7506 Switch Chassis**	34 127 Kč	68 255 Kč	13 651 Kč	81 906 Kč
4	**HP 7500 384Gbps Fab Mod w/2 XFP Ports**	72 929 Kč	291 717 Kč	58 343 Kč	350 061 Kč
2	**HP 7500 24-port GbE SFP Module**	32 397 Kč	64 795 Kč	12 959 Kč	77 754 Kč
2	**HP 7500 48-port Gig-T Module**	39 359 Kč	78 719 Kč	15 744 Kč	94 462 Kč
2	**HP 7500 8-port 10G SFP+ Module**	79 819 Kč	159 638 Kč	31 928 Kč	191 565 Kč
2	**HP 3100-48 v2 Switch**	12 102 Kč	24 205 Kč	4 841 Kč	29 046 Kč
2	**HP 6602 Router Chassis**	73 610 Kč	147 221 Kč	29 444 Kč	176 665 Kč
2	**HP 6600 1p 10GbE XFP HIM Rtr Module**	32 748 Kč	65 496 Kč	13 099 Kč	78 596 Kč
20	**HP 5120-48G-PoE+ EI Switch w/2 Intf Slts**	33 203 Kč	664 060 Kč	132 812 Kč	796 872 Kč
3	**HP 5800-48G Switch with 2 Slots**	74 154 Kč	222 463 Kč	44 493 Kč	266 955 Kč
3	**HP 5800 16-port SFP Module**	8 776 Kč	26 328 Kč	5 266 Kč	31 593 Kč
3	**HP 5800 4-port 10GbE SFP+ Module**	15 833 Kč	47 498 Kč	9 500 Kč	56 998 Kč
1	**Příslušenství -AC Power Supply, Cable, SFP Transceiver ,1G SFP LC LX Transceiver, 1G SFP LC SX Transceiver , 10G SFP+ LC SR Transceiver¨, 10G SFP+ LC LR Transceiver ..**	1 073 257 Kč	1 073 257 Kč	214 651 Kč	1 287 909 Kč
4	**HP 8/40 SAN Switch -** HP 8/40 Base 24-ports Enabled SAN Switch ,16x HP 8Gb Shortwave B-series FC SFP+ 1 Pack , 2x HP 8Gb LW B-series 10km FC SFP+ 1 Pack, 2x HP B-ser 32-64 ISL Trnk SW LTU	350 882 Kč	1 403 529 Kč	280 706 Kč	1 684 235 Kč
2	**Load-Balancing F5** BIG-IP 3900 Local Traffic Manager (8 GB Memory)	618 544 Kč	1 237 089 Kč	247 418 Kč	1 484 506 Kč
2	**Load-Balancing F5** BIG-IP SSL Licence Upgrade for 3900 LTM (Max TPS)	121 248 Kč	242 496 Kč	48 499 Kč	290 995 Kč
1	**Firewall - Kernun FW ++ cluster**	1 233 759 Kč	1 233 759 Kč	246 752 Kč	1 480 511 Kč
2	**IPS TippingPoint -** HP S1200N IPS Module ,HP vSMS for VMware vSphere 1-host SW Lic	544 704 Kč	1 089 408 Kč	217 882 Kč	1 307 290 Kč
			8 139 932 Kč	1 627 986 Kč	9 767 919 Kč

Management a monitoring					
počet	Položka	Cena v Kč bez DPH	Cena Celkem v Kč bez DPH	Cena DPH (DPH 20 %)	Cena celkem v Kč s DPH
5	**HP NNM i 250+/50 SW E-LTU**	17 551 Kč	87 757 Kč	17 551 Kč	105 308 Kč
5	**HP NNM i 250+/50 NP SW E-LTU**	5 265 Kč	26 325 Kč	5 265 Kč	31 590 Kč
1	**HP NNM iSPI for Perf 50+/50 SW E-LTU**	53 139 Kč	53 139 Kč	10 628 Kč	63 767 Kč
1	**HP NA 50 Node Pack SW E-LTU**	105 397 Kč	105 397 Kč	21 079 Kč	126 477 Kč
1	**HP NA 50+/ Node Pack DV NP SW E-LTU**	6 923 Kč	6 923 Kč	1 385 Kč	8 307 Kč
1	**HP NNM iSPI for Perf 50+/50 NP SW E-LTU**	15 942 Kč	15 942 Kč	3 188 Kč	19 131 Kč
			295 483 Kč	59 097 Kč	354 580 Kč

Maintenance , Carepacky - 3 roky (Záruka 5 let) OD okamžiku řádného ukončení zkušebního provozu - Akceptace					
počet	Položka	Cena v Kč bez DPH	Cena Celkem v Kč bez DPH	Cena DPH (DPH 20 %)	Cena celkem v Kč s DPH
1	**Infrastruktura Datového centra**	237 514 Kč	237 514 Kč	47 503 Kč	285 017 Kč
1	**Serverová infrastruktura**	248 485 Kč	248 485 Kč	49 697 Kč	298 182 Kč
1	**Serverová virtualizace**	2 341 250 Kč	2 341 250 Kč	468 250 Kč	2 809 500 Kč
1	**Datová úložiště**	1 294 460 Kč	1 294 460 Kč	258 892 Kč	1 553 352 Kč
1	**Disková virtualizace**	2 462 154 Kč	2 462 154 Kč	492 431 Kč	2 954 585 Kč
1	**Zálohování a obnova dat**	741 827 Kč	741 827 Kč	148 365 Kč	890 192 Kč
1	**Bezpečná komunikační infrastruktura TCK**	5 900 077 Kč	5 900 077 Kč	1 180 015 Kč	7 080 093 Kč
1	**Management a monitoring**	363 312 Kč	363 312 Kč	72 662 Kč	435 975 Kč
			13 589 080 Kč	2 717 816 Kč	16 306 895 Kč

Implementační a servisní služby DO okamžiku řádného ukončení zkušebního provozu - Akceptace					
počet	Položka	Cena v Kč bez DPH	Cena Celkem v Kč bez DPH	Cena DPH (DPH 20 %)	Cena celkem v Kč s DPH
1	**Infrastruktura Datového centra**	714 285 Kč	714 285 Kč	142 857 Kč	857 142 Kč
1	**Serverová infrastruktura**	143 000 Kč	143 000 Kč	28 600 Kč	171 600 Kč
1	**Serverová virtualizace**	374 000 Kč	374 000 Kč	74 800 Kč	448 800 Kč
1	**Datová úložiště**	310 000 Kč	310 000 Kč	62 000 Kč	372 000 Kč
1	**Disková virtualizace**	591 902 Kč	591 902 Kč	118 380 Kč	710 282 Kč
1	**Zálohování a obnova dat**	143 000 Kč	143 000 Kč	28 600 Kč	171 600 Kč
1	**Bezpečná komunikační infrastruktura TCK**	938 900 Kč	938 900 Kč	187 780 Kč	1 126 680 Kč
1	**Management a monitoring**	638 000 Kč	638 000 Kč	127 600 Kč	765 600 Kč
1	**Projektové vedení**	770 000 Kč	770 000 Kč	154 000 Kč	924 000 Kč
			4 623 087 Kč	924 617 Kč	5 547 704 Kč

CELKEM TC					
počet	Položka	Cena v Kč bez DPH	Cena Celkem v Kč bez DPH	Cena DPH (DPH 20 %)	Cena celkem v Kč s DPH
1	**Infrastruktura Datového centra**	2 764 483 Kč	2 764 483 Kč	552 897 Kč	3 317 380 Kč
1	**Serverová infrastruktura**	3 445 606 Kč	3 445 606 Kč	689 121 Kč	4 134 727 Kč
1	**Serverová virtualizace**	2 083 989 Kč	2 083 989 Kč	416 798 Kč	2 500 787 Kč
1	**Datová úložiště**	4 240 471 Kč	4 240 471 Kč	848 094 Kč	5 088 565 Kč
1	**Disková virtualizace**	2 847 219 Kč	2 847 219 Kč	569 444 Kč	3 416 663 Kč
1	**Zálohování a obnova dat**	1 374 270 Kč	1 374 270 Kč	274 854 Kč	1 649 124 Kč
1	**Bezpečná komunikační infrastruktura TCK**	8 139 932 Kč	8 139 932 Kč	1 627 986 Kč	9 767 919 Kč
1	**Management a monitoring**	295 483 Kč	295 483 Kč	59 097 Kč	354 580 Kč
			25 191 453 Kč	5 038 291 Kč	30 229 744 Kč

CELKEM MAINTENANCE a SLUŽBY					
počet	Položka	Cena v Kč bez DPH	Cena Celkem v Kč bez DPH	Cena DPH (DPH 20 %)	Cena celkem v Kč s DPH
1	**Maintenance , Carepacky - 3 roky OD okamžiku řádného ukončení zkušebního provozu - Akceptace**	13 589 080 Kč	13 589 080 Kč	2 717 816 Kč	16 306 895 Kč
1	**Implementační a servisní služby DO okamžiku řádného ukončení zkušebního provozu - Akceptace**	4 623 087 Kč	4 623 087 Kč	924 617 Kč	5 547 704 Kč
			18 212 166 Kč	3 642 433 Kč	21 854 600 Kč

Část B. – Integrace vnitřního systému

Integrace vnitřního systému					
Cena za plnění oblasti Integrace vnitřního systému		Nabídková cena			
počet	Položka	Kusová cena v Kč bez DPH	Cena Celkem v Kč bez DPH	Cena DPH (DPH 20 %)	Cena celkem v Kč s DPH
1	Analýza	1 649 700 Kč	1 649 700 Kč	329 940 Kč	1 979 640 Kč
1	Návrh IDM	174 300 Kč	174 300 Kč	34 860 Kč	209 160 Kč
1	Návrh ESB	174 300 Kč	174 300 Kč	34 860 Kč	209 160 Kč
1	Návrh integrace na Nintex (práce společně s PASem)	87 200 Kč	87 200 Kč	17 440 Kč	104 640 Kč
1	Návrh integrace AIS n	871 700 Kč	871 700 Kč	174 340 Kč	1 046 040 Kč
1	Návrh integrace HR	348 700 Kč	348 700 Kč	69 740 Kč	418 440 Kč
1	Součinnost ze strany dodavatele HR	200 000 Kč	200 000 Kč	40 000 Kč	240 000 Kč
1	Návrh integrace GINIS	87 200 Kč	87 200 Kč	17 440 Kč	104 640 Kč
1	Návrh integrace Portál	87 200 Kč	87 200 Kč	17 440 Kč	104 640 Kč
1	Návrh Kukátka	87 200 Kč	87 200 Kč	17 440 Kč	104 640 Kč
1	Návrh eProxy	87 200 Kč	87 200 Kč	17 440 Kč	104 640 Kč
1	Vývoj IDM	1 133 200 Kč	1 133 200 Kč	226 640 Kč	1 359 840 Kč
1	Vývoj eProxy	261 500 Kč	261 500 Kč	52 300 Kč	313 800 Kč
1	Vývoj kukátko	122 000 Kč	122 000 Kč	24 400 Kč	146 400 Kč
1	Vývoj nad ESB	5 230 300 Kč	5 230 300 Kč	1 046 060 Kč	6 276 360 Kč
1	Portálové řešení, portál úředníka - aplikace a WorkFlow	1 026 000 Kč	1 026 000 Kč	205 200 Kč	1 231 200 Kč
1	Instalace a základní konfigurace ESB (TEST + PROD)	52 300 Kč	52 300 Kč	10 460 Kč	62 760 Kč
1	Instalace a základní konfigurace IDM (TEST + PROD)	52 300 Kč	52 300 Kč	10 460 Kč	62 760 Kč
1	Nasazení řešení TEST	87 200 Kč	87 200 Kč	17 440 Kč	104 640 Kč
1	Nasazení řešení PROD	87 200 Kč	87 200 Kč	17 440 Kč	104 640 Kč
1	Dokumentace instalační, administratorska, technicka, uživatelská	289 300 Kč	289 300 Kč	57 860 Kč	347 160 Kč
1	Testy integrační	1 394 700 Kč	1 394 700 Kč	278 940 Kč	1 673 640 Kč
1	Testy výkonností	523 000 Kč	523 000 Kč	104 600 Kč	627 600 Kč
1	Testy funkční	348 700 Kč	348 700 Kč	69 740 Kč	418 440 Kč
1	Testy oprávnění	174 300 Kč	174 300 Kč	34 860 Kč	209 160 Kč
1	Analytická podpora analytika při vývoji	871 700 Kč	871 700 Kč	174 340 Kč	1 046 040 Kč
1	Projektové řízení	348 700 Kč	348 700 Kč	69 740 Kč	418 440 Kč
1	IS pro podporu správních řízení (zahrnuje nevýhradní neomezenou licenci)	802 400 Kč	802 400 Kč	160 480 Kč	962 880 Kč
1	JBoss Enterprise SOA Platform with Management, 16 Core Standard, vč. maintenance	1 315 604 Kč	1 315 604 Kč	263 121 Kč	1 578 725 Kč
2	SharePoint Svr 2010 OLP NL GOVT	93 936 Kč	187 872 Kč	37 574 Kč	225 446 Kč
1	Nintex WorkFlow 2010 standard edice, vč. maintenance	221 157 Kč	221 157 Kč	44 231 Kč	265 388 Kč
			18 384 133 Kč	3 676 827 Kč	22 060 960 Kč

Část C. – Elektronická spisová služba

Elektronická spisová služba					
Cena za plnění oblasti Elektronická spisová služba		Nabídková cena			
počet	Položka	Kusová cena v Kč bez DPH	Cena Celkem v Kč bez DPH	Cena DPH (DPH 20 %)	Cena celkem v Kč s DPH
1	Jádro systému (neomezený počet dokumentů ročně)	225 000 Kč	225 000 Kč	45 000 Kč	270 000 Kč
1	Rozšíření jádra - elektronické dokumenty + el.podpis + časové razítk	67 500 Kč	67 500 Kč	13 500 Kč	81 000 Kč
1	ADM - Základní administrace systému (T-klient)	3 000 Kč	3 000 Kč	600 Kč	3 600 Kč
1	AKC - Administrace kontrolních chodů (T-klient)	2 100 Kč	2 100 Kč	420 Kč	2 520 Kč
1	ADK - Správa kartotéky externích subjektů (T-klient)	3 750 Kč	3 750 Kč	750 Kč	4 500 Kč
1	ADS - Administrace sestav (T-klient)	1 500 Kč	1 500 Kč	300 Kč	1 800 Kč
1	SSD - Systém správy dokumentů (server, neomezená licence)	13 500 Kč	13 500 Kč	2 700 Kč	16 200 Kč
260	SSD - Systém správy dokumentů (L-klient, nevýhradní neomezená multilicence)	1 858 Kč	483 000 Kč	96 600 Kč	579 600 Kč
1	XRG - Webová služba pro napojení na ISDS	59 500 Kč	59 500 Kč	11 900 Kč	71 400 Kč
1	Analýza, projekt	200 000 Kč	200 000 Kč	40 000 Kč	240 000 Kč
1	Implementace, konfigurace, administrace	250 000 Kč	250 000 Kč	50 000 Kč	300 000 Kč
1	Implementace SSD (funkčnost POD, VYP, USU, SPI a TPD)	500 000 Kč	500 000 Kč	100 000 Kč	600 000 Kč
1	Podpora zkušebního provozu	200 000 Kč	200 000 Kč	40 000 Kč	240 000 Kč
			2 008 850 Kč	401 770 Kč	2 410 620 Kč

Část D. – Datové sklady (DS), manažerské informační systémy a nástroje Business Intelligence (BI) Jihomoravského kraje

Datové sklady (DS), manažerské informační systémy a nástroje Business Intelligence (BI)					
Cena za plnění oblasti Datové sklady (DS), manažerské informační systémy a nástroje Business Intelligence (BI)		Nabídková cena			
počet	Položka	Kusová cena v Kč bez DPH	Cena Celkem v Kč bez DPH	Cena DPH (DPH 20 %)	Cena celkem v Kč s DPH
300	Komplexní analýza a návrh datového skladu	2 200 Kč	660 000 Kč	132 000 Kč	792 000 Kč
200	-dokumentace - tvorba	1 600 Kč	320 000 Kč	64 000 Kč	384 000 Kč
40	-administrace globálních číselníků	1 600 Kč	64 000 Kč	12 800 Kč	76 800 Kč
16	-grantovací skript	1 100 Kč	17 600 Kč	3 520 Kč	21 120 Kč
1	Ekonomika zdravotnických zařízení (přímo řízená zdravotnická zařízení JMK) - Licence MVY - Tržiště výkazů aj.dle ZD	75 000 Kč	75 000 Kč	15 000 Kč	90 000 Kč
40	-kustomizace ETL	1 600 Kč	64 000 Kč	12 800 Kč	76 800 Kč
240	-Vývoj ETL	1 600 Kč	384 000 Kč	76 800 Kč	460 800 Kč
40	-Datový model	1 600 Kč	64 000 Kč	12 800 Kč	76 800 Kč
40	-testování	1 100 Kč	44 000 Kč	8 800 Kč	52 800 Kč
1	Ekonomika školských zařízení (školská zařízení zřizovaná JMK) - Licence MVY - Tržiště dle ZD	75 000 Kč	75 000 Kč	15 000 Kč	90 000 Kč
1	-kustomizace ETL	1 600 Kč	1 600 Kč	320 Kč	1 920 Kč
140	-Vývoj ETL	1 600 Kč	224 000 Kč	44 800 Kč	268 800 Kč
80	-Datový model	1 600 Kč	128 000 Kč	25 600 Kč	153 600 Kč
40	-testování	1 100 Kč	44 000 Kč	8 800 Kč	52 800 Kč
1	Ekonomika ostatních neškolských zařízení -Licence MVY - Tržiště dle ZD	75 000 Kč	75 000 Kč	15 000 Kč	90 000 Kč
10	-kustomizace ETL	1 600 Kč	16 000 Kč	3 200 Kč	19 200 Kč
140	-Vývoj ETL	1 600 Kč	224 000 Kč	44 800 Kč	268 800 Kč
40	-Datový model	1 600 Kč	64 000 Kč	12 800 Kč	76 800 Kč
40	-testování	1 100 Kč	44 000 Kč	8 800 Kč	52 800 Kč
1	Ekonomika krajského úřadu JMK - funkčnost dle ZD -Licence MEK Tržiště Ekonomické (kostky dle ZD)	1 320 000 Kč	1 320 000 Kč	264 000 Kč	1 584 000 Kč
40	-kustomizace ETL	1 600 Kč	64 000 Kč	12 800 Kč	76 800 Kč
40	-testování	1 100 Kč	44 000 Kč	8 800 Kč	52 800 Kč
170	Základní přehledové údaje příspěvkových organizací dle ZD -Vývoj ETL	1 600 Kč	272 000 Kč	54 400 Kč	326 400 Kč
40	-Datový model	1 600 Kč	64 000 Kč	12 800 Kč	76 800 Kč
40	-testování	1 100 Kč	44 000 Kč	8 800 Kč	52 800 Kč
390	Statistika a výkony zdravotní péče (přímo řízená zařízení JMK) - Vývoj ETL	1 600 Kč	624 000 Kč	124 800 Kč	748 800 Kč
80	-Datový model	1 600 Kč	128 000 Kč	25 600 Kč	153 600 Kč
80	-testování	1 100 Kč	88 000 Kč	17 600 Kč	105 600 Kč
1	Data ČSÚ (demografická data získaná od ČSÚ) -Licence Statistika	142 500 Kč	142 500 Kč	28 500 Kč	171 000 Kč
40	-kustomizace ETL	1 600 Kč	64 000 Kč	12 800 Kč	76 800 Kč
40	-testování	1 100 Kč	44 000 Kč	8 800 Kč	52 800 Kč
80	Metadata (řeší požadavky dle ZD) -Vývoj ETL	1 600 Kč	128 000 Kč	25 600 Kč	153 600 Kč
40	-Datový model	1 600 Kč	64 000 Kč	12 800 Kč	76 800 Kč
40	-testování	1 100 Kč	44 000 Kč	8 800 Kč	52 800 Kč
80	Interní portál a jeho funkce dle ZD -Sites (oborové stránky, týmy atd.)	1 600 Kč	128 000 Kč	25 600 Kč	153 600 Kč
100	-KPI (indikátory)	1 600 Kč	160 000 Kč	32 000 Kč	192 000 Kč
300	-Reporting (Reporting Services, Excel Services)	1 600 Kč	480 000 Kč	96 000 Kč	576 000 Kč
260	-Dashboardy (Performance Point Services)	1 600 Kč	416 000 Kč	83 200 Kč	499 200 Kč
40	-administrace interního portálu	1 600 Kč	64 000 Kč	12 800 Kč	76 800 Kč
40	-testování	1 100 Kč	44 000 Kč	8 800 Kč	52 800 Kč
80	Externí portál a jeho funkce dle ZD -Sites (oborové stránky, týmy atd.)	1 600 Kč	128 000 Kč	25 600 Kč	153 600 Kč
40	-KPI (indikátory)	1 600 Kč	64 000 Kč	12 800 Kč	76 800 Kč
150	-Reporting (Reporting Services, Excel Services)	1 600 Kč	240 000 Kč	48 000 Kč	288 000 Kč
40	-administrace externího portálu	1 600 Kč	64 000 Kč	12 800 Kč	76 800 Kč
40	-testování	1 100 Kč	44 000 Kč	8 800 Kč	52 800 Kč
40	seznámení - analytiků	1 600 Kč	64 000 Kč	12 800 Kč	76 800 Kč
40	-seznámení administrátorů	1 600 Kč	64 000 Kč	12 800 Kč	76 800 Kč
30	-seznámení pro zaměstnance	1 600 Kč	48 000 Kč	9 600 Kč	57 600 Kč
24	-příprava seznámení pro občany	1 600 Kč	38 400 Kč	7 680 Kč	46 080 Kč
40	Další služby -Propojení na GIS aj.	1 600 Kč	64 000 Kč	12 800 Kč	76 800 Kč
140	-web services	1 600 Kč	224 000 Kč	44 800 Kč	268 800 Kč
40	-testování	1 100 Kč	44 000 Kč	8 800 Kč	52 800 Kč
	Všechny výše uvedené licence jsou nevýhradní neomezené multilicence, uváděné počty jsou pouze pro účely kalkulace ceny				
1	Microsoft SharePoint Server 2010	93 936 Kč	93 936 Kč	18 787 Kč	112 723 Kč
640	Microsoft SharePoint Enterprise CAL 2010 (User CAL)	1 686 Kč	1 079 040 Kč	215 808 Kč	1 294 848 Kč
4	Microsoft SQL Server Standard Edition 2012 - Core 2Lic	72 925 Kč	291 700 Kč	58 340 Kč	350 040 Kč
1	Microsoft SharePoint Internet Sites Standard 2010	239 870 Kč	239 870 Kč	47 974 Kč	287 844 Kč
1	Windows Server 2008 External Connector	41 068 Kč	41 068 Kč	8 214 Kč	49 282 Kč
			9 846 714 Kč	1 969 343 Kč	11 816 057 Kč

Část E. – Krajská digitální spisovna (KDS), Krajský digitální repozitář (KDR)

Krajská digitální spisovna (KDS), Krajský digitální repozitář (KDR)					
Cena za plnění oblasti Krajská digitální spisovna (KDS), Krajský digitální repozitář (KDR)		Nabídková cena			
počet	Položka	Kusová cena v Kč bez DPH	Cena Celkem v Kč bez DPH	Cena DPH (DPH 20 %)	Cena celkem v Kč s DPH
1	Dodávka KDS	652 484 Kč	652 484 Kč	130 497 Kč	782 981 Kč
1	Dodávka KDR	652 484 Kč	652 484 Kč	130 497 Kč	782 981 Kč
1	Implementace KDS	4 085 529 Kč	4 085 529 Kč	817 106 Kč	4 902 635 Kč
1	Implementace KDR	2 609 501 Kč	2 609 501 Kč	521 900 Kč	3 131 401 Kč
			7 999 998 Kč	1 600 000 Kč	9 599 998 Kč

Příloha č. 3 – Část Díla, jejíž plnění je zajištěno prostřednictvím subdodavatele

Specifikace části Díla, jejíž plnění bude Zhotovitel realizuje prostřednictvím subdodavatele.

Subdodavatel Zhotovitele	**Část Plnění Díla, kterou Zhotovitel realizuje prostřednictvím subdodavatele**
GORDIC spol. s r.o. Erbenova 4 586 01 Jihlava IČ: 47903783 Zastoupená: Ing. Jaromír Řezáč jednatel společnosti Jaromir_Rezac@gordic.cz	Podíl na plnění: - funkční oblast Elektronická spisová služba - funkční oblast Datové sklady (DS), manažerské informační systémy a nástroje Business Intelligence (BI) Jihomoravského kraje - funkční oblast Krajská digitální spisovna (KDS), Krajský digitální repozitář (KDR) - kapitola Aplikační software pro podporu správních řízení, jenž je obsažena ve funkční oblasti Vnitřní integrace krajského úřadu

Příloha č. 4 – Projektová metodika

Úvod

Projektová metodika je založena a vychází ze základního projektového rámce PRINCE2 (zkratka z anglického **PR**oject **IN CO**ntrolled **E**nvironments)**.** V současné době patří projektový rámec PRINCE2, společně s IPMA a PMI k nejznámějším a nejpoužívanějším metodikám. Na té metodě staví projektové řízení vlády států Evropské unie, významné mezinárodní instituce jako je OSN, NATO nebo významné komerční subjekty (DHL, Deutsche Post aj.).
Základy projektového rámce PRINCE2 byly položeny v roce 1989 na popud britské vlády a jejím primárním zaměřením byly IT projekty. Již v základu zahrnoval hierarchickou strukturu řízení projektů, orientaci na výsledek, plánování, řízení zdrojů a kontrolu. V roce 1996 byla metodika revidována a obohacena o zkušenosti ze 150 evropských společností a byla transformována pro obecné použití v různorodých prostředích na rozmanité druhy projektů.

Výhody projektové metody PRINCE2

Mezi hlavní výhody projektové metody patří:

- vysoká míra flexibility a aplikovatelnosti na různorodé projekty
- důrazně zahrnuje a uplatňuje projektové řízení na základě procesů
- pokrývá celý životní cyklus projektu
- popisuje důležité prvky projektového řízení
- jasně a přehledně definuje role, strukturu a odpovědnosti v hierarchicky organizované struktuře
- dbá na primární motivaci projektu a verifikuje přínos v rámci celého běhu projektu
- pracuje s jasně měřitelnými výstupy a produkty

Základní charakteristika

Projektový rámec PRINCE2 je charakterizován několika pevnými stavebními prvky:

- projekt je řízen z určitého důvodu, jehož oprávněnost se v průběhu projektu verifikuje
- má jasně definovanou strukturu rolí a odpovědností
- zakládá se na procesním řízení (sedmi procesech)
- procesy jsou podporovány sedmi tématy
- řídí projekt po etapách
- je zaměřena na měřitelný výsledek

Projektová metoda je řešena v rámci čtyř, níže uvedených pohledů:

- Principy
- Témata
- Procesy
- Prostředí (Přizpůsobení PRINCE2 danému projektu)

Principy PRINCE2

Projektová metoda PRINCE2 je vybudována na sedmi principech, které jsou aplikovány nezávislé na rozsahu projektu, kultuře, geografickému umístění nebo typu organizace. Vycházejí z universálnosti, jsou ověřeny dlouholetými praktickými zkušenostmi.

Průběžné ověřování důvodů (Continued business justification)

Projekt musí mít oprávněný důvod zahájení a tento důvod musí být v průběhu celého projektu sledovaný, oprávněný, i když se může v průběhu projektu vyvíjet. Důvod projektu musí být popsán a schválen.

Využití zkušeností (Learn from experience)

V rámci přípravy, průběhu i ukončení projektu jsou ověřovány zkušenosti z minulých projektů, jsou přenášeny do stávajícího projektu a jsou evidovány a vyhodnocovány při ukončení projektu. Každý projekt by měl znamenat v důsledku zkušeností kvalitativní posun.

Definice rolí a odpovědností (Defines roles and responsibilities)

V rámci projektu jsou definovány role a odpovědnosti, které zahrnují vedení (business), dodavatele a další participující skupiny (uživatele, odběratele produktu). Důraz je kladen na porozumění jednotlivých a rolí a zejména odpovědností vyplývajících z jednotlivých rolí.

Řízení dle etap (Manage by Stages)

Projekt je plánován, řízen a kontrolován podle jednotlivých etap. Projekt je rozdělen dle složitosti, rozsahu na několik etap, kde je možné efektivně řídit dodání produktu. Minimální počet etap jsou dvě.

Řízení dle výjimek (Manage by exception)

Projektová metoda PRINCE2 definuje přijatelnou míru výjimky pro každou delegovanou pravomoc. Výjimka může být v různých oblastech projektu. Konkrétně se jedná o odchylku v čase, nákladech, rozsahu, kvalitě, rizicích a benefitech. Cílem řízení dle odchylek je dosáhnout vyvážené míry řízení projektu, tzn. eskalovat na sponzora projektu (Executive) pouze relevantní výjimky od plánu, nezahltit jej přílišným množstvím požadavků na rozhodnutí při zachování dostatečné míry kontroly.

Orientace na produkt (Focus on products)

Důležitým principem metody je orientace na výsledek projektu (produkt). Projekt je pouze prostředek pro dosažení produktu. Tento princip sleduje definici produktu se zaměřením ne měřitelnou kvalitu a jeho dodání. Důležitým prvkem tohoto principu je zahrnou do popisu a akceptace produktu participující strany (uživatele, odběratele).

Přizpůsobení (Tailor to suit the project environment)

Princip sleduje úpravu PRINCE2 dle konkrétního prostředí, rozsahu, složitosti, geografického a kulturního prostředí. Cílem je sladit projektovou metodiku s konkrétním projektovým prostředím, metodikami společnosti, s interními procesy apod. Je kladen důraz na efektivitu získávání informací a rozhodování.

Procesy PRINCE2

Metoda je řízena sedmi základními procesy, které zahrnují už předprojektovou přípravu a pokrývají celý životní cyklus projektu až po jeho ukončení.

Předprojektová příprava (Starting Up a Project)

Předprojektová příprava zahrnuje definici mandátu projektu, jmenování sponzora projektu (Executive), projektového vedoucího (Project Manager) a definuje se základní zdůvodnění projektu vyjádřené základy obchodního případu (Outline Business Case). Dále se shromáždí relevantní a dostupné informace vymezující rozsah projektu a stanoví základní postup pro dosažení výsledného produktu. Připraví se zahájení dalšího procesu.

Řízení projektu (Directing Project)

Proces řízení projektu, který pokrývá téměř celý životní cyklus projektu. Tento proces pokrývá řízení projektu ze strany projektového výboru (Project Board) a má za cíl monitorovat průběh projektu, rozhodovat o výjimkách projektu, schvalovat zahájení a ukončení jednotlivých etap projektu. Zajišťuje komunikaci s vedením společnosti, popřípadě s vedením projektového programu.

Iniciace projektu (Initiating a Project)

V rámci iniciace projektu je vytvořena strategie řízení rizik, řízení kvality, konfigurace a komunikace. Je vytvořen plán projektu a nastaveny kontrolní mechanismy. Detailně popsány měřitelné výstupy projektu (produkty). Vytváří se registr rizik a otevřených bodů (Issue).

Řízení etapy projektu (Controlling a Stage)

Tento proces má za cíl sledovat průběh dodávky produktu dané etapy v požadované kvalitě, ceně, času, rozsahu, rizicích a benefitech. Sleduje výjimky od plánu, rizika a otevřené body provázející danou etapu.

Řízení dodávky produktu (Managing Product Delivery)

Cílem tohoto procesu je vytvoření vlastního produktu od jeho schválení, vytvoření plánu, sledování kvalitativních kritérií a jeho vlastního předání.

Řízení hranic etapy (Managing Stage Boundry)

Řízení hranic etapy si klade za cíl poskytnout projektovému výboru (Project Board) dostatečné informace o průběhu projektu pro schválení ukončení etapy a zahájení etapy další, popřípadě pro schválení výjimky z plánu projektu.

Ukončení projektu (Closing a Project)

Proces ukončení projektu si klade za cíl ověřit splnění akceptačních kritérií, ověřit schopnost následné podpory produktu, vyhodnotit projekt oproti plánu, ověřit dosažení plánovaných benefitů, vypořádat se s otevřenými body a riziky formou doporučení.

Témata metodologie PRINCE2

Témata projektové metodologie popisují aspekty projektového řízení, které musí být neustále sledovány. Každé téma je integrováno do projektové metodiky a jsou vzájemně provázána. V rámci metodiky jsou témata chronologicky uspořádána.

Obchodní případ (Business Case)

Jedná se o základní motivační prvek projektu a definuje očekávaný cíl, který má být dosažen prostřednictvím projektu. Odpovídá na otázku: „Proč by měl být projektu zahájen?“.

Organizace (Organization)

Pro realizaci projektu vzniká dočasná organizační struktura, která zahrnuje tři základní klíčové složky:

- obchod
- uživatel
- dodavatel

Pro všechny tyto složky jsou popsány a definovány role a příslušné odpovědnosti tak, aby byl projekt realizován efektivně. Odpovídá na otázku: „Kdo bude projekt realizovat?“.

Kvalita (Quality)

Tato téma má za cíl v rámci projektu definovat a ověřovat naplnění měřitelných kvalitativních kritérií výsledného produktu. Odpovídá na otázku: „Co je produktem projektu?“.

Plány (Plans)

PRINCE2 je postaven na realizaci jednotlivých schválených plánů. Zahrnuje kroky, které je nutné uskutečnit pro dosažení produktu v plánované kvalitě. Důležitou součástí tématu je komunikace a kontrola. Téma odpovídá na otázku: „Jak, kolik a kdy se bude projekt realizovat?“.

Rizika (Risks)

Typickým rysem projektu je větší míra rizika, než je u běžného rutinního provozu. Cílem tohoto tématu je řídit neočekávané stavy projektu. Odpovídá na otázku „Co se v projektu stane když?“.

Změna (Change)

Zde se jedná o popis reakce a způsobu zpracování problému, pokud má dopad na plán projektu. Dopady na projekt mohou být různé a je nutné je posoudit ocenit a zvážit. Téma odpovídá na otázku: „Jaký je dopad na projekt?“.

Progres (Progress)

Téma se zabývá rozhodovacím procesem pro dosažení plánu, sleduje životaschopnost plánu, monitoruje aktuální stav a eskaluje případné výjimky od plánovaného stavu. Odpovídá na otázku: „Kde se nyní v projektu nacházíme, kam směřujeme a můžeme pokračovat?“.

Přizpůsobení metodiky prostředí (Tailoring to the project environment)

Vysoká použitelnost a škálovatelnost projektové metodologie vyžaduje její uzpůsobení konkrétnímu prostředí a konkrétním podmínkám provázející daný projekt. Na konkrétní podobu realizace projektu má vliv např. komplexnost projektu, geografické a kulturní prostředí, to, zda je projekt součástí programu aj.
V rámci nastavení projektu jsou:

- aplikovány principy (nejsou nastavovány)
- témata jsou přizpůsobena interním standardům společnosti (metodiky, procesy, způsoby dokumentace apod.)
- je dohodnuta používaná terminologie
- přizpůsoben způsob popisu produktu
- přizpůsobeny role
- přizpůsobeny procesy

V rámci nastavení projektové metodiky pro konkrétní prostředí je vhodné zahrnout faktory jako je např.:

- zda je projekt součástí programu
- zda se jedná o projekt za účasti externího subdodavatele
- zda je projekt realizován v komerční nebo jiné sféře
- zda jde o projekt v multifiremním prostředí

V tabulce je uveden příklad uzpůsobení projektové metodiky na základě rozsahu projektu.

Rozsah projektu		**Popis**	**Aplikace PRINCE2**
Vysoký	Program	Změna podnikání	Použít rámec pro řízení programů OGC's Managin Succesful. PRINCE2 může být použit k řízení jednotlivých projektů.
	Rizikový projekt	Vysoká rizika, náklady, důležitost, zasahuje do více organizací a více odborných disciplín, popř. mezinárodní projekt.	Projekt s více etapami, s širším zastoupením v Projektovém výboru, samostatné role vedoucích týmů, projektová podpora je zajišťována samostatnou rolí. Jednotlivé produkty jsou dodávány samostatně.
	Normální projekt	Střední míra rizika, důležitosti, nákladů, vztah zákazník/dodavatel, projekt realizován na více místech.	Jedna nebo více produkčních etap, Standardní Projektový výbor výbor, je vhodné mít samostatnou roli týmového vedoucího a projektové podpory. Produkty lez dodávat sdruženě.
	Jednoduchý projekt	Nízká rizika, náklady, důležitost, jedno místo realizace.	Jedna produkční fáze, Jednoduché složení Projektového výboru, projektový vedoucí plní úlohu i vedoucího realizačního týmu. Produkty jsou dodávány sdruženě.
Nízký	Úkol	Většinou jednočlenný Projektový výbor v roli, Sponzora projektu bývá liniovým manažerem projektového	Dodává se jeden produkční balíček. Použije se pouze popis produktu, report o stavu prací a registr problémů a rizik.

		vedoucího. Projektový manažer může i přímo plnit stanovený úkol.	

Plánování a řízení projektu

Organizační struktura projektu

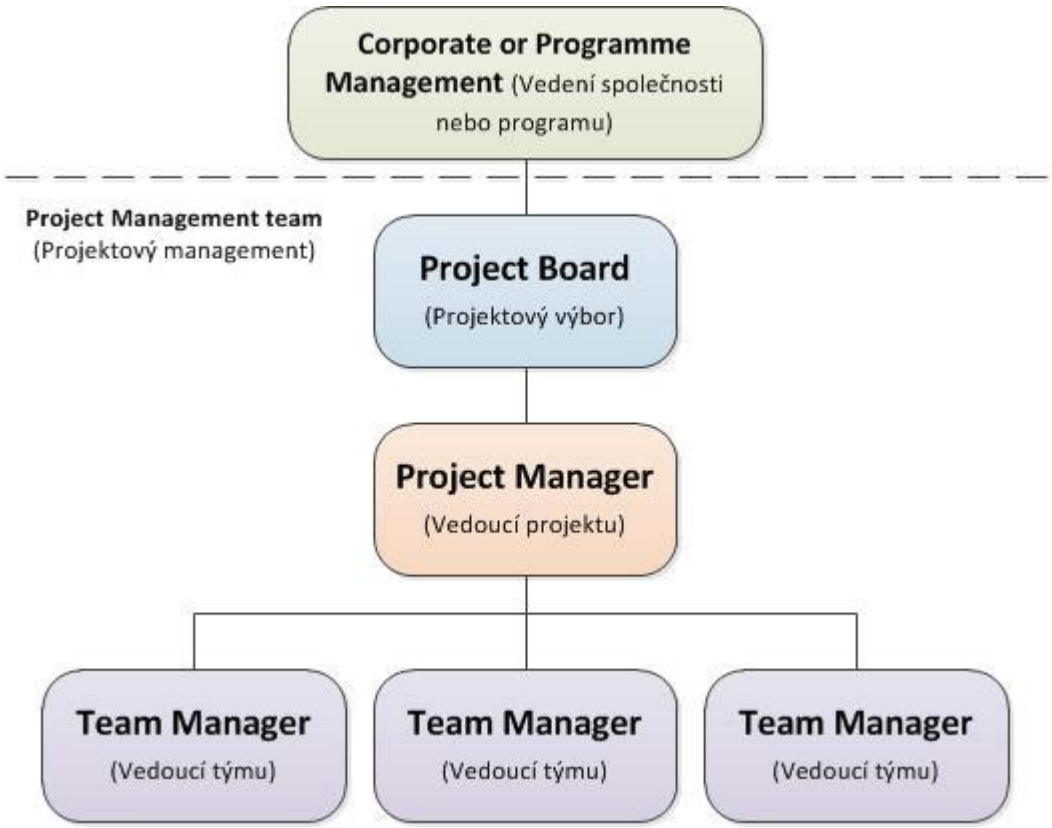
PRINCE2 klade důraz na hierarchickou strukturu řízení a již se své podstaty klade důraz na definici rolí a odpovědností.

Vedení společnosti nebo programu (Corporate or programme management)

Jedná se o úroveň managementu, která nenáleží do organizační struktury projektového týmu, ale je odpovědná za schválení projektu jako celku, definuje povolené odchylky v rámci celého projektu, popř. přenáší standardy z úrovně řízení projektového programu.

Projektový výbor (Project Board)

Je odpovědný vedení společnosti nebo programovému za úspěch projektu. Schvaluje základní plán projektu a zdroje, schvaluje výjimky v plánu projektu, ukončení jednotlivých etap, schvaluje zahájení etap a zajišťuje komunikaci s dalšími zainteresovanými stranami.



Složení Projektového výboru je Sponzor projektu (Executive), Hlavní uživatel (Senior User) a Hlavní dodavatele (Senior Supplier).

Projektový vedoucí (Project Manager)

Je odpovědný za řízení projektu na denní bázi v rámci tolerance definované Projektovým výborem. Primárně je projektový vedoucí odpovědný za dodání produktu v plánovaném čase, nákladech, rozsahu, kvalitě, rizicích a přínosech.

Vedoucí týmu (Team Manager)

Je odpovědný za dodávku produktu ve stanovém čase, kvalitě a nákladech. Dále je odpovědný za vedení týmu specialistů.

Plán projektu

V procesu startu projektu je schválen základní plán projektu a případně první etapa projektu, která je rozpracována do detailu. Jsou stanoveny povolené výjimky pro jednotlivé kategorie odpovědností. Plánování projektu může být, dle komplexnosti projektu, vedeno v různých úrovních detailu.

Úroveň „plán projektu“

Zde jsou zachyceny základní etapy projektu a jsou podkladem pro rozhodování Projektového výboru. Jsou zde základní kontrolní body vztahující se například ke sledování nákladů, případně benefitů projektu.

Úroveň „plán etapy“

Plán etapy v sobě zahrnuje výsledný produkt, zdroje, aktivity a kontrolní body, na základě kterých lze sledovat postup prací na etapě.

Úroveň „plán týmu“

Pokud je použit tak definuje časovou osu tvorby konkrétního balíku prací.

Projektová dokumentace

Rozsah a konkrétní podoba dokumentace závisí na rozsahu a složitosti projektu. U složitějších projektů jsou jednotlivé oblasti řešeny samostatnými dokumenty, u jednodušších pouze kapitolami v souhrnném dokumentu. Rozsah a podoba dokumentace je ustanovena v rámci přizpůsobení projektové metodiky pro konkrétní projekt.

Dokumentace o Nastavení projektu (Project Initiation Documentation)

Jedná se o souhrn informací a dokumentů sloužící jako vstupní podklad pro zahájení projektu. Dokument obvykle postihuje následující oblasti:

- Obchodní záměr (Business Case)
- Chartu projektu (Project Brief)
- Organizační strukturu projektu, popis rolí a odpovědností
- Strategie řízení kvality (Quality Management Strategy)
- Strategie řízení konfigurace (Configuration Management Strategy)
- Strategie řízení komunikace (Communication Management Strategy)
- Strategie řízení rizik (Risk Management Strategy)
- Plán projektu, etapy
- Plán revize přínosů (Benefits review Plan)
- Popis produktu (Project Produkt Description)

Reporty

V průběhu projektu jsou monitorovány a reportovány stavy na různých úrovních a různou intenzitou. V rámci projektu jsou zejména vedeny reporty:

- Zpráva o ukončení etapy (End Stage Report)
- Zpráva o stavu etapy (Highlight Report)
- Zpráva o výjimce (Exeption Report)
- Zpráva o stavu balíku práce (Checkpoit Report)
- Závěrečné hodnocení etapy (End Stage Assessment)
- Zpráva o otevřených bodech (Issue Report)
- Report k ukončení projektu (End Project Report)

Další dokumenty

Dalšími dokumenty, které jsou vedeny v rámci celého životního cyklu projektu, jsou:

- Registr otevřených bodů (Issue Register)
- Registr rizik (Risk Register)
- Plán realizace výjimky (Exception Plan)
- Přehled kontroly kvality (Quality Log)
- Registr kvality (Quality Register)
- Zápisy z jednání (Meeting Minutes)
- Akceptační protokol (Aceptance Record)

Příloha č. 5 – Technické parametry SLA

Pro sledování plnění jednotlivých parametrů SLA je využíváno Service Desku Zhotovitele, který obsahuje i systémy pro sledování průběhu procesů z hlediska plnění definovaných metrik – notifikační systém a Workflow management.
Pro měření procesů existuje **Katalog metrik** (měření tvrdých dat, měření měkkých dat – např. spokojenost zákazníka se službami pomocí dotazníku je měřeno individuálně)

- Interval měření – jeden měsíc
- Báze dat – uzavřené požadavky v období, realizované tel. hovory za období

Mimo sledování a vyhodnocování parametrů SLA se vyhodnocují i následující ukazatele procesů:

- Příjem kontaktů
    - Obslužnost: Metrika stanoví minimální hranici příjmu kontaktů (většinou telefonického hlášení) oproti všem příchozím kontaktům.
    - Odezva: Metrika definuje parametr pro rychlost odezvy na příjem kontaktů.
- Zpracování požadavků
    - Reakční doba: Metrika vyhodnocuje reakci na změnu stavu.
    - Čas vlastního plnění: Metrika měří čas na zpracování/vyřešení požadavků
- Výkon Service Desku
    - Počet vstupních kontaktů: Suma všech vstupních kontaktů definovanými kanály
    - Počet řešených požadavků: Suma všech vyřešených požadavků.
- Kvalitativní metriky
    - Komunikace: Kontrola kvality komunikace operátora s uživatelem.
    - Záznam: Kontrola záznamů zapsaných do systému Service Desku.
    - Dispečink: Kontrola chybných přidělení na řešitele, nebo řešitelské skupiny.

PARAMETRY SLA PRO OBLASTI PODPORY

- Závady
- Požadavky na provozní správu
- Požadavky na expertní podporu
- Změny provozní dokumentace
- Monitroing Hw a základního SW

Zhotovitel garantuje Objednatelem požadovanou dostupnost ve smyslu Objednatelem požadované úrovně poskytovaných služeb servisní podpory (SLA) na úrovni 99,620% v režimu 24/7, kterou zajišťuje službami podpory v profesionální kvalitě za:

- důsledného dodržování doporučení technologických standardů vyplývajících ze standardů ISO 9001, ISO 20000, ISO 27001, ISO 16001, ITIL a interní projektové metodiky,
- zajištění dostatečného počtu kvalifikovaného personálu,
- proaktivního používání nástrojů Service Desku pro měření a vyhodnocování kvality poskytovaných služeb.

SLA – závady					
Část (modul)	**Dostupnost služby**	**Příjem požadavku**	**Klasifikace závady**	**Doba reakce**	**Doba vyřešení**
A – TCK	24x7	24x7	A	1 hodina	4 hodiny (pro HW 2 hodiny vzdáleně, 4 hodiny onsite)
			B	4 hodiny	8 hodin
			C	6 hodin	Do konce následujícího pracovního dne
B – VIU **D – DS**	8x5	8x5	A	4 hodiny	Do konce následujícího pracovního dne
			B	8 hodin	Do 3 pracovních dnů
			C	Do konce následujícího pracovního dne	Do 10ti pracovních dnů
C – eSPS **E – KDS a KDR**	12x5	12x5	A	2 hodiny	4 hodiny
			B	4 hodiny	8 hodin
			C	6 hodin	Do konce následujícího pracovního dne

SLA – požadavky na provozní správu			
Část (modul)	**Dostupnost služby**	**Příjem požadavku**	**Doba reakce**
A – TCK	5x8	24x7	Do konce následujícího pracovního dne
B – VIU **C – eSPS** **D – DS** **E – KDS a KDR**	8x5	8x5	Do konce následujícího pracovního dne

SLA – požadavky na expertní podporu			
Část (modul)	**Dostupnost služby**	**Příjem požadavku**	**Doba reakce**
A – TCK	5x8	24x7	Do konce následujícího pracovního dne
B – VIU **C – eSPS** **D – DS** **E – KDS a KDR**	8x5	8x5	Do konce následujícího pracovního dne
SLA – změny provozní dokumentace			
Část (modul)	**Dostupnost služby**	**Příjem požadavku**	**Doba reakce**
A – TCK	5x8	24x7	Do konce následujícího pracovního dne
B – VIU **C – eSPS** **D – DS** **E – KDS a KDR**	8x5	8x5	Do konce následujícího pracovního dne
SLA – monitoring HW a základního SW			
Část (modul)	**Dostupnost služby**	**Příjem požadavku**	**Doba reakce**
A – TCK	24x7	24x7	30 minut

- U konkrétních HW a SW komponent třetích stran mohou být uplatňované parametry uzpůsobeny podmínkám jejich dodavatele.
- Pokud není určeno jinak, zásah za účelem řešení závady nebo může být proveden vzdáleně nebo onsite.
- Služby budou na vyžádání zadavatele poskytnuty i mimo níže uvedenou provozní dobu zadavatele s ohledem na minimalizaci omezení provozovaných systémů (např. požadavek na aplikaci bezpečnostních oprav může být směřován do nočních hodin nebo dnů volna a pracovního klidu),
- Klasifikace závad:
    - A - Kritická závada = závada bránící zadavateli poskytovat hlavní předmět jeho činnosti (např. služby veřejnosti).
    - B - Střední závada = funkčnost systému významným způsobem degradována nebo silně omezena, opakovaný výskyt závady.
    - C - Nízká závada = funkčnost systému vykazuje určité problémy bez výrazného dopadu na služby poskytované klientům zadavatele.
- Hodnotou 24x7 se rozumí nepřetržité poskytování služby (24 hodin denně, 7 dnů v týdnu, tedy 365 dnů v roce), hodnotou 8x5 se rozumí poskytování v pracovních dnech v době 8.00-16.00 hod., hodnotou 12x5 se rozumí poskytování v pracovních dnech v době 6.00-18.00 hod.
- Počet požadavků na poskytnutí podpory nebude omezován.

Příloha č. 6 – Výčet standardů

Standardy v oblasti vývoje a implementace IS

Zhotovitel - společnost AutoCont a.s je certifikována dle normy ISO 9001. Ta se přímo nevztahuje na vývoj software, a proto je doplněna závazným používáním norem ISO/IEC 20000 a ISO/IEC 27001, které při vývoji důsledně dodržujeme.
V oblasti testování je používána vlastní metodika postavená na normě ISO 9126, která je zakotvena v zavedených pracovních postupech v rámci životního cyklu realizace projektů a vývoje aplikací. Kvalita testování je také podpořena certifikací testerů ISTQB Foundation Level.
Subdodavatel – společnost Gordic
Implementace informačního systému se bude řídit interními normativy z oblasti řízení projektů a vývoje SW v rámci norem ISO 9001:2001 Systém managementu jakosti a ISO 10006:1997 Zabezpečení jakosti při řízení projektů.
Metodologie pro komplexní dodávky se skládá z optimální kombinace následujících celků využívajících důsledně „best practice" přístupy. Řízení projektů je založené na metodologii **PRINCE2 (Projects in Controlled Enviroments)** a implementaci standardů **PMBOK (Project Management Body of Knowledge)**. Je v souladu se standardem ISVS 005/02.01 pro náležitosti životního cyklu informačního systému a normou **ČSN ISO/IEC 12207.**
Pro vývoj SW je používán iterační model RUP (Rational Unified Process). Pro podporu řešení a zajištění správy provozu implementovaných systémů potom metodologie založená na **doporučení ITIL (IT Infrastructure Library)**, což umožňuje pružně reagovat na měnící se požadavky zákazníka dle jeho potřeb. Použití výše uvedených metodologií se vzájemně prolíná v závislosti na druhu projektu.
Projekty se řídí interní směrnicí pro projektový management, směrnicí pro vývoj SW a směrnicí pro zajištění podpory řešení v rámci norem ISO implementované ve společnost Gordic.
Subdodavatel akceptuje postupy a přijímá standardy primecontractora pro oblast vývoje a implementace a v oblastech společného aplikačního vývoje se bude řídit výše uvedeným standardy. Tato shoda je nutná pro naplnění části plnění Integrace, kde se budou Aplikační moduly produktu Ginis napojovat na Integrační sběrnici. Jen takto lze zadavateli garantovat předmět plnění v požadovaném harmonogramu, čase a kvalitě.

Portál a datové sklady

Technologické standardy spojené s technologickou platformou Microsoft Business Intelligence.
(Pozn.: Produkt Microsoft SQL Server 2012, který obsahuje nástroje BI a produkt Microsoft SharePoint 2010 jsou defacto standardem díky obrovskému počtu jejich uživatelů po celém světě.)

Integrační platforma a Workflow

Nabízený systém bude respektovat implementační best practices Javy. Způsob nasazení a správu aplikací pro JBoss AS 7.1 se bude řídit platnými doporučeními a postupy JBoss . Daný server navíc implementuje JEE 6, které je standardem, a prošel schvalovacím procesem, kde schvalovací komisi tvoří zástupci mj. firem Oracle, IBM, RedHat, Apache. JBoss SOA také splňuje standard na definici SOA a využívá všech standardů pro komunikaci a integraci. Dodaná integrační vrstva bude tvořena návrhovými vzory a postupy Enterprise Application Integration (EAI).
Spojení standardů, *„best practices"* a otevřených a ověřených technologií je základním úspěchem každého systému. Integrační platforma nebude postavena z uzavřených neznámých systémů, které zná jen hrstka lidí. Nabízený systém je možné doplnit o nové adaptéry na uzavřené systémy pomocí standardů a otevřít tak systém i jiným aplikacím. Uzavřené systémy navíc nemusí dodržovat standardy, *„best practices"* a nejmodernější technologie.

Technologické standardy:

- Java SE 7 (NIO, JNDI, JMX,)
- JEE 6 (JMS, EJB 3.1, JTA, JPA JMS, JavaMail, JAX-WS, JACC, JCA)
- SQL
- SOA (BPMN2, BPEL, ESB, BR, JAXR)

- Web 2.0 (http/https, e-mail, JSON, Servlet, JSP, JSTL, EL, JSF, WebBeans)
- WS (SOAP, REST, JAX-RCP)
- File Protocols (ftp, sftp, file)
- SCA
- Standard odvozený z BPMN a užívaný pro vizuální modelování Workflow

Spisová služba a IS Správních řízení

Technologické standardy:

- Databázová platforma Microsoft SQL, Oracle, Informix
- Serverová platforma Microsoft Windows Server, Windows/Linux pro Oracle
- Aplikační platforma Microsoft Internet Information Server
- Uživatelské prostředí Microsoft Internet Explorer s podporou nejnovější verze
- Přístup uživatelů do systému prostřednictvím LDAP
- Podpora synchronizace s Active Directory
- Komunikace s jinými aplikacemi pomocí standardů WS* (std. webových služeb)

Metodické a legislativní standardy, soulad

- se zákonem 499/2004 Sb. o archivnictví a spisové službě a o změně některých zákonů, ve znění pozdějších předpisů
- se zákonem č. 227/2000 Sb. o elektronickém podpisu, ve znění pozdějších předpisů
- se zákonem č. 300/2008 Sb. o elektronických úkonech a autorizované konverzi dokumentů, ve znění pozdějších předpisů,
- se zákonem č. 500/2004 Sb., správní řád, ve znění pozdějších předpisů,
- s vyhláškami a usneseními vlády, které se týkají této oblasti (např. vyhláška č. 191/2009 Sb. o podrobnostech výkonu spisové služby, vyhláška č. 194/2009 Sb. o stanovení podrobnosti užívání a provozování informačního systému datových schránek, vyhláška č. 496/2004 Sb. o elektronických podatelnách, atd.)
- s technickými a systémovými normami (ČSN ISO 9001)
- s požadavky uvedenými v Národním standardu pro elektronické systémy spisové služby (Věstník Ministerstva vnitra částka 101/2010 v aktuálním znění)

KDS/KDR

- NSESS Národní standard pro elektronické systémy spisové služby KDS firmy GORDIC plně v souladu s českou legislativou.
- OAIS Open Archival Information SystémArchitektura KDS i KDR jsou založeny na standardu OAIS.

Standardy v oblasti projektového řízení

Zastřešujícím standardem pro řízení životního cyklu projektů je metodika PRINCE2.

Standardy v oblasti bezpečnosti

Při auditní a analytické činnosti se budeme řídit platnými zákony a vyhláškami v aktuálním znění, národními i mezinárodními normami či standardy, doporučovanými pro danou oblast a také etickými zásadami.
Související legislativa, normy a standardy:

- Zákon č. 101/2000 Sb., O ochraně osobních údajů;
- Zákon č. 111/2009 Sb., O základních registrech;
- Zákon č. 227/2000 Sb., O elektronickém podpisu;
- Zákon č. 300/2008 Sb., O elektronických úkonech a autorizované konverzi dokumentů;
- Zákon č. 365/2000 Sb., O informačních systémech veřejné správy v aktuálním znění;
- Vyhláška č. 529/2006 Sb., O dlouhodobém řízení ISVS;
- Zákon č. 106/1999 Sb., O svobodném přístupu k informacím;
- Zákon č. 412/2005 Sb., O ochraně utajovaných informací a o bezpečnostní způsobilosti;
- Zákon č. 499/2004 Sb., O archivnictví a spisové službě;
- ČSN ISO/IEC 27001 – Informační technologie – Bezpečnostní techniky – Systémy managementu bezpečnosti informací – Požadavky;
- pův. ČSN ISO/IEC 17799 – Informační technologie – Soubor postupů pro řízení informační bezpečnosti,
- a ČSN BS 7799-2 – Systém managementu bezpečnosti informací – Specifikace s návodem pro použití;
- ČSN ISO/IEC TR 13335 – Informační technologie – Směrnice pro řízení bezpečnosti IT;
- ISO/IEC 27004 – Information Security Management Measurements;
- ISO/IEC 27005 – Information Security Risk Management;
- BS 25999-1:2006 – Business Continuity Management – Část 1: Code of practice for business continuity management (ČSN BS 25999);
- BS 25999-2 – Business Continuity Management – Část 2: Specification;
- BS 25777:2008 – Information and communications technology continuity management. Code of practice (původně PAS 77:2006, nově ISO/IEC 27031);
- NIST Special Publication 800-34 – Contingency Planning Guide for Federal Information Systems.

Standardy v oblasti poskytování servisních služeb

AutoCont je certifikován podle normy **ISO9001:2001** v oblasti poskytování servisu a služeb.
Všechny procesy související s poskytováním servisu a služeb jsou řízeny v souladu s normami ISO9001:2001 respektive mezinárodně uznávaným rámcem pro správu služeb ITIL. Je tak zajištěna vysoká odbornost poskytovaných služeb a standardizovaná kvalita a stálost jejich provedení.
AutoCont si je vědom požadavků zákazníků a snaží se nabídnout širokou škálu služeb s nejvyšší kvalitou, podpořenou zejména procesním zpracování podpory zákazníků rámcem ITIL potvrzeným certifikátem na normu **ISO 20000:05**, dále pak také týmem technologicky a technicky vyškolených odborníků, kteří svou odbornost mají podloženou certifikáty několika desítek partnerských společností.
Poskytované služby jsou interně nastaveny dle ISO 20000:5 kde základním principem je **Demingův cyklus PDCA** (anglicky: Plan, Do, Check, Act, tedy plánování, provádění, kontrola a akce).
Při zprovozňování a následném běhu služeb tedy plánujeme potřebné zdroje a jejich kapacity, pravidelně měříme a vyhodnocujeme jejich využití a dosažení interně a externě nastavených SLA tak aby zákazníkům byla poskytována požadována kvalita služeb. V případě, že při vyhodnocení zjistíme nedostatky, je ihned zahájen běh opatření, které vedou k nápravě. Nad těmito opatřeními a celým během těchto procesů pak bdí interní manažer kvality.
Společnost AutoCont CZ a.s. získala certifikaci dle normy **ISO/IEC 27001:2005**. Tato norma ověřuje a garantuje, že zpracování informací a jejich zabezpečení odpovídá nejvyšším požadovaným standardům.
Společnost AutoCont CZ a.s. je tak jedna z prvních v ČR, která garantuje kvalitu poskytovaných IT služeb dle normy ISO/IEC 20000 a současně vysokou bezpečnost zpracovávaných informací v souladu s požadavky ISO/IEC 27001. Audit prováděl Elektrotechnický zkušební ústav s.p.

Standardy v oblasti plnění Technologické centrum

Oblast plnění	Komponenta	Technologie	Technologický standard
A - Technologické centrum Jihomoravského kraje			
Infrastruktura Datového centra	Zabezpečení výpadku el. energie - UPS	UPS PW Eaton Blade	EMI – IEC 62040 VFI SS 111 dle IEC EN 62040-3 Ochrana proti přepětí ANSI C62.41, Cat B-3
	Klimatizace	ZDC -Sálová jednotka 23,3kW, HDC - CRV20 In, ZDC - Sálová jednotka 23,3kW	Certifikováno dle EUROVENT Výkon uváděn dle EN 14511:2007 Další: 2006/42/EC; 2004/108/EC; 2006/95/EC; 97/23/EC - Module H
Serverová infrastruktura	Uložení infrastruktury do Racků	HP 642 1075mm Shock Intelligent Rack	Standardní rack 19 palců odpovídající normě EIA-310D Type A
	Blade technologie	HP BladeSystem c7000	ISO 7779 (ECMA 74) ISO 9296 (ECMA 109)
		HP Virtual Connect Flex-10	802.1AB LLDP 802.1Q (VLAN, 1024 maximum, includes Native VLAN support and server side VLAN tag mapping) IEEE 802.2 LLC 802.3ad Link Aggregation IEEE 802.3ae 10Gb Fiber Ethernet IEEE 802.3ak 10Gb CX-4 Ethernet IEEE 802.3aq 10Gb LRM Ethernet SNMP v.1, v.2 IGMP v1, v2, v3
		HP Virtual Connect Fibre Channel	ANCI T11 N_Port ID Virtualization FC-PH Rev. 4.3 FC-PH-2 FC-PH-3 FC-AL Rev 4.6 FC-AL-2 Rev 7.0 FC-FLA FC-GS FC-GS-2 FC-GS-3 FC-FG FC-VI
		HP ProLiant BL685c G7	EMC: Class A CISPR 22:2005 +A1:2005 EN 55022:2006 +A1:2007 EN 55024:1998 +A1:2001 +A2:2003 Safety: EN 60950-1:2006 +A11:2009 IEC 60950-1:2005 EN 62311:2008
Serverová virtualizace	Serverová virtualizace	VMware vSphere 5 Enterprise Plus	VMware Ready – technologický standard pro TAP program (Technology Alliance Partner) – 1300 technologických partnerů. 1600 certifikovaných Serverů 1200 certifikovaných Storage systémů 700 certifikovaných Storage Controllers 400 certifikovaných Network I/O Cards 1400 Softwarových vendorů podporuje technologii VMware Standard SDK and API technical resources
Datová úložiště	Disková pole Tier 0	EFS Tier0 Storage	Fibre channel rozhraní splňuje standardy FC-PH Rev. 4.3 FC-PH-3 FC-AL Rev 4.6 FC-AL-2 Rev 7.0

	Disková pole Tier1 , Tier 2	HP Enterprise Virtual Array P6500	Fibre channel rozhraní splňuje standardy FC-PH Rev. 4.3 FC-PH-3 FC-AL Rev 4.6 FC-AL-2 Rev 7.0 Rozhraní pro disky je standardní SAS2 rozhraní dle INCITS T10
	Garantované uložiště Tier 3	Hitachi HCP 300	Certifikace dle zákona č. 499/2004 Sb., o archivnictví a spisové službě SEC Rule 17a-4, 21CFR Part 11, HIPAA, Sarbanes-Oxley, GoBs, DoD 5015.2, Moreq II Certifikace US SEC 17 CFR 240.17a-4 popř. certifikáty EU dle OAIS - ISO 14721:2003 Přístupové protokoly dle standardů CIFS, NFS, HTTP, HTTPS, WEBDAV, XAM, SMTP, NDMP a REST
Disková virtualizace	Disková virtualizace	FalconStor Software	Fibre channel rozhraní splňuje standardy FC-PH Rev. 4.3 FC-PH-3 FC-AL Rev 4.6 FC-AL-2 Rev 7.0 iSCSI rozhraní je odpovídá definici IETF RFC 3720
Zálohování a obnova dat	Zálohování a obnova	MSL4048 Tape Library	**EMC**: Class A CISPR 22:2005+A1:2005+A2:2006 EN 55022:2006 +A1:2007 EN 55024:1998 +A1:2001 +A2:2003 EN 61000-3-2:2006 +A1:2009 +A2:2009 EN 61000-3-3:2008 FCC CFR 47 Part 15 **Safety:** IEC 60950-1:2005 +A1 EN 60950-1:2006
		HP Data Protector Software	Nástroje využívají následující technologické standardy: OS: HP-UX, Windows, Solaris, Tru64, OpenVMS, NetWare, Linux, AIX Oracle®, Informix, Sybase, MS SQL Server, MS SQL, MS Exchange, MS SharePoint, MS DPM, SAP, SAP DB/MaxDB, Baan IV, Lotus Notes, Lotus Domino, DB2 Clusters: RH & SLES Clusters, Microsoft® Cluster Server, HP MC/Serviceguard, VERITAS Cluster, Zero-downtime backup: HP Business Copy XP/P9000 and Continuous Access XP/P9000, HP Business Copy EVA HP Continuous Access EVA, HP SAN/iQ Snapshots, HP 3PAR Virtual Copy, HP P2000 Snapshots , EMC TimeFinder and EMC SRDF, EMC CLARiiON SnapView-Snapshots and NetApp Snapshots Instant recovery: HP Disk Array XP/P9000, EVA and P4000 iSCSI (SCSI over TCP/IP), FCIP (FC over IP) and iFCP (Internet FC Protocol) Tru64 Cluster, Novell Netware Cluster, OpenVMS Cluster and HP EFS Clustered Gateway HP Tape libraries, StorageTek, ADIC, IBM Java Runtime Environment (JRE) 1.5.0_06 or newer (for example, 1.5.0_07), Netscape Navigator 4.7.x, Netscape7.x, Mozilla 1.7 and Microsoft Internet Explorer 6.0 or later. DDS, DLT, DLT1, Super DLT, QIC/Travan, Magneto-Optical, Mammoth M2, Eliant, IBM 3590 (Magstar), STK 9840, STK 9940, AIT and LTO Ultrium
Bezpečná komunikační infrastruktura	Páteřní přepínače	HP Switches, Routers	Best practices standardy výrobce
		Protokoly založené na obecných standardech skupiny IEEE a jejich RFC	BGP RFC 1771 BGPv4 RFC 1772 Application of the BGP RFC 1965 BGP4 confederations RFC 1997 BGP Communities Attribute RFC 1998 PPP Gandalf FZA Compression Protocol RFC 2385 BGP Session Protection via TCP MD5 RFC 2439 BGP Route Flap Damping RFC 2796 BGP Route Reflection RFC 2858 BGP-4 Multi-Protocol Extensions RFC 2918 Route Refresh Capability RFC 3065 Autonomous System Confederations for BGP RFC 3392 Capabilities Advertisement with BGP-4 RFC 4271 A Border Gateway Protocol 4 (BGP-4) RFC 4272 BGP Security Vulnerabilities Analysis

			RFC 4273 Definitions of Managed Objects for BGP-4 RFC 4274 BGP-4 Protocol Analysis RFC 4275 BGP-4 MIB Implementation Survey RFC 4276 BGP-4 Implementation Report RFC 4277 Experience with the BGP-4 Protocol RFC 4360 BGP Extended Communities Attribute RFC 4456 BGP Route Reflection: An Alternative to Full Mesh Internal BGP (IBGP) RFC 5291 Outbound Route Filtering Capability for BGP-4 RFC 5292 Address-Prefix-Based Outbound Route Filter for BGP-4 Denial of service protection RFC 2267 Network Ingress Filtering Automatic filtering of well-known denial-of-service packets CPU DoS Protection Rate Limiting by ACLs Device management RFC 1157 SNMPv1/v2c RFC 1305 NTPv3 RFC 1902 (SNMPv2) RFC 2271 FrameWork RFC 2579 (SMIv2 Text Conventions) RFC 2580 (SMIv2 Conformance) RFC 2819 (RMON groups Alarm, Event, History and Statistics only) HTTP, SSHv1, and Telnet Multiple Configuration Files Multiple Software Images SSHv1/SSHv2 Secure Shell TACACS/TACACS+ Web UI General protocols IEEE 802.1ad Q-in-Q IEEE 802.1ag Service Layer OAM IEEE 802.1p Priority IEEE 802.1Q VLANs IEEE 802.1s Multiple Spanning Trees IEEE 802.1w Rapid Reconfiguration of Spanning Tree IEEE 802.1X PAE IEEE 802.3ab 1000BASE-T IEEE 802.3ac (VLAN Tagging Extension) IEEE 802.3ad Link Aggregation Control Protocol (LACP) IEEE 802.3ae 10-Gigabit Ethernet IEEE 802.3af Power over Ethernet IEEE 802.3ah Ethernet in First Mile over Point to Point Fiber - EFMF IEEE 802.3at IEEE 802.3u 100BASE-X IEEE 802.3x Flow Control IEEE 802.3z 1000BASE-X RFC 768 UDP RFC 783 TFTP Protocol (revision 2) RFC 791 IP RFC 792 ICMP RFC 793 TCP RFC 826 ARP RFC 854 TELNET RFC 894 IP over Ethernet RFC 903 RARP RFC 906 TFTP Bootstrap RFC 925 Multi-LAN Address Resolution RFC 950 Internet Standard Subnetting Procedure RFC 951 BOOTP RFC 959 File Transfer Protocol (FTP) RFC 1027 Proxy ARP RFC 1035 Domain Implementation and Specification RFC 1042 IP Datagrams RFC 1058 RIPv1 RFC 1142 OSI IS-IS Intra-domain Routing Protocol

			RFC 1195 OSI ISIS for IP and Dual Environments RFC 1213 Management Information Base for Network Management of TCP/IP-based internets RFC 1256 ICMP Router Discovery Protocol (IRDP) RFC 1293 Inverse Address Resolution Protocol RFC 1305 NTPv3 RFC 1350 TFTP Protocol (revision 2) RFC 1393 Traceroute Using an IP Option RFC 1519 CIDR RFC 1531 Dynamic Host Configuration Protocol RFC 1533 DHCP Options and BOOTP Vendor Extensions RFC 1591 DNS (client only) RFC 1624 Incremental Internet Checksum RFC 1701 Generic Routing Encapsulation RFC 1721 RIP-2 Analysis RFC 1723 RIP v2 RFC 1812 IPv4 Routing RFC 2030 Simple Network Time Protocol (SNTP) v4 RFC 2082 RIP-2 MD5 Authentication RFC 2091 Trigger RIP RFC 2131 DHCP RFC 2138 Remote Authentication Dial In User Service (RADIUS) RFC 2236 IGMP Snooping RFC 2338 VRRP RFC 2453 RIPv2 RFC 2644 Directed Broadcast Control RFC 2763 Dynamic Name-to-System ID mapping support RFC 2784 Generic Routing Encapsulation (GRE) RFC 2865 Remote Authentication Dial In User Service (RADIUS) RFC 2966 Domain-wide Prefix Distribution with Two-Level IS-IS RFC 2973 IS-IS Mesh Groups RFC 3022 Traditional IP Network Address Translator (Traditional NAT) RFC 3277 IS-IS Transient Blackhole Avoidance RFC 3567 Intermediate System to Intermediate System (IS-IS) Cryptographic Authentication RFC 3719 Recommendations for Interoperable Networks using Intermediate System to Intermediate System (IS-IS) RFC 3784 ISIS TE support RFC 3786 Extending the Number of IS-IS LSP Fragments Beyond the 256 Limit RFC 3787 Recommendations for Interoperable IP Networks using Intermediate System to Intermediate System (IS-IS) RFC 3847 Restart signaling for IS-IS RFC 4251 The Secure Shell (SSH) Protocol Architecture RFC 4884 Extended ICMP to Support Multi-Part Messages RFC 4941 Privacy Extensions for Stateless Address Autoconfiguration in IPv6 RFC 5130 A Policy Control Mechanism in IS-IS Using Administrative Tags IP multicast RFC 2236 IGMPv2 RFC 2283 Multiprotocol Extensions for BGP-4 RFC 2362 PIM Sparse Mode RFC 3376 IGMPv3 RFC 3446 Anycast Rendezvous Point (RP) mechanism using Protocol Independent Multicast (PIM) and Multicast Source Discovery Protocol (MSDP) RFC 3618 Multicast Source Discovery Protocol (MSDP) RFC 3973 PIM Dense Mode RFC 4541 Considerations for Internet Group Management Protocol (IGMP) and Multicast Listener Discovery (MLD) Snooping Switches RFC 4601 Draft 10 PIM Sparse Mode

			RFC 4604 Using Internet Group Management Protocol Version 3 (IGMPv3) and Multicast Listener Discovery Protocol Version 2 (MLDv2) for Source-Specific Multicast RFC 4605 IGMP/MLD Proxying RFC 4607 Source-Specific Multicast for IP RFC 4610 Anycast-RP Using Protocol Independent Multicast (PIM) RFC 5059 Bootstrap Router (BSR) Mechanism for Protocol Independent Multicast (PIM) IPv6 RFC 1886 DNS Extension for IPv6 RFC 1887 IPv6 Unicast Address Allocation Architecture RFC 1981 IPv6 Path MTU Discovery RFC 2080 RIPng for IPv6 RFC 2081 RIPng Protocol Applicability Statement RFC 2292 Advanced Sockets API for IPv6 RFC 2373 IPv6 Addressing Architecture RFC 2375 IPv6 Multicast Address Assignments RFC 2460 IPv6 Specification RFC 2461 IPv6 Neighbor Discovery RFC 2462 IPv6 Stateless Address Auto-configuration RFC 2463 ICMPv6 RFC 2464 Transmission of IPv6 over Ethernet Networks RFC 2473 Generic Packet Tunneling in IPv6 RFC 2526 Reserved IPv6 Subnet Anycast Addresses RFC 2529 Transmission of IPv6 Packets over IPv4 RFC 2545 Use of MP-BGP-4 for IPv6 RFC 2553 Basic Socket Interface Extensions for IPv6 RFC 2710 Multicast Listener Discovery (MLD) for IPv6 RFC 2740 OSPFv3 for IPv6 RFC 2767 Dual stacks IPv46 & IPv6 RFC 2893 Transition Mechanisms for IPv6 Hosts and Routers RFC 3056 Connection of IPv6 Domains via IPv4 Clouds RFC 3307 IPv6 Multicast Address Allocation RFC 3315 DHCPv6 (client and relay) RFC 3484 Default Address Selection for IPv6 RFC 3513 IPv6 Addressing Architecture RFC 3736 Stateless Dynamic Host Configuration Protocol (DHCP) Service for IPv6 RFC 3810 MLDv2 for IPv6 RFC 4214 Intra-Site Automatic Tunnel Addressing Protocol (ISATAP) RFC 4861 IPv6 Neighbor Discovery RFC 4862 IPv6 Stateless Address Auto-configuration MIBs RFC 1156 (TCP/IP MIB) RFC 1157 A Simple Network Management Protocol (SNMP) RFC 1215 A Convention for Defining Traps for use with the SNMP RFC 1229 Interface MIB Extensions RFC 1493 Bridge MIB RFC 1573 SNMP MIB II RFC 1643 Ethernet MIB RFC 1657 BGP-4 MIB RFC 1724 RIPv2 MIB RFC 1757 Remote Network Monitoring MIB RFC 1850 OSPFv2 MIB RFC 1907 SNMPv2 MIB RFC 2011 SNMPv2 MIB for IP RFC 2012 SNMPv2 MIB for TCP RFC 2013 SNMPv2 MIB for UDP RFC 2096 IP Forwarding Table MIB RFC 2233 Interfaces MIB RFC 2452 IPV6-TCP-MIB RFC 2454 IPV6-UDP-MIB RFC 2465 IPv6 MIB RFC 2466 ICMPv6 MIB RFC 2571 SNMP Framework MIB

			RFC 2572 SNMP-MPD MIB RFC 2573 SNMP-Notification MIB RFC 2573 SNMP-Target MIB RFC 2578 Structure of Management Information Version 2 (SMIv2) RFC 2580 Conformance Statements for SMIv2 RFC 2618 RADIUS Client MIB RFC 2620 RADIUS Accounting MIB RFC 2665 Ethernet-Like-MIB RFC 2668 802.3 MAU MIB RFC 2674 802.1p and IEEE 802.1Q Bridge MIB RFC 2787 VRRP MIB RFC 2819 RMON MIB RFC 2925 Ping MIB RFC 2932IP (Multicast Routing MIB) RFC 2933 IGMP MIB RFC 2934 Protocol Independent Multicast MIB for IPv4 RFC 3414 SNMP-User based-SM MIB RFC 3415 SNMP-View based-ACM MIB RFC 3417 Simple Network Management Protocol (SNMP) over IEEE 802 Networks RFC 3418 MIB for SNMPv3 RFC 3595 Textual Conventions for IPv6 Flow Label RFC 3621 Power Ethernet MIB RFC 3813 MPLS LSR MIB RFC 3814 MPLS FTN MIB RFC 3815 MPLS LDP MIB RFC 3826 AES for SNMP's USM MIB RFC 4133 Entity MIB (Version 3) RFC 4444 Management Information Base for Intermediate System to Intermediate System (IS-IS) MPLS RFC 2205 Resource ReSerVation Protocol RFC 2209 Resource ReSerVation Protocol (RSVP) RFC 2702 Requirements for Traffic Engineering Over MPLS RFC 2858 Multiprotocol Extensions for BGP-4 RFC 2961 RSVP Refresh Overhead Reduction Extensions RFC 3031 Multiprotocol Label Switching Architecture RFC 3032 MPLS Label Stack Encoding RFC 3107 Carrying Label Information in BGP-4 RFC 3209 RSVP-TE: Extensions to RSVP for LSP Tunnels RFC 3212 Constraint-Based LSP Setup using LDP RFC 3479 Fault Tolerance for the Label Distribution Protocol (LDP) RFC 3487 Graceful Restart Mechanism for LDP RFC 3564 Requirements for Support of Differentiated Service-aware MPLS Traffic Engineering RFC 4364 BGP/MPLS IP Virtual Private Networks (VPNs) RFC 4379 Detecting Multi-Protocol Label Switched (MPLS) Data Plane Failures RFC 4447 Pseudowire Setup and Maintenance Using LDP RFC 4448 Encapsulation Methods for Transport of Ethernet over MPLS Networks RFC 4664 Framework for Layer 2 Virtual Private Networks RFC 4665 Service Requirements for Layer 2 Provider Provisioned Virtual Private Networks RFC 4761 Virtual Private LAN Service (VPLS) Using BGP for Auto-Discovery and Signaling RFC 4762 Virtual Private LAN Service (VPLS) Using Label Distribution Protocol (LDP) Signaling RFC 5036 LDP Specification Network management IEEE 802.1AB Link Layer Discovery Protocol (LLDP) RFC 1155 Structure of Management Information RFC 1157 SNMPv1 RFC 1448 Protocol Operations for version 2 of the

			Simple Network Management Protocol (SNMPv2) RFC 2211 Controlled-Load Network RFC 2819 Four groups of RMON: 1 (statistics), 2 (history), 3 (alarm) and 9 (events) RFC 3176 sFlow RFC 3411 SNMP Management Frameworks RFC 3412 SNMPv3 Message Processing RFC 3414 SNMPv3 User-based Security Model (USM) RFC 3415 SNMPv3 View-based Access Control Model VACM) ANSI/TIA-1057 LLDP Media Endpoint Discovery (LLDP-MED) OSPF RFC 1245 OSPF protocol analysis RFC 1246 Experience with OSPF RFC 1765 OSPF Database Overflow RFC 1850 OSPFv2 Management Information Base (MIB), traps RFC 2154 OSPF w/ Digital Signatures (Password, MD-5) RFC 2328 OSPFv2 RFC 2370 OSPF Opaque LSA Option RFC 3101 OSPF NSSA RFC 3137 OSPF Stub Router Advertisement RFC 3623 Graceful OSPF Restart RFC 3630 Traffic Engineering Extensions to OSPFv2 RFC 4061 Benchmarking Basic OSPF Single Router Control Plane Convergence RFC 4062 OSPF Benchmarking Terminology and Concepts RFC 4063 Considerations When Using Basic OSPF Convergence Benchmarks RFC 4222 Prioritized Treatment of Specific OSPF Version 2 Packets and Congestion Avoidance RFC 4577 OSPF as the Provider/Customer Edge Protocol for BGP/MPLS IP Virtual Private Networks (VPNs) RFC 4811 OSPF Out-of-Band LSDB Resynchronization RFC 4812 OSPF Restart Signaling RFC 4813 OSPF Link-Local Signaling RFC 4940 IANA Considerations for OSPF QoS/CoS IEEE 802.1P (CoS) RFC 1349 Type of Service in the Internet Protocol Suite RFC 2211 Specification of the Controlled-Load Network Element Service RFC 2212 Guaranteed Quality of Service RFC 2474 DSCP DiffServ RFC 2475 DiffServ Architecture RFC 2597 DiffServ Assured Forwarding (AF) RFC 2598 DiffServ Expedited Forwarding (EF) Security IEEE 802.1X Port Based Network Access Control RFC 1321 The MD5 Message-Digest Algorithm RFC 1334 PPP Authentication Protocols (PAP) RFC 1492 TACACS+ RFC 1994 PPP Challenge Handshake Authentication Protocol (CHAP) RFC 2082 RIP-2 MD5 Authentication RFC 2104 Keyed-Hashing for Message Authentication RFC 2408 Internet Security Association and Key Management Protocol (ISAKMP) RFC 2409 The Internet Key Exchange (IKE) RFC 2716 PPP EAP TLS Authentication Protocol RFC 2865 RADIUS Authentication RFC 2866 RADIUS Accounting RFC 2867 RADIUS Accounting Modifications for Tunnel Protocol Support RFC 2868 RADIUS Attributes for Tunnel Protocol Support RFC 2869 RADIUS Extensions

			Access Control Lists (ACLs) Guest VLAN for 802.1x MAC Authentication Port Security SSHv1/SSHv2 Secure Shell VPN RFC 2403 - HMAC-MD5-96 RFC 2404 - HMAC-SHA1-96 RFC 2405 - DES-CBC Cipher algorithm RFC 2407 - Domain of interpretation RFC 2547 BGP/MPLS VPNs RFC 2917 A Core MPLS IP VPN Architecture RFC 3947 - Negotiation of NAT-Traversal in the IKE RFC 4302 - IP Authentication Header (AH) RFC 4303 - IP Encapsulating Security Payload (ESP) IPsec RFC 1828 IP Authentication using Keyed MD5 RFC 1829 The ESP DES-CBC Transform RFC 2085 HMAC-MD5 IP Authentication with Replay Prevention RFC 2401 IP Security Architecture RFC 2402 IP Authentication Header RFC 2406 IP Encapsulating Security Payload RFC 2410 - The NULL Encryption Algorithm and its use with IPsec RFC 2411 IP Security Document Roadmap
	SAN přepínače	HP 8/40 SAN Switch	Fibre Channel Standardy FC-AL-2 INCITS 332: 1999 FC-GS-5 ANSI INCITS 427:2006 FC-GS-4 ANSI INCITS 387: 2004 FC-IFR revision 1 FC-SW-4 INCITS 418:2006 FC-SW-3 INCITS 384: 2004 FC-VI INCITS 357: 2002 FC-TAPE INCITS TR-24: 1999 FC-DA INCITS TR-36: 2004 FC-FLA INCITS TR-20: 1998 FC-PLDA INCIT S TR-19: 1998 FC-MI-2 ANSI/INCITS TR-39-2005 FC-PI INCITS 352: 2002 FC-PI-2 INCITS 404: 2005 FC-FS-2 ANSI/INCITS 424:2006 FC-FS INCITS 373: 2003 FC-LS revision 1.51 FC-BB-3 INCITS 414: 2006 FC-BB-2 INCITS 372: 2003 FC-SB-3 INCITS 374: 2003 INCITS 374: 2001)
	Systém pro dělení zátěže na servery (loadbalancery)	Load-Balancing F5 BIG-IP 3900	Best practices standardy výrobce
		Podpora aplikací	Microsoft .NET Framework Active Directory Federation Services Application Virtualization BizTalk Server Commerce Server Exchange Server Forefront family ··Forefront management products ··Forefront platform technologies ··Forefront protection and access products Lync Server Opalis Outlook Web App Project Server Search Server SharePoint Server SQL Azure SQL Server System Center family ··System Center Configuration Manager ··System Center Data Protection Manager ··System Center Essentials ··System Center Mobile Device Manager

			··System Center Operations Manager ··System Center Service Manager ··System Center Virtual Machine Manager Team Foundation Server Visual Studio Virtual Server Windows Azure Windows Server family ··Windows Server Hyper-V ··Windows Server Remote Desktop Services ··Windows Server Update Services Windows Storage Server IBM FileNet Lotus Domino, iNotes Lotus Sametime Tivoli Monitoring Tivoli OMNIbus Tivoli Orchestrator Tivoli Service Automation Manager WebSphere Server Oracle Applications ··Beehive ··E-Business Suite ··Enterprise Manager ··Fusion Applications ··Hyperion ··JD Edwards EnterpriseOne ··PeopleSoft Enterprise ··Siebel Middleware ··Access Manager ··Coherence ··Identity Management ··SOA ··WebCenter ··WebLogic Server Database ··Database Firewall ··Data Guard ··GoldenGate ··Streams ··Real Application Clusters (RAC) ··Recovery Manager SAP ERP NetWeaver Portal Adobe Acrobat Connect Pro Flash Media Server InDesign ColdFusion Other CA eHealth E-Business Suite ANGEL Learning Blackboard SunGard IntelliSUITE SunGard Higher Education
		Standardy implementace	F5 Dynamic services model
	Management síť	HP 3100-48 v2	Best practices standardy výrobce
		Protokoly založené na obecných standardech skupiny IEEE a jejich RFC	General protocols IEEE 802.1ad Q-in-Q IEEE 802.1ag Service Layer OAM IEEE 802.1D MAC Bridges IEEE 802.1p Priority IEEE 802.1Q VLANs IEEE 802.1s (MSTP) IEEE 802.1w Rapid Reconfiguration of Spanning Tree IEEE 802.1X PAE IEEE 802.3ad Link Aggregation Control Protocol (LACP) IEEE 802.3af Power over Ethernet

			IEEE 802.3i 10BASE-T IEEE 802.3u 100BASE-X IEEE 802.3x Flow Control IEEE 802.3z 1000BASE-X RFC 768 UDP RFC 783 TFTP Protocol (revision 2) RFC 791 IP RFC 792 ICMP RFC 793 TCP RFC 826 ARP RFC 854 TELNET RFC 951 BOOTP RFC 959 File Transfer Protocol (FTP) MIBs IEEE 8021-PAE-MIB IEEE 8023-LAG-MIB RFC 1213 MIB II RFC 1493 Bridge MIB RFC 2011 SNMPv2 MIB for IP RFC 2013 SNMPv2 MIB for UDP RFC 2233 Interface MIB RFC 2273 SNMP-NOTIFICATION-MIB RFC 2571 SNMP Framework MIB RFC 2572 SNMP-MPD MIB RFC 2573 SNMP-Notification MIB RFC 2618 RADIUS Authentication Client MIB RFC 2620 RADIUS Accounting Client MIB RFC 2665 Ethernet-Like-MIB RFC 2674 802.1p and IEEE 802.1Q Bridge MIB RFC 2819 RMON MIB RFC 2925 Ping MIB RFC 3414 SNMP-User based-SM MIB RFC 3418 MIB for SNMPv3 RFC 3621 Power Ethernet MIB RFC 3826 AES for SNMP's USM MIB RFC 4133 Entity MIB (Version 3) LLDP-EXT-DOT1-MIB LLDP-EXT-DOT3-MIB LLDP-MIB Network management IEEE 802.1AB Link Layer Discovery Protocol (LLDP) RFC 2819 Four groups of RMON: 1 (statistics), 2 (history), 3 (alarm) and 9 (events) ANSI/TIA-1057 LLDP Media Endpoint Discovery (LLDP-MED) SNMPv1/v2c/v3 QoS/CoS IEEE 802.1P (CoS) RFC 2474 DSCP DiffServ
	Hraniční routery pro připojení do Internetu	HP 6602	Best practices standardy výrobce
		Protokoly založené na obecných standardech skupiny IEEE a jejich RFC	BGP RFC 1267 Border Gateway Protocol 3 (BGP-3) RFC 1657 Definitions of Managed Objects for BGPv4 RFC 1771 BGPv4 RFC 1772 Application of the BGP RFC 1773 Experience with the BGP-4 Protocol RFC 1774 BGP-4 Protocol Analysis RFC 1965 BGP4 confederations RFC 1997 BGP Communities Attribute RFC 1998 PPP Gandalf FZA Compression Protocol RFC 2385 BGP Session Protection via TCP MD5 RFC 2439 BGP Route Flap Damping RFC 2796 BGP Route Reflection RFC 2842 Capability Advertisement with BGP-4 RFC 2858 BGP-4 Multi-Protocol Extensions RFC 2918 Route Refresh Capability Denial of service protection CPU DoS Protection Rate Limiting by ACLs Device management RFC 1155 Structure and Mgmt Information (SMIv1)

			RFC 1157 SNMPv1/v2c RFC 1305 NTPv3 RFC 1901 (Community based SNMPv2) RFC 1901-1907 SNMPv2c, SMIv2 and Revised MIB-II RFC 1902 (SNMPv2) RFC 1908 (SNMP v1/2 Coexistence) RFC 1945 Hypertext Transfer Protocol -- HTTP/1.0 RFC 2068 Hypertext Transfer Protocol -- HTTP/1.1 RFC 2271 FrameWork RFC 2452 MIB for TCP6 RFC 2454 MIB for UDP6 RFC 2573 (SNMPv3 Applications) RFC 2576 (Coexistence between SNMP V1, V2, V3) RFC 2578-2580 SMIv2 RFC 2579 (SMIv2 Text Conventions) RFC 2580 (SMIv2 Conformance) RFC 2819 (RMON groups Alarm, Event, History and Statistics only) RFC 2819 RMON RFC 3410 (Management Framework) RFC 3416 (SNMP Protocol Operations v2) RFC 3417 (SNMP Transport Mappings) Multiple Configuration Files Multiple Software Images SNMP v3 and RMON RFC support SSHv1/SSHv2 Secure Shell TACACS/TACACS+ General protocols IEEE 802.1ad Q-in-Q IEEE 802.1ad Q-in-Q IEEE 802.1ag Service Layer OAM IEEE 802.1ah Provider Backbone Bridges IEEE 802.1AX-2008 Link Aggregation IEEE 802.1D MAC Bridges IEEE 802.1p Priority IEEE 802.1Q (GVRP) IEEE 802.1Q VLANs IEEE 802.1s (MSTP) IEEE 802.1s Multiple Spanning Trees IEEE 802.1v VLAN classification by Protocol and Port IEEE 802.1w Rapid Reconfiguration of Spanning Tree IEEE 802.1X PAE IEEE 802.3 Type 10BASE-T IEEE 802.3ab 1000BASE-T IEEE 802.3ac (VLAN Tagging Extension) IEEE 802.3ad Link Aggregation (LAG) IEEE 802.3ad Link Aggregation Control Protocol (LACP) IEEE 802.3ae 10-Gigabit Ethernet IEEE 802.3ag Ethernet OAM IEEE 802.3ah Ethernet in First Mile over Point to Point Fiber - EFMF IEEE 802.3i 10BASE-T IEEE 802.3u 100BASE-X IEEE 802.3x Flow Control IEEE 802.3z 1000BASE-X RFC 768 UDP RFC 783 TFTP Protocol (revision 2) RFC 791 IP RFC 792 ICMP RFC 793 TCP RFC 826 ARP RFC 854 TELNET RFC 855 Telnet Option Specification RFC 856 TELNET RFC 857 Telnet Echo Option RFC 858 Telnet Suppress Go Ahead Option RFC 894 IP over Ethernet RFC 896 Congestion Control in IP/TCP Internetworks RFC 906 TFTP Bootstrap RFC 925 Multi-LAN Address Resolution RFC 950 Internet Standard Subnetting Procedure RFC 951 BOOTP

			RFC 959 File Transfer Protocol (FTP) RFC 1006 ISO transport services on top of the TCP: Version 3 RFC 1027 Proxy ARP RFC 1034 Domain Concepts and Facilities RFC 1035 Domain Implementation and Specification RFC 1042 IP Datagrams RFC 1058 RIPv1 RFC 1071 Computing the Internet Checksum RFC 1091 Telnet Terminal-Type Option RFC 1093 NSFNET routing architecture RFC 1122 Host Requirements RFC 1141 Incremental updating of the Internet checksum RFC 1142 OSI IS-IS Intra-domain Routing Protocol RFC 1144 Compressing TCP/IP headers for low-speed serial links RFC 1171 Point-to-Point Protocol for the transmission of multi-protocol datagrams over Point-to-Point links RFC 1195 OSI ISIS for IP and Dual Environments RFC 1213 Management Information Base for Network Management of TCP/IP-based internets RFC 1253 (OSPF v2) RFC 1256 ICMP Router Discovery Protocol (IRDP) RFC 1293 Inverse Address Resolution Protocol RFC 1305 NTPv3 RFC 1315 Management Information Base for Frame Relay DTEs RFC 1321 The MD5 Message-Digest Algorithm RFC 1332 The PPP Internet Protocol Control Protocol (IPCP) RFC 1333 PPP Link Quality Monitoring RFC 1334 PPP Authentication Protocols (PAP) RFC 1334 PPP Authentication Protocols (PAP) RFC 1349 Type of Service RFC 1350 TFTP Protocol (revision 2) RFC 1377 The PPP OSI Network Layer Control Protocol (OSINLCP) RFC 1381 SNMP MIB Extension for X.25 LAPB RFC 1389 RIPv2 MIB Extension RFC 1471 The Definitions of Managed Objects for the Link Control Protocol of the Point-to-Point Protocol RFC 1472 The Definitions of Managed Objects for the Security Protocols of the Point-to-Point Protocol RFC 1490 Multiprotocol Interconnect over Frame Relay RFC 1519 CIDR RFC 1531 Dynamic Host Configuration Protocol RFC 1533 DHCP Options and BOOTP Vendor Extensions RFC 1534 DHCP/BOOTP Interoperation RFC 1541 DHCP RFC 1542 BOOTP Extensions RFC 1542 Clarifications and Extensions for the Bootstrap Protocol RFC 1552 The PPP Internetworking Packet Exchange Control Protocol (IPXCP) RFC 1577 Classical IP and ARP over ATM RFC 1631 NAT RFC 1638 PPP Bridging Control Protocol (BCP) RFC 1661 The Point-to-Point Protocol (PPP) RFC 1662 PPP in HDLC-like Framing RFC 1695 Definitions of Managed Objects for ATM Management Version 8.0 using SMIv2 RFC 1700 Assigned Numbers RFC 1701 Generic Routing Encapsulation RFC 1702 Generic Routing Encapsulation over IPv4 networks RFC 1721 RIP-2 Analysis RFC 1722 RIP-2 Applicability RFC 1723 RIP v2 RFC 1812 IPv4 Routing RFC 1829 The ESP DES-CBC Transform RFC 1877 PPP Internet Protocol Control Protocol Extensions for Name Server Addresses RFC 1944 Benchmarking Methodology for Network Interconnect Devices RFC 1945 Hypertext Transfer Protocol -- HTTP/1.0 RFC 1973 PPP in Frame Relay RFC 1974 PPP Stac LZS Compression Protocol RFC 1981 Path MTU Discovery for IP version 6 RFC 1990 The PPP Multilink Protocol (MP) RFC 1994 PPP Challenge Handshake Authentication Protocol (CHAP) RFC 2082 RIP-2 MD5 Authentication

			RFC 2091 Trigger RIP RFC 2104 HMAC: Keyed-Hashing for Message Authentication RFC 2131 DHCP RFC 2132 DHCP Options and BOOTP Vendor Extensions RFC 2138 Remote Authentication Dial In User Service (RADIUS) RFC 2205 Resource ReSerVation Protocol (RSVP) - Version 1 Functional Specification RFC 2209 Resource ReSerVation Protocol (RSVP) -- Version 1 Message Processing Rules RFC 2236 IGMP Snooping RFC 2246 The TLS Protocol Version 1.0 RFC 2251 Lightweight Directory Access Protocol (v3) RFC 2252 Lightweight Directory Access Protocol (v3): Attribute Syntax Definitions RFC 2280 Routing Policy Specification Language (RPSL) RFC 2283 MBGP RFC 2284 EAP over LAN RFC 2338 VRRP RFC 2338 VRRP (Premium Edge License) RFC 2364 PPP Over AAL5 RFC 2374 An Aggregatable Global Unicast Address Format RFC 2451 The ESP CBC-Mode Cipher Algorithms RFC 2453 RIPv2 RFC 2510 Internet X.509 Public Key Infrastructure Certificate Management Protocols RFC 2511 Internet X.509 Certificate Request Message Format RFC 2516 A Method for Transmitting PPP Over Ethernet (PPPoE) RFC 2529 Transmission of IPv6 over IPv4 Domains without Explicit Tunnels RFC 2616 HTTP Compatibility v1.1 RFC 2622 Routing Policy Specification Language (RPSL) RFC 2644 Directed Broadcast Control RFC 2661 L2TP RFC 2663 NAT Terminology and Considerations RFC 2684 Multiprotocol Encapsulation over ATM Adaptation Layer 5 RFC 2694 DNS extensions to Network Address Translators (DNS_ALG) RFC 2702 Requirements for Traffic Engineering Over MPLS RFC 2716 PPP EAP TLS Authentication Protocol RFC 2747 RSVP Cryptographic Authentication RFC 2763 Dynamic Name-to-System ID mapping support RFC 2765 Stateless IP/ICMP Translation Algorithm (SIIT) RFC 2766 Network Address Translation - Protocol Translation (NAT-PT) RFC 2767 Dual Stacks IPv4 & IPv6 RFC 2784 Generic Routing Encapsulation (GRE) RFC 2787 Definitions of Managed Objects for VRRP RFC 2865 Remote Authentication Dial In User Service (RADIUS) RFC 2866 RADIUS Accounting RFC 2868 RADIUS Attributes for Tunnel Protocol Support RFC 2869 RADIUS Extensions RFC 2961 RSVP Refresh Overhead Reduction Extensions RFC 2966 Domain-wide Prefix Distribution with Two-Level IS-IS RFC 2973 IS-IS Mesh Groups RFC 2993 Architectural Implications of NAT RFC 3022 Traditional IP Network Address Translator (Traditional NAT) RFC 3027 Protocol Complications with the IP Network Address Translator RFC 3031 Multiprotocol Label Switching Architecture RFC 3032 MPLS Label Stack Encoding RFC 3036 LDP Specification RFC 3046 DHCP Relay Agent Information Option RFC 3063 MPLS Loop Prevention Mechanism RFC 3065 Support AS confederation RFC 3137 OSPF Stub Router Advertisement RFC 3209 RSVP-TE Extensions to RSVP for LSP Tunnels RFC 3210 Applicability Statement for Extensions to RSVP for LSP-Tunnels RFC 3212 Constraint-Based LSP setup using LDP (CR-LDP) RFC 3214 LSP Modification Using CR-LDP RFC 3215 LDP State Machine RFC 3246 Expedited Forwarding PHB RFC 3268 Advanced Encryption Standard (AES) Ciphersuites for

			Transport Layer Security (TLS) RFC 3277 IS-IS Transient Blackhole Avoidance RFC 3279 Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile RFC 3280 Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile RFC 3392 Support BGP capabilities advertisement RFC 3410 Applicability Statements for SNMP RFC 3416 Protocol Operations for SNMP RFC 3417 Transport Mappings for the Simple Network Management Protocol (SNMP) RFC 3479 Fault Tolerance for the Label Distribution Protocol (LDP) RFC 3487 Graceful Restart Mechanism for LDP RFC 3509 OSPF ABR Behavior RFC 3526 More Modular Exponential (MODP) Diffie-Hellman groups for Internet Key Exchange (IKE) RFC 3564 Requirements for Support of Differentiated Services-aware MPLS Traffic Engineering RFC 3567 Intermediate System to Intermediate System (IS-IS) Cryptographic Authentication RFC 3602 The AES-CBC Cipher Algorithm and Its Use with IPsec RFC 3619 Ethernet Automatic Protection Switching (EAPS) RFC 3623 Graceful OSPF Restart RFC 3704 Unicast Reverse Path Forwarding (URPF) RFC 3706 A Traffic-Based Method of Detecting Dead Internet Key Exchange (IKE) Peers RFC 3768 VRRP RFC 3768 VRRP RFC 3768 VRRP (Premium Edge License) RFC 3784 ISIS TE support RFC 3786 Extending the Number of IS-IS LSP Fragments Beyond the 256 Limit RFC 3811 Definitions of Textual Conventions (TCs) for Multiprotocol Label Switching (MPLS) Management RFC 3812 Multiprotocol Label Switching (MPLS) Traffic Engineering (TE) Management Information Base (MIB) RFC 3847 Restart signaling for IS-IS RFC 4213 Basic IPv6 Transition Mechanisms IP Ping IP multicast RFC 1112 IGMP RFC 2236 IGMPv2 RFC 2283 Multiprotocol Extensions for BGP-4 RFC 2362 PIM Sparse Mode RFC 2362 PIM Sparse Mode (Premium Edge License) RFC 2362 PIM Sparse Mode RFC 2934 Protocol Independent Multicast MIB for IPv4 RFC 3376 IGMPv3 RFC 3376 IGMPv3 (host joins only) RFC 3569 An Overview of Source-Specific Multicast (SSM) RFC 3618 Multicast Source Discovery Protocol (MSDP) RFC 3973 Draft 2 PIM Dense Mode RFC 3973 Draft 2 PIM Dense Mode RFC 3973 PIM Dense Mode RFC 3973 PIM Dense Mode (Premium Edge License) RFC 3973 PIM Dense Mode RFC 4601 Draft 10 PIM Sparse Mode RFC 4601 Draft 10 PIM Sparse Mode RFC 4605 IGMP/MLD Proxying IPv6 RFC 1350 TFTP RFC 1881 IPv6 Address Allocation Management RFC 1886 DNS Extension for IPv6 RFC 1887 IPv6 Unicast Address Allocation Architecture RFC 1981 IPv6 Path MTU Discovery RFC 2080 RIPng for IPv6 RFC 2292 Advanced Sockets API for IPv6 RFC 2373 IPv6 Addressing Architecture RFC 2375 IPv6 Multicast Address Assignments

			RFC 2460 IPv6 Specification RFC 2461 IPv6 Neighbor Discovery RFC 2462 IPv6 Stateless Address Auto-configuration RFC 2463 ICMPv6 RFC 2464 Transmission of IPv6 over Ethernet Networks RFC 2472 IP Version 6 over PPP RFC 2473 Generic Packet Tunneling in IPv6 RFC 2475 IPv6 DiffServ Architecture RFC 2529 Transmission of IPv6 Packets over IPv4 RFC 2545 Use of MP-BGP-4 for IPv6 RFC 2553 Basic Socket Interface Extensions for IPv6 RFC 2710 Multicast Listener Discovery (MLD) for IPv6 RFC 2711 IPv6 Router Alert Option RFC 2740 OSPFv3 for IPv6 RFC 2893 Transition Mechanisms for IPv6 Hosts and Routers RFC 2925 Definitions of Managed Objects for Remote Ping, Traceroute, and Lookup Operations (Ping only) RFC 2925 Remote Operations MIB (Ping only) RFC 3056 Connection of IPv6 Domains via IPv4 Clouds RFC 3162 RADIUS and IPv6 RFC 3306 Unicast-Prefix-based IPv6 Multicast Addresses RFC 3307 IPv6 Multicast Address Allocation RFC 3315 DHCPv6 (client and relay) RFC 3315 DHCPv6 (client only) RFC 3363 DNS support RFC 3484 Default Address Selection for IPv6 RFC 3493 Basic Socket Interface Extensions for IPv6 RFC 3513 IPv6 Addressing Architecture RFC 3542 Advanced Sockets API for IPv6 RFC 3587 IPv6 Global Unicast Address Format RFC 3596 DNS Extension for IPv6 RFC 3810 MLDv2 (host joins only) RFC 3810 MLDv2 for IPv6 RFC 3810 Multicast Listener Discovery Version 2 (MLDv2) for IPv6 RFC 4022 MIB for TCP RFC 4113 MIB for UDP RFC 4251 SSHv6 Architecture RFC 4252 SSHv6 Authentication RFC 4252 SSHv6 Transport Layer RFC 4253 SSHv6 Transport Layer RFC 4254 SSHv6 Connection RFC 4291 IP Version 6 Addressing Architecture RFC 4293 MIB for IP RFC 4419 Key Exchange for SSH RFC 4443 ICMPv6 RFC 4541 IGMP & MLD Snooping Switch RFC 4861 IPv6 Neighbor Discovery RFC 4862 IPv6 Stateless Address Auto-configuration RFC 5095 Deprecation of Type 0 Routing Headers in IPv6 RFC 5340 OSPF for IPv6 RFC 5340 OSPFv3 for IPv6 RFC 5722 Handling of Overlapping IPv6 Fragments MIBs IEEE 8021-PAE-MIB IEEE 8023-LAG-MIB RFC 1156 (TCP/IP MIB) RFC 1212 Concise MIB Definitions RFC 1213 MIB II RFC 1229 Interface MIB Extensions RFC 1286 Bridge MIB RFC 1493 Bridge MIB RFC 1573 SNMP MIB II RFC 1643 Ethernet MIB RFC 1650 Ethernet-Like MIB RFC 1657 BGP-4 MIB RFC 1724 RIPv2 MIB RFC 1757 Remote Network Monitoring MIB RFC 1850 OSPFv2 MIB RFC 1907 SNMPv2 MIB RFC 2011 SNMPv2 MIB for IP RFC 2012 SNMPv2 MIB for TCP RFC 2013 SNMPv2 MIB for UDP RFC 2021 RMONv2 MIB RFC 2096 IP Forwarding Table MIB RFC 2233 Interface MIB

			RFC 2233 Interfaces MIB RFC 2273 SNMP-NOTIFICATION-MIB RFC 2452 IPV6-TCP-MIB RFC 2454 IPV6-UDP-MIB RFC 2465 IPv6 MIB RFC 2466 ICMPv6 MIB RFC 2571 SNMP Framework MIB RFC 2572 SNMP-MPD MIB RFC 2574 SNMP USM MIB RFC 2618 RADIUS Client MIB RFC 2620 RADIUS Accounting MIB RFC 2665 Ethernet-Like-MIB RFC 2668 802.3 MAU MIB RFC 2674 802.1p and IEEE 802.1Q Bridge MIB RFC 2688 MAU-MIB RFC 2737 Entity MIB (Version 2) RFC 2787 VRRP MIB RFC 2819 RMON MIB RFC 2863 The Interfaces Group MIB RFC 2925 Ping MIB RFC 2932IP (Multicast Routing MIB) RFC 2933 IGMP MIB RFC 3273 HC-RMON MIB RFC 3414 SNMP-User based-SM MIB RFC 3415 SNMP-View based-ACM MIB RFC 3418 MIB for SNMPv3 RFC 3621 Power Ethernet MIB RFC 3813 MPLS LSR MIB RFC 3814 MPLS FTN MIB RFC 3815 MPLS LDP MIB RFC 3826 AES for SNMP's USM MIB RFC 4113 UDP MIB RFC 4133 Entity MIB (Version 3) RFC 4221 MPLS FTN MIB LLDP-EXT-DOT1-MIB LLDP-EXT-DOT3-MIB LLDP-MIB Network management IEEE 802.1AB Link Layer Discovery Protocol (LLDP) IEEE 802.1D (STP) RFC 1098 A Simple Network Management Protocol (SNMP) RFC 1155 Structure of Management Information RFC 1157 SNMPv1 RFC 1215 SNMP Generic traps RFC 1757 RMON 4 groups: Stats, History, Alarms and Events RFC 1901 SNMPv2 Introduction RFC 1902 SNMPv2 Structure RFC 1903 SNMPv2 Textual Conventions RFC 1904 SNMPv2 Conformance RFC 1905 SNMPv2 Protocol Operations RFC 1906 SNMPv2 Transport Mappings RFC 1918 Private Internet Address Allocation RFC 2272 SNMPv3 Management Protocol RFC 2273 SNMPv3 Applications RFC 2274 USM for SNMPv3 RFC 2275 VACM for SNMPv3 RFC 2570 SNMPv3 Overview RFC 2571 SNMP Management Frameworks RFC 2572 SNMPv3 Message Processing RFC 2573 SNMPv3 Applications RFC 2574 SNMPv3 User-based Security Model (USM) RFC 2575 SNMPv3 View-based Access Control Model (VACM) RFC 2575 VACM for SNMP RFC 2576 Coexistence between SNMP versions RFC 2578 SMIv2 RFC 2581 TCP6 RFC 2819 Four groups of RMON: 1 (statistics), 2 (history), 3 (alarm) and 9 (events) RFC 3164 BSD syslog Protocol RFC 3176 sFlow RFC 3411 SNMP Management Frameworks

			RFC 3412 SNMPv3 Message Processing RFC 3414 SNMPv3 User-based Security Model (USM) RFC 3415 SNMPv3 View-based Access Control Model VACM) ANSI/TIA-1057 LLDP Media Endpoint Discovery (LLDP-MED) SNMPv1/v2 SNMPv1/v2c SNMPv1/v2c (read only) SNMPv1/v2c/v3 OSPF RFC 1245 OSPF protocol analysis RFC 1246 Experience with OSPF RFC 1253 OSPFv2 MIB RFC 1583 OSPFv2 RFC 1587 OSPF NSSA RFC 1745 OSPF Interactions RFC 1765 OSPF Database Overflow RFC 1850 OSPFv2 Management Information Base (MIB), traps RFC 2178 OSPFv2 RFC 2328 OSPFv2 RFC 2328 OSPFv2 RFC 2328 OSPFv2 (Premium Edge License) RFC 2370 OSPF Opaque LSA Option RFC 3101 OSPF NSSA RFC 3623 Graceful OSPF Restart RFC 5340 OSPF for IPv6 RFC 5340 OSPFv3 for IPv6 QoS/CoS IEEE 802.1P (CoS) RFC 2474 DiffServ Precedence, including 8 queues/port RFC 2474 DiffServ precedence, with 4 queues per port RFC 2474 DS Field in the IPv4 and IPv6 Headers RFC 2474 DSCP DiffServ RFC 2474, with 4 queues per port RFC 2475 DiffServ Architecture RFC 2597 DiffServ Assured Forwarding (AF) RFC 2597 DiffServ Assured Forwarding (AF)- partial support RFC 2598 DiffServ Expedited Forwarding (EF) Ingress Rate Limiting Security IEEE 802.1X Port Based Network Access Control RFC 1321 The MD5 Message-Digest Algorithm RFC 1492 TACACS+ RFC 2082 RIP-2 MD5 Authentication RFC 2104 Keyed-Hashing for Message Authentication RFC 2138 RADIUS Authentication RFC 2139 RADIUS Accounting RFC 2209 RSVP-Message Processing RFC 2246 Transport Layer Security (TLS) RFC 2459 Internet X.509 Public Key Infrastructure Certificate and CRL Profile RFC 2548 Microsoft Vendor-specific RADIUS Attributes RFC 2716 PPP EAP TLS Authentication Protocol RFC 2818 HTTP Over TLS RFC 2865 RADIUS (client only) RFC 2865 RADIUS Authentication RFC 2866 RADIUS Accounting RFC 2867 RADIUS Accounting Modifications for Tunnel Protocol Support RFC 2868 RADIUS Attributes for Tunnel Protocol Support RFC 2869 RADIUS Extensions RFC 3567 Intermediate System (IS) to IS Cryptographic Authentication RFC 3576 Dynamic Authorization Extensions to

			RADIUS RFC 3579 RADIUS Support For Extensible Authentication Protocol (EAP) RFC 3580 IEEE 802.1X RADIUS Access Control Lists (ACLs) Guest VLAN for 802.1x MAC Authentication Port Security Secure Sockets Layer (SSL) SSHv1 Secure Shell SSHv1.5 Secure Shell SSHv1/SSHv2 Secure Shell SSHv2 Secure Shell VPN RFC 2403 - HMAC-MD5-96 RFC 2404 - HMAC-SHA1-96 RFC 2405 - DES-CBC Cipher algorithm RFC 2407 - Domain of interpretation RFC 2547 BGP/MPLS VPNs RFC 2764 A Framework for IP Based Virtual Private Networks RFC 2796 BGP Route Reflection - An Alternative to Full Mesh IBGP RFC 2842 Capabilities Advertisement with BGP-4 RFC 2858 Multiprotocol Extensions for BGP-4 RFC 2917 A Core MPLS IP VPN Architecture RFC 2918 Route Refresh Capability for BGP-4 RFC 3107 Carrying Label Information in BGP-4 RFC 4301 - Security Architecture for the Internet Protocol RFC 4302 - IP Authentication Header (AH) RFC 4303 - IP Encapsulating Security Payload (ESP) RFC 4305 - Cryptographic Algorithm Implementation Requirements for ESP and AH IPsec RFC 1828 IP Authentication using Keyed MD5 RFC 2401 IP Security Architecture RFC 2402 IP Authentication Header RFC 2406 IP Encapsulating Security Payload RFC 2407 - Domain of interpretation RFC 2408 - Internet Security Association and Key Management Protocol (ISAKMP) RFC 2409 - The Internet Key Exchange RFC 2410 - The NULL Encryption Algorithm and its use with IPsec RFC 2411 IP Security Document Roadmap RFC 2412 – OAKLEY RFC 2865 - Remote Authentication Dial In User Service (RADIUS) IKEv1 RFC 2865 - Remote Authentication Dial In User Service (RADIUS) RFC 3748 - Extensible Authentication Protocol (EAP)
	Systém IDS/IPS	HP Tippingpoint S1200N	Best practices standardy výrobce
		Protokoly založené na obecných standardech skupiny IEEE a jejich RFC	IEEE 802.3i 10BASE-T IEEE 802.3u 100BASE-X IEEE 802.3x Flow Control IEEE 802.3z 1000BASE-X RFC 768 UDP RFC 783 TFTP Protocol (revision 2) RFC 791 IP RFC 792 ICMP RFC 793 TCP RFC 826 ARP RFC 854 TELNET RFC 855 Telnet Option Specification RFC 856 TELNET RFC 857 Telnet Echo Option RFC 3031 Multiprotocol Label Switching Architecture RFC 1157 SNMPv1/v2c RFC 2236 IGMPv2 RFC 2362 PIM Sparse Mode RFC 3376 IGMPv3

			RFC 3446 Anycast Rendezvous Point (RP) mechanism using Protocol Independent Multicast (PIM) and Multicast Source Discovery Protocol (MSDP) RFC 3618 Multicast Source Discovery Protocol (MSDP) RFC 3973 PIM Dense Mode RFC 4541 Considerations for Internet Group Management Protocol (IGMP) and Multicast Listener
	Systém firewallové ochrany	Firewall - Kernun FW	Certifikát NBÚ ČR o bezpečnostní způsobilosti Vývoj i podpora Kernun FW+ se řídí mezinárodními certifikáty ČSN EN ISO 9001:2009 a ČSN ISO/IEC 27001:2006 certifikačního orgánu TÜV.
Management a monitoring	Network management systém a Centrální management portál	HP NNM, NA	Nástroje využívají následující technologické standardy: Komunikace a discovery: primární protokol TCPIP, nad ním discovery v souladu se SNMP v1,v2,v2c,v3, WMI, SSH Integrace: Web services, SNMP, CLI
		HP NA, HP iSPI	Definované security a config reporty podle doporučení : ITIL, PCI, HIPAA