# Realizace systému pro řízení identit

## Identity management systém (IdM)

Identity management systém musí splňovat následující technické specifikace:

* automatizovanou a centralizovanou správu životního cyklu identit
* aktuální přehled přístupů a oprávnění všech uživatelů v systémech
* auditování a logování všech změn oprávnění a nastavení ve správě identit
* procesy spojené s životním cyklem zaměstnance i externistů
* přehled o aktivních a neaktivních účtech MS AD a dalších napojených systémech
* pravidelná recertifikace stavu účtů
* správu pravidel pro tvorbu a nastavení uživatelských oprávnění
* nastavení uživatelských oprávnění dle šablony (automatické role)
* přehledný reporting pro bezpečnostní audit
* správa a předávání prvotního hesla
* pomoc se splněním NIS 2 požadavků na správu identit, hesel a přístupů včetně auditní stopy

### POŽADOVANÉ ŘEŠENÍ

IdM systém bude spravovat a synchronizovat údaje v adresářové službě (AD) a v samostatných aplikacích používaných v organizaci zadavatele na základě údajů získaných z personálního systému Vema. Automatický proces správy identit bude pracovat následovně. Údaje o novém zaměstnanci se zadají do personálního systému. IdM systém zpracuje a ověří pracovní zařazení zaměstnance. Podle příslušné pracovní pozice a organizační jednotky vybere pro zaměstnance vhodné role. Na základě rolí IdM systém vytvoří záznam v adresářovém systému (AD, přístupy do NIS apod). Podobný proces nastává při změně pracovního zařazení zaměstnance a při jeho odchodu. Veškeré operace a změny budou detailně logovány s možností vytvoření reportů.

### PROPOJENÉ SYSTÉMY S IDM

* Personální systém Vema
* Doménová adresářová služba Active Directory (dále MS AD)
* Nemocniční informační systém AMIS\*HD
* Laboratorní systém TIS
* Docházkový systém ShiftMaster
* Informační systém Nefris
* Dokumentační systém EISODX
* Lékárenský informační systém
* Mailserver
* Service desk nástroj

Další systémy budou připojeny v evidenčním módu:

* Parkovací systém
* Účetní a ekonomický systém

### IMPLEMENTACE

Předmětem řešení budou i veškeré služby související s dodávkou – doprava, návrh řešení, instalace, implementace do stávající infrastruktury, konfigurace a napojení přímo i evidenčně spravovaných systémů, zaškolení obsluhy a správy systému, testování a 14 denní testovací provoz. Veškeré školení bude probíhat v prostorách zadavatele v časech podle možností zadavatele a v českém jazyce. Implementace bude realizována do virtuálního prostředí zadavatele.

### LICENCE

Je požadována dodávka:

* licencí identity managementu
* dalších licencí potřebných pro provoz identity managementu (pokud jsou potřebné)
* listinného potvrzení dodaných licencí -  co do jejich počtu a rozsahu – od výrobce SW
* Požadovaný počet identit: 2100 (1800 interních, 300 externích - dodavatelé Nemocnice Břeclav)

Dodavatel se zaváže systém po dobu minimálně 5 let (doba poskytování podpory) udržovat správně licencovaný, splňující veškeré požadavky kladené na bezpečnost, ochranu osobních údajů a v souladu s legislativou.

Dodavatel se zaváže po dobu minimálně 2 let (doba poskytování podpory) dále poskytovat zejména:

* Opravu zjištěných chyb v programovém kódu IdM formou aktuálně vydávaných softwarových opravných kódů (hot-fix nebo patch).
* Updaty a upgrady IdM, které byly výrobcem uvolněny na trh. Dodavatel musí zajistit aktuálnost IdM na všech aktivních i neaktivních nodech použité virtualizace.
* Proaktivní řešení bezpečnostních chyb a zranitelnosti IdM.
* Odstranění zranitelnosti identifikované nezávislými subjekty (např. NIST), NÚKIB.
* Aktualizaci IdM tak, aby byl v souladu s relevantními platnými právními předpisy ČR a EU.

POVINNÉ PARAMETRY DODÁVANÉHO IDM

Uchazeč musí všechny povinné parametry splnit.

|  |  |
| --- | --- |
| **Parametr** | **Popis povinného parametru** |
| Základní funkce | IDM (dále IDM nebo Systém) bude udržovat a spravovat identity a organizační strukturu organizace. Spravované identity budou sloužit jako referenční identity pro ostatní vnitřní i vnější informační systémy. |
| Evidence aplikací a rolí | Integrovaný registr aplikací a informačních systémů (souhrnně IS) a jejich uživatelských rolí včetně možnosti importu rolí přes webové služby. |
| Uživatelské role | Integrovaná správa uživatelských rolí, včetně zařazení uživatele do odpovídající role v příslušných IS. |
| 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 libovolných atributů identity a přidružených referenčních objektů (organizační jednotka, aplikační role, systematizované místo atd.). |
| Logování | Systém bude poskytovat auditní logy pro systém typu SIEM |
| Logování systému | Systém obsahuje logování min. následujících typů událostí:  události systému změny entit evidovaných systémem a změny konfigurace systému synchronizace s napojenými systémy odeslané notifikace a upozornění |
| Správa identit | Systém bude spravovat organizační strukturu- umožní evidovat více organizačních struktur (bez omezení) |
| 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 GUI | IDM bude obsahovat webové GUI, který bude sloužit jako hlavní rozhraní pro uživatele i správce pro přístup k datům, funkcím, správu a konfiguraci Systému. |
| Požadavky na GUI – přístup | Správa systému IDM musí být implementována jako webová konzole/aplikace přístupná přes poslední verze prohlížeče Edge, Chrome a Firefox. Tato webová konzole musí být přístupná výhradně šifrovaným protokolem HTTPS. |
| Požadavky na GUI – náhled uživatele | IDM musí umožnit náhled do IDM pohledem jiného uživatele v režimu pro čtení. Tato funkce je zpřístupněna vybraným uživatelům dle nastavených práv v IDM - například pro uživatele podpory nebo IT administrátora IDM, aby zajistili support běžným uživatelům. |
| Podpora mobilních zařízení | GUI bude implementován s responzivním designem (přizpůsobení vzhledu typu zařízení, ze kterého je k GUI přistupováno) |
| Správa referenčních objektů | GUI 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. |
| 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 | IDM bude obsahovat grafické zobrazení identit (uživatelských účtů) ve stromové organizační struktuře. Součástí jednoho pohledu v IDM 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. |
| 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). |
| Export údajů | Vestavěný export přehledů a seznamů zobrazených na GUI 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. |
| 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 | IDM bude obsahovat editor oprávnění. V rámci editoru bude administrátor definovat oprávnění do IDM 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 IDM, 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 IDM provádět. |
| Správa licencí | IDM umožní spravovat licence pro jednotlivé evidované aplikace a přiřazovat je jednotlivým uživatelům (identitám).  IDM umožní přehledně zobrazit počet a typ vydaných licencí u každého uživatele. V systémech, které správu licencí podporují ve svém rozhraní (AD, o365 atd…) umožní IDM skrze své konektory licence přidělovat a odebírat uživatelům.  IDM umožní v samoobsluze uživatelů požádat o licenci a její vydání je schvalováno podobně jako přidělení rolí. |
| Časová omezení | IDM 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 IDM rolí přiřazenému objektu automaticky odebere. |
| Vícenásobné vazby | Možnost přiřazení identit k systematizovaným místům ve vazbě M : N. Identita může být v IDM evidována na více systematizovaných místech a současně na systematizovaném místě může být evidováno více identit. |
| Přehled rolí | IDM bude zajišťovat zobrazení přidělených rolí 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 IDM souhrnně zobrazen seznam všech rolí včetně informace o tom, odkud uživatel roli zdědil (z organizační jednotky, systematizovaného místa, skupiny apod.). |
| Skupiny | IDM bude obsahovat správu skupin s možností začleňovat více skupin do sebe, přiřazovat do skupin jednotlivé uživatele i systematizovaná místa. |
| Správa osobních údajů | IDM umožní správu evidence osobních údajů - bude obsahovat správu evidence subjektů údajů a evidenci jejich osobních údajů včetně jejich kategorií a klasifikací. IDM umožní archivovat nebo rovnou smazat vybrané uživatele, pokud to bude z důvodu ochrany jejich osobních údajů požadováno. |
| Obnovení hesla | IDM bude obsahovat samoobslužné uživatelské rozhraní pro reset hesla jednotlivých účtů daného uživatele. Zasílání kódů pro reset hesla danému uživatele musí být možno provádět pomocí SMS (tj. IDM musí být možné na SMS bránu či službu napojit). Rozhraní musí umožnit i běžnou změnu hesla (bez resetu). |
| Synchronizace hesla z MS AD | IDM nabídne možnost online synchronizace hesla z napojeného systému - domény MS AD) jak pro validaci zadaného hesla, tak pro jeho možnou distribuci do jiných systémů při jeho změně. IDM může sloužit pro centrální vynucení politik hesel a možnost nastavení změny jednoho hesla i do systémů, které nejsou v současnosti autentizovány vůči doméně. |
| 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. |
| Externí subjekty | IDM bude obsahovat samoobslužné uživatelské rozhraní s konfigurovatelnými registračními formuláři pro registraci externích organizací a identit i jejich žádostí o konkrétní aplikační role nebo přiřazení do skupin. |
| 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 Možnost vkládání systémových kroků s voláním webových služeb a spuštěním skriptů |
| Upozornění | IDM zajistí zasílání konfigurovatelných emailových upozornění. Mechanismus správy notifikací včetně náhledu na odeslané notifikace musí být spravován přímo v IDM. |
| Včasná upozornění | IDM 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. |
| 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. |
| 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. |
| Reporty - historie | Automatické ukládání vygenerovaných reportů s možností pozdějšího zobrazení či stažení. |
| Univerzální API (např. REST) | IDM umožní kromě správy přes grafické webové rozhraní také kompletní správu přes univerzální API. Toto lze využít například pro napojení provozních systémů - monitoring, datawarehouse, SIEM nebo pro aktivní (push) správu dat v IDM – například dávkové založení uživatelů, stažení reportu, stažení certifikátů atd…    Veškeré operace umožněné v grafickém rozhraní musí být dostupné i pro automatizovanou správu přes univerzální API    Univerzální rozhraní komunikuje vždy šifrovaně. |
| Volání a dokumentace univerzálního API | Univerzální API bude také možné přímo v IDM volat interaktivně přes grafické rozhraní. Obsluha IDM si tak bude moci bez programování vyzkoušet metody API například pro definici napojení na dávkové zpracování dat nebo nově zaváděné systémy v organizaci. |
| Logování WS | Volání webových služeb bude logováno a bude možné je zobrazit v prostředí GUI |
| Služby rozhraní WS | Rozhraní bude poskytovat minimálně následující služby: - Získání organizační struktury - Získání hierarchie systematizovaných míst - Získání seznamu identit - Získání nadřízené osoby pro daného zaměstnance - Získání seznamu aplikační rolí - Získání seznamu uživatelů dané aplikace - Zápis seznamu aplikačních rolí do IDM - Zápis certifikátů do IDM - Zápis a změna identit |
| 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 GUI. |
| 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.  - 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. |
| Synchronizace - správa | Vestavěná správa jednotlivých synchronizací včetně nastavení připojení na synchronizované systémy, nastavení plné a změnové synchronizace, počet změn, které je možné zpracovat, 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 GUI. |
| Obecné konektory | Vestavěné obecné konektory pro správu identit v napojených systémech:  ·       konektor pro spouštění CMD příkazů  ·       konektor pro práci s CSV soubory  ·       konektor pro práci s databázi Microsoft SQL  ·       konektor pro napojení na SOAP webové služby  ·       konektor pro napojení na REST webové služby  ·       konektor pro napojení na LDAP server s podporou LDAP v3 |
| Aplikační konektory | IDM bude spravovat identity a řídit oprávnění v dále vyjmenovaných systémech. V těchto systémech bude IDM vytvářet, aktualizovat, vytvářet uživatele a nastavovat jim oprávnění k rolím.   * Personální systém Vema * Doménová adresářová služba Active Directory (dále MS AD) * 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 * Nemocniční informační systém AMIS\*HD * Laboratorní systém TIS * Docházkový systém ShiftMaster * Informační systém Nefris * Dokumentační systém EISODX * Lékárenský informační systém * Mailserver * Service desk nástroj |
| 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. |