

## SEZNAM POŽADAVKŮ NA SYSTÉM IdM - FUNKČNÍ A NEFUNKČNÍ VLASTNOSTI

Oblast	ID	Požadavek	Funkční/Nefunkční	Stav	Uživatelsky/garantem spravované	Administr. spravované	Portál uživatele	API/web service
<b>A Obecné požadavky</b>								
	A.1	IdM musí v návaznosti na zdrojové systémy dat - SAP, JIRA (CMDB + Service desk), AD 1-n, o identitách udržovat a spravovat kompletní životní cyklus identity. Jedná se zejména o příchod zaměstnance, přidělení business rolí dle jeho organizačního zařazení (systematizovaného místa), činnostiho zařazení, doplňování business rolí i mimo systemizované místo, změna rolí v případě jeho změny jeho zařazení, odchod zaměstnance spočívající v deaktivaci, anonymizaci a následně 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 business 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 (souhrnné 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 konkrétní aplikační role a na základě jakého důvodu a zároveň umožňuje zobrazit jaké 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 musí umožňovat export a import 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. IdM musí umožňovat synchronizaci všech výše uvedených objektů a vlastností prostřednictvím API obousměrně do CMDB (Jira) zadavatele.	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 pracovní právního nebo jiného smluvního vztahu fyzické osoby nemá na jedinečný identifikátor identity vliv. Tato fyzická osoba může mít více účtů.	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. Zároveň musí umožnit přiřazení jednoho uživatelského účtu jedné identitě i v případě, že má tato identita více pracovních poměrů.	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 rolích, změny členství ve skupinách atd.). Požadavky na přidělení nebo odebrání členství uživatelského účtu identity v aplikační nebo business roli, budou v IdM schvalovány definovanými schvalovateli (tzv. "schvalovací workflow"). 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. IdM musí umožňovat provést schvalovací workflow i mimo IdM a to prostřednictvím API, které musí umožňovat přenesení seznamu aplikací, jejich atributů, byznys rolí, schématu workflow a jeho schvalovatelů z IdM do aplikace JIRA a zrcadlit celý průběh schvalovacího workflow při každé akci zpět do IdM včetně výsledku schvalování.	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 nahraovat 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 (dle všech zákonných požadavků)	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/DPC běžný účet, pracovník DPP/DPC administrátorský účet, externista dodavatel běžný účet, externista dodavatel administrátorský účet, externista dopravce běžný účet atd.)	Funkční	Požadované				Ano

PŘEDBĚŽNÉ FUNKČNÍ A NEFUNKČNÍ POŽADAVKY  
NA BUDOUCÍ SYSTÉM IDM

A.10	Integrace se systémem JIRA. IdM musí obousměrně komunikovat s CMDB provozovaným v rámci aplikace JIRA, minimálně v těchto oblastech: - seznam aplikací a jejich atributů, vlastností, které mají být řízeny prostřednictvím IdM - seznam business rolí k aplikacím včetně aplikačních rolí, z kterých se skládají - seznam požadovaných aktérů (rolí) přiřazených k jednotlivým schvalovacím workflow, které budou probíhat v rámci JIRA - zrcadlení jednotlivých schvalovacích workflow (ticketů) probíhajících v JIRA přímo do IdM a to při každém kroku schválení včetně finálního výsledku schvalování a to včetně všech atributů workflow náležitě.	Funkční	Požadované		Ano		Ano
A.11	IdM musí být schopno provozu v režimu vysoké dostupnosti (HA)	Funkční	Požadované				
A.12	IdM musí v rámci integrací na všechny adresářové služby Microsoft AD komunikovat způsobem vždy na celou doménu (nikoliv pouze na konkrétní řadič). IdM musí umožňovat komunikaci na vícero AD instancí.	Funkční	Požadované				
A.13	IdM musí umožňovat provoz, kdy za účelem správné segmentace sítí bude do tomu určených sítí umístěna IdM sonda (případně druhá instance IdM), která bude na základě pokynů hlavní IdM instance vykonávat všechny úkony nutné pro zajištění řízení účtů a rolí aplikací v této podsíti a to včetně schvalovacích workflow. Způsob komunikace mezi hlavní IdM a IdM sondy musí být v odpovídající úrovni zabezpečení.	Funkční	Požadované				
A.14	IdM musí ze zdrojového systému (SAP) importovat a udržovat organizační strukturu a využívat ji a to včetně organizačních struktur externích subjektů. Přístup k dané struktuře a v ní zařazených identitách musí být na základě oprávnění.	Funkční	Požadované				
A.15	IdM musí umožňovat řízení přístupu k jednotlivým částem aplikace samotné na základě rolí uživatele a musí umožňovat k těmto rolím přiřadit přístup ke konkrétní části UI aplikace IdM (do úrovně atributů jednotlivých entit). Například náhled manažera na podřízené.	Funkční	Požadované				
A.16	IdM musí zajistit bezchybnou správu identity v rozsahu minimálně 40 000 aktivních uživatelů a komplexní správu všech neaktivních a anonymizovaných identit.	Funkční	Požadované				
A.17	IdM musí u VPN pro externí subjekty evidovat platnou smlouvu s dodavatelem v SAPu a konec platnosti.	Funkční	Požadované				
A.18	IdM musí evidovat informaci o poslední změně hesla.	Funkční	Požadované				
<b>B</b>	<b>Podpora procesů</b>						
B.1	IdM musí (v návaznosti na zdrojové systémy dat) podporovat procesy správy životního cyklu identity a jejich uživatelských účtů a související obslužné 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	Funkční	Požadované	Ano	Ano		
B.1.5	změny organizačního zařazení	Funkční	Požadované	Ano	Ano		
B.1.6	změny platnosti vlastností identity = změna platnosti uživatelských účtů identity a jejich atributů, změna 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 apod.) 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 určuje platnost jejich uživatelských účtů v napojených aplikacích, zároveň přiřazení / odebrání aplikačních a business rolí, atributů apod., přičemž musí umět rozlišit automatické a ruční provedení dle typu osoby (zaměstnanec, externista atd.).	Funkční	Požadované	Ano	Ano		
B.1.11	Zneplatnění identity a následná anonymizace definovaných údajů identity a jejich uživatelských účtů na základě pravidla nebo na vyžádání po definované době.	Funkční	Požadované	Ano	Ano		
B.2	Všechny procesy dle bodu B.1 musí být realizovatelné jak automaticky (převzetím ze zdrojového systému) tak manuálně na úrovni IdM tomu oprávněnou rolí uživatele.	Funkční	Požadované	Ano	Ano		
B.3	IdM musí umožňovat převedení rolí jedné identity na garantem určenou jinou identitu za účelem zajištění kontinuity činností	Funkční	Požadované	Ano	Ano		
<b>C</b>	<b>Řízení identit, rolí, systemizace, atributů</b>						

PŘEDBĚŽNÉ FUNKČNÍ A NEFUNKČNÍ POŽADAVKY  
NA BUDOUCÍ SYSTÉM IDM

C.1	IdM umožní přesun členství uživatelských účtů identity mezi aplikačními a business rolemi pro uživatelské účty zaměstnanců, externistů, dodavatelů, externistů dopravců atd. Na základě automatických 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 účtů do aplikační 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 kopírování přiřazené aplikačních role do business role odpovídající 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 business role bude zároveň možné žádat prostřednictvím uživatelského portálu IdM (a zároveň prostřednictvím JIRA SD, do které bude schvalovací proces přenášen) a každá tato žádost musí obsahovat důvod žádosti a datum platnosti přiřazení od a do. X dnů před vypršením platnosti přiřazení je uživatel 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 systém 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 jakékoliv 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 business rolích přiřazených manuálně správcem aplikační nebo business role nebo na základě žádosti o přiřazení členství do aplikační nebo business 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 oprávnění (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 definovatelné jako časově omezené s platností do a do, kdy se po nastaveném intervalu nastavená delegování automaticky v IdM zruší.	Funkční	Požadované	Ano	Ano		Ano
C.11	Správu business rolí představujících činnost uživatelů vyplývající z jejich zařazení do organizační struktury (systemizace) nebo činnost nevplývající 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 systemizované místo, organizační jednotku, skupinu, pracovní pozici, funkci do aplikační role, skupiny aplikačních 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 certifikátů (vypšení platnosti apod.).	Funkční	Požadované	Ano	Ano	Ano	Ano

PŘEDBĚŽNÉ FUNKČNÍ A NEFUNKČNÍ POŽADAVKY  
NA BUDOUCÍ SYSTÉM IDM

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, zároveň musí umožňovat import těchto aplikací a jejich parametrů prostřednictvím webových služeb.	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 aplikačních 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 aplikačních 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 umožňovat 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/deaktivaci role, tak i jen upozornění na případnou aktivaci/deaktivaci role.	Funkční	Požadované	Ano	Ano	Ano	Ano
C.25	IdM umožní definovaným specifickým rolím v IdM zobrazování a výpis aktuálního stavu žádostí uživatelských účtů o aplikační a business role, jejich platnosti, schvalovatele a průběh schvalování. IdM zároveň umožní definovaným specifickým rolím v IdM přístup k reportingu, tzn. souboru funkcí a filtrování, jejichž použitím bude možné získat aktuální výpisy: - přiřazení rolí uživatelským účtům a zobrazení důvodu přiřazení (přes business roli, přímé přiřazení apod.) s možností filtrování dle parametrů - přehledu všech oprávnění konkrétního typu, dle zařazení v organizační struktuře apod.	Funkční	Požadované		Ano		
C.26	IdM musí spravovat byznys role hierarchicky tak, aby bylo možné je skládat z aplikačních rolí, nebo jiných byznys rolí a to do minimálně 25 úrovní.	Funkční	Požadované	Ano	Ano		
C.27	IdM musí umožňovat správu vícero stromů organizačních struktur a definovat vícero parametrů pro jednotlivé objekty struktur a musí je v rámci UI vhodně vizuálně zobrazovat. Přístupy do jednotlivých stromů na základě oprávnění.	Funkční	Požadované	Ano	Ano		
C.28	IdM musí umožňovat přiřazení identity nebo role do více organizačních struktur.	Funkční	Požadované	Ano	Ano		
C.29	IdM musí umožňovat vytvoření pravidel pro konfliktní role a implementovat tato vytvořená pravidla do logiky aplikace včetně schvalovacích workflow.	Funkční	Požadované	Ano	Ano		
C.30	IdM musí umožnit vytvářet role pro aktéry při přiřazování rolí u aplikací, jako vlastníci, schvalovatelé, věcní garanti, techničtí garanti a přiřazovat jim platnost od do.	Funkční	Požadované		Ano		
C.29	IdM musí umožnit pracovat s objekty z řízených aplikací typu Organizace a její Organizační struktura, Skupina, Uživatel, Role a synchronizovat je formou API.	Funkční	Požadované		Ano		Ano
<b>D Automatizace řízení živ. cyklu identity, automatizace procesů</b>							
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.), založených na principu BPM. 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 nadřazeným a vlastníkem objektu 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	- víceřadkové schvalování bez limitu počtu kroků	Funkční	Požadované		Ano		
D.1.7	- schvalování jedním nebo více schvalovateli (skupinou) - bez limitu počtu schvalovatelů	Funkční	Požadované		Ano		
D.1.8	- větvení pro ošetření výjimek vzniklých při schvalování	Funkční	Požadované		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 administrátorský nastavitelnou automatizaci procesů správy životního cyklu osobních údajů subjektu údajů.	Funkční	Požadované		Ano		
D.3	IDM automatizovaně provede (vyžádá u příslušné CA) zneplatnění certifikátů, u kterým má uložené informace na základě definovaných podmínek (změn pracovně právního vztahů, 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. Zaslání kódů pro reset hesla danému uživateli 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). IDM musí spravovat historii hesel jednotlivých identit a log průběhu jejich změn, včetně neúspěšně provedených. Při změně hesla musí být provedena kontrola dle nastavených pravidel tvorby hesel. IDM musí umět pracovat s definovatelnou politikou hesel v rámci UI a to minimálně minimálně v rozsahu: - doba platnosti hesla a frekvence obnovy - počet znaků hesla, přičemž umožňuje zadat heslo o délce alespoň 64 znaků - minimální počet speciálních znaků, číslic, velkých písmen, malých písmen - ověření a zamezení použití minimálně 12 posledních hesel (počet lze konfigurovat) - kontrola a zamezení použití nejčastěji používaných hesel - doba mezi dvěma změnami hesla nesmí být menší než 30 minut - kontrola a zamezení tvorby hesla na základě mnohonásobně opakujících se znaků, přihlašovacího jména, e-mailu, názvu systému	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 ohledu 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 business roli vidět v seznamu aplikačních a business rolí a mohou o ni požádat. IDM zároveň zamezí žádosti 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	Požadované		Ano	Ano	Ano
<b>E Propojení na koncové (cílové) systémy, synchronizace</b>							
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 většinou probíhat tvorba rozhraní na straně IDM).	Funkční	Požadované		Ano		Ano
E.2	IDM musí podporovat propojení na systémy typu PAM a v rámci toho efektivně provádět správu privilegovaných účtů	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 export všech dat (včetně pravidel a workflow) do strojově čitelného formátu.	Funkční	Požadované		Ano		Ano

E.8	IdM musí obsahovat Centrální GUI pro administraci.	Funkční	Požadované		Ano		
E.9	IdM musí podporovat komunikaci SAML a napojení na vícero MS AD najednou.	Funkční	Požadované		Ano		Ano
E.10	IdM musí podporovat napojení na systém SAP	Funkční	Požadované		Ano		Ano
E.11	IdM musí umožnit obousměrnou synchronizaci identit, jejich uživatelských účtů a jejich atributů v jednotlivých spravovaných systémech a jejich permanentní rekongiliaci s centrálním stavem identit v IdM. Tuto rekongiliaci musí být možné nastavit tak, aby IdM bylo pro koncové aplikace autoritativní.	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 umožňovat synchronizaci dat jiných než idetnitních (aplikačních rolí, jejich parametrů atd.) z řízených (koncových) aplikací pro jejich využití v rámci tvorby byznys rolí.	Funkční	Požadované				
E.14	IdM musí umožňovat opakování synchronizace, nebo propagace změn v případě selhání a zároveň musí všechny tyto aktivity logovat.	Funkční	Požadované				
E.16	IdM musí umožňovat práci se složenými i binárními atributy uživatele (např. certifikáty, fotografie, autentizační tokeny).	Funkční	Požadované				
E.17	IdM musí umožňovat řešení výsledků rekongiliace formou vynucení přepsání, nebo smazání neoprávněných účtů, ale i ponechání účtů označených v koncových aplikacích jako "nesynchronizovat".	Funkční	Požadované				
E.18	IdM musí umožňovat i řízení identit a rekongiliaci off-line systémů způsoby: - manuálním nastavením v koncové aplikaci a potvrzením řešitelskou skupinou, přičemž zaslání úkolu skupině a potvrzení jeho vyřízení může probíhat jak v rámci IdM tak prostřednictvím napojení na JIRA SD - specifickým rozhraním aplikace, umožňující import dat získaných z manuálního exportu z koncového systému	Funkční	Požadované				
E.19	IdM musí umužňovat provádění hromadných akcí typu: - hromadné schvalování přidělných úkolů - hromadné změny v organizační struktuře - hromadné přiřazování rolí uživatelům dle kritérií	Funkční	Požadované				
E.20	IdM musí umožňovat napojení na systémy LDAP na portu 636 s vlastním interním certifikátem s podporou EC algoritmu	Funkční	Požadované				
<b>F Logování, auditní stopy, ostatní požadavky</b>							
F.1	IdM musí umožňovat logování, tj. záznam definovaných důležitých událostí v IdM a následný audit a reporting a to minimálně v rozsahu stanovených legislativními požadavky v oblasti kybernetické bezpečnosti: - přihlašování a odhlašování ke všem účtům, a to včetně neúspěšných pokusů, - činností provedených administrátory, - úspěšné i neúspěšné manipulace s účty, oprávněními a právy, - neprovedení činností v důsledku nedostatku přístupových práv a oprávnění, - činností uživatelů, které mohou mít vliv na bezpečnost informačního a komunikačního systému, - zahájení a ukončení činností technických aktiv, - kritických i chybových hlášení technických aktiv a - přístupů k záznamům o událostech, pokusy o manipulaci se záznamy o událostech a změny nastavení nástrojů pro zaznamenávání událostí	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 použít 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 dodavatelem integrován na servicedeskový nástroj JIRA Atlassian (Cloud) v rozsahu: - předávání informací z a do CMDB - předávání ticketů v rámci schvalovacích workflow	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		

PŘEDBĚŽNÉ FUNKČNÍ A NEFUNKČNÍ POŽADAVKY  
NA BUDOUCÍ SYSTÉM IDM

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
F.9	IdM musí podporovat správu technických a privilegovaných účtů a jejich zvláštností v rámci správy (platnost hesel atd.).	Funkční	Požadované				
F.10	IdM musí zajišťovat komplexní proces odesílání notifikací včetně napojení na vícero poštovních serverů za účelem jejich odeslání.	Funkční	Požadované		Ano		
F.11	IdM musí umožňovat tvorbu a správu šablon notifikačních emailů v HTML formátu, včetně hypertextových odkazů.	Funkční	Požadované		Ano		
F.12	IdM musí zajistit šifrování všech hesel a případně jiných objektů dle aktuálně platných standardů a požadavků kybernetické bezpečnosti.	Funkční	Požadované				