3.1 ARCHITEKTONICKÉ MODELY

Kapitola popisuje architektonické modely EnvilAM řešení.

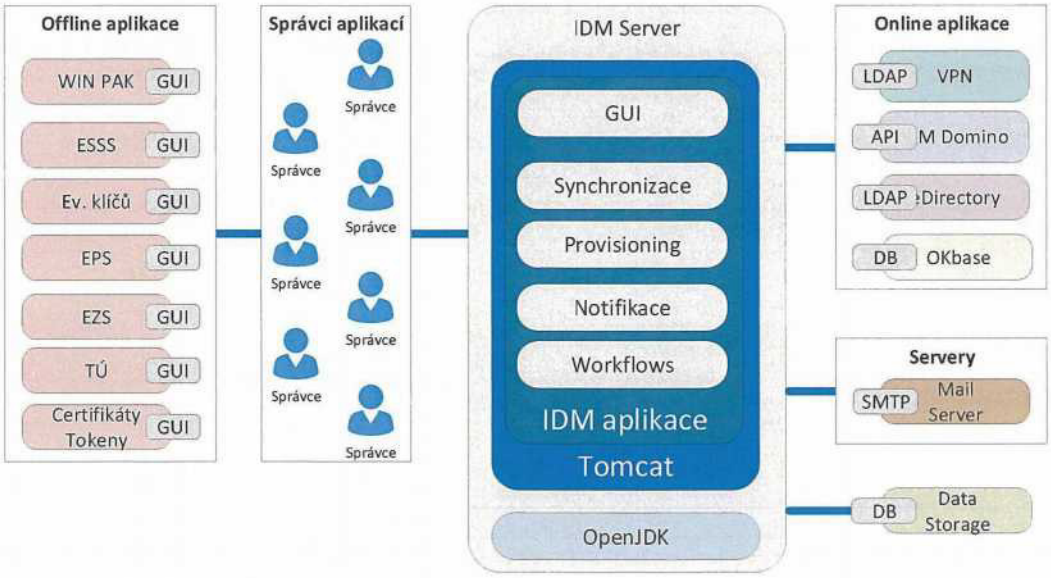
3.1.1 Infrastrukturní model IDM

Infrastrukturní model EnvilAM IDM ukazuje předpokládané propojení IS a komponent architektury:

- IDM server je umístěn na vlastním serveru
- řízené koncové systémy jsou napojeny napřímo (online)
- nepřipojené systémy jsou řízeny prostřednictvím správců (offline)
- dále je využit mailový server a server s datovým úložištěm (databáze, součást řešení)

IDM server sestává z těchto komponent:

- Java JDK
- Apache Tomcat
- Evolveum midPoint
- PostgreSQL pro data storage

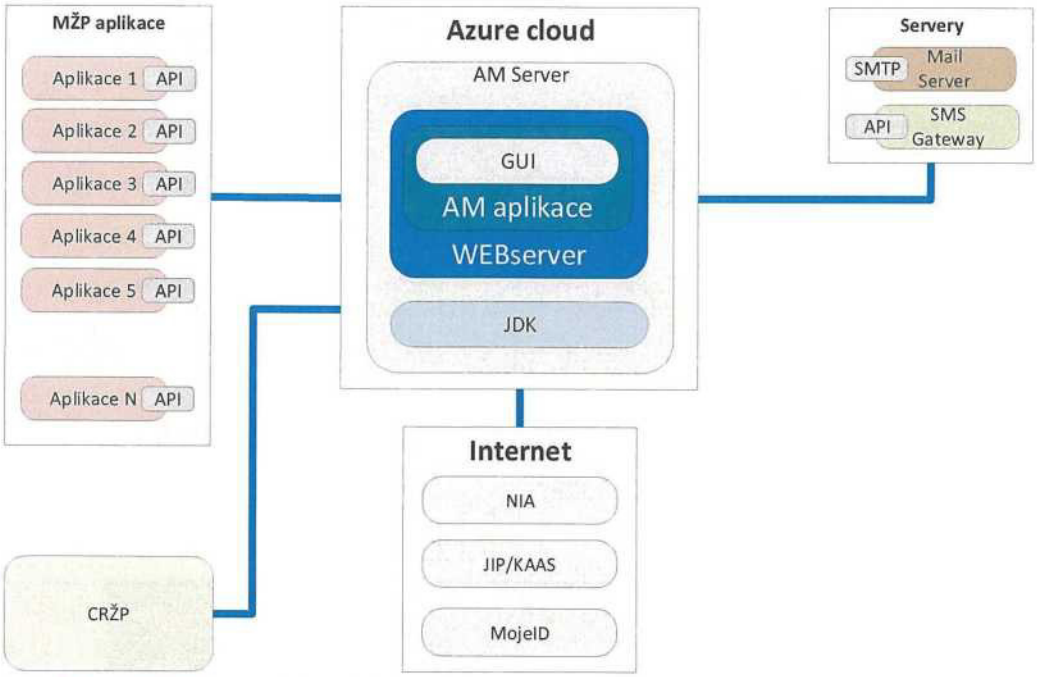


Obrázek 3 EnvilAM IDM - architektonický model

3.1.2 Infrastrukturní model AM

Infrastrukturní model EnvilAM AM ukazuje předpokládané propojení IS a komponent architektury:

- AM server je umístěn v cloudu
- slouží jako service provider pro externí IdP
- slouží jako IdP pro aplikace MŽP
- využívá CRŽP jako autentizační repozitář
- OTP je zasílán přes SMS nebo email



Obrázek 4 EnvilAM AM - architektonický model

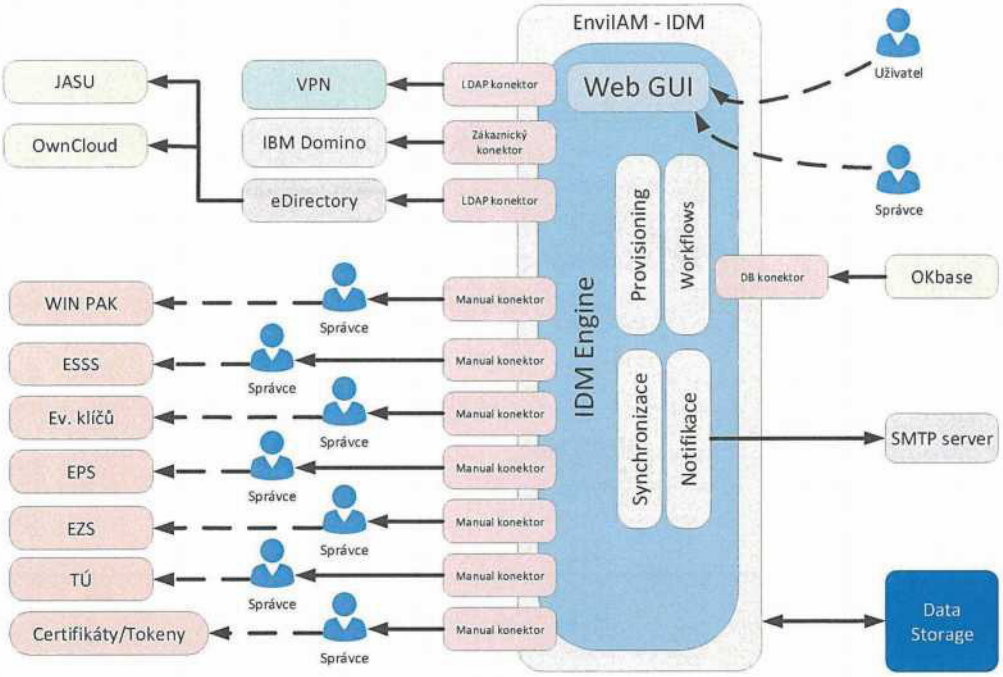
AM server sestává z těchto komponent:

- Azure service virtual serveru
- Java JDK verze 11
- Apache Tomcat 9
- Apereo CAS 6
- PostgreSQL pro data storage

3.1.3 Aplikační model IDM

Aplikační model EnvilAM IDM zobrazuje toky dat:

- data IDM jsou uložena v datovém úložišti (repositáři)
- IDM načítá data z autoritativního zdroje interních identit, OKbase
- jsou volány online systémy přes odpovídající konektory pro řízení účtů identit
- JASU a OwnCloud jsou řízeny nepřímo přes eDirectory pomocí rolí
- SMTP server je používán pro mailové notifikace
- správci off-line systémů na základě požadavků v IDM modifikují off-line systémy
- správci a uživatelé používají rozhraní IDM

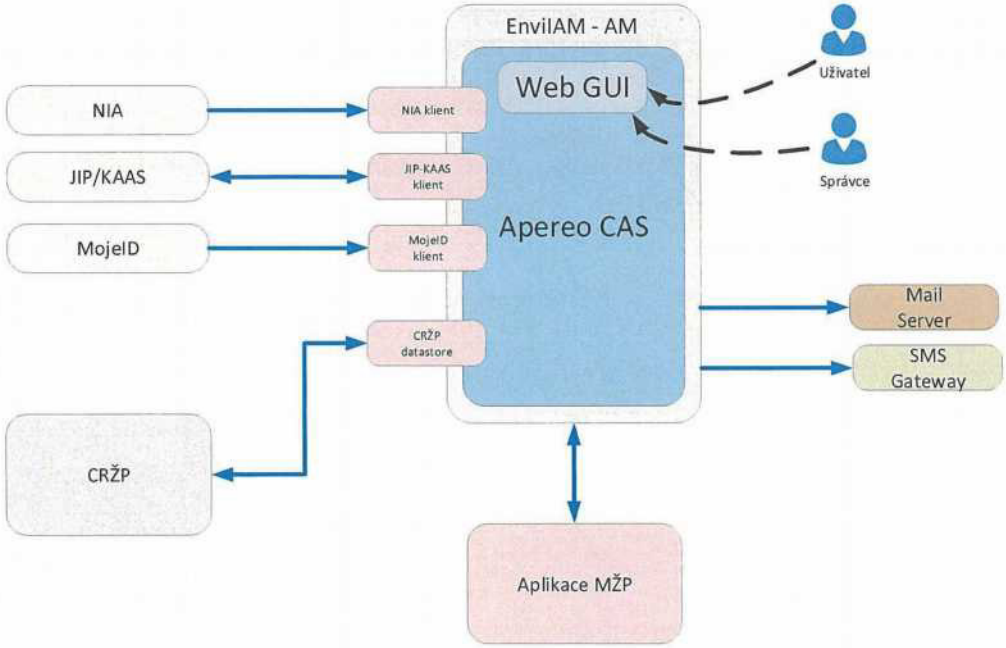


Obrázek 5 EnvilAM AM - aplikační model

3.1.4 Aplikační model AM

Aplikační model EnvilAM AM zobrazuje toky dat:

- autentizační údaje jsou uloženy v CRŽP DB
- po autentizaci externími IdP jsou uživatelé identifikováni v AM
- můžou jim být zaslán druhý faktor přes email nebo SMS
- aplikacím MŽP je na vyžádání zasílán profil uživatele z CRŽP DB
- správci a uživatelé využívají rozhraní AM

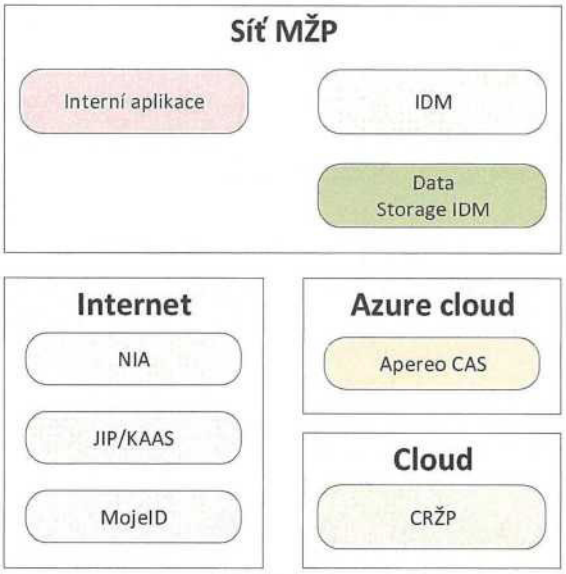


Obrázek 6 EnvilAM IDM - aplikační model

3.1.5 Model okolí EnvilAM

Model okol EnvilAM ukazuje zasazení EnvilAM do ICT prostředí:

- IDM je i se svým datovým repositářem umístěno do interní sítě
- AM je umístěno v cloudovém prostředí Azure



Obrázek 7 EnvilAM - model prostředí

3.2 SYSTÉMOVÉ A KAPACITNÍ POŽADAVKY

Systémové a kapacitní požadavky ve vazbě na aplikační model jsou plněny dle následujících kapitol takto:

- Access Manager: HW i SW zajišťuje Dodavatel
- Identity Manager: HW zajišťuje Zadavatel, SW zajišťuje Dodavatel
- Monitorovací server: HW zajišťuje Zadavatel, SW zajišťuje Dodavatel

3.2.1 Access Manager

Server pro Access Manager bude provozován námi na platformě Microsoft Azure. Je navržen 1 server, s vysokou dostupností a balancingem zajištěným cloudovou platformou.

Tabulka 2 - Access manager

Položka	Testovací prostředí	Produkční prostředí
Počet serverů	1 server	1 server
Typ serveru	Aplikační	
CPU [jádro]	4 jádra	4 jádra
Paměť [GB]	8 GB	16 GB
Disky [GB, IOPS]	72 GB, 25 000 IOPS (SSD)	128 GB, 25 000 IOPS
Operační systém	CentOS 7.7	
Aplikace	Apereo Central Authentication Server 6	

3.2.2 Identity Manager

Servery pro Identity Manager budou zajištěny Zadavatelem v prostředí Zadavatele:

- Jsou navrženy 2 servery pro vlastní Aplikaci v souladu s požadavky Zadavatele, s vysokou dostupností a balancingem zajištěným Zadavatelem.
- Dále je navržen 1 server pro databázi – repositář Aplikace.

Tabulka 3 - Identity manager (aplikační server)

Položka	Testovací prostředí	Produkční prostředí
Počet serverů	2 servery	2 servery
Typ serveru	Aplikační	
CPU [jádro]	4 jádra	16 jader
Paměť [GB]	16 GB	32 GB
Disky [GB, IOPS]	50 GB, 25 000 IOPS (SSD)	100 GB, 25 000 IOPS
Operační systém	CentOS 7.7	
Aplikace	MidPoint 4.x	

Tabulka 4 - Identity manager (databázový server)

Položka	Testovací prostředí	Produkční prostředí
Počet serverů	1 server	1 server
Typ serveru	Databázový	

CPU [jádro]	4 jádra	4 jádra
Paměť [GB]	24 GB	32 GB
Disky [GB, IOPS]	32 GB, 25 000 IOPS (SSD)	100 GB, 25 000 IOPS
Operační systém	CentOS 7.7	
Aplikace	PostgreSQL 11	

3.2.3 Monitorovací server

Pro splnění požadavků Zadavatele pro nepřetržitý monitoring řešení bude nasazen monitorovací server. Server poběží na HW prostředcích Zadavatele, s vysokou dostupností zajištěnou Zadavatelem.

Tabulka 5 - Monitorovací server

Položka	Testovací prostředí	Produkční prostředí
Počet serverů	1 server	1 server
Typ serveru	Monitorovací	
CPU [jádro]	4 jádra	4 jádra
Paměť [GB]	4 GB	16 GB
Disky [GB, IOPS]	32 GB	32 GB
Operační systém	CentOS 7.7	
Aplikace	Nagios XI	

3.3 POPIS ŘEŠENÍ

Kapitola obsahuje popis řešení pro EnvilAM. Předpokládá se, že řešení bude fungovat podle popisu v Zadávací dokumentaci. Tato kapitola tedy nepopisuje celé řešení, ale pouze upřesňuje některé oblasti, které Dodavatel považoval za přínosné dodefinovat. Pokud Zadávací dokumentace či tato nabídka některou funkci či vlastnost řešení explicitně neuvádí, bude toto dodáno ve výchozím (out-of-the-box) chování použitého produktu AM či IDM. Dodavatel nepředpokládá úpravu zdrojových kódů použitých produktů v těch částech, které jsou tvořeny výrobci produktu. Tímto přístupem zajišťujeme Zadavateli vysokou míru servisovatelnosti řešení a snazší povyšování verzí.

3.3.1 EnvilAM AM

Níže je uveden strukturovaný popis navrhovaného řešení EnvilAM AM, které bude realizováno konfigurací a customizací produktu Apereo CAS. Navrhované řešení bude dále rozpracováno a upřesněno v rámci fáze Analýza a návrh.

3.3.1.1 Odezva nasazené služby

Odezva nasazené služby bude měřena z monitorovacího serveru pomocí dohodnutých testovacích scénářů. Od tohoto času je zapotřebí odečíst faktory, které jsou mimo působnost Dodavatele – odezvu infrastruktury Zadavatele a případně také systémů, jejichž nasazení či úpravu neprovádí Dodavatel. V případě Apereo CAS je tedy zapotřebí odečíst odezvu externích identity providerů, databázového serveru CRŽP a chráněných aplikací.

3.3.1.2 Příručka pro připojení budoucího AIS

Součástí dodaného řešení bude příručka popisující připojení nové AIS k Apereo CAS – popis konfigurace Apereo CAS a úpravy nově připojované AIS.

3.3.1.3 Napojení na CRŽP DB

Vzhledem k tomu, že Apereo CAS bude přístupný z extranetu a bude umístěn v Azure, je zapotřebí zajistit Zadavatelem zabezpečené spojení s dB CRŽP. Dle informace Zadavatele je dB CRŽP umístěn v cloudovém prostředí. Předpokládáme proto přímé napojení z AM na CRŽP dB na úrovni cloud-

cloud. Očekáváme zde od Zadavatele zajištění součinnosti Dodavatele CRŽP dB pro potřeby napojení.

3.3.1.4 Branding

Úprava grafického rozhraní Apereo CAS bude spočívat v přidání loga Zadavatele a úpravy barvy pozadí stránky tak, aby Apereo CAS zapadal do portfolia aplikací Zadavatele.

3.3.1.5 Napojení na externí identity providery

Propojení Apereo CAS s identity providery bude realizováno pomocí standardizovaných protokolů, resp. ovladačů (handlerů) dodávaných společně s Apereo CAS: NIA - SAML2, JIP-KAAS – klient SOAP 1.1, mojeID - OpenID Connect. Do grafického rozhraní Apereo CAS budou doplněna tlačítka umožňující uživateli využití libovolného z podporovaných identity providerů. Uživatel má též možnost se přihlásit jménem a heslem, které Apereo CAS ověřuje v databázovém serveru CRŽP.

3.3.1.6 Konfigurace autentizace a autorizace chráněných aplikací

Součástí dodávky bude konfigurace profilů služby pro chráněné aplikace ISPOP2 a CRŽP umožňující nastavení autentizace, MFA a vracených atributů.

3.3.1.7 Single Logout

Dodavatel provede konfiguraci Single Logout (SLO) na úrovni Apereo CAS. Apereo CAS bude v SLO nastavení notifikovat veškeré chráněné aplikace o neplatnosti SSO session. Zodpovědností chráněné aplikace je zareagovat na takovou notifikaci zničením své vlastní session s přihlášeným uživatelem – nezbytné úpravy chráněné aplikace budou provedeny v gesci Zadavatelem. Výše uvedenou konfigurací je zajištěna konzistence v přihlášení/odhlášení.

3.3.1.8 Napojení na Legacy Architekturu

V současné době jsou uvažovány následující dvě varianty:

- **Varianta A**, ve které je kompatibilita s Legacy Architekturou zajištěna napojením Legacy SSO na dB CRŽP – konfiguraci Legacy Architektury provádí Zadavatel.
- **Varianta B**, ve které je kompatibilita s Legacy Architekturou zajištěna napojením Legacy SSO na Apereo CAS. Toto znamená oproti *Variantě A* potřebu dodatečné konfigurace Legacy SSO (vytvoření federace – konfiguraci provádí Zadavatel) a Apereo CAS – konfigurace dalšího profilu služby pro chráněné legacy aplikace.

Přesto i v rámci fáze detailní analýzy a návrhu se může objevit další varianta, která bude splňovat požadavky Zadavatele lépe. Nejvhodnější varianta bude vybrána po diskuzi se Zadavatelem a vzájemném odsouhlasení.

3.3.1.9 MFA ověření

OTP přes SMS bránu bude realizováno přes standardní http SMS bránu Zadavatele s ověřením typu Basic Access Authentication – v rámci http požadavku jsou odesílány také autentizační informace (jméno a heslo). Konfiguraci SMS brány provádí Zadavatel.

OTP přes email bude realizováno zasláním emailu přes SMTP server Zadavatele (konfiguraci SMTP serveru provádí Zadavatel) pomocí Javového emailového klienta.

MFA ověření pomocí certifikátu bude realizováno tlačítkem, které po kliknutí (pokud má uživatel importován ve webovém prohlížeči příslušný certifikát) vyvolá modální okno webového prohlížeče s potvrzením použití příslušného certifikátu.

3.3.1.10 Řešení migrace

Apereo CAS bude konfigurován tak, aby bylo MFA ověření aktivováno od určitého data. Dále bude vytvořena vlastní zpráva, která bude reagovat na existenci/neexistenci atributů potřebných pro MFA. Uživatel tak bude s patřičným předstihem informován o tom, že je zapotřebí doplnit příslušné atributy.

3.3.1.11 Evidence posledního času přihlášení uživatele

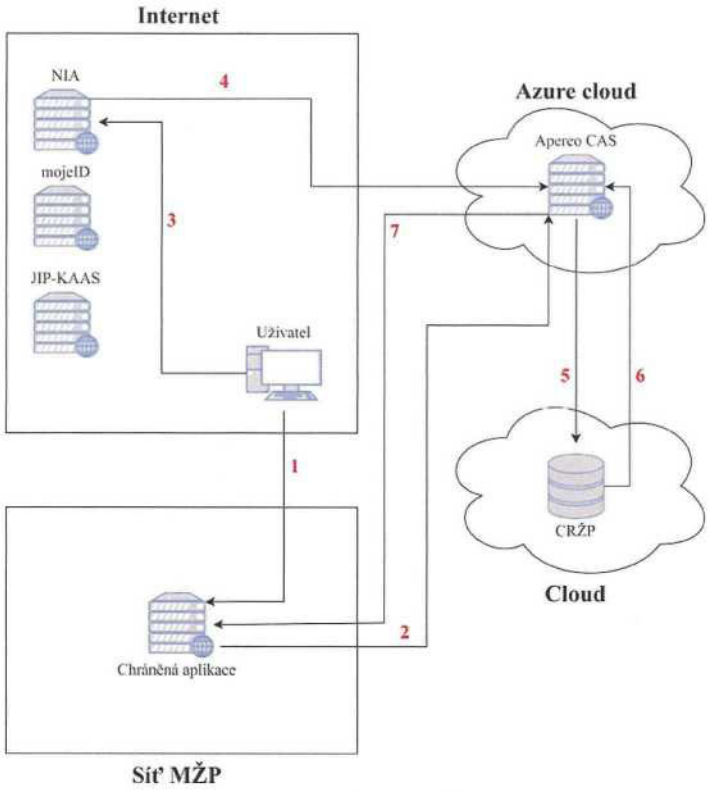
Apereo CAS umožňuje ukládání autentizačních událostí. Apereo CAS bude nakonfigurován tak, aby ukládal do databáze záznam o přihlášení uživatele, který se bude skládat z unikátního identifikátoru uživatele, unikátního identifikátoru AIS a času přihlášení.

3.3.1.12 Logování

Logy aplikace Apereo CAS budou umístěny na souborovém systému serveru, na kterém je Apereo CAS nasazen. K efektivnímu vyhledávání v uložených souborech s logy budou využívány produkty dodávané společně s OS (např. příkaz less) nebo open-source produkty třetích stran (např. vim).

3.3.1.13 Datový tok

Na Obrázek 8 je znázorněn příklad datového toku pro případ, že se uživatel přihlašuje do aplikace pomocí externího Identity Providera.



Obrázek 8 - Datový tok AM

Níže jsou popsány jednotlivé kroky:

1. Uživatel se pokusí přistoupit k aplikaci – neautorizovaný přístup.
2. Uživatel je přesměrován na Apereo CAS server.
3. Uživatel vybere autentizaci pomocí NIA.
4. Uživatel zadá své přihlašovací údaje, NIA provede autentizaci a výsledek je společně s informacemi o profilu vrácen zpět na Apereo CAS server. Apereo CAS server vytvoří session uživatele a přesměruje uživatele zpět do aplikace. Aplikace vytvoří místní session pro identitu a dotáže se Apereo CAS serveru na profil uživatele.
5. Apereo CAS server se dotáže dB CRŽP na doplňující údaje o uživateli, např. role.
6. Doplňující údaje jsou vráceny Apereo CAS serveru.
7. Apereo CAS server zformuje odpověď do uživatelského profilu. Profil identity je vrácen zpět do chráněné aplikace. Aplikace na základě těchto informací nastaví příslušná oprávnění, která uživateli náleží.

3.3.2 EnvilAM IDM

Níže je uveden strukturovaný popis navrhovaného řešení EnvilAM IDM, které bude realizováno konfigurací a customizací produktu Evolveum midPoint (dále IDM). Navrhované řešení bude dále rozpracováno a upřesněno v rámci fáze Analýzy a Návrhu.

3.3.2.1 Odezva nasazené služby

Odezva nasazené služby bude měřena z monitorovacího serveru pomocí dohodnutých testovacích scénářů. Od tohoto času je zapotřebí odečíst faktory, které jsou mimo působnost Dodavatele – odezvu infrastruktury Zadavatele a případně také systémů, jejichž nasazení či úpravu neprovádí Dodavatel. V případě IDM je tedy zapotřebí od odezvy synchronních operací odečíst zejména odezvu koncových systémů, databáze a síťové infrastruktury.

3.3.2.2 Migrace stávajících uživatelů, rolí a jejich přiřazení

Zadavatel dodá export všech objektů v dostatečné kvalitě bez duplicit do strojově zpracovatelného formátu – např. XML, Json, CSV. Dodaný export bude poté zpracován Dodavatelem a převeden do nového IDM.

3.3.2.3 Vysoká dostupnost

Vysoká dostupnost bude řešena nasazením dvou uzlů IDM a jejich následnou konfigurací. Zajištění load balanceru a jeho konfigurace pro rozvažování zátěže bude provedena Zadavatelem (např. uživatel bude při přihlášení přesměrován na méně vytížený node).

3.3.2.4 Nastavení odesílání zpráv přes SMTP

Parametry SMTP serveru (jméno serveru, uživ. jméno/heslo) či více serverů lze nastavit pomocí grafického rozhraní IDM.

3.3.2.5 Branding

Do grafického rozhraní IDM bude přidáno logo Zadavatele a bude provedena změna barvy hlavičky tak, aby IDM zapadalo do portfolia aplikací Zadavatele.

3.3.2.6 Připojení koncových systémů

On-line systémy budou připojeny pomocí konektorů dodávaných společně s IDM (OKbase, eDirectory, VPN) nebo vytvořených na míru Dodavatelem (IBM Domino/Notes). Následně bude pro každý systém vytvořeno mapování, ve kterém budou specifikovány typy synchronizovaných objektů (např. role či identity), synchronizované atributy, směr synchronizace atd. Rekonciliace a případné další pravidelné úlohy budou prováděny pomocí periodicky se opakujících serverových úloh. V rámci dodávky budou připojeny 3 online systémy: OKbase, eDirectory a VPN.

V případě IBM Domino/Notes serveru je nezbytné, aby Zadavatel jako součinnost poskytl moderní technické rozhraní, volatelné z programovaného prostředí Java.

Autoritativním zdrojem identit, organizací a systemizovaných míst bude koncový systém OKbase – tento koncový systém je připojen v režimu pro čtení (read-only). Konzistence OKbase s případnými úpravami provedenými manuálně v IDM (změna organizačního zařazené např.) bude zajištěna Zadavatelem. Automatické synchronizace ve směru IDM → on-line koncové systémy se tedy netýkají OKbase.

Koncový systém OKbase bude reprezentován následujícími databázovými pohledy či tabulkami, které budou poskytnuty Zadavatelem:

- 1 pohled/tabulka pro uživatele,
- 1 tabulka/pohled pro organizace,
- 1 tabulka/pohled pro systemizovaná místa.

Off-line systémy nebudou fyzicky připojeny k IDM, budou mít všechny 1 stejný datový model a v IDM budou řízeny pomocí tzv. „případů" – work itemů. V IDM tedy budou pouze objekty, které budou off-line systémy reprezentovat, takže bude možné dohledat, kdo v nich má skutečně založený účet atd. V případě změny identity, která má účet v off-line systému bude v IDM vytvořen případ, kde bude řečeno, jakou změnu má administrátor off-line systému provést. Administrátor bude o vytvoření případu informován pomocí notifikace. Díky tomu mohou administrátoři udržovat identity v konzistentním stavu napříč všemi systémy Zadavatele. Na rozdíl od on-line systémů bude rekonciliace prováděna manuálně – požadovaný stav bude porovnán se stávajícím pomocí reportů. V rámci dodávky bude připojeno maximálně 6 off-line systémů, další si bude moci připojit Zadavatel svépomocí pomocí správců IDM. Případné natažení iniciálního stavu účtů off-line systémů do IDM provede Zadavatel ručně přiřazením rolí.

3.3.2.7 Vznik identity

Interní identity budou v IDM zakládány automaticky z koncového systému OKbase pomocí periodicky prováděných serverových úloh. IDM provede při založení interní identity následující kroky:

1. Ověření unikátnosti loginu.
    - Pokud je nalezena shoda s již dříve použitým loginem, IDM o této skutečnosti notifikuje personální odbor a k založení identity nedochází.
2. Vygenerování iniciálního hesla dle nastavené bezpečnostní politiky – zasláno pomocí notifikace SMS či emailem uživateli.
3. Vygenerování unikátní emailové adresy (kontrola vůči alternativním emailům).

4. Přidělení základních zaměstnaneckých rolí – dojde ke spuštění schvalovacího workflow.
5. Upozornění nadřízeného pracovníka o založení nové identity pomocí notifikace, synchronizace do ostatních on-line systémů, administrátorům off-line systémů je zaslána notifikace o vytvoření případu.

Externí identity budou vytvářeny garantem externisty manuálně v IDM ve struktuře pro externisty (představuje smlouvy). Po vyplnění základních informací o externistovi jeho garantem provede IDM následující kroky:

1. Spuštění dvou-krokového schvalovacího workflow – 1. krok schvaluje garant, 2. krok schvaluje speciální role za smluvní a právní oblast.
2. V případě schválení je provedeno vygenerování unikátního loginu, unikátní emailové adresy (kontrola vůči alternativním emailům) a iniciálního hesla dle nastavené bezpečnostní politiky – zasláno pomocí notifikace SMS či emailem uživateli.
3. Vytvoření externí identity – synchronizace do on-line systémů, administrátorům off-line systémů bude zaslána notifikace o vytvoření případu.
4. Notifikování garanta externisty o jeho založení.

Technické identity budou vytvářeny manuálně pověřenou osobou přímo v IDM. Po vyplnění základních informací o technické identitě pověřenou osobou provede IDM následující kroky:

1. Vygenerování iniciálního hesla dle nastavené bezpečnostní politiky – zasláno pomocí notifikace emailem uživateli.
2. Vytvoření technické identity – synchronizace do on-line systémů, administrátorům off-line systémů bude zaslána notifikace o vytvoření případu.
3. Notifikování garanta technické identity o jejím založení.

Pro veškeré uvedené typy identit platí, že maximální počet přidaných zákaznických atributů je 10.

Hesla budou generována podle sady předem vytvořených bezpečnostních politik, jejichž specifikace bude dodána Zadavatelem. Hesla interních identit synchronizovaných z on-line systému OKbase budou generována podle stanovené výchozí bezpečnostní politiky. Heslo bude možné v případě potřeby přegenerovat uživatelem s příslušnými oprávněními stejným způsobem jako u externích a technických identit.

3.3.2.8 Aktualizace identity

V případě interních identit jsou manuálně provedené změny (kromě jména a příjmení – dostupná pouze pro externí identity) v IDM propagovány okamžitě do všech připojených on-line koncových systémů (kromě OKbase – konzistenci zajišťuje zadavatel), administrátorům off-line systémů bude zaslána notifikace o vytvoření případu. Při změně interní identity v OKbase je tato změna automaticky propagována do ostatních připojených on-line koncových systémů v rámci periodicky prováděné serverové úlohy, administrátorům off-line systémů bude zaslána notifikace o vytvoření případu. Pokud je v OKbase změněno jméno a příjmení, IDM provede přegenerování (včetně kontroly unikátnosti) loginu a emailové adresy (stará emailová adresa je uložena v IBM Notes/Domino jako alternativní emailová adresa).

V případě externí či technické identity lze změny provádět pouze manuálně v IDM, včetně manuální změny jména a příjmení. Manuálně provedené změny jsou okamžitě propagovány do všech připojených on-line koncových systémů (kromě OKbase), administrátorům off-line systémů bude zaslána notifikace o vytvoření případu.

3.3.2.9 Řízení životního cyklu identity

Platnost bude u interních identit řízena automaticky, nicméně administrátorovi bude umožněno změnit stav identity i manuálně v IDM, u externích identit bude platnost řízena pouze manuálně v IDM garantem daného externisty. V on-line systémech bude identita zneplatněna. V případě off-line systémů bude pro změnu platnosti vždy vytvořen příslušný případ, který bude realizovat administrátor daného off-line systému. O ukončení platnosti identity bude daný uživatel informován pomocí notifikace.

Zánik interní identity je indikován koncovým systémem OKbase ukončením pracovního vztahu zaměstnance, v případě externí identity je řízen z IDM platností identity. V případě zániku identity provede IDM změnu hesla na náhodné (propagováno do připojených on-line systémů, vytvoření příslušného případu pro off-line systémy), nastaví platnost identity i jí přiřazených rolí na D+30 a zašle notifikace požadované Zadavatelem pro konkrétní typ identity. Toto je možné provést také manuálně administrátorem z grafického rozhraní IDM. V případě manuálního zneplatnění provede administrátor

IDM následující úkony: změnu hesla na náhodné, zneplatnění identity, nastavení platnosti identity a přiřazených rolí na D+30.

Archivace identit bude řešena pomocí periodické serverové úlohy, která projde všechny identity s exspirovanou platností, nastaví jejich status na „Archivovaný", odebere jim veškeré přiřazené role a oprávnění v připojených on-line systémech a v IDM a provede vyčištění osobních dat identity (odstranění, anonymizace a stanovení účelu dalšího uchování a jejich ponechání). U off-line systémů bude archivace řešena vytvářením příslušných casů, které budou realizovány jejich administrátory. Na administrátora jde také požadavek na nastavení emailové schránky identity na neaktivní. Další detaily archivace dopřesní fáze Analýza a návrh.

3.3.2.10 Změna hesla

U připojených on-line systémů bude provedena změna hesla automaticky pomocí mapování prakticky okamžitě – záleží pouze na odezvě koncového on-line systému.

3.3.2.11 Reset hesla

Reset hesla samotným uživatelem bude realizován pomocí odkazu „Zapomenuté heslo" na přihlašovací obrazovce. Uživateli bude na email zaslán odkaz pro reset hesla a po kliknutí na odkaz mu bude automaticky vygenerováno nové heslo, které mu přijde zpátky na email. Řešení lze realizovat pouze za předpokladu, že autentizace je realizována přímo proti repositáři IDM.

Reset hesla garantem uživatele či administrátorem bude řešen pomocí atributu identity „Resetovat heslo – Ano/Ne". Po volbě „Ano" se vygeneruje nové heslo a odešle na email či SMS. Vygenerované heslo přepisuje aktuální.

3.3.2.12 Řízení rolí

Role budou vytvářeny v systému IDM *Metodikem* a nebudou synchronizovány do žádného systému jako objekty. Synchronizována budou pouze přiřazení rolí. Role budou členěny do dvou kategorií – business a aplikační.

Pro aplikační a business role platí, že maximální počet přidaných zákaznických atributů je 10. Verzování rolí zajišťuje procesně Zadavatel.

U jednotlivých rolí budou dle požadavků Zadavatele nastavena pravidla pro vzájemně vylučující se role – Segregation of Duties (SoD).

Jednotlivá přiřazení uživatel-role a business role-aplikační role bude možné recertifikovat. Součástí řešení bude

- 1 šablona certifikační kampaně pro recertifikaci přiřazení uživatel-role,
- 1 šablona certifikační kampaně pro recertifikaci přiřazení business role-aplikační role.
- Každá z těchto šablon bude obsahovat 2 úrovně ověření: vedoucí pracovník a garant role.

3.3.2.13 Organizační struktura

Strom organizační struktury a systemizovaných míst bude synchronizovat IDM z on-line koncového systému OKbase. IDM bude dále provádět kontrolu a čištění tzv. mrtvých referencí – přiřazení již neexistující organizace. Kontrola a čištění bude prováděno pomocí periodické serverové úlohy.

3.3.2.14 Autorizační role – přístupová oprávnění

Přístupová oprávnění v rámci IDM budou konfigurována pomocí tzv. autorizačních rolí, kterých bude vyhotoveno maximálně 9. V těchto rolích je definováno, co může uživatel v grafickém rozhraní vidět a jaké úkony může provádět.

3.3.2.15 Registrace a přihlášení uživatele

Aplikace umožňuje samo-registraci nových uživatelů pomocí konfigurace výchozích vlastností produktu midPoint. Konfiguraci provádí Zadavatel.

IDM podporuje SSO, nicméně to není součástí dodávky. Uživatel se bude autentizovat přímo proti repositáři IDM.

3.3.2.16 Logování

Logování přihlašování a odhlašování ke všem účtům (i neexistujících účtů), a to včetně neúspěšných pokusů, lze realizovat pouze za předpokladu, že autentizace je realizována přímo proti repositáři IDM.

IDM generuje a aktivně posílá auditní logy ve formě Syslog na aplikační server IDM (CEF formát), odkud jsou směrovány do SIEM na Zadavatelem definovanou IP adresu a port. Systém SIEM pak bude nakonfigurován Zadavatelem.

3.3.2.17 Workflow

Jednotlivé schvalovací úrovně workflow bude možné u jednotlivých rolí vypínat/zapínat přímo v grafickém rozhraní IDM. Tato funkcionalita bude samozřejmě dostupná pouze uživatelům s dostatečným oprávněním. Workflow bude realizováno v Zadavatelem požadované granularitě – maximálně 6 schvalovacích úrovní.

IDM umožní schvalovateli v průběhu schvalování požadavku doplnit maximálně 2 zákaznické atributy – např. číslo místnosti, telefonní číslo atd.

3.3.2.18 Notifikace

V rámci řešení bude vyhotoveno 12 šablon notifikací. Toto by mělo pokrýt všechny notifikace požadované Zadavatelem.

3.3.2.19 Audit a reporting

Auditní logy k jednotlivým objektům lze dohledat přímo v grafickém rozhraní IDM, po kliknutí na libovolný typ objektu. Oprávněnému uživateli je umožněno filtrování změn a také zobrazení podrobností o změně v XML formátu.

Z výše uvedených auditních logů lze vytvářet rozsáhlé reporty v Zadavatelem požadované míře detailu (např. kompletní informace o operacích s identitami) – reporty lze spouštět z grafického rozhraní (záložka „Reporty") či periodicky pomocí serverových úloh např. se zasíláním vytvořeného reportu v zipu na email.

Uživatelský report může mít i formu strukturovaného zobrazení v grafickém uživatelském rozhraní Identity manageru – midPointu.

Rekonciliační reporty týkající se uživatelských účtů jsou dodávány společně s IDM v rámci jediného reportu, který lze parametrizovat (volba konkrétního koncového systému, zobrazení pouze účtů bez vlastníka atd). Report umožňující výpis chronologického seznamu akcí nad koncovým systém bude doprogramován Dodavatelem IDM.

Recertifikační reporty umožňují zobrazení kampaní, jejich stavu a rozhodnutí ověřovatelů v jednotlivých fázích kampaně.

Reporty o uživatelích a rolích umožňují zobrazení organizační struktury a rolí společně s přiřazenými identitami (přímo i nepřímo). Dále budou dodány následující reporty:

- Report identit s filtrováním dle kritérií.
- Manažerský report podřízených identit exspirujících na konci daného měsíce.
- Kontrola konzistence datového modelu Aplikace – primárně pro vyhledávání chyb (např. role má neplatného vlastníka, manažer je neplatný atd., příjemcem je Metodik).

Kontrolní export rolí – kontrola správnosti přiřazení aplikačních rolí do business rolí, kontrola atributů rolí (schvalovatelé atd.).

Reporting konfliktních práv (rolí) u uživatelů bude realizován na základě nastavených SoD u jednotlivých rolí. Pokud má tedy uživatel např. přiřazené 2 role, které se vzájemně vylučují, bude tento stav reportován.

3.3.3 Analýza a návrh

V rámci analýzy procesů bude prozkoumáno těchto 8 procesů:

- Vznik identity
- Aktualizace identity
- Změnu hesla v On-line i Off-line systémech
- Reset hesla
- Řízení rolí – oprávnění
- Řízení platnosti identity
- Řízení zániku identity
- Archivaci identity

Pro každý proces proběhnou maximálně 2 workshopy se Zadavatelem pro přesné popsání průběhu procesu.

Z analýzy a návrhu vznikne dokument o rozsahu do 50 stránek.

3.3.4 Dokumentace

Dokumentace komunikačního rozhraní bude popisovat rozhraní softwaru *Identity Manager* a *Access Manager*. Dokument nebude popisovat rozhraní napojených koncových systémů, toto je odpovědnost dodavatelů daných systémů a Zadavatele. Dokumentace komunikačního rozhraní však může tyto popisy obsahovat jako přílohu.

3.3.5 Testovací scénáře

Pro řešení EnvilAM IDM bude vytvořeno těchto 20 scénářů pokrývající typické use casy práce s IDM:

1. založení interní identity
2. založení externisty
3. založení technického účtu
4. aktualizace identity
5. změna hesla
6. reset hesla uživatelem
7. reset hesla garantem
8. samoregistrace uživatele
9. žádost o přiřazení role v online systému
10. žádost o přiřazení role v off-line systému
11. schvalování žádosti o roli
12. odebrání role
13. spuštění reportu
14. audit změn nad identitou
15. recertifikace obsahu role
16. napojení na SIEM
17. synchronizace stromu organizační struktury
18. synchronizace stromu systemizovaných míst
19. přidělování oprávnění dle systemizovaného místa
20. nastavení politiky hesla

Pro řešení EnvilAM AM bude vytvořeno těchto 6 scénářů pokrývající typické use casy práce s AM:

1. přihlášení uživatele jménem a heslem bez doplněných údajů pro OTP (přechodná doma)
2. přihlášení uživatele s OTP
3. přihlášení uživatele přes MojeID
4. přihlášení uživatele přes eIdentitu (NIA)
5. přihlášení uživatele přes JIP-KAAS
6. odhlášení uživatele

Na základě těchto scénářů bude vytvořen uživatelský manuál.

3.3.6 Školení

V rámci proškolení bude provedeno následující:

- proškolení k EnvilAM AM
  - 1 školení pro uživatele v rozsahu 2 hodin, maximálně 20 účastníků
  - 1 školení pro správce v rozsahu 2 hodin, maximálně 2 účastníci
- proškolení k EnvilAM IDM
  - 3 školení pro uživatele v rozsahu 4 hodin, maximálně 7 účastníků
  - 1 školení pro správce v rozsahu 4 hodin, maximálně 2 účastníci

4 POUŽITÉ SW PRODUKTY, LICENCE A MAINTENANCE

Přehled SW licencí					
	Všechny SW komponenty: - komerční SW - svobodný SW (opensource) - zadavatelem již vyvinutý SW, který bude customizován - programové části vyvíjené na míru pro zadavatele. Ke každé položce uveďte přesný popis **edice** a její nabízenou **verzi. Není-li daný typ SW součástí řešení – vyplňte „řešení neobsahuje“**	Licence: - přesný popis licence (předmět licence) - typ a vlastník licence (autorské dílo vybraného dodavatele, proprietární SW vybraného dodavatele, proprietární produkt 3. strany, opensource) - rozsah a omezení licence (tj. počet uživatelů, CPU, formulářů, sites, období/čas, zařízení, virtuální stroj, počet instalací, senzorů apod.).	Pořizovaná SW maintenance - přesný popis (co maintenance obsahuje). Pozn.: v případě nezakoupení SW maintenance tuto skutečnost uveďte a zdůvodněte s ohledem na požadavky na provozní podporu.	Podpora ze strany výrobce (i pro svobodný SW) s ohledem na udržitelný provoz.	Způsob lokalizace komponenty do českého jazyka.
Operační systém	CentOS 7.7 (build 1908)	Opensource – GNU Vlastník licence je Zadavatel, licence je bez omezení	Nepořizuje se, bezpečnostní updaty a aktualizace jsou dostupné bez potřeby zakoupení maintenance	Opravy chyb, bezpečnostní aktualizace	Nevyplňuje se
Databázový systém	PostgreSQL 11	Opensource – PostgreSQL License Vlastník licence je Zadavatel, licence je bez omezení	Nepořizuje se, bezpečnostní updaty a aktualizace jsou dostupné bez potřeby zakoupení maintenance	Opravy chyb, bezpečnostní aktualizace	Nevyplňuje se
Aplikační, webový server	Apache Tomcat 9	Opensource – Apache License 2.0 Vlastník licence je Zadavatel, licence je bez omezení	Nepořizuje se, bezpečnostní updaty a aktualizace jsou dostupné bez potřeby zakoupení maintenance	Opravy chyb, bezpečnostní aktualizace	Lokalizovány jsou komponenty (IDM/AM), které poběží na aplikačním serveru.
Formulářový systém	Řešení neobsahuje				
Vyhledávací systém	Řešení neobsahuje				

IDM	MidPoint 4.0	Opensource – Apache License 2.0. Vlastník licence je Zadavatel, licence je bez omezení	„Subscription" – obsahuje prioritní opravy chyb v produktu	Opravy chyb, bezpečnostní aktualizace	Celý produkt je již lokalizován do českého jazyka.
AM	Apereo CAS 6	Opensource – Apache 2.0 License Vlastník licence je Zadavatel, licence je bez omezení	Nepořizuje se, bezpečnostní updaty a aktualizace jsou dostupné bez potřeby zakoupení maintenance	Opravy chyb, bezpečnostní aktualizace	Celý produkt je již lokalizován do českého jazyka.
Process management	Řešení neobsahuje				
Portálová techn.	Řešení neobsahuje				
CMS, prezent. služby	Řešení neobsahuje				
Reporty, Bussiness Intelligence	Integrováno v rámci IDM – Jasper Reports. Viz položka IDM				
Integrační vrstva	Integrováno v rámci IDM – konektory. Viz položka IDM				
Helpdesk/ Servicedesk	Bugzilla	Mozilla Public License Vlastník licence je Zadavatel, licence je bez omezení	Nepořizuje se, bezpečnostní updaty a aktualizace jsou dostupné bez potřeby zakoupení maintenance	Opravy chyb, bezpečnostní aktualizace	Celý produkt je již lokalizován do českého jazyka.
Monitoring	Nagios XI	Nagios XI free license Vlastník licence je Zadavatel, licence je bez omezení	Nepořizuje se, bezpečnostní updaty a aktualizace jsou dostupné bez potřeby zakoupení maintenance	Opravy chyb, bezpečnostní aktualizace	----
Auditování	Integrováno v rámci IDM/AM.				
Zálohování	Řešení bude využívat zálohovací možnosti Zadavatele				
Testování	Řešení neobsahuje				
Zabezpečení	Integrováno ve všech výše uvedených produktech – např. Apache Tomcat (HTTPS), MidPoint (šifrování hesel, zabezpečené spojení s koncovými systémy – např. SSL)				

5 POPIS ZABEZPEČENÍ PODPORY PROVOZU (SERVIS) A ROZVOJE DÍLA

AMI Praha nabízí zajištění podpory provozu a rozvoje dle parametrů specifikovaných v Zadávací dokumentaci, konkrétně v rozsahu následujících služeb:

Služby podpory provozu

- KL_IAM_01 – Dostupnost a odezva EnvilAM
- KL_IAM_02 – Standardní podpora EnvilAM
- KL_IAM_03 – Podpůrné centrum (service desk a hot-line)
- KL_IAM_04 – Řízení vad (incidentů)
- KL_IAM_05 – Přesun díla
- KL_IAM_06 – Realizace exit plánu

Služba rozvoje

- KL_IAM_07 – Rozvoj EnvilAM

Personální zajištění
Za dodržení parametrů konkrétní servisní smlouvy je zodpovědný servisní manažer AMI. Ten typicky komunikuje s pracovníky Objednatele a předává požadavky k řešení konkrétním osobám z týmu specialistů AMI.

Eskalační úroveň tvoří account manager AMI, případně vedoucí servisních služeb AMI.

5.1 KL_IAM_01 – DOSTUPNOST A ODEZVA ENVIIAM

Služba bude pokrývat tento rozsah činností:

- monitoring dostupnosti a odezvy IdM a AM,
- garanci dostupnosti AM,
- garanci odezvy AM.

Monitoring dostupnosti a odezvy IdM bude prováděn nástrojem Nagios XI umístěném na samostatném monitorovacím virtuálním serveru.

Monitoring dostupnosti a odezvy AM bude prováděn interními nástroji cloudu MS Azure.

Zavazujeme se k plnění konkrétních parametrů služby, jak jsou uvedené v Zadávací dokumentaci.

Doplňující informace a bližší popis jsou uvedeny v kapitole 3.3.1.1 Odezva nasazené služby.

5.2 KL_IAM_02 – STANDARDNÍ PODPORA ENVIIAM

Služba bude pokrývat tento rozsah činností:

- zajištění cloudových služeb pro provoz AM vč. zálohování a případné obnovy ze záloh – provoz v cloudu MS Azure,
- SW údržba AM a IdM včetně jejich Technologických platforem dle požadavků uvedených v Příloze A – Specifikace služeb.

Zavazujeme se k plnění konkrétních parametrů služby, jak jsou uvedené v Zadávací dokumentaci v popisu služby KL_IAM_02.

Zálohování IdM bude prováděno zálohovacím nástrojem Objednatele (Veeam). Zálohování AM bude prováděno interními nástroji cloudu Azure, obojí v souladu s odsouhlasenou specifikací záloh.

Monitorování vnějších útoků pro AM, který bude dostupný z veřejného internetu, bude prováděn interními nástroji cloudu Azure.

Implementace updatů / bezpečnostních záplat některých komponent řešení nebo technologické platformy může vyžadovat krátkodobou odstávku AM nebo IdM. Toto bude vždy předem dohodnuto se Zadavatelem tak, aby byl minimální dopad do provozu řešení.

5.3 KL_IAM_03 – PODPŮRNÉ CENTRUM (SERVICE DESK A HOT-LINE)

Služba bude pokrývat tento rozsah činností:

- provoz Service Desku a Hot-line pro zadávání incidentů a požadavků Objednatele.

Centrálním místem pro zadávání a evidenci požadavků je service desk aplikace https://helpdesk.ami.cz, která je nepřetržitě dostupná z prostředí veřejného internetu.
V service desku se provádí kompletní evidence a správa požadavků, včetně řízení priorit, změn stavů, přidávání komentářů apod.
Do service desku je možné požadavky vkládat i posláním na dedikovanou e-mailovou adresu, stejným způsobem lze i přidávat komentáře.
Pro telefonické zadávání slouží telefonní linka 737 646 646 provozovaná v režimu 9x5 dle požadavků zadávací dokumentace. Během poskytování služby může být dle aktuálních potřeb počet telefonních linek rozšířen.

Všechny požadavky hlášené přes telefonickou hotline budou kvůli evidenci zadané do service desku.

5.4 KL_IAM_04 – ŘÍZENÍ VAD (INCIDENTŮ)

Služba bude pokrývat tento rozsah činností:

- odstranění vad vzniklých v dodaném díle nebo na technologické platformě s cílem udržování EnvilAM v řádném provozním stavu dle požadavků uvedených v Příloze A – Specifikace služeb, popis služby KL_IAM_04.

Incidenty jsou zadávány přes kanály služby Podpůrné centrum a veškerá další komunikace probíhá prostřednictvím aplikace Service Desk (https://helpdesk.ami.cz). Je potvrzeno převzetí incidentu a případně položeny doplňující dotazy, aby byla zajištěno co nejlepší vyhodnocení situace a navrženo vhodné řešení. Po analýze incidentu je Objednateli sdělen způsob a odhad doby provizorního a trvalého vyřešení.

Budou dodrženy lhůty pro odpověď i odstranění vad specifikované v Příloze A – Specifikace služeb, popis služby KL_IAM_04, část Způsob měření.

6 POPIS NAVRHOVANÝCH TECHNICKÝCH A ORGANIZAČNÍCH OPATŘENÍ DLE GDPR A ZPŮSOBU JEJICH NAPLNĚNÍ

Zpracovatel se zavazuje zejména, nikoliv však výlučně, že přijme následující organizační a technická opatření:

- Zpracovatel je držitelem platných certifikátů ISO 9001, 20000 a 27001
- Zpracovatel mé zpracované interní směrnice a bezpečnostní politiky pro nakládání s osobním údaji a tyto směrnice pravidelně školí
- pověří zpracováním Osobních údajů pouze své vybrané zaměstnance a subdodavatele, které poučí o jejich povinnosti zachovávat mlčenlivost ohledně Osobních údajů a o dalších povinnostech, které jsou povinni dodržovat tak, aby nedošlo k porušení ZOOÚ či jiných platných právních předpisů;
- bude používat odpovídající technické zařízení a programové vybavení způsobem, který vyloučí neoprávněný či nahodilý přístup k Osobním údajům ze strany jiných osob, než pověřených;
- bude Osobní údaje uchovávat v náležitě zabezpečených objektech a místnostech;
- Osobní údaje v elektronické podobě bude uchovávat na zabezpečených serverech nebo na nosičích dat, ke kterým budou mít přístup pouze pověřené osoby na základě přístupových kódů či hesel a bude Osobní údaje pravidelně zálohovat;
- zajistí dálkový přenos Osobních údajů buď pouze prostřednictvím veřejně nepřístupné sítě, nebo prostřednictvím zabezpečeného přenosu po veřejných sítích, a to v souladu s dohodou se Správcem o úrovni daného zabezpečeného přenosu; nicméně způsob přenosu určuje Správce
- bude v co největší míře zpracovávat pouze pseudonymizované a šifrované Osobní údaje, je-li takové opatření vhodné a nezbytné ke snížení rizik plynoucích ze zpracování Osobních údajů; nicméně za stav předávaných Osobních údajů je zodpovědný Správce
- zajistí neustálou důvěrnost, integritu, dostupnost a odolnost systémů a služeb zpracování;
- prostřednictvím vhodných technických prostředků zajistí schopnost obnovit dostupnost Osobních údajů a přístup k nim včas v případě fyzických či technických incidentů;
- zajistí pravidelné testování posuzování a hodnocení účinnosti zavedených technických a organizačních opatření pro zajištění bezpečnosti zpracování; a
- při ukončení zpracování Osobních údajů zajistí Zpracovatel dle dohody se Správcem fyzickou likvidaci Osobních údajů, nebo tyto Osobní údaje předá Správci;
- v případě, že Osobní údaje jsou uloženy u Správce nebo u jiného Zpracovatele, je za uchování, ochranu, bezpečnost, dostupnost, obnovu a likvidaci zodpovědný Správce;
- Zpracovatel rozvíjí a aktualizuje systém Správce, není jeho administrátor. Rozvoj systému provádí na základě žádostí Správce. Správce zpracovává v systému zapsané osobní údaje sám přes administrativní rozhraní. Způsob zobrazování Osobních údajů v systému a způsob jejich přenosu určuje Správce.
- Správce si je vědom, že veškeré Osobní údaje v systému jsou na základě jeho požadavku nešifrované a neanonymizované.
- Zpracovatel nenese žádnou zodpovědnost za ztrátu nebo únik Osobních údajů přes administrační rozhraní systému zaviněný činností Správce, nebo jiných jeho subdodavatelů (např. nedodržení technických požadavků, ztráta či prozrazení hesla, nevhodné nastavení přenosu, nezabezpečený hosting, atp.).

7 ZPŮSOB ZAJIŠTĚNÍ INFRASTRUKTURNÍCH SLUŽEB (CLOUD) PRO ENVIIAM – AM

EnvilAM AM bude nasazeno v prostředí cloudových služeb **Microsoft Azure** - https://azure.microsoft.com/.

Microsoft Azure je neustále se rozšiřující sada cloudových služeb, které pomáhají organizacím překonávat překážky v podnikání. Nabízejí svobodu při sestavování, správě a nasazování aplikací v rozsáhlé globální síti pomocí oblíbených nástrojů a architektur.

Bezpečnost

Platforma Azure obsahuje integrované zabezpečení a ochranu osobních údajů. Microsoft klade důraz na nejvyšší úroveň důvěry, transparentnosti, dodržování norem a zákonných předpisů prostřednictvím nejširší nabídky produktů pro dodržování předpisů ze všech poskytovatelů cloudových služeb.

Rozšířenost

Své podnikání svěřilo platformě Microsoft Cloud devadesát pět procent společností z žebříčku Fortune 500.

Podpora technologií

Azure podporuje technologie open source, takže lze používat rozličné oblíbené nástroje a technologie. Prakticky jakoukoli aplikaci lze spustit s využitím vlastního zdroje dat, na svém operačním systému a ve svém zařízení.

Porovnání s jinými cloudy

Azure je jediný konzistentní hybridní cloud, nabízí víc oblastí než jakýkoli jiný poskytovatel cloudu, umožňuje vyšší produktivitu vývojářů a má širší pokrytí v oblasti dodržování předpisů, včetně vyhovění požadavkům obecného nařízení o ochraně osobních údajů (GDPR). Viz např Azure versus AWS - https://azure.microsoft.com/cs-cz/overview/azure-vs-aws/.

8 STRUČNÝ POPIS POSTUPU ŘEŠENÍ PŘESUNU DÍLA

8.1 ENVIIAM IDM

V případě přesunu EnvilAM IDM na jinou HW platformu je třeba dodržet tento postup:

1. instalace prostředí po úroveň aplikačního serveru dle dodaných instalačních postupů
2. zajištění prostupů mezi komponentami řešení dle dodané dokumentace prostupů
3. v případě cloudu zajištění viditelnosti z cloud prostředí do prostředí Zadavatele
4. nasazení vlastního řešení dle dodané dokumentace
5. odpojení připojených systémů od dosavadního řešení a připojení k novému
6. přesměrování adresy pro koncové uživatele v DNS
7. zajištění zálohování v novém úložišti
8. vypnutí překonaného řešení

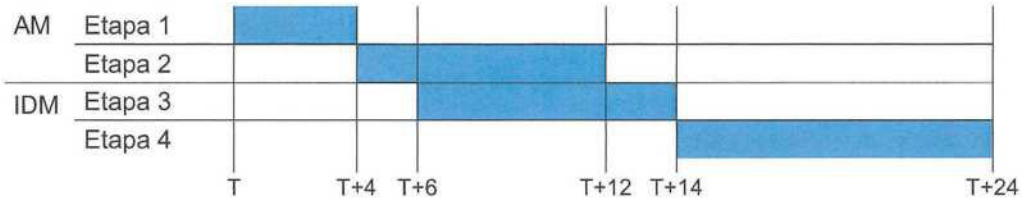
8.2 ENVIIAM AM

V případě přesunu EnvilAM AM na jinou HW platformu je třeba dodržet tento postup:

1. instalace prostředí po úroveň aplikačního serveru dle dodaných instalačních postupů
2. zajištění prostupů mezi komponentami řešení dle dodané dokumentace prostupů
3. nasazení vlastního řešení dle dodané dokumentace
4. napojení na externí IdP – může vyžadovat delší čas na administrativu
5. přepojení aplikací, využívajících A/A služby EnvilAM AM
6. přesměrování adresy pro koncové uživatele v DNS
7. zajištění zálohování v novém úložišti
8. vypnutí překonaného řešení

9 ČASOVÝ RÁMEC PLNĚNÍ VEŘEJNÉ ZAKÁZKY

Níže je uveden orientační harmonogram prací, který bude dále rozpracován a upřesněn v rámci Analýzy a Návrhu realizace jednotlivých částí Díla. Pro dodržení termínů uvedených v harmonogramu je nutnou prerekvizitou včasné splnění požadovaných součinností dle této nabídky. Některé kroky uvedené v harmonogramu níže mohou probíhat souběžně. Postup dodávky jednotlivých částí Díla je uveden na časové ose níže (T – zahájení projektu / den účinnosti smlouvy; termíny uvedeny v měsících).



9.1 PRVNÍ ČÁST DÍLA (ENVIIAM – AM)

9.1.1 Etapa I – Analýza a Návrh Implementace

Krok	Popis	Odpovědnost	Termín (v měsících)
I.A	Zahájení projektu, den účinnosti smlouvy	Objednatel (O), Dodavatel (D)	T
I.B	Předání Prováděcího projektu k připomínkám	O	I.A + 1
I.C	Vypořádání připomínek k Prováděcímu projektu	O, D	I.B + 1
I.D	Akceptace Prováděcího projektu	O	I.B + 1
I.E	Předání Specifikace Díla k připomínkám	D	I.A + 3
I.F	Vypořádání připomínek ke Specifikaci Díla	O, D	I.E + 1
I.G	Akceptace Specifikace Díla (Etapy I)	O	I.E + 1
I.H	Fakturace Etapy I	D	I.E + 1

9.1.2 Etapa II – Dodávka a implementace

Krok	Popis	Odpovědnost	Termín (v měsících)
II.A	Zahájení Etapy II	O, D	I.G
II.B	Nasazení a konfigurace (TEST a PROD)	D	II.A + 2
II.C	Integrace a migrace (CRŽP, ISPOP v2, …)	D	II.B + 3
II.D	Školení uživatelů / administrátorů	O, D	II.C + 1
II.E	Akceptace Finálního testování	O, D	II.C + 2
II.F	Akceptace Dokumentace	O, D	II.C + 2
II.G	Akceptace SW Licencí, zdroj. kódů	O, D	II.E + 1
II.H	Ověření produkčního provozu	O	II.E + 1
II.I	Akceptace první části Díla (Etapy II)	O, D	II.E + 1
II.J	Fakturace první části Díla (Etapy II)	D	II.E + 1

9.2 DRUHÁ ČÁST DÍLA (ENVIIAM – IDM)

9.2.1 Etapa III – Analýza a Návrh Implementace

Krok	Popis	Odpovědnost	Termín (v měsících)
III.A	Zahájení Etapy III	O, D	T + 6
III.B	Předání Prováděcího projektu k připomínkám	O	III.A + 2
III.C	Vypořádání připomínek k Prováděcímu projektu	O, D	III.B + 1
III.D	Akceptace Prováděcího projektu	O	III.C + 1
III.E	Předání Specifikace Díla k připomínkám	D	III.D + 3
III.F	Vypořádání připomínek ke Specifikaci Díla	O, D	III.E + 1
III.G	Akceptace Specifikace Díla (Etapy III)	O	III.E + 1
III.H	Fakturace Etapy III	D	III.E + 1

9.2.2 Etapa IV – Dodávka a implementace

Krok	Popis	Odpovědnost	Termín (v měsících)
IV.A	Zahájení Etapy IV	O, D	III.G
IV.B	Nasazení a konfigurace (TEST a PROD)	D	IV.A + 3
IV.C	Integrace (OKbase, JASU, ...)	D	IV.B + 4
IV.D	Školení uživatelů / administrátorů	O, D	IV.C + 1
IV.E	Akceptace Finálního testování	O, D	IV.C + 2
IV.F	Akceptace Dokumentace	O, D	IV.C + 2
IV.G	Akceptace SW Licencí, zdroj. kódů	O, D	IV.E + 1
IV.H	Ověření produkčního provozu	O	IV.E + 1
IV.I	Akceptace druhé části Díla (Etapy IV)	O, D	IV.E + 1
IV.J	Fakturace druhé části Díla (Etapy VI)	D	IV.E + 1

10 ZHODNOCENÍ RIZIK REALIZACE VEŘEJNÉ ZAKÁZKY A MOŽNOSTI JEJICH SNÍŽENÍ/ŘEŠENÍ.

Po celou dobu trvání projektu bude probíhat identifikace možných rizik spolu s návrhy na jejich eliminaci či vypořádání. V souladu se zadáním bude detailní postup popsaný v Prováděcím projektu. Tabulka níže obsahuje obecná rizika, která mohou nastat v průběhu implementace projektu. Tento přehled nelze považovat za úplný a konečný seznam možných rizik. Seznam bude v průběhu projektu pravidelně aktualizován.

Možné riziko	Návrh eliminace / vypořádání
Závislost na jediném dodavateli – Vendor lock-in	Využití open-source nástrojů s dostatečným pokrytím potencionálních dodavatelů na českém trhu.
Nepřipravenost koncových systémů na připojení k IAM	Včasné předání požadovaných parametrů na interface. Včasné zajištění součinnosti Objednatele či dodavatelů připojovaných aplikací a provedení nutných úprav na koncových systémech.
Nedodání požadovaných součinností s dopadem na posun v harmonogramu	Včasné definování požadovaných součinností. Informování třetích stran o požadovaných součinnostech v dostatečném předstihu. Průběžný dohled nad plněním poskytovaných součinností.
Nedodržení lhůt pro předání připomínek k dokumentům či jejich zapracování.	Včasné informování o průběhu prací a plánovaných termínech předání. Plánování kapacit dle domluvených termínů. Termíny zohlednit na pracovní dny (mimo víkendů a státních svátků)
Neexistující vývojové instance připojovaných koncových systémů	Vytvoření vývojových instancí koncových systémů nebo alespoň dummy/mock interface
Neexistující testovací instance připojovaných koncových systémů	Vytvoření testovacích instancí koncových systémů
Nedostatečná kvalita dat v koncových systémech na testovacím/integračním prostředí	Zajištění reprezentativních dat v testovacím/integračním prostředí, aby byla relevantní s produkčními daty
Neochota správců/vlastníků systémů k připojení jejich systémů k IAM	Vysvětlení benefitů, zapojení do projektu
Alokace a spolupráce s třetími stranami při vývoji rozhraní koncových systémů	Zapojení do projektu, včasná komunikace
Nekontrolované/nehlášené změny v rozhraní koncových systémů a tím způsobená nefunkčnost integrace	Komunikace a schvalování úprav interfaces před zahájením implementace změn
Nemožnost vytvořit online konektor na koncovém systému	Připojení koncového systému v režimu read-only, offline nebo descope systému
Nedostatečná alokace klíčových členů projektového týmu, přetížení klíčových osob	Zajištění dostatečných alokací
Nedostupnost klíčových osob z důvodů organizačních změn či dovolených	Zajištění zastupitelnosti a sdílení know-how v průběhu celého projektu
Nejasné/neúplné zadání	Vyjasnění požadavků nejpozději ve fázi analýzy – Specifikace díla

Provádění změn dílčích částí Díla s odkazem na testování s dopadem na termín či cenu dodávky	Realizační fáze (zejména implementace, integrace, testování) bude probíhat důsledně dle Specifikace Díla. Všechny změny budou projednány v rámci změnového řízení.
Zásahy do Zdrojového kódu Objednatelem nebo třetí stranou ohrozí funkcionalitu Díla či jeho provoz a případnou obnovu	Změny ve Zdrojovém kódu bude provádět výhradně smluvní partner Objednatele, který má uzavřenou platnou smlouvu na Dodávku či provoz Díla
Nedostatečná distribuce informací	Předávání úplných a včasných informací mezi členy projektového týmu. Využití eskalačních mechanismů.
Legislativní změny (např. GDPR, ZoKB aktualizace)	Pravidelná revize legislativních změn ve vztahu k implementovanému řešení
Nemožnost nastavit VPN přístup a firewall prostupy na IAM a koncové systémy	Vhodné umístění všech částí do infrastruktury
Nenaplnění očekávání od nástroje IDM	Vyzkoušení dema produktu, diskuze nad splněním klíčových požadovaných funkcionalit
Nedodržení nejpozději přípustného konce projektu nebo jednotlivých milníků	Dodržení postupů odsouhlasených v rámci Prováděcího projektu – zejména průběžná kontrola stavu projektu, pružné poskytování součinností, včasné zahájení projektu, případné eskalace na řídící výbor
Zadávání nových požadavků/změn v průběhu projektu, které nesouvisí se scope/předmětem projektu	Hlídání scope projektu, včasná identifikace a předání požadavků do změnového řízení
Nedostatečná podpora managementu pro projekt IAM	Zapojení zainteresovaných osob do projektu

Níže jsou uvedeny základní součinnosti Objednatele, které jsou nezbytným předpokladem pro plynulý průběh dodávky Díla. Konkrétní technické požadavky musejí být ze strany Objednatele splněny před zahájením etapy *Dodávka a implementace* pro každou část Díla (AM a IDM). Nesplnění či nedodání požadovaných součinností je projektovým rizikem s možným dopadem na harmonogram či cenu Díla.

Konkrétní technické požadavky

- Zajištění HW pro instalaci všech komponent (IDM AS, IDM DB, Monitorovací server…) dle dodané specifikace ve všech prostředích.
- Připravené funkční testovací/vývojové verze připojovaných koncových systémů (včetně spravovaných dat).
- Zajištění kvality dat v testovacím prostředí tak, aby odpovídala datům v produkčním prostředí.
- Koncové systémy musí být připojitelné, případně zajištění provedení nezbytných změn v koncových systémech, aby byly připojitelné (např. webové služby, databázová tabulka, CSV, LDAP apod.). Úpravy na koncových systémech nejsou součástí nabídkové ceny a jsou v odpovědnosti Objednatele. Tyto úpravy provede/zajistí Objednatel do 14 dnů od vyžádání.
- Zajištění správy a běhu připojených aplikací ve všech prostředích.
- Zajištění prostupů na koncové/zdrojové systémy.
- Zajištění přístupu do CRŽP databáze
- Zajištění registrace u externích poskytovatelů IDP.
- Rekonfigurace Legacy SSO s ohledem na zvolenou variantu.
- Zajištěný VPN přístup do všech prostředí pro celý projektový tým.
- Hlášení případných plánovaných výpadků připojených systémů ve všech prostředích předem.

Obecné principy součinnosti

- Poskytnutí potřebných podkladů pro realizaci projektu. Podklady musí být dodány v odpovídajícím termínu a formě, které budou před započetím prací společně domluveny a schváleny dodavatelem.
- Schvalování výstupů a stavu projektu v termínech pro to určených a dále testování funkčních částí projektu bez zbytečných odkladů.

- Poskytování konzultací při potřebě konkretizování nejasných bodů zadání, analýzy a v průběhu celého projektu.
- Zajištění kapacit k provedení akceptačních testů.
- Dodávat informace k projektu úplně a včas.

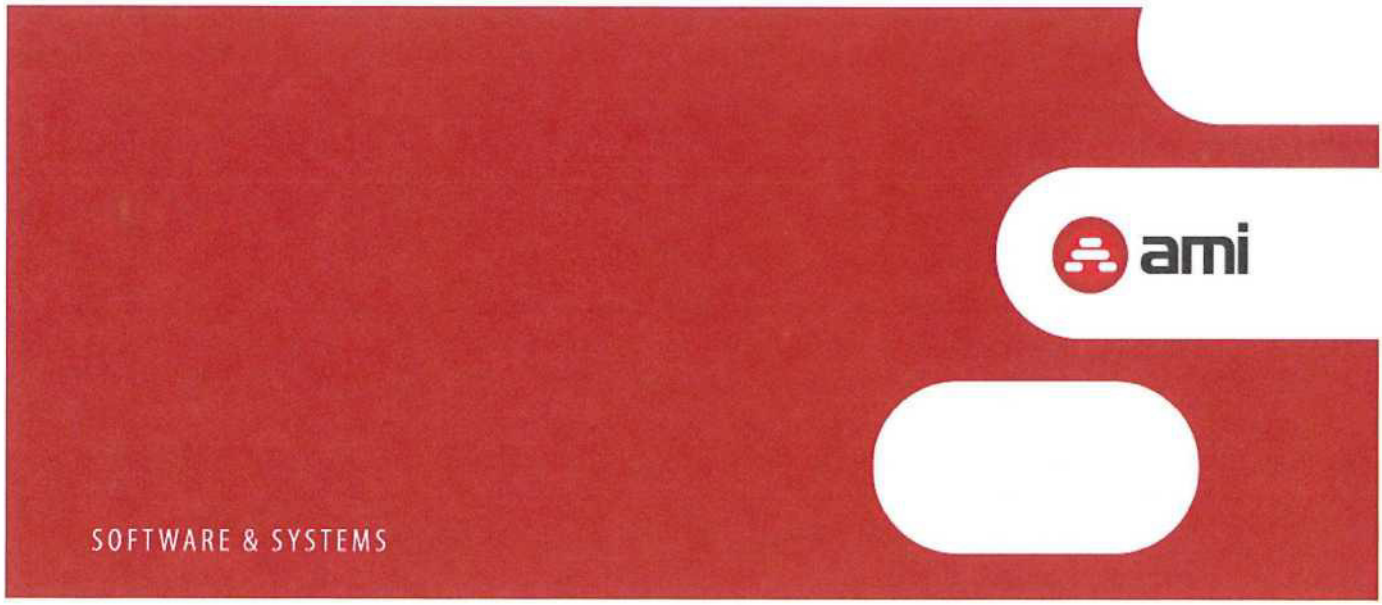
Reakční doby poskytování součinností

Pro dodržení termínů projektu je nezbytné, aby byla součinnost ze strany Objednatele poskytovaná v co nejkratším čase. Zejména v úvodní fázi projektu hrozí největší riziko zpoždění. Obecně v průběhu projektu očekáváme splnění požadavku na součinnost do pěti pracovních dnů od vyžádání, jinak bude požadavek eskalován dle dohodnutého procesu, pokud by byly ohroženy termíny projektu.

Během analytických schůzek očekáváme následující reakční doby:

- dodání požadovaných dokumentů do 3 pracovních dnů od vyžádání,
- zajištění odpovědných osob na analytické schůzky do 5 pracovních dnů od vyžádání.

Příloha B – Katalog požadavků



Příloha č. 5: Katalog požadavků na EnvilAM

nadlimitní veřejné zakázky „Dodávka Identity & Access Management systému (EnvilAM) včetně zajištění provozu a rozvoje“ pro zadavatele Česká republika – Ministerstvo životního prostředí

Obsah

1 IDM (APLIKACE) / NE-FUNKČNÍ POŽADAVKY

1.1 OBECNÉ – ZÁKLADNÍ NE-FUNKČNÍ POŽADAVKY

1.1.1 UŽIVATELSKÉ ROZHRANÍ (GUI)

ID	Požadavek*	Součást**
1	Obsahuje kompletní lokalizaci do českého jazyka.	ANO
2	Umožňuje vyhledávání ve všech entitách podle jejich - atributu, a - pomocí „full textu" – hledání řetězce současně ve více atributech.	ANO
3	Obsahuje nástroje – opatření proti útoku typu „Cross – Site Request Forgery".	ANO
4	Umožňuje export dat minimálně do souboru formátu CSV z jednotlivých obrazovek s výpisem uživatelů a rolí.	ANO

* Požadavek => všechny požadavek jsou mandatorní.

** Součást => Dodavatel deklaruje, že Aplikace (SW řešení) obsahuje tuto vlastnost, funkci – požadavek.

1.1.2 SYSTÉMOVÉ

ID	Požadavek	Součást
5	Řešení podporuje rozvoj pomocí skriptovacích jazyků (např. jazyků Groovy nebo Python).	ANO
6	Řešení podporuje přístup pomocí zabezpečeného protokolu HTTPS s podporou technologie RSA a ECC.	ANO
7	Řešení je možné provozovat na aplikačních serverech (v aktuálně dostupných verzích): - Java platforma – standard J2EE (např. Apache Tomcat, WebLogic Srv, WebSphere Appl. Srv, ...), nebo - Microsoft .NET Appl. Server, nebo - Aplikační servery na PHP platformě (např. Zend Server), nebo - Aplikační servery na Python platformě (např. Django CMS)	ANO
8	Řešení podporuje kódování UTF-8 i UTF-16.	ANO
9	Export/Import konfigurace IdM nástroje v minimálně v těchto uvedených formátech: XML, JSON a YAML.	ANO
10	Možnost definovat a pravidelně spouštět serverové úlohy (např. transformační, kontrolní a notifikační).	ANO
11	Schopnost pracovat v režimu vysoké dostupnosti za pomoci více uzlů aplikace (např. automatické spuštění úlohy na dostupném uzlu aplikace) Zhotovitel zajistí takový návrh architektury, aby splňoval požadavky na: - Škálovatelnost výkonnosti, - Rozložení zátěže, - Vysokou dostupnost, a - Cloudovatelnost. Objednatel požaduje umístění na HW prostředí Objednatele s možností jednoduchého a rychlého k jinému poskytovateli infrastrukturních služeb (přesun na jinou HW platformu včetně migrace veškerých dat a souvisejících činností musí být max. 15 MD).	ANO
12	Možnost volat jakoukoliv datovou operaci, která je dosažitelná z webového rozhraní pomocí API (např. založení uživatele, tvorba rolí, správa organizační struktury apod.).	ANO

1.1.3 INTEGRAČNÍ (INTEGRAČNÍ ROZHRANÍ)

Rozhraní pro integraci musí splňovat níže uvedené požadavky.

ID	Požadavek	Součást
13	Umožní číst nebo zapisovat všechna data a volat operace nad objekty v Aplikaci pomocí programového rozhraní (API - např. SOAP, REST, JSON).	ANO
14	Umožní bezpečný přenos dat mezi Aplikací a rozhraním koncového systému (např. prostřednictvím SSL/TLS, pro AD Kerberos nebo NTLM2).	ANO
15	Aplikace se k rozhraní koncových systémů autentizuje dedikovaným technickým uživatelem.	ANO
16	Umožní vystavit aplikační rozhraní (API – SOAP, REST, Java API apod.) nebo rozhraní datového úložiště (např. LDAP, DB procedury, DB tabulka).	ANO
17	Aplikace musí obsahovat následující konektory: - MS Active Directory Connector (včetně podpory PowerShell, WinRM a CredSSP), - LDAP Connector, - CSV Connector, - SSH Connector, a	ANO

	- Database Connector. Konektory musí být konfigurovatelné bez nutnosti vývoje.	
18	Umožní vývoj vlastních konektorů – jedná se minimálně o připojení: - k webovým službám a využití jejich metod. - k databázovým strukturám pro čtení a zápis dat. - pomocí protokolu LDAP.	ANO
19	Aplikace musí obsahovat také níže uvedené konektory: - IBM Domino Connector, - MS Exchange Connector, - MS Office365 Connector, - SCIM Connector. Konektory a jejich konfiguraci je možné dodat i pomocí vlastního vývoje, ale bez nároku na další odměnu.	ANO

1.1.4 LICENCE A LICENCOVÁNÍ

ID	Požadavek	Součást
20	Licence jsou neomezené min. v počtech: - instancí (PROD, TEST), - uživatelů, - napojených koncových systémů, - konektorů, - CPU/CPU cores, RAM a dalších HW/SW/App parametrech.	ANO
21	Dodavatel garantuje možnost připojení budoucích nových koncových systémů a vložení jejich přístupových rolí a logiky do Aplikace bez dodatečných licenčních nákladů.	ANO
22	Licence opravňuje Objednatele k tomu, aby: - využíval dílo bez omezení v rámci své činnosti, - si pořídil neomezený počet kopií díla pro vlastní potřebu, - sám nebo prostřednictvím třetích osob měnil, rozšiřoval a jinak upravoval dílo v souladu se svými potřebami.	ANO
23	Licence nesmí vyžadovat, aby byly případné úpravy Aplikace Objednatelem nebo třetí osobou veřejně publikovány na Internetu.	ANO
24	Součástí dodávky je předání kompletních zdrojových kódů implementovaných funkcionalit, včetně všech zdrojových kódů Aplikace.	ANO

1.2 SPECIFICKÉ NE-FUNKČNÍ POŽADAVKY

1.2.1 UŽIVATELSKÉ ROZHRANÍ (GUI)

ID	Požadavek	Součást
25	GUI je celé minimálně v českém jazyce.	ANO
26	Responsivní design.	ANO
27	Rozlišení minimálně 1280 x 768 a vyšší.	ANO
28	Full-textové vyhledávání minimálně pro objekty uživatel a role.	ANO
29	Rozhraní Aplikace přizpůsobené firemnímu designu (tzv. jednotnému vizuálnímu stylu – loga, barvy atd.).	ANO

1.2.2 ARCHITEKTURA

ID	Požadavek	Součást
30	On-line koncové systémy jsou řízené – spravované přímo Aplikací a evidence této správy je vedena tamtéž.	ANO
31	Off-line koncové systémy jsou řízené – spravované nepřímo přes systémové administrátory, ale evidence této správy je uložená v Aplikaci	ANO
32	Aplikace je nasazena ve třech prostředích: - 1x Vývojové (DEV), slouží pro vývoj a úpravy. - 2x Testovací (TEST), slouží pro testování úprav, konfigurace a školení. - 2x Produkční (PROD), slouží produkčnímu (reálnému) provoz.	ANO
33	On-line koncové systémy jsou připojené pomocí: - proprietárního konektoru, nebo - databázového konektoru, nebo - rozhraní webových služeb.	ANO

1.2.3 KONCOVÉ SYSTÉMY

Požadavky na připojení koncových systémů k Aplikaci.

1.2.3.1 On-line koncové systémy

ID	Požadavek	Součást
34	**eDirectory** – adresářový systém (LDAP) pro Novell - Rozhraní: konektor LDAP nebo proprietární, - Prostředí: PROD, TEST (nutné zařídit), - Podporované operace s účtem: založení, aktualizace, změna login/hesla, řízení oprávnění (přes skupiny), aktivace/deaktivace, zánik (účet je zachován, oprávnění jsou odebrána, heslo je změněno).	ANO
35	**IBM Notes/Domino** – aplikační a mailingový groupware systém - Rozhraní: konektor proprietární, - Prostředí: PROD, TEST (nutné zařídit), - Podporované operace s účtem: založení, aktualizace (včetně certifikátů), změna login/hesla, změna emailu (původní mezi alternativní emaily), řízení oprávnění (přes skupiny), aktivace/deaktivace, zánik (účet je zachován, oprávnění jsou odebrána, heslo je změněno, email nastaven neaktivní).	ANO
36	**OKbase** – personální systém - Rozhraní: databázový přístup k tabulkám a pohledům, - Prostředí: PROD, TEST, - Podporované operace s účtem: založení, aktualizace, změna login/hesla, řízení oprávnění, aktivace/deaktivace, zánik (= deaktivace).	ANO
37	**VPN** – připojení uživatele do interní sítě organizace - Rozhraní: konektor LDAP, - Prostředí: PROD, TEST, - Podporované operace s účtem: založení, aktualizace, změna login/hesla, řízení oprávnění, aktivace/deaktivace, zánik (= deaktivace).	ANO
38	**IS IdP** – JIP/KAAS, NIA, MojeID a další informační systémy poskytovatelů identit (IdP) - Aplikace musí být připravena na budoucí integraci se systémy dalších poskytovatelů identity (IdP).	ANO

1.2.3.2 Off-line koncové systémy

ID	Požadavek	Součást
39	**WIN-PAK** – systém evidence vstupních karet a přístupů do budovy	ANO

	- Rozhraní: off-line, - Prostředí: PROD, - Podporované operace s účtem: založení, aktualizace, změna login, řízení oprávnění, aktivace/deaktivace, zánik, ale vše jsou to úkoly pro správce koncového systému.	
40	**JASU** – ekonomický informační systém - Řízení přístupu do tohoto koncového systému probíhá prostřednictvím skupin v eDirectory.	ANO
41	**ownCloud** – souborové úložiště pro sdílení dokumentů (souborů) - Řízení přístupu do tohoto koncového systému probíhá prostřednictvím skupin v eDirectory. - Rozšířené atributy nad rámec přihlašovacích (např. jméno, příjmení) je možné mapovat přes LDAP z eDirectory. - Mazání zaniklých účtů včetně jejich dat je v režii samotného koncového systému.	ANO
42	**Certifikáty/Tokeny** – IBM Notes/Domino aplikace - Rozhraní: off-line, - Prostředí: PROD, - Podporované operace s účtem: založení, aktualizace, změna login, řízení oprávnění, aktivace/deaktivace, zánik, ale vše jsou to úkoly pro správce koncového systému.	ANO
43	**ESSS** – elektronický systém spisové služby - Rozhraní: off-line, - Prostředí: PROD, TEST, - Podporované operace s účtem: založení, aktualizace, změna login, řízení oprávnění, aktivace/deaktivace, zánik, ale vše jsou to úkoly pro správce koncového systému.	ANO
44	**Evidence klíčů** - Rozhraní: off-line, - Prostředí: PROD, - Podporované operace s účtem: založení, aktualizace, změna login, řízení oprávnění, aktivace/deaktivace, zánik, ale vše jsou to úkoly pro správce koncového systému.	ANO
45	**EPS** – elektronický požární systém - Rozhraní: off-line, - Prostředí: PROD, - Podporované operace s účtem: založení, aktualizace, změna login, řízení oprávnění, aktivace/deaktivace, zánik, ale vše jsou to úkoly pro správce koncového systému.	ANO
46	**EZS** – elektronický zabezpečovací systém - Rozhraní: off-line, - Prostředí: PROD, - Podporované operace s účtem: založení, aktualizace, změna login, řízení oprávnění, aktivace/deaktivace, zánik, ale vše jsou to úkoly pro správce koncového systému.	ANO
47	**Telefonní ústředna** – ústředna pro interní telefonní linky - Rozhraní: off-line, - Prostředí: PROD, - Podporované operace s účtem: založení, aktualizace, změna login, řízení oprávnění, aktivace/deaktivace, zánik, ale vše jsou to úkoly pro správce koncového systému.	ANO

1.2.4 MIGRACE

ID	Požadavek	Součást
48	Provést iniciální načtení identit a rolí do Aplikace, dle výsledků provedené Analýzy.	ANO
49	Provést import vazeb mezi identitami a rolemi.	ANO
50	Realizovat načtení zaměstnanců mimo evidenci (např. mateřské a rodičovské dovolené).	ANO

1.2.5 BEZPEČNOST

ID	Požadavek	Součást
51	Osobní údaje jsou v Aplikaci zabezpečené tak, aby k nim mohla jen oprávněná osoba.	ANO
52	Uživatel vidí svoje údaje nebo údaje svých podřízených kromě vyjmenovaných informací (např. heslo).	ANO
53	Testovacím prostředí (TEST) používá kopii produkčních dat a využívá stejnou politiku přístupů jako PROD prostředí.	ANO
54	Napojení Aplikace na systém pro správu a monitoring privilegovaných účtů (PIM/PAM systém) Zadavatele.	ANO

1.2.6 ROLE A PŘÍSTUPOVÁ OPRÁVNĚNÍ

ID	Požadavek	Součást
55	Správce (Administrátor systému), který má neomezený přístup.	ANO
56	Metodik, který má přístup ke správě rolí.	ANO
57	IT Podpora (Helpdesk systému), který má přístup k seznamu uživatelů.	ANO

58	Business vlastník (vlastník aktiva), vidí své role a jejich členy. Schvaluje žádosti o role na své schvalovací úrovni.	ANO
59	Licenční specialista, vidí své role a jejich členy. Schvaluje žádosti o role na své schvalovací úrovni.	ANO
60	Bezpečnostní manager ICT (Compliance), vidí své role a jejich členy. Schvaluje žádosti o role na své schvalovací úrovni	ANO
61	Školitel, vidí své role a jejich členy. Schvaluje žádosti o role na své schvalovací úrovni	ANO
62	Manažer, vidí podřízené identity, může pro tyto identity (uživatele) žádat o role a schvaluje žádosti o role na své schvalovací úrovni.	ANO
63	Běžný uživatel, může: - zobrazit informace o sobě, - žádat o role a měnit své heslo, a - měnit některé vybrané údaje o sobě. Oprávnění běžného uživatele je součástí všech výše zmíněných oprávnění (zn. že každý uživatel má tuto roli).	ANO

1.2.7 *NASAZENÍ*

ID	Požadavek	Součást
64	Prostředí bude nasazeno následovně: - PROD = produkční prostředí, - TEST = vývojové a testovací prostředí.	ANO

1.2.8 *AUDIT A REPORTING*

ID	Požadavek	Součást
65	Reporty je možné generovat ve formátu PDF, XLS či CSV.	ANO
66	Reporty je možné na vyžádání zasílat emailem jako přílohu.	ANO
67	Na vyžádání je možné report – přílohu zazipovat.	ANO

1.2.8.1 *Auditní logy*

ID	Požadavek	Součást
68	Aplikace eviduje všechny změny nad spravovanými objekty – identita, role, oprávnění, koncový systém, organizační jednotka.	ANO
69	Míra detailu této evidence je: - datum a čas včetně specifikace časového pásma (KDY), - typ činnosti (CO), - identifikaci technického aktiva, které činnost zaznamenalo, - jednoznačnou identifikaci účtu, pod kterým byla činnost provedena, - jednoznačnou síťovou identifikaci zařízení původce – zdrojová IP adresa (ODKUD) - úspěšnost nebo neúspěšnost činnosti.	ANO
70	Logováno musí být: - přihlašování a odhlašování ke všem účtům (i neexistujících účtů), a to včetně neúspěšných pokusů, - všechny činnosti provedené administrátory, - úspěšné i neúspěšné manipulace s účty, oprávněními a právy, - neprovedení činností v důsledku nedostatku přístupových práv a oprávnění, - činnosti uživatelů, které mohou mít vliv na bezpečnost informačního a komunikačního systému, - zahájení a ukončení činností technických aktiv, - kritická i chybová hlášení technických aktiv, - přístupy k záznamům o událostech, pokusy o manipulaci se záznamy o událostech, - změny nastavení nástrojů pro zaznamenávání událostí.	ANO
71	Aplikace generuje a aktivně posílá auditní logy ve formě Syslog na: - aplikační server Aplikace (CEF formát), odkud jsou směrovány do SIEM, a na - definovanou IP adresu a port.	ANO
72	Logy musí být jednořádkové. Jedna událost v Aplikaci odpovídá jedné syslog zprávě s jedním řádkem. Položky logu musí být ve formátu: položka 1 = hodnota 1, položka 2 = hodnota 2 atd.	ANO

1.2.8.2 *Auditní reporty*

ID	Požadavek	Součást
73	Aplikace generuje report „Aplikace vs. koncový systém", který obsahuje kompletní přehled historie událostí mezi Aplikací a koncovým systémem včetně informací, KDO, KDY, CO a PROČ (na základě čeho) změnu provedl.	ANO

74	Aplikace generuje report „Role a organizace", který obsahuje kompletní přehled historie změn provedených nad libovolnými rolemi a organizacemi včetně informací, KDO, KDY, CO a PROČ (na základě čeho) změnu provedl.	ANO
75	Report „Identita", který obsahuje kompletní přehled historie změn provedených nad identitou – například synchronizace atributů, přidělení role, změn atd., a to včetně informací KDO, KDY a PROČ (na základě čeho) změnu provedl.	ANO
76	Aplikace generuje report z auditních záznamů.	ANO

1.2.8.3 Reporty o uživatelích a rolích

ID	Požadavek	Součást
77	Report organizační struktury i s přiřazenými identitami.	ANO
78	Report rolí s přímo i nepřímo přiřazenými identitami.	ANO
79	Report identit s filtrováním dle kritérií.	ANO
80	Manažerský report podřízených identit exspirujících na konci daného měsíce.	ANO
81	Kontrola konzistence Aplikace – primárně pro vyhledávání chyb (např. role má neplatného vlastníka, manažer je neplatný atd., příjemcem je Metodik).	ANO
82	Kontrolní export rolí – kontrola správnosti přiřazení aplikačních rolí do business rolí, kontrola atributů rolí (schvalovatelé atd.).	ANO

1.2.8.4 Rekonciliační reporty

ID	Požadavek	Součást
83	Report – identifikace účtů, ke kterým nebyl v Aplikaci nalezen vlastník (nespárované účty).	ANO
84	Report účtů v koncových systémech a jejich napojení na identity v Aplikaci.	ANO
85	Rekonciliační report pro vybraný koncový systém – chronologický seznam akcí nad koncovým systémem.	ANO

1.2.8.5 Recertifikační reporty

ID	Požadavek	Součást
86	Report o všech recertifikačních kampaních a jejich stavech.	ANO
87	Report o řešených případech v recertifikačních kampaních.	ANO
88	Report o rozhodnutí jednotlivých ověřovatelů.	ANO

1.2.9 RETENCE DAT

ID	Požadavek	Součást
89	Aplikace uchovávána data po neomezenou dobu.	ANO
90	Výjimku tvoří tato data: - auditní záznamy (logy), retence je 1 rok, - workflow a výsledky procesních aktivit, retence je 1 měsíc,	ANO

1.2.10 SSO

ID	Požadavek	Součást
91	Aplikace bude schopná integrovat budoucí nasazení Single Sign On (SSO). Poznámka: *V současné době systémová architektura organizace neumožňuje nasazení SSO, ale v budoucnu se plánuje nasazení MS Active Directory, které nasazení SSO umožní. Aplikace musí počítat s nasazením SSO a se změnou procesů (viz Podpora a Rozvoj).*	ANO

1.2.11 VERZOVÁNÍ APLIKACE

ID	Požadavek	Součást
92	Aplikace je verzována v Git Repository.	ANO
93	Aplikace je nasazována do jednotlivých prostředí (PROD, TEST) z Git Repository pomocí nasazovacích nástrojů.	ANO

1.2.12 ZÁLOHOVÁNÍ A OBNOVA, ODSTÁVKA

ID	Požadavek	Součást
94	Zálohování je realizováno minimálně na dvou úrovních: - záloha souborového systému aplikačního serveru, - pravidelným exportem dat z databáze Aplikace.	ANO
95	Obnova Aplikace splňuje minimálně následující požadavky: - Recovery Time Objective (RTO), neboli čas na obnovu Aplikace po výpadku <= 1 den, - Recovery Point Objective (RPO), neboli maximální povolená ztráta dat po výpadku <= 4 hodiny.	ANO
96	Aplikace má vyhrazená servisní okna pro údržbu a aktualizace: - pracovní dny 22:00 – 05:00 hodina,	ANO

	- víkendy a svátky, výpadky v tato okna se nepočítají do SLA.	

1.2.13 *Akceptační testování*

1.2.13.1 *Uživatelské*

ID	Požadavek	Součást
97	Než bude akceptováno nasazení Aplikace do PROD, jsou popsány testy – akceptační scénáře, které budou sloužit pro akceptaci Aplikace.	ANO
98	V rámci **identity** je testováno minimálně: - založení účtu zaměstnance, - založení účtu externisty, - založení technického účtu, - změna a ukončení pracovního poměru zaměstnance i externisty, - změna loginu a hesla a jejich propagace, - reset hesla,	ANO
99	V rámci **oprávnění** je testováno minimálně: - žádost o přidělení oprávnění, - vícestupňové schvalovací workflow, - odebrání oprávnění.	ANO
100	V rámci **role** je testováno minimálně: - vytvoření role, - aktualizace role, - aktivace/deaktivace role, - archivace role.	ANO
101	V rámci **rekonciliace** je testováno minimálně spuštění rekonciliace mezi Aplikací a on-line i off-line koncovým systémem.	ANO
102	V rámci **recertifikace** je testováno minimálně: - nová definice recertifikace, - spuštění recertifikace, - ověřování přístupů ověřovateli, - znovuspuštění recertifikace pro nerozhodnuté případy po časovém limitu.	ANO
103	V rámci **reportů** je testováno minimálně jejich spuštění s výstupem: - do souboru na sdílené úložiště, - jako příloha emailu, - jako zip příloha emailu.	ANO

1.2.13.2 *Zátěžové*

ID	Požadavek	Součást
104	Než bude akceptováno nasazení Aplikace do PROD, jsou popsány testy – akceptační scénáře, které budou sloužit pro akceptaci Aplikace na minimálně následující zátěž: - 1 000 změn / hodinu na vstupu z personálního systému, - 100 současně přihlášených uživatelů.	ANO

1.2.14 *Dokumentace a školení*

ID	Požadavek	Součást
105	Dokumentace obsahuje: - Dokumentaci skutečného nasazení – nastavení, - Administrátorskou příručku, - Uživatelskou příručku	ANO
106	Dokumentace se vytváří, a verze k revizím se předávají, ve formátu MS Office.	ANO
107	Finální verze dokumentace dodává Dodavatel ve formátu prohledávatelného PDF.	ANO
108	Pro práci s Aplikací a její správu je nutné proškolit: - uživatele, minimálně klíčové uživatele Aplikace (vybere Objednatel minimálně v počtu 20), - administrátory – správce (vybere Objednatel minimálně v počtu 2).	ANO

1.2.15 *Podpora a Rozvoj*

ID	Požadavek	Součást
109	Podpora Aplikace je poskytována minimálně v rozsahu 5 x 8, v pracovní dny od 9:00 – 17:00h.	ANO
110	Součástí podpory jsou minimálně následující položky: - garance reakční doby a řešení incidentů,	ANO

	- hlášení požadavků telefonicky a pomocí helpdesk/servicedesk, - pravidelný měsíční report řešených incidentů,	
111	Minimální parametry SLA – Vada / Čas reakce / Čas opravy - Vysoká / 2 h / nejpozději do konce pracovního dne, - Střední / 4 h / nejpozději do konce následujícího pracovního dne, - Nízká / 4 h / nejpozději do pěti pracovních dnů,	ANO
112	Specifikace vad: - Vysoká – zabraňuje provozu, znemožňuje provoz, - Střední – omezuje provoz, ale vady se dají dočasně obejít (např. jiným technickým nebo organizačním opatřením), - Nízká – neomezuje provoz, jde o drobné vady Zařazení vady navrhuje Dodavatel, ale schvaluje (určuje) Objednatel služby.	ANO
113	Rozvoj Aplikace je určen pro: - drobný rozvoj a úpravy, - konzultace a školení, a to v rozsahu max. 115 člověkodnů ročně. Hodiny podpory budou vykazovány a schvalovány na bázi měsíčního výkazu (reportu).	ANO

1.2.16 LICENCE A LICENCOVÁNÍ

ID	Požadavek	Součást
114	Aplikace podporuje minimálně **1 200** aktivních identit (uživatelských a technických), do tohoto počtu nejsou zahrnuty archivované identity.	ANO

2 IDM (APLIKACE) / FUNKČNÍ POŽADAVKY

2.1 OBECNÉ – ZÁKLADNÍ FUNKČNÍ POŽADAVKY

2.1.1 AUTORIZACE

ID	Požadavek	Součást
115	Založena na „Role-Based Access Control (RBAC)" a umožňuje nastavit, k jaké části uživatelského rozhraní Aplikace a k jakým objektům v Aplikaci mají uživatelé přístup, a to až do úrovně atributů entit.	ANO
116	Umožní definovat oprávnění k jednotlivým objektům pomocí aplikačních a business rolí.	ANO
117	Umožní definovat oprávnění k funkcionalitám Aplikace pomocí aplikačních a business rolí.	ANO
118	Dovolí nastavovat autorizaci na jednotlivé části GUI nebo pomocí filtrů na jakékoliv entity, které splňují (nebo nesplňují) definované podmínky.	ANO
119	Umožní definovat autorizaci na základě podmínky – např. vedoucí odboru (oddělení apod.) smí upravovat autorizace svých podřízených.	ANO
120	Dovolí vytvořit administrátorská práva nad určitými organizačními jednotkami, koncovými systémy, nad skupinami uživatelů nebo obecně nad definovanými objekty Aplikace. Účelem je umožnit administrátorovi správu nad uživateli patřícími do samostatného podřízeného celku - např. nad externími entitami, kterými jsou dodavatelské účty.	ANO
121	Umožní konfigurovat práva všech uživatelů tak, aby si mohli zobrazit: - přiřazené koncové systémy, - přiřazená oprávnění, - přiřazení do organizační struktury.	ANO
122	Dovolí nastavit práva všech uživatelů tak, aby si mohli provést schválení přiřazených požadavků a spouštět reporty.	ANO
123	Nastavit oprávnění až na úroveň jednotlivých atributů, např. uživatel si může editovat pouze atribut telefonního čísla.	ANO

2.1.2 AUTENTIZACE

ID	Požadavek	Součást
124	Aplikace musí obsahovat Access Management (AM), jehož funkcí je možnost automatického přihlášení (SSO) pomocí protokolu Kerberos oproti AD nebo LDAP.	ANO
125	Uživatel přihlášený do AD nebo LDAP je automaticky přihlášen do Aplikace.	ANO
126	Uživateli, který není zaveden v AD nebo LDAP, je zobrazen přihlašovací formulář, ve kterém se pomocí jména/hesla může přihlásit do Aplikace. Jméno/heslo které je ověřeno proti úložišti Aplikace.	ANO
127	Operace související s autentizací jsou vždy zaznamenávány do auditního logu Aplikace.	ANO
128	Aplikace umožní provést odhlášení uživatele.	ANO
129	Aplikace umožňuje samo-registraci nového uživatele. Samo-registrační formulář obsahuje kontrolu mechanismem CAPTCHA. Uživateli je po potvrzení formuláře z Aplikace zaslán e-mail obsahující aktivační link.	ANO
130	Aplikace podporuje vedení historie hesel uživatelů, v případě jejich změny přes Aplikaci. Nově zadávaná hesla jsou kontrolována proti historii.	ANO
141	Aplikace umožní hesla uživatele zabezpečovat symetrickou šifrou nebo hashem dle globální konfigurace.	ANO

2.1.3 RECERTIFIKACE OPRÁVNĚNÍ

ID	Požadavek	Součást
142	Aplikace obsahuje nástroj, který provádí recertifikaci přiřazení identita – role a umožňuje tak v pravidelných intervalech spouštět přeschvalování existujících oprávnění (vazeb identita – role).	ANO
143	Recertifikace musí umožňovat:	
144	- automatické (plánované) spouštěné certifikace	ANO
145	- ruční spouštěné certifikace – tzv. na vyžádání	ANO
146	- automatické akce při zamítnutí přístupu (např. při odebrání role)	ANO
147	- definovat rozsah recertifikací podle identit, rolí a organizační struktury	ANO
148	- logovat (a reportovat) stavy kroků a výsledku recertifikace	ANO
149	- spouštět neomezený počet současně běžících recertifikací	ANO
150	- konfigurovat vícekrokové workflow s podporou eskalace a delegace	ANO
151	Aplikace rovněž umožní recertifikovat obsah business rolí (vazbu na aplikační role).	ANO

152	Stavy recertifikací jednotlivých případů a rozhodnutí lze sledovat v reportech a reagovat na případné nestandardní stavy (např. neřešené recertifikace ke schválení).	ANO

2.1.4 *SYNCHRONIZACE A REKONCILIACE*

ID	Požadavek	Součást
153	Aplikace načítá data z koncových systémů (synchronizace) a porovnává schválený a skutečný stav na koncovém systému (rekonciliace) a dále musí zabezpečit (umožnit):	ANO
154	Synchronizaci změn v reálném čase podle časové značky u záznamu.	ANO
155	Vestavěnou podporu opakování propagace změn v případě neúspěchu.	ANO
156	Obousměrnou synchronizaci dat mezi Aplikací a koncovým systémem (např. uživatele a jejich atributy, role v koncovém systému).	ANO
157	Mapování atributů mezi koncovými systémy na základě pravidel/vzorců.	ANO
158	Práci se složenými i binárními atributy uživatele (např. certifikáty, fotografie, autentizační tokeny).	ANO
159	Rekonciliaci účtů - tzn. pravidelnou automatickou kontrolu stavu účtů na koncových systémech s autoritativním vypořádáním nesouladu.	ANO
160	Zaznamenání stavu účtu při rekonciliaci vzhledem k (ne)existenci vlastníka v Aplikaci.	ANO
161	Nastavení automatických akcí pro nespárované účty (např. zneplatnění).	ANO
162	Nastavení „Whitelistu" účtů, které Aplikace nikdy nemění (např. pro technické účty).	ANO
163	Pravidelnou automatickou kontrolu stavu oprávnění na koncových systémech a vynucení stavu chtěného (např. výmaz nadbytečných oprávnění).	ANO
164	Nastavení korelačních pravidel pro párování mezi identitou a jejím účtem (např. nastavení politiky, že část e-mailové adresy účtu odpovídá username dané identity).	ANO
165	Logování veškerých aktivit synchronizací a rekonciliací.	ANO
166	Reportování výsledků rekonciliací pomocí uživatelsky definovaných reportů.	ANO
167	Podporu pro objekty v koncovém systému typu uživatel, skupina, role a organizace.	ANO
168	V koncovém systému měnit jiné typy objektů, než je uživatelský účet (např. role, skupiny, profily). Jde především o objekty oprávnění a organizačních jednotek. Příklad: Aplikace umožní vytvořit roli, která je zodpovědná nejen za přiřazení oprávnění uživateli, ale i za existenci objektu oprávnění v koncovém systému.	ANO
169	Rekonciliaci off-line systémů – tzn. že Aplikace umožní: - řízení identit a oprávnění v připojených systémech, - off-line řízení oprávnění a identit na základě manuálního potvrzení akce odpovědnou osobou. Off-line řízení oprávnění probíhá v GUI rozhraní Aplikace nebo na základě informací získaných z exportu koncového systému. - spustit každou rekonciliaci tak, aby zpracování objektů koncových systémů běželo ve více vláknech.	ANO
170	Hromadné akce – spouštění minimálně těchto hromadných akcí: - hromadné přiřazení rolí uživatelům, kteří vyhovují podmínkám, - hromadnou změnu organizační jednotky vybraných uživatelů, - hromadné vytvoření rolí, - hromadné schvalování přidělených úkolů, a všechny hromadné akce jsou auditovány.	ANO
171	Simulaci změn – Aplikace poskytuje grafický přehled změn atributů před vlastním uložením vybraného objektu. Tato simulace se týká minimálně uživatelů, rolí a organizační struktury.	ANO

2.1.5 *NOTIFIKACE (E-MAIL NOTIFIKACE)*

ID	Požadavek	Součást
172	Aplikace umožňuje definovat šablony e-mailů s podporou vícejazyčnosti (min. čeština a angličtina) a HTML.	ANO
173	Aplikace podporuje skriptovací jazyk s možností čerpání dat ze zdrojové databáze.	ANO
174	Aplikace podporuje konfiguraci parametrů odesílání zpráv přes SMTP server (např. jméno serveru, jméno/heslo, SSL, ...).	ANO
175	Aplikace dovoluje zvolit v nastavení více odesílacích SMTP serverů.	ANO
176	Aplikace umožňuje vkládání hypertextových linků na konkrétní obrazovky v Aplikaci.	ANO
177	Aplikace provádí notifikaci minimálně těchto akcí: - vytvoření, změna, smazání identity, - přiřazení a odebrání role, - výzva k akci pro uživatele, - zakázání a povolení uživatele, - přejmenování uživatele,	ANO

	- požadavek na schválení role nebo na její ověření, - libovolné akce ve workflow podle nastavení administrátorem, - změna uživatelského hesla, - propagace hesla z Aplikace do koncového systému.	

2.1.6 *WORKFLOW (DLE PRINCIPŮ BPM)*

ID	Požadavek	Součást
178	Aplikace umožnuje vytvářet a modifikovat workflow založené na principech Business Process Management (BPM).	ANO
179	Aplikace umožnuje aktivovat workflow při splnění nastavené podmínky (např. nastavení hodnoty atributu).	ANO
180	Aplikace dovoluje aktivovat workflow automaticky při schvalovacím procesu přidělování rolí uživatelům.	ANO
181	Umožňuje vizualizaci průběhu workflow včetně výhledu do budoucna – přehled budoucích schvalovatelů.	ANO
182	Aplikace dovoluje definovat neomezený počet schvalovacích kroků.	ANO
183	Dovoluje nastavit neomezený počet schvalovatelů.	ANO
184	Dovoluje nastavit schválení typu „1 z N", „X z N" nebo „N z N".	ANO
185	Umožňuje nastavit sériové i paralelní schvalování.	ANO
186	Aplikace dovoluje definovat schvalovatele na základě jejich členství v roli, organizační struktuře nebo podle jejich funkce.	ANO
187	Umožňuje automatické schvalování na základě hodnoty atributů identity.	ANO
188	Umožňuje automatické schvalování na základě pracovního místa, funkce nebo zařazení v organizační struktuře.	ANO
189	Aplikace umožňuje schvalovateli doplnit další potřebné informace v průběhu schvalování požadavku (např. číslo místnosti, telefonní číslo, ...).	ANO
190	Dovoluje zobrazit přehled úkolů schvalovatele.	ANO
191	Aplikace nabízí schvalovateli schválení/zamítnutí požadavku s přidáním odůvodnění.	ANO
192	Aplikace umožňuje administrátorům i koncovým uživatelům nastavení, změnu hesel a přehled svých oprávnění v rámci aplikací na jednom místě, přes webové rozhraní.	ANO

2.1.7 *SPRÁVA OBJEKTŮ (OS, ROLE, KONCOVÉ SYSTÉMY)*

2.1.7.1 *Organizační struktura (OS)*

Aplikace musí podporovat minimálně dále uvedené funkce pro správu organizační struktury.

ID	Požadavek	Součást
193	Administrační webové rozhraní pro správu stromové struktury.	ANO
194	Správu prostřednictvím integrační vrstvy.	ANO
195	Umožnit volání funkcionalit Aplikace prostřednictvím programového rozhraní (API - např. SOAP, REST, JSON).	ANO
196	Vytvářet libovolné počty stromů organizačních struktur.	ANO
197	Vytvářet nezávislé objekty ve stromě (pracovní pozice, funkční místa apod.).	ANO
198	Umožnit definování atributy těchto objektů ve stromě.	ANO
199	Přiřazovat nezávislé objekty organizačním jednotkám ve stromě – minimálně uživatele, role, uzly z jiných stromů.	ANO
200	Vizualizovat entity pomocí stromové struktury.	ANO
201	Přiřazovat identity nebo role do více stromů zároveň (např. uživatel může být ve více organizačních strukturách, v různém zařazení a s odlišnými oprávněními).	ANO
202	Nastavení časové období „od – do" pro přiřazení identity do stromové struktury. Pokud časové období uplyne nebo ještě nenastalo, je toto zařazení neaktivní.	ANO

2.1.7.2 *Role*

Aplikace musí podporovat dále uvedené vlastnosti pro role.

ID	Požadavek	Součást
203	Administrační webové rozhraní pro správu business a aplikačních rolí.	ANO
204	Správu prostřednictvím integrační vrstvy včetně možnosti volání funkcí prostřednictvím programového rozhraní (API).	ANO
205	Role musí být možné hierarchicky skládat do hloubky minimálně 25 úrovní.	ANO

206	Přiřazení role na organizační jednotku s jejím promítnutím k uživatelům přiřazeným do organizační jednotky.	ANO
207	Vazbu uživatele na roli v kardinalitě 1: N s určením typu vazby (např. vlastník, schvalovatel role, a s nastavením platnosti přiřazení role „od – do").	ANO
208	Vazbu koncových systémů na roli v kardinalitě 1: N.	ANO
209	Nastavení platnosti role „od – do" a pokud časové období uplyne nebo ještě nenastalo, nesmí být přiřazení role aktivní.	ANO
210	Nastavení schvalovacích procesů pro garanty koncových systémů při tvorbě business rolí.	ANO
211	Správu role vlastníkem bez přiřazení explicitní autorizace.	ANO
212	Nastavení role jako vlastníka objektu v koncovém systému (oprávnění, účtu) podobně jako je uživatel vlastníkem účtu. Rekonciliace role pak provede aktualizaci objektu v koncovém systému.	ANO
213	Podporu tzv. parametrické role (hybridní RBAC).	ANO
214	Nastavení pravidel pro vzájemně se vylučující role „Segregation of Duties (SoD)".	ANO
215	Reporting a notifikace konfliktních práv.	ANO
216	Nastavování povolení/zamítnutí konfliktů SoD ve schvalovacím Workflow.	ANO
217	Zažádání o kopii vybraných rolí podle existujícího uživatele a spuštění příslušného schvalovacího workflow jako v případě manuálního přiřazení daných rolí.	ANO
218	Dědičnost vybraných vlastností rolí (např. atributů a typu schvalování z nadřazené role).	ANO

2.1.7.3 Koncové systémy

Aplikace musí podporovat dále uvedené funkce pro koncové systémy (třetí aplikace/AIS/IS).

ID	Požadavek	Součást
219	Administrační webové rozhraní pro správu koncových systémů (např. nastavení parametrů připojení, zobrazení skutečných účtů kontrolou v koncovém systému, a nikoliv v úložišti Aplikace).	ANO
220	Správu prostřednictvím integrační vrstvy včetně volání funkcí prostřednictvím programového rozhraní (API).	ANO
221	Evidenci koncových systémů včetně popisných atributů.	ANO
222	Vazbu na uživatele.	ANO
223	Vazbu na aplikační role přiřazené ke koncovému systému v kardinalitě 1: N.	ANO
224	Rozlišení různých kategorií účtů (např. administrátorské a běžné účty).	ANO
225	Různou business logiku plnění atributů pro různé kategorie účtů.	ANO
226	Povolení jednotlivých operací nad koncovým systémem (např. dočasně deaktivovat zápis do koncového systému).	ANO
227	Využití více nezávislých konektorů z koncového systému do Aplikace (např. CSV soubor pro čtení, webové služby pro zápis).	ANO