48	Systém musí splňovat následující technické požadavky: • Podpora jednoho z operačních systémů: UNIX/Linux, Windows • Jediné úložiště dat (repozitory) a to relační databázi, pro svůj provoz nevyžaduje LDAP server • Repozitory podporuje minimálně jednu z těchto relačních databází - MySQL 5, MS SQL Server 2014, Oracle DB 12, PostgreSQL 9.4, nebo novější verze • Řešení podporuje technologii Java 8 či .NET 4.5, nebo novější verze • Řešení je možné provozovat na jednom z aplikačních serverů: Apache Tomcat 8, Oracle Glassfish 3.1, Oracle WebLogic 12c, nebo novější verze • Řešení podporuje přístup pomocí zabezpečeného protokolu HTTPS s podporou technologie RSA a ECC	Ano	Řešení podporuje operační systémy UNIX/Linux a Windows. Řešení využívá jediné úložiště dat podporujíce veškeré změněné databáze. Řešení pro svůj běh využívá a podporuje technologii Java 8 a je možné jej provozovat nad webovými servery podporujícími Java konteinery včetně jmenovaných serverů a jejich verzí. Standardně je pro běh využíván Tomcat 8. Řešení podporuje přístup pomocí zabezpečeného protokolu HTTPS s podporou technologie RSA a ECC.	Bude hodnoceno
49	Systém poskytne takovou funkcionalitu, která zajistí, že uživatelé s administrátorským oprávněním se musí přihlašovat pomocí dvou faktorů. Prvním z nich je jméno a heslo (může být přebíráno automaticky z přihlášení do domény). Druhým z nich je jednorázové heslo, které je zasláno uživateli na e-mail, který je v systému pro správu identit u dané osoby evidován. Tato funkcionalita musí být realizována za pomoci nástroje CAS od společnosti Apereo, který je pro dané účely v prostředí MHMP provozován.	Ano	Řešení podporuje úpravu pro využití externích přihlašovacích zdrojů umožňujících popisované dvou-faktorové přihlašování. Systém CAS bude nakonfigurován dle popsaných parametrů.	Bude hodnoceno

2 Oblast PAM

Základní požadavky na řešení:

- Zajištění identifikace a správy všech správcovských účtů.
- Systém musí být integrován s běžně využívanými prvky infrastruktury (OS, virtuální servery, doménové a servisní účty, síťové a bezpečnostní prvky, SŘBD, standardně využívané aplikace).
- Řízení a správa centrální bezpečnostní politiky pro privilegované a správcovské účty aplikací, DB, uživatelů a zařízení.
- Poskytování privilegovaných přístupů a hesel k systémům pouze pro oprávněné administrátory na základě pověření.
- Vytváření záznamů (logů) o činnosti administrátorů, včetně možnosti nad kritickými systémy a aplikacemi pořizovat videonahrávky a pro CLI relace také textový přepis.
- Automatické změny hesel privilegovaných účtů v definovaných časových intervalech anebo jako jednorázové heslo pro přístup.
- Zabezpečení lokálních cache přihlašovacích údajů proti zneužití.
- Zajištění kontroly minimální formy hesel účtů.
- Zabezpečení nemožnosti vypnutí bezpečnostních pravidel a ochran privilegovanými uživateli (administrátory).
- Centrální nastavování oprávnění přístupu k systémům a aplikacím pro jednotlivce a skupiny uživatelů.
- Vysoce zabezpečené úložiště aplikačních a systémových přihlašovacích údajů.
- Realizace autentizace aplikací a skriptů na základě parametrů (např. cesta, uživatelské jméno, IP adresa); komunikace musí probíhat zabezpečeným kanálem (např. SSL).
- Autentizace do systému s 2faktorovou autentizací, SSO, AD.
- Samotné řešení nesmí poskytovat informace výrobci ani nikomu jinému bez souhlasu Zadavatele.

Systém PAM musí dále zajišťovat následující funkční požadavky:
- Správa sdílených hesel k účtům
- Správa privilegovaných relací
- Správa oprávnění silných uživatelů
- Správa hesel pro přístup z aplikace do jiné aplikace

Detailní technické požadavky na systém jsou popsány ve formuláři plnění technických požadavků.

2.1 Vypracování detailního návrhu řešení PAM

Součástí detailního návrhu řešení bude zejména:

- Detailní analýza současného stavu rolí/oprávnění privilegovaných účtů ve spravovaných systémech. Dodavatel v rámci analýzy vytvoří seznam rolí/oprávnění těchto privilegovaných účtů, navrhne model správy a monitoringu přístupu k těmto účtům, a tento model projedná s příslušnými správci systémů. Tato analýza taktéž popíše aktuální způsob přidělování přístupů uživatelů k privilegovaným účtům a navrhne nový model odpovídající standardním bezpečnostním požadavkům.
- Analýza stávajících interních předpisů Zadavatele dotčených projektem PAM a návrhy jejich optimalizace potřebné pro implementaci systému PAM.
- 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 PAM včetně datového a funkčního modelu a včetně jeho přizpůsobení potřebám Zadavatele.
- Detailní popis rozsahu úkonů údržby a rozsahu parametrů a vlastností PAM nastavitelných tak, aby proškolení pracovníci Zadavatele mohli provádět správu PAM a měnit jeho parametry a nastavení.
- Detailní popis implementace PAM, zejména:
  1.15 popis integrací PAM s požadovanými informačními systémy (dle přílohy č. 3 ZD) provozovanými nebo využívanými Zadavatelem, které budou umožňovat napojení na zdroj identit, napojení na cílové systémy obsahující spravované privilegované účty, napojení na SIEM / log management systém, napojení na e-mailový systém pro zasílání notifikací, atd.,
  1.16 popis řešení SSO,
  1.17 detailní popis implementace včetně časového harmonogramu,
  1.18 popis věcného a organizačního zabezpečení testovacího provozu,
  1.19 popis instalačních procedur pro instalaci PAM a nastavení parametrů pro práci v PAM,
  1.20 popis rozhraní pro integraci s jinými systémy (jeho datový a funkční model),
  1.21 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.

2.2 Dodávka řešení a zajištění licencí k užití SW a implementace PAM

Zadavatel předpokládá vybudování PAM na již existujících softwarových produktech, které jsou na trhu k dispozici, a jejich přizpůsobení dle potřeb Zadavatele. Jiné řešení, např. vlastní vývoj, není preferováno.

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

Součástí dodávky jsou:

1.22 licence na používání PAM pro zajištění provozu v testovacím a produkčním prostředí s možností HA režimu,

1.23 licence na používání PAM pro možnost definice pravidel pro automatické generování hesel k privilegovaným účtům a jejich automatická změny v systémech

1.24 licence na používání PAM pro možnost řízení přístupu k privilegovaným účtům na až 15 systémech včetně SSO, tedy bez možnosti/nutnosti znát heslo ke konkrétnímu privilegovanému účtu,

1.25 licence na možnost nahrávat uživatelské relace při práci pod privilegovanými účty na až 15 systémech.

Další potřebný SW:

- Součástí zakázky bude kromě licencí vlastního informačního systému PAM 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. To se týká operačního systému, databází, aplikačních serverů, či jiných komponent potřebných pro provoz řešení).
- Součástí nabídkové ceny je i cena licencí a dodání serverového operačního systému nutného pro provoz nabídnutého řešení, a to včetně jeho maintenance po dobu 48 měsíců 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 formou tzv. virtual appliance (předkonfigurovaný virtuální image od výrobce daného řešení) je přípustný provoz na platformě VMware.

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

Implementace PAM (včetně instalace všech potřebných softwarových a databázových součástí dodaného řešení) proběhne v souladu s akceptovaným Detailním návrhem řešení PAM na produkční a testovacího prostředí Zadavatele.

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 PAM s vybranými informačními systémy provozovanými nebo využívanými Zadavatelem

Předmětem plnění zakázky je mimo jiné zajištění plně funkční integrace PAM části s IDM částí.

Tato integrace spočívá zejména v možnosti správy životního cykly uživatelů systému PAM, tedy uživatelů přistupujících k privilegovaným účtům.

Případná implementace dalších rozhraní nad rámec přílohy č. 3 ZD (například nově pořizované systémy) bude řešena v rámci rozšířené podpory.

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

Požadavky na správu životního cyklu uživatelů systému PAM v rámci systému IDM:

- 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
- Zařazení a vyřazení uživatele do / ze skupiny
- Změna skupiny
- Změna rozsahu přidělených práv

2.3 Školení pracovníků Zadavatele pro administrátory a uživatele PAM, zpracování provozní dokumentace v českém jazyce

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

- Školení 5 administrátorů PAM a 5 uživatelů webového portálu PAM v celkovém rozsahu 32 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 klientských aplikací PAM (jsou-li třeba) na PC v učebně provede dodavatel.

Zadavatel požaduje, aby dodavatel 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.

2.4 Poskytování služeb technické podpory provozu PAM

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

2.5 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:

1.26 vypracováni detailního návrhu řešení včetně upřesnění dílčích částí hrubého harmonogramu,
1.27 interní oponentura a vypořádání připomínek,
1.28 akceptace a převzetí detailního návrhu řešení.

b) Druhá etapa zahrnuje:

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

c) Třetí etapa zahrnuje:

1.33 zkušební provoz, v rámci kterého bude prověřena funkčnost díla v rutinním prostředí Zadavatele,

1.34 akceptaci a převzetí díla do rutinního provozu.

d) Čtvrtá etapa představuje:

1.35 rutinní provoz a podporu systému.

2.6 Formulář plnění technických požadavků

V níže uvedené tabulce jsou uvedeny veškeré povinné minimální parametry kladené na celý systém PAM. 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
1	Systém umožňuje centralizovanou správu, ideálně pomocí webové konzole.	ANO	CA PAM poskytuje centrální správcovskou konzoli založenou na webové konzoli.	Bude hodnoceno
2	Nabízené řešení musí obsahovat bezpečné úložiště hesel k privilegovaným účtům bez možnosti neoprávněného přístupu, čtení a zápisu s certifikací FIPS 140-2.	ANO	Výchozím modulem šifrování v nabízeném produktu CA PAM je Cloakware Security Kernel, který je ověřen certifikátem FIPS 140-2 CMVP 1443. Systém lze také konfigurovat tak, aby používal modul OpenSSL FIPS, který je ověřen certifikátem FIPS 140-2 CMVP 1747.	Bude hodnoceno
3	Systém umožňuje auditovatelné vyzvedávání hesel k privilegovaným účtům ze strany autentizovaných uživatelů, a to na předem definovanou dobu. Po jejím uplynutí systém automaticky změní pro daný privilegovaný účet heslo.	ANO	Řešení CA PAM umožňuje definici politik pro vyzvedávání hesel k privilegovaným účtům ze strany oprávněných uživatelů. Dobu, po které bude vyzvednuté heslo validní, lze v systému nastavit.	Bude hodnoceno
4	Systém umožňuje automatické přihlášení uživatele k privilegovanému účtu na pozadí, a to tak, že uživatel nezná heslo a ani se ho při přihlašování nedozví.	ANO	Řešení CA PAM poskytuje funkci SSO (single sign-on) umožňující automatické přihlášení oprávněného uživatele k privilegovanému účtu, tedy tak, že uživatel heslo vůbec nezná a ani se ho při přihlašování nedozví.	Bude hodnoceno

ID	Popis požadavku	Vyjádření [ANO/NE]	Popis jak bude požadavek splněn/řešen	Poznámka k hodnocení
5	Systém musí umožnit vynucené ukončení relace z důvodu delší nečinnosti uživatele, používání nepovolených příkazů, nebo zásahem oprávněného pracovníka.	ANO	V systému lze definovat dobu nečinnosti, po které se otevřené relace automaticky uzavřou. Současně lze relace sledovat s ohledem na používané příkazy, a v případě porušení bezpečnostních pravidel automaticky či manuálně vynutit ukončení dané relace.	Bude hodnoceno
6	Systém musí umožnit definovat komplexitu hesel pro různé privilegované účty včetně jejich následného generování a změny přímo v systémech.	ANO	CA PAM poskytuje nástroj pro definici různých politik pro složitost hesel, a tyto politiky následně aplikovat na automatické generování a změnu hesel k privilegovaným účtům.	Bude hodnoceno
7	Systém umožňuje nahrávání všech nebo jen vybraných uživatelských relací bez nutnosti instalace agenta na koncový systém.	ANO	CA PAM obsahuje modul pro videonahrávání grafických i CLI (textových) relací na bázi „proxy“ a tedy bez instalace agentů na koncové systémy.	Bude hodnoceno
8	Veškerá konfigurace a parametrizace systému probíhá přes grafické či textové prostředí, a to vždy bez zásahu do kódu.	ANO	CA PAM se spravuje výhradně přes grafické webové rozhraní bez nutnosti zásahů do kódu.	Bude hodnoceno
9	Všechny události v systému jsou logovány a zasílány do centrálního log management systému.	ANO	CA PAM generuje logy ve formátu syslog, které lze automaticky zasílat do log management nebo SIEM systému pro další zpracování a archivaci.	Bude hodnoceno
10	Systém umožňuje integraci se systémy dvoufaktorové autentizace	ANO	CA PAM podporuje integraci s autentizačními systémy třetích stran pro dvou a vícefaktorovou autentizaci, a to na bázi několika protokolů, např. RADIUS.	Bude hodnoceno

ID	Popis požadavku	Vyjádření [ANO/NE]	Popis jak bude požadavek splněn/řešen	Poznámka k hodnocení
11	Při definovaném počtu nesprávných přihlášení bude uživatel zablokován. Jeho odblokování může provést pouze oprávněný pracovník.	ANO	CA PAM umožňuje nastavit ´maximální počet nesprávných přihlášení a dobu, během které musí tato nesprávná přihlášení nastat. Po vyčerpání tohoto počtu se účet zablokuje a je třeba ho oprávněným pracovníkem odblokovat.	Bude hodnoceno
12	Systém musí být rozšiřitelný i na privilegované účty na platformách VMware, AWS a Office365, a to včetně vytváření dočasných účtů s definovanou sadou oprávnění.	ANO	CA PAM lze rozšířit o nativní správu přístupu k privilegovaným účtům a správu jejich hesel na platformách VMware, Amazon Web Services, Office 365.	Bude hodnoceno
13	Systém musí být rozšiřitelný o granulární řízení přístupových oprávnění k privilegovaným účtům dle identity přistupujícího uživatele přímo na úrovni kritických serverů (např. serverů podléhajících požadavkům ZoKB).	ANO	CA PAM lze rozšířit o modul CA PAM Server Control, který zajistí maximální ochranu kritických serverů proti zneužití privilegovaných účtů přímo na úrovni jejich kernelu, a to na platformách Windows, Unix a Linux.	Bude hodnoceno

3 Používané pojmy a zkratky

3.1 Pojmy

Autorizace je pojem z oblasti řízení bezpečnosti a znamená ověření oprávnění k nějakému úkonu nebo operaci. Tedy zjištění, zdali daný subjekt může danou činnost či operaci provést (má k tomu pravomoc či oprávnění). Obvykle navazuje na ověření identity, tedy autentizaci. Někdy lze využít stejné technické prostředky (například identifikační vstupová karta nese informaci o identitě i o oprávnění přístupu). Autorizace je proces získávání souhlasu s provedením nějaké operace, povolení přístupu někam, k někomu nebo něčemu (nejen ve smyslu přístupu do konkrétních prostor nebo k nějaké osobě, ale také přístup k informacím, funkcím, programovým objektům a podobně).

Autorizovaný uživatel – Uživatel, který má určité právo nebo povolení pracovat v IS a s aplikacemi podle stanovených zásad přístupu.

Autentizace je pojem z oblasti řízení bezpečnosti a znamená ověření identity nějakého subjektu (osoby, systému). Tedy zjištění zdali je daný subjekt ten, za který se vydává. Autentizace je proces ověření proklamované identity subjektu.

Aplikační role – Je elementární role/oprávnění k jednotlivým aplikacím. Tuto roli přiděluje oprávněná osoba (nadřízený pracovník, vedoucí oddělení informatiky, správce IdM,...) a přidělení by mělo podléhat schválení odpovědnou osobou (manažer systému, vedoucí kanceláře primátora, apod.).

Business role – Je to sada oprávnění, které uživatel získá na základě daných pravidel, která při přidělení nevyžaduje žádné další dodatečné schválení (sada oprávnění se považuje za předem schválenou). Role je přidělována automaticky na základě atributů uživatele (typ uživatele, zařazení do organizační jednotky, pracovní pozice, apod.).

Funkční místo – Funkční místo je virtuální seskupení pracovních pozic (alias systematizovaných míst) se stejným názvem (např. kurátor - mládež), které mají obdobný (často totožný) rozsah vykonávaných činností. Pracovní pozice jsou takto vytvářeny s cílem definovat, na základě stanovených kompetencí, požadavky na Business role.

Federalizovaná identita – Propojená sada identit do jedné identity.

Federace identity – sada politik, standardů a nastavení umožňující univerzálnost a přenositelnost identity napříč bezpečnostními doménami.

Organizační struktura – Organizační struktura je formalizovaná struktura organizačních jednotek, kde jsou jednoznačně definovány vztahy nadřízenosti a podřízenosti. Organizační struktura je deklarována pomocí organizačního řádu a vizualizována prostřednictvím organizačního schématu.

Identita – Unikátní jméno, užité pro identifikaci uživatele, osoby nebo role. Identita je užívaná pro přidělení práv tomuto uživateli, osobě nebo roli.

Identitní prostor – pojem, který označuje zabezpečenou adresářovou službu obsahující údaje pro autentizaci a autorizaci uživatelů. Jedná se o pojem používaný v souvislosti se zaváděním a provozem základních registrů, je vymezený v souladu se zákonem Zákon o základních registrech - č. 111/2009 Sb. a má proto omezenou platnost pouze v České republice.

Uživatelská identita – Termín vyžívaný při implementaci systému správy identit. Může se rozdělovat na identity interní (kmenový zaměstnanci) a externí (dodavatelé).

Trezor identit – centrální místo, kde jsou uloženy informace o identitách.

Single Sign-On – jediné přihlášení. Jediné uživatelské jméno, jediné heslo a jediné přihlášení pro přístup k aplikacím.

Self Management – samoobslužná samospráva. Jednoduchá intuitivní samospráva prostřednictvím webového prohlížeče, kterou zvládne běžný uživatel i bez nutnosti podpory IT, případně HelpDesku – např. reset hesla.

Systémový účet – speciální účty v systému.

Entita – Základní stavební jednotkou IM jsou entity. Jako entita může být definována osoba, lokalita, organizační jednotka, účet a případně další prvky, pro které jsou stanoveny vztahy prostřednictvím politik.

Uživatel – Součást systému, která v rozsahu přidělených pravomocí využívá informace (služby, funkce) systému, zajišťuje vstupní informace potřebné pro identifikaci objektu nebo prostředku.

Role – Představuje skupinu uživatelů se shodně nastaveným oprávněním na spravovaných systémech. Určená množina funkčně příbuzných činností a potřebných autorizací pro provádění těchto činností, jež může být přidělena uživatelům.

Single Sign-Off – Analogie se Single Sign-On kdy je uživatel automaticky ze všech systémů odhlášen.

Workflow je jedním ze základních prostředků IM. Slouží pro modelování procesů vedoucích k vytvoření požadovaného účtu či nastavení atributu při zachování všech formálních požadavků na takovýto proces v organizaci.

Middleware – software, který slouží jako konverzní nebo překladatelská vrstva. Slouží také jako integrátor.

3.2 Zkratky

ESB – Enterprise Service Bus – kategorie v oblasti technologie middleware. Jedná se o implementaci SOA (service oriented architecture), která představuje konkrétní produkt konkrétního dodavatele. Jedná se tedy o middlewarovou technologii obsahující předávání zpráv a webové, či jiné, služby.

ID – Identifikátor uživatele

IS – Informační systém

IT – Informační technologie

ICT – Informační a komunikační technologie

JIP – Jednotný identitní prostor

AD – Active Directory

MS AD – Microsoft Active Directory

HW – Hardware

SW – Software, programové vybavení

DPP – Dohoda o provedení práce

DPČ – Dohoda o pracovní činnosti

IdM – Identity management

LDAP – Centrální adresář prezentující údaje o uživateli, jeho uživatelském jménu, heslu a oprávněních, atd.

MHMP – Magistrát Hlavního Města Prahy

VPN – Virtual private network

CLI – Příkazový řádek (Command line interface)

SSO - Single Sign-On je vlastnost k přístupu k souvisejícím, ale nezávislým softwarovým systémům. S touto vlastností se uživatel přihlásí jednou a získá přístup ke všem dalším systémům bez dalšího přihlašování.

SŘBD – Systém řízení báze dat