NÁRODNÍ PLÁN OBNOVY

Financováno Evropskou unií NextGenerationEU

MINISTERSTVO VNITRA ČESKÉ REPUBLIKY

TECHNICKÁ SPECIFIKACE

KYBERBEZPEČNOST

„Bezpečná infrastruktura města Znojma“

ČÁST 1: NÁSTROJ PRO SPRÁVU A ŘÍZENÍ IDENTIT

Veškeré produkty, které dodavatel dodává v rámci plnění zadavateli, musí splňovat následující podmínky a dodavatel splnění těchto podmínek potvrdí samostatným čestným prohlášením:

(a) jsou nové, byly oprávněně uvedeny na trh v EU nebo pochází z autorizovaného prodejního kanálu výrobce,
(b) mají plnou záruku od výrobce,
(c) jsou podporovány výrobcem a jsou součástí servisního a podpůrného programu výrobce,
(d) obsahují všechny nezbytné licence na používání příslušného softwaru,
(e) jsou v databázi výrobce uvedeny jako prodaná kupujícímu,
(f) jsou určeny pro provoz v České republice.

Tyto skutečnosti dodavatel doloží potvrzením výrobce daného zařízení, nebo čestným prohlášením distributora, nelze-li prohlášení výrobce získat.

Zadavatel si vyhrazuje právo na ověření všech dodaných informací od výrobce daného zařízení a zjištění původu výrobků před podpisem smlouvy a nejpozději při jejich předávání, a to dle příslušných sériových čísel a právo podpisu akceptačního protokolu, osvědčujícího převzetí dodávky, až po ověření původu výrobku.

Dodavatel doloží toto potvrzení ke všem nabídnutým technologiím

IDM – Identity management

Správa řízení uživatelů			
Parametr	**Popis povinného parametru**	**Uchazeč popíše detailní návrh způsob naplnění tohoto povinného parametru včetně značkové specifikace nabízených dodávek**	**Uchazeč uvede odkaz na přiloženou část nabídky, kde je možné ověřit naplnění parametru**
Licence	Poskytnutá licence umožní nasazení a provoz systému bez omezení na počet uživatelů, spravovaných identit a napojených systémů. Nejsou přípustná žádná další omezení omezující obvyklé nasazení a provoz s ohledem na charakter organizace Zadavatele (počet záznamů, velikost databází atd.). Předpokládaný počet uživatelů je do 450. Záruka 5Y		
Škálovatelnost	Systém musí umožnit zvyšování výkonu (zlepšování odezvy) rozložením komponent Systému na více serverů – minimálně oddělení rolí (serverů) uživatelského rozhraní od výkonu integračních a provozních úloh. Data systému budou uchovávána v databázi. Systém bude podporovat režimu běhu ve vysoké dostupnosti.		
Uživatelské role	Integrovaná správa aplikačních rolí včetně zařazení uživatele do odpovídající role v příslušných IS. V rámci dané role bude možné definovat jemné členění různých významů role. Například roli „editor webu“ bude možné rozšířit o významy		

	odpovídající jednotlivým oddělením, pro které jsou části webu určené. Tyto rozšiřující významy rolí bude možné přímo přiřazovat systematizovaným místům, skupinám, organizačním jednotkám, uživatelům spravovaných v systému. Systém umožní správu zákazových rolí. Zákazová role přiřazená systematizovanému místu, skupině, organizační jednotce nebo přímo uživateli zajistí odebrání této role v synchronizovaných systémech. Systém umožní delegaci aplikačních rolí. Při delegaci jsou aplikační role předány na nového uživatele s možností nastavení platnosti, do kdy je delegace platná. Následně jsou role vráceny delegujícímu uživateli a odebraný delegovanému.		
Historizace	Vestavěná detailní databázové historizace pro evidenci změn identit včetně referenčních objektů a vazeb mezi nimi. Historizace poskytne data v libovolném časovém okamžiku – aktuálním nebo zpětně v minulosti.		
Automatizace	Podpora intuitivní tvorby pravidel v grafickém prostředí pro automatické vytváření uživatelských účtů, začleňování uživatelů do skupin a přiřazování aplikačních rolí uživatelům na základě kombinace libovolných atributů identity a přidružených referenčních objektů (organizační jednotka, aplikační role, systematizované místo atd.). Provádění vyhodnocení pravidel bude mít stejné vlastnosti jako jiné synchronizační procesy systému. Ruční vs plánované spuštění, historii běhů, simulační režim atd.		

Logování SIEM	Systém bude exportovat auditní logy pro systém typu SIEM ve formátu CSV nebo XML. Systém bude auditní, aplikační a historizační logy aktivně zapisovat do systému SIEM přes SYSLog.		
Logování systému	Systém obsahuje logování min. následujících typů událostí: - události systému (aplikační log) - změny entit evidovaných systémem a změny konfigurace systému (auditní log) - synchronizace s napojenými systémy (synchronizační log) - odeslané notifikace a upozornění (notifikační log)		
Systematizovaná místa	Systém bude implementovat princip systemizovaných míst. Umožní systemizaci pracovních míst v souladu se strukturou organizace a bude spravovat jednotlivá systematizovaná místa a sadu oprávnění a rolí pro jednotlivé IS organizace vztažené ke konkrétnímu systemizovanému místu.		
Vícefaktorová autentizace	Systém podporuje dvoufaktorové přihlášení do IDM pomocí TOTP (první faktor – jméno a heslo, druhý faktor pomocí jednorázově vygenerovaného unikátního kódu: MS Authenticator nebo Google Authenticator).		
Podpora eIDAS	Systém umožní implementaci procesů a rozhraní, která jsou vyžadována v Nařízení Evropského parlamentu a Rady (EU) č. 910/2014 ze dne 23. července 2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES.		

Požadavky na portál – obecné	Systém bude obsahovat webový portál (dále jen Portál), který bude sloužit jako hlavní rozhraní pro uživatele i správce pro přístup k datům, funkcím, správu a konfiguraci Systému.		
Požadavky na portál – přístup	Správa systému musí být implementována jako webová konzole/aplikace přístupná přes prohlížeče Internet Explorer verze 10 a vyšší a poslední verze prohlížečů Firefox, Chrom. Tato webová konzole musí být přístupná výhradně protokolem https.		
Podpora mobilních zařízení	Portál bude implementován s responzivním designem (přizpůsobení vzhledu typu zařízení, ze kterého je k portálu přistupováno).		
Správa referenčních objektů	Portál bude umožňovat přehlednou správu samostatných identifikovatelných objektů – referenčních objektů, na které se identity mohou odkazovat: min. systematizované místo, organizační jednotka, skupina, aplikace, skupina aplikací, aplikační role, certifikát.		
Referenční objekty	Systém umožní přidávání a správu dalších typů referenčních objektů, a to i v průběhu správy konkrétní identity s možností okamžitého použití referenčního objektu u spravované identity. Systém bude v modulu správy identit u scénáře správy konkrétní identity implementovat v grafickém rozhraní přímý odkaz (proklik) na referenční objekty, na která se daná identita odkazuje včetně toho, aby administrátor mohl po přechodu na tento odkaz vytvářet a editovat další referenční objekty a následně po		

	vrácení zpět na detail identity je v tomto scénáři přiřadil dané spravované identitě. Systém bude podporovat tvorbu vlastních referenčních objektů. V rámci těchto objektů bude možné přidat libovolných seznam atributů k objektu. Referenční objekty je možné připojovat jako atributy k jiným objektům (např. k uživatelským účtům). Systém umožní deaktivaci položek referenčních objektů a celých referenčních objektů v režimu aktivní/neaktivní.		
Zabezpečení referenčních objektů	Systém umožní nastavení samostatných nezávislých administrátorských oprávnění pro správu jednotlivých referenčních objektů		
Rozšiřující atributy	Systém umožní dodatečné rozšiřování identit a referenčních objektů o další atributy a zajistí publikaci těchto nových atributů externím aplikacím prostřednictvím rozhraní webových služeb IDM.		
Přehledné zobrazení	Systém bude obsahovat grafické zobrazení identit (uživatelských účtů) ve stromové organizační struktuře. Součástí jednoho pohledu v systému bude zobrazení organizační struktury včetně systematizovaných míst organizace až do úrovně jednotlivých uživatelských účtů (identit). V grafickém zobrazení stromové struktury bude možné vyhledávat jednotlivé identity, systematizovaná místa, organizační jednotky.		
Vyhledávání – diakritika	Portál bude umožňovat vyhledávat i bez diakritiky (např. zadání Novak vyhledává i Novák apod.)		

Správa certifikátů	Správa uživatelů (identit) bude umožňovat i správu údajů o uživatelských digitálních certifikátech. Data o certifikátech bude možné nahrávat do systému prostřednictvím rozhraní webových služeb. Systém umožní automatické zneplatnění uložených certifikátů po vypršení data platnosti.		
Obrázky	Systém umožní k jednotlivým účtům (identitám) přikládat obrázky – fotografie.		
Přesun identit	Systém umožní přesun identit mezi jednotlivými organizacemi či jejich odděleními.		
Kopírování rolí	Systém IDM umožní kopírování aplikačních, činnostních rolí a skupin mezi uživateli nebo pracovními pozicemi. Systém IDM umožní výběr konkrétních položek pro kopírování.		
Ochrana proti chybám	Systém bude obsahovat mechanismus zabránění hromadným změnám z důvodu případných chybných vstupních dat (např. z personálního systému), aby nedošlo k hromadným nežádoucím změnám (například smazání objektů v Active Directory apod).		
Aktivní uživatelé	Systém bude obsahovat přehled uživatelů aktuálně pracujících s Portálem		
Slučování identit	Systém umožní sjednocení více uživatelů (identit) do jedné a odpovídající sjednocení spravovaných účtů.		
Export údajů	Vestavěný export přehledů a seznamů zobrazených na portále do souborů CSV nebo obdobného strojově		

	zpracovatelného a současně běžně čitelného formátu		
Filtrování	Vestavěný editor filtrů pro vyhledávání identit a referenčních identit. Možnost filtrování libovolných atributů identity včetně přidružených referenčních objektů. Možnost uložení filtrů pro opakované použití.		
Správa oprávnění	Víceúrovňová správa administrátorských oprávnění s možností nastavení oprávnění min. na úrovni organizační jednotky (nebo hlouběji) a detailní přiřazení rolí a oprávnění (např. přiřazení činnostní role, přiřazení aplikační role, editace identity apod.)		
Editor oprávnění	Systém bude obsahovat editor oprávnění. V rámci editoru bude administrátor definovat oprávnění do Systému a následně tato oprávnění přiřazovat konkrétním uživatelům. Oprávnění bude definováno pro jednotlivé entity a moduly systému (identity, referenční objekty, konfigurace notifikací, konfigurace synchronizací, konfigurace systému, reporty, workflow, správa webových služeb IDM atd.) Dále bude oprávnění u entit (identit a referenčních objektů) definováno až na jejich konkrétní atributy včetně zobrazení / nezobrazení daného atributu, možnosti editace atributu uživatelem, povinnosti atributu, pořadí zobrazení atributů ve formuláři. U jednotlivých entit a modulů bude možnost definovat akce, které může uživatel s entitami a v rámci systému provádět.		

Kontextový výběr organizační jednotky	Na úrovní organizační jednotky bude možné pro výběr a přiřazování rolí nastavit sady povolených aplikační rolí, skupiny, systematizovaných míst dostupných pro identity z dané organizační jednotky.		
Správa licencí	Systém umožní spravovat licence pro jednotlivé evidované aplikace a přiřazovat je jednotlivým uživatelům (identitám). Pro schvalování přiřazování licencí bude IDM obsahovat workflow platformu s možností vytváření víceúrovňových schvalovacích workflow.		
Časová omezení	Systém bude umožňovat přiřazení rolí konkrétní identitě, systemizovanému místu, skupině a organizační jednotce včetně možnosti nastavení data a času vypršení platnosti přiřazení. Po vypršení platnosti přiřazení systém roli přiřazenému objektu automaticky odebere.		
Vícenásobné vazby	Možnost přiřazení identit k systematizovaným místům ve vazbě M:N. Identita může být v systému evidována na více systematizovaných místech a současně na systematizovaném místě může být evidováno více identit.		
Přehled rolí	Systém bude zajišťovat zobrazení přidělených rolí a jejich rozšiřujícím významům k jednotlivým identitám s rozdělením na role navázané na systemizované místo, role navázané na identitu, role navázané na organizační jednotku, role navázané na skupinu. U identity musí být evidován a v systému souhrnně zobrazen seznam všech rolí včetně informace o tom, odkud uživatel		

	roli zdědil nebo mu byla delegována (z organizační jednotky, systematizovaného místa, skupiny apod.).		
Skupiny	Systém bude obsahovat správu skupin s možností začleňovat více skupin do sebe, přiřazovat do skupin jednotlivé uživatele i systematizovaná místa.		
Zastupitelnost	Systém bude obsahovat správu vztahů zastupitelnosti mezi uživateli. Musí umožnit uživatelům, aby v souladu se strukturou organizace mohli uživatelé delegovat v případě potřeby (dovolená, služební cesta) svoje role, nebo jejich část na jiné pověřené osoby, a to i v režimu, kdy jeden uživatel může mít pro každou svou činnost nastaveného jiného uživatele jako zástupce.		
Delegování oprávnění	Možnost delegování administrátorských práv.		
Obnovení hesla	Systém bude obsahovat samoobslužné uživatelské rozhraní pro reset hesla jednotlivých účtů daného uživatele. Zasílání kódů pro reset hesla danému uživatele musí být možnou provádět pomocí SMS (tj. v systému musí být možné na SMS bránu či službu napojit). Rozhraní musí umožnit i běžnou změnu hesla (bez resetu).		
Žádosti	IDM bude obsahovat samoobslužné uživatelské rozhraní pro zadávání žádostí o přidělení jednotlivých 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.		

Kontextový výběr	Samoobslužné rozhraní umožní na úrovní organizace a organizační jednotky definovat seznam rolí a skupin, o které mohou žadatelé požádat.		
Individualizace	Systém umožní uživatelům individuálně nastavit vlastní zobrazení rozhraní - min. zobrazení / skrytí sloupců u všech seznamů, počet zobrazených záznamů na stránku – vždy pro každý seznam samostatně		
Workflow	Integrované workflow pro řízení životního cyklu změn identit a schvalování změn. Funkční požadavky: - Zadávání požadavků uživatelů na změny v přiřazení rolí a skupin ke schválení nadřízeným - Možnost sledování stavu svých požadavků uživateli - E-mailové upozornění schvalovatele na požadavek ke schválení - Přehled úloh ke schválení pro každého schvalovatele - Schvalování či zamítnutí požadavků včetně uvedení zdůvodnění - Podpora vícekrokového schvalování - Podpora schvalování jedním nebo více schvalovateli (skupinou schvalovatelů) - Správce IDM může pracovat se všemi úlohami - Možnost větvení pro ošetření výjimek vzniklých při schvalování - Řešení zastupitelnosti - Eskalace - upozornění při překročení termínu splnění - Možnost vkládání systémových kroků s voláním webových služeb a spuštěním skriptů		

Workflow – sledování	Workflow bude možné sledovat v grafické podobě ve formě diagramu. Diagram bude v obvyklém formátu pro zobrazení workflow např. aktivity diagram, BPMN nebo Archimate		
Recertifikační workflow	Recertifikační workflow pro kontrolu oprávnění v pravidelných intervalech a podporu Compliance.		
SoD	Hlídání přiřazení konfliktních rolí – ochrana systému v případě pokusu o přiřazení konfliktní role – pokud dojde k pokusu o přiřazení role identitě, která již má jinou konfliktní roli, musí systém konflikt oznámit a vlastní přiřazení neprovede.		
Upozornění	Systém zajistí zasílání konfigurovatelných emailových upozornění min. pro následující události: vytvoření a změna identity, referenčního objektu (systematizované místo, organizační jednotka, skupina, aplikace, skupina aplikací, aplikační role atd.), problém při synchronizaci, vypršení hesla v Active Directory, vypršení platnosti certifikátu. Mechanismus správy notifikací včetně náhledu na odeslané notifikace musí být spravován přímo v Portálu systému.		
Včasná upozornění	Portál bude obsahovat notifikační šablony a notifikace pro upozornění na vypršení hesla v Active Directory a vypršení platnosti certifikátů. Notifikaci lze nastavit na několik dní dopředu před vlastním vypršením hesla nebo certifikátu.		
Šablony upozornění	Šablony upozornění umožní definovat příjemce, předmět a obsah upozornění.		

	U upozornění vázaného k identitám musí být možné nastavovat různé příjemce pro různé části organizační struktury (např. odbor, oddělení) apod. Šablony musí umožnit vložit do obsahu upozornění libovolný atribut identity a/nebo referenčního objektu.		
Kontext upozornění	U notifikací ve vazbě na identity a referenční objekty musí být možné konfigurovat nastavení na úroveň jednotlivých atributů. V šabloně musí být možné vybrat libovolné atributy identity a referenčních objektů a následně je vložit a použít v definici textu pro emailové zprávy. Dále musí být možné u notifikací konfigurovat podmínky pro provedení notifikace na základě hodnot jednotlivých libovolných atributu identity a referenčních objektů. (například notifikace je generována pouze pro identitu v konkrétních uvedených skupinách, která má uvedenu konkrétní aplikační roli, systematizované místo atd.). V Portálu musí být možné notifikace aktivovat pro jednotlivé zdrojové systémy, které v IDM změnu identity nebo referenčního objektu provedly.		
Logování	Systém musí umožnit logování minimálně v tomto rozsahu: - události systému (aplikační log) - změny entit evidovaných systémem a změny konfigurace systému (auditní log) - synchronizace s napojenými systémy (synchronizační log) - odeslané notifikace a upozornění (notifikační log)		

Logování	Veškeré změny vyvolané požadavky uživatele a administrátorů/správců IDM budou provedeny transakčně. Budou logovány tak, aby bylo možné zpětně prokázat co, kdo a kdy měnil v identitách a referenčních objektech i v administraci a konfiguraci IDM. Záznam v logu bude obsahovat původní i novou hodnotu.		
Důvěryhodnost logování	Veškeré požadavky na změny v IDM bude možné zadávat výhradně prostřednictvím Portálu. Není přípustné realizovat požadavky ručními změnami textových soubory jako XML, CSV atd. z důvodu zajištění úplného logování všech změn jednotlivých konfigurovaných parametrů IDM.		
Trust domény	V systému IDM bude možné evidovat více domén s možností definice vztahu důvěry (nastavení trust) mezi jednotlivými doménami. Mezi doménami bude možné v systému IDM nastavit rozsah důvěry, zda je jednosměrná (kdo komu důvěřuje), případně obousměrná. Dle konfigurace důvěry mezi doménami umožní/neumožní systém vkládání objektů z jedné domény do druhé (uživatelé, skupiny) včetně odpovídající správy v napojených adresářových strukturách organizace.		
Auditní report	IDM umožní export auditního reportu z údajů o identitách uložených v IDM, a to i historických. Auditní reporty budou minimálně ve formátu XML nebo CSV a budou obsahovat souhrnné zobrazení daných uživatelů (identit) a jejich rolí v		

	IS napojených na IDM, přiřazených skupin ve vybraném časovém okamžiku od aktuálního času do minulosti.		
Auditní report – výběr	IDM bude obsahovat editor pro vyhledávání identit a referenčních objektů v systému IDM pro vytvoření reportu. Do filtru musí být možné zadat libovolné atributy identity, které jsou v systému IDM evidovány včetně přidružených referenčních objektů.		
Reporty uživatelů	Vestavěné reporty obsahující uživatele s přímo přiřazenými aplikačními rolemi a s aplikačními rolemi delegovanými od jiných uživatelů. Reporty budou exportovatelný do CSV souboru.		
Reporty – zasílání	IDM bude obsahovat možnost generovat do CSV souboru report uživatelů přiřazených aplikačním rolím a možnost nastavení pravidel pro automatického zasílání reportu emailem.		
Karta uživatele	IDM bude obsahovat report, který do formátu PDF vygeneruje kartu uživatele obsahující informace o uživateli včetně seznamu rolí, které uživatel má, skupin, certifikátů atd.		
Reporty – historie	Automatické ukládání vygenerovaných reportů s možností pozdějšího zobrazení či stažení.		
Reporty – porovnání	Snadné porovnání změn mezi vygenerovanými reporty stejného typu v prostředí Portálu.		
Dashboard	IDM bude obsahovat centrální dashboard, který bude obsahovat následující údaje: - Synchronizační úlohy v chybě - chyby běhu synchronizací		

	- chyby při generování a odesílání notifikací - chyby volaní metod rozhraní webových služeb IMD (např. pokus o přístup k metodě, na kterou nemám oprávnění) - chyby plánovaných úloh (agentů) - nově vytvořené poznámky - workflow v chybě - neúspěšné akce systému v systému IDM Záznamy v dashboard se budou načítat za počet dnů definovaných v konfiguraci IDM		
Webové služby (WS)	IDM bude poskytovat rozhraní webových služeb pro napojení dalších systémů s možností konfigurace v Portálu.		
Standardy WS	Webové služby IDM budou definované v rozšířeném standardu WSDL a podporovat protokol SOAP. V rámci povahy předávaných identitních údajů (včetně osobních údajů) je požadováno zajistit maximální zabezpečení a zajištění spolehlivosti volání webových služeb minimálně v rozsahu specifikací WS–Security, WS-SecurityPolicy, WS-ReliableMessaging, WS-AtomicTransactions.		
Bezpečnost WS	Konfigurace webových služeb umožní konfigurovat přístup pro volání jednotlivých vybraných služeb pro každý odpovídající systémový účet samostatně.		
Logování WS	Volání webových služeb bude logováno na úrovni databáze a bude možné je zobrazit v prostředí Portálu		

Služby rozhraní WS	Rozhraní bude poskytovat minimálně následující služby: - Načtení organizační struktury - Načtení hierarchie systematizovaných míst - Načtení seznamu identit - Načtení nadřízené osoby pro daného zaměstnance - Načtené seznamu aplikační rolí - Načtení seznamu uživatelů dané aplikace - Zápis seznamu aplikačních rolí do IDM - Zápis certifikátů do IDM - Zápis a změna uživatelů a osob - Zabezpečená služba pro přihlášení aplikace k IDM - Zabezpečená služba pro přihlášení uživatele k IDM - Přidání a odebrání uživatele do/ze skupiny - Přidání a odebrání aplikační role a jejího rozšiřujícího významu na/z uživatele, organizační jednotku, systematizované místo nebo skupinu - Přidání a odebrání agendové role na uživatele nebo systematizované místo - Vyvolání synchronizace konkrétní identity s daným systémem napojeným na IDM		
Synchronizace	Ruční i automatické spuštění synchronizací s propojenými systémy.		
Synchronizace – simulace	Spuštění synchronizací i v simulačním režimu pro ověření dopadu reálného spuštění bez ovlivnění produkčních dat a napojených systémů. Simulační logy budou zobrazitelné v Portálu.		
Simulace – průběh	Zobrazení jednotlivých stavů průběhu synchronizace bude k dispozici v přehledné grafické podobě.		

Synchronizace – režimy	Pro napojení na jednotlivé systémy a implementaci jejich synchronizací s IDM umožní IDM u každého systému využít více režimů synchronizací (za předpokladu podpory napojovaného systému): - Plná synchronizace – prochází všechny objekty v IDM a synchronizuje je s objekty daného systému - Změnová synchronizace – synchronizuje vždy jen změny od poslední spuštěné synchronizace. Umožní dále spouště změnové synchronizace pro změny vybraného vstupního systému a automatické spouštění navázané synchronizace. - Okamžitá synchronizace konkrétní identity na vyžádání – synchronizuje okamžitě pouze vybranou identitu. Může se jednat o synchronizaci jednoho objektu ze zdrojového i cílového systému - Rekonciliační synchronizace – synchronizace vytvoří rekonciliační report pro porovnání změn mezi nastavením identit a jejich oprávnění pro daný systém v IDM vs. nastavení identit a oprávnění přímo v připojeném systému. - Simulační synchronizace – synchronizace vytvoří report očekávaných změn v napojeném systému pro provedení ostré synchronizace. Report změn bude evidován jako pohled nebo přehledná souhrnná tabulka. - Historie běhu synchronizací – jednotlivé běhy synchronizací budou zaznamenány v databázi a dostupné		

	v Portálu. Historie plné synchronizace bude obsahovat odkazy na objekty, které byly synchronizovány a log, co bylo u těchto objektů změněno v synchronizovaném systému. V případě změnové synchronizace pak bude v historii dále informace o události, která změnovou synchronizaci vyvolala.		
Synchronizace – správa	Vestavěná správa jednotlivých synchronizací včetně nastavení připojení na synchronizované systémy, nastavení plné a změnové synchronizace, počet změn, které je možné zpracovat, závislostí mezi synchronizacemi, nastavení časového intervalu spouštění, nastavení intervalu odstávky. U jednotlivých synchronizací je rovněž požadováno, aby bylo možné vybírat organizace, které se mají z IDM synchronizovat s danými systémy. Správa bude součástí Portálu.		
Synchronizace -sekvence	Pro napojení na jednotlivé systémy a implementaci jejich synchronizací s IDM umožní IDM sekvenční spouštění synchronizací (za předpokladu podpory napojovaných systémů) a to tak, aby jednotlivé synchronizace mohli být spouštěny po sobě v sekvencích. Navazující synchronizované systémy v sekvenci bude možné definovat dle požadavků a spouštět nebo zastavovat automaticky i ručně.		
Agenti	Pro plánované úlohy umožní IDM definici agentů a jejich plánovaných spouštění na základě akcí a triggerů v systému. Spouštění je možné definovat i pro požadované intervaly,		

	definovat omezení a další. Agenty bude možné importovat do systému IDM minimálně ve formátu JSON.		
Agenti – simulace	Systém IDM umožní spouštění agentů také v režimu simulace.		
Správa SW aktiv	V rámci systému bude možné spravovat evidenci aktiv s klasifikací dle zákona o kybernetické bezpečnosti. V systému bude možné spravovat evidenci primárních, podpůrných a technických aktiv. Technická aktiva budou dále rozdělena na datová, softwarová, hardwarová aktiva, informační služby. Jednotlivá aktiva je možné členit do hierarchie aktiv.		
Rozsah aktiv	Minimální rozsah evidovaných dat: Základní údaje: • ID Aktiva – identifikátor • Název aktiva – označení aktiva • Popis aktiva – popis aktiva • Typ aktiva – typ aktiva • Kategorizace aktiva – kategorizace aktiva • Organizace – označení organizace daného aktiva • Stav aktiva – stav daného aktiva • Kód ISVS – číselný kód přidělený informačnímu systému veřejné správy • Datum identifikace aktiva • Lokalizace aktiva • Vazby na jiná aktiva Analýza rizik • Požadavky na dostupnost aktiva • Požadavky na důvěrnost aktiva • Požadavky na integritu aktiva		

	• Celkové hodnocení aktiva – číselné hodnocení aktiva • Popis zabezpečení aktiva – popis způsobu zabezpečení aktiva • Frekvence přístupu – hodnota frekvence použití aktiva • Nedostupnost – popis hodnocení maximální doby nedostupnosti a definice náhradních postupů v případě nedostupnosti Ochrana v rámci zpracování osobních údajů: • Klasifikace – klasifikace osobních údajů • Zdroj dat – popis získání osobních údajů • Aktualizace – popis způsobu aktualizace osobních údajů • Skartace – popis skartace dat • Zpracování – popis způsobu zpracování osobních údajů • Registrace – popis registrace zpracování osobních údajů na Úřad pro ochranu osobních údajů • Kategorie – kategorie osobních údajů • Účel zpracování – účel zpracování osobních údajů • Zpracovatel – informace o zpracovateli osobních údajů • Příjemce – informaci o příjemci osobních údajů v případě, že jsou předávány		

	• Legislativa – popis legislativy vztahující se k danému aktivu. Garanti aktiv: • Vlastník – vlastník aktiva • Správce aktiva – správce aktiva (například dané aplikace) • Zástupce – zástupce správce aktiva • Uživatelé – seznam uživatelů daného aktiva. Uživatele bude možné slučovat do rolí a skupin Technické údaje (týkající se technických aktiv): • Technické prostředky (servery, databáze) – odkaz na technické prostředky, pro provoz a aktiva Zálohování – popis způsobu a frekvence zálohování		
Správa osob	Systém obsahovat správu osob, organizační strukturu, rolí. Tuto evidenci bude možné synchronizovat s personálním systémem a navázat na správu aktiv.		
Tiskové výstupy	Systém bude obsahovat funkcionalitu pro generování následujících reportů: - Přehled aktiv s možností filtrování a třídění podle všech dostupných polí - Karta aktiva se všemi navázanými údaji - Zobrazení vazeb mezi aktivy - Možnost definice vlastních sestav - Přehled žádostí o přidělení aktiva aktivních a dokončených		

	Přehled oprávnění a přístupů k danému aktivu		
Schvalovací workflow	Systém bude obsahovat implementaci následujících workflow: - Žádost o přístup k aktivu směrovaná na seznam Garantů jako schvalovatele žádosti - Periodická revize aktiv jednotlivými garanty - Periodická revize stavu evidence garantem z oblasti řízení bezpečnosti Funkční požadavky na workflow: - Zadávání požadavků uživatelů na změny v evidenci - Možnost sledování stavu svých požadavků uživateli - E-mailové upozornění schvalovatele na požadavek ke schválení - Přehled úloh ke schválení pro každého schvalovatele - Schvalování či zamítnutí požadavků včetně uvedení zdůvodnění - Podpora vícekrokového schvalování - Podpora schvalování jedním nebo více schvalovateli (skupinou schvalovatelů) - Možnost větvení pro ošetření výjimek vzniklých při schvalování - Řešení zastupitelnosti - Eskalace - upozornění při překročení termínu splnění - Možnost vkládání systémových kroků s voláním webových služeb a spuštěním skriptů Průběh workflow bude možné sledovat v grafické podobě ve formě diagramu, ve kterém bude zřejmý stav probíhajícího workflow. Diagram bude v obvyklém formátu pro zobrazení		

	workflow např. aktivity diagram, BPMN nebo Archimate		
Rozšiřující atributy	Systém umožní dodatečné konfigurační rozšiřování evidence o další atributy		
Aktivní uživatelé	Systém bude obsahovat přehled uživatelů aktuálně pracujících s Portálem		
Správa oprávnění k aktivům	Systém bude obsahovat editor oprávnění. V rámci editoru bude administrátor definovat oprávnění do systému a následně tato oprávnění přiřazovat konkrétním uživatelům. Oprávnění bude definováno pro jednotlivé části systému (aktiva, uživatelé aktiva, konfigurace notifikací, konfigurace systému, reporty, workflow, správa rozhraní atd.) Oprávnění bude definováno až na konkrétní atributy včetně zobrazení / nezobrazení daného atributu, možnosti editace atributu uživatelem, povinnosti atributu, pořadí zobrazení atributů ve formuláři. U jednotlivých entit a modulů bude možnost definovat akce, které může uživatel s entitami a v rámci systému provádět.		
Synchronizace software aktiv	Systém poskytne rozhraní pro pravidelnou synchronizaci softwarových aktiv a jim přidělených uživatelům.		
Obecné konektory	Vestavěné obecné skriptovatelné (javascript, groovy) konektory pro správu identit v napojených systémech: - konektor pro spouštění CMD a powershell příkazů, SSH - konektor pro práci s CSV soubory - konektor pro práci s databází Microsoft SQL, Oracle - konektor pro napojení na SOAP		

	webové služby - konektor pro napojení na REST webové služby U jednotlivých konektorů je možné dynamicky měnit transformační logiku pro nutnou komunikaci s danými typy rozhraní.		
Scan zranitelností	Dodavatel IDM dodá scan zranitelností systému IDM, který nebude starší než 4 měsíce a výstupem scanu zranitelností použitých knihoven v systému IDM nebude žádná zranitelnost na úrovni kritická a na úrovni vysoká nebude žádná zneužitelná vulnerabilita.		
Zdrojový systém	IDM bude napojeno na personální systém FLUX. Z personálního systému budou načítány údaje o organizační struktuře, hierarchii pracovních míst, osobách a tyto údaje budou pro IDM sloužit jako zdrojové		
Konektor na Active Directory	IDM musí obsahovat konektor umožňující napojení na Microsoft Active Directory s následující funkcionalitou: • komplexní správu účtů, kontaktů, certifikátů a skupin (založení, změnu atributů, zrušení, změnu hesla atd.) • založení domovského adresáře včetně nastavení oprávněná • správu účtů a jejich certifikátů včetně inicializačního načtení z AD • správu skupin a členství ve skupinách včetně inicializačního načtení z AD		

	• správu organizačních jednotek včetně inicializačního načtení z AD		
Konektor na Office365	IDM musí obsahovat konektor umožňující napojení na Office365 s následující funkcionalitou: • inicializační načtení dat • správa lokálních identit • správa oprávnění pro jednotlivé uživatele ve formě přiřazení skupin nebo rolí		
Konektor na GINIS	IDM musí obsahovat konektor umožňující napojení na Ginis s následující funkcionalitou: • inicializační načtení dat • správa lokálních identit • správa oprávnění pro jednotlivé uživatele ve formě přiřazení skupin nebo rolí		
Konektor na VITA	IDM musí obsahovat konektor umožňující napojení na VITA s následující funkcionalitou: • inicializační načtení dat • správa lokálních identit • správa oprávnění pro jednotlivé uživatele ve formě přiřazení skupin nebo rolí		
Konektor na YAMACO	IDM musí obsahovat konektor umožňující napojení na YAMACO s následující funkcionalitou:		

	• inicializační načtení dat • správa lokálních identit • správa oprávnění pro jednotlivé uživatele ve formě přiřazení skupin nebo rolí		
Konektor na ADVENT	IDM musí obsahovat konektor umožňující napojení na ADVENT s následující funkcionalitou: • inicializační načtení dat • správa lokálních identit • správa oprávnění pro jednotlivé uživatele ve formě přiřazení skupin nebo rolí		
Konektor na JIP a RPP	IDM musí obsahovat konektor umožňující napojení na JIP a RPP s následující funkcionalitou: • inicializační načtení dat • správa lokálních identit • správa oprávnění pro jednotlivé uživatele ve formě přiřazení skupin nebo rolí		
Konektor na ALVAO	IDM musí obsahovat konektor umožňující napojení na JIP a RPP s následující funkcionalitou: • inicializační načtení dat • správa lokálních identit • správa oprávnění pro jednotlivé uživatele ve formě přiřazení skupin nebo rolí		

Konektor na PostSignum	IDM musí obsahovat konektor umožňující napojení na certifikační autoritu PostSignum.		
Externí IDM	IDM bude obsahovat samostatnou část Portál pro správu externích uživatelů. Tato externí část IDM bude obsahovat konektor/rozhraní pro správu identit ze strany externích organizací.		

Identity management systém – Zadavatel si vyhrazuje právo k ověření funkčnosti v rámci zadávacího řízení dle níže uvedeného postupu

Místem testování funkčnosti nabízeného vzorku je místo zadavatele. Zadavatel v rámci posouzení nabídek může ověřit, zda funkčnost nabízeného řešení ze strany uchazeče splňuje základní požadované parametry uvedené v kapitolách níže na uchazečem zvoleném prostředí. Pro demonstraci funkčnosti bude možné přistoupit vzdáleně. Zadavatel umožní v rámci testu využití své infrastruktury pro přístup do Internetu a prostory pro přípravu testu ověření funkčnosti.

V případě, že nebude uchazeč scénáře uvedené níže úspěšně demonstrovat, bude jeho nabídka vyloučena.

Ověření funkčnosti scénářů z oblasti řízení uživatelů dle níže uvedených požadavků

- Správa uživatele
    - Založení uživatele v IDM
    - Změny na uživateli evidovaném v IDM
    - Zneplatnění uživatele v IDM
    - Zobrazení stavu uživatele z IDM včetně zobrazení jeho aplikačních rolí

Očekávaný výsledek: Ověření, že v portálu IDM byly provedeny scénáře a že uživatel byl založen, změněn, zneplatněn, zobrazen požadovaným způsobem.

- Správa dalších objektů
    - Založení samostatně identifikovatelných objektů v IDM – systematizované místo, organizační jednotka, skupina, aplikace, skupina aplikací, aplikační role
    - Změny na samostatně identifikovatelných objektech v IDM – systematizované místo, organizační jednotka, skupina, aplikace, skupina aplikací, aplikační role

- Deaktivace samostatně identifikovatelných objektů v IDM – systematizované místo, organizační jednotka, skupina, aplikace, skupina aplikací, aplikační role

Očekávaný výsledek: Ověření, že v Portálu IDM byly provedeny scénáře a že požadovaný objekt byl založen, změněn, zneplatněn, zobrazen požadovaným způsobem.

- Správa rolí
  - V rámci dané role bude možné definovat další členění různých významů role. Například „roli editor“ webu bude možné rozšířit o významy odpovídající jednotlivým oddělením, pro které jsou části webu určené. Tyto rozšiřující významy rolí bude možné přímo přiřazovat systematizovaným místům, skupinám, organizačním jednotkám, uživatelům spravovaných v systému IDM.

Očekávaný výsledek: Ověření, že v Portálu IDM bylo správcem definováno další členění významů role a tyto významy rolí je možné přiřadit jednotlivým organizačním jednotkám, skupinám, systematizovaným místům, uživatelům.

  - Systém IDM umožní delegaci aplikačních rolí. Při delegaci jsou aplikační role předány na nového uživatele s možností nastavení platnosti, do kdy je delegace platná. Následně jsou role odebraný delegovanému.

Očekávaný výsledek: Ověření, že v Portálu IDM je možné provést scénáře delegace výše včetně ověření automatické vypršení a zrušení přiřazení delegovaných rolí delegovanému uživateli.

- Správa pravidel
  - Ověření konfigurace pravidel a ověření funkčnosti pravidel pro automatické začleňování uživatelů do skupin na základě libovolného atributu identity. Ověření nastavení podmínky pro libovolný atribut identity a jeho libovolné hodnoty. Při splnění této podmínky ověření, že IDM automaticky začlení vyhovující identity do patřičných skupin. Ověření, že je možné v těchto podmínkách kombinovat více atributů najednou a více hodnot atributů. Provádění vyhodnocení pravidel bude mít stejné vlastnosti jako jiné synchronizační procesy IDM. Ruční vs. plánované spuštění, historii běhů, simulační režim atd.

Očekávaný výsledek: Ověření, že v Portálu IDM byly provedeny vybrané scénáře pro konfiguraci pravidel (výběr libovolných atributů, libovolných hodnot, kombinace, správa synchronizační úlohy). Dále ověření, že nastavená pravidla skutečně provedla začlenění uživatelů do skupin.

- Nastavení oprávnění
  - Ověření možnosti definovat oprávnění uživatelů portálu IDM samostatně pro jednotlivé entity a moduly systému (identity, referenční objekty, modul konfigurace notifikací, modul konfigurace synchronizací, modul konfigurace systému IDM, modul reportů, modul workflow, modul správy

webových služeb IDM). Ověření, že bude oprávnění u entit (identit a referenčních objektů) definováno až na jejich konkrétní atributy včetně zobrazení / nezobrazení daného atributu, možnosti editace atributu uživatelem, povinnosti atributu, pořadí zobrazení atributů ve formuláři portálu IDM.

Očekávaný výsledek: Ověření, že Portál IDM podporuje model oprávnění popsaný výše. Budou předvedeny scénáře přiřazení jednotlivých oprávnění pro vybrané uživatele. Pod těmito uživateli bude provedena autentizace a autorizace do portálu IDM a provedena kontrola, že mají přístup na vybrané moduly, entity, atributy a povolené akce pro operaci s těmito objekty dle přiřazeného oprávnění v portálu IDM.

- Notifikace
    - Ověření možnosti u šablon notifikací ve vazbě na identity a referenční objekty v Portálu IDM konfigurovat nastavení na úroveň jednotlivých atributů. Ověření, že je v šabloně notifikací možné vybrat libovolné atributy identity a referenčních objektů a následně ověření jejich vložení a použití v definici textu pro emailové zprávy. Ověření u těchto notifikací konfigurovat podmínky pro akci provedení notifikace na základě hodnot jednotlivých libovolných atributu identity a referenčních objektů. (například notifikace budou generovány pouze pro identity v konkrétní uvedených skupinách, které mají uvedenu konkrétní aplikační role, systematizované místo atd.)

Očekávaný výsledek: Ověření, že Portál IDM umožňuje správu notifikačních šablon dle popisu výše. Součástí ověření bude vytvoření několika šablon notifikací a následná kontrola vygenerovaných a odeslaných emailových zpráv.

- Workflow
    - Ověření workflow dle scénářů v portálu IDM:
        - Vložit pro nadřízené pracovníky požadavky na změny v přiřazení rolí, skupin pro podřízené pracovníky a sledovat stav vyřizování jejich žádostí.
        - Schválení či zamítnutí požadavků.
        - Odeslání schvalovateli upozornění ve formě emailové notifikace
        - Schvalovatelé si budou moct zobrazit přehled úloh ke schválení
        - Požadavky je možné schválit či zamítnout včetně uvedení zdůvodnění
        - Workflow podporuje vícekrokové schvalování
        - Schvalovat bude moct skupina schvalovatelů
        - Správce IDM je schopen pracovat se všemi úlohami
        - Workflow bude možné sledovat v grafické podobě ve formě diagramu. Diagram bude v obvyklém formátu pro zobrazení workflow např. aktivity diagram, BPMN nebo Archimate

Očekávaný výsledek: Ověření, že Portál IDM umožňuje scénáře pro práci s workflow dle popisu výše. Součástí ověření bude vytvoření několika workflow v portálu IDM

- Workflow
    - V rámci systému bude možné spravovat evidenci aktiv

Očekávaný výsledek: Ověření scénáře, kdy bude v Portálu možné vytvořit, změnit a deaktivovat dané aktivum.

- Systém bude obsahovat implementaci workflow: Žádost o přístup k aktivu směrovaná na seznam Garantů jako schvalovatele žádosti:
    - Zadávání požadavků uživatelů na změny v evidenci
    - Schválení či zamítnutí požadavků.
    - Odeslání schvalovateli upozornění ve formě emailové notifikace
    - Schvalovatelé si budou moct zobrazit přehled úloh ke schválení
    - Požadavky je možné schválit či zamítnout včetně uvedení zdůvodnění
    - Workflow podporuje vícekrokové schvalování
    - Schvalovat bude moct skupina schvalovatelů
    - Správce je schopen pracovat se všemi úlohami
    - Průběh workflow bude možné sledovat v grafické podobě ve formě diagramu, ve kterém bude zřejmý stav probíhajícího workflow. Diagram bude v obvyklém formátu pro zobrazení workflow např. aktivity diagram, BPMN nebo Archimate

Očekávaný výsledek: Ověření, že Portál umožňuje scénáře pro práci s workflow dle popisu výše. Součástí ověření bude vytvoření několika workflow v Portálu IDM.

- Reporty
    - Ověření exportu auditního reportu na portálu IDM z údajů o identitě uložené v IDM, a to i historické. Auditní reporty budou minimálně ve formátu XML a budou obsahovat souhrnné zobrazení daného uživatele a jeho aplikačních rolí, přiřazených skupin ve vybraném časovém okamžiku od aktuálního časového okamžiku do minulosti.

Očekávaný výsledek: Vytvoření reportů v portálu IDM na vybrané skupině uživatelů dle specifikace výše. Pokud bude vytvořen report pro aktuální čas, tak budou hodnoty zobrazovat aktuálně platná data. Pokud bude report vytvořen zpětně k nějakému datu v minulosti, tak bude obsahovat data aktuální v daném okamžiku v minulosti.

- Audit
    - Ověření, že veškeré požadavky změn, které provedou uživatelé na Portálu IDM budou provedeny transakčně. Budou historizovány a logovány tak, aby bylo možné zpětně prokázat kdo, kdy a co změnil v IDM identitách, referenčních objektech, ale i v administraci a konfiguraci IDM. Záznam v historii bude obsahovat původní i novou hodnotu.

Očekávaný výsledek: Veškeré scénáře, které byly provedeny v předchozích bodech, budou v portálu IDM zaevidovány v auditnímu logu dle specifikace výše.

- Dashboard
    - IDM bude obsahovat uživatelské rozhraní nebo uživatelská rozhraní, ze kterých budou dostupné následující údaje:
        - Synchronizační úlohy v chybě
        - chyby běhu synchronizací
        - chyby při generování a odesílání notifikací
        - chyby volaní metod rozhraní webových služeb IMD(např. pokus o přístup k metodě, na kterou nemám oprávnění)
        - chyby plánovaných úloh (agentů)
        - nově vytvořené poznámky
        - workflow v chybě
        - neúspěšné akce systému v systému IDM
        - Záznamy v uživatelském rozhraní nebo rozhraních se budou načítat za počet dnů definovaných v konfiguraci IDM

Očekávaný výsledek: Zobrazení uživatelského rozhraní v systému IDM v členění pro jednotlivé typy událostí viz výše. Zobrazení údajů k jednotlivým typům událostí.

Ověření funkčnosti scénářů z oblasti řízení uživatelů – integrace na systémy

Napojení IDM na XML soubor

- Synchronizace hierarchie organizační struktury do IDM

Očekávaný výsledek: Ověření, že ze souboru XML byly do IDM přenesena strukturovaná data o hierarchii organizační struktury včetně relevantních atributů

- Synchronizace hierarchie pracovních pozic do IDM

Očekávaný výsledek: Ověření, že ze souboru XML byly do IDM přenesena strukturovaná data o hierarchii pracovních pozic včetně relevantních atributů

- Synchronizace osob do IDM

Očekávaný výsledek: Ověření, že ze souboru XML byly do IDM přeneseny osoby včetně relevantních atributů

- Simulační režim synchronizace

Očekávaný výsledek: Ověření, že synchronizace umožňuje simulační režim pro organizační strukturu, pracovní pozice, osoby. Ověření, že synchronizace vytvoří report očekávaných změn v portálu IDM pro provedení ostré synchronizace. Report změn bude evidován jako pohled nebo přehledná souhrnná tabulka přímo v portálu IDM.

Napojení IDM na AD

- Synchronizace skupin z AD do IDM

Očekávaný výsledek: Ověření, že skupiny jsou přeneseny z AD do IDM a jsou v IDM zaevidovány.

- Synchronizace identity z IDM do AD

Očekávaný výsledek: Ověření, že identita byla z IDM přenesena do AD včetně relevantních atributů

- Synchronizace skupiny z IDM do AD

Očekávaný výsledek: Ověření, že skupina byla z IDM přenesena do AD včetně relevantních atributů

- Synchronizace organizační jednotky z IDM do AD

Očekávaný výsledek: Ověření, že organizační jednotka byla z IDM přenesena do AD včetně relevantních atributů

- Simulační režim synchronizace

Očekávaný výsledek: Ověření synchronizace umožňuje simulační režim pro uživatele, skupiny, organizační jednotky. Ověření, že synchronizace vytvoří report očekávaných změn v napojeném systému pro provedení ostré synchronizace. Report změn bude evidován jako pohled nebo přehledná souhrnná tabulka přímo v Portálu IDM.

Napojení IDM na Ginis

- Synchronizace konfiguračních skupin z Ginis do IDM

Očekávaný výsledek: Ověření, že skupiny jsou přeneseny z Ginis do IDM a jsou v IDM zaevidovány.

- Synchronizace identity z IDM do Ginis

Očekávaný výsledek: Ověření, že identita byla z IDM přenesena do Ginis včetně relevantních atributů

- Synchronizace funkčního místa z IDM do Ginis

Očekávaný výsledek: Ověření, že funkční místo bylo z IDM přeneseno do Ginis včetně relevantních atributů a vazby na konfigurační skupinu.

- Synchronizace organizační jednotky z IDM do Ginis

Očekávaný výsledek: Ověření, že organizační jednotka byla z IDM přenesena do Ginis včetně relevantních atributů a vazby na konfigurační skupinu.

- Simulační režim synchronizace

Očekávaný výsledek: Ověření synchronizace umožňuje simulační režim pro uživatele, funkční místa, konfigurační skupiny, organizační jednotky. Ověření, že synchronizace vytvoří report očekávaných změn v napojeném systému pro provedení ostré synchronizace. Report změn bude evidován jako pohled nebo přehledná souhrnná tabulka přímo v Portálu IDM.

Synchronizace

- U předchozího testování napojení IDM na AD budou prověřeny následující možnosti synchronizací:
    - Plná synchronizace – prochází všechny objekty v IDM a synchronizuje je s objekty daného systému

Očekávaný výsledek: synchronizace zpracuje všechny relevantní objekty v IDM a provede synchronizaci do cílového systému.

    - Změnová synchronizace – synchronizuje vždy jen změny od poslední spuštěné synchronizace.

Očekávaný výsledek: synchronizace zpracuje všechny relevantní změny v IDM a provede synchronizaci do cílového systému.

    - Okamžitá synchronizace konkrétní identity na vyžádání – synchronizuje okamžitě pouze vybranou identitu.

Očekávaný výsledek: synchronizace zpracuje konkrétní identitu v IDM a provede synchronizaci do cílového systému.

    - Systém bude obsahovat mechanismus zabránění hromadným změnám z důvodu případných chybných vstupních dat (např. z personálního systému), aby nedošlo k hromadným nežádoucím změnám (například smazání objektů v Active Directory apod).

Očekávaný výsledek: synchronizace se zastaví, pokud bude dosaženo povoleného limitu počtu změn.

- Historie běhu synchronizací

Očekávaný výsledek: synchronizace zpracuje historii běhu v IDM a provede synchronizaci do cílového systému. Jednotlivé běhy synchronizací budou zaznamenány v historii dostupné v Portálu IDM. Historie v případě plné synchronizace bude obsahovat odkazy na objekty v IDM, které byly synchronizovány a log, co bylo u těchto objektů změněno v synchronizovaném systému. V případě změnové synchronizace pak bude v historii na Portálu IDM navíc informace o události, která změnovou synchronizaci vyvolala.

Webové služby IDM

- Konfigurace služeb
  - Konfigurace webových služeb v Portálu IDM bude možné nastavovat přístup pro volání jednotlivých vybraných služeb pro každý odpovídající systémový účet připojené aplikace zvlášť.

Očekávaný výsledek: Provedení konfigurace v portálu IDM povolených metod rozhraní webových služeb pro vybraný systém a jeho systémový účet. Prověření, že pro daný systém jsou funkční pouze vybrané metody.

- Získání organizační struktury

Očekávaný výsledek: Zobrazení údajů organizační struktury, evidované v IDM

- Získání hierarchie systematizovaných míst

Očekávaný výsledek: Zobrazení údajů hierarchie systemizovaných míst evidované v IDM

- Získání seznamu identit

Očekávaný výsledek: Zobrazení údajů seznamu identit evidovaných v IDM

- Získání seznamu aplikační rolí

Očekávaný výsledek: Zobrazení údajů seznamu aplikačních rolí evidovaných v IDM

- Získání seznamu uživatelů dané aplikace

Očekávaný výsledek: Zobrazení údajů

- Zápis seznamu aplikačních rolí do IDM

Očekávaný výsledek: Ověření, že byl do IDM přenesen seznam aplikačních rolí a tento seznam zde byl zaevidován.

- Zápis certifikátů do IDM

Očekávaný výsledek: Ověření, že byl do IDM přenesen seznam certifikátů a tento seznam zde byl zaevidován.

- Zápis uživatele

Očekávaný výsledek: Ověření, že byl v IDM vytvořen uživatel.

- Přidání a odebrání uživatele do/ze skupiny

Očekávaný výsledek: Ověření, že byl uživatel přidán a následně odebrán ze skupiny

- Přidání a odebrání aplikační role a jejího rozšiřujícího významu na/z uživatele, organizační jednotku, systematizované místo nebo skupinu

Očekávaný výsledek: Ověření, že rozšiřující význam aplikační role přidán a následně odebrán z uživatele, organizační jednotky, systematizovaného místa, skupiny.

- Audit služeb
    - Volání webových služeb bude logováno a zobrazeno přímo v Portálu IDM.

Očekávaný výsledek: V rámci provedených scénářů volání webových služeb výše. Bude v portálu IDM zobrazen strukturovaný auditní log volání jednotlivých metod.

Společné požadavky

Požadavek
Uchazeč bere na vědomí, že součástí akceptace plnění jsou výsledky auditu, který bude prověřovat, zda jím implementovaná bezpečnostní opatření jsou funkční. Uchazeč pak poskytne součinnost nebo napraví nalezené chyby vysoké závažnosti v implementaci technických opatření.
Součástí je zajištění instalace a konfigurace veškerých komponent v návaznosti na stávající infrastrukturu úřadu (tj. včetně dopravy, montáže, instalace a implementace do stávající IT infrastruktury) v sídle zadavatele.
Součástí instalace musí být i zaškolení IT administrátorů minimálně v rozsahu nutném pro samostatnou administraci všech komponent zakázky. Administrací se rozumí zejména: konfigurace, monitoring činnosti, aktualizace, řešení problémů, zálohování konfigurace.
Zákaznická dokumentace bude zahrnovat: • popis všech prvků/zařízení, • popis způsobu zálohy a obnovy konfigurace všech prvků/zařízení • veškeré požadavky na zachování záruky/podpory (např. environmentální, kompatibilita, ...) • informaci o způsobu řešení servisních požadavků
Dodavatel do své nabídky zahrne veškerý instalační materiál a kabeláž nutnou k plnohodnotnému zprovoznění dodané technologie jako logického a funkčního celku.
Dodavatel zajistí instalaci a konfiguraci dodaných HW a SW komponent v návaznosti na stávající infrastrukturu organizace, a to včetně instalace a implementace do stávající IT infrastruktury v sídle zadavatele: • instalace zařízení do standardní RACK skříně 19“ • implementace Best Practice scénářů pro dané konfigurace • kontroly kompatibility verzí ovladačů a firmware jednotlivých zařízení a jejich aktualizace • registrace záruk u výrobců • umístění do racku a zapojení kabeláže vč. jejího označení, • inicializace a konfigurace všech dodaných zařízení • nastavení IP adres • nastavení vysoké dostupnosti • konfiguraci datových prostor polí, integrace s hypervizorem, nastavení případného dohledu a instalace SW pro monitoring výkonu • zapojení do stávající LAN • Instalace všech částí dodávky s ohledem na povahu dodávky a best practices daných technologií.

STANOVENÍ nabídkové CENY

Nabídková CENA
Nabídková cena je stanovena dohodou smluvních stran ve smyslu § 2 zákona č. 526/1990 Sb., o cenách, a vychází z cenové nabídky dodavatele v rámci zadávacího řízení. Celková cena se bude skládat z • Celková projektová cena se zárukou 5let • Maintenance po dobu 5let • Servisní práce (ZSP + RSP) Cena je stanovena jako cena jednotková – jednak jako jednotná hodinová sazba za služby **ZSP** (základní servisní podporu) i **RSP** (rozšířenou servisní podporu), a jednak jako cena roční za prodlouženou záruku.

	Sazba v Kč za ZSP/RSP	**MAINTENENCE v Kč**	**Celková nabídková cena v Kč bez DPH Dodávka KYBERNETICKÉ BEZPEČNOSTI se zárukou 5let + SLA služby (ZSP + RSP) + MAINTENENCE/5let**
cena bez DPH	**xxxx / 1 h**	**xxxx / 1 rok**	**xxxxxxxxxx / 5 let**
DPH v %	xxxx / 1 h	xxxx / 1 rok	*Cena za SLA pro účely hodnocení, vychází z:* - *Paušálu spotřeby **6 h ZSP/měs**. x 60 měs.* - *Odhadu nutnosti **4 h RSP/měs**. x 60 měs.* - *Maintenance nutná pro funkční stav SW/**5let***
cena vč. DPH	xxxx / 1 h	xxxx / 1 rok	

***částka musí korespondovat s celkovou částkou v nacenění VV**

Nabídková CENA – další ujednání
1. Hodinová sazba (za jednu člověkohodinu služeb ZSP i RSP jednotně) je dohodnuta jako cena nepřekročitelná a platná po celou dobu trvání smlouvy, která lze změnit pouze v případě změny zákonné úpravy DPH, přičemž v takovém případě bude dodavatel povinen k ceně bez DPH účtovat DPH v platné výši. Smluvní strany se dohodly, že v případě změny ceny v důsledku změny sazby DPH není nutno ke smlouvě uzavírat dodatek. 2. Roční cena za prodlouženou záruku vychází z položkového rozpočtu, jakožto dodavatelem oceněné podoby soupisu prvků KB, který byl součástí specifikace Zakázky (standardní 3 roky v rámci KS s „přikoupením“ dalších 2 let touto smlouvou do konce doby udržitelnosti projektu), tj. mimo tradiční náplň SLA služeb.

1. Jednotková cena (u roční záruky i hodinové sazby) vždy zahrnuje veškeré náklady dodavatele na kvalitní poskytování služeb, zejména veškeré náklady spojené s úplným a kvalitním provedením a dokončením činností v rámci paušálu měsíční údržby v rámci ZSP i plnění příkazů objednatele v rámci RSP, veškeré případné náklady na dopravu a/nebo související dodávky a veškeré provozní náklady, včetně nákladů souvisejících s provedením všech zkoušek a testů prokazujících dodržení požadované kvality, parametrů a funkčních požadavků specifikovaných touto smlouvou či příkazy objednatele, a ve vztahu k plnění prodloužené záruky i těch daných základními požadavky KS na Prvky KB. Cena dále zahrnuje náklady na autorská práva, pojištění, daně, projednávání připomínek ke kvalitě výstupů, či jakékoliv administrativní výdaje spojené s plněním povinností dle smlouvy.

2. Jednotková cena zahrnuje či zohledňuje i veškerý kalkulovaný zisk, včetně veškerých rizik a vlivů během poskytování služeb, i předpokládaný vývoj cen vstupních nákladů po celou dobu poskytování služeb. Na sjednanou cenu, případně její změny, nebude mít žádný vliv inflace, kursové změny, zvýšení mezd, změny cen materiálů, prací, energií, médií, jakož i další obdobné skutečnosti, není-li v ustanoveních této smlouvy dohodnuto jinak.

3. MAINTENENCE - (software maintenance) je proces pravidelného udržování, vylepšování a opravování softwarových aplikací po jejich prvotním vývoji a nasazení. Zadavatel v rámci stanovení nabídkové ceny nacení veškerou potřebnou maintenance k řádnému provozovaní dodaného řešení. Potřebnou maintenence dodavatel nacení po dobu udržitelnosti projektu 5let. Maintenance bude dle povahy dodaného řešení pokrývat níže uvedené scénáře:

   Korekční údržba: Oprava chyb a problémů, které se objeví po nasazení softwaru. To může zahrnovat opravy bezpečnostních zranitelností, chyb v kódu nebo jiné problémy, které ovlivňují funkčnost softwaru.
   Adaptivní údržba: Úpravy a změny softwaru, aby zůstal kompatibilní s měnícím se prostředím. To může zahrnovat aktualizace pro nové operační systémy, hardware nebo jiné softwarové závislosti.
   Perfekcionistická údržba: Vylepšení softwaru za účelem zvýšení jeho výkonu nebo použitelnosti. To může zahrnovat optimalizaci kódu, zlepšení uživatelského rozhraní nebo zavádění nových funkcí.
   Údržba softwaru je klíčová pro zajištění, že software zůstane funkční, bezpečný a relevantní i po dlouhou dobu po jeho původním nasazení.

Provozní podpora – uchazeč nabídne formou servisní smlouvy

Požadavek
Zadavatel požaduje detailní návrh podmínek podpory provozu formou návrhu servisní smlouvy doplňující SLA a tento dokument (v souladu s pevnými požadavky) a zajišťující plnohodnotný provoz systému prvků KB od doby zahájení poskytování služeb dle SLA. Dodavatel podle svého uvážení může provést úpravu parametrů, pokud takové úpravy nepovedou ke zhoršení podmínek zajištění podpory provozu dle SLA a tohoto dokumentu. Podpora a servis pro dodaný HW a SW budou poskytovány minimálně po celou dobu udržitelnosti projektu (tj. 60 měsíců od předání díla) – uchazeč bude kalkulovat v návrhu servisní smlouvy **6hod/měsíc**
Bude zajištěna udržitelnost HW a SW včetně třetích stran, dodaných v rámci veřejné zakázky.
Technická podpora a servis zařízení HW a SW budou realizovány dodavatelem, případně prostřednictvím odpovídajícího servisního kanálu výrobce.
Technická podpora a servis budou realizovány v místě zadavatele. Výjimku tvoří činnosti realizovatelné vzdáleným připojením.
Technická podpora bude zajišťována těmito způsoby: • Telefonicky prostřednictvím přiděleného tel. kontaktu. • Prostřednictvím servisního e-mailu. • Prostřednictvím elektronické oznamovací služby (tzv. helpdesku). • Prostřednictvím vzdáleného připojení na PC uživatele / server.
Telefonická, e-mailová podpora a podpora prostřednictvím vzdáleného připojení bude k dispozici minimálně v pracovních dnech od 8 do 16 hod.
Služba HelpDesk umožní příjem požadavku na servisní zásah v českém jazyce prostřednictvím webového rozhraní v režimu 7x24 hod (s výjimkou předem nahlášených servisních zásahů při správě systému HelpDesk). **Provozní popis helpdeskového systému a jeho obsluhy musí být součástí nabídky.**
Postup při řešení incidentů – SLA Zadavatel bude incident oznamovat dodavateli bez zbytečného odkladu jedním ze způsobů a na kontaktních místech, kam budou mít zajištěny přístup pověřené osoby Zadavatele (HelpDesk). Součástí nahlášení požadavku Zadavatelem musí být: • popis Incidentu nebo Požadavku, • jiné relevantní upřesňující informace, včetně případných textových či obrazových příloh nezbytných pro replikaci incidentu, • kontaktní osoba. Dodavatelem používaný systém pro HelpDesk musí pokrýt uvedené informace pro nahlášení požadavku. **Dodavatel zahájí řešení kritického incidentu ohrožující provoz organizace do 4 pracovních hodin od nahlášení, za pracovní hodiny se považuje období mezi 8:00 a 17:00 v pracovní dny.** **Dodavatel zahájí řešení nekritického incidentu NBD od nahlášení.**

Dodavatel neprodleně potvrdí obdržení požadavku v systému HelpDesk a poskytne Zadavateli informace o předpokládaném způsobu řešení požadavku, požadavcích na součinnost Zadavatele a předpokládaný termín vyřešení požadavku.

Dodavatel v průběhu řešení požadavku, pokud mu to charakter požadavku a způsob řešení umožňuje, průběžně informuje Zadavatele o aktuálním stavu a případných změnách v předpokládaném způsobu, požadované součinnosti a termínů vyřešení. V případě že dodavatel v průběhu řešení požadavku zjistí, že se jedná o Incident, jehož zdroj je prvek třetích stran, informuje Zadavatele o této skutečnosti, předpokládaném způsobu, požadované součinnosti a termínů vyřešení a pokračuje v řešení v režimu BE (Best Effort) tzn. dodavatel vyvine maximální možné úsilí na provedení požadavku a zejména na zajištění požadovaných parametrů předmětu plnění v nejkratší možné době.

Zjistí-li dodavatel v průběhu řešení Incidentu, že Incident je neodstranitelný, je v rámci Běžné pracovní doby povinen nepřetržitě pracovat na náhradním řešení a informovat o tomto stavu Zadavatele.

Zjistí-li dodavatel v průběhu řešení Incidentu, že Incident má přímou souvislost s neodborným či neoprávněným jednáním osob Zadavatele případně byl Incident vyvolán produkty či službami třetí osoby, je dodavatel povinen bezodkladně informovat o tomto stavu Zadavatele. Zadavatel se zavazuje bezodkladně uhradit v plné výši náklady nad rámec této smlouvy dodavatelem prokazatelně vynaložené k řešení Incidentu, přičemž samotná identifikace Incidentu je součástí plnění této smlouvy.

Zadavatel je oprávněn dořešení Incidentu kdykoliv zastavit či pozastavit, přičemž nárok dodavatele na úhradu již vynaložených prostředků zůstává nedotčen. Incident je v tomto případě považován za vyřešený.

V případě úspěšného vyřešení požadavku, je řešitel před ukončením požadavku povinen provést ověření funkčnosti služby (pokud je to možné). Iniciátora Incidentu informuje o:

- v případě Incidentu specifikuje příčinu (pokud je známa),
- vyzve iniciátora k ověření funkčnosti služby.

Po ověření funkčnosti ze strany Zadavatele se Požadavek považuje za vyřešený.

Po vyřešení požadavku dodavatel požadavek uzavře v systému HelpDesk a informuje Zadavatele.

Zadavatel má právo ve lhůtě 10 dnů od uzavření požadavku vznést výhrady nebo připomínky ke způsobu řešení nebo k výslednému stavu; v takovém případě se požadavek nepovažuje za uzavřený a Strany se zavazují zahájit společné jednání za účelem odstranění veškerých vzájemných rozporů a nalezení shody nad způsobem řešení nebo výsledném stavu, a to nejpozději do pěti (5) pracovních dnů od výzvy kterékoliv Strany.

Záruky na servisní služby

Zadavatel požaduje záruku na veškeré servisní služby provedené v rámci podpory provozu v délce trvání minimálně 3 měsíců (není-li u konkrétní služby uvedeno jinak) od okamžiku realizace. Veškeré HW opravy po dobu záruky budou bez dalších nákladů pro provozovatele.

Kvalifikační předpoklady

Požadavek
Dodavatel v posledních **5 letech** před zahájením tohoto zadávacího řízení realizoval alespoň **3 významné dodávky**, přičemž:
Předmětem každé z nich byla dodávka řešení KYBERNETICKÉ BEZPEČNOSTI zahrnující vždy též implementaci v níže uvedeném rozsahu. Celkový objem takového projektu musí činit min. **6 000 000 Kč bez DPH** I. instalace HW zařízení i s příslušným SW, II. jeho zprovoznění do funkčního stavu v provozu objednatele, resp. v místě jím určeném a III. zaškolení „obsluhy“ dodávaných prvků na straně objednatele (postačí 1 proškolená osoba na příslušnou dodávku); a v případě alespoň 1 dodávky, která splňuje parametry dle bodu I.: IV. byla jejím předmětem (či alespoň součástí v případě širšího projektu) dodávka **IDM** v pořizovací hodnotě alespoň **2 000 000** Kč bez DPH; V. byla zajišťována i služba spočívající v podpoře provozu kyberbezpečnostních řešení ve vztahu alespoň k té části, která byla předmětem dodávky, zajišťující funkčnost SW nepřetržitě alespoň po dobu 12 po sobě jdoucích měsíců. VII. Uchazeč dodá certifikáty vystavené výrobcem, nebo certifikační autoritou kterou výrobce daného řešení uznává pro minimálně **1 technika na každou níže uvedenou oblast (jeden technik může obsáhnout maximálně dvě technické oblasti)**. Musí se jednat o certifikace od výrobců na dodavatelem skutečně nabízenou technologii, na minimálně tyto požadované technologie, které zcela jasně prokazují, že je odborně způsobilý v oblasti návrhu, implementace, optimalizace a údržby nabízené technologie. • IDM • Serverová infrastruktura • Zabezpečené neměnné (Immutable) deduplikační backup úložiště Období 5 let je splněno i u dodávek v tomto období dokončených (byť započatých dříve). Pokud jde o dodávky v rámci akcí ke dni zahájení zadávacího řízení ještě nedokončených, lze uznat tu část dodávek, které byly dokončeny (nutno doložit) nejpozději ke dni prokázání kvalifikace a obsahově naplňují zde uvedené parametry.

Seznam členů realizačního týmu

Požadavek – Vedoucí realizačního týmu
v období posledních 5 let vedl realizaci (řízení a dozor nad celkovým průběhem zakázky včetně komunikace s klientem) z oblasti **kybernetické bezpečnosti**, a to:
minimálně 3 projektů v celkové hodnotě alespoň **5 000 000 Kč bez DPH/projekt,** a dále: je odborně způsobilý v oblasti projektového řízení = je držitelem certifikátu z oblasti projektového řízení – např. PMP (Project Management Professional) nebo PRINCE2: PRACTITIONER nebo IPMA: C nebo osvědčení srovnatelného s uvedenými certifikáty od jiné oprávněné osoby (v takovém případě dodavatel doplní níže k údajům osvědčení či v samostatném souboru též argumenty nasvědčující „srovnatelnosti“ s uvedenými certifikáty pro možnost posouzení zadavatelem). Období 5 let je splněno i u projektů v tomto období dokončených (byť započatých dříve). Pokud jde o projekty v rámci akcí ke dni zahájení zadávacího řízení ještě nedokončených, lze uznat tu jejich část, která byla dokončena (nutno doložit) nejpozději ke dni prokázání kvalifikace a obsahově naplňuje zde uvedené parametry.

Požadavek – Člen týmu – Bezpečnostní architekt
V období posledních 5 let se podílel jako architekt na realizaci projektů z oblasti kybernetické bezpečnosti, a to:
I. minimálně 2 projekty spočívající v dodávkách a službách v celkové hodnotě alespoň **5 000 000 Kč bez DPH/projekt**, a dále: II. je odborně způsobilý v oblasti řízení bezpečnosti informací = je držitelem platné certifikace - **na úrovni CompTIA Security+ nebo CISSP (Certified Information Systems Security Professional)** - nebo osvědčení srovnatelného s uvedenými certifikáty (v takovém případě dodavatel doplní níže k údajům osvědčení či v samostatném souboru též argumenty nasvědčující „srovnatelnosti“ s uvedenými certifikáty pro možnost posouzení zadavatelem). Období 5 let je splněno i u projektů v tomto období dokončených (byť započatých dříve). Pokud jde o projekty v rámci akcí ke dni zahájení zadávacího řízení ještě nedokončených, lze uznat tu jejich část, která byla dokončena (nutno doložit) nejpozději ke dni prokázání kvalifikace a obsahově naplňuje zde uvedené parametry.