# Technická specifikace – Část 5 Aktivita 1 Realizace systému pro řízení identit

Obsah

[1) Popis požadavků na řešení a specifické funkcionality systému pro správu identit 3](#_Toc197345059)

# Popis požadavků na řešení a specifické funkcionality systému pro správu identit

|  |  |  |
| --- | --- | --- |
| **Část** | **Parametr** | **Popis povinného parametru** |
| **Správa řízení uživatelů** | Licence | Poskytnutá licence umožní nasazení a provoz systému bez omezení na počet uživatelů, spravovaných identit a napojených systémů. Nejsou přípustná žádná další omezení omezující obvyklé nasazení a provoz s ohledem na charakter organizace Zadavatele (počet záznamů, velikost databází atd.). Předpokládaný počet uživatelů je do 1000. |
| Škálovatelnost | Systém musí umožnit zvyšování výkonu (zlepšování odezvy) rozložením komponent Systému na více serverů – minimálně oddělení rolí (serverů) uživatelského rozhraní od výkonu integračních a provozních úloh. Data systému budou uchovávána v databázi. Systém bude podporovat režimu běhu ve vysoké dostupnosti. |
| Uživatelské role | Integrovaná správa aplikačních rolí včetně zařazení uživatele do odpovídající role v příslušných IS. V rámci dané role bude možné definovat jemné členění různých významů role. Například roli „editor webu“ bude možné rozšířit o významy odpovídající jednotlivým oddělením, pro které jsou části webu určené. Tyto rozšiřující významy rolí bude možné přímo přiřazovat systematizovaným místům, skupinám, organizačním jednotkám, uživatelům spravovaných v systému.  Systém umožní správu zákazových rolí. Zákazová role přiřazená systematizovanému místu, skupině, organizační jednotce nebo přímo uživateli zajistí odebrání této role v synchronizovaných systémech.  Systém umožní delegaci aplikačních rolí. Při delegaci jsou aplikační role předány na nového uživatele s možností nastavení platnosti, do kdy je delegace platná. Následně jsou role vráceny delegujícímu uživateli a odebraný delegovanému. |
| Historizace | Vestavěná detailní databázové historizace pro evidenci změn identit včetně referenčních objektů a vazeb mezi nimi. Historizace poskytne data v libovolném časovém okamžiku – aktuálním nebo zpětně v minulosti. |
| Automatizace | Podpora intuitivní tvorby pravidel v grafickém prostředí pro automatické vytváření uživatelských účtů, začleňování uživatelů do skupin a přiřazování aplikačních rolí uživatelům na základě kombinace libovolných atributů identity a přidružených referenčních objektů (organizační jednotka, aplikační role, systematizované místo atd.). Provádění vyhodnocení pravidel bude mít stejné vlastnosti jako jiné synchronizační procesy systému. Ruční vs plánované spuštění, historii běhů, simulační režim, atd. |
| Logování SIEM | Systém bude exportovat auditní logy pro systém typu SIEM ve formátu CSV nebo XML. |
| Logování systému | Systém obsahuje logování min. následujících typů událostí: - události systému (aplikační log) - změny entit evidovaných systémem a změny konfigurace systému (auditní log) - synchronizace s napojenými systémy (synchronizační log) - odeslané notifikace a upozornění (notifikační log) |
| Systematizovaná místa | Systém bude implementovat princip systemizovaných míst. Umožní systemizaci pracovních míst v souladu se strukturou organizace a bude spravovat jednotlivá systematizovaná místa a sadu oprávnění a rolí pro jednotlivé IS organizace vztažené ke konkrétnímu systemizovanému místu. |
| Podpora eIDAS | Systém umožní implementaci procesů a rozhraní, která jsou vyžadována v Nařízení Evropského parlamentu a Rady (EU) č. 910/2014 ze dne 23. července 2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES. |
| Požadavky na portál - obecné | Systém bude obsahovat webový portál (dále jen Portál), který bude sloužit jako hlavní rozhraní pro uživatele i správce pro přístup k datům, funkcím, správu a konfiguraci Systému. |
| Požadavky na portál – přístup | Správa systému musí být implementována jako webová konzole/aplikace přístupná přes prohlížeče Internet Explorer verze 10 a vyšší a poslední verze prohlížečů Firefox, Chrom. Tato webová konzole musí být přístupná výhradně protokolem https. |
| Podpora mobilních zařízení | Portál bude implementován s responzivním designem (přizpůsobení vzhledu typu zařízení, ze kterého je k portálu přistupováno). |
| Správa referenčních objektů | Portál bude umožňovat přehlednou správu samostatných identifikovatelných objektů - referenčních objektů, na které se identity mohou odkazovat: min. systematizované místo, organizační jednotka, skupina, aplikace, skupina aplikací, aplikační role, certifikát. |
| Referenční objekty | Systém umožní přidávání a správu dalších typů referenčních objektů a to i v průběhu správy konkrétní identity s možností okamžitého použití referenčního objektu u spravované identity. Systém bude v modulu správy identit u scénáře správy konkrétní identity implementovat v grafickém rozhraní přímý odkaz (proklik) na referenční objekty, na která se daná identita odkazuje včetně toho, aby administrátor mohl po přechodu na tento odkaz vytvářet a editovat další referenční objekty a následně po vrácení zpět na detail identity je v tomto scénáři přiřadil dané spravované identitě. |
| Zabezpečení referenčních objektů | Systém umožní nastavení samostatných nezávislých administrátorských oprávnění pro správu jednotlivých referenčních objektů |
| Rozšiřující atributy | Systém umožní dodatečné rozšiřování identit a referenčních objektů o další atributy a zajistí publikaci těchto nových atributů externím aplikacím prostřednictvím rozhraní webových služeb IDM. |
| Přehledné zobrazení | Systém bude obsahovat grafické zobrazení identit (uživatelských účtů) ve stromové organizační struktuře. Součástí jednoho pohledu v systému bude zobrazení organizační struktury včetně systematizovaných míst organizace až do úrovně jednotlivých uživatelských účtů (identit). V grafickém zobrazení stromové struktury bude možné vyhledávat jednotlivé identity, systematizovaná místa, organizační jednotky. |
| Vyhledávání – diakritika | Portál bude umožňovat vyhledávat i bez diakritiky (např. zadání Novak vyhledává i Novák apod.) |
| Správa certifikátů | Správa uživatelů (identit) bude umožňovat i správu údajů o uživatelských digitálních certifikátech. Data o certifikátech bude možné nahrávat do systému prostřednictvím rozhraní webových služeb. Systém umožní automatické zneplatnění uložených certifikátů po vypršení data platnosti. |
| Obrázky | Systém umožní k jednotlivým účtům (identitám) přikládat obrázky – fotografie. |
| Přesun identit | Systém umožní přesun identit mezi jednotlivými organizacemi či jejich odděleními. |
| Kopírování rolí | Systém umožní kopírovaní aplikačních rolí, mezi jednotlivými systematizovanými místy. |
| Ochrana proti chybám | Systém bude obsahovat mechanismus zabránění hromadným změnám z důvodu případných chybných vstupních dat (např. z personálního systému), aby nedošlo k hromadným nežádoucím změnám (například smazání objektů v Active Directory apod). |
| Aktivní uživatelé | Systém bude obsahovat přehled uživatelů aktuálně pracujících s Portálem |
| Slučování identit | Systém umožní sjednocení více uživatelů (identit) do jedné a odpovídající sjednocení spravovaných účtů. |
| Export údajů | Vestavěný export přehledů a seznamů zobrazených na portále do souborů CSV nebo obdobného strojově zpracovatelného a současně běžně čitelného formátu |
| Filtrování | Vestavěný editor filtrů pro vyhledávání identit a referenčních identit. Možnost filtrování libovolných atributů identity včetně přidružených referenčních objektů. Možnost uložení filtrů pro opakované použití. |
| Správa oprávnění | Víceúrovňová správa administrátorských oprávnění s možností nastavení oprávnění min. na úrovni organizační jednotky (nebo hlouběji) a detailní přiřazení rolí a oprávnění (např. přiřazení činnostní role, přiřazení aplikační role, editace identity apod.) |
| Editor oprávnění | Systém bude obsahovat editor oprávnění. V rámci editoru bude administrátor definovat oprávnění do Systému a následně tato oprávnění přiřazovat konkrétním uživatelům. Oprávnění bude definováno pro jednotlivé entity a moduly systému (identity, referenční objekty, konfigurace notifikací, konfigurace synchronizací, konfigurace systému, reporty, workflow, správa webových služeb IDM atd.) Dále bude oprávnění u entit (identit a referenčních objektů) definováno až na jejich konkrétní atributy včetně zobrazení / nezobrazení daného atributu, možnosti editace atributu uživatelem, povinnosti atributu, pořadí zobrazení atributů ve formuláři. U jednotlivých entit a modulů bude možnost definovat akce, které může uživatel s entitami a v rámci systému provádět. |
| Kontextový výběr organizační jednotky | Na úrovní organizační jednotky bude možné pro výběr a přiřazování rolí nastavit sady povolených aplikační rolí, skupiny, systematizovaných míst dostupných pro identity z dané organizační jednotky. |
| Správa licencí | Systém umožní spravovat licence pro jednotlivé evidované aplikace a přiřazovat je jednotlivým uživatelům (identitám). Pro schvalování přiřazování licencí bude IDM obsahovat workflow platformu s možností vytvářeni víceúrovňových schvalovacích workflow. |
| Časová omezení | Systém bude umožňovat přiřazení rolí konkrétní identitě, systemizovanému místu, skupině a organizační jednotce včetně možnosti nastavení data a času vypršení platnosti přiřazení. Po vypršení platnosti přiřazení systém roli přiřazenému objektu automaticky odebere. |
| Vícenásobné vazby | Možnost přiřazení identit k systematizovaným místům ve vazbě M:N. Identita může být v systému evidována na více systematizovaných místech a současně na systematizovaném místě může být evidováno více identit. |
| Přehled rolí | Systém bude zajišťovat zobrazení přidělených rolí a jejich rozšiřujících významům k jednotlivým identitám s rozdělením na role navázané na systemizované místo, role navázané na identitu, role navázané na organizační jednotku, role navázané na skupinu. U identity musí být evidován a v systému souhrnně zobrazen seznam všech rolí včetně informace o tom, odkud uživatel roli zdědil nebo mu byla delegována (z organizační jednotky, systematizovaného místa, skupiny apod.). |
| Skupiny | Systém bude obsahovat správu skupin s možností začleňovat více skupin do sebe, přiřazovat do skupin jednotlivé uživatele i systematizovaná místa. |
| Zastupitelnost | Systém bude obsahovat správu vztahů zastupitelnosti mezi uživateli. Musí umožnit uživatelům, aby v souladu se strukturou organizace mohli uživatelé delegovat v případě potřeby (dovolená, služební cesta) svoje role, nebo jejich část na jiné pověřené osoby a to i v režimu, kdy jeden uživatel může mít pro každou svou činnost nastaveného jiného uživatele jako zástupce. |
| Delegování oprávnění | Možnost delegování administrátorských práv. |
| Obnovení hesla | Systém bude obsahovat samoobslužné uživatelské rozhraní pro reset hesla jednotlivých účtů daného uživatele. Zasílání kódů pro reset hesla danému uživatele musí být možnou provádět pomocí SMS (tj. v systému musí být možné na SMS bránu či službu napojit). Rozhraní musí umožnit i běžnou změnu hesla (bez resetu). |
| Žádosti | IDM bude obsahovat samoobslužné uživatelské rozhraní pro zadávání žádostí o přidělení jednotlivých aplikačních rolí a členství ve skupinách. Role a skupiny budou kategorizovány a kategoriím bude možné přidělit schvalovací workflow nebo může žádost vyřízena automaticky bez schválení. |
| Kontextový výběr | Samoobslužné rozhraní umožní na úrovní organizace a organizační jednotky definovat seznam rolí a skupin, o které mohou žadatelé požádat. |
| Individualizace | Systém umožní uživatelům individuálně nastavit vlastní zobrazení rozhraní - min. zobrazení / skrytí sloupců u všech seznamů, počet zobrazených záznamů na stránku - vždy pro každý seznam samostatně |
| Workflow | Integrované workflow pro řízení životního cyklu změn identit a schvalování změn. Funkční požadavky: - Zadávání požadavků uživatelů na změny v přiřazení rolí a skupin ke schválení nadřízeným - Možnost sledování stavu svých požadavků uživateli - E-mailové upozornění schvalovatele na požadavek ke schválení - Přehled úloh ke schválení pro každého schvalovatele  - Schvalování či zamítnutí požadavků včetně uvedení zdůvodnění  - Podpora vícekrokového schvalování - Podpora schvalování jedním nebo více schvalovateli (skupinou schvalovatelů) - Správce IDM může pracovat se všemi úlohami - Možnost větvení pro ošetření výjimek vzniklých při schvalování - Řešení zastupitelnosti - Eskalace - upozornění při překročení termínu splnění - Možnost vkládání systémových kroků s voláním webových služeb a spuštěním skriptů |
| Workflow - sledování | Průběh workflow bude možné sledovat v grafické podobě ve formě diagramu. Diagram bude v obvyklém formátu pro zobrazení workflow např. aktivity diagram, BPMN nebo Archimate |
| Recertifikační workflow | Recertifikační workflow pro kontrolu oprávnění v pravidelných intervalech a podporu Compliance. |
| SoD | Hlídání přiřazení konfliktních rolí - ochrana systému v případě pokusu o přiřazení konfliktní role - pokud dojde k pokusu o přiřazení role identitě, která již má jinou konfliktní roli, musí systém konflikt oznámit a vlastní přiřazení neprovede. |
| Upozornění | Systém zajistí zasílání konfigurovatelných emailových upozornění min. pro následující události: vytvoření a změna identity, referenčního objektu (systematizované místo, organizační jednotka, skupina, aplikace, skupina aplikací, aplikační role atd.), problém při synchronizaci, vypršení hesla v Active Directory, vypršení platnosti certifikátu. Mechanismus správy notifikací včetně náhledu na odeslané notifikace musí být spravován přímo v Portálu systému. |
| Včasná upozornění | Portál bude obsahovat notifikační šablony a notifikace pro upozornění na vypršení hesla v Active Directory a vypršení platnosti certifikátů. Notifikaci lze nastavit na několik dní dopředu před vlastním vypršením hesla nebo certifikátu. |
| Šablony upozornění | Šablony upozornění umožní definovat příjemce, předmět a obsah upozornění. U upozornění vázaného k identitám musí být možné nastavovat různé příjemce pro různé části organizační struktury (např. odbor, oddělení) apod. Šablony musí umožnit vložit do obsahu upozornění libovolný atribut identity a/nebo referenčního objektu. |
| Kontext upozornění | U notifikací ve vazbě na identity a referenční objekty musí být možné konfigurovat nastavení na úroveň jednotlivých atributů. V šabloně musí být možné vybrat libovolné atributy identity a referenčních objektů a následně je vložit a použít v definici textu pro emailové zprávy. Dále musí být možné u notifikací konfigurovat podmínky pro provedení notifikace na základě hodnot jednotlivých libovolných atributu identity a referenčních objektů. (například notifikace je generována pouze pro identitu v konkrétních uvedených skupinách, která má uvedenu konkrétní aplikační roli, systematizované místo, atd.). V Portálu musí být možné notifikace aktivovat pro jednotlivé zdrojové systémy, které v IDM změnu identity nebo referenčního objektu provedly. |
| Logování | Systém musí umožnit logování minimálně v tomto rozsahu:  - události systému (aplikační log) - změny entit evidovaných systémem a změny konfigurace systému (auditní log) - synchronizace s napojenými systémy (synchronizační log) - odeslané notifikace a upozornění (notifikační log) |
| Logování | Veškeré změny vyvolané požadavky uživatele a administrátorů/správců IDM budou provedeny transakčně. Budou logovány tak, aby bylo možné zpětně prokázat co, kdo a kdy měnil v identitách a referenčních objektech i v administraci a konfiguraci IDM. Záznam v logu bude obsahovat původní i novou hodnotu. |
| Důvěryhodnost logování | Veškeré požadavky na změny v IDM bude možné zadávat výhradně prostřednictvím Portálu. Není přípustné realizovat požadavky ručními změnami textových soubory jako XML, CSV, atd. z důvodu zajištění úplného logování všech změn jednotlivých konfigurovaných parametrů IDM. |
| Auditní report | IDM umožní export auditního reportu z údajů o identitách uložených v IDM a to i historických. Auditní reporty budou minimálně ve formátu XML nebo CSV a budou obsahovat souhrnné zobrazení daných uživatelů (identit) a jejich rolí v IS napojených na IDM, přiřazených skupin ve vybraném časovém okamžiku od aktuálního času do minulosti. |
| Auditní report - výběr | IDM bude obsahovat editor pro vyhledávání identit a referenčních objektů v systému IDM pro vytvoření reportu. Do filtru musí být možné zadat libovolné atributy identity, které jsou v systému IDM evidovány včetně přidružených referenčních objektů. |
| Reporty uživatelů | Vestavěné reporty obsahující uživatele s přímo přiřazenými aplikačními rolemi a s aplikačními rolemi delegovanými od jiných uživatelů. Reporty budou exportovatelný do CSV souboru. |
| Reporty - zasílání | IDM bude obsahovat možnost generovat do CSV souboru report uživatelů přiřazených aplikačním rolím a možnost nastavení pravidel pro automatického zasílání reportu emailem. |
| Karta uživatele | IDM bude obsahovat report, který do formátu PDF vygeneruje kartu uživatele obsahující informace o uživateli včetně seznamu rolí, které uživatel má, skupin, certifikátů, atd. |
| Reporty - historie | Automatické ukládání vygenerovaných reportů s možností pozdějšího zobrazení či stažení. |
| Reporty - porovnání | Snadné porovnání změn mezi vygenerovanými reporty stejného typu v prostředí Portálu. |
| Dashboard | IDM bude obsahovat centrální dashboard, který bude obsahovat následující údaje:   * Synchronizační úlohy v chybě * chyby běhu synchronizací * chyby při generování a odesílání notifikací * chyby volaní metod rozhraní webových služeb IMD(např. pokus o přístup k metodě, na kterou nemám oprávnění) * chyby plánovaných úloh (agentů) * nově vytvořené poznámky * workflow v chybě * neúspěšné akce systému v systému IDM   Záznamy v dashboard se budou načítat za počet dnů definovaných v konfiguraci IDM |
| Webové služby (WS) | IDM bude poskytovat rozhraní webových služeb pro napojení dalších systémů s možností konfigurace v Portálu. |
| Standardy WS | Webové služby IDM budou definované v rozšířeném standardu WSDL a podporovat protokol SOAP. Vrámci povahy předávaných identitních údajů (včetně osobních údajů) je požadováno zajistit maximální zabezpečení a zajištění spolehlivosti volání webových služeb minimálně v rozsahu specifikací WS–Security, WS-SecurityPolicy, WS-ReliableMessaging, WS-AtomicTransactions. |
| Bezpečnost WS | Konfigurace webových služeb umožní konfigurovat přístup pro volání jednotlivých vybraných služeb pro každý odpovídající systémový účet samostatně. |
| Logování WS | Volání webových služeb bude logováno na úrovni databáze a bude možné je zobrazit v prostředí Portálu |
| Služby rozhraní WS | Rozhraní bude poskytovat minimálně následující služby:   * Načtení organizační struktury * Načtení hierarchie systematizovaných míst * Načtení seznamu identit * Načtení nadřízené osoby pro daného zaměstnance * Načtené seznamu aplikační rolí * Načtení seznamu uživatelů dané aplikace * Zápis seznamu aplikačních rolí do IDM * Zápis certifikátů do IDM * Zápis a změna uživatelů a osob * Zabezpečená služba pro přihlášení aplikace k IDM * Zabezpečená služba pro přihlášení uživatele k IDM * Přidání a odebrání uživatele do/z skupiny * Přidání a odebrání aplikační role a jejího rozšiřujícího významu na/z uživatele, organizační jednotku, systematizované místo nebo skupinu * Přidání a odebrání agendové role na uživatele nebo systematizované místo |
| Synchronizace | Ruční i automatické spuštění synchronizací s propojenými systémy. |
| Synchronizace - simulace | Spuštění synchronizací i v simulačním režimu pro ověření dopadu reálného spuštění bez ovlivnění produkčních dat a napojených systémů. Simulační logy budou zobrazitelné v Portálu. |
| Simulace - průběh | Zobrazení jednotlivých stavů průběhu synchronizace bude k dispozici v přehledné grafické podobě. |
| Synchronizace - režimy | Pro napojení na jednotlivé systémy a implementaci jejich synchronizací s IDM umožní IDM u každého systému využít více režimů synchronizací (za předpokladu podpory napojovaného systému):  - Plná synchronizace – prochází všechny objekty v IDM a synchronizuje je s objekty daného systému  - Změnová synchronizace – synchronizuje vždy jen změny od poslední spuštěné synchronizace. Umožní dále spouště změnové synchronizace pro změny vybraného vstupního systému a automatické spouštění navázané synchronizace.  - Okamžitá synchronizace konkrétní identity na vyžádání – synchronizuje okamžitě pouze vybranou identitu.  - Rekonciliační synchronizace – synchronizace vytvoří rekonciliační report pro porovnání změn mezi nastavením identit a jejich oprávnění pro daný systém v IDM vs. nastavení identit a oprávnění přímo v připojeném systému.  - Simulační synchronizace – synchronizace vytvoří report očekávaných změn v napojeném systému pro provedení ostré synchronizace. Report změn bude evidován jako pohled nebo přehledná souhrnná tabulka.  - Historie běhu synchronizací – jednotlivé běhy synchronizací budou zaznamenány v databázi a dostupné v Portálu. Historie plné synchronizace bude obsahovat odkazy na objekty, které byly synchronizovány a log, co bylo u těchto objektů změněno v synchronizovaném systému. V případě změnové synchronizace pak bude v historii dále informace o události, která změnovou synchronizaci vyvolala. |
| Synchronizace - správa | Vestavěná správa jednotlivých synchronizací včetně nastavení připojení na synchronizované systémy, nastavení plné a změnové synchronizace, počet změn, které je možné zpracovat, závislostí mezi synchronizacemi, nastavení časového intervalu spouštění, nastavení intervalu odstávky. U jednotlivých synchronizací je rovněž požadováno, aby bylo možné vybírat organizace, které se mají z IDM synchronizovat s danými systémy. Správa bude součástí Portálu. |
| Synchronizace  -sekvence | Pro napojení na jednotlivé systémy a implementaci jejich synchronizací s IDM umožní IDM sekvenční spouštění synchronizací (za předpokladu podpory napojovaných systémů) a to tak, aby jednotlivé synchronizace mohli být spouštěny po sobě v sekvencích. Navazující synchronizované systémy v sekvenci bude možné definovat dle požadavků a spouštět nebo zastavovat automaticky i ručně. |
| Agenti | Pro plánované úlohy umožní IDM definici agentů a jejich plánovaných spouštění na základě akcí a triggerů v systému. Spouštění je možné definovat i pro požadované intervaly, definovat omezení a další. Agenty bude možné importovat do systému IDM minimálně ve formátu JSON. |
| Agenti – simulace | Systém IDM umožní spouštění agentů také v režimu simulace. |
| Správa SW aktiv | V rámci systému bude možné spravovat evidenci aktiv s klasifikací dle zákona o kybernetické bezpečnosti. V systému bude možné spravovat evidenci primárních, podpůrných a technických aktiv. Technická aktiva budou dále rozdělena na datová, softwarová, hardwarová aktiva, informační služby. Jednotlivá aktiva je možné členit do hierarchie aktiv. |
| Rozsah aktiv | Minimální rozsah evidovaných dat:  Základní údaje:   * ID Aktiva – identifikátor * Název aktiva – označení aktiva * Popis aktiva – popis aktiva * Typ aktiva – typ aktiva * Kategorizace aktiva – kategorizace aktiva * Organizace – označení organizace daného aktiva * Stav aktiva – stav daného aktiva * Kód ISVS – číselný kód přidělený informačnímu systému veřejné správy * Datum identifikace aktiva * Lokalizace aktiva * Vazby na jiná aktiva   Analýza rizik   * Požadavky na dostupnost aktiva * Požadavky na důvěrnost aktiva * Požadavky na integritu aktiva * Celkové hodnocení aktiva – číselné hodnocení aktiva * Popis zabezpečení aktiva – popis způsobu zabezpečení aktiva * Frekvence přístupu – hodnota frekvence použití aktiva * Nedostupnost – popis hodnocení maximální doby nedostupnosti a definice náhradních postupů v případě nedostupnosti   Ochrana v rámci zpracování osobních údajů:   * Klasifikace – klasifikace osobních údajů * Zdroj dat – popis získání osobních údajů * Aktualizace – popis způsobu aktualizace osobních údajů * Skartace – popis skartace dat * Zpracování – popis způsobu zpracování osobních údajů * Registrace – popis registrace zpracování osobních údajů na Úřad pro ochranu osobních údajů * Kategorie – kategorie osobních údajů * Účel zpracování – účel zpracování osobních údajů * Zpracovatel – informace o zpracovateli osobních údajů * Příjemce – informaci o příjemci osobních údajů v případě, že jsou předávány * Legislativa – popis legislativy vztahující se k danému aktivu.   Garanti aktiv:   * Vlastník – vlastník aktiva * Správce aktiva – správce aktiva (například dané aplikace) * Zástupce – zástupce správce aktiva * Uživatelé – seznam uživatelů daného aktiva. Uživatele bude možné slučovat do rolí a skupin   Technické údaje (týkající se technických aktiv):   * Technické prostředky (servery, databáze) – odkaz na technické prostředky, pro provoz a aktiva   Zálohování – popis způsobu a frekvence zálohování |
| Správa osob | Systém obsahovat správu osob, organizační strukturu, rolí. Tuto evidenci bude možné synchronizovat s personálním systémem a navázat na správu aktiv. |
| Tiskové výstupy | Systém bude obsahovat funkcionalitu pro generování následujících reportů:   * Přehled aktiv s možností filtrování a třídění podle všech dostupných polí * Karta aktiva se všemi navázanými údaji * Zobrazení vazeb mezi aktivy * Možnost definice vlastních sestav * Přehled žádostí o přidělení aktiva aktivních a dokončených   Přehled oprávnění a přístupů k danému aktivu |
| Schvalovací workflow | Systém bude obsahovat implementaci následujících workflow:   * Žádost o přístup k aktivu směrovaná na seznam Garantů jako schvalovatele žádosti * Periodická revize aktiv jednotlivými garanty * Periodická revize stavu evidence garantem z oblasti řízení bezpečnosti   Funkční požadavky na workflow:  - Zadávání požadavků uživatelů na změny v evidenci - Možnost sledování stavu svých požadavků uživateli - E-mailové upozornění schvalovatele na požadavek ke schválení - Přehled úloh ke schválení pro každého schvalovatele  - Schvalování či zamítnutí požadavků včetně uvedení zdůvodnění  - Podpora vícekrokového schvalování - Podpora schvalování jedním nebo více schvalovateli (skupinou schvalovatelů) - Možnost větvení pro ošetření výjimek vzniklých při schvalování - Řešení zastupitelnosti - Eskalace - upozornění při překročení termínu splnění - Možnost vkládání systémových kroků s voláním webových služeb a spuštěním skriptů  Průběh workflow bude možné sledovat v grafické podobě ve formě diagramu, ve kterém bude zřejmý stav probíhajícího workflow. Diagram bude v obvyklém formátu pro zobrazení workflow např. aktivity diagram, BPMN nebo Archimate |
| Rozšiřující atributy | Systém umožní dodatečné konfigurační rozšiřování evidence o další atributy |
| Aktivní uživatelé | Systém bude obsahovat přehled uživatelů aktuálně pracujících s Portálem |
| Správa oprávnění k aktivům | Systém bude obsahovat editor oprávnění. V rámci editoru bude administrátor definovat oprávnění do systému a následně tato oprávnění přiřazovat konkrétním uživatelům. Oprávnění bude definováno pro jednotlivé části systému (aktiva, uživatelé aktiva, konfigurace notifikací, konfigurace systému, reporty, workflow, správa rozhraní atd.) Oprávnění bude definováno až na konkrétní atributy včetně zobrazení / nezobrazení daného atributu, možnosti editace atributu uživatelem, povinnosti atributu, pořadí zobrazení atributů ve formuláři. U jednotlivých entit a modulů bude možnost definovat akce, které může uživatel s entitami a v rámci systému provádět. |
| Synchronizace software aktiv | Systém poskytne rozhraní pro pravidelnou synchronizaci softwarových aktiv a jim přidělených uživatelům. |
| Obecné konektory | Vestavěné obecné skriptovatelné (javascript, groovy) konektory pro správu identit v napojených systémech: - konektor pro spouštění CMD a powershell příkazů, SSH - konektor pro práci s CSV soubory - konektor pro práci s databázi Microsoft SQL, Oracle  - konektor pro napojení na SOAP webové služby - konektor pro napojení na REST webové služby  U jednotlivých konektorů je možné dynamicky měnit transformační logiku pro nutnou komunikaci s danými typy rozhraní. |
| Zdrojový systém | IDM bude napojeno na personální systém Vema. Z personálního systému budou načítány údaje o organizační struktuře, hierarchii pracovních míst, osobách a tyto údaje budou pro IDM sloužit jako zdrojové. |
| Konektor na Active Directory | IDM musí obsahovat konektor umožňující napojení na Microsoft Active Directory s následující funkcionalitou:  komplexní správu účtů, kontaktů, certifikátů a skupin (založení, změnu atributů, zrušení, změnu hesla atd.)  založení domovského adresáře včetně nastavení oprávněná  správu účtů a jejich certifikátů včetně inicializačního načtení z AD  správu skupin a členství ve skupinách včetně inicializačního načtení z AD  správu organizačních jednotek včetně inicializačního načtení z AD |
| Konektor na FONS Enterprise | IDM musí obsahovat konektor umožňující napojení na FONS Enterprise s následující funkcionalitou:  inicializační načtení dat  správa lokálních identit  správa oprávnění pro jednotlivé uživatele ve formě přiřazení skupin nebo rolí |
| Konektor OpenLIMS | IDM musí obsahovat konektor umožňující napojení na OpenLIMS následující funkcionalitou:  inicializační načtení dat  správa lokálních identit  správa oprávnění pro jednotlivé uživatele ve formě přiřazení skupin nebo rolí |
| Konektor Docházkový systém IVAR | Konektor IDM musí umožnit napojení na Docházkový systém IVAR s následující funkcionalitou:  inicializační načtení dat  správa lokálních identit  správa oprávnění pro jednotlivé uživatele ve formě přiřazení skupin nebo rolí |
| Konektor EnvisLIMS | Konektor IDM musí umožnit napojení na EnvisLIMS s následující funkcionalitou:  inicializační načtení dat  správa lokálních identit  správa oprávnění pro jednotlivé uživatele ve formě přiřazení skupin nebo rolí |
| Konektor Farmis | Konektor IDM musí umožnit napojení na Farmis s následující funkcionalitou:  inicializační načtení dat  správa lokálních identit  správa oprávnění pro jednotlivé uživatele ve formě přiřazení skupin nebo rolí |
| Konektor Helios Nefrit | Konektor IDM musí umožnit napojení na Helios Nefrit s následující funkcionalitou:  inicializační načtení dat  správa lokálních identit  správa oprávnění pro jednotlivé uživatele ve formě přiřazení skupin nebo rolí |
| Konektor IS Kredit | Konektor IDM musí umožnit napojení na IS Kredit s následující funkcionalitou:  inicializační načtení dat  správa lokálních identit  správa oprávnění pro jednotlivé uživatele ve formě přiřazení skupin nebo rolí |
| Konektor Servis Desk | Konektor IDM musí umožnit napojení na Servis Desk s následující funkcionalitou:  inicializační načtení dat  správa lokálních identit  správa oprávnění pro jednotlivé uživatele ve formě přiřazení skupin nebo rolí |
| Konektor IceWarp | Konektor IDM musí umožnit napojení na IceWarp s následující funkcionalitou:  inicializační načtení dat  správa lokálních identit  správa oprávnění pro jednotlivé uživatele ve formě přiřazení skupin nebo rolí |
| Externí IDM | IDM bude obsahovat samostatnou část Portál pro správu externích uživatelů. Tato externí část IDM bude obsahovat konektor/rozhraní pro správu identit ze strany externích organizací. |