Příloha č. 1
Specifikace předmětu plnění

doplní dodavatel dle přílohy č. 1 zadávací dokumentace

Příloha č. 1 zadávací dokumentace

Tato příloha je nedílnou součástí zadávací dokumentace veřejné zakázky s názvem „Dodávka, implementace a podpora systému pro správu, řízení a monitoring identit včetně zabezpečení privilegovaných účtů“ Obsahuje podrobné vymezení předmětu veřejné zakázky. Požadavky specifikované v přiložených tabulkách této přílohy považuje Zadavatel za minimální a na jejich splnění Zadavatel trvá.

Požadavky jsou rozděleny po oblastech IDM (Identity Management) a PAM (Privileged Access Management).

1 Oblast IDM

1.1 Vypracování detailního návrhu řešení IDM

Součástí detailního návrhu řešení bude zejména:

- Detailní analýza současného stavu rolí/oprávnění ve spravovaných systémech. Dodavatel v rámci analýzy vytvoří katalog rolí a navrhne model správy těchto rolí a tento model projedná s příslušnými správci systémů. Taktéž analýza nastaví životní cyklus rolí (založení nové role, přidělení role, zavedení role, změna role, odebrání role, zrušení role).
- Analýza stávajících interních předpisů Zadavatele dotčených projektem IDM a návrhy jejich optimalizace potřebné pro implementaci systému IDM (nařízení ředitele k ISMS a Technické bezpečnostní politiky).
- Specifikace potřebného hardware a specifikace požadavků na provozní prostředí, zpracovaná ve spolupráci s objednatelem.
- Popis metodiky vyhodnocení testovacího provozu pro předání díla do rutinního provozu.
- Detailní specifikace řešení IDM včetně datového a funkčního modelu a včetně jeho přizpůsobení potřebám Zadavatele.
- Detailní popis rozsahu úkonů údržby a rozsahu parametrů a vlastností IDM nastavitelných tak, aby proškolení pracovníci Zadavatele mohli provádět základní správu IDM a měnit jeho vyhrazené parametry a vlastnosti, a to včetně návrhu a správy procesů workflow.
- Detailní popis implementace IDM, zejména:
    - popis integrací IDM s požadovanými informačními systémy (dle přílohy č. 3 ZD) provozovanými nebo využívanými Zadavatelem, které budou umožňovat replikaci identit, organizačních struktur a funkčních míst, vytváření speciálních skupin, řízení práv, zástupy a potvrzení komunikace,
    - popis řešení SSO
    - detailní popis implementace včetně časového harmonogramu,
    - popis věcného a organizačního zabezpečení testovacího provozu,
    - popis instalačních procedur pro instalaci IDM a nastavení parametrů pro práci v IDM (na straně serveru a na straně klientských stanic),
    - popis rozhraní pro integraci s jinými systémy (jeho datový a funkční model),
    - návrh akceptačních kritérií pro předání díla do testovacího provozu včetně návrhu akceptačního protokolu pro předání díla do testovacího provozu; akceptační kritéria musí obsahovat výčet všech požadavků na funkčnost díla dle Formuláře plnění technických požadavků.

Detailní návrh řešení bude podroben interní oponentuře Zadavatele. V případě připomínek Zadavatele je dodavatel povinen tyto připomínky do detailního návrhu řešení zapracovat. Akceptace a předání detailního návrhu řešení je nutnou podmínkou pro realizaci dalších etap plnění zakázky. Detailní návrh řešení se stane jeho předáním majetkem Zadavatele, který jej bude moci plně využít pro svoje potřeby ke všem způsobům užití, a to bez dalšího souhlasu zhotovitele nebo zpracovatele.

1.2 Dodávka řešení a zajištění licencí k užití SW a implementace IDM

Zadavatel předpokládá vybudování IDM na již existujících softwarových produktech, které jsou na trhu k dispozici a jejich přizpůsobení dle potřeb Zadavatele. Jiné řešení není vyloučeno.

Součástí dodávky musí být udělení veškerých potřebných licencí pro užívání a správný chod celého IDM, a to v rozsahu dle čl. 14 návrhu smlouvy o dílo a dále následovně.

- Součástí dodávky jsou
  1.1 licence na používání IDM a potřebných integračních konektorů na požadované IS (dle přílohy č. 3 ZD),
  1.2 komplexní dokumentace licence pro SSO software v rozsahu počtu identit.

Součástí dodávky je další software:

- Součástí zakázky je kromě licencí vlastního informačního systému také dodávka a udělení potřebného počtu všech případných dalších licencí veškerého dalšího software potřebného k provozování všech požadovaných součástí této zakázky, a to včetně jejich technické podpory.
- Součástí nabídkové ceny je i cena licencí a dodání serverového operačního systému nutného pro provoz nabídnutého řešení, a to včetně jeho maintenance po dobu 4 let od zahájení podpory. V případě potřeby CALů pro přístup k MS Windows serverům zahrne dodavatel též cenu potřebných CAL licencí do nabídkové ceny.
- V případě, že serverový operační systém, který je nutný pro provoz nabídnutého řešení, není jedním z operačních systémů podporovaných v rámci IT infrastruktury Zadavatele (Microsoft Windows Server 2008 R2 a vyšší, FreeBSD, Debian, CentOS), je součástí nabídkové ceny též cena administrátorského školení v rozsahu 40 hodin pro 5 pracovníků pověřených Zadavatelem pro správu tohoto serverového systému.
- V případě nabídky řešení na jiné než databázové platformě MS SQL 2012 r2 a vyšší/Oracle 11g a vyšší/FreeMysql Maria DB/PostgeSQL server musí dodavatel započítat cenu všech potřebných licencí a podpory této platformy a též cenu administrátorského školení v rozsahu 40 hodin pro 5 pracovníků pověřených Zadavatelem pro správu této platformy.

Veškeré licence budou uděleny a dodány tak, že do nabídkové ceny bude zahrnuta možnost Zadavatele k bezplatnému přechodu na jejich nové verze.

Provozní prostředí

Infrastruktura Zadavatele je provozována na platformách Microsoft Windows Server, FreeBSD, Debian, CentOS a jsou provozovány LDAP adresáře MS Active Directory a SUN/Oracle eDirectory a OpenLDAP a MS ForeFront. Je využíváno řešení virtualizace na platformě VMware vSphere 5. Aplikační servery jsou provozovány jak virtuálně, tak hardwarově.

Zadavatel povoluje možnost rutinního provozu nabízeného řešení na těchto platformách v prostředí Zadavatele.

Je požadováno technické řešení v režimu vysoké dostupnosti (high availability) v režimu 24/7 s možností geografického oddělení clusteru.

Implementace

Implementace IDM do prostředí Zadavatele na základě akceptovaného a předaného Detailního návrhu řešení.

Implementace IDM (včetně instalace všech potřebných softwarových a databázových součástí dodaného řešení) proběhne v souladu s akceptovaným Detailním návrhem řešení IDM na produkční a testovacího prostředí Zadavatele včetně instalace na osobní počítače uživatelů (v počtu požadovaných licencí).

Dodavatel zajistí instalaci a přípravu produkčního a testovacího prostředí.

Předmětem plnění zakázky není nákup hardware. Hardware zajistí Zadavatel sám na základě požadavků specifikovaných dodavatelem (připravené harmonogram musí reflektovat požadavek na objednání a dodání). Předmětem plnění není ani příprava prostředí na úrovni hardware a jiných komponent s dodávkou souvisejících. Tuto přípravu zajistí Zadavatel. Přípravou prostředí, kterou zajistí Zadavatel, se rozumí:

a) Příprava fyzických nebo virtuálních serverů.
b) Příprava úložiště dat – diskového pole.
c) Začlenění serverů do sítě Zadavatele.
d) Konfigurace firewallů a konfigurace požadovaných portů pro přístup na požadované systémy.
e) Zřízení VPN přístupu.
f) Napojení na dohledové a zálohovací nástroje.

Dodavatel musí v rámci nabídky specifikovat parametry (sizing) příslušných infrastrukturních komponent (Hardware – CPU Cores, RAM, Disky – kapacita a dělení, typ a podporované verze operačních systémů). Vlastní dodávka infrastrukturních komponent již není předmětem zakázky.

Integrace IDM s vybranými informačními systémy provozovanými nebo využívanými Zadavatelem

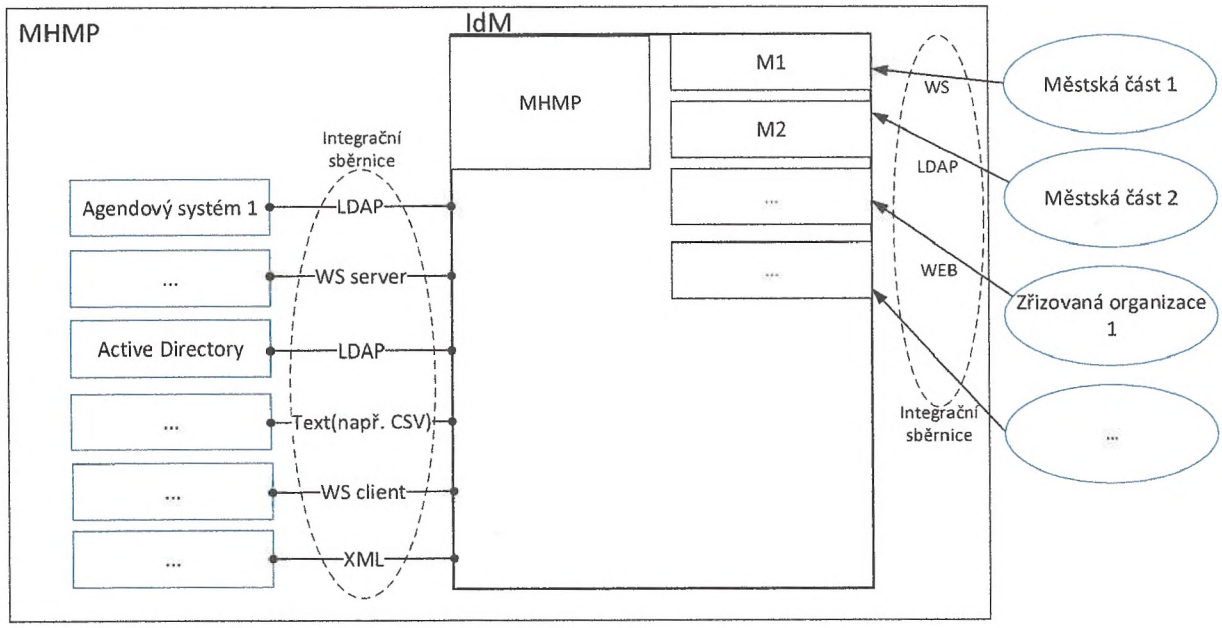
Předmětem plnění zakázky je zabezpečení obousměrné plně funkční integrace IDM a vybraných stávajících informačních systémů (dále též jen IS) provozovaných (na infrastruktuře Zadavatele) nebo využívaných (vzdáleným přístupem) Zadavatelem (dále též integrační konektory na informační systémy). Tyto integrační konektory budou umožňovat synchronizace identit, organizačních struktur a funkčních míst, event. jednotlivých rolí, pokud je IS již nyní schopen roli definovat-vygenerovat, vytváření speciálních skupin, řízení práv, zástupy v nepřítomnosti a potvrzení komunikace (mezi IDM a IS).

Zadavatel požaduje integraci s vybranými povinnými systémy viz. příloha č. 3 ZD. Pro implementaci rozhraní IDM na vybrané IS (viz příloha č. 3 ZD) Zadavatel požaduje obecnou specifikaci rozhraní systému IDM na další systémy a možností jejího přizpůsobení; všechny tyto specifikace budou vedeny v dokumentaci dle čl. 14.8 návrhu smlouvy o dílo.

Implementace dalších rozhraní, nad rámec přílohy č. 3 ZD, (například nově pořizované systémy) bude řešena v rámci rozšířené podpory nebo je zadavatel realizuje na základě dalších zakázek.

V rámci zakázky musí být zajištěna podpora systému jako celku (včetně implementovaných rozhraní).

Architektura IdM (viz obrázek 1) musí být centrálně orientovaná, přičemž jednotlivé koncové systémy budou k centrálnímu uzlu (IdM) napojeny pomocí tzv. konektorů, nebo též adaptérů či agentů. Koncové systémy jsou všechny aplikace či systémy, které obsahují vlastní úložiště uživatelských účtů. Konektor je pak komponenta IdM, která abstrahuje spojení k úložišti uživatelů v koncovém systému, případně pak obstarává další operace, jako je například řízení domovských adresářů nebo poštovních schránek.



Obrázek 1 – Schéma architektury IDM

Minimální požadavky na synchronizace identit:

- Vytvoření uživatelského účtu
- Změna uživatelského účtu
- Smazání uživatelského účtu
- Aktivace / deaktivace uživatelského účtu
- Změna a reset hesla uživatele (pomocí samoobsluhy)
- Nastavení hesla při jeho zapomenutí uživatelem
- Zpětné vrácení aktuálního stavu účtů včetně všech atributů a souvisejících identit, které se nastavují v operacích uvedených výše
- Zpřístupnění dat zrušeného uživatele
- zařazení a vyřazení uživatele do / z role
- změna role / rolí
- změna rozsahu přidělených práv
- nastavení zastupování
- úplná synchronizace atomických práv k dané roli (tak aby respektoval potřeby každého IS)
- Změna zařazení uživatele do organizační struktury (v případě, že není synchronizována)
- Nastavení dočasného zastupování jiné osoby / jiných osob a to v režimu i částečně delegovaným práv

Autoritativním zdrojem informací pro IdM bude adresářová databáze, provozovaná v rámci personálního systému. Propojení bude realizováno z důvodu čtení informací o uživatelských identitách. Personální systém ale není (a nebude) jediným zdrojem. IdM musí být vybaveno rozhraním pro vstup údajů (viz povinné parametry systému).

Synchronizace dat mezi připojenými systémy bude probíhat automaticky minimálně jednou denně, konkrétní synchronizační požadavky budou definovány individuálně pro každý připojený systém v rámci detailního návrhu řešení. Synchronizaci bude možné spustit kdykoliv ručně nebo na základě automaticky detekovaného (bezpečnostního) incidentu. **Zdrojem informací o identitě bude IdM.**

Identita bude svázána k jednotlivým fyzickým osobám (popř. aplikacím v případě technických/aplikačních účtů) s vazbami a jejím obsahem budou atributy a vazby:

- Uživatelská jména a korespondující autentizační token
- Vztah k organizační jednotce/jednotkám s typem organizační jednotky (pevné i dynamické jednotce definované v rámci IdM)
- Vztah organizační jednotky k lokalitě a umístění (MHMP, městská část, apod.)
- Role – obecná role v rámci MHMP, nikoli systému (např. účetní, sekretářka, apod.)
- Konkrétním role v rámci aplikace, systému, modulu s její strukturou – složením atomických práv – a tedy i s atomickými právy v rámci jednotlivých rolí.
- Vazba na elektronický certifikát
- Vazba na JIP, pokud má daná fyzická osoba platnou identitu v rámci JIP
- Vztah ke katalogu aplikací, systémům, modulům

Atributy identity musí být minimálně:

a. jméno,
b. příjmení,
c. osobní číslo,
d. uživatelské jméno,
e. mail,

f. telefon,
g. funkce (pracovní zařazení),
h. název oddělení,
i. název odboru
j. název sekce
k. organizační jednotka (MHMP, P1, P2, ...),
l. lokalita – pracoviště
m. fotografie,
n. datum exspirace účtu a hesla, pokud má pracovněprávní vztah zaměstnance známé datum ukončení.
o. elektronický certifikát

1.3 Školení pracovníků Zadavatele pro administrátory a uživatele IDM, zpracování provozní dokumentace v českém jazyce

Předmětem veřejné zakázky je rovněž provedení školení pro uživatele a administrátory Zadavatele k používání a správě IDM:

- Školení 5 administrátorů IDM a 5 uživatelů webového portálu IDM v maximálním počtu interních identit v minimálním rozsahu 56 hodin. Školení musí proběhnout v sídle Zadavatele, a to před zahájením testovacího provozu dle harmonogramu uvedeného v detailním návrhu řešení.

Za organizační zajištění školení zodpovídá Dodavatel. Zadavatel zajistí pro školení bezplatné použití své počítačové učebny a zasedací místnosti. Instalaci IDM na PC v učebně provede Dodavatel.

Zadavatel požaduje, aby Dodadal dodal jako součást zakázky ještě před termínem školení a prezentace provozní dokumentaci v českém jazyce ke všem systémům a aplikacím dodaným v rámci zakázky, a to na CD/DVD. Provozní dokumentace obsahuje zejména bezpečnostní, administrátorskou a uživatelskou příručku a další potřebné materiály. V rámci dodávky nových verzí systémů a aplikací je Dodavatel povinen udržovat provozní dokumentaci v aktuálním stavu a aktualizované verze předávat v elektronické formě Zadavateli nejpozději současně s dodávkou nových verzí.

1.4 Poskytování služeb technické podpory provozu IDM

- Poskytování služeb technické podpory a definice SLA je specifikován ve Smlouvě o podpoře - příloha č. 2b ZD

1.5 Jednotlivé etapy předávání díla

Dílo bude realizováno a předáváno po etapách. Etapy vycházejí z hrubého harmonogramu, které jsou uvedeny v čl. 3.1. ZD. Začátek každé etapy je vázán protokolárním převzetím předchozí etapy Zadavatelem na základě akceptačního protokolu.

a) V první etapě bude:

1.3 vypracováni detailního návrhu řešení včetně upřesnění dílčích částí hrubého harmonogramu,

1.4 interní oponentura a vypořádání připomínek,
1.5 akceptace a převzetí detailního návrhu řešení.

b) Druhá etapa zahrnuje:

1.6 implementaci systému a požadovanou integraci dle přílohy č. 3 ZD na základě upřesněného harmonogramu, jež byl akceptován v rámci detailního návrhu řešení
1.7 provedení školení, vypracování dokumentace,
1.8 akceptační zkoušky,
1.9 akceptace a převzetí implementované části díla do zkušebního provozu,
1.10

c) Třetí etapa zahrnuje:

1.11 zkušební provoz, v rámci kterého bude prověřena funkčnost díla v rutinním prostředí Zadavatele,
1.12
1.13 akceptaci a převzetí díla do rutinního provozu.

d) Čtvrtá etapa představuje:

1.14 rutinní provoz a podporu systému.

1.6 Formulář plnění technických požadavků

V níže uvedené tabulce jsou uvedeny veškeré povinné minimální parametry kladené na celý systém IDM. Nesplnění těchto požadavků je důvodem k vyřazení nabídky.

Dodavatel v níže uvedených tabulkách vyplní sloupce „Vyjádření ANO/NE" a „Popis jak bude požadavek splněn/řešen".

Sloupec „Vyjádření ANO/NE" může nabývat pouze hodnot ANO nebo NE, bude-li uvedeno něco jiného, je to rovněž důvod k vyřazení nabídky.

Sloupec „Popis jak bude požadavek splněn/řešen" bude obsahovat podrobný popis, jak dodavatel požadavek naplní.

Nebude-li popis splnění/řešení požadavku odpovídat popisu požadavku, tato skutečnost může mít za následek i to, že bude konstatováno, že dodavatel nesplnil zadávací podmínky stanovené Zadavatelem.

ID	Popis požadavku	Vyjádření [ANO/NE]	Popis jak bude požadavek splněn/řešen	Poznámka k hodnocení
Obecné požadavky				
1	Uživatelské rozhraní dodaného řešení musí být v českém jazyce a to včetně nápovědy. Jde zejména o část řešení určené pro schvalovatele a „běžné“ uživatele systému. Výjimku z tohoto pravidla může představovat část řešení určená výhradně pro administraci systému (konzole správce), kterou lze dodat i v angličtině.	Ano	Uživatelské rozhraní je standardně dodáváno kompletně lokalizované v češtině, angličtině a několika dalších světových jazycích.	Bude hodnoceno.
2	Systém pro správu identit musí umět zobrazovat české znaky.	Ano	Řešení využívá Unicode a zobrazuje tedy veškeré české znaky.	Bude hodnoceno.
3	V rámci dodávky dodavatel zajistí licence k celému navrženému řešení na minimálně 20 000 identit a bez omezení na počet koncových systémů, procesorových jader, velikost paměti a jiné hardwarové, softwarové a aplikační parametry. Licence umožňuje připojení budoucích nových koncových systémů a vložení jejich přístupových rolí a logiky do systému IDM a to bez dalších požadavků na licence.	Ano	Řešení není licenčně omezené na počet uživatelů, počet koncových systémů, procesorových jader, velikost paměti a jiných hardwarových, softwarových a aplikačních parametrů, pro aktuální i budoucí požadavky Zadavatele.	Bude hodnoceno.
4	Součástí dodávky je dokumentace, zejména bezpečnostní, administrátorská a uživatelská příručka tvořící část znalostní báze vedené v nástroji určeným zadavatelem.	Ano	Součástí dodávky je dokumentace, zejména bezpečnostní, administrátorská a uživatelská příručka tvořící část znalostní báze vedené v nástroji určeným Zadavatelem.	Bude hodnoceno.
Požadavky na architekturu systému				

ID	Popis požadavku	Vyjádření [ANO/NE]	Popis jak bude požadavek splněn/řešen	Poznámka k hodnocení
5a	Systém pro správu identit 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.	Ano	Systém pro správu identit umožňuje implementaci procesů a rozhraní dle zmiňované normy pro všechny požadavky relevantní pro identity management systém.	Bude hodnoceno.
5b	Systém pro správu identit umožní provádění správy identit v rozsahu interních a externích zaměstnanců, a to na základě propojení organizační struktury, pracovní pozice a stupně oprávnění (přístupů) jednotlivých uživatelů. Platí, že Identita se bude v organizační struktuře vyskytovat právě jednou, tedy nebudou v systému dvě různé identity odkazující na stejný subjekt (bez ohledu na to, zda se jedná o osobu nebo systémovou identitu).	Ano	Systém umožňuje spravovat veškeré zmiňované typy identit a jejich vzájemných vazeb. Veškeré entity v systému existují pod jednoznačným identifikátorem a kontrolními mechanismy zabraňujícími duplicitnímu výskytu entit. Konkrétní mapování a hierarchii identit určí analýza.	Bude hodnoceno.
6	Organizační struktura identit bude v Informačním systému pro správu identit zastoupena hierarchickou strukturou, pod kterou budou umístěny jednotlivé identity. Tato struktura bude obsahovat interní i externí organizační členění. Systém pro správu identit umožní hromadné načítání organizační struktury (například z personálního systému) nebo její manuální pořízení a editaci .	Ano	Řešení umožňuje jak přejímání a synchronizaci, organizační struktury z externího zdroje, tak její manuální editaci v rámci grafického rozhraní s následnou projekcí na koncový systém.	Bude hodnoceno.

ID	Popis požadavku	Vyjádření [ANO/NE]	Popis jak bude požadavek splněn/řešen	Poznámka k hodnocení
7	Systém pro správu identit musí umožnit práci s více organizačními strukturami: • Vytváření libovolného počtu stromů. • Vytváření nezávislých entit (pracovní pozice, funkční místa) ve stromě. • Definovat atributy entit ve stromě. • Přiřazovat entitám ve stromě jiné objekty, zejména: o role o jiné entity stromu o účty v koncových systémech. • Vizualizace entit pomocí stromové struktury. • Entity ve stromě přiřazovat k libovolnému objektu, zejména: o roli o uživateli • Uživatel nebo role může být přiřazen ve více entitách stromu zároveň. • Uživatel nebo role může být přiřazen ve více stromech zároveň. • Uživatel může mít různé role v různých strukturách (nadřízený v jedné organizační struktuře může být v jiné struktuře podřízený apod.)	Ano	Počet organizačních struktur, jejich členění ani počet stromů není řešením nijak limitováno. Je možné vytvářet různé logické pohledy na stejná data a evidovat tutéž identitu víckrát v různých stromech. Struktura je vizualizována v grafickém rozhraní. Entity ve stromě lze přiřazovat k libovolnému objektu, zejména roli a uživateli. Uživatel nebo role může být přiřazen ve více entitách stromu zároveň. Uživatel nebo role může být přiřazen ve více stromech zároveň. Uživatel může mít různé role v různých strukturách (nadřízený v jedné organizační struktuře může být v jiné struktuře podřízený apod.)	Bude hodnoceno.

ID	Popis požadavku	Vyjádření [ANO/NE]	Popis jak bude požadavek splněn/řešen	Poznámka k hodnocení
8	Systém IDM musí umožnit: • připojení dalších organizací, především městských částí a příspěvkových organizací HMP. • separovat identity a role pro jednotlivé organizační struktury. • pracovat s různými organizačními strukturami, nebo separovanými částmi IDM, tak, aby bylo možné rozdělit správu separovaných částí mezi konkrétní správce, kteří mají přístup do relevantní části IDM a mohou spravovat přístupy uživatelů identifikovaných v této části do systémů MHMP; podmínky a rozsah takové separátní správy bude nastavovat odpovědný zaměstnanec MHMP. • realizovat federalizovanou celoměstskou identitu	Ano	Řešení umožňuje multitenancy – oddělení jednotlivých tenantů (jeden tenant = jeden zákazník systému, například jedna městská část) napříč řešením. Částečnou správu řeší systém delegovanou administrací s vydefinovaným rozsahem jak do záběru, tak do schopností, které uživatel či administrátor má.	Bude hodnoceno.
9	Systém pro správu Identit bude možné postavit jako distribuovanou aplikaci, aby bylo možné jej provozovat ve vysoké dostupnosti zajištěné pouze SW konfigurací.	Ano	Řešení podporuje HA na více úrovních. Podpora pro spuštění více instancí (nodů) nad jedním repository - úlohy mohou běžet na kterémkoliv nodu (rekonciliace, schvalování), uživatelé mohou používat libovolný node. https://wiki.evolveum.com/display/midPoint/High+Availability+and+Load+Balancing	Bude hodnoceno.

ID	Popis požadavku	Vyjádření [ANO/NE]	Popis jak bude požadavek splněn/řešen	Poznámka k hodnocení
10	SSO bude fungovat tak, že se uživatel přihlásí do systému a bez nutnosti dalšího přihlašování se bude moci přihlásit k dalším informačním systémům a to jak k desktopovým, tak k webovým. Zároveň musí být zachována možnost vynutit znovu zadání přihlašovacích údajů do vyjmenovaných systémů. Řešení SSO musí být postaveno tak, aby uživatelům umožnilo přístup i v případě výpadku serverové části systému. Zároveň nesmí být údaje SSO uloženy jen na koncovém klientském zařízení, aby nemohlo dojít ke ztrátě informací v případě poruchy tohoto zařízení. SSO systém umožní přístup k systému pomoci privilegovaného přístupu. Uložiště hesel systému SSO musí být zašifrované. Po úspěšné autentizaci bude možné umožnit přístup uživateli k jeho přihlašovacím údajům. Podpora více faktorové autentizace bude součástí dodaného SSO řešení. Nasazení dalšího autentizačního faktoru nebude vyžadovat žádné další licence nebo náklady na rozšíření SSO (výjimkou mohou být náklady na uživatelské HW tokeny a certifikáty).	Ano	Řešení obsahuje komponentu CAS, která podporuje všechny běžně dostupné protokoly a standardní bezpečnostní procesy pro Single SignOn. Konkrétní postupy a protokoly budou vydefinovány na základě analýzy.	Bude hodnoceno.
11	Systém pro správu identit umožní paralelní práci uživatelů v grafickém rozhraní (tenký klient). Rozhraním systému pro správu identit bude webový prohlížeč. Podporován bude minimálně Internet Explorer, a Google Chrome.	Ano	Řešení podporuje veškeré standardně používané moderní webový prohlížeče, tedy i Internet Explorer a Google Chrome.	Bude hodnoceno.
Požadavky na funkcionalitu systému				

ID	Popis požadavku	Vyjádření [ANO/NE]	Popis jak bude požadavek splněn/řešen	Poznámka k hodnocení
12	Systém umožňuje správu různých typů objektů (identit uživatelů, funkčních míst, místností, organizační struktury, rolí, ...)	Ano	Řešení umožňuje, a je zaměřeno, na správu jmenovaných i dalších druhů objektů (identit uživatelů, funkčních míst, místností, organizační struktury, rolí, ...)	Bude hodnoceno.
13	Uživatelské rozhraní musí splňovat tyto parametry: • Použití tlustého klienta není přípustné pro uživatelské, konfigurační ani správcovské činnosti. • Rozhraní je možné upravovat dle potřeb klienta.	Ano	Řešení využívá tenkého webového klienta pro jmenované činnosti. Řešení je možno jednoduše brandovat dle potřeb Zadavatele v minimálním rozsahu logo + barvy. Dále je možná snadná úprava veškerých vstupních formulářů dle potřeby. Větší zásahy do grafického rozhraní jsou řešitelné, nicméně je generována pracnost.	Bude hodnoceno

ID	Popis požadavku	Vyjádření [ANO/NE]	Popis jak bude požadavek splněn/řešen	Poznámka k hodnocení
14	Řešení IdM musí být schopné jemné granularity přidělování autorizačních oprávnění: • Autorizační model je založen na RBAC (Role-Based Access Control) přístupu. • Oprávnění jsou součástí rolí, role jsou přiděleny uživatelům. • Musí být možné nastavit, k jaké části uživatelského rozhraní mají uživatelé přístup. • Řešení IdM musí umožňovat nastavit práva až na úroveň atributu libovolného typu objektu. Práva musí být přidělitelná uživateli, roli nebo organizaci.	Ano	Řešení podporuje jemnou granularitu přístupových oprávnění. Ta mohou obsahovat oprávnění směrem k uživatelům, organizačním jednotkám, skupinám či službám v úrovních od zakázání/povolení změny jednotlivých atributů až po viditelnost objektu. Role jsou aplikovány přímo na uživatele, je však možné role získávat na základě zařazení (např. role je přiřazena na organizační jednotku, přičemž dojde k zdědění role uživatelem, jež je do org. jednotky zařazen) Koncová oprávnění/role je možné skládat do tzv. business rolí, jež umožňují lepší čitelnost a transparentnost.	Bude hodnoceno.

ID	Popis požadavku	Vyjádření [ANO/NE]	Popis jak bude požadavek splněn/řešen	Poznámka k hodnocení
15	Správa přístupu se bude dít pouze na základě změny členství v rolích. Roli je možné přiřazovat uživatelům i organizacím. Platnost přiřazení role uživateli i organizaci od-do. Možnost nastavit další atributy přiřazení. Schvalovatelé role včetně možností dynamického výpočtu. Role je možné hierarchicky skládat. Řízení autorizačních objektů v koncovém systému Možnost svázat definici role s existencí objektu oprávnění v koncovém systému. (Například role zodpovídá za vytvoření objektu skupiny v Active Directory)	Ano	Řešení umožňuje pracovat s rolemi ve vydefinovaném rozsahu. Tato funkcionalita robustního role managementu je základním pilířem řešení. Je možná taktéž správa autorizačních objektů v autorizačních úložištích, například v AD. Veškeré objekty mohou či nemusí mít libovolný počet projekcí (reprezentací na koncových systémech), jež se při práci s touto rolí chovají dle definovaných pravidel.	Bude hodnoceno.
16	U systémů, kde nebude možné automatické správa přístupů na základě změny rolí, musí systém zaslat notifikaci s přesným popisem, co se má nastavit správci dané agendy (resp. aplikace, systému). Tento správce po provedení potvrdí založení zpět do systému pro správu Identit.	Ano	Řešení podporuje takzvané nepřipojené systémy a role s manuální konfigurací, které se používají v případě, že koncový systém nelze z IdM přímo řídit, nebo nepodporuje některou funkcionalitu. V takovém případě je přidělení oprávnění prováděno administrátorem na základě notifikace správce (sms, e-mail). Po přidělení role je zaznamenáno/potvrzeno do systému.	Bude hodnoceno.

ID	Popis požadavku	Vyjádření [ANO/NE]	Popis jak bude požadavek splněn/řešen	Poznámka k hodnocení
17	Řešení IdM musí mít implementovaný mechanismus časově omezených rolí (od-do): Musí umožňovat nastavit časové období od-do pro přiřazení role uživateli. Pokud časové období uplyne nebo ještě nenastalo, nesmí se přiřazení role uplatnit.	Ano	V rámci řešení lze na všechny spravované objekty/entity aplikovat časová omezení, která jsou systémem vyhodnocována a na základě těchto limitů realizovány příslušné akce v bodě počátku platnosti a zneplatnění.	Bude hodnoceno.
18	Řešení IdM musí umožňovat mechanismus certifikace rolí. Cílem je ověření, že všechna přidělení rolí jsou aktuální a chtěná. V nástroji Identity managementu je možné spustit úlohu z grafického rozhraní, která zajistí schvalování pro všechny role přidělené identitám. Tuto úlohu je možné opakovaně spouštět (tzv. recertifikace rolí).	Ano	Mechanismus pro ověřování rolí je integrován v rámci řešení. V řešení je možné manuálně či periodicky spouštět Recertifikační kampaně, kde dojde ke znovu-schvalování jednotlivých práv uživatele vlastníky systémů/vedoucími dle nastavených pravidel.	Bude hodnoceno.

ID	Popis požadavku	Vyjádření [ANO/NE]	Popis jak bude požadavek splněn/řešen	Poznámka k hodnocení
19	Řešení IdM musí poskytovat grafické rozhraní pro schvalovací procesy. Musí splňovat minimálně následující požadavky: Notifikace schvalovatele minimálně emailem. Schvalovatelé si mohou zobrazit přehled svých úloh. Možnost úlohu schválit či zamítnout včetně uvedení zdůvodnění. Schvalovací workflow musí podporovat vícekrokové schvalování. Schvalovat může jednotlivec nebo skupina schvalovatelů. Je možné určit typ schválení "všichni ze skupiny" nebo "jeden ze skupiny". Správce IdM musí být schopen pracovat se všemi úlohami (pro řešení nestandardních situací). Systém workflow obsahuje možnost větvení pro ošetření výjimek vzniklých při schvalování, upozorňování prostřednictvím mailu, řešení zastupitelnosti a eskalaci upozornění při nesplnění termínu splnění.	Ano	Řešení obsahuje mechanismus schvalování žádostí o přidělení oprávnění, který umožňuje mimo jiného: - Notifikaci schvalovatele emailem, SMS (včetně upomínání), - zobrazení přehledu úloh pro schvalovatele, - schválit či zamítnout úlohu včetně uvedení zdůvodnění, - vícekrokové schvalování. Schvalovat může jednotlivec nebo skupina schvalovatelů. Je možné určit typ schválení "všichni ze skupiny" nebo "jeden ze skupiny"(skupinou vnímáme roli či organizační jednotku, potažmo příznak uživatele). Správce IdM může pracovat se všemi úlohami a zasahovat do nich (pro řešení nestandardních situací). Systém workflow obsahuje možnost větvení pro ošetření různých stavů dle potřeby.	Bude hodnoceno.

ID	Popis požadavku	Vyjádření [ANO/NE]	Popis jak bude požadavek splněn/řešen	Poznámka k hodnocení
20	Systém pro správu identit umožní diferencovaný přístup pro interní a externí identity – takzvaná delegovaná administrace. Tyto identity musí mít administrátorská práva nad zvolenými komunitami nebo skupinami uživatelů. Účelem je umožnit lokálnímu administrátorovi správu nad uživateli patřícími do samostatného podřízeného celku (ať už z pohledu interního, tak externího - například dodavatelské účty).	Ano	Řešení umožňuje delegovanou administraci se specifikací rozsahu (skupiny, organizační hierarchie) a práv nad těmito entitami v rámci systému.	Bude hodnoceno.
21	Řešení IdM musí mít implementovaný mechanismus časově omezeného přiřazení do stromové struktury např. do organizací. Musí umožňovat nastavit časové období od-do pro přiřazení uživatele do stromové struktury. Pokud časové období uplyne nebo ještě nenastalo, nesmí se přiřazení uživatele do stromu uplatnit.	Ano	V rámci řešení lze na všechny spravované objekty/entity aplikovat časová omezení, která jsou systémem vyhodnocována a na základě těchto limitů realizovány příslušné akce v bodě počátku platnosti a zneplatnění.	Bude hodnoceno.

ID	Popis požadavku	Vyjádření [ANO/NE]	Popis jak bude požadavek splněn/řešen	Poznámka k hodnocení
22	Se systémem pro správu identit umožní pracovat minimálně následujícím skupinám uživatelů. Tyto jsou reprezentovány charakteristickými oprávněními v rámci IDM systému a vážou se ke stromové struktuře, kde jsou identity umístěny. Předpokládané skupiny jsou zejména následující: • administrátor IDM systému, • personalista, • helpdeskový operátor, • administrátor připojeného systému nebo vlastník aplikace či agendy, • administrátor bezpečnosti informací nebo auditor, • nadřízený zaměstnance nebo jeho delegát, • zaměstnanec interní nebo externí. Toto bude upřesněno v Detailním návrhu řešení.	Ano	Řešení obsahuje jedno jednotné uživatelské rozhraní, kde je funkcionalita řízena pouze uživatelskými oprávněními. Je možné kombinovat tato oprávnění právě tak aby odpovídala typu/skupině uživatelů, kteří pak vidí pouze potřebný rozsah z funkcionalit Identity Manageru a mají přístup dle stanoveného rozsahu (skupinou uživatelů, systémem, částí organizační struktury, ...).	Bude hodnoceno.
23	Webová konzole administrátora systému IDM bude mít grafické rozhraní, které umožní správu všech objektů IDM a nastavení samotného systému IDM: • Vyhledávat uživatele podle atributů (viz níže). • Editovat profil uživatele. • Uložit a zobrazit k uživateli fotografii. • Evidovat u uživatele atributy, které mohou být jednohodnotové, vícehodnotové, binární či definované komplexní struktury (tabulky). • Uživatele je možné zneplatnit k určitému datu. • Uživateli je možné přiřadit koncové systémy, role a organizace.	Ano	Řešení obsahuje jedno jednotné uživatelské rozhraní, kde je funkcionalita řízena pouze uživatelskými oprávněními. Role administrátora má k dispozici veškeré funkcionality v rámci grafického rozhraní. Veškeré zmiňované požadavky jsou tímto rozhraním poskytnuty (viz demo).	Bude hodnoceno.

ID	Popis požadavku	Vyjádření [ANO/NE]	Popis jak bude požadavek splněn/řešen	Poznámka k hodnocení
24	Řešení IdM musí v grafickém rozhraní umožnit vyhledávání a filtrování: • uživatelů podle loginu, jména, příjmení a celého jména, • rolí podle jména, • organizací podle jména.	Ano	V rámci řešení je možné uživatele, role i organizace filtrovat a vyhledávat dle libovolného atributu.	Bude hodnoceno.

ID	Popis požadavku	Vyjádření [ANO/NE]	Popis jak bude požadavek splněn/řešen	Poznámka k hodnocení
25	Webový portál Systému pro správu identitu umožní interním a externím zaměstnancům minimálně tyto funkce: • Zobrazení základních informací o profilu přihlášeného uživatele: o přehled schválených rolí, o přehled rolí, které jsou svázány se zastávanou pracovní pozicí, o přehled oprávnění na jednotlivých koncových systémech. • Změnu hesla na všech nebo vybraných koncových systémech. • Změnu definovaných atributů přihlášeného uživatele dle jemu přidělené role. • Poskytne informace o organizační struktuře úřadu a jim zřizovaných organizací. • Vedoucím pracovníkům umožní vložit požadavky na změny v přiřazení rolí pro podřízené pracovníky a sledovat stav vyřizování jejich žádostí. • Schvalovatelům umožní rozhodování o schválení či zamítnutí vznesených požadavků. • Auditorům umožní generovat reporty o identitách a operacích celého systému.	Ano	Řešení obsahuje uživatelskou samoobsluhu, přístupnou všem přihlášeným uživatelům. Samoobsluha umožňuje mimo jiného: - Zobrazení základních informací o profilu přihlášeného uživatele: přehled schválených rolí, přehled rolí, které jsou svázány se zastávanou pracovní pozicí, přehled oprávnění na jednotlivých koncových systémech, - změnu hesla na všech nebo vybraných koncových systémech, - změnu definovaných atributů přihlášeného uživatele dle přidělené role, - poskytuje informace o organizační struktuře úřadu a jim zřizovaných organizací. Dále řešení obsahuje rozhraní pro schvalování požadavků – součást schvalovacího workflow. Auditorům jsou poskytovány reporty o objektech a činnostech v systému (například historii změn identit) v automatickém (pravidelné zasílání na mail) či manuálním režimu.	Bude hodnoceno.

ID	Popis požadavku	Vyjádření [ANO/NE]	Popis jak bude požadavek splněn/řešen	Poznámka k hodnocení
26	Informační systém pro správu identit poskytne nástroje potřebné ke zřízení, správě a zrušení účtu uživatele na základě změny v přiřazení rolí.	Ano	Řízení změn na základě role (RBAC) je jedna ze základních funkcionalit nabízeného IdM řešení.	Bude hodnoceno
27	Systém musí zajišťovat minimálně pro následující operace s Identitou a jejími oprávněními: • vytvoření Identity interního zaměstnance, • vytvoření Identity externisty, • přidělení oprávnění, • odebrání oprávnění, • nástup do vynětí, • návrat z vynětí, • přejmenování včetně vytvoření aliasu na mailbox • změna pracovní pozice, • změna hesla, • ukončení identity interní i externí. • založení/zrušení/deaktivace mailboxu, • zánik identity definovaným způsobem dle IS: smazání, deaktivace, nastavení • vytvoření aliasu na mailbox (např. při změně příjmení) atributů, včetně možnosti zpožděného výmazu účtů počítaného od data zneplatnění identity.	Ano	Řešení reflektuje kompletní životní cyklus identity, životního cyklus zahrnuje uvedené požadavky na operace týkající se zaměstnance. Na tyto uvedené akce lze navěsit business logiku a akce dle přání Zadavatele. Operace týkající se mailboxu jsou výsledkem standardní změny v rámci IdM řešení reprodukované na koncový systém pomocí konektoru.	Bude hodnoceno.
28	Systém pro správu identit umožní definovat vlastní parametry k identitám.	Ano	Schéma identit lze bez systémové změny rozšiřovat dle přání a obohacovat tak identity o vlastní atributy.	Bude hodnoceno.

ID	Popis požadavku	Vyjádření [ANO/NE]	Popis jak bude požadavek splněn/řešen	Poznámka k hodnocení
29	Systém pro správu identit umožní administrátorovi IDM definovat a nastavit položky, které si uživatelé jednotlivých typů mohou sami měnit, které jsou povinné atd. Například externímu uživateli umožnit změnu mobilního telefonu, místnosti.	Ano	Nastavitelnými oprávněními je možno řídit přístup až po úroveň atributu uživatele. Danou problematiku je možno tedy řešit přiřazením příslušných oprávnění uživateli.	Bude hodnoceno.
30	Systém IDM eviduje k identitám veškeré přidělené certifikáty (certifikáty bankovní a dalších autorit, certifikáty, osobní, komerční, atd.)	Ano	K identitě lze přidat libovolný počet extensivních atributů různých typů zahrnujících textový i binární typ. Certifikáty je možno tedy schraňovat v této formě. Atributům lze navíc nastavit pro ukládání možnost šifrování.	Bude hodnoceno.
31	Systém pro správu identit umožní oprávněným uživatelům přehledné zobrazení, vyhledávání a filtrování v jím evidovaných položkách.	Ano	Jednotné grafické rozhraní poskytuje přehledné zobrazení, vyhledávání a filtrování položek, na něž má daný uživatel oprávnění.	Bude hodnoceno.
32	Systém IDM umožní automatické přidělení předem schválených rolí identitě na základě hodnot atributů identity (automatické přidělení role).	Ano	Řešení umožňuje automaticky přidělovat oprávnění na základě hodnoty atributů identity, její zařazení v organizační struktuře či příslušenství ke skupině, jejímž je členem.	Bude hodnoceno.

ID	Popis požadavku	Vyjádření [ANO/NE]	Popis jak bude požadavek splněn/řešen	Poznámka k hodnocení
33	Řešení umožňuje definovat a pravidelně spouštět serverové úlohy (nejrůznější transformační, kontrolní a notifikační úlohy).	Ano	Řešení plně podporuje periodické a manuální spouštění definovaných i definovatelných serverových úloh (transformačních, kontrolních, notifikačních a dalších).	Bude hodnoceno.

ID	Popis požadavku	Vyjádření [ANO/NE]	Popis jak bude požadavek splněn/řešen	Poznámka k hodnocení
34	Řešení musí splňovat požadavky na synchronizaci a rekonciliaci účtů a oprávnění: • Synchronizace změn v reálném čase • Obousměrná synchronizace dat jak z IDM do koncového systému (např. uživatele a jejich atributy), tak ze spravovaného systému do IdM (např. role v konkrétním systému). • Mapování atributů mezi informačními systémy na základě pravidel/vzorců. • Práce s komplexními (tabulky) či binárními atributy uživatele - certifikáty, fotografie, autentizační tokeny. • Rekonciliace účtů - pravidelná automatická kontrola stavu účtů na koncových systémech s autoritativním vypořádáním nesouladu. • Rekonciliace účtů - zaznamenání stavu účtu vzhledem k ne/existenci vlastníka v IdM. • Rekonciliace oprávnění - pravidelná automatická kontrola stavu oprávnění na koncových systémech oproti stavu chtěnému a náprava (notifikace, zápis do logů, výmaz nadbytečných oprávnění apod.). • Nastavení párovacích pravidel mezi identitou a účtem (například email identity na login účtu). • Synchronizace hesel z IdM do koncového systému.	Ano	Řešení umožňuje synchronizaci a rekonciliaci spravovaných entit z/ do IdM. V rámci konfigurace obsahující mapování lze uplatňovat jak transformace dat, tak i politiky uplatňování změny dat (jaká data jsou autoritativní, zda ta na koncovém systému či v IdM, zda-li data převzít pouze, když entitě chybí apod..). Veškeré tato nastavení jsou konfigurovatelná separátně pro oba směry. Systém umožňuje práci s komplexními datovými typy včetně dat v textové i binární formě (soubory veškerých typů včetně fotografií, binárních souborů, xml, autentizačních tokenů apod..) Rekonciliace je standardní plánovatelnou úlohou, jež lze nastavit v pravidelných intervalech. Úloha kontroluje nesoulady jednotlivých entit, u kterých následně dojde k úpravě ke stavu odpovídajícímu nastaveným pravidlům, popřípadě dojde k notifikaci o např. neočekávaném stavu. V rámci nastavení synchronizace je možné zavést jednoduchá i komplexní pravidla pro párování identit. Hesla jsou jedním z přenášených a porovnávaných atributů s rozdílem, že se s atributem nikdy nepracuje jako s textem, nicméně dochází k porovnávání šifrovaných otisků hesla, dle politiky systému.	Bude hodnoceno.

ID	Popis požadavku	Vyjádření [ANO/NE]	Popis jak bude požadavek splněn/řešen	Poznámka k hodnocení
35	Řešení IdM musí umožňovat zasílání emailových notifikací: • Možnost definice šablon emailů, • s podpora vícejazyčnosti. • Možnost konfigurace parametrů odesílání zpráv (SMTP server a podobně).	Ano	Řešení umožňuje zasílat emailové notifikace v jazyce uživatele dle zvolené šablony. Parametry SMTP serveru je možné konfigurovat v administrativním rozhraní.	Bude hodnoceno.
Požadavky na integraci systému				
36	Systém pro správu identit umožní udržovat organizační struktury identit ve své vnitřní databázi. Tyto identity ve vnitřní databázi budou sloužit jako referenční identity pro ostatní vnitřní i vnější informační systémy, se kterými zadavatel komunikuje.	Ano	Řešení IdM využívá vnitřní databáze pro udržování veškerých entit, včetně organizační struktury. V rámci systému lze udržovat a spravovat libovolné množství organizačních struktur synchronizovaných s koncovými aplikacemi. V synchronizovaném stavu lze tyto struktury považovat za referenční.	Bude hodnoceno.

37	Systém pro správu identit umožní spravovat identity stávajících a budoucích nových aplikací a vložení jejich přístupových rolí a logiky do systému v rámci svého grafického prostředí.	Ano	Řešení umožňuje správu identit a jejich práv na existujících systémech i těch budoucích skrze projekcí potažmo ideálně rolí reprezentujících existenci entity na koncovém systému.	Bude hodnoceno.
38	Zdrojem změn (vznik, změna login, zrušení) spravovaných interních identit systému pro správu identit bude personální systém. Bude zajištěna integrace personálních informací z HR systému se systémem pro správu identit. V IDM bude zaveden systém validace vstupních dat z personálního systému a bude prováděna pravidelná kontrola (rekonciliační audit) účtů zaměstnanců bez nutnosti ručního zásahu správce. Audit bude správcem či auditorem ručně spuštěn, systém vše dále provede automaticky. Chyby či rozdíly budou jasně a přehledně vyznačeny. Prováděné operace budou kompletně logovány Budou implementovány ochrany pro zamezení nežádoucí nekonzistence v připojených systémech vlivem možných chyb v systémech nebo datech v IdM.	Ano	Zdrojem identit může být jak samotný systém IdM, tak jeden nebo více externích zdrojů – typicky HR aplikace. Řešení obsahuje velmi flexibilní systém mapování dat, v kterém se dají aplikovat požadované validace. Řešení obsahuje obecné logování i historii o prováděných operacích nad jednotlivými entitami systému, umožňující spustitelnou úlohu auditu systému, generující report. Rekonciliační pravidla budou sloužit k zamezení jakékoliv nekonzistence systému, o případné nekonzistenci bude navíc systém informovat prostřednictvím notifikací.	Bude hodnoceno.

39	Řešení podporuje některý z rozšířených skriptovacích jazyků v konfigurovatelných částech Identity Manageru.	Ano	Řešení podporuje více skriptovacích jazyků, ovšem primárně využívaným je jazyk Groovy.	Bude hodnoceno.
40	Řešení IdM musí podporovat možnost vzdáleného programového volání: • Možnost volání za pomoci Web service API (SOAP/WSDL) nebo REST API. • Možnost volat ekvivalent jakékoli funkcionality, která je dosažitelná z webového rozhraní. • Možnost volání jen některých funkcí jádra IdM je pro tyto potřeby nedostatečná.	Ano	Řešení podporuje obě rozhraní (SOAP/WSDL) i REST API. Veškeré vykonatelné operace prostřednictvím grafického rozhraní IdM je možné provádět také skrze tato rozhraní.	Bude hodnoceno.
Požadavky na bezpečnost systému				
41	Řešení IdM musí podporovat zavádění, vynucování a kontrolu firemních politik.	Ano	Politiky jsou vynucovány pravidly, rolemi a serverovými úlohami implementovanými na úrovni IdM.	Bude hodnoceno.
42	Řešení IdM musí mít implementovaný mechanismus politiky hesla. Musí umožňovat nastavení pravidel pro minimální a maximální délku hesla, povolené skupiny znaků, počet opakování znaků, minimální a maximální výskyt znaků ze skupiny.	Ano	Řešení umožňuje definovat politiku hesel dle obvyklých kritérií zahrnující vyjmenované parametry.	Bude hodnoceno.
43	Řešení IdM musí mít implementovaný mechanismus politiky účtu. Musí umožňovat nastavení pravidel pro název účtu - minimální a maximální délka, povolené znaky, zakázaná slova v názvu (například *admin*, *info*), kontorla na platný formát emailové adresy.	Ano	Řešení umožňuje definovat politiku účtů dle zmiňovaných kritérií prostřednictvím konfigurace validace parametrů.	Bude hodnoceno.

44	Změna hesla bude prováděna pouze jednou, a tímto to jedním z níže uvedených způsobemů: • Uživatel změní heslo v samoobslužném rozhraní správy Identit. • Správa Identit zkontroluje heslo z pohledu nastavených politik, a přímo v portálu Systém pro správu identit, kdy se následně se heslo zpropaguje do ostatních spravovaných systémů .se propaguje,	Ano	Řešení funguje popsaným způsobem: Uživatel v samoobslužné části změní heslo. To je zkontrolováno proti politice hesel a následně rozesláno na definované řízené koncové systémy.	Bude hodnoceno.
45	Řešení IDM musí umět poskytnout dostatečně podrobná data pro nástroje dohledu a SIEM řešení, nicméně zahrne základní reportovací nástroj/modul, který: • umožní definovat pravidla pro vyhodnocení bezpečnostních záznamů z logů z pohledu hrozeb, anomálií, přístupů a prací s citlivými aplikačními daty. • bude provázán s IDM systémem tak, aby byla možná identifikace aktivit náležející jedné identitě ve všech systémech, kam přistupuje. • umožní v rámci správy identit reporting v kategoriích: „Kdy“, „Kdo“, „Co“ a „Kde“.		Řešení loguje veškerou svou aktivitu ve formě logů ve standardním formátu. Tyto logy je možné následně poskytnout SIEM řešení k analýze a dohledu. Logována je veškerá aktivita generována uživateli tak i pocházející ze systémových a jiných úloh a veškeré vykonávané procesy v pozadí jednotlivých operací. Model databáze Identity Manageru je dobře dokumentována, je proto také možné se na databázi napojit pomocí DWH/BI nástrojů https://wiki.evolveum.com/display/midPoint/Data+Model	Bude hodnoceno.

46	Systém pro správu identit umožní oprávněným uživatelům poskytnout aktuální reporty z jednotného grafického prostředí, zejména role a účty přiřazené identitám a sestavy požadavků v rámci workflow. Reporty budou dostupné skupinám uživatelů na základě přidělení oprávnění v IDM systému. Jedná se o reporty: Auditní report • Kompletní přehled změn provedených nad uživatelem – například synchronizace atributů, přidělení role včetně časového omezení, změna hesla atd. • Kompletní přehled změn provedených nad klíčovými entitami řešení - role, organizace, definice politik a konfigurací. • Záznam o přihlášení uživatele do webové rozhraní IdM. Report uživatelů • Informuje o tom, jaké mají uživatelé přiřazené role a účty v koncových systémech. • Možnost reportovat uživatele v určité organizaci. Report rekonciliace • Přehled účtů v koncových systémech, které jsou známy IdM k momentu spuštění reportu. • Možnost identifikace účtů, ke kterým nebyl v IdM nalezen vlastník.	Ano	Uváděné reporty jsou základní sadou reportů poskytovanou naším řešením IdM. Přístup k reportům je řízen skrze oprávnění jako u zbytku funkcionalit. Řešení dále umožnuje vytvářet další reporty dle zadání, skrze Jasper Editor - nástroj postavený na Eclipse studiu. Výsledné reporty jsou generovatelné ve formátech PDF, CSV, XLS a je možné je ukládat do databáze či na lokální úložiště.	Bude hodnoceno.

47	Systém musí logovat všechny bezpečnostně relevantní informace. Přístup k systému musí být vždy zabezpečen pomocí šifrování, a to i na interní síti (zejména použití HTTPS). Systém zahrnuje bezpečnostní dokumentaci, která bude obsahovat popis klíčových bezpečnostních mechanismů.	Ano	Logována je veškerá aktivita generována uživateli tak i pocházející ze systémových a jiných úloh a veškeré vykonávané procesy v pozadí jednotlivých operací. Přístup je zabezpečen HTTPS protokolem, řešení akceptuje certifikáty Zadavatele. Popis bezpečnostního nastavení je součástí Dokumentace skutečného provedení odevzdávané spolu s řešením po implementaci.	Bude hodnoceno