Rozvoj nástroje pro správu identit (IAM)

Technický popis požadovaného řešení

Obsah

Seznam tabulek:

1 ÚVOD

Tento dokument obsahuje technickou specifikaci řešení a autorizačních požadavků na systém Identity Management (dále uváděné také IDM) - pro správu běžných uživatelů a řízení přístupů uživatelů do koncových systémů a autentizačních požadavků na Access Management (dále uváděné také AM).
Dokument je přílohou zadávací dokumentace veřejné zakázky „Rozvoj nástroje pro správu identit (IAM) FS“ a obsahuje seznámení s konceptem požadovaného řešení, základní popis poptávaného řešení a závazné požadavky pro všechny potenciální uchazeče o zajištění realizace zakázky. Závazné požadavky jsou uvedeny v tabulkách obsahujících ID požadavku, jeho popis a a prázdný sloupec „Způsob naplnění“, kde je očekáváno jeho vyplnění dodavatelem.

1.1 Vysvětlení zkratek a pojmů použitých v dokumentu

Zkratka	Vysvětlení
AD	Microsoft Active Directory
ADIS	Automatizovaný daňový informační systém
AM	Access Management
API	Application Programming Interface, publikované rozhraní pro komunikaci s aplikací
CRUD	Create, read, update, delete. Základní operace s datovým záznamem.
DMZ	Demilitarizovaná zóna
DWH	Data warehouse, datový sklad
eIDAS	Nařízení Evropské unie č. 910/2014 o elektronické identifikaci a důvěryhodných službách pro elektronické transakce na vnitřním evropském trhu.
FO	Fyzická osoba
FOP	Fyzická osoba podnikající
FS	Finanční správa České republiky
GDPR	General Data Protection Regulation
GFŘ	Generální finanční ředitelství
IAM	Identity and Access Management, Centrální správa identit
IDM	Identity Management
IdP	Identity Provider
IDS	Interní identifikátor subjektu v rámci prostředí FS
IT	Obecné označení pro procesy správy a podpory ICT v rámci organizace
JIP	Jednotný identitní prostor
MF	Ministerstvo financí České republiky
SIEM	Security Information and Event Management
nRS	Nový registr subjektů
NIA	Národní identitní autorita
KAAS	Katalog autentizačních a autorizačních služeb

Zkratka	Vysvětlení
LDAP	Lightweight Directory Access Protocol
LoA	Úroveň záruky (Level of Assurance) vyjadřuje míru spolehlivosti prostředků pro elektronickou identifikaci při určování totožnosti dané osoby. Míra spolehlivosti, kterou úroveň záruky představuje, je definována na základě použitých postupů, řídících činností a prováděných technických kontrol.
OSIRIS	Interní systém evidence činností přidělených jednotlivým zaměstnancům FS.
RBAC	Role-Based Access Control
ROB	Registr obyvatel
ROS	Registr osob
SAML	Security Assertion Markup Language
SeP	Service Provider
SLA	Servis Level Agreement
SoD	Segregation of Duties
SSO	Single Sign-On
VoKB	Vyhláška č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti)
ZoKB	Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů
KII	Kritická informační infrastruktura

Tabulka 1 - Zkratky

Pojem	Vysvětlení
Aplikační role	Samostatná entita, která odpovídá objektu v koncovém systému (např. skupině v AD, skupině oprávnění v koncové aplikaci).
Autentizace	Proces ověření proklamované identity subjektu
Autorizace	Proces získávání souhlasu s provedením nějaké operace nebo povolení přístupu
Business role	Samostatná entita, která v sobě nese aplikační role do koncových systémů nebo jiné business role
Certifikace, Recertifikace, Atestace	Smyslem certifikace je v pravidelných intervalech ověřovat, zda uživatel má přiděleny stále ta oprávnění, která má mít vzhledem ke své pozici, projektu či procesu, který vykonává. Nadbytečná oprávnění jsou po ukončení certifikace odebrána. Proces certifikace je možné chápat jako dodatečnou kontrolu automatických rutin pomocí lidského faktoru, kterým je například nadřízený uživatele nebo auditor.
Delegace	Možnost pověřit vybraný požadavek ke schválení (nebo vybranou

Pojem	Vysvětlení
	skupinu požadavků) na jiného zvoleného schvalovatele.
eGovernment	Soubor služeb, metodik a aplikací, vytvářející prostředí informačních technologií v rámci státní správy ČR
Entitlement	Schopnost nebo nárok přistupovat ke službě či zdroji. Příklad: nový zaměstnanec má nárok (entitlement) na přístup k firemnímu emailu. Ten je mu však přidělen až poté, co je založen v informačních systémech (proběhne provisioning) a jsou mu nastavena patřičná oprávnění.
Externí identita	FS prostřednictvím IAM není vlastníkem identity a neřídí její životní cyklus, k autentizaci jsou využity externí identity provideři (NIA, JIP-KAAS).
Externí uživatel	Fyzická osoba přistupující do portálu MOJE daně pro podání daňového přiznání s identifikací v NIA
Identifikační prostředek	Identifikační prostředky slouží pro vzdálené prokazování totožnosti při využívání online služeb. Jsou vydávané v souladu se zákonem č. 250/2017 Sb., o elektronické identifikaci, ve znění pozdějších předpisů.
Identitaobcana.cz	Portál zpřístupňující funkcionalitu pro občany a funkcionalitu pro poskytovatele služeb (portál Národního bodu).
Identita občana	Národní identitní autorita zajišťuje orgánům veřejné správy státem garantované služby identifikace a autentizace včetně federace údajů o subjektu práva ze základních registrů a možnost předávání přihlašovací identity dle principu Single Sign-On. Veřejným rozhraním národní identitní autority pro přístup uživatelů a poskytovatelů online služeb je portál národního bodu - identitaobcana.cz.
Identity Provider	Kvalifikovaný správce dle zákona č. 250/2017 Sb., o elektronické identifikaci. Subjekt poskytující důvěryhodnou službu identifikace a autentizace fyzické osoby pomocí jím vydaných prostředků identifikace
Interní identita	Identita řízená v rámci IAM, FS je referenčním zdrojem identity a řídí její životní cyklus.
Interní uživatel	Interní pracovník FS, který pracuje s komponentou v rámci Automatizovaného daňového informačního systému
Jednotný identitní prostor	Zabezpečený adresář orgánů veřejné moci a uživatelských účtů úředník, který je součástí systému Czech POINT.
Katalog autentizačních a autorizačních služeb	Rozhraní webových služeb, které umožňují jednak autentizaci uživatelů přistupujících do AIS či ISVS pomocí přihlašovacích údajů v JIP, jednak umožňují editaci údajů subjektů a uživatelských účtů v JIP.
MOJE daně	Uživatelský portál mimo jiné pro podání a správu daňových přiznání
Národní bod	Zákon č. 250/2017 Sb., o elektronické identifikaci, definuje národní bod pro identifikaci a autentizaci jako informační systém, který zajišťuje

Pojem	Vysvětlení
	zprostředkování elektronické identifikace mezi poskytovateli prostředků, kterými uživatel prokazuje svoji identitu, a poskytovateli online služeb, a to včetně napojení na další ohlášené systémy v rámci EU pomocí mezinárodního uzlu.
Národní identitní autorita	Zprostředkovává služby důvěryhodných poskytovatelů identit (Identity Provider – IdP) jednotlivým důvěryhodným poskytovatelům služeb (Service Provider – SeP) vyžadujícím důvěryhodnost autentizací přistupujících subjektů (uživatelů). NIA dále zprostředkovává poskytnutí důvěryhodných údajů o těchto subjektech (tj. jejich atributů prostřednictvím tzv. assertions/claims) z připojených zdrojů těchto údajů a pro zajištění důsledného oddělení jednotlivých kmenů zajišťuje vydávání unikátních identifikátorů pro každého registrovaného SeP. Součástí NIA je podpora administrativních procesů nutných k registraci IdP a SeP a navázání jejich důvěry. Dále NIA zahrnuje persistentní úložiště a uživatelské rozhraní pro správu subjektem definovaných údajů. Rozhraní pro veřejnost (subjekty údajů) a pro správce připojených systémů (SeP, IdP) je poskytováno prostřednictvím webového portálu na identitaobcana.cz.
Oprávnění	Povolení uživateli provést nějakou operaci
Portál národního bodu	Úvodní stránka portálu národního bodu, který je umístěn na adrese https://identitaobcana.cz
Privilegovaný účet	Uživatelský účet informačního systému s širokou nebo neomezenou množinou administrátorských oprávnění, který je zpravidla nepersonalizovaný a může být sdílen mezi vícero uživateli.
Referenční údaje	Údaj vedený v základním registru, který zákon č. 111/2009 Sb., o základních registrech, označuje jako údaj, který je považovaný za správný a právně závazný, pokud není prokázán opak nebo pokud nevznikne pochybnost o jeho správnosti.
Rekonciliace	Při rekonciliaci se prochází všechny uživatelské účty v koncovém systému a na základě definovaných akcí se aktualizují identity uživatelů v IDM. Jde o uvedení účtů do souladu s IDM. Tedy účtům v koncových systémech se přidělují vlastníci (identity IDM) na základě logických podmínek např. korelace uživatelského jména, emailu apod. Účty bez vlastníka jsou reportovány, nebo rovnou mazány z koncového systému (podle nastavení IDM). Procesem rekonciliace je vynucen soulad a řád v koncových systémech.
Role	Aplikační + business role (v dokumentu pod pojmem „role“ jsou obecně míněny aplikační i business role, kdy konkrétní upřesnění v rámci IAM bude již záležitost konkrétního nastavení „správcem rolí“)
Role Based Access Control	Model, ve kterém jsou uživateli přiřazeny role, které mu dávají určitý stupeň přístupu ke zdroji. Přiřazení role garantuje uživateli definovanou sadu entitlementů (nároků na oprávnění), které jsou přiřazeny buď automaticky, nebo po splnění určité podmínky, nebo na základě

Pojem	Vysvětlení
	schválení odpovědnými osobami. Výhodou modelu RBAC je opětovná použitelnost přidělených rolí a možnost definování atributů role – např. popis.
Segregation of Duties	Kontrola konfliktních oprávnění
Service Provider	Kvalifikovaný poskytovatel dle zákona č. 250/2017 Sb., o elektronické identifikaci
Single Sign-On	Jednotné přihlášení je schéma ověřování, které umožňuje uživateli přihlásit se pomocí jediného ID do kteréhokoli z několika souvisejících, ale nezávislých softwarových systémů. Skutečné jednotné přihlášení umožňuje uživateli přihlásit se jednou a přistupovat ke službám bez opětovného zadávání ověřovacích faktorů.
Vendor lock-in	Závislost provozovatele systému nebo služby na jednom konkrétním dodavateli.
Zastupování	Možnost nastavit zástupce pro všechny požadavky, které budou na určenou dobu směrovány na vybranou zastupující osobu.

Tabulka 2 - Pojmy

2 SHRNUTÍ PROJEKTU ZADAVATELE

Tento dokument obsahuje soubor požadavků na funkční celek Identity a Access Management IDM/IAM.

Cílem zavedení IAM nástroje je centralizace a procesní řízení schvalování a přiřazování přístupů uživatelů k informačním zdrojům v podobě agend úřadu. Jedná se tedy o centralizaci řízení oprávnění (autorizací) k informačním systémům. Tato část funkcí IAM nástroje se označuje jako Identity Management (IDM). Podmnožinou tematiky IAM je i soubor autentizačních operací/procesů, jehož součástí je delegace identit z externích IdP.

IAM bude nasazeno ve dvou variantách, a to jako interní a externí. Interní bude sloužit primárně pro správu zaměstnanců a systémů, které využívají, externím IAM bude obdobně sloužit pro správu externích uživatelů.

Systém bude sloužit k transparentnímu a bezpečnému řízení oprávnění. Plošným zavedením IAM dojde k narovnání schválených a reálných přístupů uživatelů do informačních systémů s příslušným oprávněním.

IAM slouží zároveň jako základní instrument pro audity, kdy bude schopen odpovědět na dotazy: kdo z uživatelů má jaký přístup do jakého informačního systému a na základě jakého titulu (systemizované místo, schválení nadřízeným atd.). Vedle nástroje pro audit IAM zajistí i certifikační kampaně, tedy pře-ověření a pře-schválení přístupů do koncových systémů ze strany nadřízených, čímž se zajistí, že aktuální stav odpovídá aktuální potřebě úřadu.

IAM má za úkol řídit informace o uživatelích v počítačích (online identita). Spravuje jejich autorizaci, oprávnění, role a hierarchie s cílem zvýšit zabezpečení a produktivitu a zároveň snížit náklady, prostoje a opakující se úkoly. Dále IAM řídí i autentizaci (acces management) uživatelů v rámci politik a technologií k zajištění toho, aby správní lidé v podniku měli odpovídající přístup k technologickým zdrojům (IAM, viz článek autentizace uživatele a řízení přístupu). Systémy pro správu identit patří do oblasti IT bezpečnosti a správy dat. IAM systémy identifikují a autentizují nejen uživatele IT zdrojů, ale také hardware a aplikace, k nimž mají uživatelé přístup. IAM se zabývá otázkami jako jak uživatelé získávají identitu a členství ve skupině (role), ochranou identity před zcizením (krádež identity) a technologiemi, které podporují tuto ochranu, řízením životního cyklu apod.

Nutnost zavedení centrální správy identit a řízení uživatelů z pohledu autorizací a přístupů k informačním zdrojům v koncových systémech úřadu plyne také z požadavků kybernetické bezpečnosti na správu identit a přístupů.

2.1 Nástroj pro správu identit a oprávnění

Po instalaci nástroje pro správu identit a oprávnění (IDM) bude existovat centrální bod udržující přehled o přístupech všech uživatelů (interních a externích) do všech informačních systémů bez ohledu na to, zda je technicky možné informační systém na IDM napojit či nikoliv. Systém IDM by tak měl být napojen na doménu (Active Directory/LDAP), kde by měl spravovat všechny uživatelské účty a jejich členství ve skupinách. Dále by měl být systém IDM napojen na jednotlivé informační systémy FS, kde by měl být schopen řídit oprávnění jednotlivých uživatelů. V případě, kdy nebude technicky možné napojit systém IDM na některý informační systém, bude vytvořen tzv. „virtuální end-point“, kdy bude systém IAM pouze zaznamenávat přidělená oprávnění a předávat tyto informace správcům příslušných systémů pro ruční zpracování v rámci daných systémů.

2.2 Nástroj pro správu autentizací

Cílem této aktivity je především zavedení prostředků (Autentizační systém, označovaný jako Access management nebo AM) pro ověřování autenticity požadavků oprávněných osob v prostředí informačních systémů a infastruktury FS, napojení na systém IDM a otestování v ostrém provozu na sadě informačních systémů. Následným krokem je pak postupné zapojování všech aktiv organizace do tohoto systému.

Primárním cílem vybudování Autentizační infrastruktury, která mimo jiné bude poskytovat jednotné přihlašování, kdy se uživatel nemusí opakovaně autentizovat při přechodu mezi aplikacemi zapojenými do této Autentizační (SSO-Single Sign On) infrastruktury. V dnešní době je SSO funkcionalita standardně předpokládána, důraz je však kladen na autentizaci (identifikaci) přistupující osoby – uživatele. Základní (nejrozšířenější) způsob přihlašování je pomocí uživatelského jména a hesla, případně pomocí certifikátu.

V dnešní době se stává de facto standardem vícefaktorová autentizace, za použití prostředků, které uživatel vlastní, tj. nemůže je sdílet a je snaha o důvěryhodnou identifikaci přistupující osoby. V souvislosti s tím, že se uživatel může autentizovat různými metodami, se dnes hovoří i o tzv. úrovni ověření, tedy míře důvěry v použitou autentizační metodu, kterou se uživatel autentizoval, tj. v to, že osoba je skutečně tou osobou, za kterou se vydává. Tato úroveň ověření pak může být parametrem pro autorizaci do vybraných aplikací, kdy každá aplikace specifikuje minimální úroveň ověření a uživatel není vpuštěn do aplikace, která vyžaduje vyšší úroveň ověření, než má aktuálně přistupující uživatel.

Důvody těchto změn jsou zejména bezpečnostní, tj. nárůst zcizování a zneužívání přístupových údajů; právní, tj. provádění auditu provedených operací, kdy musí být prokazatelné, jaká osoba danou činnost (operaci) provedla, a v neposlední řadě legislativní, viz dále.

2.3 Implementace IAM systému

Aby bylo možné systém IAM implementovat, musí být však splněny některé předpoklady. Jednou z hlavních podmínek je zapojení konkrétních aktiv do systému IDM a také zavedení jednotného přihlašování pomocí SSO (Autentizační platformy). Tento projekt, tzn. úpravy jednotlivých systémů, již v FS probíhají a postupně jsou systémy upravovány tak, aby splňovaly požadavky na standardní ověřování – autentizaci. Hlavní podmínkou pro zapojení aktiv je však stav připravenosti a použitých technologií jednotlivých systémů pro napojení do systému IAM.

Jednotlivé systémy lze z pohledu připravenosti a použitých technologií rozdělit do několika kategorií:

- Systémy, které splňují technologické požadavky a jsou po stránce strukturální a technické připraveny k napojení na systém IAM. Tyto systémy jsou zařazeny do první sady systémů, které budou napojeny v první vlně nasazení systému IAM.
- Systémy, které splňují technologické požadavky a jsou po stránce strukturální připraveny k napojení na systém IAM, ale po stránce technické je nelze připojit. Tyto systémy bude nutné nejdříve upravit tak, aby bylo možné systém IAM napojit.
- Systémy, které splňují technologické požadavky a nejsou po stránce strukturální připraveny k napojení na systém IAM a po stránce technické je nelze připojit. Tyto systémy bude nutné nejdříve upravit tak, aby jejich struktura vyhovovala standardním bezpečnostním požadavkům a aby je bylo možné na systém IAM napojit.
- Systémy, které nesplňují technologické ani strukturální požadavky a nelze je žádným způsobem napojit na systém IAM. Jedná se o staré systémy, kde jejich stáří v některých případech přesahuje 20 let a u těchto systémů bude muset před napojením do systému IAM předcházet analýza s následným vývojem a přechodem na nejnovější technologie a standardy tak, aby i tyto systémy bylo možné do IAM napojit.

3 POPIS STÁVAJÍCÍHO IAM

Na základě průzkumu trhu a následné veřejné zakázky byl na Finanční správě nasazen nástroj IDM midPoint od slovenského výrobce Evolveum s.r.o.
K rozhodnutí o pokračování s řešením midPoint došlo na základě posouzení vhodnosti pro nasazení ve Finanční správě. Rozhodnutí ovlivnila otevřenost systému, stabilita a další aspekty, jako vybudovaná partnerská síť, a to nejen v České republice.
V rámci nasazení midPointu byly postupně realizovány toto kroky:

- Systém byl nainstalován v prostředí finanční správy.
- Implementace jednotného přihlašování pomocí SSO (Single Sign on) do IDM midPoint pomocí Kerberos.
- Připojení zdrojových databází (Uživatelé, Útvary a Činnosti).
- Konfigurace schvalovacích procesů (role Vedoucí, Koordinátor, Schvalovatel a další).
- Návrh a implementace notifikací prostřednictvím emailů (schvalovatel/operátor).
- Design autorizací (7 autorizačních rolí s různou úrovní oprávnění v IDM).
- Návrh a implementace reportů (činnosti indukující B2B, VEMA report přiřazení atd.).
- Školení administrátorů.
- Integrace na informační systémy, kde IDM řídí oprávnění identit jedním z možných způsobů připojení – podrobnosti o napojených systémech viz kapitola k architektuře.

Po realizaci uvedených kroků IDM umožňuje centralizovanou správu uživatelů v napojených informačních systémech. Jeho zavedením se zrychlily procesy spojené s přidělováním či odebíráním oprávnění, zjednodušila se správa velkého množství rolí, zvýšila se bezpečnost z pohledu přístupů uživatelů k informačním zdrojům.
Pro běžného zaměstnance poskytuje systém IDM na jednom místě informace o jeho aktuálním organizačním zařazení, o přiřazených činnostech z OSIRIS a přidělených rolích v aplikacích, které již IDM podporuje, tedy na které je již zrealizovaná integrace.
Pro vedoucí pracovníky IDM systém nabízí uživatelskou samoobsluhu, ve které mohou žádat o nové role pro své podřízené. Dále mohou v systému IDM kontrolovat na ně směřované úkoly nebo třeba sledovat, kde se ve schvalovacím procesu nachází jejich požadavek. Také mají přehled o přiřazených rolích svých podřízených zaměstnanců.

AM část řešení zajišťující primárně SSO zatím v prostředí FS není nasazena a bude realizována v rámci implementace nového IAM řešení.

3.1 Architektura nasazeného řešení IDM – midpoint (AS-IS stav)

3.1.1 Technologické uzly

Testovací prostředí a vývojové prostředí (2 servery):

Aplikační server:

Název	Parametry
Platforma	Virtuál na platformě VM Ware
Operační systém	Windows
CPU	8 jader
RAM	32 GB
Disk	200 GB

DB server:

Název	Parametry
Platforma	Virtuál na platformě VM Ware
Operační systém	Windows - SQLEXPRESS
CPU	Sdíleno s aplikačním serverem (běží na stejném stroji)
RAM	Sdíleno s aplikačním serverem (běží na stejném stroji)
Disk	Sdíleno s aplikačním serverem (běží na stejném stroji)

Produkční prostředí:

Aplikační server:

Název	Parametry
Platforma	Virtuál na platformě VM Ware
Operační systém	Windows
CPU	8 jader
RAM	32 GB
Disk	200 GB

DB server:

Název	Parametry
Platforma	Virtuál na platformě VM Ware
Operační systém	Windows - SQL server 2012
CPU	8 jader
RAM	32 GB
Disk	200 GB

3.1.2 Připojené koncové systémy

Koncové systémy musí být schopny předávat informace o oprávněních identit v daném systému do IDM a přebírat definovaná oprávnění identit z IDM. Systém IDM musí podporovat všechny protokoly vzájemné komunikace, které jsou vyžadovány koncovými systémy.

3.1.3 Způsoby připojení koncových systémů

3.1.3.1 Automatické připojení koncového systému

- IDM automaticky skrze konektory provádí akce spojené se správou autorizace v koncových systémech.
- IDM automaticky skrze konektory provádí pravidelnou kontrolu stavu účtů na koncových systémech s vypořádáním nesouladu.
- Preferovaný způsob připojení.

3.1.3.2 Read-only připojení koncového systému

- IDM neprovádí automaticky správu autorizace v koncových systémech, ale pomocí notifikace informuje administrátory koncových systémů o přidělení úkolu.
- IDM automaticky skrze konektory provádí pravidelnou kontrolu stavu účtů na koncových systémech s autoritativním vypořádáním nesouladu a eskalací bezpečnostního incidentu skrze notifikace operátorovi.

3.1.3.3 Semi-manual připojení koncového systému

- IDM neprovádí automaticky správu autorizace v koncových systémech, ale pomocí notifikace informuje administrátory koncových systémů o přidělení úkolu.
- IDM pomocí webového rozhraní a v rámci workflow procesu požaduje po administrátorovi koncového systému potvrzení splnění přiděleného úkolu.
- Přidělování rolí (přístupu do koncového systému) je řízeno na základě žádostí přes IDM.
- IDM provádí pravidelnou kontrolu stavu účtů na koncovém systému, který porovnává se stavem stínových účtů (objekt reprezentující účet na koncovém systému) v IDM. Pokud se stavy liší, požaduje po administrátorovi narovnání stavu.
- IDM nemá přímý přístup do koncového systému, nýbrž stav účtů ověřuje vůči exportu z koncového systému. Samotný export je realizován mimo IDM.

3.1.3.4 Offline připojení koncového systému

- IDM neprovádí automaticky správu autorizace v koncových systémech, ale pomocí notifikace informuje administrátory koncových systémů o přidělení úkolu.
- IDM pomocí webového rozhraní a v rámci workflow procesu požaduje po administrátorovi koncového systému potvrzení splnění přiděleného úkolu.
- Přidělování rolí (přístupu do koncového systému) je řízeno na základě žádostí přes IDM.

3.1.4 Napojené aplikace

3.1.4.1 Tabulka napojených aplikací

Název zdroje	**Doplnění informací**
APED	Evidence přístupů aplikace pro elektronické dražby
APEX	Evidence přístupů aplikace pro evidenci přístupů (podpora exekucí)
APEX2	Evidence přístupů aplikace pro evidenci přístupů nová verze (podpora exekucí)
Autoprovoz	Evidence přístupů aplikace pro rezervační systém vozidel
B2B	Správa přístupů v rámci dotazů do České správy sociálního zabezpečení
Centrální evidence exekucí	Evidence přístupů do centrální evidence exekucí
ČÚZK	Evidence přístupů do katastrálních map
eDoklady Párovací kód	Evidence udělení párovacích kódů
EPAD	Aplikace pro evidenci úroků hrazených správcem daně
Georeporty ochrany přírody	Evidence přístupů do lesních map
JIP/KAAS eDoklady	Aplikace pro správu účtů v rámci ověření totožnosti poplatníka (elektronická občanka)
LPIS	Evidence přístupů využití půdy
MISYS	Evidence přístupů do Geografické rozhraní pro zobrazení katastrálních map
NK	Evidence přístupů do Notářské komory pro Seznam listin
PAPR	Aplikace pro Správce dražeb, Veřejné vyhlášky, Volná místa a Správa úředních desek
PIS VEMA	Evidence přístupů do Personální systém
Šeky	Evidence přístupů do aplikace přijatých šeků
ÚSKS	Evidence přístupů Uložiště souborů a klíčových slov
Věstník veřejných zakázek	Evidence přístupů do Věstníku veřejných zakázek
Watchdog	Aplikace pro správu přístupů v rámci kontrolní činnosti

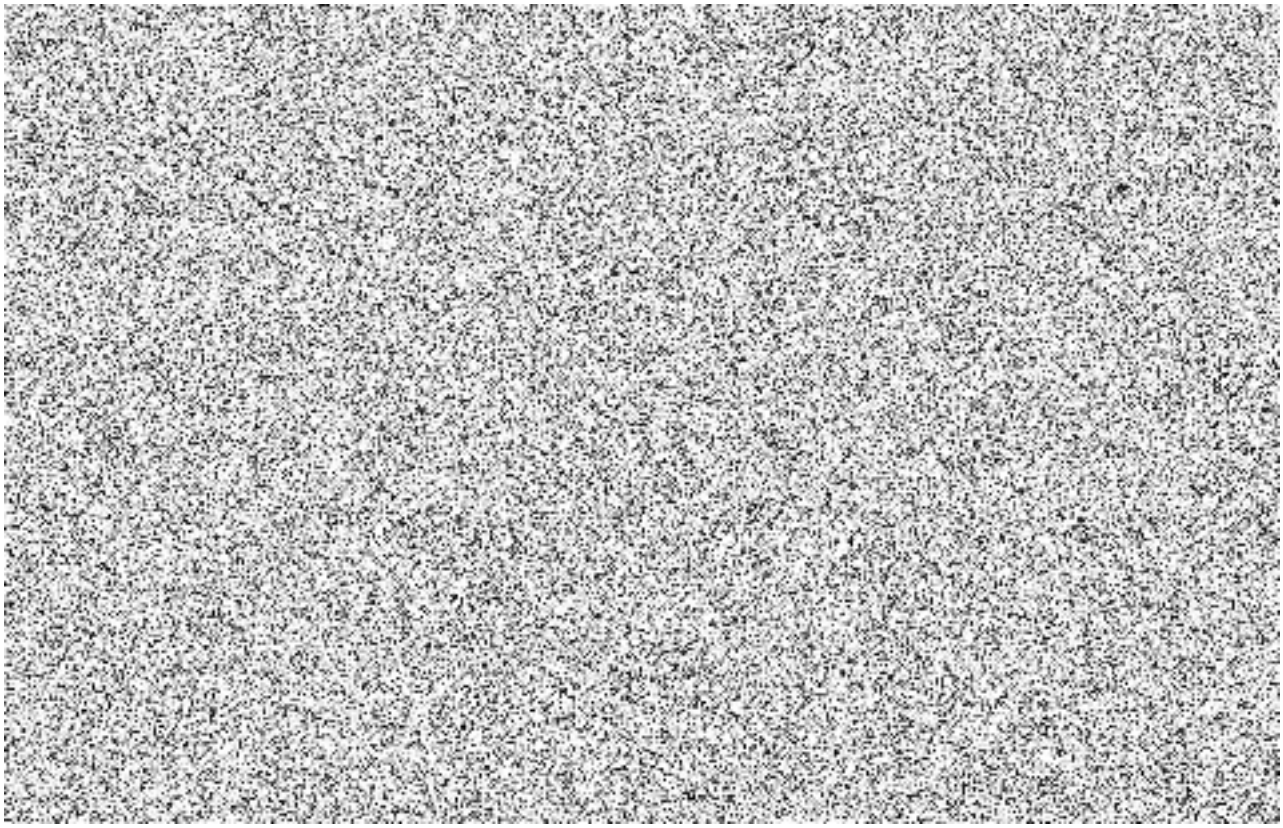
4 POŽADAVKY NA IDM

Požadavky v této kapitole jsou společné pro obě instance IDM, tedy interní i externí IAM. Kapitola 7 Požadavky na funkcionality externího IAM jako Service Providera je pak poplatná pouze pro externí IDM.

Požadavkem Zadavatele je využít stávající řešení IDM a rozvinout jej s ohledem na požadavky v tomto dokumentu uvedené a vytvořit tak robustní řešení IDM, postavené na technologii IDM midPoint. Důvodem tohoto rozhodnutí jsou již vynaložené stávající prostředky; nabitá znalost stávající technologie pracovníky Zadavatele; již vybudované řešení na technologii IDM midPoint, které bude dále využívané a zhodnocované v rámci IDM.

Zadavatel zejména požaduje naplnění následujících cílů:

1. Nasazení sjednocujícího řešení pro správu identit, uživatelských rolí, oprávnění a přístupů uživatelů, včetně jejich evidence, v prostředí Finanční správy (informační systémy FS).
2. Zefektivnění a automatizace procesů řízení identit v organizaci a zavedení centrální platformy pro řízení identit v organizaci – IDM.
3. Zavedení samoobslužných procesů pro zadávání žádostí o oprávnění a přístupů samostatnými koncovými uživateli organizace.
4. Standardizace a zajištění procesů schvalování a změny nastavení identit, včetně jejich automatizovaného předání (publikace) do připojených systémů (integrovaných aplikací).
5. Konsolidace a standardizace procesů souvisejících s personálními obměnami v organizaci (nový zaměstnanec, odchod zaměstnance, zařazení zaměstnance na pozici, změna pozice zaměstnance a další) a zajištění všech funkcionalit v souvislosti s vývojem jejich identity (zejména nabývání a ztráta oprávnění do vybraných aplikací a informačních systémů).



Obrázek 1 – Struktura požadavků na IAM

Hlavními cíli implementace systému IDM tak jsou:

- Analýza interních a externích subjektů, resp. přístupových oprávnění subjektů.
- Analýza životního cyklu identit v organizaci.
- Implementace systémového nástroje pro řízení životního cyklu identit, řízení a kontroly přístupů k jednotlivým aktivům, rekonciliace a reportování.
- Napojení zdroje identit (HR) na systém IDM.
- Definice základních business rolí určujících přístupová práva k vybraným informačním systémům.
- Definice workflow schvalovacích procesů, určující jednoznačnou zodpovědnost za konkrétní přístupová oprávnění.
- Postupné napojení informačních systémů na IDM.
- Řešení musí kromě online řízení oprávnění a identit do připojených aplikací podporovat i tzv. offline řízení oprávnění a identit na základě manuálního potvrzení akce odpovědnou osobou nebo na základě informací získaných z exportu dat aplikace.

Obecný popis přínosů po zavedení IDM:

- Nepopiratelná odpovědnost – jednoznačná identifikace uživatele oproti identitě.
- Správa přístupů a oprávnění do všech prostředků zadavatele (IS, koncové systémy, systémy atd.).
- Správa identit a uživatelů přistupujících k systémům a prostředkům Zadavatele.
- Správa přidělování oprávnění uživatelům.
- Evidence všech rolí oprávnění (aplikačních rolí) všech koncových systémů a identit, jejich uživatelů včetně přidělených oprávnění.
- Omezení vlivu lidského faktoru a automatizace procesů spojených s nástupy, změnami pozic a výstupy zaměstnanců a externích pracovníků.
- Zavedení schvalovacích procesů do řízení života identit, přidělování oprávnění i samotného zavádění do koncových systémů.
- Naplnění podmínky zákona o kybernetické bezpečnosti.
- Centralizace správy uživatelů napříč IT systémy.
- Úspora práce administrátorů zvýšením automatizace.
- Reporting aktuálního stavu uživatelských účtů a zpětný audit.
- Časově omezené přidělování přístupů a ukončování uživatelů.
- Zavedení business rolí ve vazbě na procesní analýzu.
- Omezení chyb na vstupu informací o uživatelích.
- Eliminace manuálních zásahů a s nimi spojených chyb obsluhy s výjimkou procesně definovaných manuálních operací.
- Automatizované řízení přidělování oprávnění od schválení až po zavedení do koncového systému.
- Logování a monitorování veškerých změn oprávnění, včetně exportu logů mimo dosah administrátorů IDM.
- Nastavení parametrů na kvalitu hesla a vynucení kontroly kvality hesla.

4.1 Systémové požadavky

- Podpora operačního systému Windows nebo Unix/Linux.
- Jediné úložiště dat (repository), a to relační databázi PostgreSQL.
- Podpora přístupu pomocí zabezpečeného protokolu HTTPS s podporou technologie RSA a ECC.
- Podpora kódování Unicode.
- Podpora Single Sign On s možností konfigurace využívaného protokolu.
- Schopnost pracovat v režimu vysoké dostupnosti za pomoci více uzlů IDM (např. automatické spuštění úlohy na dostupném uzlu IDM).
- Možnost volat jakoukoliv datovou operaci, která je dosažitelná z webového rozhraní pomocí API (např. založení uživatele, tvorba rolí, správa organizační struktury apod.).
- Podpora rozvoje pomocí skriptovacích jazyků.
- Export/Import konfigurace IDM nástroje v otevřeném datovém formátu.

4.2 Technické požadavky funkční a nefunkční

Instrukce pro vyplnění tabulek požadavků

Instrukce pro vyplnění níže uvedených tabulek od bodu 4.2 Technické požadavky funkční a nefunkční, kde je zapotřebí vyplnit řádek s uvedeným textem [BUDE DOPLNĚNO] sloupec „Způsob naplnění“. Níže uvádíme ilustrační příklady.

Způsob naplnění požadavku musí jasně vyjadřovat, že je požadavek naplněn kompletně. Dále dodavatel stručně popíše, jak je požadavek naplněn a doplní i podstatné technické detaily. Není přípustná odpověď pouze „ano“ nebo „ne“.

Ilustrační příklady ukazují, jak může být tabulka vyplněna:

Požadavek:
Systém MUSÍ poskytovat zabezpečené programové rozhraní (API) přístupné pouze autentizovaným uživatelům.

Způsob naplnění:
Systém poskytuje REST API dostupné pomocí protokolu HTTPS, který zajišťuje zabezpečení komunikace. Autentizace uživatelů je podporována pomocí protokolů OAuth2 nebo HTTP basic auth. Dále pouze uživatelé autorizovaní v konfiguraci mají právo používat části API pro které byli autorizováni.

Požadavek:
Webové rozhraní systému MUSÍ podporovat možnost importu uživatelů z CSV souboru.

Způsob naplnění:
Integrace systémů A a B pomocí protokolu telnet je možná, ovšem není dostatečně zabezpečená. Proto doporučujeme provést integraci protokolem SSH, který zajistí totožnou funkcionalitu, ale zvýší bezpečnost řešení.

ID	Požadavek	Způsob naplnění
0	IDM MUSÍ odpovídat ustanovením platných právních předpisů, které zahrnují zejména: - Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění pozdějších předpisů, - Vyhlášku č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti), - Zákon č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů, ve znění pozdějších předpisů, - Vyhlášku NBÚ a Ministerstva vnitra ČR č. 317/2014 Sb., významných informačních systémech a jejich určujících kritérií, ve znění pozdějších předpisů, - Zákon č. 499/2004 Sb., o archivnictví a spisové službě a o změně některých zákonů, ve znění pozdějších předpisů, - Zákon č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce, ve znění pozdějších předpisů, - Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o	Požadavek je naplněn kompletně. midPoint umožňuje vytvářet a uchovávat detailní auditní záznamy o správě identit, změnách oprávnění i schvalovacích procesech, v souladu se zákonem č. 181/2014 Sb. a vyhláškou č. 82/2018 Sb. Řešení je připraveno na nasazení v prostředí významných informačních systémů dle vyhlášky č. 317/2014 Sb. Umožňuje řízení životního cyklu osobních údajů včetně nastavení retenčních politik, pseudonymizace a transparentního přístupu, v souladu s nařízením GDPR. Podporuje správu elektronických identit a elektronickou identifikaci v souladu s nařízením eIDAS a zákonem č. 250/2017 Sb. Systém umožňuje integraci s archivačními nástroji nebo likvidaci dat dle zákona č. 499/2004 Sb. midPoint lze provozovat v souladu s požadavky zákona č. 365/2000 Sb., zákona o právu na digitální služby č. 12/2020 Sb. a zákona o službách vytvářejících důvěru č. 297/2016 Sb. Veškeré řízení přístupů lze nastavit podle interních bezpečnostních politik tak, aby byla zajištěna odpovědnost, transparentnost a minimalizace rizik.

ID	Požadavek	Způsob naplnění
	ochraně osobních údajů), - Zákon č. 250/2017 Sb., o elektronické identifikaci, ve znění pozdějších předpisů, - Zákon č. 12/2020 Sb., o právu na digitální služby, ve znění pozdějších předpisů, - Nařízení eIDAS a navazující předpisy.	

Tabulka 3 – Požadavky legislativy

4.2.1 Obecné požadavky na uživatelské rozhraní v IAM

Nabízené řešení musí splňovat následující požadavky:

- Kompletní lokalizace do českého jazyka v uživatelské úrovni, administrační prostředí je povoleno i v jazyce anglickém;
- Webové rozhraní pro administrátory i pro koncové uživatele;
- Vyhledávání libovolného obsahu v agendách podle libovolného atributu;
- Možnost grafického přizpůsobení korporátní identitě (rozhraní je možné upravovat dle potřeb Zadavatele).
- Responsivní design. Předpokládané rozlišení zobrazovacích zařízení je 1280 x 768 a vyšší.

ID	Požadavek	Způsob naplnění
0	IDM MUSÍ být do budoucna rozšiřitelné tak, aby se stalo centrální komponentou FS pro správu identit a přístupů celé FS.	Požadavek je naplněn kompletně. Řešení postavené na platformě midPoint je modulární a škálovatelné, což umožňuje jeho budoucí rozšíření na úroveň centrálního IDM systému pro celou FS. midPoint podporuje připojování dalších systémů pomocí standardních konektorů (LDAP, AD, REST, SCIM, SQL, CSV), řízení životního cyklu identit a jednotnou správu rolí a oprávnění. Lze jej provozovat ve více prostředích a rozšiřovat dle organizační struktury FS.
0	IDM MUSÍ zajistit centrální správu identity, uživatelských rolí	Požadavek je naplněn kompletně.

ID	Požadavek	Způsob naplnění
	a případně i oprávnění uživatelů v aplikacích a informačních systémech, u kterých bude provedena integrace na IDM.	Uživatelé, role a oprávnění jsou spravovány z jednoho místa, přičemž lze nastavovat přidělování práv na základě organizační struktury, atributů uživatele nebo definovaných pravidel. Systém podporuje jednotlivé modely řízení přístupů Podporuje delegaci, automatizované přidělování/odebírání oprávnění, schvalovací workflow. Oprávnění mohou být distribuována do cílových systémů dle transformačních pravidel a pomocí konektorů.
0	IDM MUSÍ umožnit automatizovaně spravovat identity (osoby, uživatelské role a oprávnění) ve všech systémech organizace, a to zejména v návaznosti na personální systém a adresářové služby.	Požadavek je naplněn kompletně. Integrace s personálním systémem probíhá typicky prostřednictvím CSV, databázového připojení nebo webových služeb, přičemž adresářové služby jako Active Directory či LDAP, jsou podporovány nativními konektory.
0	IDM MUSÍ spravovat a řídit identity (uživatele, jejich uživatelské účty a oprávnění) v rámci připojených systémů. Pro unifikovanou správu identit v systémech organizace je nutné vybudování jednotné centrální evidence uživatelů, uživatelských účtů a oprávnění uživatelů k integrovaným aplikacím. Tato evidence bude spravována centrálně v systému IDM.	Požadavek je naplněn kompletně. Každá identita v systému je spravována jako jednotný objekt, ke kterému jsou přiřazeny role a účty v jednotlivých aplikacích. midPoint zajišťuje řízený životní cyklus identit, včetně vytvoření, změny, pozastavení nebo zrušení účtu v cílových systémech. Tato jednotná správa umožňuje konsolidaci uživatelských údajů a efektivní kontrolu nad přístupovými právy, včetně napojení na schvalovací a auditní procesy. Veškerá data jsou uložena a spravována centrálně v systému IDM.
0	Na základě procesů správy personálních agend ze zdrojových systémů (personální systém) MUSÍ IDM podporovat automatizovaný vstup údajů o osobách, uživatelských účtech, zařazení v organizační struktuře, přiřazení pracovního místa, přiřazení do skupin atd.	Požadavek je naplněn kompletně. Řešení využívající platformu midPoint podporuje plně automatizovaný příjem a zpracování údajů z personálních systémů, které slouží jako primární zdroj identity. Systém umožňuje načítat data o osobách, jejich pracovním zařazení, organizační struktuře, pozicích i členství ve skupinách prostřednictvím rozhraní. Na základě těchto dat lze automaticky zakládat uživatelské účty, přiřazovat role a nastavovat oprávnění v připojených systémech. midPoint

ID	Požadavek	Způsob naplnění
		umožňuje dynamické řízení přístupů podle atributů z personálních systémů (např. typ pracovního poměru, útvar, funkce).
0	Součástí nasazení řešení bude i nastavení systemizovaných pracovních míst, jim odpovídajícím uživatelským rolím a dále skupin takových míst/uživatelských rolí. IDM MUSÍ umožnit správu, resp. načtení hierarchické struktury systemizovaných míst ve struktuře organizace zadavatele včetně správy příslušných rolí a oprávnění, přiřazených systemizovaným místům (hlavním systémem pro správu systemizovaných míst nicméně zůstane stávající personální systém.)	Požadavek je naplněn kompletně. midPoint umožňuje načítání a zpracování systemizovaných pracovních míst z externího personálního systému, který zůstává jejich primárním správcem. Tato místa lze v IDM reprezentovat jako organizační jednotky, pracovní pozice nebo role a následně k nim přiřadit konkrétní oprávnění a přístupové politiky. Systém podporuje hierarchickou strukturu organizace a umožňuje automatické mapování rolí dle zařazení uživatele na konkrétní systemizované místo.
0	Systém IDM MUSÍ reflektovat veškeré potřebné změny související s životním cyklem identity v prostředí zadavatele a ve vazbě na všechny na IDM napojené informační systémy, ve kterých bude mít daná identita uživatelské role a oprávnění. Takové změny budou reflektovány ve všech aktuálně napojených informačních systémech vždy v konkrétní rozhodné době.	Požadavek je naplněn kompletně. Změny vstupující z personálního systému jsou zpracovány na základě definovaných pravidel a reflektovány v připojených systémech automaticky a v požadované rozhodné době. Systém umožňuje plánování změn v čase, zpožděné aktivace/deaktivace účtů a nastavení konkrétních termínů přidělení nebo odebrání oprávnění.
0	Ve vztahu k napojeným systémům MUSÍ IDM zajistit samostatnou a úplnou správu v oblasti identity a uživatelských rolí ve vztahu k těmto systémům, včetně skupin uživatelů a systemizovaných míst. Ze strany zadavatele není rozhodné o kolik politik a konfiguračních operací se na straně informačních systémů jedná, ale je pro něj důležitý výsledek, tedy například správné nastavení uživatelských rolí a zařazení do skupiny. IDM bude autoritativním zdrojem informací o identitách a jejich účtech a přidělených rolích. IDM bude provádět správu	Požadavek je naplněn kompletně. Systém automaticky provádí všechny potřebné operace - bez ohledu na jejich počet nebo specifikum cílového systému - s cílem zajistit správný stav a konzistenci přístupů. Pro každého uživatele spravuje centrálně účty, role i členství ve skupinách na základě dat z personálního systému a interních pravidel. Synchronizace změn probíhá automaticky včetně podpory transformačních pravidel, plánování i schvalování, čímž je zajištěna aktuálnost a správnost údajů ve všech napojených systémech.

ID	Požadavek	Způsob naplnění
	automaticky, tak aby byly spravované systémy vždy aktuální.	
0	IDM MUSÍ být flexibilní v možnostech konfigurace, aby bylo možné ho využít při naplňování nových legislativních požadavků.	Požadavek je naplněn kompletně. Pravidla pro řízení přístupů, životní cyklus identit, audit, souhlasy se zpracováním údajů i retenční politiky lze definovat pomocí konfiguračních schémat a skriptů. Díky této flexibilitě je možné rychle reagovat na nové legislativní požadavky v oblasti ochrany osobních údajů, kybernetické bezpečnosti nebo elektronické identifikace. midPoint také disponuje silnou komunitní a komerční podporou.
0	IDM a jeho funkcionality MUSÍ respektovat standardní architekturu IS v prostředí zadavatele	Požadavek je naplněn kompletně. Řešení podporuje standardní komunikační protokoly, umožňuje provoz v různých infrastrukturách a je kompatibilní s konceptem vícevrstvé architektury. midPoint lze provozovat jako službu v rámci mikroslužebné či centralizované architektury a přizpůsobit bezpečnostním, integračním a provozním standardům organizace.
0	IDM MUSÍ pro svou integraci v maximální míře využít standardizovaná rozhraní a existující prostředky IS.	Požadavek je naplněn kompletně. Systém využívá pro integraci standardizovaná rozhraní a protokoly. Díky tomu lze systém napojit na běžně používané informační systémy bez potřeby vývoje proprietárních konektorů. Integrace probíhá s důrazem na opětovné využití již existujících prostředků a komponent IS Zadavatele, čímž se minimalizují náklady na údržbu i provoz. midPoint rovněž podporuje standardní autentizační mechanismy, což usnadňuje zapojení do stávající infrastruktury.
0	Součástí plnění MUSÍ dále být i navržení metodiky pro správu identit: • Jmenné konvence uživatelských jmen a zajištění jejich unikátnosti (sjednocení loginů), • Mechanismus práce s hesly (přidělení, změna, samoobslužný reset, reset hesla koncového účtu	Požadavek je naplněn kompletně. V rámci plnění bude dodána metodika správy identit plně reflektující požadavky Zadavatele. Tato metodika zahrne návrh jmenných konvencí s důrazem na jednoznačnost a jednotnost loginů, nastavení pravidel pro přidělování a změnu hesel včetně samoobslužného resetu i možnosti správy hesel administrátorem. Dále bude

ID	Požadavek	Způsob naplnění
	administrátorem, ...), • Postupy správy uživatelů (zavádění, změny, rušení, nastavování oprávnění...), • Návrh členění objektů v rámci IDM (osoby, účty, funkce, organizační jednotky, skupiny...), • Definice bezpečnostních zásad a pravidel pro práci s IDM.	obsahovat detailní popis životního cyklu uživatelů (zavedení, změna, zrušení, schvalování přístupů), návrh logického členění objektů v systému (osoby, účty, role, organizací, skupiny) a bezpečnostní zásady pro provoz IDM. Metodika bude připravena ve spolupráci se Zadavatelem s cílem zajištění souladu s jeho prostředím, procesy a bezpečnostními politikami.

Tabulka 4 – Základní požadavky

ID	Požadavek	Způsob naplnění
0	IDM MUSÍ udržovat a spravovat kompletní životní cyklus identity. Tedy v typickém případě příchod zaměstnance, jeho založení, přidělení rolí v informačních systémech dle jeho organizačního zařazení (systemizovaného místa), změna rolí v případě jeho povýšení nebo změny jeho zařazení, odchod zaměstnance spočívající v deaktivaci jeho identity. Systém MUSÍ zajistit změny na základě informací z personálních systémů, ručního zadání, informací zadaných manuálně přes webové rozhraní nebo z autoritativních zdrojů identit. Minimálně se jedná o následující procesy: • Vznik nové identity, • Úprava identity, • Úpravy popisných atributů, např. jméno, • Úpravy organizačního zařazení, • Změny platnosti, • Přiřazení rolí – oprávnění (automatické i manuální se schvalovacím WF), • Automatická změna rolí na základě změny stavu / typu identity, případně jiného příznaku identity, • Změna evidenčního stavu identity, • Recertifikaci oprávnění, • Aktivace/deaktivace (ruční, automatická), • Archivace identity.	Požadavek je naplněn kompletně. midPoint plně pokrývá správu životního cyklu identity od jejího vzniku až po archivaci. Na základě dat z personálního systému nebo jiných autoritativních zdrojů provádí automatizovaně založení identity, přiřazení účtů a oprávnění podle systemizovaného místa a organizačního zařazení. Při změně stavu identity (např. povýšení, přechod na jinou pozici) systém aktualizuje role, zařazení a případná oprávnění. midPoint podporuje ruční úpravy přes webové rozhraní i automatizované reakce na změnu atributů, datumu platnosti nebo příznaků identity.
0	Pro architektonické řešení IDM preferuje zadavatel udržovat identity, skupiny identit a organizační struktury ve své vnitřní databázi, kde identity ve vnitřní databázi budou sloužit jako	Požadavek je naplněn kompletně. Řešení udržuje identity, skupiny i organizační strukturu ve své vnitřní databázi a plní tak roli centrálního a referenčního systému identit. Veškeré změny jsou evidovány a zpracovávány uvnitř IDM, odkud

ID	Požadavek	Způsob naplnění
	referenční identity pro ostatní informační systémy.	jsou následně distribuovány do napojených informačních systémů prostřednictvím konektorů a synchronizačních mechanismů. Tento přístup umožňuje udržet jednotný a aktuální stav dat, zamezit nekonzistencím a plně respektuje preferovanou architekturu Zadavatele.
0	IDM MUSÍ implementovat princip založený na systemizovaných místech. IDM MUSÍ umožnit systemizaci pracovních míst v souladu se strukturou organizace, udržovat jednotlivá systemizovaná místa a sadu oprávnění a rolí pro jednotlivé informační systémy organizace vztažené ke konkrétnímu systemizovanému místu.	Požadavek je naplněn kompletně. midPoint umožňuje reprezentaci systemizovaných pracovních míst jako specifických entit v organizační struktuře a jejich propojení s konkrétními sadami rolí a oprávnění. Každému systemizovanému místu lze přiřadit odpovídající oprávnění pro jednotlivé informační systémy, přičemž přidělení těchto práv konkrétním uživatelům probíhá automatizovaně na základě jejich pracovního zařazení. Organizační struktura včetně systemizovaných míst je spravována v rámci IDM nebo synchronizována z personálního systému, přičemž změny v těchto strukturách se automaticky promítají do přístupových práv.
0	IDM MUSÍ umožnit přiřazení identit na takto vytvořená systemizovaná místa a to i ve vazbě M:N. Identita tedy může být v systému IDM evidována na více systemizovaných místech a současně na systemizovaném místě může být evidováno více identit.	Požadavek je naplněn kompletně. Každé systemizované místo může být obsazeno více identitami a zároveň jedna identita může být přiřazena k více systemizovaným místům, například v případě souběhu rolí, zástupů nebo kombinace pracovních pozic. K jednotlivým vazbám lze definovat specifické časové platnosti, role i přístupová oprávnění.
0	IDM MUSÍ umožňovat přidělení oprávnění nebo role konkrétní identitě, systemizovanému místu, skupině nebo organizační jednotce.	Požadavek je naplněn kompletně. Systém umožňuje přiřazování rolí a oprávnění na více úrovních – konkrétní identitě, systemizovanému místu, skupině i organizační jednotce. Přístupová práva mohou být definována jako přímá (např. konkrétnímu uživateli) nebo odvozená (např. na základě příslušnosti k organizační jednotce nebo systemizovanému místu).
0	IDM MUSÍ umožnit správu uživatelských rolí, včetně zařazení	Požadavek je naplněn kompletně.

ID	Požadavek	Způsob naplnění
	uživatele do odpovídající role.	midPoint poskytuje plnohodnotnou správu uživatelských rolí včetně jejich definice, hierarchie, přiřazení a odebrání. Role mohou být přiřazeny ručně, automaticky na základě pravidel (např. organizační struktura, pozice, atributy identity) nebo schvalovacím workflow. Uživatel může být zařazen do více rolí současně, přičemž každá z nich může nést specifická oprávnění pro různé informační systémy.
0	V IDM MUSÍ být možné aplikační role nastavovat dočasně. Po uplynutí nastaveného intervalu se role automaticky odebere.	Požadavek je naplněn kompletně. Systém umožňuje přiřazování rolí s definovanou dobou platnosti, a to jak v rámci konkrétního časového intervalu, tak na základě počátečního a koncového data. Po uplynutí tohoto období je role automaticky systémem odebrána bez nutnosti ručního zásahu.
0	IDM MUSÍ umožnit integraci aplikací a import rolí přes webové služby do IDM.	Požadavek je naplněn kompletně. midPoint podporuje integraci aplikací a systémů prostřednictvím webové služby REST. Umožňuje import aplikačních rolí do IDM buď automatizovaně, nebo na základě definovaného rozhraní. Tuto integraci lze provádět i obousměrně.
0	IDM MUSÍ umožnit nastavení schvalovacího workflow (při přidělení práva, role atd.), včetně emailových notifikací a potvrzování.	Požadavek je naplněn kompletně. midPoint obsahuje integrovaný modul pro definici schvalovacích workflow, který umožňuje řídit procesy přidělování rolí, oprávnění i dalších změn v identitách. Schvalovací procesy lze nastavit jedno i víceúrovňově, včetně možnosti eskalací. Součástí je systém notifikací s podporou odesílání e-mailových zpráv žadatelům i schvalovatelům a možností potvrzení nebo zamítnutí přes webové rozhraní IDM. Workflow lze upravit dle organizační struktury, typu požadované role i dalších parametrů.
0	IDM MUSÍ umožnit definovat vztahy zastupitelnosti mezi uživateli – musí umožnit uživatelům, aby v souladu se strukturou organizace mohli delegovat v případě potřeby	Požadavek je naplněn kompletně. midPoint podporuje dočasnou delegaci oprávnění mezi uživateli v rámci definovaných pravidel a organizační struktury. Každý uživatel může delegovat své role na jinou osobu s předem určeným časovým

ID	Požadavek	Způsob naplnění
	(nemoc, dovolená atd.) svoje role na jiné pověřené osoby. Delegace oprávnění bude dočasná, kdy se po nastaveném intervalu, nastavená delegace automaticky v IDM zruší.	omezením. Po uplynutí tohoto intervalu systém delegaci automaticky ukončí. Delegace může být nastavena administrátorem nebo uživatelem (např. při plánované nepřítomnosti) a je plně auditovatelná.
0	IDM MUSÍ umožnit dodatečné přidávání vlastních atributů k identitám.	Požadavek je naplněn kompletně. Systém umožňuje plně konfigurovatelnou správu datového modelu identity, včetně možnosti definice a správy vlastních atributů pomocí definice schémy v XLS formátu. Vlastní atributy lze rovněž zobrazovat ve formulářích, zahrnout do auditních záznamů či exportovat do připojených systémů.
0	IDM MUSÍ umožňovat přesun identity v rámci organizační struktury i mezi jednotlivými organizačními strukturami.	Požadavek je naplněn kompletně. Při změně zařazení identity systém automaticky aktualizuje její přiřazení k rolím, oprávněním a účtům dle nové pozice v hierarchii. Přesuny mohou být iniciovány ručně, nebo na základě změn importovaných z personálního systému.
0	IDM MUSÍ umět detekovat situaci, kdy se ve zdrojovém systému vyskytne nový uživatel, který již dříve byl v IDM založen, a přiřadit jej k existující identitě.	Požadavek je naplněn kompletně. midPoint disponuje pokročilým mechanismem korelace identit, který umožňuje detekovat shody mezi novými záznamy ze zdrojových systémů a již existujícími identitami v IDM. Pomocí konfigurovatelných korelačních pravidel (např. dle rodného čísla, e-mailu, uživatelského jména nebo jiných atributů) systém automaticky rozpozná, že se jedná o tutéž fyzickou osobu, a nepřiděluje duplicitní identitu.
0	IDM MUSÍ obsahovat funkcionalitu kopírování veškerého nastavení oprávnění jednoho uživatele na druhého.	Požadavek je naplněn kompletně. midPoint umožňuje kopírování oprávnění a rolí z jedné identity na druhou a to včetně přiřazených systémových účtů a souvisejících přístupových práv. Tato funkcionalita je dostupná v administračním rozhraní. Před zapsáním změn může být tento proces podroben schválení.

ID	Požadavek	Způsob naplnění
0	Veškeré požadavky, které provedou uživatelé na IDM, musí být logovány tak, aby bylo možné zpětně prokázat kdo, kdy a co změnil v IDM identitách, referenčních objektech, ale i v administraci. Záznam v historii musí obsahovat původní i novou hodnotu.	Požadavek je naplněn kompletně. midPoint obsahuje integrovaný auditní modul, který zaznamenává veškeré změny provedené uživateli, administrátory i automatickými procesy. Každý auditní záznam obsahuje časovou značku, identifikaci subjektu, který změnu provedl, a podrobnosti o změně – včetně původní a nové hodnoty dotčených atributů. Auditní data jsou uložena v centrálním repozitáři a je možné je vyhledávat, filtrovat i exportovat.
0	IDM MUSÍ umožnit autonomní správu hesel (samoobsluha).	Požadavek je naplněn kompletně. Systém poskytuje uživatelům samoobslužné rozhraní pro správu hesel, které zahrnuje změnu hesla a reset zapomenutého hesla. Může být doplněn o schvalovací workflow, nastavení politik složitosti hesel a možnost distribuce změněného hesla do více cílových systémů současně.
0	IDM MUSÍ podporovat bezpečnostní politiky pro nastavení politiky hesel – tj. minimální délka, složitost, maximální platnost.	Požadavek je naplněn kompletně. midPoint umožňuje detailní nastavení politiky hesel v souladu s požadavky bezpečnostních standardů organizace. Podporuje definici minimální délky, požadované složitosti (kombinace znakových sad), maximální platnosti hesla, historii hesel a definice podmínke pro zamykání účtů.
0	IDM MUSÍ podporovat i tzv. technické, systémové či servisní účty, pro které platí speciální pravidla: • Nelze na ně aplikovat procesy pro běžné personální procesy, • Nezanikají při odchodu (ukončení platnosti, deaktivace identity vlastníka), • Mají speciální režim pro správu hesel (hesla nemají časově omezenou platnost a není vynucována jejich	Požadavek je naplněn kompletně. midPoint umožňuje správu technických, systémových a servisních účtů jako samostatné typy identit s vlastními pravidly chování. Tyto účty nejsou svázány s běžnými personálními procesy a jejich životní cyklus není automaticky ukončován při změnách nebo odchodu vlastníka. Pro tyto účty lze definovat pro správu hesel výjimky z obecných bezpečnostních politik, včetně individuálního nastavení.

ID	Požadavek	Způsob naplnění
	změna po uplynutí daného časového období).	
34	Po přihlášení do IDM MUSÍ být administrátor IDM notifikován, že v systému došlo k některému z chybových stavů (např. synchronizovaný systém ve stavu chyba). Tato notifikace MUSÍ být zřetelná po přihlášení do systému a může být formou (barevného podbarvení části aplikace např. menu, pop-up okna oznamující, že je v IDM nějaký chybový stav, centrální dashboard aplikace apod.). Z notifikace MUSÍ být zřetelné, která část IDM je chybovém stavu.	Požadavek je naplněn kompletně. midPoint umožňuje informovat administrátora o výskytu chybových stavů prostřednictvím centrálního administračního dashboardu, který bude součástí dodaného řešení. Tento dashboard zobrazí aktuální stav systémových komponent, včetně přehledu napojených systémů a jejich synchronizačního stavu. V případě chyby je zajištěna přehledné zvýraznění s jasným označením, které části systému se stav týká.

Tabulka 5 – Požadované funkčnosti IDM

4.2.2 Autoritativní zdroje dat

Nabízené řešení musí být schopno se napojit na autoritativní zdroje dat, které mohou obsahovat:

- Zdroj pro komunity: interní uživatelé, externí uživatelé, zákazníci apod.
- Možnosti napojení: CSV import, LDAP, Active Directory, přímý přístup do DB, webové služby

4.2.3 Active Directory

Nabízené řešení musí být schopno spolupracovat s Active Directory. Mezi základní parametry AD patří:

- Multidoménová a multiforestová struktura
- Možnosti napojení: LDAPS, PowerShell, ADSI, .NET, vše v zabezpečených variantách.

4.2.4 Autorizační model v IDM

- Autorizační model musí být založen na RBAC (Role-Based Access Control) a musí umožňovat nastavit, k jaké části uživatelského rozhraní IDM a k jakým objektům v IDM mají uživatelé přístup až do úrovně atributů.
- Oprávnění k jednotlivým objektům a částem v IDM budou definovány v rolích.

ID	Požadavek	Způsob naplnění
35	IDM MUSÍ nabízet administrační rozhraní (GUI) pro správu rolí.	Požadavek je naplněn kompletně. midPoint poskytuje plnohodnotné webové administrační rozhraní pro správu rolí, které umožňuje jejich vytváření, úpravy, přiřazení uživatelům, definici podmínek platnosti a přiřazených oprávnění. Rozhraní je přehledné, uživatelsky konfigurovatelné a umožňuje i správu hierarchie rolí, delegaci práv a napojení rolí atd.
36	IDM MUSÍ nabízet správu rolí prostřednictvím integrační vrstvy s možností volání funkcí prostřednictvím programového rozhraní (API).	Požadavek je naplněn kompletně. midPoint poskytuje robustní REST API, které umožňuje plnohodnotnou správu rolí včetně jejich vytváření, aktualizace, mazání a přiřazování uživatelům. Prostřednictvím API je možné integrovat externí systémy a aplikace se správou rolí v IDM a automatizovat potřebné operace. Rozhraní podporuje autentizaci, autorizaci i auditovatelnost.
37	IDM MUSÍ umožňovat role hierarchicky skládat do hloubky min. 3 úrovní	Požadavek je naplněn kompletně. midPoint podporuje hierarchické skládání rolí, přičemž umožňuje definovat role v požadované hloubce.
38	IDM MUSÍ umožňovat přiřazení role na organizační jednotku s jejím promítnutím k uživatelům přiřazeným do organizační jednotky.	Požadavek je naplněn kompletně. midPoint umožňuje přiřadit roli přímo organizační jednotce, přičemž tato role je automaticky promítnuta všem uživatelům zařazeným do dané jednotky. Při změně organizačního zařazení uživatele systém automaticky aktualizuje přiřazené role podle nové organizační příslušnosti.
39	IAM MUSÍ umožňovat nastavit vazbu uživatele na roli v	Požadavek je naplněn kompletně.

ID	Požadavek	Způsob naplnění
	kardinalitě M:N. MUSÍ být možné nastavit typ vztahu uživatele k roli (např. vlastník, schvalovatel role) a nastavení platnosti přiřazení role od - do).	Systém plně podporuje vztah typu M:N mezi uživateli a rolemi, kdy jeden uživatel může mít přiřazeno více rolí a jedna role může být přiřazena více uživatelům. Ke každému přiřazení lze nastavit konkrétní typ vztahu (např. vlastník, schvalovatel, držitel) a rovněž omezit platnost přiřazení časovým intervalem (od–do). Tyto informace jsou součástí definice role a lze je využít v rámci schvalovacích procesů, delegací i auditu.
40	IDM MUSÍ umožňovat nastavit vazbu koncových systémů na role v kardinalitě M:N.	Požadavek je naplněn kompletně. midPoint umožňuje definovat vazby mezi rolemi a koncovými systémy v kardinalitě M:N, tedy že jedna role může být napojena na více systémů a zároveň jeden systém může být propojen s více rolemi. Každá role může specifikovat, jaká oprávnění mají být v konkrétním systému přidělena, a to prostřednictvím tzv. přiřazení a indukcí.
41	IDM MUSÍ umožňovat nastavení platnosti přiřazení role od – do a pokud časové období uplyne nebo ještě nenastalo, nesmí být přiřazení role aktivní.	Požadavek je naplněn kompletně. midPoint umožňuje nastavit ke každému přiřazení role konkrétní období platnosti – datum začátku a konce. Role je aktivní pouze v definovaném časovém rozsahu; pokud dané období ještě nenastalo nebo již uplynulo, přiřazení není aktivní a oprávnění se neuplatňují. Tento mechanismus je plně automatizovaný.
42	IDM MUSÍ umožňovat nastavení schvalovacích procesů pro garanty koncových systémů při tvorbě business rolí.	Požadavek je naplněn kompletně. midPoint umožňuje definovat schvalovací procesy při tvorbě a schvalování business rolí, včetně zapojení garantů koncových systémů. Schvalovatelé mohou být přiřazeni na základě konkrétního systému, organizační jednotky nebo jiného atributu a systém podporuje víceúrovňové schvalování.
43	IDM MUSÍ umožňovat správu role vlastníkem bez přiřazeni explicitní autorizace.	Požadavek je naplněn kompletně. midPoint umožňuje nastavit vlastníka role jako oprávněnou osobu pro její správu, aniž by bylo nutné explicitně přiřazovat standardní

ID	Požadavek	Způsob naplnění
		administrátorská oprávnění.
44	IDM MUSÍ umožňovat nastavení role jako vlastníka objektu v koncovém systému (oprávnění, účtu) podobně jako je uživatel vlastníkem účtu. Rekonciliace role pak provede aktualizaci objektu v koncovém systému.	Požadavek je naplněn kompletně. midPoint umožňuje nastavit roli jako vlastníka objektu v cílovém systému, obdobně jako lze přiřadit vlastnictví uživateli. Tato vazba se využívá zejména při správě oprávnění nebo skupin, kdy role zastupuje odpovědnost za konkrétní objekt. V rámci procesu rekonciliace systém vyhodnocuje změny přiřazení rolí a aktualizuje stav objektu v koncovém systému tak, aby odpovídal aktuální konfiguraci a přiřazením v IDM.
45	IDM MUSÍ umožňovat nastaveni pravidel pro vzájemně se vylučující role „Segregation of Duties (SOD)“.	Požadavek je naplněn kompletně. midPoint umožňuje definovat pravidla pro vzájemně se vylučující role (Segregation of Duties – SOD), která zabraňují tomu, aby byly nekompatibilní role přiřazeny jedné identitě současně. Tato pravidla lze uplatnit jak při ručním přiřazování, tak v automatizovaných procesech a schvalovacích workflow. V případě konfliktu systém automaticky zabrání přiřazení.
46	IDM MUSÍ nabízet reporting/notifikace konfliktních práv.	Požadavek je naplněn kompletně. midPoint podporuje detekci a reporting konfliktních oprávnění na základě pravidel Segregation of Duties (SoD). Systém umožňuje generovat přehledy identit, u kterých došlo k přiřazení konfliktních rolí, a poskytuje notifikace odpovědným osobám (např. garantům).
47	IDM MUSÍ umožňovat vyřešení konfliktů SOD ve schvalovacím workflow.	Požadavek je naplněn kompletně. midPoint umožňuje zapojit řešení konfliktů Segregation of Duties (SoD) přímo do schvalovacího workflow. V případě detekce konfliktního přiřazení rolí je možné nastavit proces, který nutí koncového uživatele vybrat sadu rolí tak, aby nebyli v konfliktu.
48	IDM MUSÍ nabízet možnost žádosti o kopii vybraných rolí podle existujícího uživatele a spuštění příslušného schvalovacího	Požadavek je naplněn kompletně. midPoint umožňuje uživateli nebo administrátorovi iniciovat

ID	Požadavek	Způsob naplnění
	workflow jako v případě manuálního přiřazení daných rolí.	žádost o přiřazení rolí podle jiného existujícího uživatele. Vybrané role jsou zkopírovány jako návrh nové žádosti, která následně prochází standardním schvalovacím workflow jako při manuálním přiřazení.
49	IDM MUSÍ umožnit dědičnost vybraných vlastností rolí (např. atributů a typu schvalováni z nadřazené role).	Požadavek je naplněn kompletně. midPoint podporuje hierarchickou strukturu rolí včetně dědičnosti vybraných vlastností z nadřazených rolí. Lze nastavit, aby podřízené role automaticky přebíraly atributy, způsob schvalování, popisy či jiné konfigurační prvky definované v nadřazené roli.

Tabulka 6 – Správa rolí

ID	Požadavek	Způsob naplnění
50	IDM MUSÍ být založeno na principu ,,Role-Based Access Control (RBAC)" a MUSÍ umožňovat nastavit, k jaké části uživatelského rozhraní IDM a k jakým objektům v IDM mají uživatelé přístup, a to až do úrovně atributů entit.	Požadavek je naplněn kompletně. midPoint je postaven na principu Role-Based Access Control (RBAC) a umožňuje detailní řízení přístupu na základě přiřazených rolí. Přístupová oprávnění lze definovat až na úroveň jednotlivých částí uživatelského rozhraní, konkrétních objektů v systému i jednotlivých atributů entit. Tím je zajištěno, že každý uživatel vidí a může spravovat pouze ty informace a funkce, které odpovídají jeho roli a oprávnění.
51	IDM MUSÍ umožnit definovat oprávnění k jednotlivým objektům pomocí rolí.	Požadavek je naplněn kompletně. midPoint umožňuje definovat přístupová oprávnění k jednotlivým objektům systému prostřednictvím přiřazených rolí. Role mohou určovat, jaké akce (čtení, zápis, úprava, mazání) může uživatel provádět nad konkrétními typy objektů (např. identity, účty, organizační jednotky, role, schvalovací žádosti). Oprávnění lze nastavit i jemněji – například pouze pro konkrétní

ID	Požadavek	Způsob naplnění
		atributy nebo objekty splňující zadané podmínky.
52	IDM MUSÍ umožnit definovat oprávnění k funkcionalitám IDM pomocí rolí.	Požadavek je naplněn kompletně. Každá role může být nastavena tak, aby uživatelům umožnila přístup k vybraným částem funkcionality IDM, jako je například správa identit, schvalovací procesy, audit, správa rolí, konfigurace systému apod. Přístup lze řídit na úrovni operací (např. čtení, zápis, mazání) i jednotlivých komponent rozhraní.
53	IDM MUSÍ dovolit nastavovat autorizaci na jednotlivé části GUI nebo pomocí filtrů na jakékoliv entity, které splňují (nebo nesplňují) definované podmínky.	Požadavek je naplněn kompletně. midPoint umožňuje detailní řízení autorizace jak na úrovni jednotlivých částí uživatelského rozhraní (GUI), tak i na úrovni konkrétních entit a jejich atributů pomocí podmínek a filtrů. Oprávnění lze konfigurovat tak, aby se vztahovala pouze na objekty, které splňují předem definované podmínky – například organizační zařazení, typ identity, stav účtu apod.
54	IDM MUSÍ umožnit definovat autorizaci na základě podmínky - např. vedoucí odboru (oddělení apod.) smí upravovat autorizace svých podřízených.	Požadavek je naplněn kompletně. midPoint umožňuje konfigurovat autorizaci na základě dynamických podmínek, jako je organizační zařazení uživatele nebo jeho pozice v hierarchii. Lze tak nastavit, že například vedoucí odboru má oprávnění upravovat přístupy a role pouze u zaměstnanců, kteří jsou v rámci struktury jeho podřízenými. Tyto podmínky jsou definovány pomocí přístupových pravidel a filtrů.
55	IDM MUSÍ dovolit vytvořit administrátorská práva nad určitými organizačními jednotkami, koncovými systémy, nad skupinami uživatelů nebo obecně nad definovanými objekty IAM. Účelem je umožnit administrátorovi správu nad uživateli patřícími do samostatného podřízeného celku - např. nad externími entitami, kterými jsou dodavatelské účty.	Požadavek je naplněn kompletně. midPoint umožňuje vytvářet administrátorské role s omezenou působností na základě organizační příslušnosti, typu uživatelů, koncových systémů nebo jiných atributů objektů. Lze tak například definovat administrátora, který má oprávnění pouze ke správě externích účtů nebo uživatelů v rámci konkrétní organizační jednotky. Přístup je řízen přes granulární autorizace s možností použití filtrů.

ID	Požadavek	Způsob naplnění
56	IDM MUSÍ umožnit konfigurovat práva všech uživatelů tak, aby si mohli zobrazit: • Přiřazené koncové systémy, • Přiřazená oprávnění, • Přiřazení do organizační struktury.	Požadavek je naplněn kompletně. Každý uživatel si může prostřednictvím samoobslužného rozhraní zobrazit seznam přiřazených účtů v koncových systémech, aktuálně přidělených rolí a oprávnění, jakož i své zařazení v organizační struktuře.

Tabulka 7 – Autorizace

4.2.5 Autentizace v IDM

- Operace související s autentizací jsou zaznamenávány do auditního logu IDM.
- IDM umožní hesla uživatele zabezpečovat symetrickou šifrou nebo pouze ukládat jejich hash, dle globální konfigurace.
- IDM podporuje vedení historie hesel uživatelů, v případě jejich změny přes IDM. Nově zadávaná hesla jsou kontrolována proti historii.
- Podpora autentizace proti AD a to jak pomocí SSO, tak i přímo s využitím protokolu Kerberos nebo LDAP.

4.2.6 Delegace a zastupování

Nabízené řešení musí podporovat delegace a zastupování:

- Na definovanou dobu (od-do) nastavit zástupce pro všechny požadavky, které budou v době od-do směrované na schvalovatele; zastupování musí být aditivní – původní schvalovatel musí být stále schopen požadavek schválit stejně, jako kdyby zástup nebyl nastaven.
- Po definovanou dobu nastavit plnou zastupitelnost na zvoleného uživatele.
- Možnost nastavení delegace i na již rozpracované požadavky.

4.2.7 Rozhraní pro integraci

Nabízené řešení musí poskytovat rozhraní pro integraci a splňovat následující požadavky:

- Za pomoci Web service API (SOAP/WSDL) nebo REST API číst, nebo zapisovat všechna data a volat operace nad objekty v IDM.
- Volat ekvivalent jakékoli funkcionality, která je dosažitelná z webového rozhraní (možnost volání jen některých funkcí jádra IDM je pro tyto potřeby nedostatečná).

Rozhraní musí splňovat následující parametry:

- Umožňovat bezpečný přenos dat mezi IDM a rozhraním koncového systému (např. SSL/TLS, pro AD Kerberos nebo NTLM2).
- IDM se k rozhraní koncového systému musí autentizovat dedikovaným technickým uživatelem.
- Aplikační rozhraní (WS SOAP, REST, Java API, Powershell apod.) nebo rozhraní datového úložiště (LDAP, DB procedury, DB tabulka).
- Musí nabízet návratové kódy při zpracování operace.

ID	Požadavek	Způsob naplnění
57	IDM MUSÍ nabízet administrační rozhraní (GUI) pro správu koncových systémů (včetně nastavení parametrů připojení pro zobrazení skutečných účtů kontrolou v koncovém systému).	Požadavek je naplněn kompletně. midPoint poskytuje administrační webové rozhraní pro správu koncových systémů, které umožňuje konfigurovat připojení, spravovat konektory, nastavovat parametry synchronizace a testovat komunikaci se systémy. Administrátor má možnost přes GUI zobrazit aktuální účty přímo z napojeného systému, ověřit jejich stav a provádět základní diagnostiku připojení.
58	IDM MUSÍ nabízet programové rozhraní (API) nabízející ekvivalentní funkcionalitu jako nabízí GUI.	Požadavek je naplněn kompletně. midPoint poskytuje rozsáhlé RESTful API, které umožňuje přístup ke všem klíčovým funkcím dostupným i prostřednictvím grafického uživatelského rozhraní (GUI). Pomocí API je možné provádět správu identit, rolí, účtů, koncových systémů, spouštět schvalovací procesy, synchronizace a další operace.
59	API rozhraní MUSÍ být být dostupné jako Web service s využitím standardizovaného protokolu (např. SOAP/WSDL nebo REST) a zabezpečeno odpovídajícím způsobem (SSL/TLS).	Požadavek je naplněn kompletně. midPoint poskytuje API rozhraní ve formě standardizovaných webových služeb – primárně prostřednictvím REST, které je rozšiřitelné a podporuje práci s JSON, XML i YML. Veškerá komunikace přes API probíhá zabezpečeně přes protokol HTTPS s využitím SSL/TLS.
60	IDM MUSÍ umožnit nastavit přístupová práva pro využití API jednotlivým uživatelům systému.	Požadavek je naplněn kompletně. midPoint umožňuje detailní řízení přístupových práv k API na základě přiřazených rolí a oprávnění jednotlivých uživatelů. Každému uživateli nebo systémové identitě lze přidělit specifická oprávnění, která určují, jaké operace prostřednictvím API může provádět – například čtení, zápis nebo mazání konkrétních objektů. Autorizace k API je řízena stejným RBAC modelem jako ostatní části systému.
61	IDM MUSÍ nabízet správu koncových systémů prostřednictvím	Požadavek je naplněn kompletně.

ID	Požadavek	Způsob naplnění
	integrační vrstvy s možností volání funkcí prostřednictvím programového rozhraní (APl).	Programové rozhraní umožňuje volat funkce pro registraci systémů, nastavení konektorů, testování připojení, spouštění synchronizací, kontrolu účtů a správu napojení identit.
62	IDM MUSÍ umožňovat evidenci koncových systémů včetně popisného atributu.	Požadavek je naplněn kompletně. midPoint umožňuje evidovat všechny napojené koncové systémy jako samostatné objekty v rámci svého datového modelu. Ke každému systému lze definovat popisné atributy, jako je název, typ systému, vlastník, technické informace o připojení, účel použití nebo stav integrace.
63	IDM MUSÍ umožňovat vazbu na aplikační role přiřazené ke koncovému systému v kardinalitě 1:N.	Požadavek je naplněn kompletně. Každý koncový systém může mít přiřazeno libovolné množství aplikačních rolí, které reprezentují konkrétní oprávnění nebo přístupové úrovně v dané aplikaci. Tyto role lze následně přiřazovat uživatelům prostřednictvím business rolí nebo přímo.
64	IDM MUSÍ umožňovat rozlišení různých kategorií účtů (např. administrátorské a běžné účty).	Požadavek je naplněn kompletně. Kategorie účtů lze evidovat jako atributy účtu nebo identity a využít je při řízení životního cyklu, aplikaci bezpečnostních politik, přidělování oprávnění nebo filtrování v reportech.
65	IDM MUSÍ umožňovat různou business logiku plnění atributů pro různé kategorie účtů.	Požadavek je naplněn kompletně. midPoint umožňuje definovat odlišnou business logiku pro plnění atributů na základě kategorie účtu (např. běžný, administrátorský, technický, externí). Pomocí konfigurovatelných mapovacích pravidel (mappings) lze pro každou kategorii nastavit specifické hodnoty, výpočetní vzorce nebo výjimky pro jednotlivé atributy, jako jsou login, e-mail, organizační příslušnost apod.
66	IDM MUSÍ umožňovat povolení jednotlivých operací nad koncovým systémem (např. dočasně deaktivovat zápis do koncového systému).	Požadavek je naplněn kompletně. Administrátor může například dočasně deaktivovat zápis do systému, zatímco čtení a synchronizace zůstávají aktivní. Tato granularita nastavení operací (read, write, delete) umožňuje

ID	Požadavek	Způsob naplnění
		pružně reagovat na provozní požadavky nebo plánované změny v napojených systémech, aniž by bylo nutné systém zcela odpojit. Změny v nastavení operací jsou auditovatelné a dostupné jak přes GUI, tak i API.

Tabulka 8 – Správa koncových systémů

4.2.7.1 Defaultní konektory

Součástí nabízeného IDM systému musí být připojení minimálně k následujícím typům koncových systémů pomocí konfigurace:

- Active Directory
- LDAP
- SQL Databáze
- CSV soubory

Připojení k těmto typům systémů musí být konfigurovatelné, nesmí se jednat o vývoj nebo využití komponenty třetí strany.

ID	Požadavek	Způsob naplnění
67	IDM MUSÍ podporovat připojení k následujícím typům koncových systémů: Active Directory, LDAP, SQL databáze, CSV soubory.	Požadavek je naplněn kompletně. midPoint nativně podporuje připojení ke koncovým systémům typu Active Directory, LDAP, relační databáze (SQL) a CSV soubory. Pro tyto systémy jsou k dispozici tzv. bundled konektory, které jsou součástí základní instalace produktu a nevyžadují dodatečný vývoj. Konektory umožňují čtení i zápis dat, synchronizaci účtů, správu atributů a detekci změn. Díky tomu je možné rychle a efektivně integrovat běžně používané systémy bez nutnosti vlastních integračních rozhraní.
68	IDM MUSÍ podporovat spouštění programovatelných skriptů, jako součást integrace koncových systémů.	Požadavek je naplněn kompletně. midPoint umožňuje spouštění programovatelných skriptů jako součást integračních procesů s koncovými systémy. Skripty lze

ID	Požadavek	Způsob naplnění
		využít při mapování atributů, transformacích dat, rozhodování o přiřazení účtů nebo řízení výjimečných scénářů. Podporovány jsou skriptovací jazyky jako Groovy, Python nebo JavaScript, přičemž skripty mohou být spouštěny při operaci/synchronizaci/importu/exportu.
69	IDM MUSÍ být integrovaný s aplikacemi, se kterými je integrovaný současný IDM (seznam aplikací je uvedený výše v tomto dokumentu).	Požadavek je naplněn kompletně. Navrhované řešení je navrhnut taktéž IDM midPoint stejné verze, nebude potřeba dointegrovávat již připojené aplikace, pouze případné konfigurace.

Tabulka 9 – IDM integrace pomocí konektorů

4.2.8 Podpora integrace s MS Active Directory (dále jen MS AD)/LDAP

- Integrace s MS AD jako zdrojem dat
- Aktualizace uživatelů na serveru MS AD se musí maximálně do 30 minut projevit v autentizačním systému
- Automatická synchronizace uživatelů z MS AD do nabízeného řešení (v případě založení/zrušení uživatele v MS AD bude tento záznam automaticky synchronizován)
- Bez nutnosti instalace jakéhokoli SW přímo na MS AD server
- Nabízený systém musí pouze číst informace služby MS AD
- Nabízený systém nesmí zapisovat žádná data na server MS AD
- Blokování uživatele v MS AD se propíše do nabízeného systému
- Nabízený systém podporuje svůj vlastní blokovací mechanismus nezávislý na MS AD
- Podpora více domén
- Možnost využití existujících MS AD skupin a definice vlastních
- Nastavení ověření dle členství ve skupině
- Ověřování provádí nabízený systém, nikoli server MS AD
- Možnost konfigurovat mapovaná data z MS AD

4.2.9 Grafické uživatelské rozhraní pro koncové uživatele

S IDM bude pracovat množství uživatelů bez hlubších technických znalostí, kteří budou moci žádat o přístup a spravovat role. Proto vybrané části uživatelského rozhraní musí být přizpůsobené těmto uživatelům tak, aby potřebné úkoly pro ně byly intuitivní a dokázali je vyřešit bez pomoci, případně jen s minimalistickým návodem nebo zaškolením. Tudíž musí být webové rozhraní IdM systému nakonfigurováno, aby splňovalo tyto požadavky nebo musí být naprogramované nové jednoúčelové rozhraní pro níže popsané operace, pokud by stávající rozhraní nebylo možné dostatečné přizpůsobit.

Vyhovující rozhraní nebude obsahovat nadbytečné položky a informace, například položky navigačního menu pro funkce, které daný uživatel nemá oprávnění používat nebo zobrazení informací které pro konkrétního uživatele nemají význam. Naopak by rozhraní mělo intuitivně uživatele navést na všechny operace potřebné pro správu rolí, a to jak svých vlastních, tak i rolí kolegů, pro jejichž správu bude daný uživatel autorizovaný. Nedílnou součástí bude schvalování žádostí o přiřazení role a nastavení zastupování ve schvalování.

V neposlední řadě bude nutné nastavit systém notifikací upozorňující uživatele na nutnost provedení akce, např. schválení žádosti o přístup, nebo informující o změnách, např. o přidělení přístupu po schválení.

Zadavatel posoudí uživatelskou přívětivost těchto částí systému na základě návrhu Dodavatele a bude s Dodavatelem průběžně spolupracovat na výsledné podobě uživatelského rozhraní.

ID	Požadavek	Způsob naplnění
70	IDM MUSÍ obsahovat GUI pro koncové uživatele umožňující podat žádost o přidělení role pro žádajícího uživatele nebo pro další uživatele pro které je aktuální uživatel oprávněný žádat.	Požadavek je naplněn kompletně. midPoint poskytuje samoobslužné webové rozhraní pro koncové uživatele, které umožňuje podání žádosti o přidělení role jak pro sebe, tak i pro jiné uživatele, pokud k tomu má oprávnění (např. nadřízený). Rozhraní je přehledné, přizpůsobitelné a podporuje výběr ze schváleného katalogu rolí. Po odeslání žádosti se automaticky spustí definovaný schvalovací proces.
71	IDM MUSÍ podporovat nastavení doby platnosti jako součást žádosti o roli, a případné nastavení dalších specifických atributů tohoto přiřazení, které bude IDM dále automaticky zpracovávat a propagovat do dalších systémů.	Požadavek je naplněn kompletně. midPoint umožňuje uživateli při podání žádosti o roli zadat dobu platnosti přiřazení (od-do), případně doplnit další specifické atributy podle konfigurace (např. poznámka). Tyto informace jsou následně uloženy v rámci přiřazení a systém je automaticky vyhodnocuje - například pro řízení platnosti oprávnění nebo jejich propagaci do cílových systémů. Atributy přiřazení lze dále využít při transformacích, reportingu nebo auditu.
72	IDM MUSÍ zobrazit v žádosti o roli pouze takové role z katalogu rolí, o které je žádající uživatel oprávněn žádat.	Požadavek je naplněn kompletně. Při podání žádosti o roli se uživateli zobrazí pouze ty role, které má oprávnění žádat - buď pro sebe, nebo pro jiné uživatele, pokud je k tomu autorizován.
73	IDM MUSÍ umožnit prohledávání katalogu rolí dle zadaných kritérií nebo aktivovat filtrování podle rolí vybraného uživatele.	Požadavek je naplněn kompletně. Systém umožňuje vyhledávání dle různých kritérií, jako je název, popis, cílový systém, úroveň přístupu či přiřazený garant. Součástí je také možnost filtrovat role podle uživatele – například zobrazit pouze role, které má uživatel aktuálně přiřazeny, nebo na které má oprávnění žádat.
74	IDM MUSÍ umožnit uživatelům zobrazit své žádosti o role a také	Požadavek je naplněn kompletně. midPoint umožňuje uživatelům v samoobslužném rozhraní

ID	Požadavek	Způsob naplnění
	seznam žádostí čekajících na jejich schválení.	zobrazit přehled všech vlastních žádostí o role, včetně jejich aktuálního stavu, detailů a historie schvalování. Zároveň systém poskytuje rozhraní pro schvalovatele, kde je dostupný seznam žádostí, které čekají na jejich rozhodnutí.
75	IDM MUSÍ oprávněným uživatelům zobrazit jejich vlastní role, i role dalších uživatelů a také seznam uživatelů majících konkrétní roli. Role bude možno takto přidávat i odebírat. Popsané funkce budou omezeny nastavenými právy aktivního uživatele.	Požadavek je naplněn kompletně. midPoint umožňuje oprávněným uživatelům zobrazit seznam vlastních přiřazených rolí, rolí jiných uživatelů a také seznam všech uživatelů, kteří mají přiřazenu konkrétní roli. Těmto uživatelům je rovněž umožněno role přidávat nebo odebírat, a to v rozsahu oprávnění definovaných jejich rolí a přístupovými pravidly. Přístup k těmto funkcím je plně řízen autorizací systému a lze jej omezit např. na konkrétní organizační jednotky, typy rolí nebo skupiny uživatelů.
76	IDM MUSÍ umožnit uživateli nastavit své zastupování ve schvalování pro případ nepřítomnosti.	Požadavek je naplněn kompletně. midPoint umožňuje uživatelům nastavit dočasné zastupování pro schvalovací procesy v případě plánované nepřítomnosti, jako je dovolená nebo pracovní neschopnost. Uživatel může prostřednictvím samoobslužného rozhraní delegovat schvalovací oprávnění na jiného uživatele s určením časového rozsahu platnosti zastupování.
77	IDM MUSÍ umožnit uživateli zobrazit informaci, zda aktuálně někoho zastupuje.	Požadavek je naplněn kompletně. V samoobslužném rozhraní je dostupný přehled aktivních zastoupení, včetně jména zastupovaného uživatele, rozsahu oprávnění a doby platnosti delegace.
78	IDM MUSÍ umožnit uživateli podporovat minimálně následující notifikace: Potvrzení o žádosti o novou roli žadateli, potvrzení o schválení nebo zamítnutí žádosti žadateli, výzva ke schválení schvalovateli, oznámení o zastupování zastupujícímu.	Požadavek je naplněn kompletně. midPoint podporuje plně konfigurovatelný systém notifikací, který umožňuje informovat uživatele o všech důležitých událostech v rámci procesu žádosti a schvalování rolí. Systém

ID	Požadavek	Způsob naplnění
		automaticky zasílá potvrzení o podání žádosti, výsledek schválení nebo zamítnutí, výzvu ke schválení příslušným schvalovatelům a také oznámení zastupujícímu uživateli při aktivaci jeho zastupování. Notifikace lze přizpůsobit dle potřeb Zadavatele a doručovat prostřednictvím e-mailu nebo jiných komunikačních kanálů dle integrace.
79	IDM MUSÍ v notifikaci s výzvou pro schválení zobrazit odkaz do webového rozhraní vedoucí přímo na místo, kde je možné provést rozhodnutí.	Požadavek je naplněn kompletně. Systém umožňuje v rámci notifikací pro schvalovatele zobrazit přímý odkaz do webového rozhraní systému, který vede přímo na konkrétní žádost čekající na schválení.

Tabulka 10 - Požadavky na přívětivost uživatelského rozhraní pro koncové uživatele

4.3 Požadavky na integraci do DWH

ID	Požadavek	Způsob naplnění
80	IDM MUSÍ zajistit identifikaci datových zdrojů, které budou relevantní pro budoucí přenos dat IDM do DWH.	Požadavek je naplněn kompletně. midPoint umožňuje jednoznačně identifikovat všechny relevantní datové zdroje a entity (např. identity, účty, role, přiřazení, schválení, změny a auditní záznamy), které mohou být využity pro přenos dat do datového skladu (DWH). Systém poskytuje možnosti exportu těchto dat ve strukturované podobě (např. JSON, XML) a přes REST API.
81	IDM MUSÍ zajistit návrh a popis způsobů extrakce datových zdrojů IDM, včetně detailní analýzy datového modelu a mapování jednotlivých atributů.	Požadavek je naplněn kompletně. midPoint umožňuje návrh a realizaci standardizovaných způsobů extrakce dat prostřednictvím REST API, exportních úloh nebo přímým přístupem k DB View.
82	IDM MUSÍ zajistit návrh technického řešení extrakce z IDM včetně způsobu, koordinace a časového harmonogramu pravidelných přenosů dat.	Požadavek je naplněn kompletně. Návrh zahrnuje volbu vhodné metody přenosu (např. REST API, exportní úlohy, synchronizované soubory), definici přenášených

ID	Požadavek	Způsob naplnění
		datových struktur, způsob zabezpečení přenosu a stanovení pravidelné frekvence exportu dle požadavků Zadavatele. Koordinace bude zajištěna pomocí plánovače úloh v IDM nebo prostřednictvím externí orchestrace.
83	IDM MUSÍ zajistit přípravu a realizaci datových extraktorů dle výše naplněných požadavků.	Požadavek je naplněn kompletně. Extraktory budou implementovány podle navrženého technického řešení a datového modelu, včetně transformace, filtrování a mapování požadovaných atributů. Součástí dodávky bude také testování, dokumentace a případná parametrizace pro změnu četnosti nebo rozsahu výstupů.
84	IDM MUSÍ zajistit návrh a přípravu jednorázové počáteční migrace relevantních dat z IDM do DWH po zprovoznění integrace datového skladu.	Požadavek je naplněn kompletně. Migrace bude zahrnovat výběr datových sad (např. identity, účty, přiřazené role, auditní záznamy), jejich transformaci do cílové struktury a bezpečný přenos do DWH. Bude připraven plán migrace včetně testování, časového harmonogramu a způsobu zajištění konzistence a integrity dat.
85	IDM MUSÍ zajistit realizaci pravidelných přenosů dat IDM do DWH.	Požadavek je naplněn kompletně. Přenosy budou prováděny prostřednictvím plánovaných exportních úloh, rozhraní REST API nebo dalších dohodnutých metod. Systém umožňuje definovat rozsah přenášených dat, jejich strukturu a způsob zabezpečení přenosu, monitoring přenosů, atd.

Tabulka 11 – Požadavky na integraci s DWH

4.3.1.1 Podpora konektorů do koncových systémů

Nabízené řešení musí podporovat vytváření a vývoj vlastních konektorů.
Jedná se minimálně o:

- Připojení k různorodým webovým službám a využití jejich metod

- Připojení k různým typům a strukturám databází a čtení a zápis dat

ID	Požadavek	Způsob naplnění
86	IDM MUSÍ podporovat možnost vývoje a následné integrace dalších konektorů pro integrace s dalšími systémy.	Požadavek je naplněn kompletně. midPoint je postaven na architektuře, která umožňuje snadný vývoj a integraci vlastních konektorů pro připojení dalších systémů.

Tabulka 12 – Vývoj konektorů

4.3.2 Synchronizace a rekonciliace

Nabízené řešení musí podporovat:

- Synchronizace změn v reálném čase s odolností proti výpadkům informačních systémů - vestavěná podpora opakování propagace změn v případě neúspěchu.
- Obousměrná synchronizace dat jak z IDM do koncového systému (např. uživatele a jejich atributy), tak z koncového systému do IDM (např. role v konkrétním koncovém systému).
- Mapování atributů mezi koncovými systémy na základě pravidel/vzorců.
- Práce s komplexními (tabulky) či binárními atributy uživatele - certifikáty, fotografie, autentizační tokeny.
- Rekonciliace účtů – pravidelná automatická kontrola stavu účtů na koncových systémech s autoritativním vypořádáním nesouladu.
- Rekonciliace účtů – zaznamenání stavu účtu vzhledem k ne/existenci vlastníka v IDM.
- Rekonciliace oprávnění - pravidelná automatická kontrola stavu oprávnění na koncových systémech oproti stavu chtěnému a náprava (notifikace, zápis do logů, výmaz nadbytečných oprávnění apod.).
- Nastavení pravidel pro párování mezi identitou a účtem (například e-mail identity na login účtu) skrze všechny koncové systémy.

ID	Požadavek	Způsob naplnění
87	IDM MUSÍ umožnit načíst data z koncových systémů (synchronizace) a porovnat schválený a skutečný stav v koncovém systému (rekonciliace) a dále MUSÍ zabezpečit (umožnit): • Synchronizaci změn v reálném čase podle časové značky u záznamu, • Podporu opakování propagace změn v případě neúspěchu, • Obousměrnou synchronizaci dat mezi IDM a koncovým systémem (např. uživatele a jejich atributy, role v koncovém systému), • Mapování atributů mezi koncovými systémy na základě pravidel/vzorců, • Práci s binárními atributy uživatele (např. certifikáty, fotografie, autentizační tokeny), • Rekonciliaci účtů - tzn. pravidelnou automatickou kontrolu stavu účtů na koncových systémech s autoritativním vypořádáním nesouladu, • Zaznamenání stavu účtu při rekonciliaci vzhledem k (ne)existenci vlastníka v IDM, • Nastavení automatických akcí pro nespárované účty (např. zneplatnění), • Nastavení „Whitelistu“ účtů, které IDM nebude měnit (např. pro technické účty), • Pravidelnou automatickou kontrolu stavu oprávnění na	<u>Požadavek je naplněn kompletně.</u> midPoint plně podporuje pokročilé funkce synchronizace a rekonciliace dat mezi IDM a koncovými systémy. Umožňuje načítání a porovnávání aktuálního a očekávaného stavu účtů, včetně podpory: – synchronizace změn na základě časových značek (incremental sync), – retry mechanizmu při selhání operace, – obousměrné synchronizace identit, rolí i atributů, – detailního mapování atributů včetně skriptovatelných transformačních pravidel, – práce s binárními daty (např. fotografie, certifikáty), – rekonciliace s možností autoritativního vyhodnocení a vynucení souladu, – detekce účtů bez přiřazeného vlastníka a nastavení akcí pro tyto účty (např. zneplatnění), – generování přehledových a auditních reportů, – podpory více typů objektů v cílovém systému (uživatel, skupina, role, organizační jednotka), – zpracování rekonciliace paralelně ve více vláknech pro vyšší výkon, – whitelistingu vybraných účtů, – pravidelné kontroly oprávnění v cílových systémech a jejich případné odebrání, – vizuální simulace změn objektů před jejich uložením, což zvyšuje kontrolu nad operacemi v systému. – kompletního logování a auditu všech změn, – realizace hromadných akcí řízených pravidly (včetně jejich

ID	Požadavek	Způsob naplnění
	koncových systémech a vynucení chtěného stavu (např. výmaz nadbytečných oprávněni), • Logování veškerých aktivit synchronizací a rekonciliací, • Reportování výsledků rekonciliací pomocí reportů, • Podporu pro objekty v koncovém systému typu uživatel, skupina, role a organizace, • V koncovém systému měnit i jiné typy objektů, než je uživatelský účet (např. role, skupiny, profily), • Spustit každou rekonciliaci tak, aby zpracování objektů koncových systémů běželo ve více vláknech, • Hromadné akce - spouštění hromadných akcí: o hromadné přiřazení rolí uživatelům, kteří vyhovují podmínkám, o hromadnou změnu organizační jednotky vybraných uživatelů, o hromadné vytvoření rolí, o hromadné schvalování přidělených úkolů, s tím, že všechny hromadné akce budou auditovány. • Simulace změn – IDM bude poskytovat grafický přehled změn atributů před vlastním uložením vybraného objektu, tato simulace se týká minimálně uživatelů, rolí a organizační struktury.	auditovatelnosti),
88	IDM MUSÍ umožnit nastavení prahových hodnot, které zabrání hromadným změnám např. z důvodu chybných dat na vstupu, tak aby nedošlo k hromadným nežádoucím změnám (např. smazání objektů v Active Directory). Tato funkcionalita umožní při větším	<u>Požadavek je naplněn kompletně.</u> midPoint obsahuje vestavěný mechanismus pro detekci a prevenci hromadných nežádoucích změn prostřednictvím nastavitelných prahových hodnot. midPoint umožňuje

ID	Požadavek	Způsob naplnění
	počtu změn zastavit frontu změn a upozornit administrátora IDM emailem a zapsat tuto informaci do logu IDM. Tato vlastnost je poplatná pro všechny vstupně/výstupní konektory.	konfigurovat maximální povolený počet změn (např. mazání, deaktivace účtů, odebrání rolí).
89	IDM MUSÍ umožnit notifikovat konfliktní stavy (např. synchronizovaný systém v chybě) v systému IDM pomocí emailu na administrátory IDM, případně na další osoby (včetně zápisu do logu IDM).	Požadavek je naplněn kompletně. midPoint umožňuje automatické rozpoznání a notifikaci chybových a konfliktních stavů v systému, jako jsou selhání synchronizace, výpadky konektorů nebo neúspěšné provedení změn. Při detekci takového stavu systém zašle e-mailové upozornění administrátorům IDM a/nebo jiným určeným osobám dle nastavení.

Tabulka 13 – Synchronizace a rekonciliace

4.3.3 E-mailové notifikace

Procesy notifikací a správa procesů musí být nastaveny v souladu s GDPR.
Nabízené řešení musí podporovat:

- Možnost definice šablon e-mailů s podporou vícejazyčnosti a HTML
- Podpora skriptovacího jazyka s možností čerpání dat z repozitáře
- Možnost konfigurace parametrů odesílání zpráv (SMTP server apod.)
- Odesílání SMS zpráv pomocí SMS brány Zadavatele
- Zvolit si v nastavení více odesílacích SMTP serverů.
- Vkládat hypertextové odkazy na konkrétní záznamy

4.3.3.1 Notifikované akce

Nabízené řešení musí podporovat notifikaci minimálně následujících akcí:

- vytvoření, změna, smazání identity,
- přiřazení a odebrání role,
- výzva k akci,
- zakázání a povolení uživatele,
- přejmenování uživatele,
- požadavek na schválení role,
- libovolné akce ve workflow.

ID	Požadavek	Způsob naplnění
90	IDM MUSÍ umožňovat zasílat notifikace pomocí e-mailu nebo SMS (s využitím SMS brány Zadavatele).	Požadavek je naplněn kompletně. midPoint podporuje zasílání notifikací prostřednictvím e-mailu a umožňuje rozšíření o další komunikační kanály, včetně integrace se SMS bránami. V rámci realizace bude možné napojit systém na SMS bránu Zadavatele a konfigurovat pravidla pro odesílání notifikací dle typu události, příjemce a závažnosti pomocí konfigurace tzv. transportu notifikace.
91	IDM MUSÍ u e-mailových notifikací podporovat šablony s možností použití skriptů pro vkládání dat, HTML formátování včetně vkládání hypertextových odkazů a více jazykových variant notifikací.	Požadavek je naplněn kompletně. Notifikace mohou být definovány jako HTML šablony s možností vkládání dynamických dat pomocí skriptovacích jazyků (např. Groovy, Python a Javascript). Lze využít podmíněné zobrazení obsahu, vícejazyčné varianty (např. na základě jazykové preference uživatele) a vkládat aktivní hypertextové odkazy vedoucí na konkrétní akce v systému (např. schválení žádosti).
92	IDM MUSÍ podporovat více SMTP serverů.	Požadavek je naplněn kompletně. midPoint umožňuje konfiguraci více SMTP serverů pro odesílání e-mailových notifikací. Lze definovat primární a záložní SMTP servery. V případě nedostupnosti jednoho serveru lze nastavit přepnutí na druhý.

Tabulka 14 – Notifikace

4.3.4 Delegování správy

- Nabízené řešení musí podporovat delegovanou správu.
- Delegovaní správci musí mít administrátorská práva nad zvolenými komunitami,
  nad skupinami uživatelů nebo obecně nad definovanými objekty IDM – účelem je umožnit lokálnímu administrátorovi správu nad uživateli patřícími do samostatného podřízeného celku (ať už z pohledu interního, tak externího - například dodavatelské účty).

ID	Požadavek	Způsob naplnění
93	IDM MUSÍ pro jednotlivé objekty nebo definované skupiny objektů nadefinovat, kdo je jejich správcem a takovému správci nastavit oprávnění pro manipulaci s danými objekty.	Požadavek je naplněn kompletně. Každému správci lze přiřadit specifická oprávnění pro manipulaci s těmito objekty, jako je vytvoření, úprava, mazání nebo schvalování změn. Tento model umožňuje delegovanou správu objektů v systému a podporuje podmíněné oprávnění na základě rolí nebo organizační struktury.

Tabulka 15 – Delegování správy

4.3.5 Workflow

Nabízené řešení musí podporovat tvorbu workflow a u nich umožnit:

- Administrátor IDM musí vytvářet nové definice workflow a modifikovat stávající, pro které se používají nejčastěji základní typy procesů:
  - Procesy monitorování – systém zjišťuje stavy záznamů, atributů a při splnění podmínky nastartuje proces s upozorněním e-mailem.
  - Řízení toku záznamů (např.: schvalovací workflow pro business role, kde business roli reprezentuje záznam v systému) – systém automaticky přiděluje úkoly zodpovědným lidem, jak je postupně záznam zpracováván.
- Workflow dále umožňuje:
  - neomezený počet schvalovacích kroků,
  - neomezený počet schvalovatelů,
  - schválení typu „jeden z X“ a typu „všichni musí schválit“,
  - paralelní schvalování a step-by-step schvalování,
  - definici schvalovatelů na základě jejich členství v roli, funkci nebo v organizační struktuře,
  - automatické schválení na základě hodnoty atributů,
  - automatické schválení na základě pracovního místa, funkce nebo zařazení v organizaci.
- Notifikovat schvalovatele e-mailem nebo pomocí SMS.
- Zobrazit schvalovatelům přehled svých úloh.
- Úlohu schválit či zamítnout včetně uvedení zdůvodnění.
- Administrátor IDM musí být schopen pracovat se všemi úlohami (pro řešení nestandardních situací).
- Možnost definovat podmíněné kroky (například přiřadit všechny aplikační role až po změně úvodního hesla).

ID	Požadavek	Způsob naplnění
94	IDM MUSÍ podporovat schvalovací workflow navázané na žádost o novou roli nebo na změnu záznamů v systému.	Požadavek je naplněn kompletně. Systém plně podporuje schvalovací workflow, které lze navázat na různé typy žádostí, včetně žádosti o přidělení nové role, odebrání role nebo změnu údajů v systému (např. atributy uživatele, organizační zařazení apod.). Workflow je plně konfigurovatelné – podporuje jedno i víceúrovňové schvalování, eskalace, podmíněné větvení.
95	IDM MUSÍ umožňovat zobrazení stavu workflow nebo o jeho stavu notifikovat.	Požadavek je naplněn kompletně. midPoint umožňuje zobrazit aktuální stav každého běžícího i historického workflow přímo v uživatelském i administrátorském rozhraní. Uživatelé i schvalovatelé mají přístup k detailům procesu, včetně informací o jednotlivých krocích, schvalovatelích, stavu a historii změn. Systém zároveň podporuje notifikace o změnách stavu workflow (např. schválení, zamítnutí, čekání na rozhodnutí), které jsou doručovány e-mailem nebo jinými integrovanými kanály.
96	IDM MUSÍ umožňovat detailní nastavení průběhu schvalování včetně možnosti automatického schválení podle nastavených podmínek.	Požadavek je naplněn kompletně. midPoint umožňuje detailní konfiguraci schvalovacích procesů – včetně definice schvalovacích cest, podmínek pro určení schvalovatelů, víceúrovňového schvalování i paralelních kroků. Součástí je také možnost automatického schválení žádosti na základě předem definovaných pravidel, jako je typ žádosti, role, žadatel, organizační příslušnost nebo jiný atribut.

Tabulka 16 – Workflow

4.3.6 Rekonciliace

Nabízené řešení musí podporovat rekonciliace a u nich umožnit definovat pro každý připojený systém zvlášť:

- plánované (automaticky spouštěné) rekonciliace a rekonciliace na vyžádání,
- nastavit plán rekonciliací,
- definovat seznam rekonciliovaných objektů,
- definovat typ rekonciliovaných objektů,
- nastavit korelační pravidla,
- podporovat rekonciliaci všech typů objektů (uživatele, role, organizační strukturu),
- logovat a reportovat stav výsledku rekonciliace,
- nastavit spuštění akce na základě výsledku rekonciliace,
- podporu pro objekty v koncovém systému typu uživatel, skupina, role a organizace.

4.3.6.1 Online a offline rekonciliace

Nabízené řešení musí kromě online řízení oprávnění a identit do připojených koncových systémů podporovat i tzv. offline řízení oprávnění a identit na základě manuálního potvrzení akce odpovědnou osobou nebo na základě informací získaných z exportu koncového systému.

ID	Požadavek	Způsob naplnění
97	IDM MUSÍ podporovat rekonciliace a to jak jednorázové, tak i periodické, včetně nastavení individuálního plánu jejich spouštění.	Požadavek je naplněn kompletně. midPoint plně podporuje realizaci rekonciliací ve dvou režimech: jednorázovém (ad hoc spuštění správcem) i periodickém (automaticky podle časového plánu). Pro každý napojený systém lze individuálně definovat plán spouštění rekonciliace s přesným nastavením frekvence (denní, týdenní, měsíční apod.), času spuštění a rozsahu zpracovávaných dat.
98	IDM MUSÍ umět definovat pro každý integrovaný systém, jaké objekty se budou rekonciliovat	Požadavek je naplněn kompletně. Systém umožňuje pro každý integrovaný (napojený) systém individuálně definovat, které typy objektů budou předmětem rekonciliace – např. uživatelé, skupiny, role, organizační jednotky nebo jiné specifické entity daného systému. Konfigurace rekonciliace je flexibilní a lze ji přizpůsobit konkrétním požadavkům každého systému včetně filtrace objektů.
99	IDM MUSÍ podporovat rekonciliaci i u systémů napojeným v režimu offline (oproti exportu dat) nebo semi-manual	Požadavek je naplněn kompletně. midPoint podporuje rekonciliaci i pro systémy, které nejsou napojeny online, ale pracují v režimu offline nebo semi-manual. V takovém případě lze rekonciliaci provádět na základě importu datových souborů (např. CSV), které reprezentují aktuální stav objektů v externím systému. Systém umožňuje tyto soubory načíst, porovnat/vyhopdnotit jejich obsah s informacemi v IDM.
100	IDM MUSÍ podporovat spuštění rekonciliace i nad objekty v IDM. V takovém případě bude provedena jejich rekonciliace ve všech integrovaných systémech, ve kterých má takový objekt	Požadavek je naplněn kompletně. midPoint umožňuje spustit rekonciliaci přímo nad objektem uloženým v IDM – tzv. rekomputaci - např. konkrétním

ID	Požadavek	Způsob naplnění
	svůj odpovídající záznam (např. účet u uživatele).	uživatelem nebo skupinou. Systém při tom automaticky identifikuje všechny připojené systémy, ve kterých daný objekt existuje (např. na základě přiřazených účtů), a provede rekonciliaci stavu ve vztahu k připojeným systémům.

Tabulka 17 – Rekonciliace

4.3.6.2 Hromadné akce

Nabízené řešení musí nabízet spouštění hromadných akcí, např. hromadné přiřazení rolí uživatelům, kteří vyhovují podmínkám, hromadné schvalování přidělených úkolů atp. Každá změna hromadné akce musí být auditovaná.

ID	Požadavek	Způsob naplnění
101	IDM MUSÍ podporovat spouštění hromadných akcí, které dovolí automatizovat sérii kroků, které by administrátor jinak prováděl ručně.	Požadavek je naplněn kompletně. midPoint umožňuje definovat a spouštět hromadné akce (bulk actions), které automatizují opakované nebo rozsáhlé úlohy, jež by jinak musel administrátor provádět manuálně. Pomocí těchto akcí lze například hromadně přiřadit role, upravit atributy, přesunout uživatele do jiné organizační jednotky, aktivovat nebo deaktivovat účty, spustit schvalovací workflow nebo provést opravy v datech. Hromadné akce lze spouštět přes GUI nebo skripty a je potřeba je nadefinovat/nakonfigurovat.

Tabulka 18 – Hromadné akce

4.3.7 Reporting

Nabízené řešení musí nabízet možnost exportovat minimálně do těchto následujících formátů: CSV, HTML.

4.3.7.1 Audit report

Nabízené řešení musí podporovat generování auditního reportu o všech aktivitách v IDM:

- Kompletní přehled změn provedených nad identitou – například synchronizace atributů, přidělení role včetně časového omezení, změn atd.
- Kompletní přehled změn provedených nad libovolnými entitami - role, organizace, definice politik a konfigurací.
- Záznam o přihlášení (úspěšném i neúspěšném) uživatele do webového rozhraní IDM.

4.3.7.2 Uživatelské reporty

Nabízené řešení musí podporovat generování reportů o stavu objektů v IDM:

- Minimálně informace o tom, jaké mají identity přiřazené role a účty v koncových systémech.
- Možnost nastavit filtr pro výběr identit (např. identity patřící do zvolené organizace).

4.3.7.3 Report o rekonciliacích

Nabízené řešení musí podporovat generování reportů o rekonciliacích:

- Přehled účtů v koncových systémech, které jsou známy IDM.
- Možnost identifikace účtů, ke kterým nebyl v IDM nalezen vlastník.

4.3.7.4 Další reporty

- Seznam uživatelů IDM
- Seznam rolí přidělených identitám v IDM
- Seznam přidělených koncových systémů (KS)
- Přehled statusů identit v IDM
- Historie změn nad identitou v IDM
- Historie změn nad identitami směrem do vybraného KS
- Historie změn nad rolemi v IDM
- Historie změn nad organizační strukturou v IDM
- Přehled úloh v IDM a jejich status
- Přehled spuštěných workflow v IDM
- Přehled zprocesovaných workflow v IDM
- Přehled přihlášení identit do GUI

4.4 Požadavky na kontrolní reporty

ID	Požadavek	Způsob naplnění
102	Přístup k reportům (spouštění reportů) MUSÍ být řízeno uživatelskými rolemi.	Požadavek je naplněn kompletně. midPoint umožňuje řídit přístup ke spouštění, zobrazení a správě reportů prostřednictvím oprávnění tak, aby byl dostupný pouze uživatelům s příslušnou rolí.
103	IDM MUSÍ umožňovat generování min. těchto kontrolních reportů: • Report přehled uživatele (uživatelů) a jejich rolí v systémech spravovaných IDM v době generování reportu, • Historie delegování práv uživatele/uživatelů v definovaném časovém období, • Auditní report pro vybraný napojený koncový systém s přehledem o přidělených oprávnění jednotlivým uživatelům (kdo a kdy, proč) a to i s informací o schvalovateli, • Reporty pro schvalovatele – přehledový report kdy komu byl schválen jaký přístup, • Report pro vedoucí zaměstnance – přehledy přidělených, žádaných nebo odebraných přístupů všech podřízených daného vedoucího pracovníka. • Zobrazení rolí přidělených k jednotlivým identitám s přehledným rozlišením rolí navázaných na systemizované místo, rolí navázaných na identitu, rolí navázaných na organizační jednotku, rolí navázaných	Požadavek je naplněn kompletně. midPoint obsahuje modul pro generování reportů, který umožňuje vytvářet výstupy ve formátech CSV či případně HTML a který plně pokrývá požadavky na kontrolní a auditní reporting. Všechny reporty lze naplánovat, exportovat, filtrovat a zabezpečit přístupově dle uživatelských rolí. Data použitá pro reporting vycházejí z interního datového modelu IDM a auditního záznamu, čímž je zajištěna konzistence a úplnost informací.

ID	Požadavek	Způsob naplnění
	na skupinu a delegovaných role, • Souhrnné zobrazení všech rolí včetně informace, odkud uživatel roli zdědil (z organizační jednotky, systemizovaného místa, skupiny) nebo zda a odkud má nějakou roli od někoho delegovánu, • Auditní report – report z údajů o identitách uložených v IDM a to i historických – auditní reporty musí obsahovat souhrnné zobrazení uživatelů (identit) a jejich rolí v systémech napojených na IDM, pracovních pozic / funkcí, přiřazených skupin ve vybraném časovém okamžiku od aktuálního času do minulosti, identity pro generování auditního reporty musí být možné vybrat (filtrovat) dle libovolných atributů identity včetně přidružených referenčních objektů, • Souhrnný online přehled o aktuálním stavu hlavních částí systému a případných chybách – chyby běhu synchronizací, generování a odesílání notifikací, volání webových služeb, plánovaných úloh a běhu automatizovaných úloh, • Zobrazení výpisu napojených informačních systémů.	
104	IDM MUSÍ umožnit generování těchto reportů ve strojově čitelném formátu (např. v XML nebo CSV).	Požadavek je naplněn kompletně. midPoint umožňuje generování všech definovaných reportů také ve strojově čitelných formátech, jako je XML, CSV, které jsou vhodné pro další automatizované zpracování nebo integraci s jinými systémy (např. DWH, nástroje pro business intelligence,

ID	Požadavek	Způsob naplnění
		bezpečnostní monitoring apod.). Uživatel si může zvolit požadovaný formát při generování reportu nebo jej nastavit v plánované úloze
105	IDM MUSÍ umožnit automatické ukládání vygenerovaných reportů s možností pozdějšího zobrazení a stažení.	Požadavek je naplněn kompletně. midPoint podporuje automatické ukládání všech vygenerovaných reportů do centrálního úložiště systému. Každý report je evidován s metadaty a je dostupný ke zobrazení nebo stažení prostřednictvím uživatelského rozhraní.
106	Reporty MUSÍ být možné zasílat automaticky e-mailem na základě konfigurovatelných pravidel.	Požadavek je naplněn kompletně. midPoint umožňuje automatické zasílání reportů e-mailem na základě předem definovaných pravidel. Pro každý report lze nastavit plán generování (např. denně, týdně, měsíčně), seznam příjemců a formát (CSV, HTML). Reporty mohou být zasílány přímo konkrétním uživatelům, správcům, vedoucím pracovníkům nebo schvalovatelům dle jejich role či organizační příslušnosti.

Tabulka 19 – Požadavky na kontrolní reporty

4.5 Rekonciliační reporty

ID	Požadavek	Způsob naplnění
107	IDM MUSÍ zajistit report pro identifikaci účtů, ke kterým nebyl v IDM nalezen vlastník (nespárované účty).	Požadavek je naplněn kompletně. midPoint umožňuje generovat specializovaný report pro identifikaci nespárovaných účtů, tedy účtů v napojených systémech, které nemají přiřazeného vlastníka v IDM (např. chybějící vazba na identitu).
108	MUSÍ být součástí report účtů v koncových systémech a jejich napojení na identity v IDM.	Požadavek je naplněn kompletně. Systém umožňuje generovat report účtů v koncových systémech včetně jejich vazby na identity spravované v IDM. Report obsahuje přehled všech účtů ve vybraných systémech, informaci

ID	Požadavek	Způsob naplnění
		o tom, zda a na kterou identitu jsou v IDM napojeny.
109	MUSÍ být součástí rekonciliační report pro vybraný koncový systém - chronologický seznam akcí nad koncovým systémem.	Požadavek je naplněn kompletně. midPoint umožňuje generovat rekonciliační report pro každý napojený koncový systém, který obsahuje chronologický seznam všech provedených akcí během rekonciliace.

Tabulka 20 – Požadavky na rekonciliační reporty

4.6 Recertifikační reporty

ID	Požadavek	Způsob naplnění
110	Součástí MUSÍ být report o všech recertifikačních kampaních a jejich stavech.	Požadavek je naplněn kompletně. midPoint obsahuje modul pro správu recertifikací přístupů a umožňuje generování reportu, který poskytuje přehled všech recertifikačních kampaní v systému. Report zahrnuje informace o názvu kampaně, schvalovatelích, zahájení a ukončení, aktuálním stavu (probíhá, dokončena, přerušena), počtu schválených a zamítnutých oprávnění.
111	Součástí MUSÍ být report o řešených případech v recertifikačních kampaních.	Požadavek je naplněn kompletně. Systém umožňuje generovat podrobný report o řešených případech v rámci recertifikačních kampaní. Tento report obsahuje seznam všech jednotlivých recertifikačních položek (např. uživatel–role, uživatel–systém), které byly v rámci kampaně posouzeny, spolu s informací o výsledku rozhodnutí (schváleno, zamítnuto, přeposláno), atd.
112	Součástí MUSÍ být report o rozhodnutí jednotlivých ověřovatelů.	Požadavek je naplněn kompletně. midPoint umožňuje generovat detailní report o rozhodnutích jednotlivých ověřovatelů (schvalovatelů) v rámci recertifikačních

ID	Požadavek	Způsob naplnění
		kampaní nebo schvalovacích procesů. Report obsahuje informace o tom, jaký ověřovatel rozhodoval, o kterém přístupu, jaké bylo jeho rozhodnutí (schválení, zamítnutí, delegace), kdy k rozhodnutí došlo, jaký byl typ přístupu (např. role, systémové oprávnění) a případné poznámky nebo odůvodnění.

Tabulka 21 – Požadavky na recertifikační reporty

4.6.1 Agendy a správa objektů

ID	Požadavek	Způsob naplnění
113	V IDM MUSÍ být udržovány minimálně tyto informace o identitě: • Přihlašovací jméno (login), • Osobní číslo, • Služební číslo (v případě služebního poměru), • Plné jméno, • Křestní jméno, • Příjmení, • Titul před jménem, • Titul za jménem, • Emailová adresa, • Alternativní emailové adresy, • Typ identity - zaměstnanec, externista a technický účet, • Název OJ, • Systemizované místo (současné) - kód a platnost od/do,	Požadavek je naplněn kompletně. Systém umožňuje spravovat a uchovávat všechny uvedené informace jako součást datového modelu identity. Každý atribut může být samostatně spravován, zobrazován v uživatelském rozhraní a synchronizován do napojených systémů.

ID	Požadavek	Způsob naplnění
	• Systemizované místo (budoucí) - kód a platnost od/do, • Nadřízený, • Telefon (číslo pevná linka), • Telefon (číslo mobilní linky), • Stav identity - povolená, zakázaná, archivovaná, … • Platnost identity – od, do,	

Tabulka 22 – Atributy identity

ID	Požadavek	Způsob naplnění

114	V IDM MUSÍ být udržovány minimálně tyto informace o roli:
	• Název role - název dle konvence,
	• Popis - uživatelský popis (např. pro koho je role určena a co umožňuje),
	• Vlastník role - identita, která je vlastníkem role a je za ni zodpovědná,
	• Příznaky:
	  ○ přidělení role schvaluje nadřízený - A/N
	  ○ přidělení role schvaluje business vlastník systému - A/N
	  ○ přidělení role schvaluje Compliance/Bezpečnost - A/N
	  ○ přidělení role podléhá proškolení - A/N
	  ○ přidělení role schvaluje „speciální role“ - A/N
	  ○ o roli lze žádat - A/N
	• Business vlastník
		Požadavek je naplněn kompletně.
		midPoint poskytuje komplexní datový model pro správu rolí, který pokrývá všechny uvedené atributy. Každá role může obsahovat název dle sjednocené konvence, uživatelsky srozumitelný popis, definici vlastníka, business vlastníka i schvalovatele. Systém umožňuje nastavit příznaky řízení přidělování rolí (např. víceúrovňové schvalování, požadavek na školení, viditelnost role v katalogu). Typ a stav role, její časová platnost i metadata o správě (včetně historie změn) jsou evidovány a auditovány. Atributy rolí lze využít pro řízení přístupových oprávnění, schvalovacích workflow i reporting.

ID	Požadavek	Způsob naplnění

	• Schvalovatel
	• Typ role - pro jakou skupinu identit je role určena,
	• Stav role - povolená, zakázaná, archivovaná, …
	• Datum platnosti role od, do,
	• Metadata o roli:
	  ○ datum a čas vytvoření
	  ○ kdo vytvořil roli
	  ○ datum a čas poslední úpravy
	  ○ kdo provedl poslední úpravu role
	  ○ kdo schválil poslední úpravu role	

Tabulka 23 – Atributy role

ID	Požadavek	Způsob naplnění
115	V IDM MUSÍ být udržovány minimálně tyto informace o oprávnění (tj. o vazbě mezi identitou a rolí): • Stav přidělení role - platné, neplatné, archivované, … • Atributy žádosti o roli, • Žadatel - login toho, kdo o oprávnění žádal, • Datum žádosti o roli, • Platnost přidělení role od .. do.	Požadavek je naplněn kompletně. midPoint uchovává všechny klíčové informace o oprávněních, včetně stavu přidělení role (platné, neplatné, archivované), atributů žádosti o roli a detailů žadatele (login). Systém také zaznamenává datum žádosti o roli a platnost přidělení role (od – do).

Tabulka 24 – Atributy vazby uživatel – role

4.6.2 Uživatelé

Nabízené řešení musí podporovat:

- Administrační webové rozhraní pro správu uživatelů bez nutnosti instalovat dodatečný SW.
- Správu skrze integrační vrstvu, tzn. přebírání identit z autoritativních zdrojů.
- Evidence atributů identity.
- Zajištění unikátnosti identity.
- Umožnit přidělit jedné osobě jeden jediný účet (identitu) a to i v případě, že má tato osoba více zaměstnaneckých úvazků.
- Zplatnění/zneplatnění identity k určitému datu.
- Přiřazení koncových systémů, rolí či organizace k identitě.
- U koncových systémů evidence uživatelských jmen ve vazbě na identitu.
- Vyhledávání a filtrování podle libovolného (i uživatelsky definovaného) atributu.

ID	Požadavek	Způsob naplnění
116	IDM MUSÍ podporovat rozšiřitelnost ukládaných atributů u uživatelů.	Požadavek je naplněn kompletně. midPoint poskytuje plně rozšiřitelný datový model identit. Nové atributy u uživatelů je možné definovat konfiguračně, bez nutnosti zásahu do kódu systému. Rozšíření se provádí prostřednictvím tzv. schema extensions, které se zapisují do XML schématu (soubor schema-extension.xml), jež se načítá při startu systému.
117	IDM MUSÍ umožnovat vyhledávání podle libovolného atributu včetně uživatelsky definovaných.	Požadavek je naplněn kompletně. midPoint podporuje pokročilé vyhledávání a filtrování objektů (např. identit, účtů, rolí) podle jakéhokoliv atributu, včetně uživatelsky definovaných (vlastních) atributů, které byly do systému přidány prostřednictvím rozšířeného schématu (schema-extension.xml). Tyto atributy se po správné konfiguraci stávají součástí datového modelu a jsou automaticky dostupné ve vyhledávacím rozhraní GUI i přes API.

ID	Požadavek	Způsob naplnění
118	IDM MUSÍ podporovat možnost jediné uživatelské identity v IDM i pro osoby mající více pracovních úvazků nebo jiných typů účtů ve zdrojových systémech. Zároveň IDM musí zjistit unikátnost každé spravované identity.	Požadavek je naplněn kompletně. midPoint umožňuje udržovat jednu centrální identitu pro osobu s více úvazky nebo účty, které jsou k ní přiřazeny pomocí pravidel. Systém zároveň zajišťuje unikátnost každé identity a při importu zjišťuje, zda má být účet spojen s existující identitou. Tím je zajištěna konzistence a přehlednost spravovaných identit.

Tabulka 25 – Atributy uživatelů

4.6.3 Oddělení komunit

Nabízené řešení musí podporovat oddělené komunity uživatelů. Řešení musí nabízet možnost nastavit tato omezení:

- Konfigurovat přístupová práva určená pro jednu komunitu tak, že nelze přiřadit identitám v jiné komunitě koncové systémy komunity původní;
- Do organizační struktury určené jedné komunitě nelze přiřadit identity z jiné komunity;
- Delegovat správu konkrétní komunity jinému administrátorovi;
- Delegovat správu konkrétní organizační struktury jinému administrátorovi.

ID	Požadavek	Způsob naplnění
119	IDM MUSÍ podporovat nastavení politik pro přidělování rolí a dalších objektů tak, aby šlo omezit, kdo dané přiřazení může získat.	Požadavek je naplněn kompletně. midPoint umožňuje omezit přidělování rolí a dalších objektů pomocí politik založených na pravidlech. Lze definovat, kdo může roli získat např. podle typu identity, organizační jednotky nebo jiného atributu. Tato pravidla se nastavují přímo v definici role.

Tabulka 26 – Politiky pro přidělování rolí a dalších objektů

4.6.4 Koncoví uživatelé

Nabízené řešení musí podporovat minimálně:

- Přehled přiřazených koncových systémů;
- Přehled přiřazených oprávnění (aplikačních rolí) na koncových systémech (pokud je nakonfigurováno);
- Přehled přiřazení do organizační struktury;
- Schvalování či zamítnutí vznesených požadavků.

ID	Požadavek	Způsob naplnění
120	IDM MUSÍ umožnovat přihlášení koncovým uživatelům, kde si budou moci zobrazit základní informace o svém účtu včetně zobrazení oprávnění, účtů v koncových systémech a správu vznesených požadavků.	Požadavek je naplněn kompletně. midPoint poskytuje samoobslužné rozhraní pro koncové uživatele. Uživatel si zde může zobrazit základní údaje o své identitě, přiřazené role, účty v koncových systémech a stav svých žádostí. Rozhraní podporuje i samoobslužné požadavky, jako je žádost o roli nebo reset hesla. Přístup je řízen podle přidělených oprávnění.

Tabulka 27 – Uživatelský profil

4.6.5 Definice rolí v IDM

Níže je uveden minimální seznam rolí, které musí být podporovány v rámci IDM nástroje:

- Administrátor IDM - Zasahuje do poloautomatických procesů, řeší výjimečné stavy, kontroluje reporting a flow identit, plně spravuje IDM. Může delegovat svá oprávnění a přidělovat oprávnění s granularitou až na jednotlivé funkce a objekty.
- Delegovaný administrátor, Delegovaný správce - Má administrátorská práva nad zvolenými komunitami, organizační strukturou, koncovými systémy, nad skupinami uživatelů nebo obecně nad definovanými objekty IDM. Účelem je umožnit delegovanému administrátorovi správu nad uživateli patřícími do samostatného podřízeného celku (ať už z pohledu interního, tak externího - například dodavatelské účty).
- Tvůrce business rolí - Má všechna nezbytná práva pro tvorbu a úpravu business rolí v IDM. Může do nich zařazovat jiné business role, aplikační role a/nebo koncové systémy.
- Přidělovatel rolí - Má všechna nezbytná práva pro přidělování business rolí a aplikačních rolí v IDM. Může identitám v IDM přidělovat business role, aplikační role a/nebo koncové systémy.
- Správce koncového systému - Má všechna nezbytná práva pro úpravu definic KS v IDM a jeho aplikačních rolí.
- Běžný uživatel - Běžný uživatel, který má práva prohlížet informace o své identitě a přidělených prostředcích v IDM.

ID	Požadavek	Způsob naplnění
121	IDM MUSÍ umožnovat detailní správu rolí definující oprávnění v rámci samotného IAM systému.	Požadavek je naplněn kompletně. midPoint umožňuje detailní správu rolí, které definují oprávnění přímo v rámci IDM systému. Lze nastavovat přístup k objektům, částem GUI i jednotlivým operacím. Oprávnění jsou řízena pomocí Role RBAC modelu (Role based access control) a lze je kombinovat s filtry a podmínkami. Tím je zajištěna bezpečná a flexibilní správa přístupů uvnitř IDM.

Tabulka 28 – Správa oprávnění v IAM

4.6.6 Organizační struktura

Nabízené řešení musí podporovat:

- Administrační webové rozhraní pro správu stromové struktury;
- Správu skrze integrační vrstvu;
- Možnost vytváření libovolného počtu stromů organizačních struktur;
- Možnost vytváření nezávislých entit (pracovní pozice, funkční místa) ve stromě;
- Možnost definovat atributy entit ve stromě;
- Možnost přiřazovat entitám ve stromě jiné objekty, minimálně uživatele, role, organizace z jiných stromů, účty v koncových systémech;
- Možnost vizualizace entit pomocí stromové struktury;
- Entity ve stromě přiřazovat k libovolnému objektu, minimálně k roli a k identitě;
- Identita nebo role může být přiřazena ve více entitách stromu zároveň;
- Identita nebo role může být přiřazena ve více stromech zároveň;
- Identita může mít různé role v různých strukturách (nadřízený v jedné organizační struktuře může být v jiné struktuře podřízený apod.);
- Možnost nastavit časové období od-do pro přiřazení identity do stromové struktury; pokud časové období uplyne nebo ještě nenastalo, nesmí se přiřazení identity do stromu uplatnit.

ID	Požadavek	Způsob naplnění
122	IDM MUSÍ nabízet administrační rozhraní (GUI) pro správu stromové struktury.	Požadavek je naplněn kompletně. midPoint nabízí administrační GUI pro správu organizační struktury ve stromovém zobrazení. Uživatelé s odpovídajícími oprávněními mohou vytvářet, upravovat a mazat organizační jednotky, včetně jejich hierarchie. Stromová struktura slouží také jako základ pro řízení přístupů, přiřazování rolí nebo schvalovací logiku. Strukturu lze spravovat ručně přes GUI nebo automatizovaně importovat ze zdrojového systému (např. HR). Pro každou jednotku je možné evidovat metadata, jako název, kód, typ či nadřízenou jednotku.
123	IDM MUSÍ nabízet správu organizační struktury prostřednictvím integrační vrstvy s možností volání funkcí prostřednictvím programového rozhraní (APl).	Požadavek je naplněn kompletně. midPoint umožňuje správu organizační struktury také prostřednictvím API. Veškeré operace jako vytvoření, úprava, mazání či načítání organizačních jednotek lze provádět přes standardizované REST rozhraní. API podporuje formáty JSON, XML i YML a je zabezpečeno autentizací a autorizací dle rolí. Tím je zajištěna snadná integrace s nadřazenými systémy (např. HR, ERP).
124	IDM MUSÍ umožňovat vytvářet libovolné počty stromů organizačních struktur.	Požadavek je naplněn kompletně. midPoint podporuje tvorbu více nezávislých stromů organizačních struktur. Každý strom může reprezentovat jiný pohled na organizaci (např. formální nebo projektový). Stromy jsou tvořeny objekty typu Org a lze je spravovat jak přes GUI, tak přes API. Tím je zajištěna flexibilita pro různé účely řízení přístupů či schvalování.
125	IDM MUSÍ umožňovat vytvářet nezávislé objekty ve stromě (pracovní pozice, funkční místa apod.).	Požadavek je naplněn kompletně. midPoint umožňuje vytvářet nezávislé objekty v rámci stromové struktury, jako jsou pracovní pozice, funkční místa

ID	Požadavek	Způsob naplnění
		nebo jiné specifické uzly. Tyto objekty jsou typu Org nebo Role a nemusí být pevně vázány na formální organizační jednotku. Lze je využít např. pro přiřazení identit a rolí.
126	IDM MUSÍ umožňovat definování atributů těchto objektů ve stromě.	Požadavek je naplněn kompletně. midPoint umožňuje definovat vlastní atributy pro objekty ve stromové struktuře. Atributy lze rozšířit pomocí schémat (schema extension) a následně je spravovat přes GUI i API. Tím lze každé organizační jednotce, pracovní pozici či funkčnímu místu přiřadit specifické informace jako kód, typ, lokalitu, kapacitu apod. Tyto atributy je možné využít i v politice přístupů, mapování či reportingu.
127	IDM MUSÍ umožňovat přiřazení nezávislých objektů organizačním jednotkám ve stromě – minimálně uživatele, role.	Požadavek je naplněn kompletně. midPoint umožňuje přiřazení různých typů objektů, jako jsou uživatelé nebo role, k libovolným uzlům ve stromové organizační struktuře. Tato vazba může být přímá nebo zprostředkovaná pomocí přiřazení (assignments). Přiřazení lze využít pro automatické přidělování oprávnění, řízení přístupů i schvalování.
128	IDM MUSÍ umožňovat vizualizovat entity pomocí stromové struktury.	Požadavek je naplněn kompletně. midPoint umožňuje vizualizaci organizační struktury a souvisejících entit ve formě stromového zobrazení. V přehledném GUI lze zobrazit hierarchii organizačních jednotek a jejich vazby na uživatele, role nebo funkční místa. Stromová struktura je interaktivní a umožňuje snadný pohyb a správu.
129	IDM MUSÍ umožňovat přiřazení identity nebo role do více stromů zároveň (např. uživatel může být ve více organizačních strukturách, v různém zařazení a s odlišnými oprávněními).	Požadavek je naplněn kompletně. midPoint podporuje přiřazení jedné identity nebo role do více organizačních struktur současně. Uživatel tak může být evidován v různých stromech (např. formálním a projektovém) s odlišným zařazením a přiřazenými oprávněními. Každé

ID	Požadavek	Způsob naplnění
		přiřazení může mít samostatná pravidla, platnost i vazbu na role.
130	IDM MUSÍ umožňovat nastavení časové období ,,od - do" pro přiřazení identity do stromové struktury. Pokud časové období uplyne nebo ještě nenastalo, je toto zařazení neaktivní.	Požadavek je naplněn kompletně. midPoint umožňuje nastavit časové období „od–do“ pro každé přiřazení identity ke stromové struktuře. Pokud je aktuální datum mimo stanovený rozsah, přiřazení je automaticky neaktivní. Toto chování platí i pro odvozená oprávnění nebo role navázané na dané zařazení. Systém tak podporuje dočasné nebo plánované zařazení identit.

Tabulka 29 – Organizační struktura

4.6.7 Business role

Nabízené řešení musí podporovat:

- Administrační webové rozhraní pro správu business rolí.
- Správu skrze integrační vrstvu.
- Evidenci business rolí, včetně popisných atributů.
- Business role musí být možné hierarchicky skládat.
- Vazbu business rolí na uživatele obsaženého v jakékoliv komunitě či organizační struktuře, označující garanta business role. Tato vazba může být v kardinalitě M:N ve smyslu hlavní garant, zástupce apod. Tato vazba je rozhodující ve workflow při přiřazování přístupů apod.
- Vazbu na koncové systémy přiřazené do business role v kardinalitě M:N.
- Vazbu na konkrétní identitu (uživatele) v kardinalitě M:N a možnost nastavení platnosti přiřazení od-do.
- Možnost nastavení platnosti business role od-do, pokud časové období uplyne nebo ještě nenastalo, nesmí se přiřazení business role uplatnit.
- Do business rolí přiřazovat jiné business role, aplikační role, resp. koncové systémy
- Podporovat definici pravidel pro automatizovanou správu členství business rolí včetně možnosti použít regulární výrazy.
- Správu efektivních práv v rámci tvorby nových business rolí.

ID	Požadavek	Způsob naplnění
131	IDM MUSÍ umožňovat zamítnout požadavek ve schvalovacím procesu s komentářem schvalovatele.	Požadavek je naplněn kompletně. midPoint umožňuje schvalovateli zamítnout požadavek v rámci schvalovacího workflow. Při zamítnutí může schvalovatel přidat komentář s odůvodněním.
132	IDM MUSÍ umožňovat definování povinných atributů rolí včetně kontroly jejich formátu.	Požadavek je naplněn kompletně. midPoint umožňuje definovat povinné atributy rolí a kontrolovat jejich formát. Validace se nastavují pomocí schématu a výrazů, např. pro kontrolu délky, povinnosti nebo vzoru (regex). Při vytváření nebo úpravě role systém ověřuje správnost údajů. Chybějící nebo nesprávné hodnoty znemožní uložení role.

Tabulka 30 – Požadavky na správu uživatelských rolí a jejich žádostí

4.6.8 Koncové systémy

Nabízené řešení musí podporovat:

- Administrační webové rozhraní pro správu koncových systémů.
- Správu přes integrační vrstvu.
- Evidenci koncových systémů, včetně popisného atributu jejich funkce, umístění apod.
- Vazbu koncových systémů na uživatele obsaženého v jakékoliv komunitě, či organizační struktuře, označující garanta koncového systému. Tato vazba může být v kardinalitě M:N ve smyslu hlavní garant, zástupce apod., může být realizována prostřednictvím role. Tato vazba je rozhodující ve workflow při vytváření business rolí, přiřazování přístupů apod.
- Vazbu na aplikační role přiřazené ke koncovému systému v kardinalitě 1:N.
- Vazbu na administrátora koncového systému, kterého může představovat uživatel obsažený v jakékoliv komunitě, či organizační struktuře. Tato vazba může být v kardinalitě M:N ve smyslu hlavní administrátor, zástupce apod. a může být realizována prostřednictvím role.
- Možnost nastavení stavu správy koncového systému na povoleno, či blokováno. Toto nastavení má přímý dopad na řízení přístupů ke koncovému systému.

ID	Požadavek	Způsob naplnění
133	IDM MUSÍ podporovat evidenci koncových systémů a správu přístupů k nim pomocí aplikačních rolí.	Požadavek je naplněn kompletně. midPoint umožňuje evidenci koncových systémů jako samostatných objektů včetně jejich atributů a stavu. Přístupy do těchto systémů jsou řízeny pomocí aplikačních rolí, které definují, jaká oprávnění se mají přiřadit. Role jsou navázané na konektor a odpovídající účty v systému.

Tabulka 31 – Koncové systémy

4.6.9 Aplikační role

Nabízené řešení musí podporovat:

- Administrační webové rozhraní pro správu rolí (soubor oprávnění).
- Správu skrze integrační vrstvu.
- Roli je možné přiřazovat koncovým systémům.
- Možnost nastavení platnosti aplikační role s dopadem na řízení přístupů ke koncovému systému.
- Možnost nastavit další atributy přiřazení (např. dle lokality identity).
- Možnost dynamického výpočtu u schvalovací role.
- Role musí být možné hierarchicky skládat.
- Možnost systému nastavit pravidla pro vzájemně se vylučující role (tzv. SoD), musí umět reportovat a notifikovat konfliktní práva.
- Ochranu systému v případě pokusu o přiřazení konfliktní role - pokud dojde k pokusu o přiřazení role identitě, která již má jinou konfliktní roli, musí systém konflikt oznámit a vlastní přiřazení neprovede.
- Možnost recertifikace rolí - opakované spouštění schvalování.

ID	Požadavek	Způsob naplnění
134	IDM MUSÍ obsahovat nástroj, který provádí recertifikaci přiřazení vazby identita - role a umožňuje tak v pravidelných intervalech spouštět přeschvalování existujících oprávnění (vazeb identita - role).	Požadavek je naplněn kompletně. midPoint obsahuje vestavěný nástroj pro recertifikaci vazeb identita–role. Umožňuje spouštět kampaně v definovaných intervalech, v jejichž rámci dochází k přezkoumání a opětovnému schválení existujících oprávnění.
135	Recertifikace MUSÍ umožňovat: • Automatické (plánované) spouštěné certifikace, • Ruční spouštění certifikace - tzv. na vyžádání, • Automatické akce při zamítnutí přístupu (např. při odebrání role), • Definovat rozsah recertifikací podle identit, rolí a organizační struktury, • Logovat (a reportovat) stavy kroků a výsledku recertifikace, • Spouštět neomezený počet současně běžících recertifikací, • Konfigurovat vícekrokové workflow s podporou eskalace a delegace.	Požadavek je naplněn kompletně. midPoint plně podporuje recertifikace s možností plánovaného i ručního spuštění. Rozsah lze definovat podle identit, rolí i organizační struktury a při zamítnutí lze nastavit automatické odebrání oprávnění. Podporováno je vícekrokové workflow s eskalací a delegací a paralelní běh více kampaní. Všechny kroky jsou logovány a reportovány. Konfigurace se provádí v objektu typu "Access Certification Campaign", dostupném přes GUI a API.
136	IDM MUSÍ umožnit recertifikovat obsah business rolí (vazbu na aplikační role).	Požadavek je naplněn kompletně. midPoint umožňuje recertifikaci obsahu business rolí, včetně jejich vazeb na aplikační role. Schvalovatelé mohou přezkoumat, zda má daná business role stále obsahovat konkrétní aplikační role. Výsledky lze využít k úpravě struktury rolí. Tato recertifikace se konfiguruje jako samostatná kampaň v GUI nebo přes XML.
137	IDM MUSÍ umožnit sledovat v reportech stavy recertifikací	Požadavek je naplněn kompletně.

ID	Požadavek	Způsob naplnění
	jednotlivých případů a rozhodnutí a reagovat na případné nestandardní stavy (např. neřešené recertifikace ke schválení).	midPoint umožňuje sledovat stav jednotlivých případů recertifikace v přehledných reportech. Zahrnují informace o rozhodnutích, časech schválení a identifikaci neřešených či zpožděných případů. Na nestandardní stavy lze navázat notifikace nebo eskalace. Stavy jsou dostupné v GUI i jako exportovatelné reporty ve formátu CSV/XML.

Tabulka 32 – Recertifikace oprávnění

4.6.10 Připojení koncových systémů

Zadavatel v rámci implementace požaduje připojení koncových systémů a propagaci unikátní identity.

Typické zpracování identity v IDM se sestává z následujících kroků:

- IDM přebírá informace o identitách z autoritativního zdroje a vytváří uživatele v IDM.
- Na základě rozlišovacích atributů uživatele slučuje do jedné unikátní identity, kterou nadále takto propaguje.
- Na základě rozlišovacích atributů ji přiřazuje do komunit, organizačních struktur.
- Na základě rozlišovacích atributů ji přiřazuje do business rolí. Business role lze přiřazovat i ručně administrátorem, který má potřebná oprávnění.
- Na základě business rolí jsou unikátní identitě přiřazeny koncové systémy a aplikační role v koncových systémech.

Následuje proces řízení identit v koncových systémech, který lze rozdělit do několika následujících bodů:

4.6.10.1 Plně automatické připojení

Plně automatické připojení ke koncovému systému splňuje tyto požadavky:

- IDM automaticky skrze konektory provádí akce spojené se správou autorizace v koncových systémech.
- IDM automaticky skrze konektory provádí pravidelnou kontrolu stavu účtů na koncových systémech s autoritativním vypořádáním nesouladu.

4.6.10.2 Read-only připojení

Read-only připojení ke koncovému systému splňuje tyto požadavky:

- IDM neprovádí automaticky správu autorizace v koncových systémech, ale pomocí notifikace informuje administrátory koncových systémů o přidělení úkolu.
- IDM automaticky skrze konektory provádí pravidelnou kontrolu stavu účtů na koncových systémech s autoritativním vypořádáním nesouladu.

4.6.10.3 Offline připojení

Offline připojení ke koncovému systému splňuje tyto požadavky:

- IDM neprovádí automaticky správu autorizace v koncových systémech, ale pomocí notifikace informuje administrátory koncových systémů o přidělení úkolu.
- IDM neprovádí automaticky kontrolu stavu účtů na koncových systémech, ale pomocí webového rozhraní a v rámci workflow procesu umožňuje administrátorovi potvrzení splnění přiděleného úkolu.
- Alternativně IDM může kontrolovat stav účtů vůči exportu z koncového systému, který je prováděný mimo IDM.

ID	Požadavek	Způsob naplnění
138	IDM MUSÍ umožňovat napojení externích systémů, a to v módu plně automatickém, read-only nebo offline.	Požadavek je naplněn kompletně. midPoint podporuje flexibilní připojení externích systémů v několika provozních režimech podle potřeb organizace. V plně automatickém režimu probíhá obousměrná synchronizace dat – např. vytváření účtů, aktualizace údajů a odebrání přístupů. V režimu read-only je možné data ze systému pouze číst a porovnávat s údaji v IDM, bez možnosti zápisu nebo změn. Offline režim slouží pro systémy bez přímého rozhraní – přenos probíhá například prostřednictvím importovaných souborů (CSV) nebo interně ve vlastním repozitáři. Každý systém se v midPointu reprezentuje jako objekt typu Resource, jehož konektor definuje způsob komunikace. V rámci tohoto objektu lze nakonfigurovat režim provozu, plán synchronizace, mapování atributů, transformační skripty i reakce na chyby. midPoint rovněž umožňuje měnit režim napojení v čase – např. dočasně vypnout zápis při výpadku systému. Všechny režimy podporují auditování operací, přehled stavu napojení a možnost rekonciliace.

Tabulka 33 – Připojení koncových systémů

4.6.11 Eskalace chyb a neplnění úkolů při správě autorizace v koncových systémech

Zadavatel požaduje konfigurovatelnou správu a eskalaci chyb při správě autorizace v koncových systémech.
IDM tak musí umožňovat nastavit tyto parametry:

- Pro plně automatické připojení
  - Počet opakování pokusů spojení s autoritativním zdrojem v určitém časovém intervalu.
  - Po vyčerpání všech určených neúspěšných pokusů vyvolání notifikace na administrátora IDM.
  - Počet opakování pokusů spojení s koncovým systémem skrze konektory v určitém časovém intervalu.
  - Po vyčerpání všech určených neúspěšných pokusů vyvolání notifikace na garanta koncového systému a administrátora IDM.
  - V rámci notifikace přenos chybové zprávy obdržené při neúspěšném spojení
  - a identifikaci akce, při které došlo k chybě.
- Pro Read-only připojení
  - Počet opakování pokusů spojení s autoritativním zdrojem v určitém časovém intervalu.
  - Po vyčerpání všech určených neúspěšných pokusů vyvolání notifikace na administrátora IDM.
  - Počet opakování pokusů spojení s koncovým systémem skrze konektory v určitém časovém intervalu.
  - Po vyčerpání všech určených neúspěšných pokusů vyvolání notifikace na garanta koncového systému a administrátora IDM.
  - V rámci notifikace přenos chybové zprávy obdržené při neúspěšném spojení
  - a identifikaci akce, při které došlo k chybě.
- Pro Offline připojení
  - Počet opakování pokusů spojení s autoritativním zdrojem v určitém časovém intervalu.
  - Po vyčerpání všech určených neúspěšných pokusů vyvolání notifikace na administrátora IDM.
  - V rámci notifikace přenos chybové zprávy obdržené při neúspěšném spojení
  - a identifikace akce, při které došlo k chybě.
  - Časový interval pro splnění úkolu, notifikovaného administrátorovi.
  - Počty a intervaly pro upozornění administrátorovi o nesplnění přiděleného úkolu, před vypršením termínu splnění úkolu.
  - Při nepotvrzení splnění úkolu a vypršení termínu splnění úkolu vyvolání notifikace na garanta koncového systému a administrátora IDM.

ID	Požadavek	Způsob naplnění
139	IDM MUSÍ v případě problémů při synchronizaci se zdrojovým nebo cílovým systémem zkusit opakovat akci později. V případě opakovaných neúspěchů musí kvantifikovat správce systému.	Požadavek je naplněn kompletně. midPoint umožňuje konfigurovat opakování akcí při chybách při synchronizaci se zdrojovým nebo cílovým systémem. Lze nastavit počet pokusů, časový interval mezi nimi a následné eskalační kroky. Po vyčerpání opakování systém odešle notifikaci s detailní chybovou zprávou a informací o neúspěšné akci administrátorovi IDM a/nebo garantovi systému. Tato logika se nastavuje v konfiguraci synchronizačních úloh a konektorů pomocí parametrů retry policy a notifikací.
140	IDM MUSÍ v podporovat notifikace i pro případ, kdy je synchronizace prováděna manuálně administrátory na základě přiřazených úkolů. MUSÍ být možné nastavit, jak často má docházet k notifikaci na základě stavu úkolu.	Požadavek je naplněn kompletně. Lze nastavit pravidelné upozornění podle stavu úkolu, např. pokud není dokončen v definovaném čase. Notifikace může být opakovaná s nastavením intervalu a cílové osoby. Konfigurace se provádí v plánovači úloh a šablonách notifikací.

Tabulka 34 – Zpracování chyb synchronizace

4.7 Integrace IDM

ID	Požadavek	Způsob naplnění
141	V rámci implementace MUSÍ být IDM integrováno na následující informační systémy způsobem, kdy IDM převezme správu veškerých identit a řízení veškerých uživatelských rolí v těchto informačních systémech za využití odpovídajících standardizovaných rozhraní těchto systémů: • Microsoft Active Directory – dle specifikace společnosti Microsoft, • Emailový server Exchange – IDM MUSÍ zajistit napojení	Požadavek je naplněn kompletně. midPoint bude integrován s Active Directory a Microsoft Exchange pomocí standardizovaných konektorů. IDM převezme plnou správu identit, účtů a rolí v těchto systémech, včetně automatického zakládání, úprav a rušení účtů. Pro Exchange bude zajištěna správa schránek a zařazení uživatelů do skupin. Integrace využívá konektory založené na AD/LDAP.

ID	Požadavek	Způsob naplnění
	na stávající emailový server Microsoft Exchange, v rámci kterého bude automaticky spravovat mailové schránky uživatelů a zařazení těchto uživatelů do komunikačních skupin.	
142	IDM MUSÍ podporovat automatické procesy s integrací do dalších systémů spojené s příchodem nového zaměstnance: 1. Údaje o novém zaměstnanci jsou zadány do personálního systému, 2. IDM si načte data o novém zaměstnanci a ověří jeho pracovní zařazení, 3. Dle pracovní pozice a organizační jednotky vybere vhodné role, 4. Na základě rolí IDM vytvoří záznam v adresářovém systému (LDAP), vytvoří schránku elektronické pošty s jedinečnou e-mailovou adresou, přidělí přístupy do aplikací a systémů.	Požadavek je naplněn kompletně. midPoint podporuje plně automatizovaný nástupní proces integrovaný s personálním systémem. Po načtení údajů o novém zaměstnanci ověří jeho zařazení a automaticky vybere role podle organizační jednotky a pracovní pozice. Na základě těchto rolí vytvoří účty v cílových systémech, jako je LDAP nebo Microsoft Exchange, včetně e-mailové schránky a přístupů do aplikací. Proces je realizován pomocí synchronizačních úloh, mapování a schvalovacích politik.
143	IDM MUSÍ podporovat automatické procesy s integrací do dalších systémů spojené s odchodem stávajícího zaměstnance.	Požadavek je naplněn kompletně. midPoint podporuje automatizovaný výstupní proces zaměstnance napojený na personální systém. Po zaznamenání odchodu deaktivuje identitu, zruší účty a odebere přidělené role v napojených systémech. Lze nastavit i postupné kroky, jako je zablokování účtů nebo archivace. Proces je řízen pomocí synchronizace, časových podmínek a schvalovacích pravidel.

Tabulka 35 – Požadavky na integraci IDM

4.7.1 Operace spojené s připojením do koncových systémů

Níže je uveden rozsah operací, které musí podporovat IDM ve vztahu k rozhraní koncového systému (KS) tak, aby mohly být řízeny uživatelské účty uložené v tomto koncovém systému. Je uveden maximální rozsah operací, které ale rozhraní koncového systému nemusí podporovat. Jedná se například o zplatnění/zneplatnění účtu, změna hesla apod. Konkrétní implementaci operací rozhraní koncového systému a jejich význam pro data určuje vlastník koncového systému. Jakékoliv operace nesmí být IDM vyžadovány ke své funkčnosti, jedná se o volitelnou možnost. U každého koncového systému bude v rámci analýzy rozhodnuto, zda a v jakém rozsahu budou operace s rolemi mezi IDM a koncovým systémem využity.

4.7.1.1 Vytvoření účtu

Systém IDM skrze konektor vytváří v koncovém systému nového uživatele a propaguje jeho unikátnost pomocí jedinečného identifikátoru. Dle typu uživatele a přiřazených rolí vytváří konkrétní přístupy. Vytvoření nového uživatele v koncovém systému tak může být například metodou „Create_user“, která musí splňovat tyto podmínky:

- IDM přenáší do koncového systému unikátní identifikátor.
- IDM, pokud je to vyžadováno vytváří dle firemních pravidel a politik nové heslo, které přenáší do koncového systému.
- IDM, pokud je to vyžadováno, vytváří dle firemních pravidel a politik nové uživatelské jméno, které přenáší do koncového systému.
- IDM přenáší do koncového systému všechny požadované atributy, jako jsou například: jméno, příjmení, uživatelské jméno apod.
- IDM notifikuje uživatele o vytvoření uživatelského jména a hesla a tyto informace mu zasílá na e-mail, nebo pomocí SMS brány na mobilní telefon. V případě, že uživatel nemá ani e-mail, ani telefon, nebo v jiném vhodném případě tyto informace zasílá přímému nadřízenému, který je identifikován skrze organizační strukturu.

4.7.1.2 Aktivace a deaktivace účtu

Systém IDM skrze konektor a pokud to koncový systém umožňuje, provádí aktivaci a deaktivaci konkrétního uživatele. K identifikaci používá přidělený unikátní identifikátor.

4.7.1.3 Čtení informací o účtu

Systém IDM skrze konektor a (pokud to koncový systém umožňuje) čte informace o zavedeném uživateli. Jedná se tak především o atributy, jako jsou například:

- Jméno
- Příjmení
- Uživatelské jméno
- Jiné atributy informačního charakteru, které se u jednotlivých koncových systémů mohou různit.

V žádném případě nelze touto metodou přenášet heslo uložené v koncovém systému, pokud koncový systém heslo ukládá.
Pro identifikaci účtu se výhradně používá jeho unikátní identifikátor.

4.7.1.4 Update informací účtu

Systém IDM skrze konektor umožňuje aktualizovat zadané informace v koncových systémech. Jedná se o shodné atributy, které jsou přenášeny v rámci metody vytváření účtu, a tato metoda může obsahovat i změnu hesla.
Pro identifikaci účtu se výhradně používá jeho unikátní identifikátor.

4.7.1.5 Přiřazení aplikačních rolí

Systém IDM skrze konektor umožňuje přiřazení aplikačních rolí unikátní identitě. Jedná se o metodu, skrze kterou se předává ID unikátní identity a unikátní ID aplikační role. Na základě volání této metody koncový systém přiřazuje aplikační roli unikátní identitě a vrací odpověď o úspěšném, či neúspěšném provedení operace.

4.7.1.6 Odebrání aplikačních rolí

Systém IDM skrze konektor umožňuje odebrání aplikačních rolí unikátní identitě. Jedná se o metodu, skrze kterou se předává ID unikátní identity a unikátní ID aplikační role. Na základě volání této metody koncový systém odebírá aplikační roli unikátní identitě a vrací odpověď o úspěšném, či neúspěšném provedení operace.

4.7.1.7 Odebrání všech aplikačních rolí

Systém IDM skrze konektor umožňuje odebrání všech aplikačních rolí unikátní identitě. Jedná se o metodu, skrze kterou se předává ID unikátní identity. Na základě volání této metody koncový systém odebírá všechny aplikační role unikátní identitě a vrací odpověď o úspěšném či neúspěšném provedení operace.

4.7.1.8 Seznam přiřazených aplikačních rolí

Systém IDM skrze konektor umožňuje čtení informací o všech přiřazených aplikačních rolích unikátní identitě. Jedná se o metodu, skrze kterou se předává ID unikátní identity. Na základě volání této metody koncový systém vrací seznam všech přiřazených aplikačních rolích unikátní identitě a vrací odpověď o úspěšném či neúspěšném provedení operace.

4.7.1.9 Seznam aplikačních rolí

Systém IDM skrze konektor umožňuje čtení informací o aplikačních rolích v koncovém systému. Na základě volání této metody koncový systém vrací seznam aplikačních rolí v koncovém systému.

4.7.1.10 Seznam uživatelů v koncovém systému

Systém IDM skrze konektor umožňuje čtení informací o všech uživatelích (unikátních identitách), které jsou v koncovém systému zavedeny. Na základě volání této metody koncový systém vrací seznam všech unikátních identit, které jsou v systému zavedeny, spolu se všemi dostupnými atributy. Seznam těchto atributů se může lišit v závislosti na konkrétním koncovém systému.

ID	Požadavek	Způsob naplnění
144	IDM MUSÍ v integrovaných systémech podporovat CRUD operace pro všechny objekty (např. uživatelé a skupiny), které jsou pro danou integraci podporovány.	Požadavek je naplněn kompletně. midPoint podporuje plný rozsah CRUD operací (Create, Read, Update, Delete) nad objekty, které daný koncový systém umožňuje spravovat – typicky uživatelé, skupiny nebo aplikační role. Operace jsou realizovány prostřednictvím konektorů, přičemž konkrétní rozsah a význam operací je přizpůsoben rozhraní cílového systému. Každý konektor lze konfigurovat tak, aby respektoval schopnosti systému a umožnil přesné řízení synchronizace a přenosu dat.
145	IDM MUSÍ podporovat správu vztahů mezi takto spravovanými objekty (např. členství ve skupině).	Požadavek je naplněn kompletně. midPoint umožňuje správu vztahů mezi objekty, jako je například členství ve skupinách, přiřazení rolí nebo vztahy mezi identitami a organizačními jednotkami. Vztahy mezi objekty jsou řízeny pomocí specifických operací, které zajišťují synchronizaci a aktualizaci těchto vztahů v koncových systémech. Všechny tyto vztahy jsou spravovány prostřednictvím konektorů a mohou být automatizovány v rámci pravidel synchronizace.
146	IDM MUSÍ podporovat nastavení a změny hesel a také aktivačního stavu u spravovaných objektů, kde je to podporováno integrovaným systémem.	Požadavek je naplněn kompletně. midPoint podporuje nastavení a změny hesel, stejně jako správu aktivačního stavu u spravovaných objektů, pokud to integrovaný systém umožňuje. U objektů, jako jsou uživatelé, lze pomocí konektorů provádět operace jako reset hesla, změna hesla nebo aktivace/deaktivace účtů. Konkrétní implementace těchto operací závisí na rozhraní a možnostech cílového systému a jsou konfigurovány v parametrech konektorů.

Tabulka 36 – Požadované funkčnosti integrace s koncovými systémy

4.8 Požadavky na integrační rozhraní

ID	Požadavek	Způsob naplnění
147	IDM MUSÍ poskytovat standardizované rozhraní webových služeb pro programové napojení dalších informačních systémů FS. Toto rozhraní bude dodáno včetně jeho dokumentace, která bude určena k přímému poskytnutí dalším dodavatelům za účelem napojení se na toto rozhraní. Rozhraní a jeho konfigurace musí být součástí plnění na takové úrovni, že napojení nového informačního systému bude možné pouze za zapojení pracovníka zadavatele, který provede konfiguraci rozhraní na straně IDM a dodavatele nového IS, který provede konfiguraci dle dodané dokumentace na straně nového IS, tedy vše bude možné bez aktivního zapojení dodavatele IDM.	Požadavek je naplněn kompletně. midPoint poskytuje standardizované webové služby pro integraci s dalšími informačními systémy. Tato rozhraní jsou založena na REST protokolu, s dokumentovanými specifikami.
148	Základní konfigurace přístupu k webovým službám MUSÍ být dostupná z grafického rozhraní IDM.	Požadavek je naplněn kompletně. midPoint umožňuje základní konfiguraci přístupu k webovým službám přímo z grafického rozhraní. Administrátor může definovat a spravovat přístupové politiky, autentizaci, autorizaci a koncové systémy pro webové služby.
149	Rozhraní IDM MUSÍ poskytovat minimálně následující služby: • Získání organizační struktury, • Získání hierarchie systemizovaných míst, • Získání seznamu identit, • Získání nadřízené osoby pro daného zaměstnance, • Získání seznamu rolí pro daného zaměstnance, včetně případné informaci o delegaci role, • Zápis seznamu rolí uživatele do IDM, • Historie uživatele a jeho oprávnění k datu uvedeném	Požadavek je naplněn kompletně. midPoint poskytuje webové služby, které umožňují přístup k uvedeným informacím. Mezi dostupné služby patří získání organizační struktury, hierarchie systemizovaných míst, seznamu identit, rolí a pracovních pozic, stejně jako zápis rolí, certifikátů a změn identit. Služby také umožňují získat nadřízenou osobu pro zaměstnance, historii uživatele a jeho oprávnění k určitému datu, a seznam uživatelů a pracovních pozic přiřazených aplikaci. Tato rozhraní jsou součástí API.

ID	Požadavek	Způsob naplnění
	v parametru, • Získání seznamu uživatelů dané aplikace, • Získání seznamu pracovních pozic / funkcí přiřazených dané aplikaci, • Zápis certifikátů do IDM, • Zápis a změna identit.	
150	IDM MUSÍ umožnit vstupně/výstupní synchronizace do připojených systémů. Typy synchronizací: • Plná, • 1 identita (možnost synchronizovat pouze 1 identitu bez nutnosti pouštět plnou nebo změnovou synchronizaci), • Změnová (pokud to napojený systém umožní).	Požadavek je naplněn kompletně. midPoint podporuje různé typy synchronizací do připojených systémů, včetně plné synchronizace, synchronizace jedné identity a změnové synchronizace. Plná synchronizace provádí kompletní synchronizaci všech dat mezi IDM a cílovým systémem. Synchronizace jedné identity umožňuje aktualizovat pouze specifickou identitu bez nutnosti spouštět celkovou synchronizaci. Změnová synchronizace je podporována, pokud to napojený systém umožňuje, a synchronizuje pouze změny od poslední synchronizace. Tyto synchronizace jsou konfigurovány prostřednictvím konektorů a plánovače úloh v grafickém rozhraní IDM.
151	Plná a změnová synchronizace MUSÍ umožňovat naplánované i ruční spuštění synchronizace, synchronizace 1 identity musí umožňovat pouze ruční spuštění. Dále musí existovat možnost (trvale nebo dočasně) vyřadit identitu ze synchronizace s daným systémem.	Požadavek je naplněn kompletně. midPoint umožňuje jak naplánované, tak ruční spuštění plné a změnové synchronizace. Synchronizace jedné identity je dostupná pouze pro ruční spuštění, což umožňuje flexibilní správu jednotlivých identit. Dále je možné trvale nebo dočasně vyřadit identitu ze synchronizace s daným systémem, což se provádí nastavením parametru v konfiguraci "stínu" identity. Tyto možnosti správy synchronizace jsou dostupné přes grafické rozhraní midPointu.
152	Jednotlivé průběhy synchronizací MUSÍ být logovány.	Požadavek je naplněn kompletně.

ID	Požadavek	Způsob naplnění
	• Log plné synchronizace musí obsahovat odkazy na objekty, které byly synchronizovány a informace, co bylo u těchto objektů změněno v synchronizovaném systému, • Log změnové synchronizace musí obsahovat informace o události, která změnovou synchronizaci vyvolala + informace požadované v logu plné synchronizace.	midPoint loguje všechny průběhy synchronizací, včetně plné a změnové synchronizace. Log plné synchronizace obsahuje odkazy na synchronizované objekty a detailní informace o změnách, které byly provedeny v cílovém systému. U změnové synchronizace je log navíc doplněn o informace o události, která synchronizaci vyvolala, a stejné detaily jako v logu plné synchronizace. Logy jsou dostupné prostřednictvím GUI a lze je exportovat pro auditní účely.
153	IDM MUSÍ umožnit publikaci objektů (osob, účtů, skupin, funkcí, org. jednotek...) informačním systémům přes datové rozhraní (API IDM) na principu webových služeb. Toto API IDM MUSÍ tedy mít čtecí metody a ideálně by mělo mít i zápisové metody (součást kvalitativního hodnocení). V rámci čtecích metod MUSÍ mít dané API IDM i autentizační metody, umožňující ověřit identitu (její login/heslo) i pro potřeby třetích aplikací. IDM MUSÍ mít historii volání API IDM z důvodu auditu (součást kvalitativního hodnocení), včetně možnosti omezit dané API IDM pro jednotlivé aplikace (pouze vydefinované metody API IDM pro potřeby dané aplikace).	Požadavek je naplněn kompletně. midPoint poskytuje webové služby (API) pro publikaci objektů jako jsou osoby, účty, skupiny, organizační jednotky a funkce pro externí informační systémy. API zahrnuje čtecí metody pro získání těchto objektů a ideálně i zápisové metody pro jejich správu. Součástí API jsou autentizační metody pro ověření identity (login/heslo), což umožňuje integraci s třetími aplikacemi. Všechny volání API jsou logována pro auditní účely a je možné omezit přístup k API pouze na vydefinované metody pro specifické aplikace.
154	IDM MUSÍ poskytovat všechny služby API prostřednictvím integrační platformy integrovaného datového rozhraní. IDM MŮŽE poskytovat služby vybraným informačním systémům FS přímo, pokud jsou vybaveny standardně dodávaným a podporovaným adaptérem.	Požadavek je naplněn kompletně. midPoint poskytuje všechny služby API prostřednictvím integrační platformy integrovaného datového rozhraní, které zajišťuje centralizovanou správu a přístup k datům. Pro některé vybrané informační systémy FS může midPoint poskytovat služby přímo, pokud jsou tyto systémy vybaveny standardními a podporovanými adaptéry, které umožňují přímou integraci.

Tabulka 37 – Požadavky na integrační rozhraní

5 POŽADAVKY NA AM

Požadavkem Zadavatele je vybudování Autentizační infrastruktury (označováno taktéž jako Access management). Dodavatel v rámci svého plnění provede analýzu, která bude analyticky popisovat tyto oblasti:

1. Aktéři autentizační infrastruktury (osoby přistupující k autentizační infrastruktuře).
2. Způsoby autentizace přistupujících osob nejen interními prostředky, ale i prostřednictvím externích poskytovatelů identity, zejména Identita občana (NIA) a JIP/KAAS (Jednotný identitní prostor / Katalog autentizačních a autorizačních služeb).
3. Způsob tvorby identit a jejich uložení v prostředí Zadavatele. V případě, že se osoba bude moci autentizovat prostřednictvím externích poskytovatelů identity, je nutné spravovat identifikátory těchto identit externích poskytovatelů v systémech Zadavatele (ve správě identit).
4. Změny v legislativě – v posledních letech bylo v oblasti kybernetické bezpečnosti a autentizační infrastruktury vydáno množství legislativního i nelegislativního materiálu, revize by měla zahrnout zejména tyto:

    - Zákon č. 181/2014 Sb., o ZoKB, ve znění pozdějších předpisů, který zmiňuje zejména oblast KII a způsob jejího provozu; a vyhláška č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti), ve znění pozdějších předpisů.
    - Podmínky stanovené Odborem hlavního architekta eGovernmentu (dále jen OHA) a dalších požadavků souvisejících s provozem a implementací Informačních systémů veřejné správy (ISVS) zejména v oblasti způsobu autentizace uživatelů s využitím v současné době požadovaných prostředků, které postupně nahrazují, případně doplňují, stávající způsoby přihlášení – čistě jménem a heslem.
    - Dokument INFORMAČNÍ KONCEPCE ČR 2018+, Implementační plán hlavního cíle č. 3 - IK ČR který popisuje rozvoj celkového prostředí podporujícího digitální technologie a budování/provoz klíčových systémů eGovernmentu, zejména kapitola IK ČR 3.06 Zavedení systému důvěryhodné elektronické identifikace do praxe, která hovoří nejen o elektronické identifikaci občanů, ale i o elektronické identifikaci úředníků prostřednictvím a zástupců právnických osob.
    - Přístupy k autentizační infrastruktuře a použití autentizačních protokolů (SAML2, OIDC, OAuth).

ID	Požadavek	Způsob naplnění
155	IAM MUSÍ poskytovat funkčnosti pro Access Management (AM), s funkcí automatického přihlášení (SSO) oproti LDAP/AD pro interní uživatele, respektive oproti IdP pro externí uživatele.	Požadavek je naplněn kompletně. CAS poskytuje funkcionality Access Management (IdP) s funkcí jednotného (automatického) přihlášení (SSO). CAS poskytuje SSO mezi aplikacemi integrovanými k CAS (SeP). CAS poskytuje autentizační konektory pro různé protokoly, včetně konektoru LDAP/AD, kdy CAS v rámci autentizace uživatele ověřuje autentizační informace (uživatelské jméno a heslo) vůči LDAP/AD serverům.
156	AM MUSÍ v rámci SSO podporovat ověření uživatele na základě jeho ověření vůči doméně v rámci Active Directory, které uživatel provádí při přihlášení do uživatelského účtu počítače, který je v doméně zaregistrován.	Požadavek je naplněn kompletně. CAS podporuje v rámci přihlášení uživatele automatickou autentizaci prostřednictvím SPNEGO/Kerberos protokolu. Tato autentizace ve spolupráci s webovým prohlížečem uživatele a AD, se kterým CAS komunikuje prostřednictvím Kerberos autentizačního konektoru, umožňuje automatické přihlášení pod doménovým uživatelským účtem, pod kterým je uživatel přihlášen do OS počítače, ve kterém je webový prohlížeč spuštěn.
157	AM MUSÍ poskytovat funkčnosti pro dynamické řízení přístupů uživatelů dle různých autentizačních kontextů/scénářů (např. uživatel se hlásí z vnitřní sítě vs. uživatel se hlásí vzdáleně).	Požadavek je naplněn kompletně. CAS umožňuje definovat autentizační politiky. Prostřednictvím těchto autentizačních politik je možné definovat různé autentizační scénáře. Do podmínek autentizačních politik mohou vstupovat informace o přistupujícím uživateli (IP adresa, http hlavičky, čas přístupu, lokace), informace o aplikaci, do které uživatel přistupuje, případně další dostupné informace. Autentizační politika pak specifikuje způsob autentizace uživatele, např. zda se použije SPNEGO autentizace, formulářová (LDAP) autentizace nebo delegovaná autentizace a jaký se

ID	Požadavek	Způsob naplnění
		použije autentizační poskytovatel/konentor. Jednodušší autentizační politiky se definují prostřednictvím konfigurace.
158	AM MUSÍ poskytovat funkčnosti pro vícefaktorové ověřování uživatelů. AM MUSÍ umožnit stanovit povinnost autentizace pomocí více faktorů pro vybranou skupinu uživatelů nebo pro určit typ autentizace (např. vynucení dalších faktorů při přístupu uživatele z prostředí Internetu).	Požadavek je naplněn kompletně. CAS podporuje vícefaktorovou autentizaci (MFA). CAS podporuje některé běžné protokoly/poskytovatele MFA: SMS, e-mail, YubiKey, Radius, Google Authenticator, FIDO2, případně je možné programově přidat konektor na jiný protokol / jiného poskytovatele MFA. V rámci autentizačních politik (viz naplnění předchozího požadavku 157) je možné specifikovat i politiky MFA. Do podmínek těchto autentizačních politik mohou vstupovat informace o přistupujícím uživateli (IP adresa, http hlavičky, čas přístupu, lokace), atributy autentizovaného uživatele, informace o aplikaci, do které uživatel přistupuje, případně další dostupné informace. Jednodušší autentizační politiky se definují prostřednictvím konfigurace. Složitější autentizační politiky je možné definovat prostřednictvím skriptovacího jazyka, tím je zajištěna velká flexibilita v definici autentizačních politik. V rámci definice autentizačních politik je možné specifikovat nejen jaká MFA bude použita, ale i tzv. MFA bypass – tj. podmínky, kdy naopak nebude MFA požadována. CAS podporuje i tzv. důvěryhodná zařízení, kdy po MFA není po definovanou dobu, pro uživatele a zařízení, ze kterého se přihlašoval, vyžadována opětovná MFA.
159	AM MUSÍ poskytovat pro napojené koncové systémy služby IdP (NIA, JIP/KASS), identifikaci a následně zabezpečuje službu autentizace.	Požadavek je naplněn kompletně. CAS podporuje v rámci autentizačních scénářů i delegovanou autentizaci. V rámci delegované autentizace CAS vystupuje vůči

ID	Požadavek	Způsob naplnění
		externím IdP (NIA, JIP/KAAS) jako SeP. CAS jako SeP podporuje protokoly SAML 2.0, OIDC/OAuth, WS-Federation a tudíž je možné ho napojit na libovolného IdP podporujícího tyto protokoly (NIA, CAIS, Bank iD, MojeID, atd.). CAS podporuje i implementaci vlastního autentizačního modulu/protokolu pro delegovanou autentizací. V rámci této podpory byla přidána do CAS možnost delegované autentizaci vůči JIP/KAAS, který používá proprietární způsob autentizace za podpory SOAP protokolu.
160	AM MUSÍ poskytovat pro napojené koncové systémy služby autorizace přístupu.	Požadavek je naplněn kompletně. CAS umožňuje globálně i v rámci konfigurace jednotlivých integrovaných koncových systémů (SeP) definovat autorizační (přístupové) politiky. Tyto politiky umožňují definovat podmínky autorizace přístupu. Do podmínek těchto autorizačních politik mohou vstupovat informace o přistupujícím uživateli (IP adresa, http hlavičky, čas přístupu, lokace), atributy autentizovaného uživatele a další informace získané z jiných systémů (SCIM, Heimdall, OpenFGA, Cerbos, Premit.io, Permify, Open Policy Agent, http, REST, Time, …). Složitější autorizační politiky je možné definovat prostřednictvím skriptovacího jazyka, tím je zajištěna velká flexibilita v definici autentizačních politik.
161	AM MUSÍ poskytovat pro napojené koncové systémy informace o aktuálně přihlášeném uživateli ve formě uživatelského profilu.	Požadavek je naplněn kompletně. CAS v rámci standardních autentizačních protokolů OIDC/OAuth, SAML 2.0, WS-Federation poskytuje atributy přihlášeného uživatele integrovaným aplikacím (SeP). U OIDC/OAuth protokolu se jedná o tzv. Claims, u SAML protokolu se jedná o Assertion attribute statements. Případně protokoly specifikují služby, prostřednictvím kterých je možné atributy získat: např.

ID	Požadavek	Způsob naplnění
		OIDC/OAuth služba user-info nebo SAML 2.0 služba AttributeQuery. V rámci konfigurace CAS se specifikují zdroje uživatelských atributů (LDAP, RDBMS, NoSQL DB, REST, SCIM, MS Entra, JSON, …), v rámci autentizační politiky se specifikují zdroje, které jsou v rámci dané politiky použity, v rámci konfigurace SeP se pak specifikují atributy, které jsou této aplikaci předány. Primárním zdrojem atributů bude IDM. V rámci OIDC/OAuth protokolu je možné definovat sady atributů/claims pomocí tzv. scopes, v rámci SAML 2.0 protokolu je pak možné v žádosti o autentizaci specifikovat výčet požadovaných atributů, případně dodatečně vyžádat další atributy. Atributy musí být v rámci konfigurace SeP povoleny.
162	AM MUSÍ zaznamenávat čas posledního přihlášení uživatele do napojených koncových systémů.	Požadavek je naplněn kompletně. Standardně AM (IdP) nezaznamenává čas posledního přihlášení uživatele do integrované aplikace SeP, obecně autentizační protokoly toto neumožňují. Informace o posledním přihlášení uživatele může být přítomna jako atribut uživatele předaný SeP, který si tuto hodnotu uloží. Případně v rámci událostí CAS je možné tuto událost (přihlášení uživatele) či další události propagovat do požadovaných (napojených) systémů prostřednictvím standardního rozhraní (REST, HTTTP, WS, …) nebo prostřednictvím auditních záznamů např. protokolem syslog či jiným do SIEM či jiného systému.
163	AM MUSÍ poskytovat služby autentizace pro napojené koncové systémy.	Požadavek je naplněn kompletně. CAS poskytuje službu autentizace (IdP) integrovaným aplikacím prostřednictvím standardních autentizačních protokolů OIDC/OAuth, SAML, WS-Federation. Autentizace probíhá zpravidla tak, že integrovaná aplikace provede přesměrování

ID	Požadavek	Způsob naplnění
		uživatele ve webovém prohlížeči na CAS s žádostí o autentizaci ve formě požadované zvoleným autentizačním protokolem (OIDC/OAuth, SAML 2.0, WS-Federation). CAS provede autentizaci uživatele dle aktuální autentizační politiky (pokud již není přihlášen v rámci SSO), získá atributy uživatele a provede autorizaci přístupu uživatele do dané aplikace. V případě úspěšného vyhodnocení provede přesměrování uživatele zpět do integrované s atributy uživatele a informacemi ve formě definované zvoleným autentizačním protokolem.
164	AM MUSÍ poskytovat funkčnost Single LogOut pro odhlášení se ze všech systémů, které Single LogOut podporují	Požadavek je naplněn kompletně. CAS podporuje Single LogOut (SLO) ve dvou režimech Frontend channel logout, který je realizován AJAX voláním z odhlašovací stránky CASu a Backend channel logout, který je realizována backend voláním integrované aplikace. Každá aplikace může používat jinou metodu. Pokud je SLO povoleno, je při odhlášení uživatele nebo při expiraci SSO session spuštěn SLO mechanismus, který odhlásí uživatele ze všech aplikací, do kterých se v rámci této SSO session přihlásil. V případě expirace SSO session je technicky možné zavolat pouze integrované aplikace metodou Backend channel logout.
165	AM MUSÍ poskytovat funkčnost automatického odhlášení v rámci AM při nečinnosti uživatele, tak aby se uživatel nemohl přihlásit do napojených systému bez provedení nového autentizačního procesu.	Požadavek je naplněn kompletně. V případě expirace SSO session je spuštěno jednotné odhlášení (SLO) nad danou session, tj. je provedeno odhlášení uživatele ze všech aplikací, do kterých se v rámci této SSO přihlásil. Vzhledem k tomu, že SLO je prováděn bez účasti prohlížeče uživatele, je možné provést pouze Backend channel logout.
166	AM MUSÍ poskytovat možnost přepnutí se mezi účty uživatele.	Požadavek je naplněn kompletně. CAS podporuje tzv. impersonaci. Po přihlášení uživatele

ID	Požadavek	Způsob naplnění
		(identity), v případě, že se uživatel může „přepnout“ za jiný uživatelský účet, je uživateli nabídnut seznam účtů, za které se může impersonovat (vydávat se za ně). Po zvolení vybraného účtu, jsou v rámci SSO předávány aplikacím atributy vybraného uživatelského účtu. V rámci auditního záznamu je patrné, jakou oficiální identitou se uživatel přihlásil a za jaký uživatelský účet se impersonoval. Přepnutí mezi různými účty musí proběhnout tak, že se uživatel odhlásí – tím dojde k odhlášení ze všech aplikací a opětovně se přihlásí a zvolí jiný účet.

Tabulka 38 – Autentizace

5.1 Systémové požadavky

- Podpora operačního systému Windows nebo Unix/Linux.
- Podpora kódování Unicode.
- Podpora Single sign on s možností konfigurace využívaného protokolu.
- Schopnost pracovat v režimu vysoké dostupnosti.

ID	Požadavek	Způsob naplnění
167	IAM MUSÍ podporovat operačního systém Windows nebo Unix/ Linux.	Požadavek je naplněn kompletně. CAS využívá čistě technologii Java JVM, tudíž není závislý na konkrétním OS, podporuje jak různé verze Windows, tak i různé distribuce a verze Linux.
168	IAM MUSÍ podporovat kódování Unicode.	Požadavek je naplněn kompletně. Java JVM standardně podporuje kódování Unicode stejně jako AM CAS na něm postavený.

ID	Požadavek	Způsob naplnění
169	IAM MUSÍ podporovat provoz v režimu vysoké dostupnosti a musí umožňovat škálování výkonnosti např. pomocí rozložení zátěže.	Požadavek je naplněn kompletně. CAS podporuje clustering (HA) prostřednictvím běhu více instancí systému. CAS může k distribuci dat mezi uzly používat různé technologie RDBMS, NoSQL DB, In memory DB. Vzhledem k tomu, že zvolená technologie musí běžet též v HA, je nejefektivnější a nejvýkonnější použití In memory DB, kdy jsou data distribuována přímo mezi uzly CASu. In memory DB je přímou součástí systému. Pro realizaci HA je nutné nasazení loadbalanceru, který provede terminaci TLS spojení a rozdělení požadavků na jednotlivé uzly CAS. Loadbalancer také musí umět detekovat nefunkční uzel. CAS v případě HA nasazení umožňuje bezvýpadkovou aktualizaci aplikace, kdy se provede postupné nasazení na jednotlivé uzly, v takovém případě nedojde ke ztrátě dostupnosti ani aktuálních SSO session.

Tabulka 39 – Systémové požadavky AM

5.2 Technické požadavky funkční a nefunkční

Řešení musí umožňovat/nabízet:

- Podporu kontextové autorizace založené na rozeznání:
  - Z jaké IP se dotyčný uživatel hlásí
  - Rozpoznaného typu zařízení
  - Na základě časového období např. v pracovní době
  - OS připojovaného zařízení
- Umožní uživateli, aby nebyl vyzván k dalšímu ověření, pokud jej dříve použil v konfigurovatelném časovém limitu nebo pro danou aplikační session
- Definovat typ vícefaktorového ověření dle kontextových podmínek
- Podporuje SSO pro cloudové aplikace, které podporují SAML, OIDC

ID	Požadavek	Způsob naplnění
170	AM MUSÍ poskytovat funkčnost pro připojení třetích aplikací pro federovanou autentizaci a autorizaci (komunikace mezi poskytovatelem identity /IdP/ a poskytovatelem služeb /SeP/) pomocí SAML 2.0 a OIDC protokolu. AM pak samo funguje v režimu IdP.	Požadavek je naplněn kompletně. CAS vystupuje v roli poskytovatele identity (IdP). Umožňuje integraci aplikací, vystupujících v roli poskytovatele služby (SeP), prostřednictvím standardních protokolů SAML 2.0, OIDC/OAuth, WS-Federation. CAS poskytuje integrovaným aplikacím služby autentizace a autorizace přístupu. CAS předává integrovaným aplikacím atributy přihlášeného uživatele.
171	AM MUSÍ podporovat model claims-based autentizace uživatelů s podporou standardů SAML 2.0 a WS-Federation a zajišťovat federaci identit z více interních a externích zdrojů – tedy spravovaných více IdP.	Požadavek je naplněn kompletně. CAS podporuje delegovanou autentizaci. V rámci delegované autentizace CAS vystupuje vůči externím IdP jako SeP. CAS jako SeP podporuje protokoly SAML 2.0, OIDC/OAuth, WS-Federation a tudíž je možné ho napojit na libovolného IdP podporujícího tyto protokoly. CAS delegovanou autentizací provádí claims-based autentizaci, kdy autentizuje uživatele na základě atributů identity získaných od externích zdrojů. Federace identit, tj. mapování identifikátorů identity z různých zdrojů je uloženo v interním zdroji atributů identity (IDM).
172	AM MUSÍ být schopna federovat jak interní identity tak identity externích IdP - povinně NIA a JIP/KAAS.	Požadavek je naplněn kompletně. CAS nabízí autentizaci interních a externích identit a jejich federaci. Autentizace interních identit je realizována prostředky CAS. Autentizace externí identit je provedena delegovanou autentizaci. V rámci delegované autentizace CAS vystupuje vůči externím IdP jako SeP. CAS jako SeP podporuje protokoly SAML 2.0, OIDC/OAuth, WS-Federation a tudíž je možné ho napojit na libovolného IdP podporujícího tyto protokoly. (NIA, CAIS, Bank iD, MojeID, …). CAS podporuje i implementaci vlastního autentizačního modulu/protokolu pro delegovanou autentizací.

ID	Požadavek	Způsob naplnění
		V rámci této podpory byla přidána možnost delegované autentizaci vůči JIP/KAAS, který má proprietární způsob autentizace a k vzájemné komunikaci používá SOAP protokol. Federace, tj. mapování identit je uloženo v IDM.
173	AM MUSÍ umožnit propojení externí identity s identitou interní. Uživatel může dle svých potřeb připojit nebo odpojit externí identity od svého účtu.	Požadavek je naplněn kompletně. Propojení interní a externí identity bude možné v uživatelském profilu IDM za podpory CAS. V IDM má uživatel ve svém profilu možnost připojení či odpojení již připojených externích IdP. Připojení proběhne tak, že IDM předá požadavek na získání externí identity uživatele u konkrétního externího poskytovatele identity na IdP CAS, CAS v roli SeP předá požadavek na získání identity uživatele externímu poskytovateli, externí poskytovatel předá identitu uživatele CAS a ten ji předá zpět IDM, který externí identitu přidá k uživateli.
174	AM MUSÍ být schopno zpracovat chybové odpovědi z autentizační brány externího IdP a relevantně propagovat chybové stavy vůči uživateli (tj. převádět chyby do srozumitelného dialogu uživateli).	Požadavek je naplněn kompletně. CAS zpracovává veškeré odpovědi a chybové stavy a příslušně na ně reaguje. Chyby se dělí na dvě skupiny business chyby a technické chyby. Business chyby jsou předány standardním komunikačním protokolem a zpravidla obsahují nějaký kód či popis chyby, v takovém případě je uživateli zobrazena příčina chyby. V případě technické chyby, která může nastat při komunikaci nebo při zpracování odpovědi se uživateli zobrazuje univerzální hláška o chybě při komunikaci s externím poskytovatelem.

Tabulka 40 – Technické požadavky AM

5.2.1 Podpora protokolů

- SAML 2.0
- OIDC
- WS-Federation

5.2.2 Bezpečnost

- Řešení používá standardy, postupy a technologie odpovídající současným bezpečnostním doporučením.
- Řešení musí podporovat vícefaktorovou autentizaci (používání čipových karet).
- Musí být implementována ochrana proti útokům hrubou silou, jako je např. automatické uzamčení účtu.
- Útočník nesmí být schopen získat uživatelská jména nebo jiné informace z procesu ověřování přihlašování.
- Automatické uzamčení nepoužívaných účtů po nastavené době nečinnosti.
- Vynucená změna hesla/PIN po uplynutí nastavené doby.
- Informace o kódu PIN uživatele nebo hesla musí být uložena zašifrovaně nebo být uloženy pouze otisky hesel.
- Systém musí podporovat vynucení silného PIN / hesla.
- Všechna připojení jsou šifrována, včetně synchronizace uživatele, ověření, protokolování.
- Řešení musí nabídnou upozorňování na klíčové události:
    - Alert na administrativní změny
    - Alert, když se administrativní účty zamknou
    - Alert na přidání autentizačního bodu-nodu
- Alert MUSÍ podporovat syslog UDP/TCP protokol a může mít podobu e-mailu nebo SMS.

ID	Požadavek	Způsob naplnění
175	AM MUSÍ podporovat vícefaktorovou autentizaci.	Požadavek je naplněn kompletně. CAS podporuje vícefaktorovou autentizaci (MFA). CAS podporuje některé běžné protokoly/poskytovatele MFA: SMS, e-mail, DuoSecurity, Radius, Google Authenticator, FIDO2, případně je možné programově přidat konektor na jiný protokol / jiného poskytovatele MFA. CAS umožňuje specifikovat na základě podmínek různé scénáře autentizačních politik včetně MFA. Do podmínek těchto autentizačních politik mohou vstupovat informace o přistupujícím uživateli (IP adresa, http hlavičky, čas přístupu, lokace), atributy autentizovaného uživatele, informace o aplikaci, do které uživatel přistupuje, případně další dostupné informace. Jednodušší autentizační politiky se definují prostřednictvím konfigurace. Složitější autentizační politiky je možné definovat prostřednictvím skriptovacího jazyka, tím je zajištěna velká flexibilita v definici autentizačních politik. V rámci definice autentizačních politik je možné specifikovat nejen jaká MFA bude použita, ale i tzv. bypass – tj. podmínky, kdy naopak nebude MFA požadována. CAS podporuje i tzv. důvěryhodná zařízení, kdy po MFA není po definovanou dobu, pro uživatele a zařízení, ze kterého se přihlašoval, vyžadována opětovná MFA.
176	AM MUSÍ implementovat ochranu proti útokům hrubou silou a zabránit v úniku informací (např. uživatelských jmen) útočníkům.	Požadavek je naplněn kompletně. CAS je zabezpečen na několika úrovních. CAS neuchovává data všech uživatelů, tudíž není možné, aby z CAS tyto informace unikly. CAS uchovává pouze informace o aktuálně přihlášených

ID	Požadavek	Způsob naplnění
		uživatelích v In memory DB v zašifrované podobě. Pokusy o autentizaci uživatelů jsou limitovány – po definovaném počtu neúspěšných pokusů o přihlášení v definovaném intervalu z jednoho zdroje dojde k zablokování možnosti přihlášení na definovanou dobu.
177	IAM musí podporovat nastavení politik pro spravovaná hesla a jiná tajemství, zahrnující jejich platnost a požadavky na kvalitu/ sílu.	Požadavek je naplněn kompletně. CAS umožňuje v rámci správy hesel definovat požadovanou politiku kvality hesla. Dále CAS podporuje uchovávání a validaci historie hesel. Hesla jsou fyzicky uložena v IDM případě ve zdrojových systémech (AD).
178	IAM musí podporovat notifikace klíčových událostí v systému.	Požadavek je naplněn kompletně. CAS podporuje zasílání notifikací o klíčových událostech v systému, zejména v rámci hodnocení rizikových událostí. CAS podporuje zasílání těchto notifikací prostřednictvím následujících kanálů/poskytovatelů: • e-mail: SMTP, SendGrid, MS Entra, Amazon SES, Mailjet, Mailgun • SMS: REST, Twilio, TextMagic, Clickatell, Amazon SNS, …, Groovy skript • notifikace: Google Firebase, Apple Push Nofification, Slack, • vlastní implementace.
179	IAM MUSÍ auditovat události spojené s autentizací a autorizací uživatelů a tento log musí být možné přenášet do SIEM systému pomocí syslog UDP/TCP protokolu.	Požadavek je naplněn kompletně. CAS má implementován systém pro zaznamenávání auditních událostí. Auditní události jsou důležité události v systému (úspěšné přihlášení, neúspěšné přihlášení, změna hesla, impersonace, odhlášení, přístup do aplikace, ….). V rámci auditní události jsou uchovávány ve strukturované podobě zásadní informace: IP adresa zdroje, user agent, datum a čas, typ události,

ID	Požadavek	Způsob naplnění
		uživatel (pokud je znám), data události (jsou specifická pro typ události). CAS podporuje několik technologií pro ukládání auditních událostí: syslog, soubor, RDBMS, Groovy, DynamoDB, MongoDB, Redis, REST, AWS Firehose.
180	IAM MUSÍ všechny události zasílat pomocí syslog UDP/TCP protokolu do SIEMu.	Požadavek je naplněn kompletně. CAS umožňuje zasílat prostřednictvím syslog protokolu nejen auditní události, ale i libovolné logové události. Logové a auditní záznamy jsou zpracovány prostřednictvím knihovny/nástroje Apache Log4j, kdy být zasílány prostřednictvím appendrů do souboru, do databáze, prostřednictvím syslog TCP/UDP do SIEMu a do dalších monitorovacích systémů.

Tabulka 41 – Požadavky na bezpečnost

5.3 Připojení koncových systémů

Součástí požadovaného řešení bude vybudování identitní brány, která bude zajišťovat příjem autentizací z externích identity providerů.

Hlavní cíle projektu na implementaci identitní brány do interních aplikací i aplikací třetích stran využívaných interními uživateli i externími spolupracujícími subjekty jsou v podobě:

- Standardizace autentizace nově realizovaných aplikací
- Napojení na informační systém pro správu a řízení identit pro přidělení autorizací
- Podpora autentizace vůči internímu způsobu ověřování (interní DB, interní systém)
- Podpora využití externí autentizační autority (NIA, JIP/KAAS, MojeID, BankID) pro autentizaci a identifikaci
- Podpora práce s LoA (level of assurance) evidovaném pro jednotlivé autentizační autority
- Vícefaktorové ověření pro zajištění bezpečného přístupu (vlastní či využití prostředků ověřených IdP – definované v rámci NIA)
- Harmonizace v přístupu k ověřování interních i externích uživatelů
- V případě souhlasu uživatele možnost čerpat dodatečné údaje od externího poskytovatele identity
- Evidence pokusů uživatelů o přihlášení do všech aplikací na jednom místě, včetně souhrnných reportů a logů možných předávat do systému SIEM
- Informace o aktuálně přihlášených uživatelích
- Jednotné přihlášení pro napojené aplikace (SSO) včetně možnosti nastavit interval přihlášení do napojených aplikací
- Řízení souhlasů uživatelů před předáním uživatelských dat a potvrzování podmínek užití
- Umožnění provozu v režimu vysoké dostupnosti (HA)

V případě napojení identitní brány na interní informační systém spravující identity uživatelů a současného propojení na externího poskytovatele identity lze od tohoto poskytovatele čerpat údaje o uživatelích a ty následně propagovat do interních záznamů identit. Vzorový scénář s využitím těchto propojení může vypadat následovně:

- Uživatel bez předchozího vztahu k internímu systému dostane pozvánku pro připojení se k aplikaci napojené na identitní bránu
- Při využití této pozvánky je uživatel přesměrován na identitní bránu
- Brána nabídne uživateli možnosti ověření identity proti externím poskytovatelům identit dle přednastavených možností (NIA, JIP/KAAS, MojeID, BankID)
    - Současně s požadavkem na ověření uživatele je na externího poskytovatele identity zaslána také žádost o poskytnutí údajů potřebných pro interní systém spravující identity uživatelů
- Uživatel se ověří dle výběru z nabízených možností a odsouhlasí poskytnutí údajů pro interní systém spravující identity uživatelů
- Údaje o uživateli poskytnuté od externího poskytovatele identit jsou odeslány do interního systému a uživateli je založena identita dle těchto údajů
    - V případě, že uživatel má již v interním systému vytvořenou identitu nebo některé zásadní identifikační údaje souhlasí s již vytvořenou identitou, tak je tato identita doplněna nově příchozími údaji

- Identitní brána povolí uživateli přístup do dané aplikace

ID	Požadavek	Způsob naplnění
181	AM MUSÍ umožnovat připojení aplikací, pro které bude poskytovat autentizaci. Podporované protokoly jsou SAML2, OIDC, http-header.	Požadavek je naplněn kompletně. CAS vystupuje v roli poskytovatele identity (IdP). Umožňuje integraci aplikací, vystupujících v roli poskytovatele služby (SeP), prostřednictvím standardních protokolů SAML 2.0, OIDC/OAuth, WS-Federation. CAS poskytuje integrovaným aplikacím služby autentizace a autorizace přístupu. CAS předává integrovaným aplikacím atributy přihlášeného uživatele. Http-header autentizace bude realizována ve spolupráci s F5 BIG-IP reverzní proxy s APM (Access Policy Manager), kterou zajistí GFŘ.
182	AM MUSÍ umožnit uživateli vybrat způsob ověření identity podle požadavků aplikace, kde aplikace může definovat povolené IdP nebo nastaví omezení podle LoA.	Požadavek je naplněn kompletně. V rámci konfigurace integrovaných aplikací (SeP) je možné specifikovat, jaké autentizační metody budou použity, případně jací jsou povolení externí poskytovatelé identity. V případě, že poskytovatel identity podporuje LoA (NIA), je možné specifikovat, jaké minimální LoA bude v rámci autentizace vyžadováno. Externí poskytovatel následně vybere pouze takové autentizační metody, které splňují minimální požadované LoA.
183	AM MUSÍ umožnit přihlašování interních uživatelů do služeb pro externí uživatele a obráceně.	Požadavek je naplněn kompletně. CAS bude rozdělen na externí a interní část, bude však sdílet repository tiketů, tj. externí uživatel bude smět (pokud bude mít oprávnění) přistoupit do aplikace integrované k internímu CAS a opačně.
184	AM MUSÍ podporovat zpracování atributů uživatele poskytovaných externími IdP.	Požadavek je naplněn kompletně. CAS v rámci delegované autentizace vystupuje v roli SeP vůči externím IdP a přebírá atributy vydané externí IdP. Tyto atributy pak může buď synchronizovat do místního úložiště, spojovat se stávajícími atributy na základě definované politiky a předávat

ID	Požadavek	Způsob naplnění
		integrovaným aplikacím (SeP).
185	AM MUSÍ podporovat vydávání harmonizované sady atributů včetně unikátního identifikátoru pro každou interní identitu.	Požadavek je naplněn kompletně. CAS umožňuje zpracovávat atributy uživatele z více zdrojů včetně atributů předaných od externího IdP a na základě definované politiky tyto atributy slučovat do jedné výsledné sady atributů autentizovaného uživatele. Tato sada základních atributů může být následně obohacena o další atributy v závislosti na integrované aplikaci, která o autentizaci žádá (do které uživatel přistupuje). V rámci konfigurace integrované aplikace se specifikuje množina atributů, které aplikace smí získat a dále je možné nad jednotlivými atributy specifikovat, jaké hodnoty se smí předávat (filtrování hodnot, transformace hodnot apod.).

Tabulka 42 – Požadavky na připojení koncových systémů AM

Aby bylo možné implementovat nástroj pro pokročilou autentizaci (SSO, případně MFA), bude nutné naplnit některé předpoklady. Jednou z hlavních podmínek zapojení konkrétních aktiv k užívání této autentizace, jak je předpokládána legislativou, je integrace s prostředky pro ověřování identity v systémech FS. Jedná se o jednotný způsob ověřování identity oproti AD. Tento projekt, tzn. úpravy jednotlivých systémů, již v naší organizaci probíhá a postupně jsou systémy upravovány tak, aby splňovaly požadavky na standardní ověřování – autentizaci s užitím technických prostředků autentizace prostřednictvím metod pokročilé kryptografie, avšak zatím bez možnosti užití více faktorů autentizace.

Jednotlivé systémy a aplikace lze z pohledu připravenosti a použitých technologií rozdělit do několika kategorií:

- Systémy, které splňují technologické požadavky a jsou po stránce strukturální a technické připraveny k užívání pokročilé autentizace. Tato skupina systémů je velmi malá a tyto systémy jsou zařazeny do první sady systémů, které budou napojeny v první vlně nasazení systému.
- Systémy, které splňují technologické požadavky a jsou po stránce strukturální připraveny k užívání pokročilé autentizace, ale po stránce technické ji nelze bez dalšího aplikovat řízeně v potřebném rozsahu. Tyto systémy bude nutné nejdříve upravit tak, aby bylo možné systém napojit k užívání pokročilé autentizace
- Systémy, které splňují technologické požadavky a nejsou po stránce strukturální připraveny k užívání pokročilé autentizace a po stránce technické je nelze připojit. Tyto systémy bude nutné nejdříve upravit tak, aby jejich struktura vyhovovala standardním bezpečnostním požadavkům a aby je bylo možné upravit k užívání pokročilé autentizace.
- Systémy, které nesplňují technologické ani strukturální požadavky a nelze je žádným způsobem zapojit k užívání pokročilé autentizace. Jedná se o staré legacy systémy, kde jejich stáří v některých případech přesahuje 20 let a u těchto systémů bude muset před napojením k užívání pokročilé autentizace předcházet analýza s následným vývojem a přechodem na nejnovější technologie a standardy tak, aby i tyto systémy bylo možné užívat společně s pokročilou autentizací.

Mezi významné vazby patří integrace s autorizačními funkcemi IDM a propojení se systémy řízení rolí a oprávnění.

6 POŽADAVKY na IAM

Požadavky v této kapitole se týkají celého IAM, platí tedy pro IDM i pro AM část řešení.

6.1 Licenční požadavky

Zadavatel požaduje, aby počet licencí byl bez omezení ve všech těchto aspektech:

1. Neomezené počty instancí produktu,
2. Neomezené počty uživatelů (15 tis. interních uživatelů, 1 mio externích uživatelů),
3. Neomezené počty koncových systémů,
4. Neomezené počty konektorů,
5. Neomezené počty procesorových jader, velikost paměti a jiných hardwarových, softwarových či aplikačních parametrů.

Zadavatel dále požaduje, aby byly licence územně neomezené a časově omezené na dobu trvání majetkových práv autorských k IAM.

Součástí dodávky je i předání kompletních zdrojových kódů včetně dokumentace.
Zadavatel požaduje možnost připojení budoucích nových koncových systémů a vložení jejich přístupových rolí a logiky do systému IAM bez dodatečných licenčních nákladů.
Dodavatel se zaručuje, že v dodávce jsou zahrnuty licence třetích stran, a používání díla jako celku nevyžaduje žádné další dodatečné náklady.
Dodavatel se zaručuje, že při uplatnění práv třetí osobou na autorská práva nese následky případných sporů dodavatel.

Licence včetně dokumentace bude Zadavateli dodavatelem poskytnuta ke všem způsobům užití IAM v rozsahu potřebném k dosažení účelu smlouvy, kterým je správa uživatelů (interních i externích) a řízení jejich přístupů do koncových systémů užívaných Finanční správou České republiky, včetně oprávnění měnit, rozšiřovat a jinak upravovat IAM v souladu se svými potřebami.

ID	Požadavek	Způsob naplnění
186	Součástí dodávky bude kompletní předání zdrojových kódů včetně dokumentace, kde licence na použití zdrojových kódů a celého díla bude splňovat výše specifikované licenční podmínky.	Požadavek je naplněn kompletně. Součástí dodávky bude kompletní předání zdrojových kódů včetně dokumentace. Tyto zdrojové kódy budou umístěny v GITu, který bude poskytovat přehlednou správu verzí a historii změn. Licence na použití zdrojových kódů a celého díla bude splňovat specifikované licenční podmínky, což umožní bezproblémové použití a modifikaci kódu v souladu s požadavky.

Tabulka 43 – Licenční požadavky

6.2 Požadavky na grafické rozhraní

ID	Požadavek	Způsob naplnění
187	IAM MUSÍ obsahovat grafické uživatelské rozhraní pro přístup administrátorů systému pro správu identit uživatelů a jejich možné založení, úpravu nebo zneplatnění.	Požadavek je naplněn kompletně. V navrhovaném IAM řešení je k dispozici grafické uživatelské rozhraní pro administrátory, které umožňuje efektivní správu identit uživatelů, včetně jejich založení, úpravy a zneplatnění, správu životního cyklu identit, přičemž administrátor může přidávat nové uživatele, měnit jejich údaje nebo deaktivovat účty.
188	IAM MUSÍ obsahovat grafické uživatelské rozhraní sloužící jako obsluha pro uživatele, ve kterém uživatelé mohou měnit/resetovat heslo, žádat o přidělení rolí pro sebe nebo své podřízené, schvalovat nebo zamítat žádost a provádět další činnosti, na které mají oprávnění. Uvedené funkce MUSÍ být začleněné do portálového prostředí uživatele.	Požadavek je naplněn kompletně. V rámci řešení IAM je součástí komponenty IDM self-service rozhraní pro koncové uživatele, které je součástí portálového prostředí. Uživatelé mohou prostřednictvím tohoto rozhraní měnit a resetovat svá hesla, žádat o přidělení rolí pro sebe nebo své podřízené, schvalovat nebo zamítat žádosti a vykonávat další činnosti, na které mají oprávnění. Tento portál poskytuje snadný přístup k funkcím, které zjednodušují správu účtů a přístupů, a

ID	Požadavek	Způsob naplnění
		zajišťuje, že uživatelé mohou samostatně spravovat své identitní a přístupové údaje.
189	IAM MUSÍ obsahovat grafické uživatelské rozhraní portálového typu funkční v obvyklých webových prohlížečích (Edge, Chrome, Firefox, Safari) bez potřeby instalace doplňku do prohlížeče, které bude sloužit uživatelům pro využívání systému i administrátorů pro jeho správu.	Požadavek je naplněn kompletně. IAM obsahuje grafické uživatelské rozhraní portálového typu, které je plně kompatibilní s běžně používanými webovými prohlížeči, jako jsou Edge, Chrome, Firefox a Safari, a nevyžaduje instalaci žádných doplňků do prohlížeče. Tento webový portál využívá standardní webové technologie jako HTML5, CSS a JavaScript, což zajišťuje kompatibilitu s moderními prohlížeči bez nutnosti instalace dalších pluginů nebo rozšíření.
190	Rozhraní MUSÍ být implementováno s responzivním designem – přizpůsobení vzhledu typu zařízení, ze kterého je k portálu přistupováno (stolní počítač, notebook, tablet).	Požadavek je naplněn kompletně. Rozhraní IAM je implementováno s responzivním designem, což znamená, že se automaticky přizpůsobí různým typům zařízení (stolní počítače, notebooky, tablety) díky použití flexibilních mřížek (CSS Grid) a media queries v CSS. Tato technologie umožňuje dynamické přizpůsobení layoutu na základě velikosti obrazovky a rozlišení zařízení, což zajišťuje optimální zobrazení a funkčnost na různých typech zařízení.

Tabulka 44 – Požadavky na grafické rozhraní IAM

6.3 Logy IAM

ID	Požadavek	Způsob naplnění
191	IAM MUSÍ umožňovat publikovat kopie logů do externího systému určeného pro sběr logů.	Požadavek je naplněn kompletně. IAM umožňuje publikování kopie logů do externího systému určeného pro sběr logů, jako jsou například SIEM systémy (Security Information and Event Management). Tento proces je realizován prostřednictvím standardizovaných protokolů, jako jsou Syslog, které umožňují bezpečné odesílání logových

ID	Požadavek	Způsob naplnění
		záznamů do externího sběrného systému. Tato integrace je konfigurovatelná a může být přizpůsobena specifickým požadavkům a prostředí zákazníka.

Tabulka 45 – Požadavky na logy IAM

6.4 Notifikace

ID	Požadavek	Způsob naplnění
192	IAM MUSÍ zajistit zasílání konfigurovatelných e-mailových upozornění min. pro následující události: • Vytvoření a změna identity, referenčního objektu (systemizované místo, organizační jednotka, skupina, pracovní pozice / funkce, aplikace, skupina aplikací, aplikační role atd.), • Identifikace problému při synchronizaci, • Vypršení hesla, • Vypršení platnosti certifikátu.	Požadavek je naplněn kompletně. IAM zajišťuje zasílání konfigurovatelných e-mailových upozornění pro klíčové události, jako je vytvoření a změna identity, změna referenčního objektu (např. systemizované místo, organizační jednotka, skupina, pracovní pozice, aplikace, aplikační role) a identifikace problémů při synchronizaci. Také podporuje upozornění na vypršení hesla a vypršení platnosti certifikátu (jakožto atributu uživatele). Tato upozornění jsou realizována prostřednictvím notifikačního systému, který využívá standardizované e-mailové protokoly (SMTP) a je plně konfigurovatelný přes rozhraní IDM.
193	Upozornění na vypršení časových termínů MUSÍ být možno zasílat v předstihu. Velikost předstihu (např. počet dnů) MUSÍ být možno konfigurovat pro každý typ upozornění samostatně.	Požadavek je naplněn kompletně. IAM umožňuje zasílání upozornění na vypršení časových termínů s konfigurovatelným předstihem. Tento předstih lze nakonfigurovat prostřednictvím administrátorského rozhraní, které umožňuje nastavit různé hodnoty pro události jako vypršení hesla, certifikátu, atributů objektů nebo platnosti

ID	Požadavek	Způsob naplnění
		role. Tato funkcionalita je zajištěna prostřednictvím notifikačního systému, který využívá konfiguraci v databázi pro uchování specifických časových předstihů a používá API pro zajištění správného doručení notifikací.
194	Systém upozornění MUSÍ obsahovat správu šablon. Šablony upozornění umožní definovat příjemce, předmět a obsah upozornění. U upozornění vázaného k identitám musí být možné nastavovat různé příjemce pro různé části organizační struktury (např. odbor, oddělení) apod. Šablony MUSÍ umožnit vložit do obsahu upozornění libovolný atribut identity a/nebo referenčního objektu.	Požadavek je naplněn kompletně. Šablony upozornění jsou plně konfigurovatelné a umožňují specifikovat různé příjemce pro různé části organizační struktury (např. odbory, oddělení, pracovní místa) na základě atributů identity nebo referenčních objektů. Šablony podporují vložení libovolného atributu identity nebo referenčního objektu do obsahu upozornění prostřednictvím dynamických placeholderů, což je implementováno prostřednictvím rozhraní API a konfigurace v databázi IDM.
195	Pro zasílání jednotlivých typů upozornění MUSÍ být možno konfigurovat podmínky, za jakých bude upozornění zasláno. V konfiguraci bude možné využít atributů identit a referenčních objektů. Např. notifikace budou generovány pouze pro identity v konkrétních uvedených skupinách, které mají uvedenu konkrétní aplikační role a konkrétní atribut atd.	Požadavek je naplněn kompletně. IAM umožňuje konfigurovat podmínky pro zasílání jednotlivých typů upozornění, přičemž lze využívat atributy identit a referenčních objektů. Upozornění mohou být generována na základě specifických podmínek, jako jsou příslušnost identity k určité skupině, přiřazené aplikační role nebo jiné atributy, které jsou součástí identity nebo referenčního objektu atd.

Tabulka 46 – Požadavky na notifikace

6.5 Migrace dat

Nedílnou součástí implementace IAM je nahrazení existujících procesů pro správu identit a řízení přístupu. K tomu bude nutná migrace existujících dat do nového systému. Počítá se ovšem s modernizací procesů pro správu identit, a proto musí Dodavatel v rámci analýzy navrhnout a zdokumentovat novou architekturu, její součástí bude minimálně návrh nových rolí, organizační struktury a životních cyklů a to vše s důrazem na sjednocení identit napříč napojenými informačními systémy.

Nové IAM řešení bude napojeno na stejné informační systémy jako stávající řešení, kde zajistí synchronizaci digitálních identit. Do budoucna se počítá s napojením dalších informačních systémů. IAM systém i navržená architektura zpracování dat, musí umožňovat rozšíření sady zpracovávaných dat a napojování dalších informačních systémů.

ID	Požadavek	Způsob naplnění
196	Pro úvodní naplnění MUSÍ být převzaty konfigurace identit a uživatelských rolí ze současných informačních systémů, kdy dojde v rámci návrhu skutečného provedení ke sjednocení těchto identit napříč pro napojené informační systémy v IAM.	Požadavek je naplněn kompletně. Tento proces zahrnuje synchronizace a import dat do IAM, kde dojde k sjednocení identit napříč napojenými systémy. Importní úkoly v IDM zajišťují načítání dat z různých zdrojů (např. LDAP, CSV, RESTAPI, atd.).
197	Dodavatel MUSÍ zajistit vytvoření dokumentace systemizovaných míst a organizační struktury identit a uživatelských rolí v organizaci zadavatele, na jejímž základě bude provedena migrace a konfigurace nově dodaného řešení, která bude vycházet z již existujících konfigurací a dat.	Požadavek je naplněn kompletně. V rámci tohoto procesu bude provedena analýza stávající struktury a následně připraven plán pro implementaci v novém řešení, který bude zahrnovat import a synchronizaci dat, včetně konfigurace systemizovaných míst a uživatelských rolí pomocí importních úloh.

Tabulka 47 – Požadavky na migraci dat

6.6 Požadavky na dokumentaci

Všechna dokumentace vznikající v rámci zakázky musí být verzována, opatřena seznamem autorů, přehledem změn jednotlivých verzí a musí být obsahově úplná pro tu část systému, kterou popisuje. Dokumentace musí být napsána v českém jazyce a před finálním odevzdáním zpracovaná jazykovým korektorem. Dokumentace se vytváří a verze k revizím se předávají ve formátu MS Office. Finální verze dokumentace dodává Dodavatel ve formátu PDF.
Dále je možné využít existující dokumentaci k existujícím komponentám a systémům které budou v rámci zakázky nasazené. Taková dokumentace musí být obsahově úplná pro tu část systému, kterou popisuje. Může být v anglickém jazyce, pokud je tato dokumentace určena pro technické správce IAM. Pokud by dokumentace byla určena pro koncové uživatele, musí být v českém jazyce.

Jako součást dodávky je požadována následující dokumentace:

6.6.1 Dokumentace jádra systému

Dokumentace jádra systému, jeho funkcí, služeb a rozhraní. Dokumentace bude obsahovat kompletní popis architektury jádra systému, výčet a podrobný popis všech jeho funkcí, přehled a popis služeb, které jádro poskytuje dalším komponentám systému, modulům a knihovnám.

6.6.2 Dokumentace pro vývoj nových konektorů

Dokumentace pro vývoj nových konektorů bude obsahovat kompletní popis tvorby nových konektorů, včetně vazeb na systém IDM tak, aby nově vzniklý konektor bylo možné zapojit do všech již existujících procesů v IDM.

6.6.3 Příručka administrátora IDM

Příručka bude distribuována úzké skupině uživatelů, správců systému. Musí obsahovat kompletní popis všech funkcí pro práci s administrací IDM. Příručka bude využívána jako materiál pro školení nových administrátorů. Příručka musí obsahovat solidně zpracovaný popis kroků pro jednotlivé implementované funkce s vhodným doprovodným obrazovým materiálem ve formě výřezů obrazovek.

6.6.4 Uživatelská příručka

Příručka bude distribuována uživatelům. Musí obsahovat kompletní popis všech uživatelských funkcí pro práci s IDM. Příručka bude využívána jako základní materiál pro školení nových uživatelů. Příručka musí obsahovat solidně zpracovaný popis kroků pro jednotlivé implementované funkce s vhodným doprovodným obrazovým materiálem ve formě výřezů obrazovek.

ID	Požadavek	Způsob naplnění
198	Součástí dodávky je následující dokumentace: Dokumentace jádra systému, Dokumentace pro vývoj nových konektorů, Příručka administrátora IDM, Uživatelská příručka	Požadavek je naplněn kompletně. Ano, bude poskytnuta požadovaná dokumentace např. v textovém formátu *.docx. Dokumentace bude v průběhu projektu a provozu systému aktualizována.

Tabulka 48 – Požadavky na dokumentaci

7 POŽADAVKY NA FUNKCIONALITY EXTERNÍHO IAM JAKO SERVICE PROVIDERA

Tato kapitola je poplatná pouze pro externí IAM.

7.1 Vysvětlení koncepce externího IAM jako Service Providera

Externí instance IAM (dále externí IAM) bude kombinovat funkčnost IAM systému a současně bude zajišťovat funkci Service Providera (SeP) v rámci jednotlivých informačních systémů FS, a to oproti Identity Providerovi (IdP) dle platných právních předpisů nebo IdP, se kterým má FS nastaven vztah důvěry – aktuálně Národní identitní autoritě (NIA) Identita občana.

7.1.1 IdP NIA

NIA, jakožto jeden z IdP dle aktuálních předpisů, bude zdrojem důvěryhodných údajů o fyzických osobách a to prostřednictvím tzv. assertions/claims, pro které jsou data přebírána ze základních registrů Registru obyvatel (ROB), Registru osob (ROS) a dalších napojených datových zdrojů. – Autentizace a identifikace přihlašující se externí osoby tedy bude v případě NIA jakožto IdP přebírána z portálu národního bodu Identita občana https://identitaobcana.cz/.

7.1.2 NIA jako SSO

Národní bod Identita občana se chová jako služba Single Sign-On. IDM neřeší, jakým identifikačním prostředkem se daná FO přes identifikační bránu Identita občana přihlásila (neřeší rozdíl a neřeší žádnou funkčnost pro přihlášení pomocí občanského průkazu, datové schránky, bankovní identity, MojeID, atd.). Jedinou podmínkou je dostatečná úroveň záruky (LoA) daného poskytovatele identity (IdP), kdy pro přihlášení do portálu MOJE daně je minimální úroveň „Substantial“.

7.2 Správa mandátů FO, FOP a PO

Externí IAM bude zajišťovat funkčnosti pro správu mandátů FO, FOP a PO pověřeným fyzickým osobám v rámci informačních systémů FS. Mandátem se rozumí zplnomocnění dané FO pro úkony v rámci informačních systémů FS.

V kontextu IAM je mandát uložen v tzv. Mandátním registru, což je samostatná aplikace, která není součástí IAM. IAM tedy odtud bude přebírat autorizační informace reprezentované udělenými mandáty a ty předávat aplikacím integrovaným s IAM nebo je bude přímo zpracovávat v IAM.

Základní pravidla pro udělení mandátu:

- Mandátem se zplnomocňuje FO,
- Mandát může být časově omezen intervalem od – do,
- Mandát může být omezen typem funkčnosti (např. pouze pro podání a správu daňového přiznání pro daň z nemovitosti).

Proces udělení mandátu pro portál MOJE daně:

- Autentizovaná FO může udělit mandát jedné či více FO – ztotožnění bude probíhat dohledáním osob v nRS, resp. v Registru obyvatel na základě údajů poskytnutých zplnomocňující FO,

- Autentizovaná FO, která je současně dohledána v nRS, resp. v Registru osob jako FOP může udělit mandát jedné či více FO – ztotožnění bude probíhat dohledáním osob v nRS, resp. v Registru obyvatel na základě údajů poskytnutých zplnomocňující FO,
- Autentizovaná FO, která je současně dohledána v nRS, resp. v Registru osob jako statutární orgán PO může udělit mandát zastupování PO jedné či více FO – ztotožnění bude probíhat dohledáním osob v nRS, resp. v Registru obyvatel na základě údajů poskytnutých zplnomocňující FO.

Udělené mandáty k FOP a PO jsou vždy znovu ověřovány oproti platným údajům v nRS a to vždy v okamžik úspěšné autentizace dané FO oproti IdP a v Mandátním registru jsou odejmuty mandáty, které byly uděleny neplatnou FOP nebo neplatným statutárním orgánem PO.

7.3 Základní požadavky na AIM jakožto SeP

ID	Požadavek	Způsob naplnění
199	Externí IAM MUSÍ poskytovat funkčnosti jakožto Service Providera (SeP) oproti Identity Providerovi (IdP) dle platných právních předpisů nebo IdP, se kterým má FS nastaven vztah důvěry.	Požadavek je naplněn kompletně. CAS v rámci podpory delegované autentizace vystupuje vůči externím IdP jako SeP. CAS jako SeP podporuje protokoly SAML 2.0, OIDC/OAuth, WS-Federation a tudíž je možné ho napojit na libovolného IdP podporujícího tyto protokoly (NIA, Bank iD, …). Do CAS byla implementována i podpora delegované autentizace (SeP) vůči JIP/KAAS. CAS bude integrován s externími IdP dle platných právních předpisů nebo s externími IdP, se kterým má FS nastaven vztah důvěry.
200	Komunikace mezi externí IAM a IdP MUSÍ podporovat standard SAML 2 a WS-Federation.	Požadavek je naplněn kompletně. CAS v rámci podpory delegované autentizace vystupuje vůči externím IdP jako SeP. CAS jako SeP vůči externím IdP podporuje protokoly SAML 2.0, OIDC/OAuth, WS-Federation.
201	Integrace IAM a IdP MUSÍ být řešena pomocí integrační platformy integrovaného datového rozhraní.	Požadavek je naplněn kompletně. CAS v rámci integrace na externí IdP používá integrační platformu dle protokolů OIDC/OAuth, SAML 2.0, WS-Federation.
202	Externí IAM MUSÍ zajistit, že ověřená osoba může měnit jen tyto údaje: • E-mail, • Telefon. V případě, že uživatel provedl aktualizaci těchto údajů, nebudou již přepisovány na základě dat obdržených z IdP po dalším přihlášení uživatele.	Požadavek je naplněn kompletně. Jako Zhotovitel vystavíme samostatnou frontendovou službu (součást externího IAM), kde si ověřená osoba bude moci bezpečně měnit své údaje – konkrétně e-mail a telefonní číslo. Tato změna bude zaznamenána a při dalším přihlášení uživatele nebude přepisována daty z IdP. Řešení zajistí jednoznačnou preferenci uživatelsky zadaných hodnot nad údaji získanými z identity provideru.
203	Externí IAM MUSÍ ukládat získané identity autentizovaných osob	Požadavek je naplněn kompletně.

	ve svém úložišti, v rámci procesu autentizace oproti IdP je vždy provedena aktualizace údajů o této osobě dle výsledných dat z IdP.	CAS bude ukládat získané identity autentizovaných osob do IDM. V rámci každé autentizace bude provedena aktualizace (synchronizace) údajů v IDM dané autentizované osoby.
204	Externí IAM MUSÍ spravovat mandáty v mandátním registru dle popisu v kapitole Správa mandátů FO, FOP a PO. (Bližší popis procesu a chování bude upřesněn v rámci vzniku analýzy dodávaného řešení.)	Požadavek je naplněn kompletně. Zhotovitel zajistí integraci externího IAM s Mandátním registrem prostřednictvím rozhraní, které bude upřesněno v rámci analýzy. Externí IAM bude na základě této integrace načítat a vyhodnocovat aktuální mandáty fyzických osob, FOP a PO, a tyto autorizační údaje předávat připojeným systémům nebo je využívat přímo při řízení přístupů. Mandáty budou zpracovávány dle definovaných pravidel, včetně kontroly platnosti v registrech nRS a aktualizace jejich platnosti. Součástí řešení bude také zajištění přehledného a bezpečného zobrazení udělených mandátů pro uživatele v rámci portálu IAM a jejich případná administrace podle oprávnění.
205	Externí IAM MUSÍ být realizován jako univerzální prostředník pro neomezený počet zdrojových systémů zadavatele (ze kterých vznikla žádost o přihlášení).	Požadavek je naplněn kompletně. CAS jakožto IdP poskytuje možnost připojení (integrace) neomezeného množství systémů/aplikací, kterým bude poskytovat službu poskytovatele identity přistupujícího uživatele (IdP), tj. autentizačního poskytovatele. Dále bude poskytovat službu autorizace přístupu.
206	Externí IAM musí při odhlášení uživatele odeslat požadavek na odhlášení daného uživatele na IdP, který byl použitý pro přihlášení.	Požadavek je naplněn kompletně. CAS v rámci jednotného odhlášení (SLO), zajistí nejen odhlášení ve všech aplikacích, do kterých se uživatel v rámci SSO session přihlásil, ale v případě delegované autentizace zajistí odhlášení uživatel i z nadřazeného externího IdP, kde proběhla autentizace tohoto uživatele.
207	Při změně kontextu mandátu uživatele (uživatel chce změnit	Požadavek je naplněn kompletně.

	aktuální mandát za jiný) MUSÍ IAM odhlásit uživatele ze všech připojených systémů podporujících standardizovaný způsob odhlášení. Z IdP se uživatel neodhlašuje a je využit princip SSO (pokud jej daný IdP podporuje).	Tento požadavek bude zajištěn implementací jednotného mechanismu pro změnu kontextu mandátu v rámci externího IAM. Při přepnutí mandátu dojde k odhlášení uživatele ze všech systémů, které podporují standardizované odhlášení, přičemž přihlášení k IdP zůstává zachováno, aby bylo možné využít SSO pro okamžité přihlášení pod novým mandátem. Tato funkcionalita bude součástí portálového rozhraní, kde si uživatel zvolí jiný aktivní mandát. IAM následně provede řízený logout u integrovaných aplikací a zajistí korektní přenos nového mandátu v rámci navazující autentizace.

Tabulka 49 – Základní požadavky na IAM jakožto SeP

7.3.1 IAM jakožto SeP pro NIA

ID	Požadavek	Způsob naplnění
208	Externí IAM MUSÍ zajistit proces ověření dané fyzické osoby prostřednictvím Národní identitní autority (NIA). Tedy jakožto SeP připraví SAML žádost o přihlášení se všemi povinnými údaji a to s úrovní záruky (LoA) na minimální úrovni „Substantial“. Registraci IAM jakožto SeP pro NIA zajistí GFŘ.	Požadavek je naplněn kompletně. CAS v rámci podpory delegované autentizace vystupuje vůči externím IdP jako SeP. CAS jako SeP podporuje protokoly SAML 2.0, OIDC/OAuth, WS-Federation a tudíž je možné ho napojit na Identitu občana (NIA). V rámci SAML 2.0 žádosti se definují požadované atributy uživatele a minimální úroveň záruky (LoA), jakou musí NIA v rámci autentizace zaručit. GFŘ, jakožto OVM musí zajistit registraci SeP (CAS), zajistit a registrovat certifikát, kterým budou SAML 2.0 žádosti podepisovány.

Tabulka 50 – IAM jakožto SeP pro NIA

8 DALŠÍ POŽADAVKY na IAM

Požadavky v této kapitole jsou společné pro celé řešení IAM – tj. interní a externí IDM, AM.

8.1 Kvantitativní a kvalitativní požadavky

ID	Požadavek	Způsob naplnění
209	IAM MUSÍ zajistit provoz pro následující počty uživatelů: - 15 tisíc interních uživatelů (ve všech rolích), - 1 milión externích uživatelů	Požadavek je naplněn kompletně. IAM (IDM + AM) je navrženo pro škálovatelnost a vysokou dostupnost, což umožňuje efektivní správu 15 tisíc interních uživatelů a 1 milionu externích uživatelů. Systém podporuje distribuované architektury a je optimalizován pro vysoký objem dat, což zahrnuje správu identit, rolí a přístupových práv pro velké množství uživatelů. Tato škálovatelnost je dosažena prostřednictvím použití robustních databázových a caching mechanizmů, což umožňuje efektivní práci i s velkými objemy dat, přičemž systém lze horizontálně škálovat přidáváním nových serverů.
210	IAM musí být schopna nárazově (v provozních špičkách) obsloužit minimálně: • 10 tisíc žádostí o autentizaci a autorizaci za hodinu a minimálně 100 současně pracujících interních uživatelů • 100.000 žádostí o autorizaci externích uživatelů za hodinu	Požadavek je naplněn kompletně. Systém bude schopný obsloužit minimálně 10 tisíc žádostí o autentizaci a autorizaci za hodinu a 100 současně pracujících interních uživatelů díky využití distribuovaných architektur a optimalizovaných databázových a cache mechanismů pro rychlé zpracování požadavků. Pro 100.000 žádostí o autorizaci externích uživatelů za hodinu je systém navržen s horizontálním škálováním, což umožňuje přidávání dalších serverů a komponent, čímž je zajištěna vysoká dostupnost a výkon i při velkém objemu požadavků.

ID	Požadavek	Způsob naplnění
211	Délka doby odezvy IAM MUSÍ při uvedeném zatížení odpovídat běžným zvyklostem/srovnatelným řešením.	Požadavek je naplněn kompletně. Při uvedeném zatížení bude systém optimalizován pro rychlé zpracování požadavků, což znamená, že doba odezvy by měla být v souladu s odvětvovými standardy pro autentizaci a autorizaci, obvykle v řádu milisekund až několika sekund. Tento výkon je zajištěn pomocí distribuovaných architektur, optimalizovaných databázových dotazů a vysoce efektivního caching systému.

Tabulka 51 – Kvalitativní a kvantitativní požadavky

8.2 Autentizace, autorizace a oprávnění

8.2.1 Požadavky na řízení oprávnění

ID	Požadavek	Způsob naplnění
212	IAM MUSÍ zajistit integrované řešení umožňující oddělení odpovědností a práv jednotlivých uživatelů dle definice rolí, navržených jako součást vybraných funkčních požadavků.	Požadavek je naplněn kompletně. Systém detailně rozděluje přístupová práva a odpovědnosti podle definovaných uživatelských rolí. Každá role je navržena na základě funkčních požadavků, čímž se zajistí jasné oddělení přístupových práv mezi různými uživatelskými skupinami. Tato funkcionalita je implementována prostřednictvím správy rolí a oprávnění v IDM.
213	Uživatelská oprávnění v informačním systému MUSÍ být přidělována výhradně na uživatelskou/aplikační roli.	Požadavek je naplněn kompletně. Uživatelská oprávnění v IAM budou přidělována výhradně na základě uživatelských a aplikačních rolí, což zajišťuje centralizovanou a flexibilní správu přístupových práv. Business role definují přístup a oprávnění na základě funkce nebo pozice v organizaci, zatímco aplikační role se vztahují na specifická oprávnění potřebná pro přístup k aplikacím a systémům. Tato separace umožňuje jasnou strukturu

ID	Požadavek	Způsob naplnění
		přístupů a oddělení odpovědností mezi různými úrovněmi řízení přístupu.
214	Autorizace veškerých uživatelů i správců v rámci informačního systému MUSÍ být realizována přiřazením aplikačních (business) rolí, minimálně v následujícím rozsahu: - Správce (Administrátor systému), který má neomezený přístup. - Metodik, který má přistup ke správě rolí. - IT Podpora (Helpdesk systému), který má přístup k seznamu uživatelů. - Bezpečnostní manager ICT (Compliance), vidí své role a jejich členy. Schvaluje žádosti o role na své schvalovací úrovni. - Školitel, vidí své role a jejich členy. Schvaluje žádosti o role na své schvalovací úrovni. - Nadřízený vidí podřízené identity, může pro tyto identity (uživatele) žádat o role a schvaluje žádosti o role na své schvalovací úrovni. - Běžný uživatel, může: o zobrazit informace o sobě o žádat o role a měnit své heslo Oprávnění běžného uživatele je součástí výše zmíněných oprávnění. Každý uživatel má minimálně jednu z těchto rolí.	Požadavek je naplněn kompletně. Tento systém řízení přístupů a autorizace je realizován prostřednictvím role-based access control (RBAC), kde každá role určuje, jaká oprávnění a přístupové úrovně má uživatel na základě své pozice v organizaci. Tento proces je plně konfigurovatelný v IDM, což umožňuje flexibilní přizpůsobení podle specifických požadavků a organizačních potřeb.
215	Systém MUSÍ umožnit definici rolí jednotlivých typových uživatelů a jejich práv při zachování datové a auditní stopy pro jednotlivé transakce pro potřeby budoucích kontrol a auditních akcí s možností zpětné kontroly a verifikace realizovaných	Požadavek je naplněn kompletně. Pro zachování datové a auditní stopy jsou všechny transakce, včetně změn rolí a přístupů, logovány do auditních logů, které jsou bezpečně uloženy pro budoucí

ID	Požadavek	Způsob naplnění
	transakcí.	kontroly a auditní akce. Tyto logy jsou dostupné prostřednictvím reportů v IDM, které umožňují zpětnou kontrolu a verifikaci realizovaných transakcí. Auditní logy mohou být zálohovány pro dlouhodobé uchování a jsou přístupné přímo v grafickém uživatelském rozhraní (GUI), kde administrátoři mohou prohlížet detaily o všech provedených akcích, včetně času, uživatele a typu změny.
216	Doplnění nebo změna oprávnění pro jednotlivé role, resp. doplnění rolí, MUSÍ být možné buď přímo oprávněným uživatelem (administrátorem), nebo za vynaložení minimálních vývojových nákladů.	Požadavek je naplněn kompletně. Systém IDM umožňuje administrátorům jednoduše přidávat nebo upravovat role a přiřazená oprávnění prostřednictvím grafického rozhraní, což zajišťuje rychlou a efektivní správu přístupů bez potřeby zásahu vývojářů. V případě složitějších požadavků je možné rolí a oprávněními manipulovat pomocí API, což umožňuje flexibilní úpravy a integraci s dalšími systémy, přičemž náklady na vývoj jsou minimální díky použitelnosti standardních integračních nástrojů a šablon.

Tabulka 52 – Požadavky na řízení oprávnění

8.2.2 Požadavky na autentizaci a kontrolu přístupu

ID	Požadavek	Způsob naplnění
217	Přístup do systému MUSÍ mít následující skupiny uživatelů: - Uživatelé systému (pracovníci zadavatele), - Pracovníci podpory (pracovníci zadavatele), - Pracovníci podpory (pracovníci dodavatele podpory – v rozsahu a způsobem omezeným na funkcionalitu nezbytnou pro zajištění běhu systému).	Požadavek je naplněn kompletně. Přístup do systémů IAM je řízen prostřednictvím autorizovaných rolí, které definují přístupová práva pro různé skupiny uživatelů.
218	IAM MUSÍ:	Požadavek je naplněn kompletně.

ID	Požadavek	Způsob naplnění
	- Vést historii uživatelských přístupů (úspěšných i neúspěšných) a logy spojené s činnostmi autentizace nutné pro provozní a bezpečnostní monitoring a ukládat tyto logy do centrální logovací komponenty.	IAM podporuje vedení historie uživatelských přístupů, včetně úspěšných i neúspěšných pokusů o autentizaci. Systém podporuje automatické odesílání těchto logů prostřednictvím standardizovaných protokolů (např. Syslog, API) a umožňuje jejich následné prohlížení a analýzu pro detekci anomálií a bezpečnostních incidentů.

Tabulka 53 – Požadavky na autentizaci a kontrolu přístupu

8.3 Požadavky na bezpečnost

8.3.1 Požadavky na bezpečnostní opatření

IAM je z pohledu bezpečnosti kategorizován následovně:

- IAM bude charakterizována jako KII dle ustanovení § 2 písm. b) zákona č. 181/2014 Sb., ZoKB, ve znění pozdějších předpisů;
- IAM je informačním systémem veřejné správy dle zákona č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů), ve znění pozdějších předpisů (dále též „ISVS“);
- IAM spadá do působnosti bezpečnostní dokumentace FS;
- Prostřednictvím IAM bude docházet ke zpracování a významné koncentraci osobních údajů[1] pro vysoký počet subjektů údajů, u jejichž identit bude IAM řídit celý životní cyklus identit. Z pohledu dopadu na práva subjektů údajů se z pohledu obecného nařízení GDPR jedná o kritický stupeň dopadu.

S ohledem na kritický charakter aktiva IAM přijal správce aktiva (FS) vhodná technická organizační opatření, a to v souladu s principy „PROTECTION BY DESIGN“[2] již v rámci přípravné (předimplementační) fáze projektu IAM. V souladu s bodem 1.4 přílohy č. 5 vyhlášky č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti) (dále jen „VoKB“ nebo „vyhláška o kybernetické bezpečnosti“), obsahuje bezpečnostní dokumentace FS pravidla řízení dodavatelů, přičemž FS tímto stanoví dále uvedené požadavky na úroveň služeb Zhotovitele a způsob a úroveň realizace bezpečnostních opatření.

Zhotovitel v rámci detailní specifikace podrobně analyzuje charakter aktiva IAM s ohledem na výše uvedenou bezpečnostní kategorizaci IAM, identifikuje hlavní bezpečnostní rizika, připraví návrh zabezpečení řešení IAM a realizuje dále popsaná bezpečnostní opatření (technická a organizační).

[1] Ve smyslu nařízení Evropského Parlamentu a Rady (EU) č. 2016/679 ze dne 27. dubna 2016, o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů) (dále též „GDPR“ či „obecné nařízení GDPR“).

[2] Protection by design je princip, jenž počítá se zabezpečením aktiva již od počátku návrhu praktického řešení, tj. preventivně a nikoliv reaktivně (ex-post), až dojde k realizaci bezpečnostního incidentu.

ID	Požadavek	Způsob naplnění
219	Zhotovitel MUSÍ: • plně určit aktiva IAM v implementované variantě IAM (tj. pro konkrétní dodavatelem navrhovanou solution architekturu IAM), a to v souladu se systémem řízení bezpečnosti informací FS (dle bezpečnostní dokumentace FS); • provést úplnou analýzu rizik pro bezpečnostní doménu/perimetr IAM (jak z pohledu ZoKB, tak i z pohledu obecného nařízení GDPR pro osobní údaje zpracovávané prostřednictvím IAM): o Identifikace relevantních hrozeb a zranitelností; o Provedení hodnocení rizik; o Zpracování a zavedení plánu zvládání rizik – určení bezpečnostních (organizačních a technických) opatření pro zvládání jednotlivých rizik.	Požadavek je naplněn kompletně. V rámci úvodní analýzy systému provedeme jako Zhotovitel identifikaci všech relevantních aktiv IAM dle navrhované architektury řeše-ní a v souladu s metodikou pro identifikaci aktiv, metodikou pro hodnocení aktiv FS. Součástí této analýzy bude také kompletní posouzení rizik, v souladu s metodikou pro určování a hodnocení rizik, včetně stanovení kritérií pro akceptovatelnost rizik FS. Při určování rizik s ohledem na aktiva budou určeny relevantní hrozby a zranitelnosti z pohledu platného ZoKB a stanovených zásad ochrany osobních údajů - GDPR FS. Na základě výsledků zpracujeme plán zvládání rizik, včetně návrhu a zavedení adekvátních organizačních a technických opatření. Celý proces bude koordinován s odpovědnými osobami Zadavatele. Toto vše v souladu s požadavky na KII. Uvedenou problematiku budeme řešit dle VoKB a dle metodiky NUKIB a podpůrných materiálů, např. Průvodce řízením aktiv a rizik dle vyhlášky o KB.
220	Zhotovitel MUSÍ v návrhu jednoznačně vymezit bezpečnostní domény/perimetry a vzájemný vztah bezpečnostních politik, bezpečnostní dokumentace a postupů SŘBI, které v nich budou uplatňovány. V rámci vymezení bezpečnostních domén musí být vymezeny komponenty a s nimi související služby zajišťované Zhotovitelem a komponenty a s nimi související služby zajišťované dalšími subjekty (FS, infrastrukturní a bezpečnostní služby SPCSS atp.). Řešení IAM musí být navrženo způsobem, kdy se v průběhu provozu mohou bezpečnostní domény i	Požadavek je naplněn kompletně. Východiskem pro zpracování bude bezpečnostní politika, bezpečnostní dokumentace a postup SŘBI FS. Jako Zhotovitel v rámci analýzy a návrhu jednoznačně vymezíme bezpečnostní domény a perimetry IAM, včetně vzájemných vztahů použitých bezpečnostních politik, dokumentace a postupů systému řízení bezpečnosti informací. Přesně určíme, které komponenty a služby budou zabezpečovány námi, a které budou zajišťovány dalšími subjekty (např. FS). Dle možností využijeme typová

ID	Požadavek	Způsob naplnění
	způsob zajištění infrastrukturních a jiných služeb měnit.	aktiva, analýzy rizik a opatření FS. Řešení IAM navrhneme flexibilně, aby bylo možné v průběhu provozu měnit nastavení bezpečnostních domén či způsob poskytování infrastruktury, bez nutnosti významných změn architektury. Tyto aspekty podrobně rozpracujeme v návrhu architektury a dodané bezpečnostní dokumentaci, čímž zajistíme transparentní řízení bezpečnostních odpovědností.
221	Zhotovitel MUSÍ při analýze rizik pracovat se všemi Varováními vydanými NÚKIB ke dni zahájení analýzy, a to primárně s Varování NÚKIB před používáním softwaru i hardwaru společností Huawei Technologies Co., Ltd., a ZTE Corporation ze dne 17. 12. 2018, ČJ 3012/2018-NÚKIB-E/110, dle metodiky k varování ze dne 17. prosince 2018 (aktuálně ve verzi 1.0 ze dne 4. 1. 2019).	Požadavek je naplněn kompletně. V rámci analýzy rizik budeme jako Zhotovitel pracovat se všemi platnými Varováními vydanými NÚKIB ke dni zahájení analýzy. Tato opatření budou zahrnuta do výsledného plánu zvládání rizik a bezpečnostní dokumentace řešení IAM. Zde budeme jako Zhotovitel vycházet z varování NÚKIB https://nukib.gov.cz/cs/infoservis/hrozby/.
222	Zhotovitel MUSÍ identifikovat v implementační analýze případy užití a stavy, které budou předmětem managementu bezpečnosti informací pro IAM a budou se týkat např. rizikových operací z pohledu zátěže IAM, mimořádných událostí, kybernetických bezpečnostních událostí a kybernetických bezpečnostních incidentů, ochrany osobních údajů (GDPR) apod.	Požadavek je naplněn kompletně. Na základě bezpečnostních politik, bezpečnostní dokumentace a postupů SŘBI FS, se zaměříme na základě provedené analýzy rizik zejména na rizikové operace spojené s vysokou zátěží IAM, situace mimořádných událostí, kybernetické bezpečnostní události a incidenty a také oblasti související s ochranou osobních údajů dle GDPR. Tyto scénáře budou zároveň začleněny do provozních procedur systému a budou vycházet z provedené analýzy rizik.
223	IAM MUSÍ být ve shodě se ZoKB a prováděcími právními předpisy, přičemž Zhotovitel je povinen realizovat organizační a technická opatření, jež FS jako správce KII stanovila a jež jsou uvedena v této technické specifikaci a v zadávací dokumentaci IAM. Stanovená organizační a technická opatření musí být implementovaná tak, aby byla ve shodě s VoKB.	Požadavek je naplněn kompletně. Potvrzujeme, že naše řešení IAM bude plně v souladu se zákonem o kybernetické bezpečnosti, prováděcími právními předpisy, vyhláškou o kybernetické bezpečnosti a s Krizovým zákonem pro kritickou infrastrukturu. Na základě výsledků analýzy rizik provedené během implementační analýzy a na

ID	Požadavek	Způsob naplnění
	Zhotovitel na základě provedené analýzy rizik v rámci implementační analýzy IAM navrhne a popíše implementaci organizačních a technických opatření. Konkrétní způsob realizace organizačních a technických opatření navrhne Zhotovitel v průběhu implementační analýzy, a to na základě zpracované analýzy rizik a jejich implementace podléhá schválení ze strany FS.	základě plánu krizové připravenosti kritické infrastruktury FS, dle nařízení vlády č. 462/2000 Sb., navrhneme konkrétní opatření technického, organizačního, administrativního a jiného rázu, ať již činěná vlastními silami a prostředky FS/dodavatele kritické infrastruktury, nebo za pomoci jiných subjektů, orgánů a složek. Zhotovitel bude realizovat rovněž opatření, která budou vycházet z již stanovených požadavků FS jako správce kritické informační infrastruktury a která budou v souladu s požadavky VoKB. Navržená opatření budou zdokumentována a předložena FS ke schválení.
224	Zhotovitel MUSÍ být povinen v souladu s požadavky VoKB a ve vzájemně odsouhlaseném rozsahu dodržovat následující pravidla řízení dodavatelů: • Během všech činností souvisejících s návrhem, implementací a podporou IS budou dodržovat pravidla stanovená legislativními pravidly; • Nakládat s daty v souladu s jejich účelem a klasifikací; • Řídit přístup a nakládání s osobními údaji; • Dodržovat bezpečnostní politiky, bezpečnostní dokumentaci a bezpečnostní opatření ve formě organizačních a technických opatření; • Komunikovat o bezpečnostních událostech a incidentech; • Řídit bezpečnostní rizika; • Řídit kontinuitu provozu;	Požadavek je naplněn kompletně. Potvrzujeme, že v rámci realizace IAM budeme plně dodržovat všechna uvedená pravidla řízení dodavatelů dle požadavků vyhlášky o kybernetické bezpečnosti, především § 3, § 6, § 30 a příloha č. 5 VKB. Veškeré činnosti během návrhu, implementace a provozní podpory systému budou prováděny v souladu s platnou legislativou a bezpečnostní dokumentací, metodikami a procesy SŘBI FS.

ID	Požadavek	Způsob naplnění
	údaje a informace vyžádané zadavatelem.	
225	IAM MUSÍ zajistit podporu pro záznam, analýzu a řešení možných bezpečnostních událostí a incidentů. V závislosti na provozním stavu systému, resp. na činnosti jednotlivých provozních rolí musí systém zaznamenávat události a data významná z pohledu bezpečnostního monitoringu s cílem maximálně přispět k identifikaci bezpečnostních událostí, resp. poskytnout součinnost při jejich odstranění. Vlastní identifikace a řízení životního cyklu bezpečnostních událostí a incidentů bude řešena v rámci bezpečnostního monitoringu zadavatele, kterému IAM MUSÍ poskytovat všechny relevantní informace.	Požadavek je naplněn kompletně. Veškeré důležité události z pohledu bezpečnosti, jako jsou pokusy o přihlášení, změny oprávnění nebo podezřelé aktivity, jsou zaznamenávány do auditních logů IAM. Zaznamenávaná data jsou formátována tak, aby umožnila jednoduchou integraci se systémem bezpečnostního monitoringu Zadavatele (např. SIEM), včetně odesílání logů pomocí standardních protokolů (např. Syslog).
226	IAM MUSÍ poskytovat nástroje pro sledování stavu informačního systému jako celku, stavu jednotlivých komponent i činností jednotlivých procesů a uživatelů. Systém také MUSÍ poskytovat veškerou součinnost při detekci, vyhodnocení a řízení odstranění bezpečnostních událostí nebo incidentů. Systém musí podporovat automatizované předávání událostí do dohledového systému Objednatele.	Požadavek je naplněn kompletně. Pro účely detekce, vyhodnocení a řešení bezpečnostních událostí systém generuje a zaznamenává auditní logy a další relevantní informace, které je možné automatizovaně předávat do dohledového systému Zadavatele prostřednictvím standardních protokolů (např. Syslog nebo REST API). Rozsah a způsob integrace IAM s dohledovým systémem Zadavatele bude detailně specifikován během implementační analýzy.
227	Součástí návrhu IAM MUSÍ být definice komponent, funkcionalit a postupů pro zajištění kontinuity činností a služeb, podporovaných informačním systémem IAM, včetně příslušné dokumentace podrobněji definované v kapitole 8.4.	Požadavek je naplněn kompletně. V rámci návrhu IAM zpracujeme definici komponent, funkcionalit a postupů pro zajištění kontinuity činností a služeb. Připravíme kompletní bezpečnostní dokumentaci dle uvedeného rozsahu v kapitole 8.4. Provedeme prezenční školení IT administrátorů s důrazem na praktické administrátorské činnosti, údržbu systému a řešení nestandardních stavů. Navrhneme a implementujeme zálohovací procedury umožňující pravidelné zálohy dat a

ID	Požadavek	Způsob naplnění
		konfigurací, včetně postupu pro jejich obnovu při havárii. Splníme požadované parametry RTO (≤ 4 hodiny) a RPO (≤ 24 hodin), přičemž zajistíme, že Zadavatel může provést obnovu i bez naší přímé součinnosti podle dodané provozní dokumentace.
228	Zabezpečení konfiguračních dat (např. přístupové údaje do dalších systémů, různá hesla v konfiguraci atd.) MUSÍ být zajištěno dostatečně silnou šifrou a v souladu s best-practice.	Požadavek je naplněn kompletně. Pro zabezpečení konfiguračních dat (např. přístupové údaje, hesla v konfiguraci) využíváme PAM řešení, která splňují požadavky na dostatečně silnou šifru a odpovídají současným bezpečnostním best-practice. Informace jsou v PAM ukládány v šifrované podobě (např. AES-256).
229	Pro autentizační data, uložená v informačním systému, MUSÍ být dostatečně zajištěna důvěrnost a integrita (např. prostřednictvím relevantní a bezpečné hash funkce).	Požadavek je naplněn kompletně. midPoint plně podporuje bezpečné ukládání autentizačních dat s důrazem na zajištění jejich důvěrnosti a integrity. Hesla uživatelů jde ukládat ve formě kryptografických hashů. Tento přístup zvyšuje bezpečnost, protože hashované heslo nelze zpětně dešifrovat, čímž je minimalizováno riziko úniku citlivých údajů. V rámci implementační analýzy bude navrženo konkrétní řešení pro bezpečné ukládání a správu autentizačních a konfiguračních dat.

Tabulka 54 – Požadavky na bezpečnostní opatření

8.3.2 Požadavky na bezpečnostní monitoring

ID	Požadavek	Způsob naplnění
230	IAM MUSÍ monitorovat bezpečnostní události.	Požadavek je naplněn kompletně. Systém bude zaznamenávat relevantní události např. přihlášení, změny oprávnění, chyby v konektivitě. IAM bude možné propojit s dohledovým nebo SIEM systémem Zadavatele pomocí standardních protokolů, což zajistí automatizovaný přenos událostí pro účely další analýzy. Rozsah zaznamenávaných událostí a způsob jejich předávání bude upřesněn v rámci implementační analýzy a přizpůsoben konkrétnímu bezpečnostnímu prostředí Zadavatele.
231	IAM a veškeré komponenty vymezené v předchozích požadavcích MUSÍ umožnit logovat veškeré z bezpečnostního pohledu významné aktivity prováděné administrátory či uživateli. Všechny tyto logované záznamy MUSÍ být volitelně, v intervalech blízkých reálnému času přenášeny do systému pro bezpečnostní monitoring zadavatele (SIEM) k jejich vyhodnocení a uložení na centrálním bezpečném místě pomocí syslog UDP/TCP protokolu. Tyto záznamy MUSÍ být zároveň přístupné přímo v GUI rozhraní IAM. IAM, včetně všech jejích komponent, MUSÍ být připraven na integraci do SIEM obdobným způsobem tak, aby naplňovaly požadavky na bezpečnostní monitoring definované v následujících požadavcích. Integrace na SIEM je součástí předmětu veřejné zakázky a zajistí ji Zhotovitel.	Požadavek je naplněn kompletně. Řešení umožňuje logování všech bezpečnostně významných aktivit prováděných administrátory i běžnými uživateli ve všech jeho komponentách. Všechny tyto události budou v reálném čase nebo blízkém intervalu přenášeny do SIEM systému Zadavatele prostřednictvím protokolů Syslog přes UDP/TCP, dle požadavků Zadavatele. Některé záznamy budou zároveň dostupné přímo v GUI rozhraní IAM pro auditní účely.
232	V rámci IAM MUSÍ být pořizovány a uchovávány auditní	Požadavek je naplněn kompletně.

ID	Požadavek	Způsob naplnění
	záznamy a to tak, aby byly využitelné pro monitorování řízení přístupu a případné budoucí řešení bezpečnostních incidentů. Záznam auditních událostí musí být dostupný ve strojově zpracovávatelném formátu a musí být vytvořen číselník ID typu událostí dle typických událostí v Aplikaci a předán jako součást bezpečnostní dokumentace.	V řešení IAM zajistíme, že auditní záznamy budou pořizovány přímo na úrovni jednotlivých komponent a uchovávány v centrálním úložišti logů. Auditní logy budou obsahovat časové razítko, typ události, ovlivněné objekty apod. Součástí dodávky bude také číselník událostí, který integrujeme do bezpečnostní dokumentace. Události budou exportovatelné přes Syslog/REST do externího systému. Auditní mechanizmus prod IDM stavíme na standardech midPointu, doplněný o logovací framework (např. Logback) a nastavení pro přenos do SIEM.
233	Pokud údaje zapisované do logu IAM obsahují citlivá data (heslo, klíč či jeho prekurzor, session ID apod.) NESMÍ být uložena v plain textu, ale musí být před zapsáním zašifrovány nebo přepsány pseudonáhodnou sekvencí.	Požadavek je naplněn kompletně. V rámci dodávaného řešení IAM zajistíme, že žádné citlivé údaje (např. hesla, session ID, kryptografické klíče) nebudou v logovacích záznamech uchovávány v nešifrované (plain text) podobě. Pokud některá komponenta loguje data, která mohou obsahovat citlivé informace, implementujeme vlastní skripty a filtry, které tyto hodnoty automaticky nahradí pseudonáhodnou sekvencí nebo je zašifrují před zápisem do logu. Tato funkcionalita bude nakonfigurována přímo v rámci logovací vrstvy.
234	V IAM MUSÍ být zavedena ochrana proti deaktivaci, selhání či změnám v pořizování auditních záznamů a ochrana proti změnám nebo zničení auditních záznamů. Implemetace této ochrany může být taková, že IAM neumožuje přímou manipulaci s auditními záznamy nebo na to existuje oprávnění, které nemusí být přiřazeno správcům systému.	Požadavek je naplněn kompletně. V rámci IAM řešení zavedeme ochranu proti deaktivaci nebo manipulaci s auditními záznamy tak, že auditní logy budou generovány automaticky a nelze je ze systému běžným způsobem mazat ani upravovat. Například v případě IDM je auditní subsystem navržen tak, aby zápisy do auditního logu probíhaly nezávisle na běžných oprávněních – neexistuje běžné uživatelské oprávnění, které by umožňovalo úpravu nebo

ID	Požadavek	Způsob naplnění
		výmaz již pořízených záznamů. Práva na konfiguraci auditního mechanismu mají pouze technicky nejvyšší úrovně správy, které není běžně přidělováno administrátorům systému. Pro ochranu proti změnám nebo zničení auditních záznamů budou tyto logy ukládány do zabezpečeného úložiště s aktivním logováním přístupů a možností replikace na jiný systém (např. do SIEM řešení), čímž se zajistí jejich neměnnost a dostupnost i při selhání primárního úložiště. Součástí ochrany je také nastavení přístupových práv na úrovni serveru – přístup k adresářům s logy budou mít výhradně vybrané technické účty, které budou spravovány prostřednictvím oprávnění nastavených v systému a kontrolovaných v rámci bezpečnostního dohledu.
235	Přístup k auditním záznamům MUSÍ být bezpečně chráněn, aby bylo zabráněno jeho zneužití nebo ohrožení. IAM MUSÍ umožnit nastavení přístupových práv k auditním záznamům tak, aby mohly být auditovány samostatnou rolí (auditor, security officer atp.).	Požadavek je naplněn kompletně. Přístup k auditním záznamům v rámci IAM bude řízen prostřednictvím přístupových oprávnění definovaných v roli, kterou lze přiřadit pouze vybraným osobám (např. auditor, bezpečnostní pracovník). V případě IDM je možné tyto přístupy granularizovat prostřednictvím autorizací v bezpečnostní politice. Auditní záznamy jsou zobrazitelné buď přes GUI s role-based přístupem, nebo exportovatelné přes zabezpečené API. Přístup je dále možné logovat, což zajišťuje transparentnost a kontrolu nad auditními daty. Současně budou auditní záznamy uloženy ve vyhrazeném úložišti s omezenými přístupy – přístup na úrovni OS bude umožněn pouze technickým účtům s kontrolovanými oprávněními. Tímto způsobem zajistíme ochranu proti

ID	Požadavek	Způsob naplnění
		neoprávněnému čtení či manipulaci přímo na úrovni souborového systému.

Tabulka 55 – Požadavky na bezpečnostní monitoring

8.3.3 Požadavky na správu certifikátů

ID	Požadavek	Způsob naplnění
236	Zhotovitel MUSÍ jako součást předmětu veřejné zakázky být připraven instalovat potřebné certifikáty a aktivně monitorovat dobu platnosti certifikátů.	Požadavek je naplněn kompletně. Zajistíme, že v rámci implementace IAM bude náš tým připraven nainstalovat všechny potřebné certifikáty důvěryhodných autorit pro komunikaci (např. HTTPS, LDAPS, SAML, OIDC) a správně je nakonfigurovat v jednotlivých komponentách systému. Současně je možné nastavit automatizovaný monitoring doby platnosti certifikátů, např. pomocí naplánovaných skriptů, které budou kontrolovat expiraci certifikátů a generovat včasná upozornění. Tyto skripty lze rozšířit o notifikace (e-mail, log, přenos do SIEM), aby Zadavatel získal přehled o nadcházející expiraci.
237	V případě, blížící se expirace certifikátů MUSÍ být vytvářen a předáván požadavek na vystavení nových certifikátů zadavateli s takovým časovým předstihem, aby bylo možné bezpečně zajistit a instalovat nové certifikáty. Certifikáty pro SSL/TLS zajistí zadavatel na základě požadavku Zhotovitele a po vzájemné dohodě.	Požadavek je naplněn kompletně. Zhotovitel v rámci dodávky zajistí nastavení upozorňování na blížící se expiraci certifikátů. Tento monitoring může být zajištěn buď přímo v rámci IAM (např. pomocí plánovaných kontrolních skriptů), nebo může být ponechán na straně Zadavatele, pokud již disponuje vlastními dohledovými nástroji. Na základě dohody se Zadavatelem a znalosti procesu vydávání certifikátů pak nastavíme přenos požadavků na nové certifikáty v dostatečném časovém předstihu tak, aby jejich výměna mohla proběhnout bez dopadu na dostupnost systému.

Tabulka 56 – Požadavky na správu certifikátů a autentizačních údajů

8.3.4 Požadavky na aplikační bezpečnost

Pro zvýšení bezpečnosti aplikací a podporu jejich nasazení a provozu je v prostření FS využíváno řešení F5 zajišťující funkcionality preautentizační reverzní proxy (PARP), load balanceru (LB), routeru a reverzního aplikačního firewallu. Očekává se, že nasazení IAM bude, stejně jako další aplikace, napojeno na řešení F5. Proto dodavatel při nasazování komponent IAM musí poskytnout součinnost potřebnou pro jejich napojení na systém F5 a jeho správnou konfiguraci. Stejně tak dodavatel musí poskytnout součinnost pro nakonfigurování F5 potřebné pro zabezpečení komunikace mezi IAM a na něj napojenými systémy.

8.4 Požadavky na provozní podporu, řízení a monitoring prostředí

8.4.1 Dokumentace softwarového díla

ID	Požadavek	Způsob naplnění
238	Bezpečnostní dokumentace MUSÍ být dodána v následujícím rozsahu: 1. Identifikace informačních aktiv IAM. 2. Analýza bezpečnostních rizik IAM včetně návrhu bezpečnostních opatření. 3. Politika bezpečnosti informací IAM. 4. Příručka systému řízení bezpečnosti informací IAM. 5. Požadavky na řízení kontinuity činností IAM (BCM).	Požadavek je naplněn kompletně. Zhotovitel jako součást plnění veřejné zakázky dodá kompletní bezpečnostní dokumentaci v požadovaném rozsahu. V rámci implementační analýzy identifikujeme informační aktiva IAM a zpracujeme analýzu bezpečnostních rizik včetně návrhů technických a organizačních opatření. Součástí dodávky bude také politika bezpečnosti informací a příručka systému řízení bezpečnosti informací v souladu s požadavky Zadavatele a legislativními normami (např. ZoKB, GDPR). Zpracujeme také návrh řízení kontinuity činností IAM (BCM), včetně opatření pro obnovu provozu, a to s ohledem na architekturu a provozní model řešení. Dokumentace bude připravena v editovatelném formátu a předána k finálnímu schválení Zadavatelem.

Tabulka 57 – Požadavky na dokumentaci softwarového díla

8.4.2 Požadavky na školení a přenos znalostí

ID	Požadavek	Způsob naplnění
239	Zhotovitel MUSÍ zrealizovat v sídle zadavatele prezenční zaškolení pro IT administrátory zadavatele minimálně v rozsahu provozní dokumentace. Školení bude pokrývat všechny komponenty dodávané v rámci předmětu plnění, a to minimálně v rozsahu: • běžných administrátorských činností pro implementované systémy,	Požadavek je naplněn kompletně. Zhotovitel provede prezenční školení v sídle Zadavatele v požadovaném rozsahu minimálně 12 hodin, přičemž alespoň 8 hodin bude věnováno oblasti správy identit (IDM). Školení pokryje všechny dodávané komponenty IAM, a to jak z pohledu běžné administrace a údržby, tak i identifikace a řešení nestandardních stavů.

ID	Požadavek	Způsob naplnění
	• standardní údržby systémů pro administrátory zadavatele • základní identifikace nestandardních stavů systému a jejich příčin. Minimální požadovaný rozsah zaškolení pro administrátory je 12 hodin, z toho min. 8 hodin pro oblast systému správy identit (Identity Management). Předpokládaný počet administrátorů (účastníků školení) je max. 7 osob. Zadavatel pro účely zaškolení zajistí a zpřístupní učebnu vybavenou notebooky, prezentační technikou (ve smyslu projektor, tabule pro psaní / kreslení) a dále zajistí konektivitu do vnitřní sítě zadavatele.	Obsah školení bude vycházet z provozní dokumentace a přizpůsobíme jej úrovni znalostí účastníků. Zaškolení provedou členové realizačního týmu, kteří se podíleli na implementaci. Konkrétní harmonogram a strukturu školení připravíme a předložíme Zadavateli ke schválení v rámci implementační fáze.

Tabulka 58 – Požadavky na školení

8.4.3 Požadavky na zálohování

ID	Požadavek	Způsob naplnění
240	Data IAM MUSÍ být Dodavatelem pravidelně zálohovaná Aplikace MUSÍ být zálohovatelná běžnými zálohovacími SW s komerční podporou (podpora MUSÍ být po dobu celého trvání smlouvy, licence MUSÍ být převedeny na FS). Aplikace MUSÍ umožnit oddělené zálohování virtuálních serverů a dat DB a struktura celého dodaného řešení MUSÍ být taková, aby byly odděleny jednotlivé serverové instance a vlastní (například databázová, aplikační) data tak, aby bylo možné zálohovat s rozdílnou četností jednotlivé serverové instance a s jinou vlastní (například databázová, aplikační) data. HW pro zálohování bude zajištěn ze strany zadavatele a bude umístěn v infrastruktuře zadavatele. Aplikační instalace, data a logy musí být oddělené tak, aby je bylo možné zálohovat s rozdílnou četností. Plné zálohování MUSÍ být možné provádět bez nutnosti provozní odstávky řešení. O pohybu zálohovaných dat (např. přesun do jiné lokality datového centra) MUSÍ být veden záznam. V případě havárie a potřebné obnovy provozu (serverů, nastavení, databází, dat) tuto obnovu provede Dodavatel. V případě havárie a potřebné obnovy provozu (serverů, nastavení, databází, dat) MUSÍ být tato obnova také realizovatelná Objednatelem, bez nutné přímé spolupráce s Dodavatelem, a to na základě Dodavatelem dodaného dokumentu „Postup při obnově provozu“.	Požadavek je naplněn kompletně. Zajistíme pravidelné zálohování veškerých relevantních dat IAM včetně konfigurací, databází a logů, a to způsobem kompatibilním s běžnými zálohovacími nástroji se zajištěnou komerční podporou po dobu trvání smlouvy. Zálohovací architektura bude navržena tak, aby byla umožněna samostatná záloha aplikačních a databázových dat, včetně oddělení jednotlivých serverových instancí (např. IDM, AM, databáze, logy). Zálohování bude možné provádět bez odstávky produkčního prostředí, pomocí snapshotů nebo replikace. Pro případ havárie dodáme podrobný návod „Postup při obnově provozu“, na jehož základě bude možné provést obnovu i bez přímé účasti Zhotovitele. Tyto postupy budou otestovány během přebírání řešení.

ID	Požadavek	Způsob naplnění
241	IDM MUSÍ umožňovat pravidelné zálohy konfigurací jednotlivých komponent pro jejich obnovení v případě výpadku nebo selhání. Dodavatel jako součást implementační analýzy identifikuje veškerá data a konfigurace, která je třeba zálohovat pro zajištění případné řádné obnovy řešení IAM v případě havárie s následkem úplné ztráty produkčního nebo testovacího prostředí. Systémy pro zálohování, konfiguraci těchto systémů, jejich testování a provoz záložních rutin zajistí Dodavatel. Zadavatel zajistí hardwarovou infrastrukturu pro provoz zálohovacího řešení navrženého Dodavatelem. Dodavatel v rámci návrhu architektury provede: • Přehled všech klíčových dat vyžadujících zálohování či jiné zabezpečení; • Návrh plánu zálohování všech klíčových dat; • Vývoj rutin nebo nastavení zálohovacího systému pro vykonávání zálohovacích úloh; • Návrh plánů a postupů pro obnovu IAM řešení v případě havárie; • Návrh procesů a postupů pro testování plánů a postupů pro obnovu řešení zahrnujících i testování záložních médií. Plán zálohování včetně všech nezbytných aktivit a jejich popisu bude uveden v provozní dokumentaci IAM. Součástí plánu a popisu budou i postupy řízeného zastavení systému a nuceného odstavení jednoho datového centra.	Požadavek je naplněn kompletně. Zhotovitel v rámci implementační analýzy identifikuje veškerá důležitá konfigurační data a komponenty systému IAM, které bude nutné pravidelně zálohovat. Navrhneme kompletní architekturu zálohování včetně frekvence záloh a jejich testování a následně zajistíme konfiguraci a nasazení zálohovacích rutin, např. pomocí plánovaných skriptů. Součástí dodávky bude přehled klíčových dat a zpracovaný plán obnovy řešení IAM, včetně postupů pro řízené zastavení systému a havarijní scénáře. Plán zálohování bude podrobně popsán v provozní dokumentaci a umožní samostatnou obnovu prostředí Zadavatelem.
242	IAM MUSÍ být navrženo tak, aby maximální doba pro obnovení	Požadavek je naplněn kompletně.

ID	Požadavek	Způsob naplnění
	dat a návratu nedostupného systému do produkce byla maximálně 4 hodiny. Tzn. že Recovery Time Objective (zkr. RTO) <= 4 hodiny.	Zhotovitel navrhne řešení IAM tak, aby v běžných provozních scénářích bylo možné provést obnovu systému do produkčního stavu do 4 hodin (RTO <= 4 hod). Tohoto cíle bude dosaženo důsledným rozdělením aplikační, databázové a zálohovací vrstvy, zavedením zálohovacích rutin bez odstávky a dokumentovaným plánem obnovy. Současně upozorňujeme, že v případě výpadku infrastruktury mimo náš vliv (např. ztráta celé lokality/datacentra) bude schopnost obnovy záviset na dostupnosti infrastruktury a spolupráci dalších dodavatelů.
243	IAM MUSÍ být zároveň navržena tak, aby maximální doba ztráty dat byla 24 hodin. Tzn. že Recovery Point Objective (zkr. RPO) <= 24 hodin.	Požadavek je naplněn kompletně. Zhotovitel navrhne řešení IAM tak, aby bylo možné zajistit maximální ztrátu dat do 24 hodin (RPO <= 24 hod). Toho dosáhneme pravidelným zálohováním databází, konfiguračních souborů a auditních záznamů v minimálně denním intervalu.

Tabulka 59 – Požadavky na zálohování

9 ROZSAH DODÁVKY – PŘESNÉ ZADÁNÍ PRO IMPLEMENTACI

Zadavatel požaduje dodat dílo v níže uvedeném rozsahu s ohledem na výše uvedené požadavky pro IAM (interní/externí IDM, AM). Níže uvedený rozsah bude realizován v rámci nulté rozvojové fáze. Další fáze s ohledem na požadavky Zadavatele a návrhy Dodavatele budou po odsouhlasení Zadavatele kryty prostředky rozvojového MD fondu.

9.1 Převzetí podpory

- Převzetí podpory stávajícího řešení IDM bude provedeno na základě akceptace.

9.2 Analýza IDM

- Analýza zdrojových dat a cílových systémů
- Analýza identit, rolí, procesů a metodik
- Analýza rizik a analýza dopadu legislativy
- Analýza a návrh datového modelu správy identit
- Analýza integrace a napojení na vybrané koncové systémy (viz níže specifikovaný počet)
- Návrh business rolí, aplikačních a technických rolí
- Návrh procesů správy životního cyklu identit
- Návrh postupu při napojování cílových systémů – podklad pro třetí strany, které budou napojovány na IDM
- Návrh architektury a infrastruktury IDM
- Návrh harmonogramu implementace IDM

9.3 Instalace IDM

Instalace IDM do třech nezávislých prostředí Zadavatele (Vývoj, Test, Produkce). Hardwarové požadavky budou upřesněny v rámci analýzy.

Součástí systémové integrace a instalace bude i konfigurace a návrh deployment procesů / nasazování nových verzí, patchů a dalších komponent IDM na jednotlivá prostředí.

On-line koncové systémy jsou řízené – spravované přímo IDM a evidence této správy je vedena tamtéž.
On-line koncové systémy jsou připojené pomocí:

- Konektoru LDAP, Active Directory, nebo
- Proprietárního konektoru, nebo
- Databázového konektoru, nebo
- Rozhraní webových služeb.

Off-line koncové systémy jsou řízené – spravované nepřímo přes systémové administrátory, ale evidence této správy je uložená v IDM.

9.4 Napojení IDM

Zadavatel požaduje jednosměrné napojení (čtení) na data personálního systému, coby autoritativního zdroje personálních dat. Konsolidace dat, resp. konsolidace identit bude upřesněna v rámci implementační analýzy a je požadována v rámci této dodávky.

9.4.1 Typy objektů

Z autoritativního zdroje dat budou do IDM načítány následující typy objektů:

- Zaměstnanci
- Pracovníci na DPČ
- Pracovníci na DPP
- Organizační struktura
- Pracovní místa

Externisté budou zakládáni přímo v GUI IDM odpovědným uživatelem.

9.4.2 Koncové systémy napojené na IDM

Zadavatel v rámci analýzy Dodavatele určí maximální počet 10 informačních systémů, které budou v první fázi implementace jako koncové systémy napojeny na IDM (interní/externí). Součinnost Dodavatelů třetích stran koncových systémů jde plně k tíži Zadavatele.

9.5 IDM životní cyklus identit

Zadavatel požaduje implementace následujícího životního cyklu pro načítané objekty:

- Načítání personálních informací o identitách z autoritativního zdroje v definovaných periodách, jejich konsolidaci a vytvoření unikátní identity.
- Dynamické vytváření objektů organizační struktury v IDM dle organizační struktury v HR systému zadavatele.
- Dynamické vytváření uživatelů v IDM, atributy uživatele evidované IDM provázané s HR, procesy (založení, aktualizace, aktivace/deaktivace identity, přejmenování, změna organizační struktury, operace s aplikačními rolemi apod.) a mechanismus generování centrálního username, password a e-mailové adresy. E-mailová notifikace. Doručení iniciálního hesla vedoucímu nového uživatele e-mailem.
- Vytvoření 3 Business rolí.
- Automatizace přiřazení do Business rolí na základě informací z HR.
- Generování unikátního ID (neměnné číslo) pro každou identitu.
- Vytváření IDM procesů v návaznosti na informace z HR a do koncových systémů (založení, aktualizace, aktivace/deaktivace identity, přejmenování, změna organizační struktury, operace s aplikačními rolemi apod.)
- Aktualizace uživatele v koncových systémech:
    - Aktualizace všech atributů identity, které jsou vzájemně evidovány v IDM a koncových systémech na základě informací z HR.
- Aktivace a deaktivace v koncových systémech:
    - Pokud to koncový systém dovoluje, aktivování nebo deaktivování uživatele v koncovém systému na základě informací z HR a atributů platnost od a do.
- Přiřazení a odebrání aplikačních rolí:
    - Přiřazování a odebírání aplikačních rolí v koncových systémech na základě Business rolí, nebo ručním zásahu administrátora.
- Načítání aplikační rolí z koncových systémů a narovnání zjištěných nesouladů mezi koncovým systémem a IDM.
- Načítání uživatelů v koncových systémech a narovnání zjištěných nesouladů mezi koncovým systémem a IDM.
- Dvou-krokové workflow pro přidání/odebrání rolí uživateli včetně schvalování.

- Rozhraní pro uživatele, ve kterém si budou moci žádat o přidělení nových aplikačních rolí.
- Vytvoření rolí, které zajišťují autorizaci uživatele pro práci v IDM (např. administrátor, správce rolí, koncový uživatel apod.)
- E-mailovou notifikaci s ohledem na operace s uživateli.
- Dodávku následujících reportů:
    - Report oprávnění, která jsou u uživatele přiřazena v koncovém systému, ale nejsou přiřazena jako role v IDM.
    - Report účtů, ke kterým existuje v IDM vlastník, ale které vznikly mimo vědomí IDM.
    - Uživatelský report, auditní report (změny provedené přes IDM), rekonciliační report.

9.6 Analýza AM

Cílem oblasti Access managementu (AM) jako součást IAM je ověření interních, případně externích identit, bezpečné a automatizované přihlašování uživatelů ke koncovým systémům Zadavatele.

Z těchto důvodů je požadavkem Zadavatele realizace analýzy v tomto rozsahu:

- Způsoby autentizace uživatelů do autentizační infrastruktury včetně externích poskytovatelů identity (NIA, JIP/KAAS). Definice jednotlivých aktérů, přistupujících k autentizační infrastruktuře, různé metody autentizace, výběr autentizační metody.
- Způsob tvorby identit a jejich uložení v prostředí Zadavatele, mapování na identifikátory u externích poskytovatelů identity (NIA, JIP/KAAS). Specifikace zdrojů identit a autentizačních údajů (AD), návrh způsobu uložení identifikátorů uživatelů externích poskytovatelů a jejich správa.
- Metodika zapojování aplikací do autentizační infrastruktury. Způsob připojení aplikací do autentizační infrastruktury prostřednictvím protokolů OIDC, SAML2, OAuth.
- Návrh autentizační infrastruktury. Popis jednotlivých komponent autentizační infrastruktury a komunikační schéma. Obsahem budou zejména diagramy jednotlivých komponent, jejich umístění v infrastruktuře Zadavatele, vzájemná komunikace mezi komponentami a komponentami třetích stran (externí poskytovatelé identit, autentizační zdroje, integrované aplikace).
- Návrh zapojení vybraných aplikací / systémů do autentizační infrastruktury. Popis, jakým způsobem budou integrovány vybrané aplikace Zadavatele do autentizační infrastruktury.
- Seznam požadavků, které musí splňovat nové / v budoucnu připojované aplikace tak, aby byly jednoduše integrovatelné s autentizační infrastrukturou Zadavatele a aby případné budoucí změny v autentizační infrastruktuře nevyvolaly požadavek na změnu v takto integrovaných aplikacích.
- V rámci analýzy Dodavatel poskytne dotazník, který bude sloužit k oslovení dodavatelů třetích stran, provozujících informační systémy Zadavatele, které mají být dotčené integrací na Access management pro zajištění procesů jednotného a automatizovaného přihlašování (SSO).
- Vyhodnocení dotazníků a provedení zhodnocení/doporučení.

- Dodavatel se Zadavatelem určí a vyberou 5 informačních systémů, které budou následně Dodavatelem napojeny na Access management za součinnosti Dodavatelů třetích stran. Součinnost Dodavatelů třetích stran jde plně k tíži Zadavatele.

9.7 Instalace AM

Instalace AM do třech nezávislých prostředí Zadavatele (Vývoj, Test, Produkce) Hardwarové požadavky budou upřesněny v rámci analýzy.
AM bude vybudované ve vysoké dostupnosti, a to z toho důvodu, že se jedná o kritický systém, jehož případný výpadek má významný dopad na poskytování služeb uživatelům.

9.8 Napojení AM

Externí uživatelé budou ověřovány prostřednictvím vybudované identitní brány. Hlavní cíle projektu na implementaci Autentizační infrastruktury a dále pak vybudování identitní brány do interních aplikací i aplikací třetích stran využívaných interními uživateli i externími spolupracujícími subjekty jsou v podobě:

- Standardizace autentizace nově realizovaných aplikací
- Napojení na informační systém pro správu a řízení identit pro přidělení autorizací
- Podpora autentizace vůči internímu způsobu ověřování (interní DB, interní systém)
- Podpora využití externí autentizační autority (NIA, JIP/KAAS, MojeID, BankID) pro autentizaci a identifikaci
- Harmonizace v přístupu k ověřování interních i externích uživatelů
- V případě souhlasu uživatele možnost čerpat dodatečné údaje od externího poskytovatele identity
- Evidence pokusů uživatelů o přihlášení do všech aplikací na jednom místě, včetně souhrnných reportů a logů možných předávat do systému SIEM
- Informace o aktuálně přihlášených uživatelích
- Jednotné přihlášení pro napojené aplikace (SSO) včetně možnosti nastavit interval přihlášení do napojených aplikací
- Řízení souhlasů uživatelů před předáním uživatelských dat a potvrzování podmínek užití
- Umožnění provozu v režimu vysoké dostupnosti (HA)

V případě napojení identitní brány na interní informační systém spravující identity uživatelů a současného propojení na externího poskytovatele identity lze od tohoto poskytovatele čerpat údaje o uživatelích a ty následně propagovat do interních záznamů identit. Vzorový scénář s využitím těchto propojení může vypadat následovně:

- Uživatel bez předchozího vztahu k internímu systému dostane pozvánku pro připojení se k aplikaci napojené na identitní bránu
- Při využití této pozvánky je uživatel přesměrován na identitní bránu
- Brána nabídne uživateli možnosti ověření identity proti externím poskytovatelům identit dle přednastavených možností (NIA, JIP/KAAS, MojeID, BankID)
    - Současně s požadavkem na ověření uživatele je na externího poskytovatele identity zaslána také žádost o poskytnutí údajů potřebných pro interní systém spravující identity uživatelů

- Uživatel se ověří dle výběru z nabízených možností a odsouhlasí poskytnutí údajů pro interní systém spravující identity uživatelů
- Identitní brána povolí uživateli přístup do dané aplikace
- Údaje o uživateli poskytnuté od externího poskytovatele identit jsou odeslány do interního systému a uživateli je založena identita dle těchto údajů
    - V případě, že uživatel má již v interním systému vytvořenou identitu nebo některé zásadní identifikační údaje souhlasí s již vytvořenou identitou, tak je tato identita doplněna nově příchozími údaji

9.9 Testování

Než bude akceptováno nasazení celého řešení IAM do produkce, budou popsány testy – akceptační scénáře, které budou sloužit pro akceptaci.

Přesné zadání doplní Zadavatel nebo bude doplněno v rámci analýzy.

Testováno bude minimálně:

- životní cyklus identit – autentizační a autorizační procesy
- životní cyklus rolí
- životní cyklus organizační struktury
- autentizace oproti Active Directory

9.10 Migrace

Zadavatel požaduje provést:

- iniciální načtení identit, rolí a organizační struktury do celého nového řešení IAM
- import vazeb mezi identitami, rolemi a organizační strukturou
- realizovat načtení zaměstnanců mimo evidenci (např. mateřské a rodičovské dovolené)
- napojení identit, rolí a organizační struktury na existující objekty v jednotlivých koncových systémech
- nastavení pravidelných synchronizačních úloh

9.11 Školení

Pro práci s IAM a jejich správu je nutné proškolit:

- uživatele, minimálně klíčové uživatele IAM
- administrátory – správce IAM

9.12 Podpora provozu a rozvoje nového řešení IAM

Provozní podporu vyvinutého řešení IAM obsahuje také monitoring IAM. Monitorovací systém bude zabudován do vnitřní sítě zadavatele.

9.13 Harmonogram

Níže je uveden požadovaný harmonogram realizace prací. Písmeno „T“ představuje termín zahájení prací na rozvoji nástroje.

Fáze	Popis	Termíny	Časová osa
Fáze 0 – Převzetí podpory	Převzetí stávajícího IDM a provedení analytických a revizních činností	T + 3 měsíce	3 měsíce
Fáze 1 – Analýza IDM int	Analýza IDM interní	T + 3 měsíce	3 měsíce
Fáze 2 – Analýza IDM ext	Analýza IDM externí	T + 5 měsíců	5 měsíců
Fáze 3 – Analýza AM int	Analýza AM interní	T + 3 měsíce	3 měsíce
Fáze 4 – Analýza AM ext	Analýza AM externí	T + 5 měsíců	5 měsíců
Fáze 5 – Poskytnutí všech potřebných licencí IAM	Licence IDM a AM pro interní a externí prostředí pro celé období projektu	T + 3 měsíce	3 měsíce
Fáze 6 – infrastruktura IDM int	Implementace a systémová integrace infrastruktury IDM interní	F1 + 1 měsíc	4 měsíce
Fáze 7 – infrastruktura IDM ext	Implementace a systémová integrace infrastruktury IDM externí	F2 + 2 měsíce	7 měsíců
Fáze 8 – infrastruktura AM int	Implementace a systémová integrace infrastruktury AM interní	F3 + 1 měsíc	4 měsíce
Fáze 9 – infrastruktura AM ext	Implementace a systémová integrace infrastruktury AM externí	F4 + 2 měsíce	7 měsíců
Fáze 10 – integrace na koncové systémy IDM int	Konfigurace a nastavení základních IDM procesů a integrace na vyjmenované koncové systémy IDM interní	F6 + 6 měsíců	10 měsíců
Fáze 11 – integrace na koncové systémy IDM ext	Konfigurace a nastavení základních IDM procesů a integrace na vyjmenované koncové systémy IDM externí	F7 + 6 měsíců	13 měsíců
Fáze 12 – integrace na koncové systémy AM int	Konfigurace a nastavení základních AM procesů a integrace na vyjmenované koncové systémy AM interní	F8 + 6 měsíců	10 měsíců
Fáze 13 – integrace na koncové systémy AM ext	Konfigurace a nastavení základních AM procesů a integrace na vyjmenované koncové systémy AM externí	F9 + 6 měsíců	13 měsíců
Fáze 14 – testování a školení IDM int	Testování IDM procesů a napojení na koncové systémy IDM interní, školení administrátorů a vybrané skupiny klíčových uživatelů	F10 + 2 měsíce	12 měsíců

Fáze 15 – testování a školení IDM ext	Testování IDM procesů a napojení na koncové systémy IDM externí, školení administrátorů a vybrané skupiny klíčových uživatelů	F11 + 2 měsíce	15 měsíců
Fáze 16 – testování a školení AM int	Testování AM procesů a napojení na koncové systémy AM interní, školení administrátorů a vybrané skupiny klíčových uživatelů	F12 + 2 měsíce	12 měsíců
Fáze 17 – testování a školení AM ext	Testování AM procesů a napojení na koncové systémy AM externí, školení administrátorů a vybrané skupiny klíčových uživatelů	F13 + 2 měsíce	15 měsíců
Fáze 18 – podpora provozu IDM int	Provozní podpora a SLA pro IDM interní	F17 + 48 měsíců	63 měsíců
Fáze 19 – podpora provozu IDM ext	Provozní podpora a SLA pro IDM externí	F17 + 48 měsíců	63 měsíců
Fáze 20 – podpora provozu AM int	Provozní podpora a SLA pro AM interní	F17 + 48 měsíců	63 měsíců
Fáze 21 – podpora provozu AM ext	Provozní podpora a SLA pro AM externí	F17 + 48 měsíců	63 měsíců
Fáze 22 – rozvoj IAM interní	Rozvoj IAM interní z časového fondu (školení, analytické, programátorské a další technické aktivity rozvoje IAM	F17 + 48 měsíců	63 měsíců
Fáze 23 – rozvoj IAM externí	Rozvoj IAM externí z časového fondu (školení, analytické, programátorské a další technické aktivity rozvoje IAM	F17 + 48 měsíců	63 měsíců