Příloha č. 2 - Technická specifikace předmětu plnění “Dodávka softwaru IDM včetně implementace na OU - dodatek č. 1”

Předmět zakázky

Předmětem zakázky je rozšíření funkcionality systému IDM na OU včetně implementační analýzy, implementace, počáteční konfigurace a odladění.

Předpokládaný postup řešení

Jedná se o rozšíření funkcionality systému AC Identita, který byl na OU implementován. Rozšíření funkcionality bude zahrnovat tyto oblasti:

- Nový modul pro integraci knihovního systému
- Nový modul pro integraci kolejního systému
- Nový modul pro integraci e-learningového systému
- Vícefaktorové přihlašování do IDM a změna autentizace pro systém IDM
- Rozšíření workflow pro správu kont
- Napojení a integrace s externím systémem pro ukládání logů
- Rozšíření IDM pro hybridní Exchange

U každé oblasti dodavatel ve spolupráci s OU provede implementační analýzu (kromě položek, kde již byla provedena – viz dále), která stanoví podrobnosti a rozsah implementace. Následně dodavatel provede implementaci, konfiguraci a odladění pro každou s výše uvedených oblastí v souladu s touto Přílohou.

Předpokládaný postup a rozsah implementace je možno po dohodě mezi zadavatelem a dodavatelem případně upravit, pokud v rámci implementační analýzy bude nalezen vhodnější postup nebo z analýzy vyplyne potřeba úpravy rozsahu funkcionalit.

1. Nový modul pro integraci knihovního systému

Nový modul zajistí integraci systému Aleph s IDM na OU dle již provedené analýzy. Systém Aleph je knihovnický IS používaný Univerzitní knihovnou OU. Z pohledu IDM bude Aleph výstupním systémem. Komunikace bude probíhat přes webové služby Alephu, data budou ve formátu XML. Vstupní data budou poskytovat již zavedené vstupní konektory v IDM, které je však nutno rozšířit o nové atributy. V současnosti jsou data do systému Aleph přenášená synchronizačním SW (vyvinut na OU). Ten bude po napojení na IDM odstaven.

Cíle:

- Zavedení automatizovaného řízení životního cyklu všech potřebných typů identit v systému Aleph včetně všech potřebný údajů / atributů.
- Zavedení automatizovaného řízení autorizace (typ uživatele) v systému Aleph.
- Zavedení rychlejší propagace změn (v řádu jednotek minut) do systému Aleph.

Výsledný stav:

- IDM bude automatizovaně řídit životní cyklus identit v Alephu pro typy identit: zaměstnanec, student, absolvent a externista.
- IDM bude přebírat veškeré potřebné údaje pro Aleph ze vstupních systémů (STAG, Magion, Absolventi, Identifikační karty).
- IDM bude nastavovat a aktualizovat všechny potřebné údaje o identitě v systému Aleph.
- IDM bude řídit autorizaci v systému Aleph.
- IDM umožní aktualizaci dat v Alephu v řádu jednotek minut pro jeden objekt. Aktualizace dat v Alephu je závislá na ostatních synchronizacích a je nutno počítat s prodlevou aktualizace z důvodu souběžně běžících synchronizací, aby byla zajištěna konzistence dat.
- IDM umožní spuštění aktualizace dat v Alephu v režimech: kompletní, změnová a rekonciliační a to včetně možnosti spuštění v režimu simulace.
- IDM umožní spuštění aktualizace dat v Alephu pro jednu identitu včetně načtení dat ze vstupních systémů. Spuštění bude možné jak administrátorem v rozhraní IDM, tak přes API.

2. Nový modul pro integraci kolejního systému

Systém ISKaM je IS pro správu kolejí a menz, právě implementovaný na OU. Z pohledu IDM bude ISKaM výstupním systémem. Komunikace bude probíhat přes webové služby ISKaMu. Vstupní data budou poskytovat již zavedené vstupní konektory v IDM. Z analýzy vyplyne případná nutnost rozšíření vstupních konektorů.

Cíle:

- Zavedení automatizovaného řízení životního cyklu všech potřebných typů identit v systému ISKaM včetně všech potřebný údajů / atributů.
- Zavedení automatizovaného řízení autorizace v systému ISKaM.

Výsledný stav:

- IDM bude automatizovaně řídit životní cyklus identit v systému ISKaM pro všechny potřebné typy identit.
- IDM bude přebírat veškeré potřebné údaje pro identity v ISKaMu ze vstupních systémů (STAG, Magion, Identifikační karty).
- IDM bude nastavovat a aktualizovat všechny potřebné údaje o identitě v systému ISKaM.
- IDM bude řídit autorizaci v systému ISKaM.
- IDM umožní aktualizaci dat v ISKaM v řádu jednotek minut pro jeden objekt. Aktualizace dat v ISKaMu je závislá na ostatních synchronizacích a je nutno počítat s prodlevou aktualizace z důvodu souběžně běžících synchronizací, aby byla zajištěna konzistence dat.
- IDM umožní spuštění aktualizace dat v systému ISKaM v režimech: kompletní, změnová a rekonciliační a to včetně možnosti spuštění v režimu simulace.
- IDM umožní spuštění aktualizace dat v systému ISKaM pro jednu identitu včetně načtení dat ze vstupních systémů. Spuštění bude možné jak administrátorem v rozhraní IDM, tak přes API. Kolejní systém neobsahuje služby (API) pro integraci na tento systém. Zadavatel spolu s dodavatelem Kolejního systému musí zajistit dostupnost takové služby, aby se IDM mohlo integrovat na tento systém. Pro dodržení požadovaného harmonogram dodání, je nutné mít tyto služby k dispozici nejpozději 2 a půl měsíce před dokončením projektu. Dodavatel předá požadavky na službu REST/SOAP, aby plnila požadavky zadavatele.

3. Nový modul pro integraci e-learningového systému Moodle

Nový modul zajistí integraci systému Moodle s IDM. Systém Moodle je e-learningový systém používaný na OU. Z pohledu IDM bude Moodle výstupním systémem. Komunikace bude probíhat přes API Moodle. Vstupní data budou poskytovat již zavedené vstupní konektory v IDM. Z analýzy vyplyne případná nutnost rozšíření vstupních konektorů.

Integrace bude pouze částečná:

- IDM bude spravovat jen vybrané uživatele a bude s nimi provádět jen vybrané operace (založení).
- IDM bude spravovat členství jen vy vybraných kurzech.
- Založení uživatelů bude probíhat až v momentě, kdy mají být přiděleni do kurzu (tedy ne při vzniku uživatele v IDM). Uživatel bude založen jen v případě, pokud v Moodle už neexistuje.

Hlavním důvodem částečné integrace je, aby správa přes IDM nekolidovala se správou studentských kont a kurzů, kterou provádí napojení ze systému STAG.

Cíle:

- Automatizace přidělení/odebrání vybraných kurzů uživatelům.
- Automatizace zakládaní uživatelů potřebných pro vybrané kurzy.

Výsledný stav:

- IDM bude automatizovaně zakládat v systému Moodle vybrané uživatele, a to až v momentě, kdy jsou v Moodle potřeba a pouze v případě, že v Moodle ještě neexistují.
- IDM bude řídit členství ve vybraných kurzech v Moodle.
- IDM bude přebírat veškeré potřebné údaje pro identity v Moodle ze vstupních systémů.
- IDM bude nastavovat a aktualizovat všechny potřebné údaje o identitě v systému Moodle.
- IDM bude evidovat vybrané kurzy jako roli.
- IDM umožní aktualizaci dat v Moodle v řádu jednotek minut pro jeden objekt. Aktualizace dat v Moodle je závislá na ostatních synchronizacích a je nutno počítat s prodlevou aktualizace z důvodu souběžně běžících synchronizací, aby byla zajištěna konzistence dat.
- IDM umožní spuštění aktualizace dat v Moodle v režimech: kompletní, změnová, a to včetně možnosti spuštění v režimu simulace.
- IDM umožní spuštění aktualizace dat v Moodle pro jednu identitu včetně načtení dat ze vstupních systémů. Spuštění bude možné jak administrátorem v rozhraní IDM, tak přes API.

4. Vícefaktorové přihlašování do IDM a změna autentizace pro systém IDM

Systém IDM používá na OU rozdílnou autentizaci pro administrátory a pro běžné uživatele. Autentizace pro administrátory bude rozšířena o vícefaktorové ověřování (MFA). Autentizace pro uživatele bude změněna tak, aby využívala interní federaci identit OU (Shibboleth).

Cíle:

- Zvýšení bezpečnosti přihlašování administrátorů zavedením MFA.
- Změna způsobu autentizace ostatních uživatelů na standardní způsob v rámci OU
- Snížení nároku na licence MS v prostředí OU.

Výsledný stav:

- IDM bude administrátory autentizovat prostřednictvím MFA.
- MFA pro administrátory bude plně kompatibilní s již používanými prostředky na OU (MS Authenticator).
- IDM bude ověřovat ostatní uživatele prostřednictvím identit využívaných v interní federaci identit OU.
- IDM pro uživatele bude zaveden jako service provider do interní federace identit OU.

5. Rozšíření workflow pro správu kont

V systém IDM na OU byly implementovány workflow pro založení a zrušení neosobního konta. Tyto workflow budou rozšířeny o nové funkcionality. Dále budou implementovány nové workflow pro správu kont. Změny budou provedeny dle již provedené analýzy.

Cíle:

- Zautomatizovat správu neosobních kont.
- Zautomatizovat správu kont pro externí uživatele.
- Zautomatizovat správu licenčních skupiny pro prostředí Microsoft 365.

Výsledný stav:

- Workflow pro založení neosobního konta bude rozšířeno o nové funkcionality.
- Workflow pro zrušení neosobního konta bude rozšířeno o nové funkcionality.
- Bude implementováno workflow pro změnu zodpovědné osoby u neosobního konta.
- Bude implementováno workflow pro změnu delegátů u neosobního konta.
- Bude implementováno workflow pro založení externího uživatele.
- Bude implementováno workflow pro zrušení externího uživatele.
- Bude implementováno workflow pro změnu externího uživatele.
- Bude implementováno workflow pro změnu licenční skupiny.
- Bude implementováno workflow pro všechny výše zmíněné požadavky, což je 8 výsledných workflow, které jsou již popsány i v analýze.

6. Napojení a integrace s externím systémem pro ukládání logů

Napojení zajistí, aby logy a auditní záznamy ze systému IDM byly ukládány nejenom interně, ale i do systému, který OU používá k centrálnímu ukládání logů (Logmanager).

Cíle:

- Zajistit ukládaní logů a auditních záznamů IDM v centrálním úložišti logů OU.

Výsledný stav:

- IDM bude integrován s centrálním úložištěm logů OU.
- Logy z IDM budou do centrálního úložiště předávány v kompatibilním formátu (CEF).
- Do centrálního úložiště budou ukládány logy:
    - Samotný provoz systému IDM, chyby systému.
    - Logy proběhlých synchronizací.
    - Změny nastavení a oprávnění v IDM.
    - Změny provedené na objektech, které jsou ve správě IDM.

7. Rozšíření IDM pro hybridní Exchange

V současnosti IDM spravuje primárně onpremise prostředí Exchange na OU, v online prostředí pouze částečně. Rozšíření zajistí plnou správu objektů v Exchange jak v prostředí onpremise, tak online.

Cíle:

- Umožnit plnohodnotnou správu uživatelů a neosobních kont v hybridním prostředí Exchange.

Výsledný stav:

- Všechny spravované objekty v Exchange bude IDM umět založit, aktualizovat a rušit jak v onpremise prostředí, tak v online prostředí.
- V IDM umožní nastavit, ve kterém prostředí má daný objekt Exchange vzniknout. Nastavení bude možné buď pomocí pravidel, nebo ručně (v admin rozhraní nebo ve workflow).
- IDM umožní nastavit zodpovědnou osobu a delegáty pro neosobní schránky. Nastavení bude možné provést bez rozdílu, jestli neosobní schránka či zodpovědné osoby a delegáti jsou v prostředí onpremise či online.
- IDM umožní nastavit všechna používána práva pro objekty Exchange: neosobních schránky. Nastavení bude možné provést bez rozdílu, jestli objekt či člen jsou v prostředí onpremise či online.
- IDM zajistí jedinečnost adres objektů v prostředí AD/Exchange na OU.

Požadavky na řešení

Seznam požadavků na řešení IDM pro OU. Tabulky obsahují položky:

- Oblast – popis požadavku.
- Doplňující vysvětlení – podrobnější popis požadavku

1. Nový modul pro integraci knihovního systému

ID	Oblast	Doplňující vysvětlení
1.1	Konektor pro systém Aleph	IDM musí integrovat systém Aleph konektorem jako výstupní systém. Komunikace musí probíhat přes webové služby Alephu, data budou ve formátu XML. Konektor podporovat tyto operace: vytvoření účtu (identity), zablokování účtu, povolení účtu, zrušení účtu, aktualizace údajů u účtu.
1.2	Typy uživatelů pro Aleph	Konektor pro Aleph musí pracovat s uživateli typu zaměstnanec, student, absolvent a externista.
1.3	Atributy předávané do Alephu	Konektor pro Aleph musí předávat a aktualizovat všechny potřebné údaje / atributy o identitě do systému Aleph. Přesný rozsah je stanoven v provedené analýze.
1.4	Řízení autorizace v Alephu	Konektor pro Aleph musí řídit autorizaci v systému Aleph (typ uživatele) formou nastavení typu uživatele.
1.5	Rozšíření vstupních konektorů	V současnosti implementované vstupní konektory pro STAG a Magion musí být rozšířeny o atributy potřebné pro Aleph.

1.6	Rychlost aktualizace dat	Konektor pro Aleph musí podporovat aktualizaci dat u jednoho uživatele (včetně načtení ze vstupních systému) tak, aby netrvala déle než jednu minutu, a to bez ohledu na případné další probíhající synchronizace dalších uživatelů spuštěné prostřednictvím API. Pro splnění požadavku musí být zajištěno, že současně nesmí běžet vstupní synchronizace a odezva výstupního systému na dotaz musí být v jednotek sekund.
1.7	Typy synchronizace	Konektor pro Aleph musí umožnit spustit synchronizaci kompletní, změnovou a rekonciliační (neboli report záznamů v cílovém systému, které nesouhlasí se stavem v IDM). Konektor musí umožňovat spuštění synchronizací v režimu simulace.
1.8	Aktualizace dat přes API	API rozhraní musí umožnit spuštění synchronizace do Alephu pro jednu identitu, a to včetně načtení dat ze vstupních systémů.
1.9	Zabezpečená komunikace	Komunikace se systémem Aleph musí probíhat zabezpečeně. Služba Aleph pro komunikaci musí být vystavena zabezpečeně.
1.10	Přechod ze současné synchronizace	Součástí zakázky musí být provedení přechodu ze současné synchronizace dat na synchronizaci dat ze systému IDM do systému Aleph.

2. Nový modul pro integraci kolejního systému

Kolejní systém neobsahuje služby (API) pro integraci na tento systém. Zadavatel spolu s dodavatelem Kolejního systému musí zajistit dostupnost takové služby, aby se IDM mohlo integrovat na tento systém. V případě, že nebude dostupné API rozhraní Kolejního systému, je možné, aby se Kolejní systém napojil na API IDM. Nicméně takováto integrace nebude splňovat požadavky na funkcionalitu v bodech 2.1 až 2.9

ID	Oblast	Doplňující vysvětlení
2.1	Konektor pro systém ISKaM	IDM musí integrovat systém ISKaM konektorem jako výstupní systém. Komunikace musí probíhat přes webové služby systému ISKaM. Konektor musí podporovat tyto operace: vytvoření účtu (identity), zablokování účtu, povolení účtu, zrušení účtu, aktualizace údajů u účtu.
2.2	Typy uživatelů pro ISKaM	Konektor pro systém ISKaM musí pracovat se všemi potřebnými typy uživatelů. Přesný rozsah bude stanoven v analýze.
2.3	Atributy předávané do systému ISKaM	Konektor pro systém ISKaM musí předávat a aktualizovat všechny potřebné údaje / atributy o identitě do systému ISKaM. Přesný rozsah bude stanoven v analýze.
2.4	Řízení autorizace v systému ISKaM	Konektor pro ISKaM musí řídit autorizaci v systému ISKaM. Přesný rozsah bude stanoven v analýze.
2.5	Rozšíření vstupních konektorů	V současnosti implementované vstupní konektory pro STAG a Magion musí být rozšířeny o atributy potřebné pro identity v ISKaMu, pokud taková potřeba vyplyne z analýzy.

2.6	Rychlost aktualizace dat	Konektor pro ISKaM musí podporovat aktualizaci dat u jednoho uživatele (včetně načtení ze vstupních systému) tak, aby netrvala déle než jednu minutu, a to bez ohledu na případné další probíhající synchronizace dalších uživatelů spuštěné prostřednictvím API. Pro splnění požadavku musí být zajištěno, že současně nesmí běžet vstupní synchronizace a odezva výstupního systému na dotaz musí být v jednotek sekund.
2.7	Typy synchronizace	Konektor pro ISKaM musí umožnit spustit synchronizaci kompletní, změnovou a rekonciliační (neboli report záznamů v cílovém systému, které nesouhlasí se stavem v IDM). Konektor musí umožňovat spuštění synchronizací v režimu simulace.
2.8	Aktualizace dat přes API	API rozhraní musí umožnit spuštění synchronizace do systému ISKaM pro jednu identitu, a to včetně načtení dat ze vstupních systémů.
2.9	Zabezpečená komunikace	Komunikace se systémem ISKaM musí probíhat zabezpečeně. Služba ISKaM pro komunikaci musí být vystavena zabezpečeně.

3. Nový modul pro integraci e-learningového systému Moodle

Pro splnění požadavků 3.1 až 3.10 musí existovat služba, která tyto operace umožní.

ID	Oblast	Doplňující vysvětlení
3.1	Konektor pro systém Moodle	IDM musí integrovat systém Moodle konektorem jako výstupní systém. Komunikace musí probíhat přes API Moodle. Konektor podporovat tyto operace: vytvoření účtu (identity), přiřazení uživatele na kurz, odebrání uživatele z kurzu.
3.2	Typy uživatelů pro Moodle	Konektor pro Moodle musí umožňovat zakládat uživatele typu zaměstnanec a externista. Správa
3.3	Založení uživatele	Konektor pro Moodle musí založit uživatele až v momentě, kdy je potřeba daného uživatele přiřadit k některému se spravovaných kurzů. Toto založení musí být provedeno pouze v případě, pokud uživatel ještě v Moodle neexistuje.
3.4	Atributy předávané do Moodle	Konektor pro Moodle musí předávat všechny potřebné údaje / atributy o identitě do systému Moodle. Přesný rozsah bude stanoven v provedené analýze.
3.5	Správa členství v kurzech.	Konektor pro Moodle musí řídit přiřazení kurzů v Moodle pouze pro vybrané kurzy. Konektor pro Moodle nesmí měnit členství u ostatních kurzů v Moodle.
3.6	Evidence kurzů v IDM a jejich přiřazení	Vybrané kurzy z Moodle musí být v IDM evidovány jako role. Přiřazení role (kurzu) v IDM musí být možné jak automaticky (na základě pravidel), tak ručně (přiřazením v admin rozhraní nebo pomocí workflow)
3.7	Rychlost aktualizace dat	Konektor pro Moodle musí podporovat aktualizaci dat u jednoho uživatele (včetně načtení ze vstupních systému) tak, aby netrvala déle než jednu minutu, a to bez ohledu na případné další probíhající synchronizace dalších uživatelů spuštěné prostřednictvím API.

		Pro splnění požadavku musí být zajištěno, že současně nesmí běžet vstupní synchronizace a odezva výstupního systému na dotaz musí být v jednotek sekund.
3.8	Typy synchronizace	Konektor pro Moodle musí umožnit spustit synchronizaci kompletní a změnovou. Konektor musí umožňovat spuštění synchronizací v režimu simulace.
3.9	Aktualizace dat přes API	API rozhraní musí umožnit spuštění synchronizace do Moodle pro jednu identitu, a to včetně načtení dat ze vstupních systémů.
3.10	Zabezpečená komunikace	Komunikace se systémem Moodle musí probíhat zabezpečeně. Služba Moodle pro komunikaci musí být vystavena zabezpečeně

4. Vícefaktorové přihlašování do IDM a změna autentizace pro systém IDM

ID	Oblast	Doplňující vysvětlení
4.1	Autentizace administrátorů přes MFA	IDM musí autentizovat vybrané uživatele s vyššími právy (administrátory) pomocí vícefaktorové autentizace (MFA).
4.2	Kompatibilita s aktuálním prostředím	MFA pro administrátory musí být kompatibilní s prostředím, které je nyní na OU využíváno (MS Authenticator).
4.3	Autentizace uživatelů přes Shibboleth	IDM musí autentizovat ostatní uživatele prostřednictvím identit využívaných v interní federaci identit OU.
4.4	Napojení do interní federace	IDM pro uživatele musí být zaveden jako service provider do interní federace identit na OU.

5. Rozšíření workflow pro správu kont

ID	Oblast	Doplňující vysvětlení
5.1	Rozšíření workflow pro založení neosobního konta	V IDM musí být rozšířeno workflow pro založení neosobního konta o nové funkcionality dle provedené analýzy.
5.2	Rozšíření workflow pro zrušení neosobního konta	V IDM musí být rozšířeno workflow pro zrušení neosobního konta o nové funkcionality dle provedené analýzy.
5.3	Implementace workflow pro změnu zodpovědné osoby u neosobního konta	V IDM musí být implementováno workflow pro změnu zodpovědné osoby u neosobního konta dle provedené analýzy.
5.4	Implementace workflow pro změnu delegátů u neosobního konta	V IDM musí být implementováno workflow pro změnu delegátů u neosobního konta dle provedené analýzy.
5.5	Implementace workflow pro založení externího uživatele	V IDM musí být implementováno workflow pro založení externího uživatele dle provedené analýzy.
5.6	Implementace workflow pro zrušení externího uživatele	V IDM musí být implementováno workflow pro zrušení externího uživatele dle provedené analýzy.
5.7	Implementace workflow pro změnu externího uživatele	V IDM musí být implementováno workflow pro změnu externího uživatele dle provedené analýzy.

5.8	Implementace workflow pro změnu licenční skupiny	V IDM musí být implementováno workflow pro změnu licenční skupiny dle provedené analýzy.

6. Napojení a integrace s externím systémem pro ukládání logů

ID	Oblast	Doplňující vysvětlení
6.1	Napojení na centrální úložiště logů na OU	IDM musí ukládat logy do centrálního úložiště logů na OU.
6.2	Kompatibilita s centrálním úložištěm logů na OU	Logy z IDM musí být centrálnímu úložišti předávány v kompatibilním formátu (například formát CEF).
6.3	Komunikace s centrálním úložištěm logů	Předávání logů musí probíhat přes protokol TCP a musí být šifrované pomocí TLS v aktuální verzi.
6.4	Volitelná úroveň logování	IDM musí umožnit volbu úrovně logů, které budou zasílány do centrálního úložiště logů.
6.5	Logy o provozu IDM	IDM musí do centrálního úložiště logů OU předávat logy o chodu systému IDM včetně chyb.
6.6	Logy o synchronizacích IDM	IDM musí do centrálního úložiště logů OU předávat logy o synchronizacích provedených systémem IDM.
6.7	Logy o nastavení IDM	IDM musí do centrálního úložiště logů OU předávat logy o změnách v nastavení IDM a změnách v oprávnění v rámci IDM.
6.8	Logy o změnách na objektech v IDM	IDM musí do centrálního úložiště logů OU předávat logy o provedených změnách na objektech, které jsou ve správě IDM.

7. Rozšíření IDM pro hybridní Exchange

ID	Oblast	Doplňující vysvětlení
7.1	Správa objektů v hybridní prostředí Exchange	IDM musí umožnit spravovat všechny spravované objekty v Exchange bez ohledu na to, jestli jsou v onpremise nebo online prostředí. IDM musí umožnit vytvoření a zrušení těchto objektů a nastavení všech potřebných atributů
7.2	Vznik objektů v hybridní prostředí Exchange	IDM musí umožnit nastavení, kde objekty vzniknou (onpremise či online). Musí to být možné buď pomocí pravidel, nebo ručně (v admin rozhraní).
7.3	Neosobní schránky v hybridní prostředí Exchange	IDM musí umožnit nastavení zodpovědné osoby a delegátů u neosobních schránek, včetně práv pro tyto osoby, bez rozdílu, jestli neosobní schránka či zodpovědné osoby a delegáti jsou v prostředí onpremise či online.
7.4	Jedinečnost adresy	IDM musí při založení či změně adresy jakéhokoliv objektu v Exchange kontrolovat jedinečnost adresy. Kontrola musí být provedena proti všem požadovaným objektům v AD.

8. Společné požadavky

ID	Oblast	Doplňující vysvětlení
8.1	Auditní stopa pro veškeré operace	Veškeré operace s dopadem na spravovaná data je nutné evidovat jako auditní záznamy. Tyto záznamy musí obsahovat minimálně – přesný čas, přihlášeného uživatele, referenci na dotčený objekt, operaci a detaily operace (např. změněné atributy).
8.2	Auditní záznamy pro administrátorské a uživatelské rozhraní	V rámci administrátorského a případně i uživatelského rozhraní musí být možnost procházet auditní záznamy. V případě dostupnosti záznamu běžným uživatelům, bude moci uživatel zobrazit jen záznamy týkající se jeho osoby nebo jeho podřízeného.
8.3	Auditní záznamy musí být možné odkládat i mimo systém IDM	Auditní záznamy musí být možné odkládat i mimo systém IDM.
8.4	Dodatečné licence třetích stran	IDM nebude vyžadovat dodatečné náklady na licence na straně OU nad rámec licencí, které jsou použity v prostředí OU.
8.5	Licenční model IDM	IDM nebude vyžadovat/obsahovat licence (dodávaného řešení) závislé na počtu spravovaných identit, počtu záznamů, velikosti databází nebo jiná podobná omezení.
8.6	Dokumentace IDM	V rámci implementace IDM řešení musí dodavatel dodat následující dokumentace: • technický popis IDM řešení – technický popis nasazení IDM • uživatelská dokumentace – dokumentace pro běžné uživatele obsahující popis uživatelského rozhraní • administrátorská dokumentace – dokumentace pro správce IDM popisující správu IDM včetně řešení nestandardních situací
8.7	Školení správců IDM	Dodavatel IDM musí poskytnout následující školení: školení správců IDM – školení pro pracovníky CIT