SPRÁVA ŽELEZNIC

Váš dopis zn.
Ze dne
Naše zn. 3730/2024-SŽ-SŽT-OPS
Listů/příloh 2/3

Vyřizuje Hemzová Miriam
Mobil +420 601 131 781
E-mail CNITptk@spravazeleznic.cz

Datum 18. 10. 2024

Pozvánka k předběžné tržní konzultaci ve věci Nasazení systému IdM v prostředí Správy železnic

Vážená paní, vážený pane,

Správa železnic, státní organizace (dále jen „***zadavatel***“) Vás touto cestou informuje, že připravuje zadávací řízení na veřejnou zakázku s názvem „Nasazení systému IdM v prostředí Správy železnic“. Vyhlášení této veřejné zakázky bude předcházet předběžná tržní konzultace (dále jen „***PTK***“), jejímž cílem bude získat relevantní informace pro správné nastavení předmětu plnění, zadávacích podmínek, volby druhu zadávacího řízení či způsobu hodnocení předložených nabídek. Zadavatel usiluje o získání kvalitního plnění, které bude splňovat jeho potřeby, a to za odpovídající cenu.

Cílem veřejné zakázky je uzavření smlouvy, jejímž předmětem bude výběr technologie a implementace systému IdM a také napojení úvodní sady vybraných cílových systémů.

Cílem PTK je transparentním způsobem získat přehled o současné situaci na trhu, možnostech dodavatelů a ujasnění otázek nezbytných pro realizaci veřejné zakázky.

PTK podle evropské zadávací směrnice (2014/24/EU) je možností zadavatele předtím, než vyhlásí veřejnou zakázku, komunikovat s dodavateli a zjišťovat (případně dalšími relevantními osobami) jejich možnosti a návrhy řešení. V rámci zvoleného modelu bude představen záměr zadavatele, včetně některých navrhovaných detailů jak předmětu veřejné zakázky, tak zadávacího řízení. Dodavatelé se pak budou moci k navrhovaným parametrům zakázky vyjádřit. Dojde tak ke zvýšení transparentnosti zadávacího řízení a získání relevantních a objektivních informací o možnostech trhu, tak aby mohl zadavatel optimálně nastavit zadávací podmínky veřejné zakázky, resp. celkové řešení zadávacího řízení. Vedení PTK je rovněž zcela v souladu s ust. § 33 zákona č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů (dále jen „***Zákon***“).

Zadavatel v rámci PTK žádá potenciální dodavatele o seznámení se záměrem a cílem Aktivity Nasazení systému IdM v prostředí Správy železnic dle Přílohy č. 1 – *Specifikace předmětu plnění*, dále o zodpovězení dotazů uvedených v Příloze č. 2 – *Otázky pro účastníky PTK* a rovněž o poskytnutí informací ohledně naplnění požadavků na systém IdM formulovaných v Příloze č. 3 – *Seznam požadavků na systém IdM - funkční a nefunkční vlastnosti*.

Forma PTK: písemná (s možností pokračování ústní či písemnou formou, podle potřeb zadavatele)

Způsob konání PTK:

Správa železniční dopravní cesty, státní organizace
zapsána v obchodním rejstříku vedeném Městským soudem v Praze, spisová značka A 48384

Sídlo: Dlážděná 1003/7, 110 00 Praha 1
IČ: 709 94 234 DIČ: CZ 709 94 234
www.szdc.cz

Správa železniční telematiky
V Celnici 1028/10
110 00 Praha 1

V prvním kole PTK zašlou dodavatelé či odborné subjekty, jež projeví zájem o účast na této PTK, odpovědi na otázky uvedené v Příloze č. 2 – *Otázky pro účastníky PTK* a informace ohledně naplnění požadavků na systém IdM v Příloze č. 3 – *Seznam požadavků na systém IdM - funkční a nefunkční vlastnosti* na e-mailovou adresu: cnitptk@spravazeleznic.cz.

Zadavatel si v případě potřeby vyhrazuje možnost uskutečnit druhé kolo PTK, přičemž v rámci tohoto druhého kola může dojít za účelem konzultace zamýšleného řešení k osobnímu setkání s jednotlivými dodavateli či odbornými subjekty. Zadavatel si vyhrazuje právo pozvat do druhého kola libovolný počet účastníků z kola předchozího, přičemž vždy bude postupovat tak, aby nedošlo ke zvýhodnění žádného z účastníků.

Předpokládaný počátek plnění předmětu veřejné zakázky je 2. kvartál roku 2025, přičemž může být na základě výsledků PTK upraven.

V případě Vašeho zájmu o účast na této PTK, prosím, zašlete odpovědi na otázky uvedené v Příloze č. 2 – *Otázky pro účastníky PTK* a informace ohledně naplnění požadavků v Příloze č. 3 – *Seznam požadavků na systém IdM – funkční a nefunkční vlastnosti*, a to na e-mailovou adresu: cnitptk@spravazeleznic.cz

Svoji odpověď prosím doručte nejpozději do 31. 10. 2024.

Dodavatel či odborný subjekt by ve své odpovědi měl uvést minimálně:

- název a sídlo dodavatele (odborného subjektu);
- IČO dodavatele (odborného subjektu);
- jméno a funkce kontaktních osob, včetně kontaktních údajů (minimálně e-mail);
- odpovědi na přiložené otázky;
- informace ohledně naplnění požadavků.

Předběžná tržní konzultace nesmí vést k porušení základních zásad Zákona. Průběh i výsledek předběžné tržní konzultace bude zaznamenán ve zprávě vytvořené zadavatelem. Informace z předběžných tržních konzultací užité v zadávacích podmínkách zadané veřejné zakázky budou v souladu s § 36 odst. 4 Zákona v zadávací dokumentaci výslovně označeny, a to včetně osob, které se na výsledku podílely.

Děkuji za spolupráci.

S pozdravem

Ing. David Miklas
21.10.2024 10:50
Podepsáno
elektronicky

Ing. David Miklas
ředitel Správy železniční telematiky

Přílohy:
Příloha č. 1 – Specifikace předmětu plnění
Příloha č. 2 – Otázky pro účastníky PTK
Příloha č. 3 – Seznam požadavků na systém IdM - funkční a nefunkční vlastnosti

Předběžná tržní konzultace ve věci Nasazení systému IdM v prostředí Správy železnic

Příloha č. 1 – Specifikace předmětu plnění

Správa železnic, státní organizace (dále také jen „***SŽ***“) plánuje implementaci systému pro správu identit, řízení přístupových oprávnění (IdM) v systémech a ICT prostředí SŽ (Aktivita Nasazení systému IdM v prostředí Správy železnic). Cílem této předběžné tržní konzultace je získání relevantních informací o možných nebo vhodných nástrojích IdM pro případné zadání budoucích veřejných zakázek dostatečně přesným, technologicky neutrálním a nediskriminujícím způsobem a současně postupem, který bude vyhovovat požadavkům a prostředí SŽ.

Záměr SŽ v oblasti systému pro správu identit a přístupů

Implementace systému IdM a jeho napojení na aktiva organizace je v souladu s dlouhodobou koncepcí řízení identit, přístupových oprávnění, jejich kontroly a zvýšení zabezpečení přístupů k aktivům organizace. S ohledem na velikost organizace a velké množství aktiv, neplánuje SŽ implementaci IdM pro všechna aktiva v rámci jedné Aktivity, ale plánuje jejich postupné připojování podle technických a organizačních možností. IdM tedy není plánováno pouze pro řízení identit a přístupových oprávnění k informačním systémům spadajícím do kritické infrastruktury, ale v optimálním případě ke všem aktivům, u kterých je třeba řídit přístupová oprávnění[1].

Cíl Aktivity Nasazení systému IdM v prostředí Správy železnic

Cílem plánované veřejné zakázky, která je součástí Aktivity Nasazení systému IdM v prostředí Správy železnic, je výběr a implementace IdM systému pro všechna aktiva, kde je nutné řídit přístupová oprávnění.

Hlavní cíle veřejné zakázky jsou:

- implementace systému pro systematickou správu celého životního cyklu identit, řízení a kontroly přístupů k jednotlivým aktivům, rekonciliace a reportování,
- systematická správa a kontrola přístupových oprávnění k cílovým systémům (aktivům) včetně automatizace (založené na rolích a atributech),
- podpora automatizace souvisejících procesů (zejména navázané na HR procesy),
- podpora automatizace schvalovacích procesů, jednoznačná odpovědnost za konkrétní přístupová oprávnění,
- zvýšení bezpečnosti a plnění legislativních požadavků, eliminace části bezpečnostních hrozeb,
- systematická a automatizovaná správa technických, servisních a správcovských účtů,
- datové oddělení procesní správy životního cyklu identit od cílových systémů (včetně autorizačních a autentizačních systémů),
- snížení nákladů na správu uživatelských účtů a HR procesů.

[1] *Tato aktiva tak obsahují především informační systémy kritické infrastruktury, ostatní informační systémy, systémy pro kontrolu přístupů do zabezpečených lokalit a ostatních prostor organizace.*

Správa železniční dopravní cesty, státní organizace
zapsána v obchodním rejstříku vedeném Městským soudem v Praze, spisová značka A 48384

Sídlo: Dlážděná 1003/7, 110 00 Praha 1
IČ: 709 94 234 DIČ: CZ 709 94 234
www.szdc.cz

Správa železniční telematiky
V Celnici 1028/10
110 00 Praha 1

Záměr Aktivity IdM: předběžné požadavky na řešení, předpokládaný postup

Požadavky na řešení

Zdrojové systémy pro IdM
Primárním autoritativním zdrojem dat pro systematickou správu životního cyklu identit a business rolí bude systém SAP HR spravující mj. data o zaměstnancích, externistech, pracovně právních vztazích a systemizaci organizace.

Zdrojové a koncové (cílové systémy)
V cílovém stavu SŽ předpokládá, že IdM bude zajišťovat řízení životního cyklu identit a přístupových oprávnění a následný výběr a implementaci IdM systému pro všechna aktiva, kde je nutné řídit přístupová oprávnění. V cílovém stavu SŽ předpokládá napojení cca 30 systémů.

Pro úvodní implementaci SŽ předpokládá, že cílovými (koncovými) systémy budou zejména:

- systémy Active Directory,
- vybrané systémy kritické informační infrastruktury (vybraná primární aktiva),
- vybrané systémy mimo kritickou informační infrastrukturu (vybraná podpůrná aktiva),
- systémy typu Privileged Access Management (PAM) pro správu technických, servisních a správcovských účtů,
- systémy interních certifikačních autorit.

Pro úvodní implementaci SŽ předpokládá rozsah přibližně 30 cílových systémů.

Požadavky na funkční vlastnosti IdM
Předběžné požadavky na funkční a nefunkční vlastnosti IdM jsou jednou z oblastí předběžné tržní konzultace, které jsou shrnuty ve formě otázek v Příloze č. 3.

Předpokládaný postup

S ohledem na rozsah implementace IdM a nutnosti úvodní přípravy prostředí, zejména po stránce organizace a odpovědností, datových zdrojů a jejich kvality a oblasti procesů, SŽ rozdělila implementaci IdM na dvě na sebe navazující etapy, přičemž první etapa zahrnující organizační, procesní a datovou přípravu již proběhla.

Druhá etapa, jež je předmětem tohoto PTK, zahrnuje výběr technologie a implementace systému IdM a napojení úvodní sady vybraných cílových systémů.

Předběžné vymezení, rozsah a výstupy Etapy 2
Etapa 2 bude navazovat na předchozí Etapu 1 a využije její výsledky. V Etapě 2 SŽ předpokládá zejména:

- výběr technologie (systému) IdM s ohledem na funkční i nefunkční požadavky, ICT prostředí SŽ a výstupy Etapy 1,
- implementaci vybraného systému IdM,
- nastavení podpory procesů, včetně automatizace procesů a podpory schvalovacích procesů, uživatelské samoobsluhy apod.,
- napojení zdrojových a řídících systémů: SAP HR, Atlasian Jira, MS Active Directory,
- postupné napojení definované skupiny cílových systémů podle priorit SŽ (celkem až 30),
- zajištění technické podpory a rozvoje systému IdM.

Předběžná tržní konzultace ve věci Nasazení systému IdM v prostředí Správy železnic

Příloha č. 2 – Otázky pro účastníky PTK

V rámci předběžné tržní konzultace bychom Vás požádali o odpovědi a komentáře k následujícím oblastem, předpokládanému průběhu Aktivity a předběžným funkčním požadavkům na systém Identity & Access Management (dále jen „***IdM***“) pro Správu železnic, státní organizaci (dále jen „***SŽ***“). Specifikace předmětu plnění je přílohou č. 1 Pozvánky k PTK, a obsahuje předběžné požadavky na řešení. Seznam konkrétních požadavků na systém IdM je uveden v příloze č. 3. Je proto nutné se s celou přílohou č. 1 a přílohou č. 3 seznámit před zodpovídáním dotazů v této příloze.

Dotaz 1	**Vaše odpověď**
Žádáme o vyplnění níže uvedených údajů: • název dodavatele a sídlo dodavatele, • IČO dodavatele, • jméno a funkce kontaktních osob, včetně kontaktních údajů (minimálně e-mail).	

Dotaz 2	**Vaše odpověď**
Žádáme o vyjádření k Příloze č. 1 – Specifikace předmětu plnění: • Je záměr a cíl Aktivity Nasazení systému IdM v prostředí Správy železnic pochopitelný a srozumitelný?	ANO / NE / ČÁSTEČNĚ
Váš komentář k Příloze č. 1 – Specifikace předmětu plnění	

Oblast Technického řešení

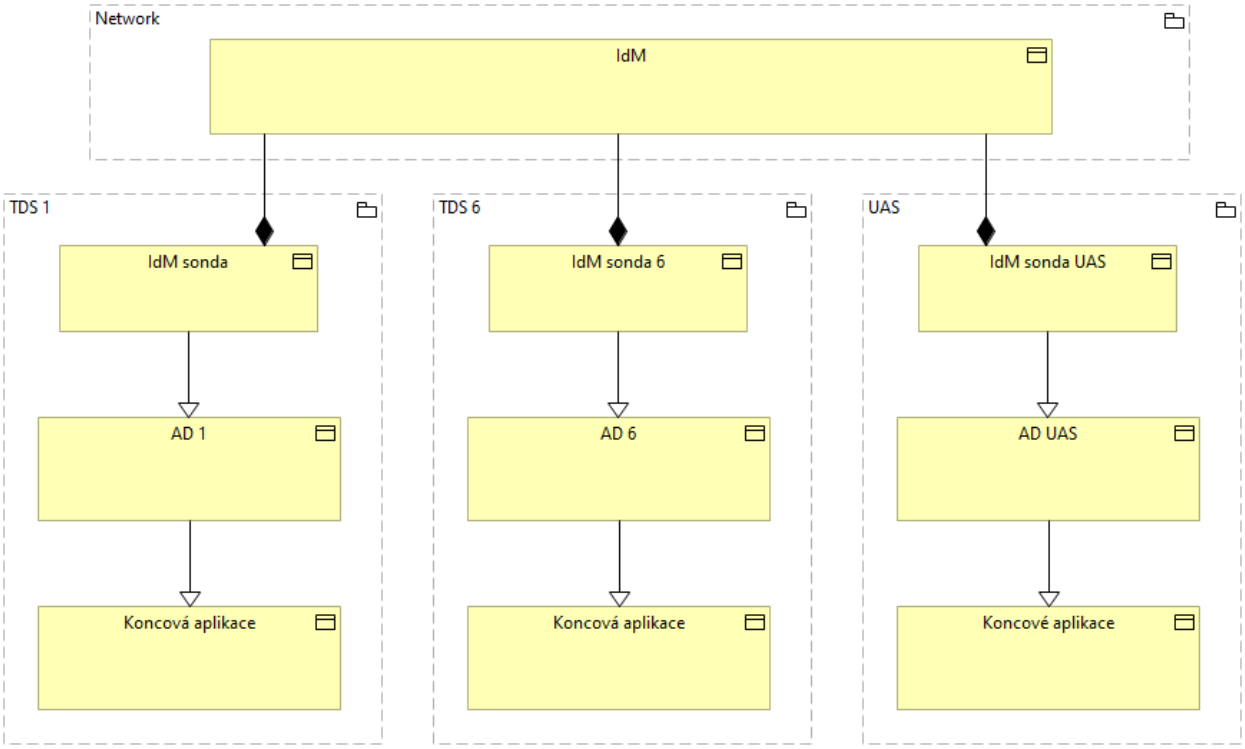
Implementace předpokládá variantu napojení IdM ke zdrojovému systému SAP HR, prostřednictvím jehož budou do IdM získávány údaje o osobách a organizační struktuře a dále k servicedeskovému řešení JIRA, prostřednictvím něhož bude probíhat schvalování přidělovaných oprávnění. Do SAP HR je zároveň integrována aplikace KAFR, která do HR systému předává údaje o smlouvách.

IdM bude instalováno formou centrální instance, která komunikuje se svými sondami umístěnými v jednotlivých technologických sítích (6x TDS) a uživatelských sítích (UAS). V rámci sítí bude existovat i konkrétní strom AD.

Správa železniční dopravní cesty, státní organizace
zapsána v obchodním rejstříku vedeném Městským soudem v Praze, spisová značka A 48384

Sídlo: Dlážděná 1003/7, 110 00 Praha 1
IČ: 709 94 234 DIČ: CZ 709 94 234
www.szdc.cz

Správa železniční telematiky
V Celnici 1028/10
110 00 Praha 1

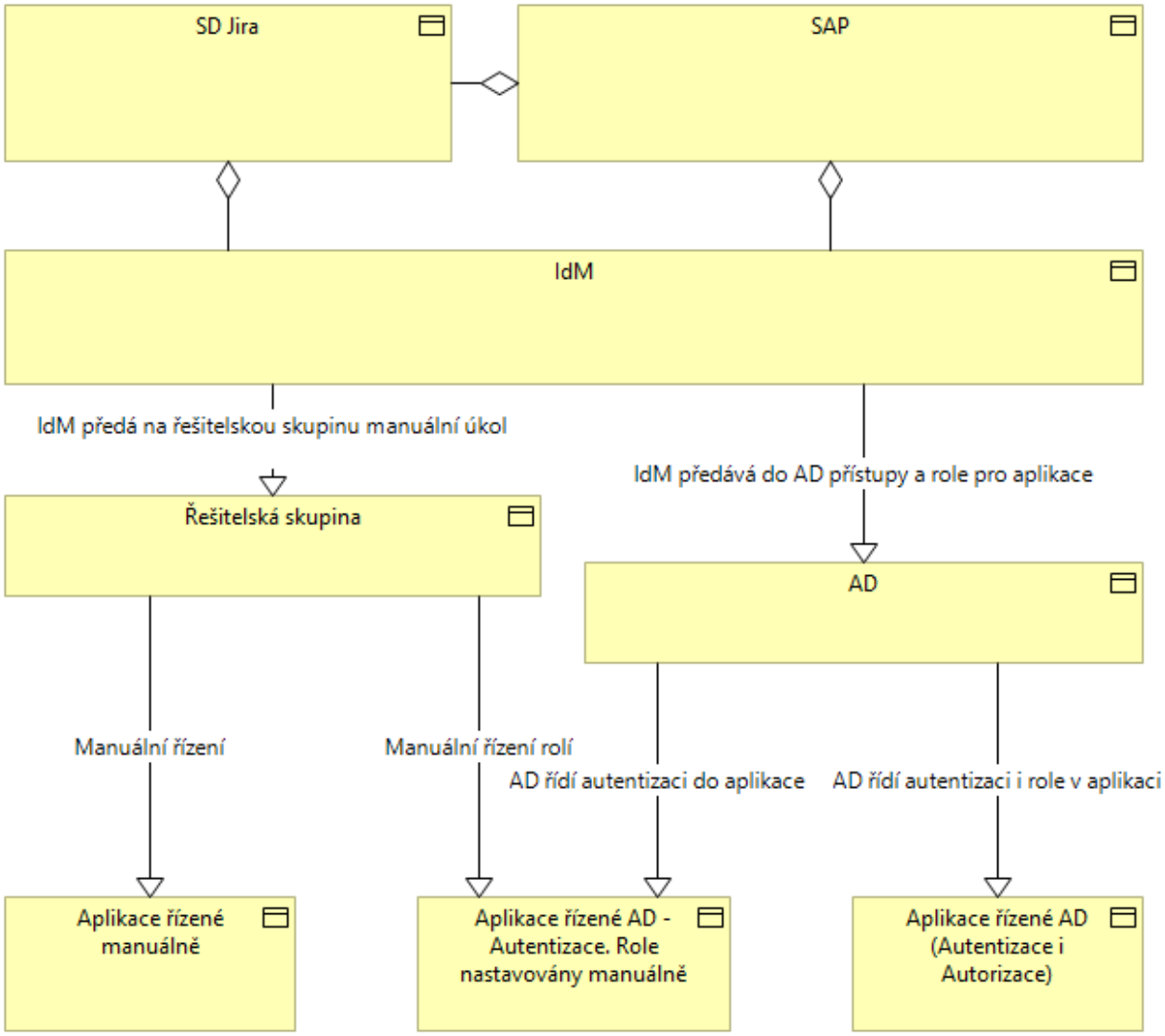


Iniciace procesu schvalování oprávnění bude začínat buďto požadavkem ze strany SAPu (nástup zaměstnance, změna pracovní pozice, ukončení zaměstnance) v rámci integrace mezi SAP a SD JIRA, nebo manuálním vyplněním žádosti ze strany uživatele v SD JIRA.

Iniciace i postup schvalování v JIRA bude v každém kroku reflektován do IdM a to včetně finálního rozhodnutí o schválení nebo neschválení požadavku.

IdM bude řídit koncové aplikace:

- prostřednictvím MS Active Directory. Předpokládá se tedy integrace těchto koncových systémů s MS AD, a to za účelem Autentizace a / a nebo také Autorizace.
- prostřednictvím požadavku na Řešitelskou skupinu, která zajistí manuální úpravu v dotčené aplikaci.



Své odpovědi k otázkám v této oblasti, prosíme, uveďte v následující tabulce. **V případě odpovědi „NE" nebo „ČÁSTEČNĚ" Vás žádáme o upřesnění Vaší odpovědi.:**

Dotaz 3	**Vaše odpověď**
Implementace předpokládá dva způsoby řízení koncových systémů. Způsob a) IdM řídí koncové systémy požadavkem na řešitelské skupiny (prostřednictvím SD JIRA), jejichž členové manuálně nastavují účty a role v koncových systémech. Je tento způsob realizovatelný?	ANO / NE / ČÁSTEČNĚ
Váš komentář k navrhovanému řešení.	

Dotaz 4	Vaše odpověď
Implementace předpokládá dva způsoby řízení koncových systémů. Způsob b) IdM řídí koncové systémy prostřednictvím AD a to jak za účelem autentizace, tak / anebo i za účelem Autorizace. Je tento způsob realizovatelný?	ANO / NE / ČÁSTEČNĚ
Váš komentář k navrhovanému řešení.	

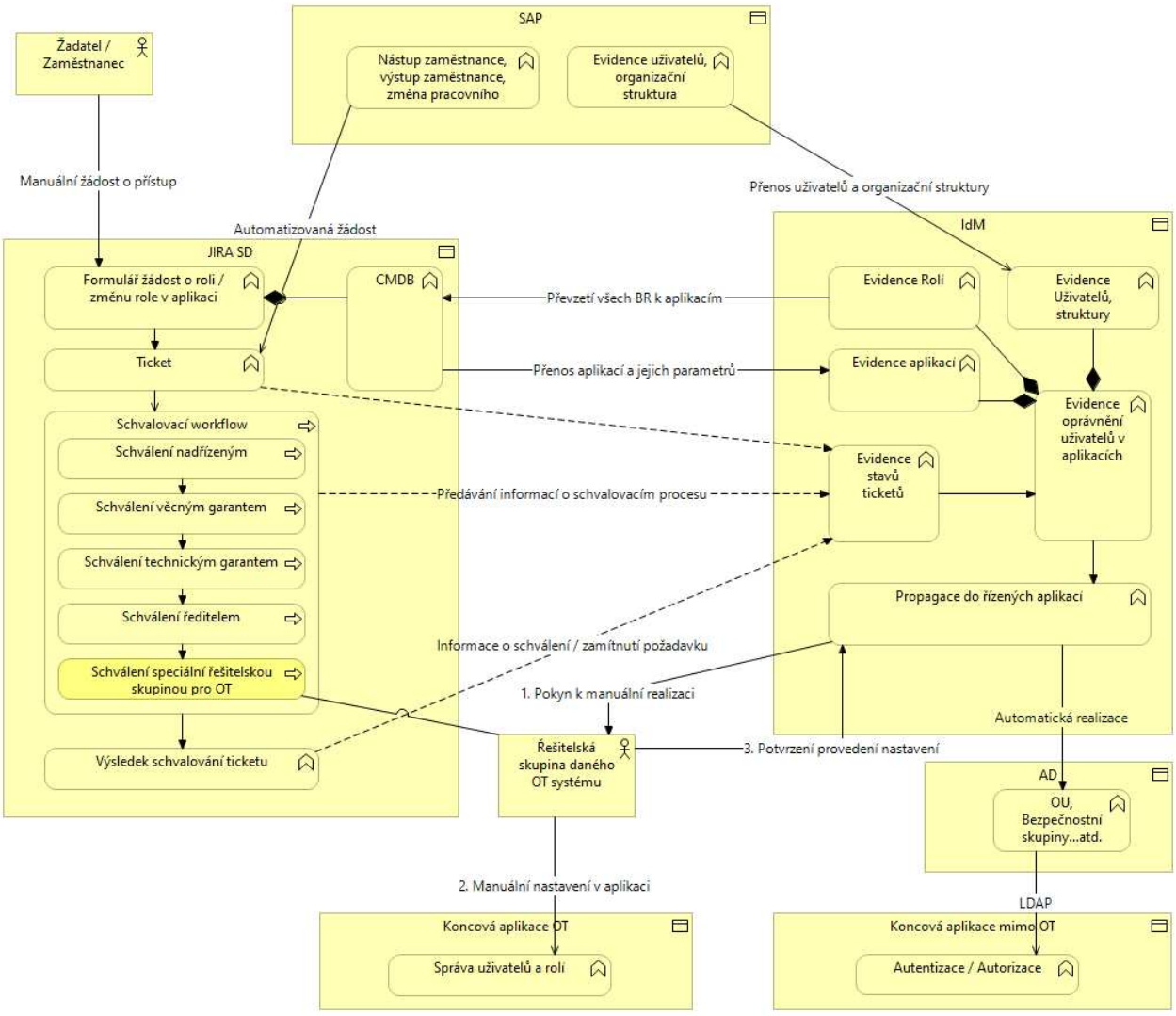
Dotaz 5	Vaše odpověď
Existuje v rámci vašeho technického řešení i řešení pro zajištění konzistence stavu účtů a oprávnění v aplikacích vůči IdM (rekonciliace) pro způsob a)?	ANO / NE / ČÁSTEČNĚ
Váš komentář k navrhovanému řešení.	

Dotaz 6	Vaše odpověď
Existuje v rámci vašeho technického řešení i řešení pro zajištění konzistence stavu účtů a oprávnění v aplikacích vůči IdM (rekonciliace) pro způsob b)?	ANO / NE / ČÁSTEČNĚ
Váš komentář k navrhovanému řešení.	

Dotaz 7	Vaše odpověď
Aplikace budou zaváděny do IdM prostřednictvím synchronizace s aplikací JIRA, která vede CMDB. V číselníku aplikací v CMDB budou správcem označeny aplikace, které mají být řízeny prostřednictvím IdM a ty budou následně předmětem synchronizace. Je tento způsob realizovatelný?	ANO / NE / ČÁSTEČNĚ
Váš komentář k navrhovanému řešení.	

Dotaz 8	Vaše odpověď
V rámci dodržení interních pravidel segmentace bude mít IdM své sondy v jednotlivých technologických sítích. Je tento způsob realizovatelný?	ANO / NE / ČÁSTEČNĚ
Váš komentář k navrhovanému řešení.	

Aktuální navržená forma schvalovacího procesu přidělování oprávnění zahrnuje integraci se Servicedesk JIRA, kdy požadavek vznikne v IdM, a prostřednictvím API bude předán do workflow v rámci SD JIRA.



V rámci schvalovacího procesu bude výsledek předán zpět do IdM a při kladném vyřízení bude buďto prostřednictvím AD požadavek realizován automatizovaně, nebo bude předán do tzv. řešitelské skupiny, která provede manuální realizaci (v případě koncových systémů OT).

Dotaz 9	Vaše odpověď
Předpokládá se, že proces schvalování bude prováděn v SD JIRA a zrcadlen do IdM. Je tento navržený poustup realizovatelný?	ANO / NE / ČÁSTEČNĚ
Váš komentář k navrhovanému řešení.	

Dotaz 10	Vaše odpověď
Spatřujete v takto navrženém schvalovacím procesu (včetně schválení řešitelskou skupinou OT) problém v souvislosti s legislativními požadavky? Pokud ano, prosíme o upřesnění Vaší odpovědi níže.	ANO / NE / ČÁSTEČNĚ
Váš komentář k navrhovanému řešení.	

Dotaz 11	Vaše odpověď
Umí Vaše řešení IDM integraci na nástroj JIRA?	ANO / NE / ČÁSTEČNĚ
Váš komentář k navrhovanému řešení.	

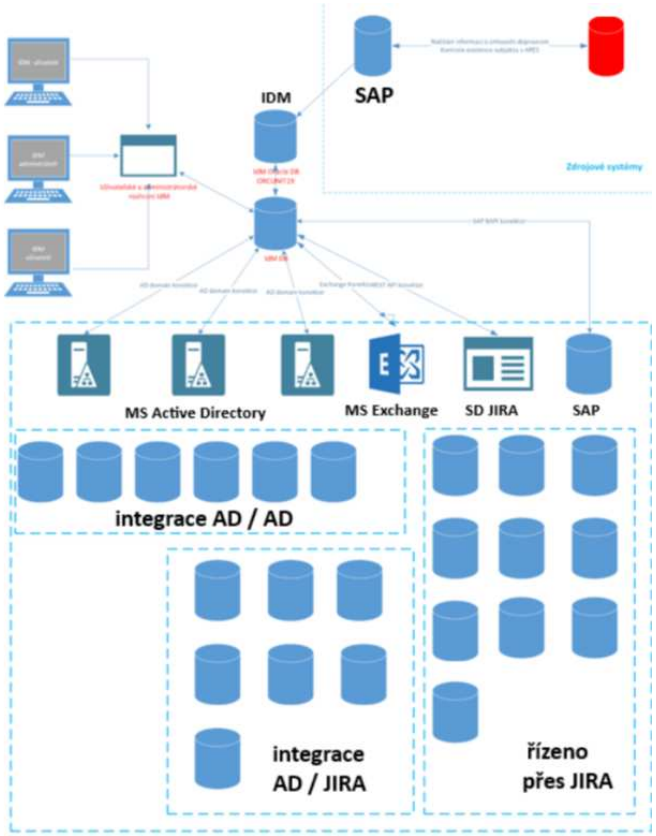
Dotaz 12	Vaše odpověď
Jste schopni v rámci realizace veřejné zakázky implementovat integraci nástroje IDM na JIRA?	ANO / NE / ČÁSTEČNĚ
Váš komentář k navrhovanému řešení.	

Dotaz 13	Vaše odpověď
Napojení řízeného systému na LDAP – požadujeme zabezpečenou variantu – LDAPs na portu 636 s vlastním interním SSL certifikátem s podporou EC algoritmu (nejen současně používaného RSA). Umožňuje Vaše řešení toto napojení?	ANO / NE / ČÁSTEČNĚ
Váš komentář k navrhovanému řešení.	

Oblast implementace řešení – harmonogram

V případě odpovědi „NE" nebo „ČÁSTEČNĚ" Vás žádáme o upřesnění Vaší odpovědi.

Aktuálně je předpokládáno napojení 30 koncových systémů, z čehož se předpokládá 8 systémů prostřednictvím AD za účelem Autentizace i Autorizace a 8 systémů prostřednictvím AD za účelem Autentizace s využitím JIRA SD pro manuální přiřazování rolí.



Aktuální harmonogram realizace Aktivity IdM (etapa 2) zahrnuje:

Část plnění	Popis poskytovaných služeb	Termín plnění		Výstupy
		Začátek	Konec (T + počet prac. dní)	
1	Analýza připojení autoritativních zdrojů dat.	T	T+5	Schválený dokument Analýzy a návrhu řešení kapitoly Analýza připojení autoritativních zdrojů dat
	Předimplementační analýza	T	T+10	Schválený dokument Předimplementační analýza
	Plán nasazení IdM a připojení systémů.	T	T+20	Schválený dokument Předimplementační analýza kapitoly Plán nasazení IdM a připojení systémů

2	Popis provedení analýzy rizik informačního systému IdM.	T1	T1+5	Schválení popisu provedení analýzy rizik systému IdM
	Analýzy rizik informačního systému IdM: • Hodnocení aktiv s ohledem na dostupnost, integritu a důvěrnost. • Provázání aktiv. • Hodnocení rizik. • Plán zvládání rizik.	T1	T1+10	Předávací protokol k Analýze rizik informačního systému IdM
3	Příprava komunikační kampaně	T2	T2+25	Schválený dokument Koncepce komunikační kampaně
	Realizace komunikační kampaně	T2	T2+80	Potvrzení protokolu o realizaci komunikační kampaně
4	Úprava interní dokumentace SŽ	T2	T2+85	Schválené upravené interní dokumenty SŽ dle potřeb Zadavatele.
5	Nasazení testovacího a produkčního prostředí.	T2	T2+5	Instalované, nakonfigurované řešení IdM v testovacím a produkčním prostředí integrované na zdrojové a řízené systémy Migrace dat do systému IdM
	Integrace autoritativních zdrojů dat.	T2	T2+15	
	Integrace řízených systémů ve správě IdM.	T2	T2+48	

6	Dokumentace architektonického a technického návrhu řešení.	T5	T5+10	Podepsaný akceptační protokol k o převzetí dokumentace
	Dokumentace funkčního a bezpečnostního nastavení řešení včetně metodiky testování.			
	Plán zotavení z havárie.			
	Správcovské a uživatelské příručky pro výkon jednotlivých rolí.			
	Přehled všech použitých technologií a souvisejících licencí s plánem plné a omezené produktové podpory.			
7	Integrační testování.	T6	T6+5	Potvrzení protokolu o úspěšné realizaci testů
	Zátěžové testování.	T6	T6+10	
	Bezpečnostní testování.	T6	T6+20	
	Akceptační testování.	T6	T6+25	
8	Migrace dat.	T7	T7+10	V systému IdM jsou veškeré údaje o uživatelích, aplikačních rolích a vazbách mezi uživateli a aplikačními rolemi. Systém je připravený na spuštění zkušebního provozu.
9	Školení technických správců systému.	T7	T7+5	Potvrzení protokolu o realizaci školení se seznamem účastníků školení

	Školení správců identit.	T7	T7+10	
10	Zkušební provoz	T7	T7+30	Protokol o realizaci zkušebního provozu a odstranění zjištěných nedostatků.
11	Další rozvoj aplikací dle požadavků SŽ	T10	T10+185	
12	Podpora na vyžádání/provozní podpora	T11	T11+5 let	Provozní podpora – měsíční sazba Podpora na vyžádání – cena za 1 MD
	Celkem		**T+328**	

Dotaz 14	**Vaše odpověď**
Jsou součástí vašeho standardně dodávaného řešení: - Testovací instance (plně funkční napojená na zdrojové i koncové testovací instance aplikací? - Školící instance?	ANO / NE / ČÁSTEČNĚ
Váš komentář k navrhovanému řešení.	

Dotaz 15	**Vaše odpověď**
Je tento navržený harmonogram realizovatelný?	ANO / NE / ČÁSTEČNĚ
Váš komentář k navrhovanému řešení.	

Dotaz 16	**Vaše odpověď**
Vykazuje předložený harmonogram části, které je možné zkrátit nebo nutné prodloužit?	ANO / NE / ČÁSTEČNĚ
Váš komentář k navrhovanému řešení.	

Oblast zakázky a její předpokládané hodnoty

V případě odpovědi „NE" nebo „ČÁSTEČNĚ" Vás žádáme o upřesnění.

Dotaz 17	Vaše odpověď
V rámci podání nabídky bude požadováno dodání specifických dokumentů, zejména pak seznamu použitých technologických komponent, knihoven a frameworků, včetně jejich verzí. Je tento požadavek z vaší strany realizovatelný?	ANO / NE / ČÁSTEČNĚ
Váš komentář k navrhovanému řešení.	

Dotaz 18	Vaše odpověď
Je možné po dodavateli v rámci implementační zakázky požadovat participaci na úpravě interní dokumentace zadavatele? (metodiky, politiky, směrnice). Pokud ano, v jakém rozsahu a na jak dlouho?	ANO / NE / ČÁSTEČNĚ
Váš komentář k navrhovanému řešení.	

Dotaz 19	Vaše odpověď
Prosíme o vyplnění rámcové ceny pro jednotlivé části plnění	Prosíme o doplnění tabulky níže
Váš komentář k nacenění částí plnění.	

Část plnění	Očekávaná hodnota (v Kč bez DPH)
1	
2	
3	
4	
5	
6	
7	
8	
9	
10	
11	
12a – Podpora provozní – měsíční sazba	
12b - Podpora na vyžádání - cena za 1 MD	
Celkem	

Dotaz 20	Vaše odpověď
V případě, že u aplikací řízených prostřednictvím SD JIRA dojde v budoucnu k umožnění integrace prostřednictvím AD, jaké jsou odhadované náklady na tuto integraci za 1 aplikaci (pouze náklady na straně IdM)? Tyto dodatečné náklady nezahrnujte do otázky č. 19.	

Dotaz 21	Vaše odpověď
Jaký dopad na pracnost by měla změna způsobu integrace jedné aplikace z SD na AD v průběhu implementace?	

Dotaz č. 22	Vaše odpověď
Byla vaší společností již někdy realizována implementace IdM v rozsahu a způsobem dle výše uvedené specifikace, bodů a dotazů? V případě, že ano, můžete specifikovat významná rizika, která se u nich objevila a která by měla být v rámci tohoto projektu důsledně řízena?	

Vaše další komentáře k této PTK

V případě, že považujete za vhodné nám sdělit Vaše další komentáře nebo doporučení k předmětu této PTK nebo možným budoucím veřejným zakázkám realizovaným v souvislosti s touto PTK, prosíme o Vaše další vyjádření v následující tabulce:

Vaše další komentáře k předmětu PTK

Oblast	ID	Požadavek	Funkční/Nefunkční	Stav	Uživatelsky/ garantem spravované	Administr. spravované	Portál uživatele	API/web service
A		**Obecné požadavky**						
	A.1	IDM musí v návaznosti na zdrojové systémy dat o identitách udržovat a spravovat kompletní životní cyklus identity. Jedná se zejména o příchod zaměstnance, přidělení business rolí dle jeho organizačního zařazení (systematizovaného místa), doplňování business rolí i mimo systemizované místo, změna rolí v případě jeho změny jeho zařazení, odchod zaměstnance spočívající v deaktivaci, archivaci jeho identity apod. Seznam požadavků na podporu procesů řízení životního cyklu identity je uveden v oblasti B.	Nefunkční	Požadované				
	A.2	IDM musí zajistit přiřazení aplikačních rolí a souvisejících uživatelských účtů pro cílové systémy na základě budiness rolí a dalších vlastností nebo atributů identity. Současně musí zajistit aktualizaci členství uživatelských účtů v aplikačních rolích při změně členství uživatelských účtů v business rolích, do kterých jsou tyto aplikační role vnořeny nebo při změně atributů identity.	Funkční	Požadované	Ano	Ano		Ano
	A.3	IDM musí obsahovat registr aplikací a informačních systémů (souhrnně IS), registr aplikačních rolí s možností jejich filtrování podle aplikace aplikační role, registr business rolí a registr uživatelských účtů s možností filtrování v registrech dle atributů objektů v registru. IDM umožňuje zobrazit informace kdo je členem konkrétná aplikační role a na základě jakého důvodu a zároveň umožňuje zobrazit jeké aplikační role má přiřazený uživatelský účet a zda tyto aplikační role má uživatelský účet přiřazené přímo nebo prostřednictvím business role a jaké business role, IDM má možnost exportu a importu aplikací, aplikačních rolí, business rolí, uživatelských účtů přes definované rozhraní (webová služba, API apod.) a zároveň má IDM možnost importu vazeb mezi aplikací a aplikační rolí, aplikační rolí a business rolí, uživatelem a business rolí, uživatelem a aplikační rolí.	Funkční	Požadované	Ano	Ano		Ano
	A.4	Jedna fyzická osoba musí mít v IDM jednu jedinečnou identitu rozpoznatelnou na základě jedinečného identifikátoru identity neměnného po celý život fyzické osoby. Změna pracovně právního nebo jiného smluvního vztahu fyzické osoby nemá na jedinečný identifikátor identity vliv.	Nefunkční	Požadované				
	A.5	IDM musí umožnit přiřazení více uživatelských účtů ("loginů") jedné identitě v závislosti na cílových systémech, například na základě role nebo atributu apod. Uživatelský účet dané aplikace nebo IS může být přiřazen i více identitám, ale v tom případě sdílený účet není řízen systémem IDM.	Funkční	Požadované		Ano		
	A.6	IDM musí obsahovat samoobslužné uživatelské rozhraní (portál uživatelské samoobsluhy) pro zadávání žádostí o přiřazování uživatelských rolí a přístupů (přidělování a změny členství v business nebo aplikačních rolí, změny členství ve skupinách atd.). Požadavky na přidělení nebo odebrání členství uživatelského účtu identity v aplikační nebo business roli, budou na portále schvalovány definovanými schvalovateli. Pro každou aplikační nebo business roli nebo pro každou skupinu aplikačních nebo business rolí bude možné oprávněným uživatelem na portále IDM definovat samostatné a specifické schvalovací workflow nebo nastavit vyřízení žádosti o aplikační nebo business roli nebo skupinu aplikačních nebo business rolí automaticky bez schválení.	Funkční	Požadované	Ano	Ano	Ano	Ano
	A.7	Správa uživatelů (identit) musí obsahovat i správu údajů o uživatelských digitálních certifikátech. Data o certifikátech bude možné nahrávat do systému prostřednictvím definovaného rozhraní (např. webová služba)	Funkční	Požadované	Ano	Ano		Ano
	A.8	IDM musí pro deaktivované a archivované identity zajistit anonymizaci jejich údajů (podle požadavků UOOU)	Funkční	Požadované		Ano		
	A.9	IDM musí v závislosti na zdrojových systémech zajistit správu identit a jejich uživatelských účtů, tak že jednotlivé typy identit a jejich uživatelských účtů je možné spravovat specifickými procesy ve vazbě na typ identity a typ uživatelského účtu (například zaměstnanec HPP běžný účet,zaměstnanec HPP administrátorský účet , pracovník DPP/DPČ běžný účet,pracovník DPP/DPČ administrátorský účet , externista dodavatel běžný účet,externista dodavatel administrátorský účet externista dopravce běžný účet atd.)	Funkční	Požadované				Ano
B		**Podpora procesů**						
	B.1	IDM musí (v návaznosti na zdrojové systémy dat) podporovat procesy správy životního cyklu identity a jejich uživatelských účtů a sovisející obslužbé procesy, zejména:	Nefunkční	Požadované				
	B.1.1	vznik nové identity a jejího uživatelského účtu	Funkční	Požadované		Ano		
	B.1.2	nový pracovněprávní vztah a vytvoření nebo změna uživatelského účtu	Funkční	Požadované		Ano		
	B.1.3	změna pracovněprávního vztahu a následná změna údajů identity a uživatelských účtů identity	Funkční	Požadované	Ano	Ano		
	B.1.4	změny popisných atributů, např. jméno	Funkční	Požadované	Ano	Ano		
	B.1.5	změny organizačního zařazení	Funkční	Požadované	Ano	Ano		
	B.1.6	změny platnosti vlastností identity = změna paltnosti uživatelských účtů identity a jejich atributů, zaměna přiřazení aplikačních a business rolí atd.	Funkční	Požadované	Ano	Ano		
	B.1.7	automatická změna rolí na základě změny typu nebo stavu identity a typu nebo stavu uživatelských účtů identity, případně jiného příznaku identity	Funkční	Požadované		Ano		

	B.1.8	změna evidenčního stavu identity (zejména v oblasti pracovně-právních vztahů, např. změna HPP, DPČ, mateřská, překážky na straně zaměstnavatele appd.) dle definovaných pravidel pro jednotlivé typy změn, tj. například podporovat jen změnu evidenčních údajů, kdy se nemění pracovně-právní vztah apod.	Funkční	Požadované	Ano	Ano		
	B.1.9	ukončení pracovněprávního vztahu	Funkční	Požadované	Ano	Ano		
	B.1.10	aktivace/deaktivace (ruční, automatická) identity jejich uživatelských účtů,přiřazení aplikačních a business rolí, atributů apod.	Funkční	Požadované	Ano	Ano		
	B.1.11	Anonymizace definovaných údajů identity a jejich uživatelských účtů na základě pravidla nebo na vyžádání	Funkční	Požadované	Ano	Ano		
C		**Řízení identit, rolí, systemizace, atributů**						
	C.1	IDM umožní přesun členství uživatelských účtů identity mezi aplkačními a business rolemi pro uživatelské účty zaměstnanců, externistů dodavatelů, externistů dopravců atd. Na základě automatickyých pravidel definujících atributy uživatelských účtů identity a jejich hodnoty, při kterých se mění členství uživatelských účtů v aplikačních a business rolích nebo na základě žádosti o odebrání nebo přiřazení aplikační nebo business role a schválení žádosti definovanými schvalovateli. Všechny žádosti o přiřazení členství uživatelských účtu do apliakční nebo business role musí mít definovaný důvod žádosti a datum platnosti přiřazení od a do. Zamítnuté žádosti musí obsahovat důvod zamítnutí.	Funkční	Požadované	Ano	Ano		
	C.2	IDM umožní kopírovaní přiřazené aplikačních role do business role odpvídající pracovnímu místu nebo činnosti uživatele, z jedné definované business role do jiné definované business role.	Funkční	Požadované		Ano		
	C.3	IDM umožní automatizované přiřazení nebo odebrání členství uživatelského účtu v aplikačních a business rolích na základě definovaných atributů uživatelského účtu a jejich definovaných hodnot např.podle hodnoty systemizovaného místa, organizační jednotky. O tyto aplikační nebo nebo bussiness role bude zároveň možné žádat prstřednictvím uživatelského portálu IDM a každá tato žádost musí obsahovat důvod žádosti a datum platnosti přiřazení od a do. X dnů před vypršením platnosti přiřazení je uživatels notifikován zda chce žádost prodloužit. Pokud ano musí znovu zadat důvod žádosti a platnost přiřazení od a do. Po vypršení platnosti žádosti o přiřazení do aplikační nebo business role sytém IDM automaticky odebere členství uživatelského účtu z aplikační nebo business role u které vypršela platnost žádosti.	Funkční	Požadované		Ano		Ano
	C.4	IDM umožní přidělení a odebrání role členství uživatelského účtu identity v aplikační nebo business roli na základě organizačního zařazení nebo činnosti, nebo typu smluvního vztahu nebo typu účtu nebo jekékoliv jiné kombinace jakéhokoliv atributu nebo skupiny atributů uživatelského účtu.	Funkční	Požadované	Ano	Ano		
	C.5	IDM umožní správu business/aplikačních rolí, včetně zařazení uživatele do odpovídající role.	Funkční	Požadované	Ano	Ano		
	C.6	IDM umožní dočasné nastavování členství uživatelského účtu v aplikačních nebo busness rolích přiřazených manuálně správcem aplikační nebo business role nebo na základě žádosti o přiřazení členství do aplikační nebo buisiness role a jejím schválení. Všechny tyto typy přiřazení musí mít platnost od a do a po uplynutí nastaveného intervalu se role automaticky odebere.	Funkční	Požadované	Ano	Ano	Ano	
	C.7	IDM umožní automatizované nastavování rolí nebo atributů na základě pravidel (událostí).	Funkční	Požadované	Ano	Ano	Ano	
	C.8	IDM umožní kopírovat přiřazené aplikační role mezi jednotlivými business rolemi.	Funkční	Požadované		Ano		
	C.9	IDM musí obsahovat funkcionalitu umožňující přenesení přiřazených oprávění (členství uživatele v aplikačních a business rolích) na jiného uživatele. Toto přenesení musí mít nastavitelné časové omezení platnosti od a do stejně jako vyplněný důvod přenesení. Přenesení oprávnění je schvalováno stejným způsobem jako by uživatel,na kterého jsou oprávnění přenášena o tato oprávnění žádal sám. Tedy stejně jako jsou schvalovány žádosti o přiřazení členství uživatelského účtu v aplikačních a business rolích, které jsou přenášeny.	Funkční	Požadované		Ano		
	C.10	IDM umožní definovat vztahy zastupitelnosti (delegování). IDM musí umožnit uživatelům, aby na portálovém rozhraní IDM mohli: – definovat zástup ve schvalovacích workflow, ve kterých je zastupovaný členem v případě potřeby (nemoc, dovolená atd.) – delegovat v případě potřeby (nemoc, dovolená atd.) svoje role, nebo vybrané role na jiné pověřené osoby. Delegování bude defonavetlné jako časově omezené s platností do a do, kdy se po nastaveném intervalu n nastavená delegování automaticky v IDM zruší.	Funkční	Požadované	Ano	Ano		Ano
	C.11	Správu business rolí představujících činnost uživatelú vyplývající z jejich zařazení do organizační struktury (systemizace) nebo činnost nevyplývajících z organizačního zařazení, ale smluvního vztahu nebo z projektu apod. bude možné automatizovat na základě dat ze zdrojových systémů s možností volby rozdílných pravidel pro jejich automatizované vytváření v systému IDM na základě typu business role např. zaměstnanecké, dodavatelské atd.	Funkční	Požadované	Ano			Ano
	C.12	IDM zajistí možnost přidávání členství uživatelského účtu identity do dalších typů referenčních objektů v systému IDM a na portále IDM (například do business role reprezentující systematizované místo, organizační jednotku, skupinu, pracovní pozici, funkci do aplikační role, skupiny apliakčních rolí nebo přiřadí certifikát apod.) a to i v průběhu zakládání či úpravy konkrétního uživatelského účtu identity s možností okamžitého použití referenčního objektu u spravovaného účtu identity v synchronizaci s cílovými systémy.	Funkční	Požadované	Ano	Ano		Ano
	C.13	IDM zajistí dodatečné rozšiřování identit, uživatelských účtů a referenčních objektů o další atributy a zajistí publikaci i těchto nových atributů externím aplikacím prostřednictvím rozhraní webových služeb IDM nebo konektorů IDM na cílové systémy.	Funkční	Požadované		Ano		Ano

	C.14	Správa identity bude umožňovat i správu údajů o uživatelských digitálních certifikátech. Data o certifikátech bude možné nahrávat do systému prostřednictvím rozhraní webových služeb. Současně zajistí IDM notifikace uživatelů na základě definovaných pravidel správy certifikátu (vypšení platnosti apod.).	Funkční	Požadované	Ano	Ano	Ano	Ano
	C.15	IDM umožní k identitám přikládat obrazové soubory (fotografie)	Funkční	Požadované	Ano	Ano	Ano	Ano
	C.16	IDM musí obsahovat registr aplikací a informačních systémů (souhrnně IS) a jejich aplikačních rolí včetně možnosti importu rolí přes webové služby	Funkční	Požadované		Ano		Ano
	C.17	IDM musí obsahovat integrovanou správu aplikačních rolí, včetně zařazení uživatele do odpovídající role v napojených IS.	Funkční	Požadované		Ano		Ano
	C.18	IDM musí obsahovat integrovanou správu samostatných identifikovatelných objektů – referenčních objektů, na které se identity mohou odkazovat:například do business role reprezentující systematizované místo, organizační jednotku, skupinu, pracovní pozici, funkci a do aplikační role, skupiny apliakčních rolí nebo přiřadí certifikát apod.	Funkční	Požadované		Ano		Ano
	C.19	IDM umožní správu evidence osobních údajů, která bude obsahovat správu evidence subjektů údajů a evidenci jejich osobních údajů včetně jejich kategorií a klasifikací.	Funkční	Požadované		Ano		
	C.20	IDM umožní evidenci účelů pro nakládání s osobními údaji subjektů údajů. V rámci daného účelu budou definována oprávnění, aplikační role pro přístup k osobním údajům.	Funkční	Požadované		Ano		
	C.21	IDM bude obsahovat správu apliakčních rolí s možností začleňovat více aplikačních rolí do business rolí a začleňování více business rolí do jedné business role. Uživatelské účty spravovaných identit se pak při přiřazení do business role automaticky stanou členy všech vnořených business a aplikačních rolí.	Funkční	Požadované		Ano		
	C.22	IDM musí umožnovat správu organizačních a činnostních business rolí, jejich vytváření a synchronizace do spravovaných systémů (provisioning) IDM podporuje přiřazování aplikačních rolí uživatelským účtům identit na základě členství uživatelských účtů v organizačních a činnostních business rolích na principu RBAC, popř. ABAC	Funkční	Požadované		Ano		
	C.23	IDM podporuje vytváření neomezených vazeb mezi jednotlivými typy business a aplikačních rolí. Tyto vazby je možné vytvářet manuálně se začleněním podmínky schválení přiřazení aplikační role do business role nebo jedné business role do druhé business role definovanými schvalovateli. Business role a jejich vzájemné vazby je možné vytvářet automatizovaně na základě pravidel s využitím dat ze zdrojových systémů.	Funkční	Požadované	Ano	Ano	Ano	
	C.24	IDM umožní aktivovat nebo deaktivovat přiřazené role na základě splnění definovaných podmínek (vyhodnocení pravidla), např. aktivovat roli na základě absolvovaného školení uživatele (případně neaktivovat na základě vypršení platnosti školení) nebo absolvování zdravotní prohlídky apod.. Požadovaná vlastnost musí volitelně umožnit jak okamžitou aktivaci/dekativaci role, tak i jen upozornění na případnou aktivaci/dekativaci role.	Funkční	Požadované	Ano	Ano	Ano	Ano
	C.25	IDM umožní zobrazování a výpis aktuálního stavu žádostíuživatelských účtů o aplikační a business role, jejich platnosti, schvalovatele a průběh schvalování. Zároveň umožní výpis aktuálního stavu přiřazení aplikačních rolí a business rolí uživatelském účtům a zobrazení důvodu přiřazení, přes business roli, přímé přiřazení.	Funkční	Volitelné		Ano		
D		**Automatizace řízení živ. cyklu identity, automatizace procesů**						
	D.1	IDM musí disponovat integrovanou podporou automatizace – na úrovni intuitivní tvorby pravidel v grafickém prostředí (např. pro automatické vytváření uživatelských účtů, začleňování identit nebo účtů do skupin, přiřazování business/aplikačních rolí na základě libovolných atributů identity a přidružených referenčních objektů – business role, aplikační role atd.). Integrovaná automatizace pro řízení životního cyklu změn identit a schvalování změn musí umožnit minimálně následující:	Funkční	Požadované		Ano		
	D.1.1	- zadávání požadavků uživatelů na změny v přiřazení rolí a skupin ke schválení nadřízeným a vlastníkem obejktu nebo správcem přístupů aplikační role	Funkční	Požadované		Ano		
	D.1.2	- možnost sledování stavu svých požadavků uživateli	Funkční	Požadované		Ano		
	D.1.3	- emailové upozornění schvalovatele na požadavek ke schválení	Funkční	Požadované		Ano		
	D.1.4	- vytvoření a zobrazení přehledu úloh ke schválení pro každého schvalovatele	Funkční	Požadované		Ano		
	D.1.5	- schvalování či zamítnutí požadavků včetně uvedení zdůvodnění	Funkční	Požadované		Ano		
	D.1.6	- vícekrokové schvalování	Funkční	Požadované		Ano		
	D.1.7	- schvalování jedním nebo více schvalovateli (skupinou)	Funkční	Požadované		Ano		
	D.1.8	- větvení pro ošetření výjimek vzniklých při schvalování	Funkční	Volitelné		Ano		
	D.1.9	- řešení zastupitelnosti (delegování)	Funkční	Požadované		Ano		
	D.1.10	- eskalace – upozornění při překročení termínu splnění	Funkční	Požadované		Ano		
	D.1.11	- vkládání systémových kroků s voláním webových služeb a spuštěním skriptů	Funkční	Požadované		Ano		
	D.1.12	- pro správce IDM pracovat se všemi úlohami	Funkční	Požadované		Ano		
	D.2	IDM bude obsahovat administrátorsky nastavitelnou automatizaci procesů správy životního cyklu osobních údajů subjektu údajů.	Funkční	Požadované		Ano		

	D.3	IDM automatizovaně provede (vyžádá u příslušné CA) zneplatnění certifikátů, o kterým má uložené informace na základě definovaných podmínek (změn pracovně právního vztahům, vypršení platnosti certifikátu atd.)	Funkční	Požadované		Ano		Ano
	D.4	IDM umožní autonomní správu hesel (samoobsluha)., tj. bude obsahovat uživatelské rozhraní pro reset hesla jednotlivých účtů daného uživatele. Zasílání kódů pro reset hesla danému uživatele musí být možno provádět pomocí SMS (tj. IDM musí být možné na SMS bránu či službu napojit). Rozhraní musí umožnit i běžnou změnu hesla (bez resetu).	Funkční	Požadované	Ano	Ano	Ano	Ano
	D.5	IDM bude obsahovat samoobslužné uživatelské rozhraní pro zadávání žádostí o přidělení jednotlivých business nebo aplikačních rolí a členství ve skupinách. Role a skupiny budou kategorizovány a kategoriím bude možné přidělit schvalovací workflow nebo může žádost vyřízena automaticky bez schválení.	Funkční	Požadované	Ano	Ano	Ano	Ano
	D.6	IDM musí podporovat vytváření workflow s více stupni schvalování a eskalací bez oheldu na organizační strukturu na základě definovaného pravidla. Umožní přidělení oprávnění nebo role konkrétnímu uživatelskému účtu identity, organizační business roli, skupině nebo business roli reprezentující organizační jednotku	Funkční	Požadované				
	D.7	Samoobslužné rozhraní umožní definovat white list pro každou aplikační a business role pomocí pravidel definovaných atributem nebo kombinací atributů uživatele. Pouze uživatelé splňující definované pravidlo na white listu aplikační nebo business role mohou definovanou aplikační a busoness roli vidět v seznamu aplikačních a business rolí a mohou o ni zažádat. IDM zároveň zamezí zažádosti uživatele o aplikační roli, kterou již má přidělenou na základě automatického pravidla nebo přes business roli.	Funkční	Požadované				
	D.8	IDM bude obsahovat rozhraní pro řešení uzamčených/neplatných účtů pro případ, že uživatel nemá přístup k SD/HD nástroji (implementace "captive portálu")	Funkční	Volitelné		Ano	Ano	Ano
E		**Propojení na koncové (cílové) systémy, synchronizace**						
	E.1	Při napojování IDM na cílové (koncové) systémy pro automatizovanou synchronizaci rolí, účtů a přístupů se bude IDM přizpůsobovat koncovým systémům a nikoli naopak (tedy při vytváření rozhraní pro připojení cílového systému bude většinově probíhat tvorba rozhraní na straně IDM).	Funkční	Požadované		Ano		Ano
	E.2	IDM musí podporovat propojení na systémy typu PAM	Funkční	Požadované		Ano		Ano
	E.3	IDM musí procesně podporovat napojení systémů bez API (vytvářením workorderů k práci s účty).	Funkční	Požadované		Ano		Ano
	E.4	IDM musí podporovat napojení na systém distribuce, ukládání, bezpečnou archivaci, změny, ničení, kontrolu a audit klíčů s využitím PAM.	Funkční	Požadované		Ano		Ano
	E.5	IDM musí podporovat napojení na RADIUS Server.	Funkční	Požadované		Ano		Ano
	E.6	IDM musí obsahovat API pro připojení dalších systémů SŽ	Funkční	Požadované		Ano		Ano
	E.7	IDM musí umožnit migraci z a do jiného Identity Manažeru.	Funkční	Volitelné		Ano		Ano
	E.8	IDM musí obsahovat Centrální GUI pro administraci administrátorem.	Funkční	Požadované		Ano		
	E.9	IDM musí podporovat komunikaci SAML a napojení na AD.	Funkční	Požadované		Ano		Ano
	E.10	IDM musí podporovat napojení na systém SAP	Funkční	Požadované		Ano		Ano
	E.11	IDM musí umožnit synchronizaci identit, jejich uživatelských účtů a jejich atributů v jednotlivých spravovaných systémech a jejich permanentní rekonciliaci s centrálním stavem identit v IDM (reconciliation)	Funkční	Požadované		Ano		Ano
	E.12	IDM musí podporovat SCIM 2.0 (System for Cross-domain Identity Management)	Funkční	Požadované		Ano		Ano
	E.13	IDM musí podporovat definici SCIM						
F		**Logování, auditní stopy, ostatní požadavky**						
	F.1	IDM musí umožňovat záznam definovaných důležitých událostí v IdentityManageru a následný audit a reporting.	Nefunkční	Požadované				
	F.2	IDM musí podporovat auditní procesy, zejména evidenci nastavení vlastností objektu (identity, role, aplikační role, atributů apod.) v zadaném čase. IDM musí zajistit možnost zjistit nastavení daného objektu v požadovaném čase (příklad: možnost zjistit nastavení vlastností identity k určitému časovému okamžiku, tj. přiřazené business role, účty, aplikační role, atributy atd. + log záznam o přenesených změnách cílového systému platných ke zvolenému časovému okamžiku). Retence zachování těchto auditních informací je požadována jako parametrizovaná.	Nefunkční	Požadované		Ano		Ano
	F.3	IDM musí podporovat napojení na Logmanagement systém. Zaznamenávají se všechny aktivity v IDM a použit bude standardní logovací protokol (např. syslog).	Funkční	Požadované		Ano		Ano
	F.4	IDM musí podporovat napojení na systémy typu SIEM.	Funkční	Požadované		Ano		Ano
	F.5	IDM musí být integrován na nástroj typu ServiceDesk	Funkční	Požadované		Ano		Ano
	F.6	IDM musí umožňovat ochranu před špatnými datovými vstupy na základě kontroly vyplnění povinných atributů, kontroly datového typu vstupních atributů, případně kontroly hodnot atributů. Tato kontrola datové konzistence musí probíhat jak na integračních rozhraních ze zdrojových systémů tak na uživatelském rozhraní pro hromadný import dat a portálovém uživatelském rozhraní systému IDM. Nepovolené hodnoty nebude možné do systému IDM přes jakékoliv z integračních a výše definovaných rozhraní zapsat.	Nefunkční	Požadované		Ano		
	F.7	IDM musí podporovat vysokou dostupnost a být implementován jako vysoce dostupný systém včetně geografické dostupnosti respektující geografické rozmístění systémů SŽ a topologii sítě (cluster s geografickou redundancí apod.).	Nefunkční	Požadované				

	F.8	IDM musí jako speciální use-case požadavku F.2 obsahovat uživatelské rozhraní pro zjištění aktuálního stavu nastavení aplikačních rolí a přístupových oprávnění spravovaných identit, příklad pro pravidelný audit a kontrolu těchto oprávnění.	Funkční	Požadované	Ano	Ano	Ano	Ano