ŘEDITELSTVÍ SILNIC A DÁLNIC ČR

D Í L Č Í O B J E D N Á V K A č. 5

Číslo související rámcové dohody: 01IN-003773 (dále jen „rámcová dohoda")

Číslo dílčí objednávky: 01IN-004080

Ze dne: 9. 10.2019

Objednatel:
Ředitelství silnic a dálnic ČR
Adresa sídla: Na Pankráci 56,
140 00 Praha 4 - Nusle
IČO: 65993390
DIČ: CZ65993390

Dodavatel:
IBA CZ, s.r.o.
Adresa: Radlická 751/113e,
158 00 Praha 5
IČO: 25783572
DIČ: CZ25783572
[redacted]

Tato dílčí objednávka je návrhem na uzavření dílčí smlouvy ve smyslu čl. III uzavřené Rámcové dohody. Způsob akceptace dílčí objednávky Dodavatelem (uzavření dílčí smlouvy), obchodní a platební podmínky a další práva a povinnosti Smluvních stran touto dílčí dohodou výslovně neupravená stanovuje rámcová dohoda.

Na základě uzavřené rámcové dohody u Vás objednáváme:

Návrh řešení na IDM a CAS, v rozsahu obsahu odsouhlaseného návrhového dokumentu ze dne 09. 10. 2019 (dále jen „Návrh řešení");

Místo dodání: Ředitelství silnic a dálnic ČR, generální ředitelství Praha 4, Čerčanská 2023/12, 140 00 Praha 4 – Krč;

Termín dodání: Zahájení poskytování podpory je stanoveno do 10 pracovních dnů od zveřejnění této dílčí objednávky v registru smluv. Práce na realizaci ad-hoc požadavku L3 podpory v rozsahu do vyčerpání disponibilního paušálního limitu jsou zahájeny neprodleně po jeho obdržení, nebo dle specifikace v něm uvedené. Případné vícepráce nad disponibilní limit budou vykonány na základě samostatné dílčí objednávky. Služba bude poskytována 12 vyhodnocovacích období, kdy 1. vyhodnocovací období započne podpisem protokolu o zahájení poskytování podpory/služby.

Kontaktní osoba Objednatele: [redacted]

Celková hodnota objednávky v Kč bez DPH / s DPH: 1 302 560,-Kč/ 1 576 097,60,-Kč

Fakturační adresa: Ředitelství silnic a dálnic ČR, Na Pankráci 546/56, 145 05 Praha 4 - Nusle. Fakturu prosíme zaslat na adresu: Ředitelství silnic a dálnic ČR, Čerčanská 2023/12,

140 00 Praha 4 - Krč, v případě faktury v elektronické podobě na adresu: posta@rsd.cz. Nedílnou součástí faktury jsou předávací listy/protokoly potvrzené zástupcem Objednatele.

Jméno a příjmení oprávněné osoby objednatele: [redacted]

V případě akceptace této dílčí objednávky, Dodavatel objednávku elektronicky podepíše a zašle na e-mailovou adresu kontaktní osoby Objednatele, s kopií na e-mailovou adresu [redacted]. Objednávka je účinná dnem uveřejnění v Registru Smluv.

PODEPSÁNO PROSTŘEDNICTVÍM UZNÁVANÉHO ELEKTRONICKÉHO PODPISU DLE ZÁKONA Č. 297/2016 SB., O SLUŽBÁCH VYTVÁŘEJÍCÍCH DŮVĚRU PRO ELEKTRONICKÉ TRANSAKCE, VE ZNĚNÍ POZDĚJŠÍCH PŘEDPISŮ.

Příloha: Návrh řešení na IDM a CAS
(Návrh řešení na IDM a CAS.pdf)

Návrh řešení na IDM a CAS

Pro společnost:

Ředitelství silnic a dálnic ČR

Za společnost IBA CZ, s.r.o. zpracoval:

[redacted]

Project Manager

Dne: 9. 10. 2019

OBSAH

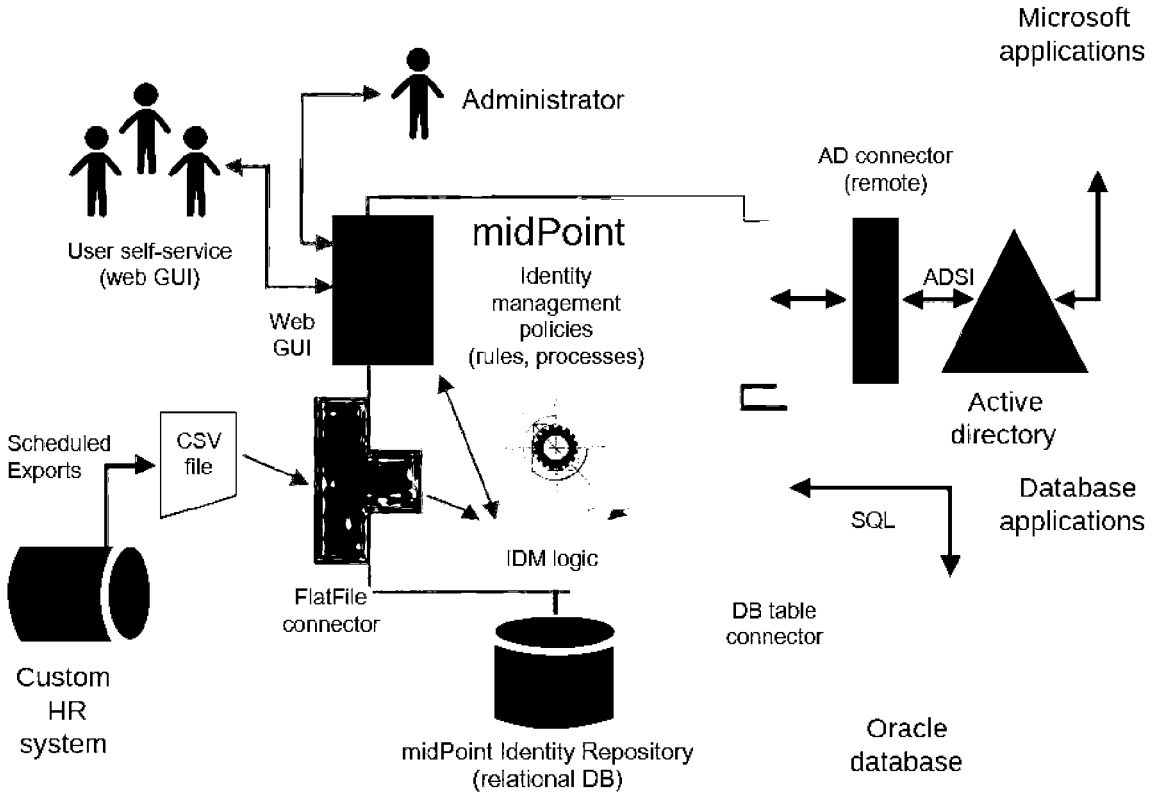
1. Popis požadavku

1.1 Shrnutí

Návrh řešení je vytvořen na základě požadavku ŘSD, kdy cílem požadavku je úprava Nadstavbového systému řízení účtů a jeho integrace do prostředí ŘSD ČR včetně komunikace s novým personálním systémem OKBASE, včetně 2 faktorové autorizace. V rámci před projektové aktivity vznikly ze strany ŘSD požadavky, ke kterým IBA CZ vypracovala upravený návrh řešení, jehož detail je uveden kapitole 4 návrhu řešení.

1.2 Identity and Access Management (IAM)

MidPoint jako hlavní prvek řešení zajišťuje služby centrálního úložiště identit, rolí, politik, vlastní napojení na koncové systémy a centrální propagaci účtů. Produkt obsahuje komplexní workflow pro schvalování jako out-of-box funkcionalitu. Většinu standardních scénářů je tak možné jednoduše nakonfigurovat bez nutnosti programování (s výjimkou skriptovacích výrazů v atributech pro mapování). Ze zkušeností je toto workflow dostačující pro 80 % schvalovacích procesů.



Obrázek 1 Deployment diagram midPoint IAM

Součástí produktu jsou odděleny uživatelská rozhraní (prostřednictvím povolení) pro administrátory i koncových uživatelů. Jejich vzhled lze upravit dle požadavků zákazníka. Rozhraní je velmi intuitivní, koncový uživatel v něm má k dispozici všechny potřebné nástroje pro vytvoření žádostí o přidělení rolí, změnu uživatelského profilu, změnu hesla apod. Samotné řešení je vysoce modulární, což umožňuje jeho škálovatelnost a rozložení výkonu na jednotlivé komponenty.

IBA CZ, s. r. o.,
Radlická 751/113e, 158 00 Praha 5
www.ibacz.eu info@ibacz.eu (+420) 251 050 100

NAPOJENÍ AUTORITATÍVNÍCH/KONCOVÝCH SYSTÉMOV: pro potřeby integrace koncových systémů je možné využít jakýkoliv z nativních konektorů. Aktuálně je k dispozici několik desítek konektorů, pokrývající téměř všechny rozšířené koncové systémy.

Seznam podporovaných (out-of-box) konektorů umožňujících integraci s cílovými systémy je k dispozici zde: https://wiki.evolveum.com/display/midPoint/Identity+Connectors

V případě že zákazník využívá vlastní proprietární systém, který disponuje vlastním integračním rozhraním, je možné vyvinout také vlastní konektor.

WORKFLOW: ZPRÁVA ŽIVOTNÍHO CYKLU IDENTIT: součástí produktu je zabudovaný workflow engine, který zajišťuje procesní vazby mezi jednotlivými kroky vedoucími ke změně parametrů identit nebo účtů na cílových systémech. Produkt podporuje mechanismy pro zpětné načtení a validaci účtů z koncových systémů tzv. proces rekoncilace. Primární tento proces slouží ke kontrole dodržování nastavených pravidel (dodržování compliance) jakož i kontrolu konzistence dat mezi IDM a koncovým systémem.

WORKFLOW: SCHVALOVÁNÍ: v rámci produktu je možné modelovat vlastní schvalovací schémata – produkt má nativní podporu jednoúrovňového ale i N-úrovňového schvalování, kde při přechodu mezi jednotlivými stavy je možné zasílat různé notifikační zprávy.

ZPRÁVA ŽIVOTNÍHO CYKLU ROLÍ (RBAC): produkt poskytuje nástroje pro kompletní správu životního cyklu rolí (založení, modifikaci, odstranění role, přiřazení uživateli). Nativně podporuje mechanismy pro definici oddělení odpovědnosti a neslučitelnosti rolí (principy SoD – Segregation of Duties).

MANAGEMENT PŘÍSTUPŮ IDENTIT: přiřazení rolí identitě může být na základě vytvořeného požadavku (principy Role Based Access Control), přičemž v rámci žádosti lze omezit platnost role na vybrané časové období. Po uplynutí doby platnosti přiřazení je role automaticky identitě odebrána, což má za následek modifikaci účtu na straně koncového systému.

Kromě RBAC přístupu lze nakonfigurovat dynamické přidělování rolí, například na základě specifického atributu identity (principy Attribute Based Access Control), typicky podle nákladového střediska / lokality, nebo také přidělování rolí na základě funkčního zařazení (principy Functional Based Access Control) např. podle pracovní pozice zaměstnance.

ZPRÁVA ORGANIZAČNÍ STRUKTURY: produkt poskytuje kompletní nástroje pro správu a modelování organizačních struktur. Nativní vlastností produktu je možnost definování a přiřazení více (paralelních) organizačních struktur na identitu, což umožňuje kategorizovat identity např. podle pracovních skupin / týmů / projektové hierarchie apod.

EMAILOVÉ NOTIFIKACE: se používají v rámci produktu na oznamování různých událostí z procesů běžících na úrovni systému MIDPOINT. Formát odesílaných emailových oznámení je prostý text (plain-text) nebo také HTML. Produkt disponuje nativními notifikačními šablonami (plain-text), případně je možné definovat vlastní notifikační šablony na základě požadavků zákazníka.

SMS NOTIFIKACE: systém lze integrovat s vlastní SMS bránou (prostřednictvím REST služeb), typicky se tento typ oznámení využívá při distribucí inicializačních hesel.

SAMOOBSLUHA: je určena pro koncové uživatele, kde má uživatel možnost např. vytvořit požadavek na přiřazení nebo odebrání role, požádat o změnu hesla nebo také schvalovat přiřazení žádosti, sledovat stav realizace vlastních požadavků. Viditelnost vybraných sekci je možné kontrolovat prostřednictvím autorizací.

UI PRO ADMINISTRACI: autorizovaná zóna pro komplexní administraci identit, rolí a organizačních jednotek. Produkt podporuje fulltextové vyhledávání, filtrování výsledků na základě vstupních parametrů jako hromadný import jednotlivých entit. Rozhraní je vytvořeno jako webová stránka s dynamickými prvky.

REST API ROZHRANÍ: poskytuje plnohodnotné externí rozhraní na bázi protokolu REST. Toto rozhraní tak umožňuje integraci na další aplikace v prostředí zákazníka.

IBA CZ, s. r. o., Radlická 751/113e, 158 00 Praha 5 www.ibacz.eu info@ibacz.eu (+420) 251 050 100

RECERTIFIKÁCE PŘÍSTUPŮ: umožňuje pravidelně kontrolovat přístupová práva identit pomocí řízeného re-certifikačního procesu.

LOKALIZACE: produkt je lokalizován do několika světových jazyků, včetně českého, slovenského i anglického jazyka.

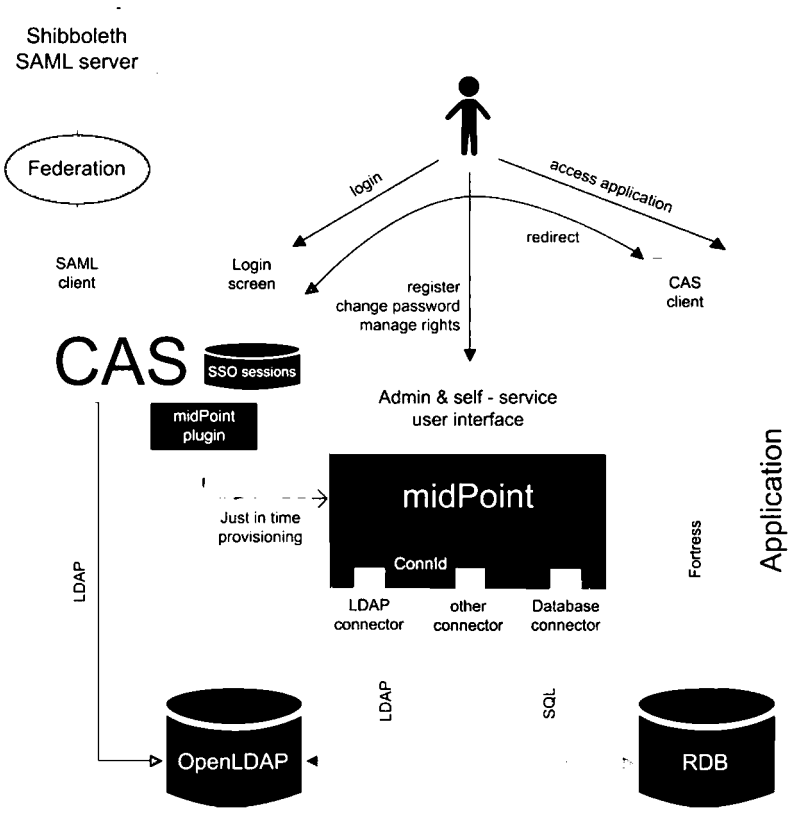
REPORTING A AUDITING: produkt nativně poskytuje přehledy o stavu systému a prováděných aktivitách. Zaznamenává a poskytuje historické informace a umožňuje reprezentaci těchto dat prostřednictvím nativních reportů.

1.3 Popis a integrace na centrální Autentizační Službu (CAS)

Integrace IDM a CAS bude zajištěna na základě nativních vlastností obou produktů. Integrační platformou bude datové úložiště na platformě LDAP. Konkrétně se jedná o apereo CAS server https://apereo.github.io/cas/6.0.x/index.html. Jedná se Open Source SSO platformu, která je dobře škálovatelná. Má OOTB podporu různých typu MFA, včetně emailu. MFA je řešena prostřednictvím provideru a pokud by nevyhovoval ani jeden z nabízených, lze si provider jednoduše doprogramovat.

Kompletní management uživatelských entit jakož i ostatních objektů úložiště (ou, skupiny, role apod.) bude zajišťován IAM. Pro koncové uživatele bude IAM poskytovat služby uživatelské samoobsluhy, jejímž prostřednictvím budou realizovat své žádosti o přístupová oprávnění případně provádět aktualizaci vlastních vybraných atributů, změnu hesla. Pro klíčové uživatele bude IAM navíc poskytovat služby pro správu přístupových oprávnění, schvalování žádostí apod.

Integrace LDAP úložiště s IAM bude prostřednictvím nativního LDAP konektoru, kterým řešení disponuje.



Obrázek 2 High-level integrace řešení CAS a IAM

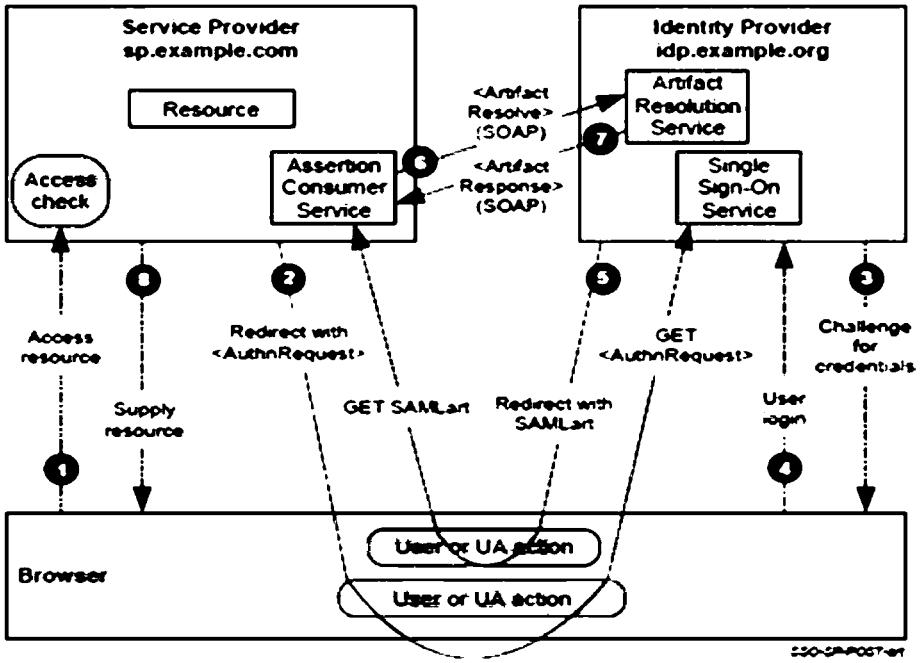
IBA CZ, s. r. o.,
Radlická 751/113e, 158 00 Praha 5
www.ibacz.eu info@ibacz.eu (+420) 251 050 100

Konzumentem dat v LDAP bude systém CAS. Ten bude data v úložišti využívat jako svou datovou základnu (user-base repository) pro potřeby autentifikačních procesů. V případě potřeby aktualizace atributů v LDAP úložišti z prostředí CAS lze integraci zajistit prostřednictvím vystavených REST API. Veškeré změny nad identitou tak budou auditované přímo v IAM.

Nabízené řešení je postaveno na Open Source, které primárně zajišťuje autentizaci autorizační služby. Typickým případem užití řešení je zajištění služeb pro Single Sign On (SSO). Řešení je možné použít také pro autentizaci uživatelů prostřednictvím mobilních aplikací, API Access Management, 2FA spolu s integrací s IDM řešením midPoint např. i pro automatizovanou správu identit – partnerů, dodavatelů apod., kdy je možné dynamicky vytvářet uživatelů přímo do IDM prostřednictvím SCIM

Pro potřeby přihlašování bude na straně CAS vystavena Přihlašovací stránka (Login Screen), která bude pro uživatele poskytovat služby přihlašování do jednotlivých Aplikací.

Příklad přihlašování koncového uživatele



Samotné přihlášení bude definováno standardem SAML2 a sestává z následujících kroků:

1. *Uživatel se pokusí o přístup k chráněnému zdroji (aplikaci) na straně Service Providera.*
2. *Service Provider identifikuje požadovaný zdroj jako chráněný, vytvoří tzv. autentifikační request obsahující informace o SP, požadované roli atd. a přesměruje uživatele na CAS (pokud je použit tzv. Redirect binding).*
3. *CAS na základě konfigurace a stavu uživatelské session vyhodnotí, které autentifikační metody jsou dostupné a nabídne jejich uživateli (přesměruje na přihlašovací stránku).*
4. *CAS zkontroluje platnost zadaných údajů (jméno / heslo, SMS token atd.), V případě úspěchu spustí příslušné attribute Gatherer a výsledný seznam atributů uloží do CAS session.*
5. *CAS přesměruje zpět na Service Providera, přičemž mu přepošle tzv. SAML Artifact (identifikátor, který později SP použije na Assertion request).*
6. *SP si přes backend channel vyžádá tzv. Authentication response, která obsahuje výsledek autentifikace (seznam získaných rolí) a uživatelské atributy povolené pro daného Service Providera.*

CAS zašle požadované informace.

IBA CZ, s. r. o.,
Radlická 751/113e, 158 00 Praha 5
www.ibacz.eu info@ibacz.eu (+420) 251 050 100

2. Implementace řešení

Z pohledu úspěšné realizace projektu je důležitá volba etap implementace tak, aby při minimální náročnosti poskytla maximální přínos a zajistily výchozí podmínky pro další postup.

Realizace projektu předpokládá velmi úzkou spolupráci se zadavatelem, a to především v oblasti analýzy existujícího prostředí, definice rolí, pravidel a postupů. Tyto práce budou vyžadovat účast osob odpovědných za vytváření postupů pro správu účtů a přístupových oprávnění. Pro ostatní zúčastněné strany se předpokládají konzultace pro určení optimálního způsobu správy na daném systému. Přesný rozsah spolupráce bude specifikován v rámci přípravné fáze projektu.

Navržené etapy jsou:

- Začátek projektu
- Analýza a designe projektu
    - Analýza současného stavu, návrh řešení
    - Akceptace analytické části projektu
- Vývoj a integrace řešení
    - Příprava vývojového prostředí (instalace a konfigurace)
    - Vývoj požadovaných funkčností (úprava a vývoj workflow/adaptérů)
    - Integrace řešení, napojení koncových systémů
    - Akceptace vývojové části projektu
- Testovaní
    - Příprava testovacího prostředí (instalace a konfigurace)
    - Testování integrovaného řešení (QA testy)
    - Akceptace testování
- Produkční nasazení
    - Příprava produkčního prostředí
    - Zavedení pravidelného zálohování, monitoring řešení (poskytnutí součinnosti)
    - Dokumentace skutečného řešení, administrátorské příručky
    - Zaškolení klíčových uživatelů
    - Nasazení do produkčního prostředí, migrace dat, pilotní provoz
- Ukončení projektu
    - Odevzdání a ukončení projektu
    - Akceptace celkového řešení

Pro řešení projektu se předpokládá, že zadavatel poskytne dodavateli prostor pro řešení projektu v budově zadavatele na dobu nezbytně nutnou.

IBA CZ, s. r. o.,
Radlická 751/113e, 158 00 Praha 5
www.ibacz.eu info@ibacz.eu (+420) 251 050 100

3. Součinnost

Požadavky na prostředí zákazníka

Popis síťové a HW infrastruktury potřebné pro provoz navrhovaného řešení.

Návrh infrastruktury nezbytné pro provoz systému závisí na uvažovaném počtu uživatelů a připojených systémů, počtu a četnosti požadavků uživatelů a administrátorů / auditorů. Vycházející ze zkušeností jiných instalaci jsou doporučené následující systémové požadavky.

Aplikačný server:

	Typical up to 5 000 users
CPU	2 cores
RAM	4 GB
Disk space	10 GB
Disk I/O	negligible

Databázový systém:

	Typical up to 5 000 users
CPU	2 cores
RAM	3 GB
Disk space	5 GB
Disk I/O	medium

Během vývoje a nasazení řešení navrhujeme využít následující prostředí:

- *Vývojové prostředí:* slouží k bezprostřední vývoj komponent řešení a může být distribuovány mezi členy realizačního týmu. Sem patří zejména osobní počítače, na kterých se připravuje konfigurace pro chování systému MidPoint / CAS (mapování, pravidla apod.) A konektory pro koncové systémy. V rámci analýzy bude rozhodnuto, zda vývojové prostředí bude u Zadavatele anebo pouze u Zhotovitele.
- *Testovací prostředí:* slouží k otestování funkčnosti vyvinutých komponent a předběžné testování dílčího i celého řešení. Architektura testovacího prostředí je zjednodušená oproti produkčnímu prostředí, nemusí obsahovat reálné údaje o uživatelích, musí však obsahovat všechny typy dat, pomocí kterých se bude řešení testovat (testovací koncové systémy, všechny atributy testovacích uživatelů).
- *Produkční prostředí:* slouží pro provoz řešení.

Požadavky na součinnost

V rámci analytické / vývojové fázi projektu požadujeme součinnost zaměstnanců ŘSD (nebo dodavatelů systému) v roli:

Garant systému (byznys vlastník): v analytické fázi projektu poskytuje konzultace v rozsahu implementovaných procesů, konvenci, implementované politice hesel, poskytovaných integračních rozhraní

IBA CZ, s. r. o.,
Radlická 751/113e, 158 00 Praha 5
www.ibacz.eu info@ibacz.eu (+420) 251 050 100

umožňujících automatizovanou správu účtů, má přehled o významu atributů uživatelského účtu, obsahu atributu (specifikuje algoritmy / pravidla), specifikuje požadovaný syntaxi atributu (např. osobní číslo je 6-ti místné číslo, zleva zarovnané nulami), specifikuje jednoznačné identifikátory, specifikuje číselníkové hodnoty atributů.

Administrátor koncového systému: v analytické fázi projektu (Etapa I) poskytuje konzultace v rozsahu: procesů správy účtu, integračních rozhraních, formátu atributů, jednoznačných identifikátorech, číselníkových hodnotách. V implementační fázi projektu (Etapa II) zajišťuje konfiguraci, funkčnost a dostupnost integračních rozhraní koncového systému.

Dodavatel koncového systému: v případě, že zákazník nespravuje koncový systém ve vlastní režii, nebo nedisponuje zaměstnanci, kteří by měli dostatečné znalosti v rozsahu Garant systému (business vlastník) / Administrátor koncového systému požadujeme zajistit součinnost dodavatele koncového systému, který tyto informace dokáže poskytnout.

Realizace napojení
Integrace koncového systému s MidPoint bude realizována na základě analytické dokumentace vypracované dodavatelem a schválené zákazníkem v rámci Etapy I, projektu IDM. Dokumentace bude obsahovat detailní informace umožňující v rámci Etapy II, provést integraci koncového systému v dohodnutém rozsahu.

Informace potřebné pro realizaci napojení (analytická dokumentace) bude v rozsahu:

- Základní informace o koncovém systému (název, verze, dodavatel, platforma, technologie, vazby na jiné systémy ...)
- Procesy spojené se správou systému (uživatelé, skupiny, role, profily...)
- Seznam a popis lokálních oprávnění definovaných v koncovém systému / aplikaci
- Spravované atributy uživatelských účtů koncového systému / aplikace
- Konfiguraci mapování a transformačních pravidel pro jednotlivé atributy
- Jmenné konvence uživatelských účtů (vhodné pro jejich automatizaci)
- Jmenné konvence technických účtů (účty nebudou spravované v midPoint)
- Politiku hesel (vhodné pro jejich automatizaci)
- Popis nastavených (doporučených) synchronizačních pravidel
- detailní specifikaci rozhraní umožňujících automatizovanou správu účtů

3.1 Požadavky na projektový tým

Kapitola popisující zastoupení organizačních rolí v IDM projektovém týmu.

Projektový manažér
Zastřešuje koordinaci činností, realizaci integračních požadavků projektu IDM na straně zákazníka.

Garant HR / HR procesů
Zaměstnanec, má přehled o HR procesech, údajích (o zaměstnancích, externistů, obchodních partnerech, organizační struktuře) které jsou evidovány v rámci Personálního systému. Personální systém slouží jako autoritativní zdroj dat pro MidPoint. Zaměstnanec ve spolupráci s projektovým manažerem definuje příští procesní model MidPoint. (Procesy: nástup zaměstnance, přejmenování, změna údajů, odchod ...). Zaměstnanec je garantem HR procesů implementovaných v rámci IDM.

Zaměstnanec je součástí CORE IDM projektového týmu a účastní se pravidelných projektových setkání.

Garant IT Bezpečnosti
Zaměstnanec je znalý bezpečnostních pravidel, politik implementovaných na koncových systémech integrovaných s MidPoint. Ve spolupráci s projektovým manažerem definuje bezpečnostní požadavky (jmenné konvence, politika hesel na koncových systémech, viditelnost dat v rámci IDM pro jednotlivé

IBA CZ, s. r. o., www.ibacz.eu info@ibacz.eu (+420) 251 050 100
Radlická 751/113e, 158 00 Praha 5

organizační role, podílí se na definici rolí – neslučitelnosti oprávnění ...), je garantem IDM řešení za oblast IT Bezpečnosti.

Zaměstnanec je součástí CORE IDM projektového týmu a účastní se pravidelných projektových setkání.

Garant IT Architektury (Integrační architekt)

Zaměstnanec je garantem projektu v oblasti architektury řešení. V průběhu projektu je obeznámen s architekturou MidPoint IDM, na straně zákazníka zabezpečuje (formálně) integraci midPoint do existujícího prostředí.

V rámci projektu IDM ověří integrační požadavky, zajišťuje případné změny v architektuře, validuje rozhraní koncových systémů, na základě požadavků MidPoint validuje celkovou připravenost koncových systémů pro integraci.

Zaměstnanec je součástí CORE IDM projektového týmu a účastní se pravidelných projektových setkání.

Garant koncového systému (Byznys vlastník)

Zaměstnanec má přehled o implementaci koncového systému z pohledu implementovaných procesů konvenci, implementované politice hesel, poskytovaných integračních rozhraní umožňujících automatizovanou správu účtů, má přehled o významu atributů uživatelského účtu, obsahu atributu (specifikuje algoritmy / pravidla), specifikuje požadovaný syntaxi atributu (např. osobní číslo je 6-ti místné číslo, zleva zarovnané nulami), specifikuje jednoznačné identifikátory, specifikuje číselníkové hodnoty atributů.

Dodavatel koncového systému / aplikace

Dodavatel koncového systému, má přehled o implementaci koncového systému v ŘSD z pohledu procesů, konfigurace, existujících integračních rozhraní umožňujících automatizovanou správu účtů. Pro projekt IDM poskytuje konzultace v rozsahu: procesů správy účtu, integračních rozhraních, formátu atributů, jednoznačných identifikátorech, číselníkových hodnotách.

Administrátor koncového systému

Zaměstnanec v roli administrátor koncového systému zajišťuje provoz integračních rozhraní, definuje přístupy pro technického uživatele MidPoint na straně koncového systému.

Zaměstnanec je garantem za konfiguraci rozhraní na straně koncového systému. Ve spolupráci s IDM administrátorem zajišťuje konfiguraci Resource na straně MidPoint, samotnou konfiguraci Resource v midPoint neprovádí.

Pro projekt IDM poskytuje konzultace v rozsahu: procesů správy účtu, integračních rozhraních, formátu atributů, jednoznačných identifikátorech, číselníkových hodnotách. Zaměstnanec může být zařazen jako schvalovatel (Role Approver) nebo vlastník role (Role Owner).

Test Leader / Tester

Zaměstnanec v roli Test Leader ve spolupráci s projektem zajišťuje přípravu akceptačních testovacích scénářů (UAT, integrační testy rozhraní koncových systémů) dle metodiky zákazníka. Zaměstnanec zajišťuje koordinaci a vyhodnocování testů. Výsledky testů poskytuje projektovému týmu.

Zaměstnanec v roli Tester ve spolupráci s projektem zabezpečuje exekuci testovacích scénářů (UAT, integrační testy rozhraní koncových systémů) podle metodiky zákazníka.

3.2 Požadavky na obsazení provozních rolí

Požadavky na obsazenost rolí po nasazení produktu MidPoint do produkčního prostředí (podle IDM best practice). Tento základní seznam rolí může být doplněn o další organizační role vyplývajících z požadavků během analytické fázi projektu.

IDM Administrátor HW řešení
Zaměstnanec (skupina zaměstnanců) zajišťují provoz IDM řešení (HW komponenty).

IDM Administrátor SW řešení
Zaměstnanec (skupina zaměstnanců) zajišťují provoz IDM řešení (SW komponenty: OS, Tomcat, MidPoint, DB).

IDM Business vlastník
Zaměstnanec v roli IDM Business vlastník získá během projektu detailní přehled procesech a pravidlech implementovaných v IDM. Po nasazení řešení do produkčního provozu bude zajišťovat následný rozvoj IDM řešení. Organizační role může být sloučena s rolí IDM Administrátora.

Zaměstnanec je součástí CORE IDM projektového týmu, kde se účastní projektových setkání.

IDM Administrátor
Zaměstnanec se účastní všech setkání během IDM projektu. Během projektu získá detailní přehled o procesech a pravidlech implementovaných v IDM i konfiguraci samotného řešení. Po nasazení řešení do produkčního provozu bude zajišťovat úpravu konfigurace řešení, podle dalších požadavků zákazníka. Roli lze sloučit s rolí IDM Business vlastníka.

Zaměstnanec je součástí CORE IDM projektového týmu, kde se účastní projektových setkání.

IDM RBAC Administrátor
Zaměstnanec v roli RBAC Administrátor bude zajišťovat definici rolí a bude zodpovědný za aktuálnost RBAC modelu v rámci IDM. Ve spolupráci s Byznys vlastníky koncových systémů bude zajišťovat vytváření nových rolí, jejich mapování na oprávnění koncových systémů.

Zaměstnanec je součástí CORE IDM projektového týmu, kde se účastní projektových setkání.

IDM Schvalovatel role (oprávnění)
Zaměstnanec v roli Schvalovatel oprávnění (Role Approver) se účastní schvalovacího procesu a je zodpovědný za schvalování žádostí zaměstnanců o konkrétní IDM roli.

Podle best practice, do této role bývá zařazen zaměstnanec v roli Business vlastník systému / vlastník oprávnění / vlastník dat, ke kterým schvalovatel uděluje přístup.

IDM Vlastník role (oprávnění)
Zaměstnanec v roli Vlastník role (Role Owner) se účastní schvalovacího procesu v případě modifikace IDM role Typicky: změna parametru role- např. změna názvu role, změna popisu role, apod.

Podle best practice bývá do této role obsazován Administrátor koncového systému.

3.3 Požadavky na správu systému IDM/CAS

Na základě našich zkušeností doporučujeme následující strukturu podpůrných týmů:

L1 – HelpDesk – každodenní uživatelská podpora

L2 – provoz midPoint/CAS – pokročilé konfigurace řešení

L2 – podpora databází

L3 – analýza a oprava chyb

IBA CZ, s. r. o.,
Radlická 751/113e, 158 00 Praha 5
www.ibacz.eu info@ibacz.eu (+420) 251 050 100

4. Harmonogram a konkrétní fáze

Celá realizace proběhne na základě původního požadavku ŘSD v následujících fázích:

- **Fáze 1**: Nevytváříme, nevymýšlíme jen přebíráme již nastavené a „funkční“ řešení a komunikujeme pouze s AD. (termín cca do 1.11)
- **Fáze 2**: Vytváříme komunikaci s OK Base, případně s dalšími systémy a řešíme procesy, avizaci atd. (termín do konce roku)
- **Fáze 3**: Další vývoj např. CAS, postupné nasazování dalších systémů a dalších funkcionalit systému (termín únor–březen 2020).

kdy oproti původním termínům dochází s ohledem na problematiku a složitost k posunům termínům takto:
start: ASAP
Fáze I bude dokončena do 16.12.2019 při objednání do 11.10.2019
Fáze II bude dokončena 30.01.2020
Fáze III začne 02/2020

Předmětem fáze 1 je:
- Integrace na 2 DB pohledy (zaměstnanci, org. struktura)
- Integrace na AD (Windows AD 2016)
- Integrace na proprietární IDM systém (tento bude sloužit jako zdroj dat o přiřazení rolí)
- Základní procesy pro LC Zaměstnanec / externistů a OS
- Základní organizační role
- Instalace TEST prostředí + instalační příručka

Předmětem fáze 2 je:
- Rozšířené organizačně role s ohledem na procesy (zaměstnanec, Schvalovatel, RBAC administrator …)
- Schvalovací flow (max. 3 úrovně)
- V rámci analýzy a cílového řešení předpokládáme komunikaci s OK Base, kdy předpokládáme součinnost při řešení procesů anebo funkčnosti

V rámci součinnosti ŘSD připraví pro fázi 1 a fázi 2:
- testovací scénáře
- případné procedury pro data-mining z původního IDM řešení (jak bude zapotřebí)

Předmětem fáze 3 je:
- Implementace CAS, sms / email notifikace
- Zprava technických a servisních účtů
- Příručky pro koncové uživatele, adminů a klíčových uživatelů
- Školení

5. Řešitelský tým

[redacted]

IBA CZ, s. r. o.,
Radlická 751/113e, 158 00 Praha 5
www.ibacz.eu info@ibacz.eu (+420) 251 050 100

6. Cena

Položka (role, příp. skupina rolí)	MD	Cena dle smlouvy ŘSD	Celkem
konzultant/ analytik	16,80	4 400,00 Kč	73 920 Kč
projektových manažer	36,40	5 400,00 Kč	196 560 Kč
architekt/ návrhář	61,60	6 000,00 Kč	369 600 Kč
programátor/kodér	127,40	5 200,00 Kč	662 480 Kč
specialista (L2, L3 podpory, release, technical writ	0	4 400,00 Kč	0 Kč
specialista L1 podpory	0	3 400,00 Kč	0 Kč

Cena celkem	**1 302 560,00 Kč**

Všechny uvedené ceny jsou bez DPH.

6.1 Fakturační milníky

Fakturační milníky pro jednotlivé fáze jsou následující:

Fáze I - 434 188 Kč bez DPH
Fáze II - 434 186 Kč bez DPH
Fáze III - 434 186 Kč bez DPH

Každá fáze bude ukončena akceptačním protokolem, na jehož základě bude vystavena faktura.

[redacted]

IBA CZ, s. r. o.,
Radlická 751/113e, 158 00 Praha 5
www.ibacz.eu info@ibacz.eu (+420) 251 050 100