Technická specifikace k veřejné zakázce “Dodávka softwaru IDM včetně implementace na OU”

Předmět zakázky

Předmětem zakázky je dodání softwaru IDM včetně implementační analýzy, implementace, počáteční konfigurace, odladění a roční podpory.

Předpokládaný postup řešení

Komplexní zavedení IDM na OU nebude jen o IDM samotném – bude zahrnovat změny architektury v IT infrastruktuře, redesign a migraci adresářových služeb, úpravy architektury aplikací a změny procesů. Provedení změn v rámci jednoho komplexního projektu přináší rizika, a proto implementace bude rozčleněna do tří fází, které mohou být řešeny samostatně. Smyslem každé fáze bude doručit výsledky až do produkce a položit tak základ pro fázi následující.

Potřebné změny v IT infrastruktuře vyplynuly ze změn, které proběhnou na straně identit. V rámci implementace IDM bude dodavatel řešit přechod na nový model identit pro systémy, které budou jako cílové napojeny na IDM. Toto řešení bude zahrnovat analýzu i implementaci správy identit v daném systému. Změny v daném systému potřebné pro využití nového modelu identit budou záležitosti OU, případně dodavatele tohoto systému.

Předpokládaný postup implementace je možno po dohodě mezi zadavatelem a dodavatelem změnit případně doplnit, pokud v rámci implementační analýzy bude nalezen vhodnější postup nebo z analýzy vyplyne potřeba další funkcionality.

Rozdělení do fází:

První fáze: Řízení adresářových služeb

a. Implementační analýza 1. fáze
b. Akceptace analýzy 1. fáze
c. Převedení identit pod kontrolu dedikovaného systému OU
d. Zredukování závislosti na dodavatelích adresářových služeb
e. Rozšíření automatizace
f. Akceptace implementace 1. fáze
g. Uvedení 1. fáze do ostrého provozu
h. Servisní podpora implementační 1. fáze

Druhá fáze: Nový model identit

a. Implementační analýza 2. fáze
b. Akceptace analýzy 2. fáze
c. Zavedení modelu 1 identita ~ 1 člověk
d. Akceptace implementace 2. fáze
e. Uvedení 2. fáze do ostrého provozu
f. Servisní podpora implementační 2. fáze

Třetí fáze: Řízení práv a procesy

a. Implementační analýza 3. fáze

b. Akceptace analýzy 3. fáze
c. Zavedení řízení aplikačních rolí
d. Schvalovací workflow
e. Akceptace implementace 3. fáze
f. Uvedení 3. fáze do ostrého provozu

Hlavní systémy na OU ve vztahu k IDM

- STAG – informační systém studijní agendy, který eviduje studenty a absolventy. Založen na databázi Oracle.
- EIS MAGION - informační systém evidující informace o zaměstnancích. Založen na databázi Oracle.
- Kmen - systém, který eviduje jedinečný identifikátor osob v rámci OU. Založen na databázi Oracle.
- Centrální e-mailový server - systém pro centrální správu aliasů. Založen na linuxu.
- Evidence karet – systém evidující karty a informace o nich. Založen na databázi Oracle.

Řízení adresářových služeb (fáze 1)

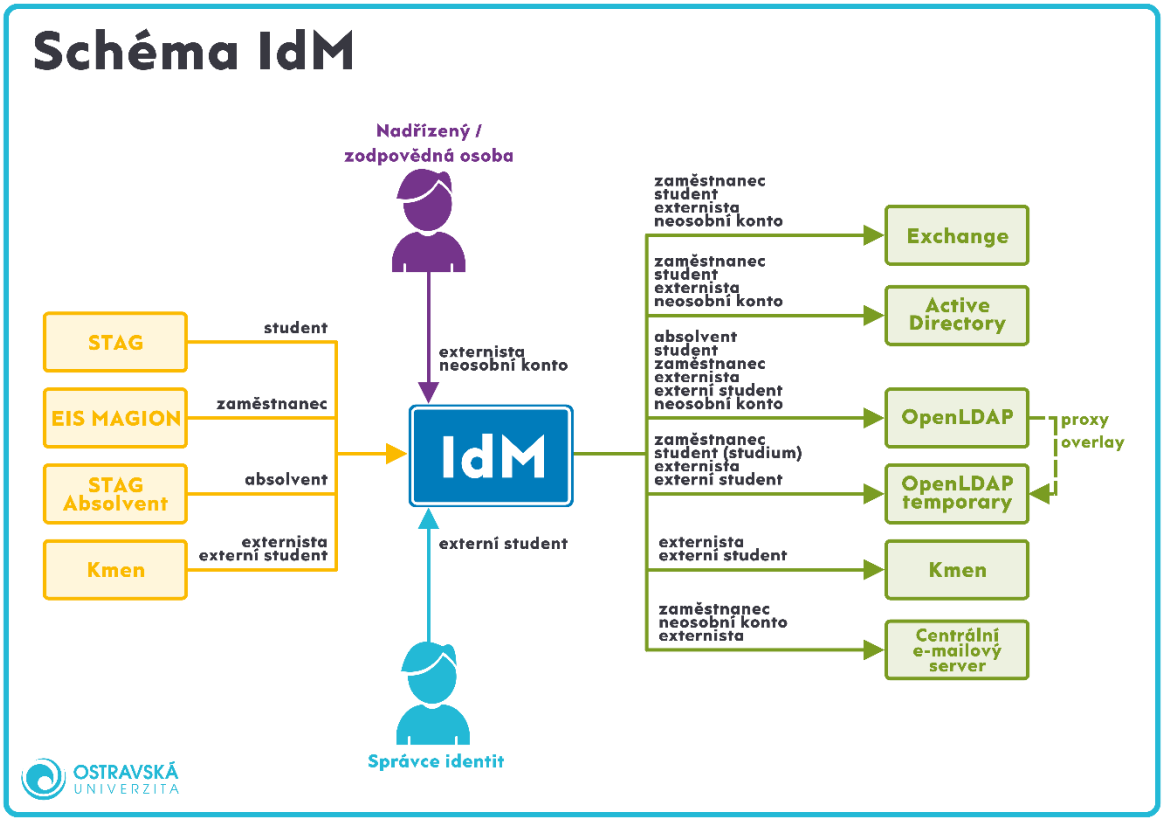
Cíle:

- Zavedení automatizovaného řízení kompletního životního cyklu všech typů identit
- Zavedení žádostí o zřízení identity pro externisty a neosobní konta (sdílené schránky), které budou dostupné nadřízeným / odpovědným osobám
- Nahrazení stávající adresářové služby Novell eDirectory za OpenLDAP, přičemž struktura dat bude z důvodu zpětné kompatibility zachována

Výsledný stav 1. fáze:

- IDM bude automatizovaně řídit životní cyklus stávajících identit
- IDM bude podporovat tyto typy identit: student, zaměstnanec, absolvent, externista, neosobní konto, externí student
- IDM bude evidovat právě jednu identitu pro každého studenta, navázaná studia budou evidována odděleně
- adresářová služba Novell eDirectory bude nahrazena novou službou založenou na OpenLDAP (v přehledovém schématu označeno jako *OpenLDAP temporary*)
    - OpenLDAP bude mít z důvodu zpětné kompatibility stejnou adresářovou strukturu a bude rovněž podporovat všechny atributy využívané v rámci Novell eDirectory
    - veškerá evidovaná data budou přemigrována do nové adresářové služby
    - služba bude provozována po přechodnou dobu do doby migrace všech aplikací na nový OpenLDAP obsahující nové účty pro studenty a zaměstnance
- IDM bude přebírat informace o studentovi (studiu) ze systému STAG

- IDM bude přebírat informace o zaměstnanci ze systému EIS MAGION
- IDM bude přebírat informace o absolventovi ze systému STAG a jeho modulu Absolvent
- IDM bude přebírat kmenové identifikátory pro externisty a externí studenty ze systému Kmen
- IDM bude nadřízeným / odpovědným osobám poskytovat žádosti pro správu životního cyklu identit externistů a neosobních kont (zřízení, zrušení, úprava atributů)
- IDM bude privilegovaným uživatelům (správcům identit) poskytovat funkcionalitu pro správu životního cyklu identit externích studentů
- IDM bude v systému Active Directory řídit účty pro tyto typy identit:
    - zaměstnanec – účty již existují
    - student – účty reprezentující studenty jako fyzické osoby, nyní neexistují
    - externista – účty již existují
    - neosobní konto – účty již existují
- IDM bude v systému OpenLDAP řídit účty pro tyto typy identit:
    - absolvent – účty již existují
    - student – účty reprezentující studenty jako fyzické osoby, nyní neexistují
    - zaměstnanec – účty pro zaměstnance, účty nyní neexistují
    - externista – účty pro externisty, účty nyní neexistují
    - externí student – účty pro externí studenty, účty nyní neexistují
    - neosobní konto – účty reprezentující neosobní konta, účty nyní neexistují
- IDM bude v systému OpenLDAP temporary (náhrada za Novell eDirectory) řídit účty pro tyto typy identit:
    - zaměstnanec – účty již existují
    - student (studium) – účty reprezentující jednotlivá studia studenta, účty již existují
    - externista – účty již existují
- IDM bude v systému Exchange řídit e-mailové schránky pro tyto typy identit:
    - zaměstnanec – schránky již existují
    - student – schránky pro studenty, nyní neexistují
    - externista – schránky již existují
    - neosobní konto – schránky již existují
- IDM bude zasílat informace o externistech a externích studentech do systému Kmen
- IDM bude zasílat informace o zaměstnancích, neosobních kontech a externistech do Centrálního e-mailového serveru
- Systém OpenLDAP bude s využitím *proxy overlay* zpřístupňovat účty zaměstnanců, externistů a studentů (studií) ze systému OpenLDAP temporary (náhrada za Novell eDirectory)
    - IDM musí zpřístupněné účty ignorovat (předpokládá se oddělení účtů pro jednotlivé typy identity na úrovni LDAP kontextu)



Integrační model první implementační fáze

Nový model identit (fáze 2)

Cíle:

- Zavést jednu identitu pro fyzickou osobu
- Zrušení systému OpenLDAP temporary (systém zaveden v první fázi jako náhrada za Novell eDirectory)

Výsledný stav 2. fáze:

- Zrušení identit studentů, které byly vytvářeny pro každé studium
- IDM bude při přebírání informací ze zdrojových systémů (STAG, EIS MAGION) provádět korelaci za účelem evidence právě jedné identity pro fyzickou osobu
- V rámci IDM proběhne sloučení identit zaměstnanců a studentů reprezentujících stejnou fyzickou osobu
- Přechodný OpenLDAP („OpenLDAP temporary“) bude bez náhrady zrušen
- IDM bude přebírat informace o přístupových kartách ze zdrojového systému karet

Řízení přístupových práv (fáze 3)

Cíle:

- Zavedení automatického řízení aplikačních rolí s vazbou na business parametry identit (např. typ pracovního vztahu, pracoviště, ...).
- Zavedení uživatelských žádostí o aplikační role, které budou schvalovány odpovědnými osobami (nadřízenými, garanty aplikací apod.)

Aplikační rolí se rozumí role pro konkrétní aplikaci, někdy je označována jako *technická role* nebo přímo oprávnění (např. *table-xyz-read*). Třetí fáze si neklade za cíl budování katalogu business rolí (logická role reprezentující funkci v rámci organizace, např. *sekretářka*) a bude pracovat jen a pouze s aplikačními rolemi. Od řešení bude nicméně požadováno, aby budoucí zavedení business rolí umožňovalo.

Výsledný stav 3. fáze:

- V rámci IDM bude existovat evidence aplikací a jejich aplikačních rolí
- IDM bude podporovat automatické přiřazení aplikačních rolí na základě definovaných pravidel využívajících business parametry identit
- IDM umožní uživatelské žádosti o přiřazení / odebrání aplikační role
- V rámci žádostí o přiřazení / odebrání aplikační role bude možné zavést schvalování odpovědnými osobami (nadřízený, garant aplikace apod.)
- IDM umožní online realizaci přístupových práv, tedy automatické nastavení příslušných vlastností účtů (atribut, přiřazení skupiny, apod.) přímo v cílovém systému (Active Directory, OpenLDAP)
- IDM umožní offline realizaci přístupových práv, kde nastavení práv provede správce manuálním zásahem na základě aktivity v realizačním workflow
    - obdoba helpdeskových tiketů
    - vhodné pro aplikace, které není možné řídit s využitím online realizace
- IDM umožní privilegovaným uživatelům zobrazení reportu přiřazených aplikačních rolí uživatele
- IDM umožní garantovi aplikace zobrazení reportu aplikačních rolí dané aplikace a jejich přiřazení uživatelům

Požadavky na řešení

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

- Oblast – popis požadavku.
- Doplňující vysvětlení – podrobnější popis požadavku
- Splňuje – vyjádření, jestli nabízené řešení splňuje požadavek.

Požadavky, které jsou výsledkem předběžné tržní konzultace jsou označeny kurzívou a podtržením.

1 Řízení adresářových služeb (fáze 1)

1.1 Procesy

ID	Oblast	Doplňující vysvětlení	Splňuje (ano/ne)
1.1.1	Zavedení studenta	IDM musí podporovat automatizovaný proces zavedení nového studenta. Proces bude iniciován načtením dat ze zdrojového systému IS/STAG, po kterém dojde k založení identity v IDM. IDM následně automaticky založí účet v Active Directory, OpenLDAP a rovněž založí e-mailovou schránku v Exchange. V systému OpenLDAP temporary bude založen účet reprezentující studium.	ANO
1.1.2	Evidence atributů studenta	IDM musí evidovat standardní atributy studenta – jméno, příjmení, tituly (před a za jménem), studijní číslo, kmenové číslo, studia, kontaktní údaje (e-mailová adresa, telefon, ...).	ANO
1.1.3	Přerušení studenta	IDM musí podporovat automatizovaný proces přerušení studenta. Proces bude iniciován načtením dat ze zdrojového systému IS/STAG, po kterém dojde k přerušení platnosti identity a zablokování souvisejících účtů. Po uplynutí definované lhůty dojde k úplnému smazání identity i účtů.	ANO
1.1.4	Odchod studenta	IDM musí podporovat automatizovaný proces odchodu studenta. Proces bude iniciován načtením dat ze zdrojového systému IS/STAG, po kterém dojde k zablokování identity studenta a všech souvisejících účtů. Po uplynutí definované lhůty dojde k úplnému smazání identity i účtů.	ANO
1.1.5	*Změna atributů studenta*	*IDM musí podporovat automatizovaný proces změny atributů studenta (např. změna příjmení, změna fakulty). Proces bude iniciován načtením dat ze zdrojového systému IS/STAG.*	ANO
1.1.6	Zavedení zaměstnance	IDM musí podporovat automatizovaný proces zavedení nového zaměstnance. Proces bude iniciován načtením dat ze zdrojového systému EIS Magion, po kterém dojde k založení identity v IDM. IDM následně automaticky založí účet v Active Directory, OpenLDAP a OpenLDAP temporary. IDM dále pro zaměstnance založí e-mailovou schránku v MS Exchange a zašle informace do Centrálního e-mailového serveru.	ANO
1.1.7	Evidence atributů zaměstnance	IDM musí evidovat standardní atributy zaměstnance – jméno, příjmení, tituly (před a za jménem),	ANO

		zaměstnanecké číslo, kmenové číslo, pracovní vztahy, kontaktní údaje (e-mailová adresa, telefon, ...).	
1.1.8	Odchod zaměstnance	IDM musí podporovat automatizovaný proces odchodu zaměstnance. Proces bude iniciován načtením dat ze zdrojového systému EIS Magion, po kterém dojde k zablokování identity zaměstnance a všech souvisejících účtů. Po uplynutí definované lhůty dojde k úplnému smazání identity i účtů.	ANO
1.1.9	*Změna atributů zaměstnance*	*IDM musí podporovat automatizovaný proces změny atributů zaměstnance (např. změna příjmení, změna organizační jednotky). Proces bude iniciován načtením dat ze zdrojového systému EIS Magion.*	ANO
1.1.10	Zavedení externisty	IDM musí podporovat automatizovaný proces zavedení nového externisty. Proces bude iniciován žádostí nadřízeného / odpovědné osoby. Po vyplnění a odeslání žádosti dojde k založení identity v IDM. IDM následně automaticky založí účet v Active Directory, OpenLDAP a OpenLDAP temporary. IDM dále pro externistu založí e-mailovou schránku v MS Exchange, zavede externistu do systému Kmen a zašle informace do Centrálního e-mailového serveru.	ANO
1.1.11	Evidence atributů externisty	IDM musí evidovat standardní atributy externisty – jméno, příjmení, tituly (před a za jménem), kmenové číslo, kontaktní údaje (e-mailová adresa, telefon, ...).	ANO
1.1.12	Odchod externisty	IDM musí podporovat automatizovaný proces odchodu externisty. Proces bude iniciován žádostí nadřízeného / odpovědné osoby v IDM, kde po jejím odeslání dojde k okamžitému smazání identity externisty a všech jeho účtů v řízených systémech.	ANO
1.1.13	Vznik neosobního konta	IDM musí podporovat automatizovaný proces zavedení nového neosobního konta. Proces bude iniciován žádostí nadřízeného / odpovědné osoby. Odeslaná žádost bude schvalována odpovědným pracovníkem CITu. Po schválení žádosti dojde k založení identity v IDM. IDM následně automaticky založí účet v Active Directory a OpenLDAP. IDM dále pro neosobní konto založí e-mailovou schránku v MS Exchange a zašle informace do Centrálního e-mailového serveru.	ANO
1.1.14	Evidence atributů neosobního konta	IDM musí evidovat potřebné atributy neosobního konta – garant, e-mailová adresa, ...	ANO
1.1.15	Zrušení neosobního konta	IDM musí podporovat automatizovaný proces zrušení neosobního konta. Proces bude iniciován žádostí nadřízeného / odpovědné osoby v IDM, kde po jejím	ANO

		odeslání dojde k okamžitému smazání identity reprezentující neosobní konto a všech souvisejících účtů v řízených systémech.	
1.1.16	Vznik externího studenta	IDM musí správci umožnit ruční založení identity pro externího studenta. IDM pro takovou identitu automaticky založí účet v OpenLDAP a OpenLDAP temporary. IDM dále pro externího založí e-mailovou schránku v MS Exchange, zavede externistu do systému Kmen a zašle informace do Centrálního e-mailového serveru.	ANO
1.1.17	Evidence atributů externího studenta	IDM musí evidovat standardní atributy externího studenta – jméno, příjmení, tituly (před a za jménem), kmenové číslo, kontaktní údaje (e-mailová adresa, telefon, ...).	ANO
1.1.18	Zrušení externího studenta	IDM musí podporovat automatizovaný proces zrušení externího studenta. V rámci IDM musí existovat proces, který smaže identitu externího studenta a všechny související účty po uplynutí jednoho roku od poslední aktivity.	ANO
1.1.19	Aktivace dříve založené identity	IDM musí umět založit identitu i před datem jejího nástupu. Takto založená identita bude neaktivní, neaktivní budou rovněž účty v integrovaných systémech. Aktivace identity a souvisejících účtů proběhne automaticky v den nástupu.	ANO
1.1.20	Zablokování identity	Správci IDM musí mít k dispozici nástroj, kterým s okamžitou platností pozastaví veškeré přístupy konkrétní osoby (identity) na dobu určitou nebo neurčitou. Identitu bude možné opětovně povolit a tím povolit i všechny její přístupy.	ANO
1.1.21	Jmenné politiky dle definovaných pravidel	IDM musí generovat uživatelská jména pro jednotlivé typy identit dle definovaných politik, a to včetně řešení jmenných konfliktů. IDM musí zabránit recyklaci historických uživatelských jmen.	ANO
1.1.22	Generované atributy	IDM musí umožnit generování hodnot pro všechny potřebné atributy (e-mailová adresa, sekvenční číslo pro absolventy). V případně potřeby musí IDM zajistit řešení konfliktů (například přidáním číselného sufixu apod.).	ANO
1.1.23	Zasílání e-mailových notifikací	IDM musí umožnit zasílání e-mailových notifikací navázaných na jednotlivé procesy (vznik identity, zrušení identity, ...). Příklady notifikací pro proces vzniku identity zaměstnance: zaslání notifikace s uživatelským jménem zaměstnanci, zaslání notifikace o založení identity nadřízenému, ...	ANO

1.1.24	Zasílání SMS notifikací	IDM musí umožnit integraci s SMS bránou za účelem zasílání notifikací navázaných na jednotlivé procesy (např. vznik identity). Příkladem je zaslání hesla v rámci procesu vzniku identity zaměstnance.	ANO

1.2 Zdrojové systémy k integraci

ID	Oblast	Doplňující vysvětlení	Splňuje (ano/ne)
1.2.1	Zdrojový systém – IS/STAG (Oracle DB)	IDM musí implementovat pravidelný import dat o studentech a jejich studiích ze studentské agendy IS/STAG. Předpokládaným zdrojem dat budou databázové VIEWS.	ANO
1.2.2	Okamžitá propagace změn z IS/STAG	IDM musí podporovat detekci změn dat o studentech ve zdrojovém systému IS/STAG a data importovat s maximálním zpožděním desítek sekund.	ANO
1.2.3	Mapování studentů na existující identity	Importovaní studenti musejí být mapování na existující identity buď explicitně podle identifikátoru ve studentské agendě nebo podle kmenového čísla. Noví studenti jsou založeni jako nové identity, identity existujících studentů jsou updatovány podle informací ze studentské agendy. IDM nesmí zakládat duplicitní identity pro stejného studenta.	ANO
1.2.4	Zdrojový systém – EIS MAGION (Oracle DB)	IDM musí implementovat pravidelný import dat o zaměstnancích a jejich pracovních vztazích z personálního systému EIS MAGION. Předpokládaným zdrojem dat budou databázové VIEWS	ANO
1.2.5	Okamžitá propagace změn z EIS MAGION	IDM musí podporovat detekci změn dat o zaměstnancích ve zdrojovém systému EIS MAGION a data importovat s maximálním zpožděním desítek sekund.	ANO
1.2.6	Mapování zaměstnanců na existující identity	Importovaní zaměstnanci musejí být mapování na existující identity buď explicitně podle identifikátoru v personálním systému nebo podle kmenového čísla. Noví zaměstnanci jsou založeni jako nové identity, identity existujících zaměstnanců jsou updatovány podle informací z personálního systému. IDM nesmí zakládat duplicitní identity pro stejného zaměstnance.	ANO
1.2.7	Zdrojový systém – IS/STAG Absolvent (Oracle DB)	IDM musí implementovat pravidelný import dat o absolventech ze zdrojového systému IS/STAG a jeho modulu Absolvent. Předpokládaným zdrojem dat bude databázové VIEW.	ANO

1.2.8	Okamžitá propagace změn z IS/STAG Absolvent	IDM musí podporovat detekci změn dat o absolventech ve zdrojovém systému IS/STAG Absolvent a data importovat s maximálním zpožděním desítek sekund.	ANO
1.2.9	Mapování absolventů na existující identity	Importovaní absolventi musejí být mapování na existující identity podle identifikátoru ve zdrojovém systému. Noví absolventi jsou založeni jako nové identity, identity existujících absolventů jsou updatovány podle informací ze zdrojového systému. IDM nesmí zakládat duplicitní identity pro stejného absolventa.	ANO
1.2.10	Zdrojový systém – Kmen (Oracle DB)	IDM musí implementovat pravidelný import kmenových identifikátorů pro externisty a externí studenty ze zdrojového systému Kmen. Předpokládaným zdrojem dat bude databázové VIEW.	ANO

1.3 Cílové systémy k integraci

Konektory IdM musí umět synchronizovat přístupy (číst, zapisovat a modifikovat účty a další struktury nutné pro přístup do cílového systému) a jejich práv (přiřazení nebo odebrání práva).

ID	Oblast	Doplňující vysvětlení	Splňuje (ano/ne)
1.3.1	Mapování účtů dle jmenných konvencí a případně dalších atributů účtu.	IDM musí mapovat účty dle jmenných konvencí a případně dalších atributů účtu (kmenové číslo) na konkrétní identity. Účty bez vlastníka budou hlášeny jako tzv. *orphan* účty.	ANO
1.3.2	Vynucení atributů účtů v cílových systémech, aby odpovídaly stavu v IDM	IDM musí vynutit atributy účtů v cílovém systému tak, aby reflektovaly schválený stav v IDM.	ANO
1.3.3	Podporované konektory	IDM musí podporovat přímé konektory do AD, MS Exchange (v hybridním režimu s Exchange online), MS SQL, DB table (ODBC nebo JDBC), LDAP a CSV / TXT souboru.	ANO
1.3.4	Synchronizace hesel do vybraných integrovaných systémů	IDM musí reagovat na změnu hesla a toto heslo propagovat do vybraných integrovaných systémů.	ANO
1.3.5	Zabezpečená komunikace se systémy	Komunikace mezi IDM a vzdálenými systémy musí probíhat zabezpečeným kanálem.	ANO
1.3.6	Rychlost konektoru (nastavitelný interval propagace změn)	IDM musí mít možnost nastavit interval propagace změn do integrovaných cílových systémů (pro každý systém samostatně).	ANO

Řešení IDM musí napřímo integrovat tyto systémy:

ID	Oblast	Doplňující vysvětlení	Splňuje (ano/ne)
1.3.7	Cílový systém – Active Directory (přímý konektor)	IDM musí integrovat systém AD přímým konektorem a podporovat tyto operace: vytvoření účtu, zablokování účtu, povolení účtu, zrušení účtu.	ANO
1.3.8	Cílový systém – Exchange (přímý konektor)	IDM musí integrovat systém Exchange (v hybridním režimu s Exchange online) přímým konektorem a podporovat tyto operace: zřízení schránky, přejmenování schránky, zrušení schránky.	ANO
1.3.9	Cílový systém – OpenLDAP (přímý konektor)	IDM musí integrovat systém OpenLDAP přímým konektorem a podporovat tyto operace: vytvoření účtu, zablokování účtu, povolení účtu, zrušení účtu.	ANO
1.3.10	Cílový systém – Kmen (přímý konektor)	IDM musí integorvat systém Kmen přímým konektorem a podporovat tyto operace: zavedení nového uživatele do Kmene.	ANO
1.3.11	Cílový systém – Centrální e-mailový server (přímý konektor)	IDM musí integorvat systém Centrální e-mailový server přímým konektorem a podporovat tyto operace: zavedení e-mailového aliasu, upravení e-mailového aliasu, zrušení e-mailového aliasu.	ANO

1.4 Správa hesel

ID	Oblast	Doplňující vysvětlení	Splňuje (ano/ne)
1.4.1	Evidence různých hesel	IDM musí podporovat evidenci různých hesel („centrální heslo“, eduroam heslo).	ANO
1.4.2	Synchronizace hesel napříč cílovými systémy	IDM musí umožňovat synchronizaci hesel napříč cílovými systémy připojenými přímým konektorem.	ANO
1.4.3	Změna hesla strojovým způsobem	IDM musí umožňovat změnu evidovaných hesel strojovým způsobem (např. prostřednictvím webových služeb).	ANO
1.4.4	Možnost definice heslové politiky a její vynucení	IDM musí umožňovat definici heslových politik, které musí následně vynucovat.	ANO
1.4.5	Šifrování hesel	IDM musí umožnit ukládání hesel v šifrované podobě.	ANO
1.4.6	Vynucení změny implicitního hesla	IDM musí umožnit vynucení změny implicitního hesla. Uživateli s implicitním heslem musí být přístupná jen omezená množina funkcionalit.	ANO
1.4.7	*Obnova hesla*	*IDM musí umožnit uživatelům reset hesla (self-service).*	ANO

1.5 Migrace dat

ID	Oblast	Doplňující vysvětlení	Splňuje (ano/ne)
1.5.1	Iniciální načtení dat strojovým způsobem (zdroje dat: LDIF, CSV)	IDM musí umožnit provedení iniciálního načtení dat strojovým způsobem (například s využitím webových služeb IDM, ze zdrojové databáze DB, ...). Vstupním podkladem musí být soubor, který je schopna OSU připravit jednoduchým způsobem (LDIF export adresářových služeb, CSV soubor). V rámci migrace musí být možné ponechání generovaných hodnot (uživatelské jméno, e-mailová adresa, ...) pro existující identity. Veškeré provedené operace musí být auditovány.	ANO
1.5.2	Režim simulovaného zápisu	IDM musí umožnit napojení integrovaného systému v režimu simulovaného zápisu, kdy zamýšlené změny jsou jen a pouze reportovány.	ANO

2 Nový model identit (fáze 2)

2.1 Procesy

ID	Oblast	Doplňující vysvětlení	Splňuje (ano/ne)
2.1.1	Korelace identity s využitím komplexních pravidel	IDM musí při načítání nové identity umožnit korelaci s využitím komplexních pravidel za účelem dohledání již existující identity pro fyzickou osobu. V případě existující identity nesmí dojít k založení nové, duplicitní, identity. Pro existující identitu musí dojít k navázání nových vztahů (studium, pracovní poměr), případně upravení atributů.	ANO
2.1.2	Prioritizace atributů identity	IDM musí pro identitu, která je zároveň zaměstnancem i studentem, umožnit prioritizaci zdroje atributů ve smyslu zdrojových systémů (EIS MAGION, STAG). Hodnoty pro některé atributy tedy mohou být přebírány ze STAGU pouze pokud nejsou nastaveny v EIS MAGION a podobně.	ANO
2.1.3	Evidence atributy identity o ID kartě	IDM musí evidovat standardní atributy přístupové karty – evidenční číslo, číslo čipu, počátek platnosti, konec platnosti.	ANO

2.2 Zdrojové systémy k integraci

ID	Oblast	Doplňující vysvětlení	Splňuje (ano/ne)
2.2.1	Zdrojový systém – karty (Oracle DB)	IDM musí implementovat pravidelný import dat o přístupových kartách z evidence karet. Předpokládaným zdrojem dat budou databázové VIEWS.	ANO

2.3 Migrace dat

ID	Oblast	Doplňující vysvětlení	Splňuje (ano/ne)
2.3.1	*Sloučení identit*	*IdM musí umožnit sloučení identit (student, zaměstnanec) reprezentujících stejnou fyzickou osobu (například s využitím API, přímo v DB, ...), kdy bude ponechána vždy právě jedna identita, na kterou budou navázány veškeré vztahy (studia, pracovní poměry) osoby. Na ponechanou identitu musí být možné přenést z mazaných identit evidované atributy.*	ANO

3 Řízení přístupových práv (fáze 3)

3.1 Datový model

ID	Oblast	Doplňující vysvětlení	Splňuje (ano/ne)
3.1.1	Katalog aplikací	IDM musí podporovat evidenci katalogu aplikací a jejich základních atributů – název, popis, garanti (pro účely realizace přístupových práv), apod.	ANO
3.1.2	Katalog aplikačních rolí	IDM musí podporovat evidenci aplikačních rolí a jejich základních atributů – název, popis, způsob realizace, parametry pro online realizace apod.	ANO
3.1.3	Katalog business rolí	IDM musí podporovat evidenci business rolí a jejich základních atributů – název, popis, vazba na organizační strukturu apod.	ANO
3.1.4	*Katalog systematizovaných míst*	*IDM musí podporovat evidenci systematizovaných míst, jejich základních atributů, přiřazení aplikačních rolí k systematizovaným místům. IDM umožní kopírování rolí mezi systematizovanými místy. Pro přiřazení identit k systematizovaným místům musí být možná vazba M:N (tedy identita může být na více*	ANO

		systémových místech, a současně na jednom systematizovaném místě může být více identit)	
3.1.5.	*Organizační struktura*	*IDM musí podporovat evidenci organizační struktury a její načtení a aktualizaci z EIS Magion.*	ANO
3.1.6	*Skupiny*	*IDM musí podporovat evidenci skupin a parametrické přiřazení členství ve skupinách. Skupiny musí být možno vnořovat.*	ANO
3.1.7	Parametrizované přiřazení aplikační role	IDM musí podporovat parametrizované přiřazení role uživateli nebo skupině, kde mezi minimální množinu parametrů patří – datum počátku platnosti přiřazení, datum konce platnosti přiřazení.	ANO

3.2 Procesy

ID	Oblast	Doplňující vysvětlení	Splňuje (ano/ne)
3.2.1	Automatické přiřazení aplikační role na základě definovaných pravidel	IDM musí podporovat automatizované přiřazení aplikačních rolí uživatelům nebo skupinám na základě definovaných pravidel. Tato pravidla mohou využívat libovolné evidované parametry identit.	ANO
3.2.2	Žádost o přiřazení aplikační role	IDM musí podporovat žádosti o přiřazení aplikačních rolí uživatelům. Žádost může být iniciována samotným uživatelem (zaměstnancem) případně jeho nadřízeným. *Součástí žádosti bude možnost nastavit platnost přiřazení práv (od-do).*	ANO
3.2.3	Žádost o odebrání aplikační role	IDM musí podporovat žádosti o odebrání aplikačních rolí uživatelům. Žádost může být iniciována samotným uživatelem (zaměstnancem), jeho nadřízeným nebo správcem aplikace.	ANO
3.2.4	Schvalování žádosti	V rámci žádosti musí být možné definovat libovolný počet schvalovacích aktivit. V rámci iniciální implementace se předpokládá schvalování nadřízeným. IDM musí umožnit přeskakování schvalovacích aktivit (například právě tehdy, když je schvalovatelem i iniciátorem žádosti stejná osoba). *IDM musí umožnit vícekrokové schvalování a řešení zastupitelnosti při schvalování.*	ANO
3.2.5	Online realizace přístupových práv	IDM musí umožnit online realizaci přístupových práv prostřednictvím nastavení potřebných vlastností účtu (atribut, přiřazení skupiny) v závislosti na konkrétní aplikační roli.	ANO
3.2.6	Offline realizace přístupových práv	IDM musí umožnit offline realizaci přístupových práv, kdy je po schválení žádosti přiřazen realizační tiket na	ANO

		správce aplikace. IDM musí umožnit správci označení tiketu jako realizovaného, čímž je potvrzeno přiřazení přístupového práva.	

3.3 Migrace dat

ID	Oblast	Doplňující vysvětlení	Splňuje (ano/ne)
3.3.1	Načtení katalogu aplikací a aplikačních rolí	IDM musí umožnit hromadné načtení aplikací a aplikačních rolí. Konkrétní způsob migrace bude určen v rámci implementačního projektu.	ANO
3.3.2	Načtení existujících přiřazení aplikačních rolí	IDM musí umožnit hromadné načtení existujících přiřazení aplikačních rolí uživatelům. Konkrétní způsob bude migrace určen v rámci implementačního projektu.	ANO

4 Požadavky společné pro všechny tři fáze:

4.1 Audit a reporting

ID	Oblast	Doplňující vysvětlení	Splňuje (ano/ne)
4.1.1	Report – orphan účty	IDM musí poskytnout ucelený report orphan účtů (účtů bez vlastníka) pro vybraný cílový systém.	ANO
4.1.2	Report – non-compliance	IDM musí poskytnout ucelený report nesouladu v nastavení práv evidovaném v rámci IDM a stavu evidovaném v konkrétním cílovém systému.	ANO
4.1.3	Report – identity a jejich přístupy	IDM musí poskytnout ucelený report vybraných uživatelů, jejich práv a jejich účtů v cílových systémech.	ANO
4.1.4	Report – historie změn	IDM musí poskytnout ucelený report změn / provedených operací nad konkrétní identitou. *IDM musí poskytnout report dat o příslušné identitě ve zvoleném časovému okamžiku (informace o stavu v minulosti)*	ANO
4.1.5.	*Konfigurovatelné reporty*	*IDM musí umožnit konfigurovat další reporty (a emailové upozornění) na základě definovaných události nebo změn.*	ANO
4.1.6	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).	ANO

4.1.7	Auditní záznamy pro administrační a uživatelské rozhraní	V rámci administračního 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.	ANO
4.1.8	Auditní záznamy musí být možné odkládat i mimo systém IDM	Auditní záznamy musí být možné odkládat i mimo systém IDM.	ANO

4.2 Uživatelské rozhraní

ID	Oblast	Doplňující vysvětlení	Splňuje (ano/ne)
4.2.1	Přizpůsobení rozhraní vzhledu dle OU	Uživatelské rozhraní musí být graficky přizpůsobeno prostředí OU.	ANO
4.2.2	Autentizace vůči provozní databázi IDM nebo integrovaného systému	Uživatelské rozhraní musí podporovat autentizaci s využitím uživatelského jména a hesla (kontrola proti provozní databázi IDM nebo integrovanému systému – AD, OpenLDAP, apod.)	ANO
4.2.3	Autentizace – maximální platnost session	IDM musí podporovat definování maximální platnosti session, kdy po jejím vypršení je uživatel nucen provést opětovné přihlášení.	ANO
4.2.4	Zobrazení detailu identity	Každý uživatel má právo vidět atributy své identity, svoje účty a jim přiřazená práva.	ANO
4.2.5	Obnova zapomenutého hesla	Uživatelské rozhraní musí poskytovat formulář pro obnovu zapomenutého hesla (inicializace procesu, nastavení nového hesla po ověření uživatele). Vygenerovaný token pro ověření uživatele musí mít omezenou platnost.	ANO
4.2.6	Změna kontaktních údajů	Uživatelské rozhraní musí poskytovat formulář pro změnu vybraných kontaktních údajů identity (soukromá e-mailová adresa, mobilní telefon, ...).	ANO
4.2.7	Žádost o založení identity pro externistu	V rámci uživatelského rozhraní bude moci nadřízený požádat o založení identity pro externistu. Žádost bude iniciována odesláním příslušného formuláře a nebude podléhat schvalování.	ANO
4.2.8	Žádost o založení identity pro neosobní konto	V rámci uživatelského rozhraní bude moci nadřízený požádat o založení identity pro neosobní konto. Žádost bude iniciována odesláním příslušného formuláře a bude schvalována odpovědným pracovníkem CITu.	ANO
4.2.9	Žádost o založení identity pro externího studenta	V rámci uživatelského rozhraní bude moci uživatel požádat o založení identity pro externího studenta.	ANO

		Žádost bude iniciována odesláním příslušného formuláře a bude schvalována odpovědným pracovníkem (správcem identit).	
4.2.10	Žádost o přiřazení aplikační role	V rámci uživatelského rozhraní bude moci uživatel (i jeho nadřízený) požádat o přiřazení aplikační role. Žádost bude iniciována odesláním příslušného formuláře a bude schvalována nadřízeným (v případě iniciování uživatelem). V případě offline realizace bude po schválení následovat realizační část prováděná správcem aplikace.	ANO
4.2.11	Žádost o odebrání aplikační role	V rámci uživatelského rozhraní bude moci uživatel (i jeho nadřízený) požádat o odebrání aplikační role. Žádost bude iniciována odesláním příslušného formuláře a bude schvalována nadřízeným (v případě iniciování uživatelem). V případě offline realizace bude po schválení následovat realizační část prováděná správcem aplikace.	ANO
4.2.12	Přehled žádostí	Uživatelské rozhraní musí obsahovat přehled žádostí. Pro běžného uživatele budou zobrazeny pouze jím vytvořené žádosti. Privilegovaný uživatel (správce) bude mít přístupné všechny žádosti.	ANO
4.2.13	Přehled schvalovacích úkolů	V rámci uživatelského rozhraní bude dostupný seznam úkolů ke schválení. Schvalovatel bude moci jednotlivé úkoly schválit nebo zamítnout a případně připojit poznámku.	ANO
4.2.14	Zablokování a odblokování identity	Privilegovaný uživatel (správce) musí mít možnost vybranou identitu zablokovat nebo odblokovat.	ANO
4.2.15	Povolení identity	Privilegovaný uživatel (správce) musí mít možnost ručně prodloužit platnost identity a tím zachovat aktivní její přístupy.	ANO
4.2.16	Změna atributů identity	Privilegovaný uživatel (správce) musí mít možnost ručně upravit vybrané atributy identity (uživatelské jméno, kontaktní údaje, ...).	ANO
4.2.17	Reporty	Privilegovaní uživatelé budou mít v rámci uživatelského rozhraní přístup ke generování reportů.	ANO
4.2.18	Lokalizace do českého a anglického jazyka	Uživatelské rozhraní musí být plně lokalizováno do českého a anglického jazyka.	ANO

4.3 Administrátorské rozhraní

ID	Oblast	Doplňující vysvětlení	Splňuje (ano/ne)
4.3.1	Autentizace - přístup pouze pro	Přístup do administrátorského rozhraní musí být umožněn jen a pouze privilegovaným uživatelům	ANO

	privilegované uživatele	(správcům). *Autentizace musí podporovat vícefaktorové přihlášení.*	
4.3.2	Přehled cílových systémů	Administrátorské rozhraní musí nabídnout přehled cílových systémů a jejich stav (datum poslední synchronizace atp.).	ANO
4.3.3	Manuální spuštění synchronizačních procesů	Administrátorské rozhraní musí umožnit manuální spuštění jednotlivých synchronizačních procesů (načtení zdrojových systémů a propagace změn do cílových systémů).	ANO
4.3.4	*Správa objektů*	*Administrátorské rozhraní musí umožnit správu objektů evidovaných v IDM.*	ANO
4.3.5	*Vyhledávání bez diakritiky*	*Administrátorské rozhraní musí umožnit vyhledávání bez diakritiky (např. zadání Novak vyhledává i Novák apod.)*	ANO
4.3.6	*Export do CSV*	*Administrátorské rozhraní musí umožňovat export výpisů či přehledů do souboru typu CSV a případně XML.*	ANO
4.3.7	*Nastavení administrátorských práv*	*Administrátorské rozhraní musí mít možnost nastavit práva jednotlivým privilegovaným uživatelům (správcům), aby bylo možno nastavit správce s nižším oprávněním (např. read-only).*	ANO
4.3.8.	*Dashboard*	*Administrátorské rozhraní musí obsahovat dashboard, který bude obsahovat přehled chyb v systému IDM.*	ANO

4.4 Příprava produktivního provozu a provoz IDM

ID	Oblast	Doplňující vysvětlení	Splňuje (ano/ne)
4.4.1	Přechod do produkce (fáze 1):	Dodavatel IDM musí (v součinnosti s OU) zajistit přechod systému IDM v rozsahu fáze 1 do produkce. Toto zahrnuje iniciální načtení dat do IDM a postupné napojení integrovaných systémů. Každý integrovaný systém musí být nejdříve napojen v režimu simulovaného zápisu, kdy IDM vždy vygeneruje report zamýšlených změn, ale tyto ve skutečnosti neprovádí. Až po odsouhlasení správnosti změn OU bude systém napojen v režimu zápisu a změny budou skutečně provedeny.	ANO
4.4.2	Přechod do produkce (fáze 2):	Dodavatel IDM musí (v součinnosti s OU) zajistit sloučení evidovaných identit za účelem přechodu na nový model identit. Dále musí dodavatel IDM poskytnout součinnost při rušení přechodného adresářového úložiště (OpenLDAP temporary).	ANO

4.4.3	Přechod do produkce (fáze 3):	Dodavatel IDM musí (v součinnosti s OU) zajistit přechod systému IDM v rozsahu fáze 3 do produkce. Toto zahrnuje iniciální načtení dat aplikací, aplikačních rolí a přiřazení aplikačních rolí uživatelům.	ANO
4.4.4	Řešení zálohování tak, aby bylo součástí standardního procesu zálohování na OU	Řešení IDM musí být součástí standardního procesu zálohování na OU tak, aby v případě poškození datového úložiště nebo IDM serveru bylo možné provoz v minimálním čase obnovit.	ANO
4.4.5	Příprava a otestování plánu obnovy (DRP)	Dodavatel IDM musí vytvořit a otestovat plán obnovy IDM infrastruktury.	ANO
4.4.6	Implementační servisní podpora	Podpora implementovaného řešení IDM pro OU musí být zajištěna od ukončení fází 1 a 2 až do finálního uvedení celého projektu do ostrého provozu. Podpora musí zahrnovat řešení problémů s konfigurací a funkčností IDM a dodávky nových verzí SW. Požadovaný režim podpory je online. U kritických incidentů, které znemožňují provoz systémů na OU nebo jej závazně narušují, musí být počátek řešení problému do 4 pracovních hodin od nahlášení. U nekritických problémů musí být počátek řešení do jednoho pracovního dne.	ANO
4.4.7	Postimplementační servisní podpora	Podpora implementovaného řešení IDM pro OU musí být zajištěna od uvedení celého projektu do ostrého provozu alespoň po dobu 12 měsíců. Podpora musí zahrnovat řešení problémů s konfigurací a funkčností IDM a dodávky nových verzí SW. Požadovaný režim podpory je online. U kritických incidentů, které znemožňují provoz systémů na OU nebo jej závazně narušují, musí být počátek řešení problému do 4 pracovních hodin od nahlášení. U nekritických problémů musí být počátek řešení do jednoho pracovního dne.	ANO

4.5 Licenční požadavky

ID	Oblast	Doplňující vysvětlení	Splňuje (ano/ne)
4.5.1	Dodatečné licence adresářových služeb (třetích stran)	IDM by nemělo vyžadovat dodatečné náklady na licence adresářových služeb na straně OU (AD, eDirectory) nad rámec licencí, které jsou použity bez IDM.	ANO

4.5.2	*Licenční model IDM*	*IDM nebude vyžadovat/obsahovat licence (dodávaného řešení) závislé na počtu spravovaných identit, počtu záznamů, velikosti databází nebo jiná podobná omezení.*	ANO

4.6 Ostatní požadavky

ID	Oblast	Doplňující vysvětlení	Splňuje (ano/ne)
4.6.1	Kapacitní požadavky	IDM musí spravovat identity pro všechny typy uživatelů na OU (cca 15000 identit). Takový počet identit nesmí mít negativní vliv na výkon / odezvu IDM. IDM musí umožnit evidenci historických neaktivních identit za účelem umožnění opětovného nástupu.	ANO
4.6.2	*Změny transakčně*	*IDM musí veškeré změny provádět transakčně.*	ANO
4.6.3	*Ochrana proti hromadným změnám*	*IDM musí obsahovat mechanismus pro zabránění hromadným změnám v případě chybných vstupních dat, aby nedošlo nežádoucím hromadným změnám (např. odstranění velkého množství účtů).*	ANO
4.6.4	*Rozšiřitelnost*	*IDM musí podporovat možnost změn konfigurace - např. přidání nového typu uživatele, rozšíření atributů u libovolného typu objektu, vytvoření nových nebo změna nastavených workflow atd.*	ANO
4.6.5	*Workflow*	*IDM musí podporovat ty možnosti u workflow:* *- Zadávání požadavků uživateli* *- Možnost sledování stavu svých požadavků uživateli* *- E-mailové upozornění schvalovatele na požadavek ke schválení* *- Přehled úloh ke schválení pro každého schvalovatele* *- Schvalování či zamítnutí požadavků včetně uvedení zdůvodnění* *- Podpora vícekrokového schvalování* *- Podpora schvalování jedním nebo více schvalovateli (skupinou schvalovatelů)* *- Možnost větvení pro ošetření výjimek vzniklých při schvalování* *- Řešení zastupitelnosti* *- Eskalace - upozornění při překročení termínu splnění* *- Možnost vkládání systémových kroků s voláním webových služeb a spuštěním skriptů* *- Periodická revize aktiv jednotlivými garanty*	ANO
4.6.6	*Synchronizace*	*IdM musí umožňovat nastavit režim synchronizace separátně pro každý konektor. Režimy synchronizace musí umožňovat:*	ANO

		- Plná synchronizace – prochází všechny objekty v IdM a synchronizuje je s objekty daného systému *- Změnová synchronizace – synchronizuje vždy jen změny od poslední spuštěné synchronizace.* *- Okamžitá synchronizace konkrétní identity na vyžádání – synchronizuje pouze vybranou identitu.* *- Rekonciliační synchronizace – synchronizace vytvoří rekonciliační report pro porovnání změn mezi nastavením identit a jejich oprávnění pro daný systém v IDM vs. nastavení identit a oprávnění přímo v připojeném systému.* *- Simulační synchronizace – synchronizace vytvoří report očekávaných změn v napojeném systému pro provedení ostré synchronizace.*	
4.6.7	Okamžitá odezva uživatelského rozhraní, spouštění komplexních operací na pozadí.	Uživatelské rozhraní musí poskytovat okamžitou odezvu pro koncové uživatele IDM. Pokud je z uživatelského rozhraní zadán požadavek na vytvoření komplexního reportu, žádosti nebo provedení administrativní operace, která má charakter dávkové operace, pak musí být spuštěna „na pozadí“. Uživatel musí být notifikován o zahájení a dokončení takové operace.	ANO
4.6.8	*Zvyšování výkonu*	*IDM musí umožňovat zvyšování výkonu (zlepšování odezvy) např. rozložením na více serverů.*	ANO
4.6.9	*Strojové rozhraní (API) pro správu objektů v IDM*	*IDM musí poskytovat strojové rozhraní (WSDL, REST, SOAP), které umožní správu objektů evidovaných v rámci IDM. Rozhraní musí splňovat specifikace WS–Security, WS-SecurityPolicy, WS-ReliableMessaging, WS-AtomicTransactions.* *Konfigurace umožní nastavit přístup pro volání jednotlivých vybraných služeb strojového rozhraní pro každý odpovídající systémový účet samostatně.* *Volání strojového rozhraní bude logováno na úrovni databáze*	ANO
4.6.10	*Autentizační brána*	*Řešení musí umožňovat případné použití autentizační brány v budoucnu (vybudování autentizační brány není součástí projektu IDM). Musí umožnit ověření identit vůči externím poskytovatelům identit (NIA).*	ANO
4.6.11	*Vícefaktorová autentizace*	*Řešení musí umožňovat využití vícefaktorové autentizace v budoucnu (vícefaktorová autentizace pro uživatele není součástí projektu IDM).*	ANO
4.6.12	*Podpora eIDAS*	*IDM umožní implementaci procesů a rozhraní, která jsou vyžadována v Nařízení Evropského parlamentu a Rady (EU) č. 910/2014 ze dne 23. července 2014 o*	ANO

		elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES.	
4.6.13	*Splnění požadavků VIS*	*IDM musí splňovat požadavky na významný informační systém (VIS) dle zákona o kybernetické bezpečnosti (č. 181/2014 Sb.)*	ANO
4.6.14	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	ANO
4.6.15	Školení správců IDM	Dodavatel IDM musí poskytnout následující školení: školení správců IDM – školení pro pracovníky CIT	ANO

doc. Mgr. Pavel Drozd, Ph.D.
Digitálně podepsal doc. Mgr. Pavel Drozd, Ph.D.
Datum: 2022.12.19 14:36:00 +01'00'

Bc. Vladimír Vybíral, MBA
Digitálně podepsal Bc. Vladimír Vybíral, MBA
Datum: 2022.12.01 14:37:20 +01'00'