

POPIS NÁVRHU ŘEŠENÍ

k veřejné zakázce

Jednotný informační systém práce a sociálních věcí – Provozní integrační prostředí

Ev.č.: 498306

zadávané v otevřeném nadlimitním řízení dle zákona č. 137/2006 Sb.,
o veřejných zakázkách, ve znění pozdějších předpisů (dále jen „ZVZ“)

Zadavatel veřejné zakázky:

Česká republika – Ministerstvo práce a sociálních věcí
se sídlem Na Poříčním právu 1/376, 128 01 Praha 2

IČO: 00551023



(dále jen „zadavatel“ nebo „MPSV“)

Osoba oprávněná zastupovat zadavatele

Mgr. Michaela Marksová, ministryně práce a sociálních věcí

Zástupce zadavatele

Sdružení ROTGO

vedoucí člen sdružení ROWAN LEGAL,
advokátní kancelář s.r.o., člen sdružení
GORDION s.r.o. a člen sdružení FIALA,
TEJKAL A PARTNEŘI, ADVOKÁTNÍ
KANCELÁŘ, S.R.O.

Kontaktní adresa pro komunikaci s uchazeči

FIALA, TEJKAL A PARTNEŘI,
ADVOKÁTNÍ KANCELÁŘ, S.R.O.
Helfertova 2040/13
613 00 Brno – Černá Pole
kontaktní osoba Mgr. Jan Tejkal, advokát,
tel.: +420 602 298 566
e-mail: tejkal@akfiala.cz

OBSAH

Manažerské shrnutí	4
Základní požadavky	5
Požadavky na licenční zajištění	5
Požadavky na vlastnosti systému	5
Integrační požadavky	7
Výkonnostní požadavky	7
Provozní požadavky	8
Požadavky na testování	9
Požadavky na dokumentaci	11
Požadavky na migraci	12
Požadavky na školení	14
komponenty Systému	17
Active Directory	17
Identity management	19
Microsoft Exchange	22
Certifikační autorita a čipové karty	26
ESB – Enterprise Service Bus	39
Microsoft SharePoint Server (DMS)	45
SCCM a WSUS	56
Provozní dohled	60
Microsoft SQL Server	63
Síťové služby DNS, DHCP a WINS	66
Architektura a návrh řešení	67
Obecné požadavky	67
Požadavky na architekturu systému	67
Požadavky na bezpečnost	68
Harmonogram plnění veřejné zakázky	70
Harmonogram plnění	70
1.2 Aplikovaná metodika řízení dodávky Díla	74
1.2.1 Projektová příprava, řízení projektu	74
1.2.2 Procesy řízení projektu a hlavní výstupy	74
Aplikace služeb podpory provozu	82
Požadavky na součinnost zadavatele	84
Součinnost zadavatele pro analýzu a návrh	84
Součinnost Zadavatele pro testování	85

Součinnost Zadavatele pro migraci dat.....	86
Součinnost Zadavatele pro nasazení.....	87
Součinnost Zadavatele pro školení	88
Součinnost pro projektové řízení.....	90
Seznam potřebného HW.....	91
Použité termíny	92

1 MANAŽERSKÉ SHRNUÍ

AutoCont CZ a.s. předkládá tuto nabídku na implementaci a podporu řešení k veřejné zakázce Jednotný informační systém práce a sociálních věcí – Provozní integrační prostředí (JISPSV-PIP), která je součástí celku Jednotný informační systém práce a sociálních věcí (JISPSV).

Předkládané řešení splňuje všechny požadavky, uvedené v zadávací dokumentaci. Jedná se zejména o oblasti:

- Active Directory – nasazení nového forestu a domény s několika řadiči a migrace nezbytných dat ze stávajících systémů
- Identity Management – implementace Microsoft ForeFront Identity Manager s více servery a napojením na požadované zdroje dat, workflow a mechanismem samoobslužných úprav definovaných atributů
- Microsoft Exchange – implementace více serverů s rolí Mailbox Server a Client Access Server a serverů pro publikaci služeb na Internetu. Ze stávajících systémů budou migrována nezbytná data
- Certifikační autorita a čipové karty – nasazení systému PKI s více servery a dodávka čipových karet.
- Enterprise Service Bus – implementace Microsoft BizTalk se servery ve vysoké dostupnosti, integrací s dalšími požadovanými zdroji a implementací požadovaných funkcionalit a procesů zpracování
- Microsoft SharePoint / DMS – implementace Microsoft SharePoint na více serverech s vysokou dostupností zajišťující uložení a přístup k dokumentům, a to včetně zachování jejich důvěryhodnosti. DMS bude určen jak pro elektronické systémy spisové služby jako fyzické úložiště datových souborů s digitálními dokumenty, tak i bude sloužit pro uložení dokumentů, jež nejsou spravovány v rámci ESS. Uvedené dílčí aplikace budou využívat služeb sdíleného úložiště poskytujícího technologické prostředky pro ukládání dokumentů
- SCCM a WSUS – implementace Microsoft System Center a WSUS pro správu koncových stanic včetně antivirového řešení SC EndPoint Protection
- Provozní dohled – implementace monitoringu PRTG Network Monitor
- Microsoft SQL – některé z implementovaných komponent systému jsou ve své funkcionalitě závislé na databázových službách, jejich realizace je pro tento projekt navržena na technologii Microsoft SQL Server. Vedle SQL serveru, který je instalovaný jako součást aplikace SCCM, budou nasazeny dva samostatné SQL systémy s vysokou dostupností
- Síťové služby DNS, DHCP a WINS – služby budou instalovány na řadiče domény a budou pro ně migrována nezbytná data

AutoCont CZ a.s. je ryze česká IT firma, disponující dostatečným potenciálem pro realizaci ICT dodávky požadovaného typu a rozsahu. Velice dobře známe prostředí státní a veřejné správy a máme s ním z realizace předchozích projektů bohaté zkušenosti. V případě úspěchu ve výběrovém řízení budeme proto k realizaci přistupovat nejen jako k obchodní příležitosti, ale také jako k profesní výzvě, umožňující nám prokázat naše schopnosti a přispět k vytvoření díla, potřebného pro správu a další rozvoj našeho státu.

2 ZÁKLADNÍ POŽADAVKY

Kapitola obsahuje podle požadavků zadávací dokumentace popis splnění požadavků, kladených na realizaci předmětu plnění v kapitolách 2.1 a 2.3.4 – 2.3.10 Přílohy č. 6 Zadávací dokumentace.

2.1 POŽADAVKY NA LICENČNÍ ZAJIŠTĚNÍ

V kapitole jsou sumarizovány podle požadavků kapitoly 2.1 Přílohy č. 6 Zadávací dokumentace licenční požadavky na řešení, uvedené v dalších kapitolách, rozdělené podle typu prostředí.

Protože Uchazeči není známo, jak je zalicencována virtualizační platforma Hyper-V Zadavatele, vycházejí dále uvedené počty licencí z předpokládaných parametrů nasazovaných serverů Systému. Při výkonnostních testech a v rámci etapy Návrh realizace může dojít k dalšímu zpřesnění počtů.

Produkční prostředí

Tabulka 1: Licence Microsoft pro produkční prostředí

Licence	Počet	Poznámka
Windows Server 2012R2 Standard	190	
Forefront Identity Manager 2010R2	2	
Exchange Server 2013 Standard	6	
Exchange Server 2013 Enterprise	10	
BizTalk Server 2013R2	4	
SharePont Server 2013	10	
SQL Server 2012R2 Standard	8	
SQL Server 2014 Enterprise	32	
Windows Server CAL	16 000	Podle počtu uživatelů
Forefront Identity Manager CAL	16 000	Podle počtu uživatelů
Exchange Server CAL Standard / Enterprise	16 000	Podle počtu uživatelů
SharePoint Server CAL Standard / Enterprise	16 000	Podle počtu uživatelů
System Center Configuration Management Client	20 000	Podle počtu spravovaných koncových stanic Součástí je serverová + SQL licence (pouze pro účely SCCM)

Tabulka 2: licence dalších produktů pro produkční prostředí

Licence	Počet	Poznámka
Office Web Apps Server (free)	2	
OSTA – O2 Smart Trusted Archive	1	

PRTG Network Monitor	1	
SUPLECINSPIRE – Lectora® Inspire	1	
ReadyAPI SoapUI NG Pro	3	
Visual Studio Professional Edition + MSDN Subscription	1	

Testovací prostředí

Pro testovací prostředí nejsou uváděny CAL, protože tyto lze sdílet s produkčním prostředím

Tabulka 3: Licence pro testovací prostředí

Licence	Počet	Poznámka
Windows Server 2012R2 Standard	69	
Forefront Identity Manager 2010R2	2	
Exchange Server 2013 Standard	8	
BizTalk Server 2013R2	3	
SharePoint Server 2013	5	
SQL Server 2012R2 Standard	2	
SQL Server 2014 Enterprise	8	
System Center Configuration Management Client	Neznámé	Podle počtu spravovaných koncových stanic Součástí je serverová + SQL licence (pouze pro účely SCCM)

Tabulka 4: licence dalších produktů pro testovací prostředí

Licence	Počet	Poznámka
Office Web Apps Server (free)	2	
OSTA - O2 Smart Trusted Archive	1	
PRTG Network Monitor	1	

2.2 POŽADAVKY NA VLASTNOSTI SYSTÉMU

Kapitola uvádí splnění požadavků Zadavatele, kladených na realizaci předmětu plnění podle kapitoly 2.3.4 – 2.3.10 Přílohy č. 6 Zadávací dokumentace.

2.2.1 INTEGRAČNÍ POŽADAVKY

Kapitola uvádí splnění požadavků Zadavatele, kladených na realizaci předmětu plnění podle kapitoly 2.3.4 Přílohy č. 6 Zadávací dokumentace.

2.2.1.1 Součinnost při integraci

V rámci implementace bude Uchazečem zajištěna nezbytně nutná součinnost při vytváření integračních propojení mezi externími systémy a řešením JISPSV-PIP. Součinnost lze rozdělit na:

- Odbornou konzultaci publikovaného rozhraní jednotlivých agend v rámci JISPSV-PIP a zpřístupnění technické dokumentace.
- Technické zpřístupnění API dle parametrů nezbytně nutných pro úspěšné a bezpečné napojení v souladu s respektováním oprávnění a nastavení dle rozsahu příslušných agend a zákonných požadavků a limitů.
- Technická spolupráce na provedení integračních testů s předáním logovacích výstupů rozhraní v souladu s rozsahem příslušné agendy a zákonných požadavků a limitů.
- Technická konzultace a součinnost nezbytně nutná pro integraci JISPSV-PIP s dalšími komponentami v infrastruktuře Zadavatele.

Součinnost bude plánována, evidována a řešena v rámci projektového řízení dle vzájemně odsouhlasených pravidel způsobu plánování součinností s dostatečným předstihem.

2.2.1.2 Způsob transformace XML zpráv

Implementace výměny zpráv a dat mezi systémem JISPSV-PIP a jinými systémy, popř. i v rámci systému JISPSV-PIP samotného bude probíhat primárně prostřednictvím XML zpráv. Jestliže povaha XML zprávy bude nutně vyžadovat provedení transformace do jiného tvaru XML zprávy, bude pro tuto činnost výhradně použita technologie XSLT.

2.2.1.3 Kontroly XML

Implementace výměny zpráv a dat mezi systémem JISPSV-PIP a jinými systémy, popř. i v rámci systému JISPSV-PIP samotného bude probíhat primárně prostřednictvím XML zpráv. Každá taková zpráva bude přesně definována XSD předpisem. Všechny XSD předpisy stejně jako samotné zprávy budou specifikovány v rámci fáze Návrh realizace. Následně v rámci implementace budou technicky dodefinovány a následně implementovány.

Každá předávaná zpráva bude považována za relevantní za předpokladu, že vyhoví jak na vstupu, tak na výstupu předpisu XSD schématu. Každé volání i přijímání zprávy bude mandatorně XSD předpisem validováno. Vyhovění předpisu však nutně neznamená postačující podmínku vyhovění příchozí zprávy, je však podmínkou nutnou.

2.2.2 VÝKONNOSTNÍ POŽADAVKY

Kapitola uvádí splnění požadavků Zadavatele, kladených na realizaci předmětu plnění podle kapitoly 2.3.5 Přílohy č. 6 Zadávací dokumentace.

Škálovatelnosti je dosaženo na základě rozšiřitelnosti počtu jednotlivých komponent tak, aby bylo možné reagovat na zvyšování požadovaného výkonu pro zabezpečení potřeb dalšího rozvoje.

Modularita systému JISPSV-PIP umožní snazší propojení s dalšími systémy i zapojení do stávající infrastruktury Zadavatele.

Principy škálování:

- Prezentační vrstva – přidáním dalších serverů pro dané úlohy
- Aplikační vrstva – přidáním dalších serverů pro dané úlohy
- Databázová vrstva – rozšiřováním HW zdrojů serveru

Zvolené principy umožňují lineární škálovatelnost systému JISPSV-PIP a to nejen v případě nutného posílení výkonu.

JISPSV-PIP je navržen pro provoz ve dvou stávajících datových centrech, přičemž design nijak neomezuje případné budoucí rozšíření. Klíčové prvky dodávané infrastruktury JISPSV-PIP jsou redundantní, což umožňuje dosáhnout požadované úrovně vysoké dostupnosti.

Redundance je zajištěna na všech logických vrstvách, tedy jak v oblasti hardwarového, tak i softwarového řešení. V oblasti softwarového řešení pak od operačního systému, přes serverové softwarové prvky až po aplikační vrstvu. Zároveň je pro zajištění redundance použito jen nezbytného množství komponent daného typu tak, aby byly optimalizovány pořizovací a provozní náklady systému JISPSV-PIP, ale nebylo ohroženo dodržení požadované úrovně dostupnosti.

Volba databázového produktu Microsoft SQL Server též zajišťuje požadavek na neomezenou možnost škálování licencí pro provoz databáze.

Systém JISPSV-PIP je navržen tak, že minimalizuje používání zámků a bude využívat zámky jen v nezbytně nutné míře a na položky tak, aby garantoval souběžnou práci v systému. Výjimku tvoří případné dávkové úlohy, které se ale plánují v rámci pracovního období mimo uživatelskou špičku, ale i v tomto případě, lze úlohy transakčně atomizovat.

Systém JISPSV-PIP je navržen dostatečně robustně tak, aby zvládl obsloužit požadovaných až 20 000 souběžně pracujících koncových uživatelů.

JISPSV-PIP je navržen tak, aby výsledná doba žádné z on-line operací zadaná uživatelem na koncové stanici, s výjimkou generování sestav, nebyla delší než 4 sekundy. V případě, že nebude ověřovat data v jiném systému, je JISPSV-PIP navržen tak, že bude schopen reagovat na požadavky na službu přes definované API v řádu milisekund.

V rámci implementace bude provedeno primární testování požadované výkonnosti a budou poskytnuty podklady a součinnost pro zátěžové testování aplikací třetí stranou. Ověřování výkonnosti bude realizováno okamžitě po úspěšném provedení funkčních testů. V průběhu realizace funkčních testů bude zpracována analýza pro vlastní ověřování výkonnosti, ve které budou definovány podklady pro vlastní testování zátěže. Zátěžové testy provádíme za účelem stanovení výkonnostního stropu systému JISPSV-PIP a demonstrace, že systém v běžných provozních podmínkách tohoto stropu nedosáhne. Testování probíhá simulací zátěže, která v reálném provozu nenastává.

2.2.3 PROVOZNÍ POŽADAVKY

Kapitola uvádí splnění požadavků Zadavatele, kladených na realizaci předmětu plnění podle kapitoly 2.3.6 Přílohy č. 6 Zadávací dokumentace.

157

Vývojové prostředí

Vývoj bude probíhat na prostředcích a v prostředí Uchazeče. Pouze v odůvodněném případě, kdy bude nutné z důvodu návaznosti na další komponenty, bude do prostředí Zadavatele dodán obraz potřebných VM.

Testovací prostředí

Součástí dodávky bude dodání plně funkčního testovacího prostředí do prostředí Zadavatele pro realizaci funkčních testů.

Produkční prostředí

Systém bude zajišťovat primárně on-line práci koncových uživatelů podle požadavků na výkonnost a dostupnost aplikací. Některé funkcionality budou řešeny jako dávkové s možností plánování na libovolný čas a budou probíhat nezávisle na on-line systémech a bez ovlivnění výkonnosti systému z pohledu uživatele.

Správa systému

Pro správu Systému a jeho jednotlivých komponent budou vytvořeny administrátorské role, umožňující úplnou administraci a správu Zadavatelem.

Přístupová práva a hesla administrátorských rolí k Systému budou předána neprodleně po provedení fáze „Implementace – migrace dat“ a jejich změna bude provedena výlučně na základě písemného souhlasu Zadavatele.

Správa a administrace dodaných systémů bude zajišťována Zadavatelem. Uchazeč zajistí v rámci „Služeb podpory provozu“ službu „Správa a administrace systémů“ na základě požadavků předkládaných přes ServiceDesk v požadovaném rozsahu a SLA.

Alokace zdrojů

Většina komponent Systému bude provozována na virtualizační platformě Microsoft Hyper-V v datových centrech Zadavatele. Pro alokaci zdrojů bude využito dostupných technologií tak, aby byl provoz optimalizován a nedocházelo ke zbytečnému plýtvání systémovými zdroji.

2.2.4 POŽADAVKY NA TESTOVÁNÍ

Kapitola uvádí splnění požadavků Zadavatele, kladených na realizaci předmětu plnění podle kapitoly 2.3.7 Přílohy č. 6 Zadávací dokumentace.

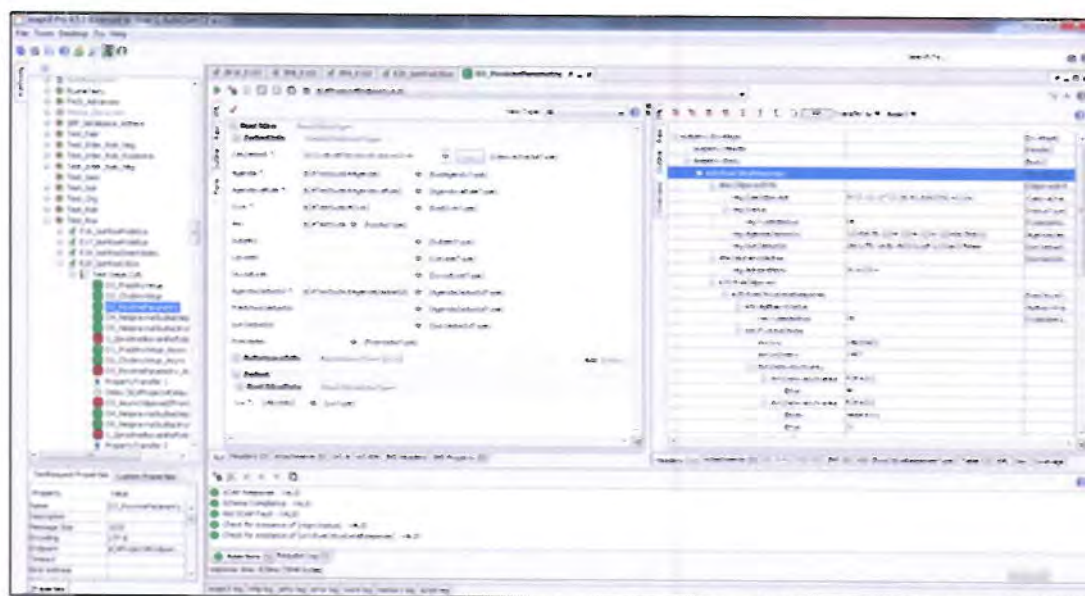
2.2.4.1 Funkční testy

Pro potřeby provedení funkčních testů pro řádnou akceptaci díla připraví Uchazeč testovací plán a sadu testovacích scénářů vážících se ke každému z implementovaných případů užití, jak budou popsány v rámci výstupů etapy Návrh realizace.

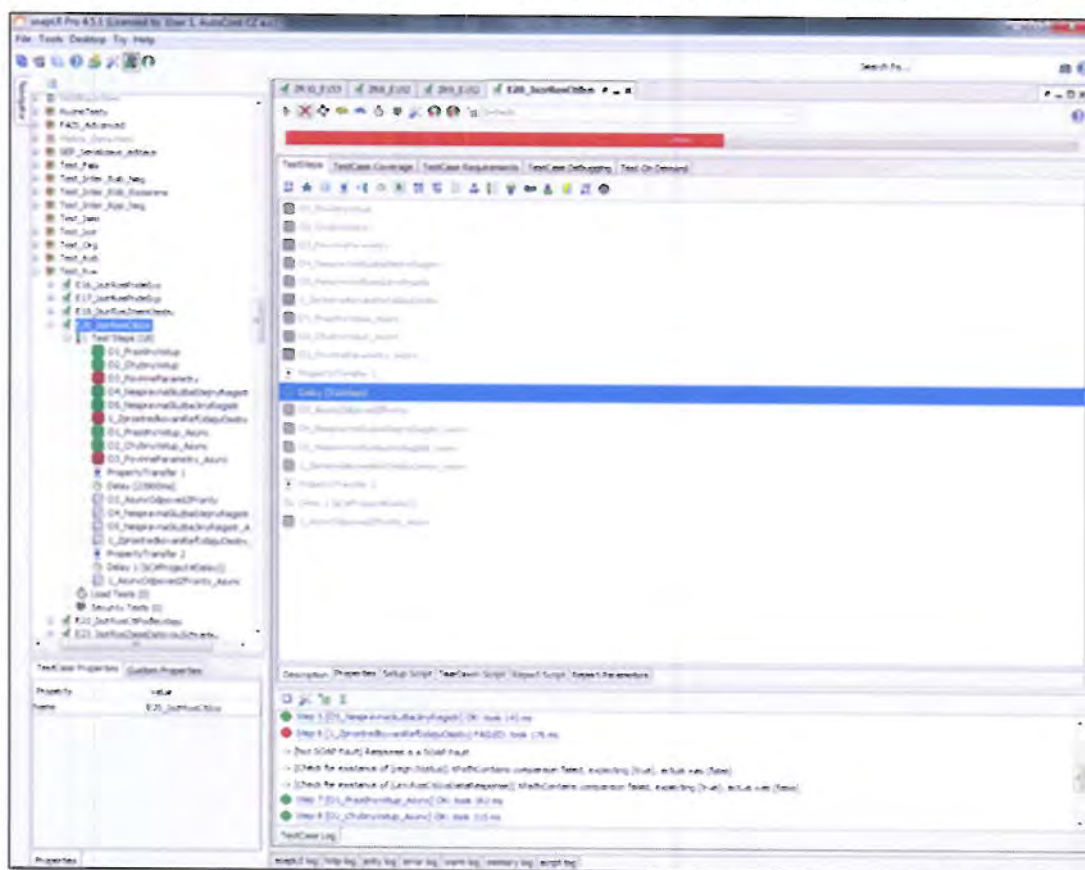
Samotné provedení testů v rámci akceptace bude na základě připravených scénářů realizovat Zadavatel anebo jím pověřená třetí strana. Případné chyby nalezené při testování Uchazeč odstraní.

Pro každý z testovacích scénářů připraví Uchazeč automatizovaný skript nebo postup, který umožní opakované, automatické provádění testů.

Pro technologii webových služeb využijeme nástroj SoapUI, který je zahrnut SW licencích. S využitím uvedeného nástroje jsme schopni maximálně optimalizovat samotný průběh testů a vytvářet srozumitelné výstupy k následné analýze a promítnutí oprav do systému JISPSV-PIP.



Obrázek 1 – Příklad testu v SoapUI – Request, Response a kontroly (Assertions)



Obrázek 2 – Příklad běhu testu v SoapUI

2.2.4.2 Bezpečnostní testy

Uchazeč v souladu s požadavkem Zadávací dokumentace poskytne nezbytnou součinnost odborné třetí straně pro provedení bezpečnostních testů (penetrační testy, testy zabezpečení uživatelského rozhraní,

testy ochrany údajů, testy havarijních scénářů). Veškerá rizika identifikovaná v rámci těchto testů budou následně eliminována a doložena v rámci standardního projektového řízení.

2.2.4.3 Výkonnostní testy

Uchazeč v souladu s požadavkem Zadávací dokumentace poskytne nezbytnou součinnost odborné třetí straně pro provedení výkonnostních (zátěžových) testů. Veškerá rizika identifikovaná v rámci těchto testů budou následně eliminována a doložena v rámci standardního projektového řízení.

2.2.5 POŽADAVKY NA DOKUMENTACI

Kapitola uvádí splnění požadavků Zadavatele, kladených na realizaci předmětu plnění podle kapitoly 2.3.8 Přílohy č. 6 Zadávací dokumentace.

Instalační příručka, provozní příručka a uživatelský manuál budou dodány formou dokumentů ve formátu MS Word a PDF (každý dokument v obou formátech) a to ve verzi aktuálně uvolněné ke dni akceptace. Ve stejném formátu bude dodána i doplňková dokumentace ve vztahu ke zdrojovým kódům, vývojovému prostředí a softwarovým knihovnám.

Analytická a vývojářská dokumentace vytvářené formou modelu budou dodány ve formě modelu nástroje Sparx Systems Enterprise Architect ve verzi aktuálně uvolněné ke dni akceptace. Podmínkou dodávky zmíněných typů dokumentací v tomto formátu, je zpřístupnění centrálního modelu Zadavatelem, jak je popsáno v rámci součinnosti v kapitole 5.1.

2.2.5.1 Instalační příručka

Instalační příručka bude dodána tak, aby popisovala jednotlivé kroky instalace, konfigurace a zprovoznění systému JISPSV-PIP. Příručka bude zahrnovat všechny nezbytné instalační kroky nad rámec instalace operačního systému. Dále bude zahrnovat výčet všech nezbytných komponent včetně verzí, licencí a konfigurací a to včetně operačního systému, databáze a použitých softwarových frameworků.

Příručka se může odkazovat do instalačních příruček produktů třetích stran či produktů Uchazeče, přičemž taková dokumentace bude též předaná na samostatném nosiči CD/DVD ROM.

2.2.5.2 Provozní příručka

Provozní příručka bude dodána tak, aby popisovala z pohledu správce (administrátora) činnosti nezbytné pro zajištění chodu systému JISPSV-PIP. Součástí provozní příručky jsou operátorské procedury, které zahrnují provozní postupy údržby systému JISPSV-PIP, plány obnovy, zálohovací plány a postupy archivace.

Příručka se může odkazovat do příruček produktů třetích stran či produktů Uchazeče, přičemž taková dokumentace bude též předaná na samostatném nosiči CD/DVD ROM.

2.2.5.3 Uživatelský manuál

Uživatelský manuál pro práci se systémem JISPSV-PIP bude dodán v rozsahu umožňujícím novému uživateli systému začít samostatně pracovat se systémem.

2.2.5.4 Analytická dokumentace

Výstupy fáze Návrh realizace budou dodány ve formě modelu v nástroji Sparx Systems Enterprise Architect s minimálním obsahem tvořeným katalogem detailních požadavků, modelu části podnikové architektury, která je pokryta systémem a modelem podporovaných procesů.

Model části podnikové architektury bude využívat notaci ArchiMate® 2.1 (či novější revizi), model procesů notaci BPMN 2.0 (či novější revizi).

2.2.5.5 Vývojářská dokumentace

Výstupy fáze Návrh realizace a Implementace budou formou modelu s využitím notace UML2 (verze 2.4.1 či novější) a bude obsahovat model tříd, model případů užití, model komponent a model nasazení. Nad rámec dílčích UML2 modelů bude model obsahovat katalog požadavků (rozpracovaný a doplněný z analytické dokumentace) a model perzistence (schéma relační databáze).

Součástí vývojářské dokumentace bude také výčet a informativní popis s odkazy na dokumentaci všech použitých knihoven zahrnutých v řešení.

2.2.5.6 Příručka pro administrátory

Příručka pro administrátory systému JISPSV-PIP bude podrobně popisovat postupy administrace. V případě částí Active Directory a IdM budou součástí příručky i ostatní dokumentace nezbytné pro řádnou správu a administraci těchto prostředí. Příručka bude v rozsahu umožňujícím novému administrátoru začít samostatně systém administrovat.

2.2.5.7 Dokumentace k vývojovému prostředí

V souladu s požadavkem na dodání vývojového prostředí bude též dodána jeho technická dokumentace v takovém rozsahu, že bude popisovat instalaci, konfiguraci, způsob použití prostředí pro vývoj systému JISPSV-PIP tak, aby na jejím základě mohlo být takové prostředí vybudováno a sestaveny komponenty systému JISPSV-PIP na základě předaných zdrojových kódů (tam, kde bude docházet k vývoji).

2.2.5.8 Zdrojové kódy

Zdrojové kódy a související konfigurační soubory k veškerému softwarovému vybavení, které budou vytvořeny v rámci plnění, budou předány Zadavateli. Zdrojové kódy budou předány podepsáním protokolu o předání v rámci projektu a předáním kódů na datovém nosiči určeném pouze pro čtení.

Zdrojové kódy budou exportovány z vývojného prostředí Uchazeče jako soubor adresářů a v nich uložených souborů tak jak budou uloženy v systému pro správu verzí.

2.2.5.9 Úložiště dokumentace a zdrojových kódů

Všechny dokumentace včetně příruček a manuálů, budou udržovány a aktualizovány po celou dobu plnění v primárním úložišti veškeré dokumentace a zdrojových kódů, které bude provozováno Zadavatelem v infrastruktuře resortu. Taktéž veškeré změny ve zdrojových kódech, podpůrných skriptech budou v rámci úložiště uloženy a aktualizovány.

V rámci primárního úložiště budou také zachovány historické verze veškeré dokumentace a zdrojových kódů, skriptů (verzování). Dokumentace a zdrojový kód budou předány Uchazečem Zadavateli formou předávacího protokolu, jehož součástí bude také datový nosič (CD/DVD/BD/USB) s celým obsahem k datu relevantnímu datu převzetí.

2.2.6 POŽADAVKY NA MIGRACI

Kapitola uvádí splnění požadavků Zadavatele, kladených na realizaci předmětu plnění podle kapitoly 2.3.9 Přílohy č. 6 Zadávací dokumentace.

Migrace dat ze stávajících systémů podle platné legislativy a poskytnuté součinnosti uvedené v Zadávací dokumentaci, bude probíhat formou importu dat z podkladů poskytnutých Zadavatelem v rámci součinnosti. Znamená to tedy, že přístup do stávajících systémů nebude umožněn, což umožňuje definovat základní migrační strukturu následovně.

Struktura a formát dat

Veškerá migrovaná data musí být sdružována do tzv. datových vět, které budou skládáním tvořit migrovaný celek. Datová věta bude tvořena z párových elementů PRVEK-HODNOTA, přičemž PRVEK může v sobě zapouzdřovat další PRVEK. Takto bude možné na nejobecnější úrovni sestavit data ve formátu XML, CSV a také jako tabulkové databázové exporty.

Příklad XML: Soubor Ciselniky_StatyEU.xml

```
<Staty>
  <Stat>
    <Nazev>Francie</Nazev>
    <Zkratka>F</Zkratka>
    <Aktivni>1</Aktivni>
    ...
  </Stat>
  ...
</Staty>
```

Uvedené datové věty budou primárně odpovídat řádkům databáze. V případě, že budou mezi daty vazby v rámci různých migračních částí, bude toto explicitně specifikováno, aby byl nalezen přesný mechanismus postupného importování dat. V tomto případě bude nezbytně nutné, aby byl pro migraci dodán export databáze, který integrační vazby bude nativně udržovat.

Plán migrace

Plán migrace zde uvedený je tedy obecnou metrikou, jak bude postupováno. Případné specifické singularity budou řešeny v rámci detailního plánu migrace při konkrétní fázi realizace s přihlédnutím k dohodnutým projektovým pravidlům.

Činnost	Náplň
Návrh migračního rozhraní	Navržení a určení technologických prostředků (DBMS apod.) pro předání dat
Návrh formy reportu chyb a událostí	Navržení způsobu žurnálování a logování průběhu zpracování migrovaných dat za účelem následných analýz těchto výstupů
Definice procesu nápravy vadných a nekompletních dat	Navržení způsobu zpracování chybných nebo nezpracovaných dat na základě logů průběhu zpracování
Návrh struktur datových vět	Vytvoření datového modelu na úrovni entit, které budou až na úrovni datových typů popisovat jednotlivé atributy datových vět.
Kategorizace struktur datových vět, dle účelu	Vytvoření členění datových struktur na základě funkčních celků systému JISPSV-PIP
Stanovení pořadí migrace	Sestavení tabulky priorit dle funkčních celků a referenční integrity
Tvorba rozhraní	Implementace struktur v rámci zvoleného DBMS
Příprava migračních komponent na úrovni migračního nástroje	Vytvoření definic popisující vztah mezi zdrojovými strukturami a cílovými strukturami v kontextu migračního nástroje
Otestování migračních komponent	Podrobné otestování funkčních částí na úrovni jednotkových a aplikačních testů
Zátěžové testy s odhadem časové náročnosti	Podrobné otestování z hlediska strojového času a rozložení výkonu s ohledem na množství migrovaných dat s následným odhadem doby migrace
Harmonogram migrace	Sestavení časového plánu na základě odhadnutého času a pořadí migrace jednotlivých funkčních celků

Činnost	Náplň
Testovací migrace	Komplexní ověření migračního postupu nad reprezentativním vzorkem dat
Kontroly integrity a úplnosti dat testovací migrace	Prověření korektně provedené migrace
Ostrá migrace	Provedení celkové migrace dat dle ověřeného postupu migrace
Kontroly integrity a úplnosti dat ostré migrace	Prověření korektně provedené migrace

Tabulka 5 – Plán migrace

Seznam činností uvedených v předchozí tabulce bude stejný jak pro migrace v rámci fáze prototypu, tak i pro migrace v rámci fáze implementace. Rozdíl mezi těmito dvěma migracemi bude dán rozsahem funkcionalit zahrnutých do prototypu.

2.2.6.1 Migrace dat

Datová migrace bude probíhat jen na ta data, u nichž požadavek na dostupnost z aplikace bude ke dni odstávky stávajícího systému odpovídat zákonným lhůtám. Při migraci nedojde k žádnému zkreslení, ztrátě nebo duplicitě dat.

Minimální kontroly během migrace budou na formáty a platnost dat tam, kde je možné provést jejich ověření pomocí kontrolních součtů, intervalů a/nebo číselníků. Po migraci proběhnou kontroly na integritu a úplnost migrovaných dat, které budou po vzájemné dohodě připraveny dle podkladů poskytnutých Zadavatelem.

2.2.6.2 Nepřerušitelnost provozu

Migrační nástroje budou implementovány tak, aby plně respektovaly všechny bezpečnostní požadavky kladené na ochranu dat a jejich vysokou dostupnost. Zejména s ohledem na:

- Ochranu před neoprávněným přístupem a to jak pro přístup k poskytnutým exportovaným datům, tak i k datům v průběhu jejich migrace.
- Respektování nastavení granularity oprávnění na úrovni databázových operací, přístupu k tabulkám nebo sloupcům tabulek.
- Zajištění integrity importovaných i naimportovaných dat a to i v případě, že dojde v průběhu migrace k nenadálým událostem (např. rozsáhlý výpadek proudu).
- Implementované logování všech DB operací, tj. již migrace bude znamenat auditní stopu nad daty.
- Výkonnost samotné migrace tak, aby byla migrační zátěž v případě potřeby rozložitelná na více serverů, popř. běžících vláken.

2.2.7 POŽADAVKY NA ŠKOLENÍ

Kapitola uvádí splnění požadavků Zadavatele, kladených na realizaci předmětu plnění podle kapitoly 2.3.10 Přílohy č. 6 Zadávací dokumentace.

2.2.7.1 Podklady pro školení

Uchazeč vytvoří podklady pro školení uživatelů ve formě prezentace školených vlastností a funkcionalit systému JISPSV-PIP. Podklady pro školení budou strukturovány podle dílčích aplikací a modulů, reflektujících skupiny samostatně prováděných činností. Součástí podkladů ke každému typu školení budou interaktivní eLearning kurzy ve formátu SCORM v poslední uvolněné verzi SCORM 2004 4th Edition. Všechny podklady budou předávány i ve zdrojovém formátu.

Podklady pro školení budou sestávat z několika materiálů, minimálně však:

- Prezentace s přehledem pravidel školení a obecné časování školení

- Časy přestávek a obědu
- Pokládání dotazů
- Používání mobilních telefonů a jiné výpočetní techniky
- aj.
- Prezentace s detailním přehledem časového plánu školení z pohledu školené problematiky
 - Rozpad na jednotlivá školená témata
 - Časový rozsah školeného téma
 - Syllabus jednotlivých témat
 - Předpoklad minimálních znalostí proškoleného uživatele
- eLearning kurzy pro jednotlivá témata
 - eLearning bude vytvořen pomocí nástroje Lectora® Inspire od společnosti Trivantis Corporation Inc.
 - Výstupem bude formát SCORM dle požadavku, který bude možné importovat do odpovídajícího eLearningového nástroje
- Detailní prezentace školeného tématu

Prezentace budou pro každého účastníka školení k dispozici ve vytištěné podobě pro možnost tvorby poznámek. Tisk bude připraven tak, aby na liché stránce byly dva až tři obrazy prezentace a na sudé stránce pak volný list určený k provedení poznámek k daným obrazovkám.

Současně budou podklady školení v souladu s požadavkem na portál školení (viz kapitola 2.2.7.2) umístěny na portále školení a dokumentace.

Veškeré podklady pro samotné školení budou připraveny ve formátu MS PowerPoint ve verzi aktuálně uvolněné ke dni předání podkladů pro školení. Konkrétní verzi včetně případných servisních oprav (sevice pack, kb opravný balíček, hot-fix, atp.) si obě strany před předáním dokumentace dohodnou na projektové úrovni a stvrdí dohodu zápisem. V této souvislosti je vyžadována na straně Zadavatele součinnost popsaná v kapitole 5.5.

2.2.7.2 Portál školení

Součástí JISPSV-PIP bude jednoduchá portálová aplikace na platformě Microsoft .NET, která bude poskytovat veškerou uživatelskou dokumentaci a školící podklady. Odkazy na tyto dokumenty pak budou distribuovány v rámci školících materiálů, popř. e-mailové komunikace.

2.2.7.3 Školení

Školení uživatelů bude probíhat na PC (popř. mobilním pracovišti) s přístupem na testovací (školící) prostředí Zadavatele a bude provedeno následovně, přičemž je třeba, aby byla zajištěna minimální součinnost Zadavatele popsaná v kapitole 5.5.

- 4 x 1 den školení administrátorů, přičemž každý den bude doškolen minimálně 20 osob tak, aby bylo dle požadavku proškolen 80 administrátorů.
- 10 x 1 den školení správců aplikace, přičemž každý den bude proškolen minimálně 20 osob tak, aby bylo dle požadavků proškolen 200 správců aplikace.

Všechna školení budou provedena prezenční formou v součinnosti se Zadavatelem na základě požadavků na součinnost popsanych v kapitole 5.5. Uchazeč poskytne až pět školitelů dle povahy a rozsahu konkrétního školení.

Uchazeč zajistí pro potřeby školení základní občerstvení pro účastníky školení. To bude podle potřeby sestávat z dopolední a odpolední přesnídávky a nápojů.

2.2.7.4 Dodávka mobilních pracovišť

Dodávka mobilních pracovišť bude sestávat z dodávky 80-ti přenosných notebooků dle požadované specifikace. Bude se jednat o notebooky značky Lenovo typ ThinkPad L440.

Vlastnost	Popis
Displej	14" HD (1600*900)
Procesor	Intel Celeron 2950M
OS	Win 7/8.1 Pro (64bit)
Záruka	3roky on-site NBD
Konektivita	wifi, 3G, bluetooth, HDMI (redukci z mini DP), USB 3.0, čtečka paměť. karet
Grafický adaptér	Intel HD 4600
Bezpečnost	Čtečka SmartCard, Security Chip
Paměť	8GB RAM
HDD	256 SSD
Baterie	6 Cell Baterie, výdrž více než 4h v úsporném režimu
Zdroj	65W AC Adapter
Klávesnice	CZ klávesnice
Brašna	Kensington Contour
Myš	Optická myš, 1000 DPI, USB, černá
Maintenance	3 roky v režimu NBD (next business day)

Tabulka 6 – Mobilní pracoviště

2.3 KOMPONENTY SYSTÉMU

Kapitola uvádí splnění požadavků Zadavatele, kladených na realizaci předmětu plnění podle kapitol 2.4.1 – 2.4.6 Přílohy č. 6 Zadávací dokumentace.

2.3.1 ACTIVE DIRECTORY

Kapitola obsahuje popis nasazení Active Directory (AD) podle požadavku Přílohy č. 6 Zadávací dokumentace v kapitole 2.4.1.

Jako centrálním systémem pro uchování identit uživatelů a zařízení a řízení přístupových oprávnění bude použita adresářová služba Active Directory s jediným forestem a jedinou doménou. Pro zajištění vysoké dostupnosti a výkonnosti bude s ohledem na počet uživatelů a zařízení, uvedený v rámci Zadávací dokumentace a Dodatečných informací, nasazeno více řadičů domény.

Role, kterou má uživatel přidělena v rámci IS, bude primárně řízena přes členství uživatelů ve speciálně vytvořených skupinách v AD. Pro správu členství ve skupině bude sloužit Forefront Identity Manager (FIM), implementovaný v rámci tohoto projektu (viz 2.3.2).

Postup implementace a migrace bude upřesněn v průběhu etapy Návrh realizace – analýza. Součástí návrhu bude zejména:

- Návrh architektury a funkční struktury nově založené Active Directory (FSMO role, kontejnery, skupiny, GPO atd.) s ohledem na možnost delegace správy.
- Seznam a typ objektů, migrovaných ze stávajících Active Directory, a definice migrovaných atributů podle technologických podmínek (SID, veřejná část certifikátu uživatele atd.).
- Postup migrace a volba migračního nástroje.
- Návrh správy účtů a skupin a souvisejících procesů (uložení veřejné části certifikátu a jeho použití pro autentizaci uživatele, autentizace prostřednictvím LDAP protokolu, SSO pomocí protokolu Kerberos, KDC atd.)

Produkční prostředí

Pro potřeby služeb AD v produkčním prostředí bude využito celkově čtyř serverů, po dvou v každém datovém centru.

Server	Typ serveru	Umístění	Poznámka
AD01	Fyzický HW	DC1	Řadič domény
AD02	Virtuální počítač	DC1	Řadič domény
AD03	Virtuální počítač	DC2	Řadič domény
AD04	Virtuální počítač	DC2	Řadič domény

Údaje jsou uvedeny orientačně a budou upřesněny v etapě Návrh realizace – analýza.

Testovací prostředí

Implementace AD v testovacím prostředí bude kopírovat nasazení v produkčním prostředí s omezením počtu a výkonnosti serverů.

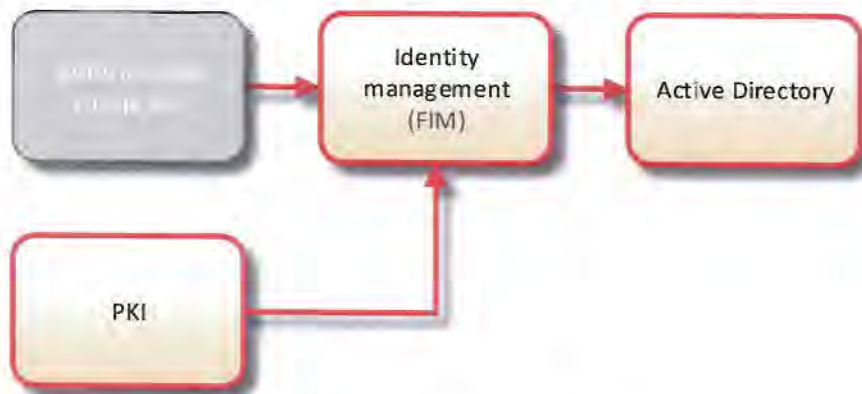
Server	Typ serveru	Umístění	Poznámka
AD01	Virtuální počítač	DC1	Řadič domény

AD02	Virtuální počítač	DC2	Řadič domény
------	-------------------	-----	--------------

Údaje jsou uvedeny orientačně a budou upřesněny v etapě Návrh realizace – analýza.

2.3.2 IDENTITY MANAGEMENT

V rámci plnění zajistí Uchazeč nasazení platformy Microsoft Forefront Identity Manager 2010R2 (dále jen FIM) podle požadavku Přílohy č. 6 Zadávací dokumentace v kapitole 2.4.4.



Obrázek 3: Implementace FIM

2.3.2.1 Architektura IdM

IdM bude sloužit jako centrální bod zajišťující jednotnou administraci identit uživatelů a jejich rolí.

Implementace se bude skládat z několika celků:

- FIM Synchronizace – bude sloužit pro synchronizaci identit z napojených datových zdrojů
- FIM Service / Portál – bude sloužit pro procesování logiky (workflows), interface IdM pro administrátory a uživatele a jako rozhraní pro externí webové služby (typu JIP a KAAS). Jako portál bude použita custom komponenta napsaná pro tyto účely.
- Veškeré informace budou uloženy v dedikované instanci SQL databáze.

FIM Synchronizace

FIM Synchronizace bude implementována pomocí produktu Microsoft Forefront Identity Manager 2010R2.

Předpokládáme implementaci na jednom serveru v primární lokalitě. V záložní lokalitě bude implementována hot stand-by instance Synchronizační služby, která bude aktivována v případě přechodu do záložní lokality.

Jako podkladové datové úložiště bude použit Microsoft SQL Server 2012 (respektive jeho dedikovaná instance). Použitý bude stejný SQL server jako v případě IdM portálu.

FIM Synchronizace bude navázána přes datové interface k většině používaných systémů na MPSV. Zvláště se bude jednat o následující systémy/aplikace:

- Active Directory – centrální úložiště všech identit
 - Nativní FIM AD connector s napojením objektů typu uživatel a skupina z vybraných Organizačních jednotek
- Docházkový systém MPSV
 - Custom ECMA connector pro napojení do aplikace
- HR systém
 - Několik datových úložišť pro různé typy pracovníků (internista, externista apod.)
 - Dle typu systému bude použit buď SQL nebo ECMA connector
- Databáze Certifikační Autority
- Číselníky pro systemizaci, identifikátory apod.

- Další aplikační systémy - odhadovaný počet systému je 10-15

Předpokládáme, že celkem bude napojeno maximálně 20 systémů / aplikací, z nichž většina bude napojena pokud možno přes SQL connector.

Pro FIM budou použity tyto autoritativní zdroje dat:

- Personální systém (systémy) – napojení na synchronizační část
- JIP/KAAS. Specifikace systému JIP/KAAS – napojení na portálovou část
- Certifikační Autorita jako zdroj veřejného klíče certifikátu – napojení na synchronizační část
- Číselník klientů jako zdroj IK MPSV – napojení na synchronizační část (několik separátních konektorů)

Konkrétní aplikace a způsob provázání systémů bude definován v rámci fáze Návrh realizace – analýza.

FIM Service / Portál

Portálová část bude implementována pomocí custom vývoje. Bude zahrnovat moduly pro:

- Jednotný interface pro uživatele (zadávaní a vyřizování požadavků do IdM)
- Interface pro administrátory (management spravovaných identit, provisioning a de-provisioning)
- Napojení na systémy, které jako interface používají webové služby.
- Systém pro workflow – zakládání, schvalování, procesování (využití hierarchie uživatelů pro schvalování požadavků)
- Reporting

Předpokládáme implementaci na dvou serverech, po jednom v každém datovém centru Zadavatele.

Jako podkladové datové úložiště bude použit Microsoft SQL Server 2012 (respektive jeho dedikovaná instance), stejně jako v případě FIM synchronizační služby.

2.3.2.2 Naplnění požadavků IdM

Implementace IdM pokrývá následující funkcionality:

- Správa identit na základě workflow z autoritativních zdrojů ve spravovaných systémech
 - V rámci FIM synchronizační části budou nastaveny konektory do autoritativních zdrojů, ze kterých budou přenášeny identity a informace o nich do centrální databáze Metaverse. Z ní budou následně na základě logických pravidel tyto identity propisovány do dalších neautoritativních (spravovaných) systémů, společně s vybranou sadou informací (atributů z autoritativních zdrojů).
- Vznik, správa identit a přiřazení rolí na základě distribuované administrace v IdM
 - Součástí logiky ve FIM synchronizační části budou pravidla pro vznik / zánik (provisioning / deprovisioning) identit ve spravovaných systémech. Logika bude obsahovat i logické toky pro atributy spravovaných identit.
- Zajištění jednotného hesla ve spravovaných systémech
 - Implementace FIM Synchronizační části bude obsahovat komponentu pro ukládání hesla z Active Directory (jako autorizovaného místa pro vznik hesla). Toto heslo bude dále replikováno do napojených systémů, které toto podporují
- Správa organizačních a procesních rolí, jejich vytváření a synchronizace do spravovaných systémů (provisioning) na principu RBAC (Role-Based Access Control)
 - Role budou implementovány na základě členství ve skupinách v Active Directory. Členství v příslušné skupině následně spustí Workflow pro další zpracování této informace.
- Vytváření organizačních rolí na principu role podle organizačního zařazení a role podle jednotlivých lokalit

- V Metaverse bude založena speciální třída pro správu informace členství v organizační struktuře (například podle lokality nebo příslušnosti k organizačnímu oddělení). Bude vytvořena logická vazba mezi spravovanými identitami a jejich členství v organizační struktuře.
- Testování vytvářených rolí a ověřování jejich správnosti
 - Testování správnosti zakládaných rolí bude implementováno pomocí funkce „Preview“ v synchronizační části, která dokáže procesovat „budoucí stav objektu“ před vlastním procesováním pravidel nad novým objektem.
- Synchronizace identit a jejich atributů v jednotlivých spravovaných systémech s centrálním stavem identit v IdM (reconciliation)
 - Centrální úložiště identit bude implementováno pomocí databáze Metaverse. Napojení identit do Metaverse bude implementováno pomocí synchronizačních pravidel v synchronizační části.
- Vytváření workflow s více stupni schvalování a eskalací
 - Workflow budou implementovány v portálové části, budou plně customizovatelná a budou obsahovat i víceúrovňové schvalování.
- Uživatelská samoobsluha bude implementována minimálně pro správu hesla a žádosti o přiřazení role

Pro uživatele bude k dispozici IdM portál, na kterém budou schopni zadávat svoje požadavky (v případě managerů i požadavky schvalovat). Požadavky zahrnují změnu atributů uživatele (například adresa), nebo členství ve skupině (tj. role).

Produkční prostředí

V produkčním prostředí budou pro implementaci FIM použity celkově čtyři servery. Pro databázovou vrstvu bude sloužit SQL Server (viz 2.3.9).

Server	Typ serveru	Umístění	Poznámka
FIM01	Virtuální počítač	DC1	FIM Synchronizace
FIM02	Virtuální počítač	DC1	FIM Service / Portál
FIM03	Virtuální počítač	DC2	FIM Synchronizace
FIM04	Virtuální počítač	DC2	FIM Service / Portál

Údaje jsou uvedeny orientačně a budou upřesněny v etapě Návrh realizace – analýza.

Testovací prostředí

V testovacím prostředí bude pro FIM použita dvojice serveru a pro databázovou vrstvu bude použit SQL Server (viz 2.3.9).

Server	Typ serveru	Umístění	Poznámka
FIM01	Virtuální počítač	DC1	FIM Synchronizace
FIM02	Virtuální počítač	DC2	FIM Service / Portál

Údaje jsou uvedeny orientačně a budou upřesněny v etapě Návrh realizace – analýza.

2.3.3 MICROSOFT EXCHANGE

Kapitola obsahuje popis nasazení Microsoft Exchange podle požadavku Přílohy č. 6 Zadávací dokumentace v kapitole 2.4.1.

Implementace Microsoft Exchange bude dodržovat všechny požadavky na vysoce dostupný a bezpečný provoz. Pro instalaci bude použita verze Microsoft Exchange Server 2013 SP1. Exchange bude instalován do produkčního i testovacího prostředí, a to jak servery role Mailbox Server (MBS), tak Client Acces Server (CAS) v režimu aktiv - aktiv a jejich počet navrhne uchazeč v souladu s navrženou architekturou systému. Pro roli MBS bude použita licence Enterprise z důvodu rozdělení na dostatečný počet databází.

Jako podklad pro nabídku byly použity informace obsažené v Zadávací dokumentaci a Dodatečných informacích. Systém je s ohledem na požadavek rozšíření bez dodatečných nákladů dimenzován na plný počet schránek.

2.3.3.1 Klientský přístup

Požadovaná verze Exchange podporuje klientský přístup:

- Microsoft Outlook a Entourage
- Webový přístup
- Mobilní klient

Microsoft Outlook

Microsoft Outlook je nativním klientem Microsoft Exchange a podporovány jsou všechny požadované funkcionality. Dostupná funkcionality v závislosti na verzi CAL viz Tabulka 7.

Tabulka 7: Funkcionality Outlook podle CAL

Licence	Standard CAL	Enterprise CAL
Email, calendar, contacts, and tasks	Ano	Ano
Outlook Web App (Internet Explorer, Firefox, Chrome, and Safari support)	Ano	Ano
Rich Outlook inbox experience, including enhanced conversation view and MailTips	Ano	Ano
Apps for Outlook and Outlook Web App	Ano	Ano
Site mailboxes*	Ano	Ano
Role-based access control (RBAC) capabilities	Ano	Ano
Federated calendar sharing	Ano	Ano
Exchange ActiveSync mobile management policies	Standard	Advanced
Journaling	Per database	Per user / distribution list
Journal decryption	Ne	Ano
Unified Messaging	Ne	Ano
Retention policies	Default	Custom
In-Place Archive*	Ne	Ano

Multi-mailbox search	Ano	Ano
In-Place Hold	Ne	Ano
Data Loss Prevention (DLP)*	Ne	Ano
Information protection and control (IPC): transport protection rules, Outlook protection rules, Information Rights Management (IRM) search	Ne	Ano

* Vyžaduje specifickou verzi Outlook

Webový přístup

Webový přístup k mailboxu je k dispozici formou Outlook Web App. Podporované prohlížeče jsou:

- Microsoft Internet Explorer 7 a vyšší
- Firefox 17 a vyšší
- Chrome 24 a vyšší
- Safari 5 a vyšší

Přístup z interní sítě MPSV bude umožněn prostřednictvím CAS serverů, přístup ze sítě Internet bez použití dodatečné VPN bude umožněn prostřednictvím publikace prostřednictvím serverů s rolí Internet Information Server a modulem Application Request Routing nebo rolí Web Application Proxy (bude upřesněno v etapě Návrh realizace – analýza).

Mobilní klient

Mobilním klientem je myšleno komunikační zařízení (chytrý mobilní telefon, tablet) využívající operační systém Android, iOS nebo Windows Phone.

Přístup k poštovní schránce z mobilních zařízení bude umožněn jak v rámci sítě MPSV, tak ze sítě Internet a to bez použití dodatečné VPN s podporou protokolů:

- Active Sync
- POP3 / IMAP / SMTP

Systém bude v souladu s požadavky Zadavatele podporovat minimálně tři politiky zabezpečení pro mobilní klienty:

- Vysoké zabezpečení – mobilní zařízení musí podporovat šifrování svého úložiště a umožnit automatické uzamykání telefonu při stanovené době nečinnosti. Komunikace probíhá za pomoci protokolu ActiveSync. Protokol IMAP, POP3 není povolen.
- Standardní zabezpečení – mobilní zařízení schopné komunikovat s poštovním serverem v rámci protokolu ActiveSync a umožnit automatické zamykání telefonu při stanovené době nečinnosti. Komunikace probíhá za pomoci protokolu ActiveSync.
- Nízké zabezpečení – mobilní zařízení není schopno akceptovat jakoukoliv politiku zabezpečení. Komunikace může probíhat za pomoci protokolu IMAP, POP3.

Tyto politiky budou zabezpečeny nativními prostředky Exchange.

Metodika přiřazení jednotlivých politik zabezpečení konkrétním uživatelům bude definována Zadavatelem.

2.3.3.2 Serverová infrastruktura

Servery Microsoft Exchange budou implementovány s oddělením rolí (Single Role), tj. pro MBS a CAS nebudou instalovány na stejný server.

Po implementaci serverové infrastruktury budou provedeny výkonostní testy prostřednictvím standardních nástrojů výrobce, tj. Microsoft Exchange Server Jetstress 2013.

Následující návrh může být v etapě Návrh realizace upřesněn.

Role MBS

Pro zajištění možnosti použít dostatečný počet databází bude na servery v produkčním prostředí instalována verze Microsoft Exchange Server 2013 SP1 Enterprise. V testovacím prostředí je navrženo použít pro MBS roli verze Microsoft Exchange Server 2013 SP1 Standard.

Servery budou propojeny pro zachování vysoké dostupnosti prostřednictvím technologie DAG.

V produkčním prostředí bude mít každá databáze s mailboxy celkem čtyři kopie, rozdělené po dvou do datového centra, jedna z databází bude mít odložený zápis. Podle doporučení výrobce není v tomto případě třeba databáze zálohovat, při této konfiguraci jsou data ochráněna mechanismy Exchange. Tím je umožněno se vyhnout zátěži při zálohování a prodlevě v případě nutnosti obnovy.

V testovacím prostředí bude mít každá databáze s mailboxy dvě kopie, po jedné v každém datovém centru.

Role CAS

Bude instalována verze Microsoft Exchange Server 2013 SP1 Standard v kombinaci s rolí Network Load Balancing operačního systému pro zajištění vysoké dostupnosti.

Publikace do Internetu

Pro publikaci služeb Exchange do Internetu bude využita role operačního systému Internet Information Server a modulem Application Request Routing nebo rolí Web Application Proxy (bude upřesněno v etapě Návrh realizace – analýza) v kombinaci s rolí Network Load Balancing operačního systému pro zajištění vysoké dostupnosti.

Produkční prostředí

Pro implementaci role MBS jsou z důvodu výkonosti a očekávaného požadavku na velikost databází navrženy fyzické servery s lokálním JBOD datovým úložištěm. Celkem je navrženo použít v produkčním prostředí deset fyzických a deset virtuálních serverů, rozdělených symetricky mezi obě datová centra.

Server	Typ serveru	Umístění	Poznámka
EXM01	Fyzický HW	DC1	Exchange MBS
EXM02	Fyzický HW	DC1	Exchange MBS
EXM03	Fyzický HW	DC1	Exchange MBS
EXM04	Fyzický HW	DC1	Exchange MBS
EXM05	Fyzický HW	DC1	Exchange MBS
EXM06	Fyzický HW	DC2	Exchange MBS
EXM07	Fyzický HW	DC2	Exchange MBS
EXM08	Fyzický HW	DC2	Exchange MBS
EXM09	Fyzický HW	DC2	Exchange MBS
EXM10	Fyzický HW	DC2	Exchange MBS

EXC01	Virtuální počítač	DC1	Exchange CAS, NLB CAS
EXC02	Virtuální počítač	DC1	Exchange CAS, NLB CAS
EXC03	Virtuální počítač	DC1	Exchange CAS, NLB CAS
EXC04	Virtuální počítač	DC2	Exchange CAS, NLB CAS
EXC05	Virtuální počítač	DC2	Exchange CAS, NLB CAS
EXC06	Virtuální počítač	DC2	Exchange CAS, NLB CAS
EXP01	Virtuální počítač	DC1	Publikace Exchange, NLB PUB
EXP02	Virtuální počítač	DC1	Publikace Exchange, NLB PUB
EXP03	Virtuální počítač	DC2	Publikace Exchange, NLB PUB
EXP04	Virtuální počítač	DC2	Publikace Exchange, NLB PUB

Údaje jsou uvedeny orientačně a budou upřesněny v etapě Návrh realizace – analýza.

Testovací prostředí

Server	Typ serveru	Umístění	Poznámka
EXM01	Virtuální počítač	DC1	Exchange MBS
EXM02	Virtuální počítač	DC1	Exchange MBS
EXM03	Virtuální počítač	DC2	Exchange MBS
EXM04	Virtuální počítač	DC2	Exchange MBS
EXC01	Virtuální počítač	DC1	Exchange CAS, NLB CAS
EXC02	Virtuální počítač	DC1	Exchange CAS, NLB CAS
EXC03	Virtuální počítač	DC2	Exchange CAS, NLB CAS
EXC04	Virtuální počítač	DC2	Exchange CAS, NLB CAS
EXP01	Virtuální počítač	DC1	Publikace Exchange, NLB PUB
EXP02	Virtuální počítač	DC1	Publikace Exchange, NLB PUB
EXP03	Virtuální počítač	DC2	Publikace Exchange, NLB PUB
EXP04	Virtuální počítač	DC2	Publikace Exchange, NLB PUB

Údaje jsou uvedeny orientačně a budou upřesněny v etapě Návrh realizace – analýza.

2.3.3.3 Migrace

V etapě Návrh realizace - analýza bude vyspecifikován seznam objektů, migrovaných z původních systémů. Zároveň bude upřesněna metoda migrace v závislosti na technologických podmínkách. Pokud nebude garantována dostupnost zdrojových systémů, bude nutné použít migraci pomocí skriptů a PST souborů (export a následně import dat z mailboxů).

2.3.4 CERTIFIKAČNÍ AUTORITA A ČIPOVÉ KARTY

Kapitola obsahuje popis nasazení PKI podle požadavku Přílohy č. 6 Zadávací dokumentace v kapitole 2.4.2.

Kapitola obsahuje popis nasazení PKI podle požadavku Zadávací dokumentace.

IMPLEMENTACE PKI

V rámci implementace PKI infrastruktury budou vybudovány:

2 hierarchie Certifikačních Autorit (zkráceně CA)

- Hierarchie PKI v provozním prostředí
- Hierarchie PKI v testovacím prostředí

Je možné, že v rámci auditu vznikne nárok na vybudování

- hierarchie pro poskytování certifikátů na algoritmu SHA-1

Hierarchie PKI bude budována jako:

1 x server v primárním datovém centru

1 x server v záložním datovém centru

Pro zajištění vysoké dostupnosti budou servery v clusteru - nativními prostředky služeb MS Server OS:

- počet uzlů clusteru: 2 uzly
- režim clusteru: Active / Passive

Servery budou sdílet:

- databázi certifikační autority
- privátní klíč certifikační autority
- list odvolaných certifikátů (CRL)

Parametry Serveru certifikační autority budou:

Server OS:	Microsoft Server 2012R2 Standard
Virtualizace:	Ano, server poběží jako virtuální v Hyper-V
Typ CA:	Kořenová–Podniková / Root-Enterprise
Algoritmus:	SHA-256 RSA
Délka klíče:	4096 bitů
Platnost:	Bude definována v rámci auditu, očekává se v rozsahu 10-30 let.

Role a oprávnění Certifikační autority:

Vzhledem k tomu, že certifikační autorita bude instalována jako podniková/Enterprise, je svázána ze službou Active Directory. Všechny role a oprávnění tedy budou definovány v rámci účtů a skupin v AD.

Seznamy odvolaných certifikátů:

Certifikační autorita bude pravidelně vydávat seznam odvolaných certifikátů, CRL, i Delta CRL. Tyto seznamy budou publikovány do:

- Active Directory
- na Interní publikační server

- na Internetový/Extranetový publikační server

Na vyjmenovaných serverech bude také dostupný samotný certifikát certifikační autority

Poskytované služby certifikační autoritou:

Vybudovaná CA bude vydávat certifikáty jak uživatelům, tak pro severy a prvky infrastruktury.

Certifikační autorita zajistí vydávání elektronických certifikátů pro subjekty budovaného prostředí:

Certifikáty budou používat algoritmus SHA-2 a budou délky 2048 bitů.

V případě existence 3 hierarchie, budou certifikáty využívat algoritmus SHA-1.

- Certifikáty pro servery
- Certifikáty pro aplikace
- Certifikáty pro uživatele
- Certifikáty pro stanice
- Certifikáty užívané pro účely interního elektronického podpisu (případně časového razítka)
- Certifikáty užívané pro šifrování elektronické pošty (email)
- Certifikáty užívané pro šifrování dokumentů

Pro každý použitý typ certifikátů bude vytvořena a nastavena šablona obsahující převážně:

- Účel certifikátu
- Platnost certifikátu
- Požadované informace obsažené v certifikátu
- Práva na skupinu v AD pro právo žádat o typ certifikátu
- Práva na skupinu v AD pro právo editovat typ certifikátu
- Budou navrženy procesy životního cyklu
- Budou popsány nástroje pro správu certifikátů.

Uživatelské certifikáty budou vydávány na čipové karty.

- Pro provoz karet bude navržen životní cyklus karet
- Dodány softwarové nástroje pro zprovoznění karet v OS.
- Dodány softwarové nástroje pro správu karet.

Dokumentace PKI:

Instalační dokumentace:

Instalační dokument bude obsahovat podrobné postupy pro zprovoznění hierarchie CA. Součástí dokumentu budou postupy pro:

- Přípravu sdíleného úložiště dat clusteru CA
- Konfiguraci hostitelských operačních systémů
- Zprovoznění clusterové vrstvy operačního systému
- Instalace certifikační služby na primárním uzlu clusteru (vč. vygenerování páru klíčů a certifikátu CA)
- Ustavení clusteru na obou uzlech CA
- Konfigurace CA v Active Directory
- Konfigurace publikačních bodů CRL a certifikátu CA (CDP/AIA), vč. publikace CRL a certifikátu CA

- Ověření funkčnosti certifikační služby a clusteru CA

Pro každý krok postupu bude specifikováno:

- Jaký nástroj je pro daný krok použit
- Která role daný krok provádí, které role na kroku participují
- Na kterém zařízení (např. na kterém uzlu clusteru) se daný krok provádí

Dle instalační dokumentace bude provedena instalace a zprovoznění CA

Provozní dokumentace:

Pro provoz hierarchie PKI budou zpracovány podrobné dokumentace.

V rámci dodané dokumentace budou podrobně rozpracována témata:

- Role a oprávnění pro správu CA
- Podmínky pro standardní provoz CA
- Podmínky pro restart CA
- Přepínání mezi uzly clusteru (plánované, neplánované)
- Vydávání CRL (automatizované, manuální i nouzové)
- Obnova certifikátu CA, distribuce nového certifikátu CA
- Zálohování CA, správa, ochrana a dostupnost záloh
- Zálohování klíčů CA
- Profylaxe CA
- Havarijní plány a postupy obnovy funkcí CA
 - Nouzové vydání a publikace CRL
 - Obnova CA po havárii, vč. obnovy ze záloh

Na základě provozní dokumentace budou pověřeni pracovníci provádět správu CA.

Součástí dodávky CA nebudou formalizované dokumenty Certifikační politiky a Certifikační prováděcí směrnice, tyto dokumenty je možné vytvořit v rámci rozvoje CA.

Postup instalace a zprovoznění CA

Na základě předem připravených postupů bude provedena instalace technického základu CA, vč. clusterové vrstvy.

Po instalaci podkladové infrastruktury bude provedena ceremonie zprovoznění CA

V testovacím prostředí bude uvedení Certifikačních Autorit do provozu méně formální, přesto budou dodrženy přesné scénáře a vyžadované role odpovídajícím pro uvedení Certifikačních Autorit v produkčním prostředí.

Ceremonie se budou účastnit osoby, nominované do příslušných rolí, včetně zástupců zadavatele.

V rámci ceremonie budou provedeny bezpečnostní úkony, především:

- instalace služby serveru AD CS
- generování klíčů CA
- vydání certifikátu CA
- ustavení clusteru CA

Výstupem operace bude funkční cluster CA, vydaný certifikát CA a CRL, vč. jejich publikace na příslušná publikační místa.

Distribuční místo pro CRL a Authority Information Access

V rámci implementace se počítá s publikováním Certifikační autority a to jak samotného certifikátu CA tak seznamu CRL jak do intranetu/interního perimetru tak do internetu/extranetu.

Pro vybudování CDP/AIA

- Bude využit webový server na platformě MS Windows Server 2012.
- Přístup k severu protokolem HTTP bude vystaven do internetu.
- Publikační server CDP bude použit také pro publikaci informací vztahujících se k certifikační autoritě, například na publikovaném portále může být vystavena certifikační politika.

Školení administrátorů CA

Bude provedeno školení pověřených administrátorů CA. Školení bude realizováno jako prezentace produktu v Microsoft PowerPoint.

V rámci školení budou předány postupy

- pro rutinní správu CA
- pro řešení problémových stavů CA

Předmětem školení budou postupy správy, v rámci nově vybudované CA, nejedná se o školení role ADCS na platformě MS Windows Server. Předpokládá se, že školení pověřených administrátorů CA bude jako navazující na produktové školení Active Directory Certificate Services.

Bude dodán eLearningový kurz ve formátu Sharable Content Object Reference Model (SCORM).

Zátěžové testy CA

Bude dodán návrh k provedení zátěžových (výkonnostních) testů budované CA. Součástí návrhu bude i seznam nástrojů a postupů k provedení zátěžových testů. Budou také uvedena oprávnění, nezbytná pro realizaci zátěžových testů.

Provedení zátěžových testů se dle informací dodaných zadavatelem bude provádět v testovacím prostředí.

Funkční testy CA

Součástí dodávky řešení bude návrh k provedení funkčních testů CA. Součástí návrhu bude i seznam nástrojů a postupů k provedení funkčních testů. Budou také uvedena oprávnění, nezbytná pro realizaci funkčních testů.

Návrh funkčních testů bude zaměřen na prověření standardních činností prováděných v rámci služeb sole CA, např.:

- Vydání certifikátu (pro všechny podporované typy certifikátů)

- Autorizace žádosti o certifikát (pro všechny podporované typy certifikátů)
- Manuální schválení žádosti o certifikát (bude-li taková šablona existovat)
- Obnova certifikátu (pro všechny typy certifikátů, u kterých to bude vyžadováno)
- Revokace certifikátu (s ověřením funkce certificate hold)
- Vydání a publikace CRL
- Provedení zálohy a obnovy CA

Pro provedení funkčních testů budou dodány skripty, kterými bude možné automatizovat provedení funkčních testů na CA, jako jsou např.:

- Vydání certifikátu (pro všechny podporované typy certifikátů)
- Autorizace žádosti o certifikát (pro všechny podporované typy certifikátů)
- Odvolání certifikátu
- Vydání a publikace CRL
- Provedení zálohy CA

IMPLEMENTACE TSA

Součástí hierarchie PKI bude implementována autorita časového razítka (TSA – Time Stamp Authority), hostovaná na platformě MS Windows Server 2012 Standard.

Hierarchie TSA bude budována jako CA a to:

- 1 x server v primárním datovém centru
- 1 x server v záložním datovém centru

Pro zajištění vysoké dostupnosti budou servery v clusteru - nativními prostředky služeb MS Server OS:

- počet uzlů clusteru: 2 uzly
- režim clusteru: Active / Passive

Servery budou sdílet:

- databázi TSA (DB razítek a žádostí o časová razítka)
- privátní klíč TSA

Parametry Serveru pro TSA autority budou:

- Server OS: Microsoft Server 2012R2 Standard
- Virtualizace: Ano, server poběží jako virtuální v Hyper-V
- Podpisové schéma: SHA-256 RSA

TSA bude implementována jako síťová služba. TSA komunikační formát protokolu bude v souladu s mezinárodním průmyslovým standardem RFC3161.

Transportním protokolem zpráv TSA bude HTTP, resp. HTTPS.

TSA není možné vybudovat nativními prostředky OS Microsoft, a bude tedy ve formě software 3 strany:

- Certifikát pro TSA vydá doménová CA.
- Pro přesný zdroj času bude využíván externí NTP server s časovou úrovní stratum 1.

V budovaném prostředí tedy bude pro všechny uživatele a aplikace domény umožněno čerpat funkce, které poskytuje služba TSA. Podmínkou bude, aby aplikace používala standardní protokol pro komunikaci vůči službě TSA.

Pro vybrané agendy s požadavkem na kvalifikované TSA bude vydávat časová razítka externí kvalifikovaná TSA.

Součástí dodávky nebude formalizovaný dokument Politika vydávání časových razítek.

Instalační dokumentace TSA:

Instalační dokument bude obsahovat podrobné postupy pro zprovoznění hierarchie TSA. Součástí dokumentu budou postupy pro:

- Přípravu sdíleného úložiště dat clusteru TSA
- Konfiguraci hostitelských operačních systémů
- Konfiguraci hostitelského aplikačního serveru
- Zprovoznění clusterové vrstvy operačního systému
- Instalaci a konfiguraci služby TSA
- Napojení na NTP server
- Ustavení clusteru na obou uzlech
- Ověření funkčnosti certifikační služby a clusteru TSA

Pro každý krok postupu bude specifikováno:

- Jaký nástroj je pro daný krok použit
- Která role daný krok provádí, které role na kroku participují
- Na kterém zařízení (např. na kterém uzlu clusteru) se krok provádí

Na základě zpracované instalační dokumentace bude následně provedena instalace a zprovoznění TSA.

Provozní dokumentace TSA

Pro provoz hierarchie TSA budou zpracovány podrobné dokumentace.

V rámci dodané dokumentace budou podrobně rozpracována témata:

- Role a oprávnění pro správu TSA
- Podmínky pro standardní provoz TSA
- Restart TSA
- Přepínání mezi uzly clusteru (plánované, neplánované)
- Konfigurace dostupnosti NTP
- Vydání certifikátu TSA a distribuce na uzly clusteru
- Zálohování TSA, správa, ochrana a dostupnost záloh
- Zálohování databáze TSA
- Profylaxe TSA
- Havarijní plány, postupy obnovy funkcí TSA

Na základě provozní dokumentace budou pověřeni pracovníci provádět správu TSA.

Postup instalace a zprovoznění TSA

Na základě předem připravených postupů bude provedena instalace technického základu TSA, vč. clusterové vrstvy. Následně budou na TSA provedeny kroky:

- Napojení na zdroj času
- Vygenerování páru klíčů a žádosti o certifikát
- Vydání a instalace certifikátu

Výstupem operace bude funkční cluster TSA.

Školení administrátoru TSA

Bude provedeno školení pověřených administrátorů TSA. Školení bude realizováno jako prezentace produktu v Microsoft PowerPoint.

V rámci školení budou předány postupy

- pro rutinní správu TSA
- pro řešení problémových stavů TSA

Předpokládá se, že školení pověřených administrátorů TSA bude jako navazující na produktové školení Administrátorů CA.

Bude dodán eLearningový kurz ve formátu Sharable Content Object Reference Model (SCORM).

Zátěžové testy TSA

Bude poskytnuta jak součinnost tak vytvořeny skripty pro zátěžové testy služby TSA.

Skripty pro funkční testování TSA

Pro automatizované testování budou dodány skripty.

SMART KARTY

Součástí řešení je dodání karet pro autentizaci uživatelů. Smart Karta je HW zařízení - čip, která pracuje s asymetrickou kryptografií. Čip umožňuje bezpečné generování a uložení privátních klíčů RSA.

Výhody Smartkaret

- Karta umožňuje dvou faktorovou autentizaci
- K přístupu na privátní klíč se musí provést autentizace vůči kartě (pin)
- Na kartě se generuje privátní klíč
- operace s privátním klíčem probíhají v čipu – klíč nemůže opustit HW
- privátní klíč uložený na kartě není možné vyexportovat
- klíče se do karty mohou importovat (například klíč z kvalifikované CA)

Dodané karty splňují standard Smart Card Minidriver Specification společnosti Microsoft, tj. mají nativní podporu v MS OS Windows Vista a novějších.

Kontaktní čip Smart Karty

Čip splňuje mezinárodní kryptografické standardy FIPS 140-2 Level 3 a CC EAL5+.

Bezkontaktní část Smart Karty

Bezkontaktní část karty se využívá u přístupových či docházkových systémech, platbách v rámci společnosti (například závodní jídelna apod.).

Čtečky karet

Dodávané karty jsou kompatibilní se čtečkami čipových karet, splňujícími standard PC/SC.

Middleware

Do OS stanic je třeba instalovat middleware pro funkce karty. Ten je ve formě instalačního balíčku MSI, který je možno instalovat pomocí instalačního průvodce, tak pomocí bezobslužné instalace vhodné pro hromadné instalace.

Podporované OS

- MS Windows XP SP3 a novějších
- Linux (oficiálně jsou podporovány jen vybrané distribuce), přes standardní rozhraní PKCS#11

Správa karet

Ke kartám bude dodán software potřebný pro:

- Přípravu na distribuci karet uživatelům
- Personifikace karet
- Vytisknutí informací pro provoz karty (Pin / Puk)
- Evidence karet v centrální aplikaci (ID karty, Typ Karty, Stav Karty aj.)
- Evidence držitele karty (Datum vydání karty, informace kdo vydal kartu, kdy byla karta vydána, aj.)

Fotografie držitelů karet

Pro tisk fotografií na těla karet je třeba do aplikace nahrát a přiřadit fotografie k účtům uživatelů, či bude načteno z AD.

Přesný způsob se upřesní v průběhu analytické fáze.

Školení administrátorů karet

Školení bude realizováno jako prezentace produktu v Microsoft PowerPoint.

Bude dodán eLearningový kurz ve formátu Sharable Content Object Reference Model (SCORM).

Plány a scénáře funkčního testování Kartového centra

Bude dodán dokument testovacích scénářů pro otestování funkcí v nově budovaném prostředí.
Očekávaná součinnost při ladění software dodavatele vůči tiskárně na potisk karet zadavatele.
Očekávaná součinnost při ladění a testech tisku přístupových údajů karty na tiskárny zadavatele.

Recyklace Smart karet

Registrační místa budou vybaveny nástroje pro recyklace karet

Hlavní úkony:

- Smazání obsahu karty
- Příprava karty pro nového uživatele

Náhradní karty

V rámci analýzy bude rozhodnuto, jak se bude řešit stav uživatele, který nemá svou kartu (možná ztráta/zapomenutí) a zda a jak budou využívány dočasné karty.

V rámci analýzy bude rozhodnuto, jak se bude řešit náhrada karty uživatele po nahlášení karty jako ztracené. Vázané při šifrovacích klíčích na key recovery.

V rámci požadavku zadavatel se očekává pro práci s certifikáty využívání nástrojů nativně v OS Microsoft.

Školení obslužného vydávání certifikátů

Bude provedeno proškolení operátorů pro vydávání certifikátů.

Bude provedeno proškolení operátorů pro vydávání obnovených certifikátů.

Školení bude realizováno jako prezentace produktu v Microsoft PowerPoint.

Bude dodán eLearningový kurz ve formátu Sharable Content Object Reference Model (SCORM).

Notifikace - zasílání e-mailů před koncem doby platnosti certifikátů

Microsoft certifikační autorita nedisponuje nativními prostředky možnosti upozornit na blížící se expiraci certifikátů. Pro zasílání e-mailových zpráv s informací o blížící se expiraci certifikátů bude do doménového prostředí implementovány programy – skripty které tuto vlastnost poskytnou.

Skripty budou umět notifikovat jak konkrétní uživatele, na základě informace uvedeného emailu ve vlastnostech certifikátů, tak na základě šablony například pro správce serverů.

Držitelé si tak mohou naplánovat obnovení svých certifikátů ještě před vypršením jejich platnosti.

E-mailové zprávy držitelům certifikátů odesílá skript prostřednictvím SMTP serveru jako emailové upozornění.

Požadavky na fungování

Skripty je možné provozovat na operačním systému Server 2012R2. Hostitelský server musí být členem domény a musí mít přístup na email server. Skript bude spouštěn pod servisním účtem.

Způsob dodání a implementace

Skript bude zprovozněn na serverech CA, Instalace proto bude dodána formou:

- Vzorový konfigurační soubor
- Postup instalace / konfigurace.

Plány a scénáře funkčního testování zasilání e-mailů expirace certifikátů

Bude dodán dokument testovacích scénářů pro otestování funkcí v nově budovaném prostředí.

Skripty pro funkční testování zasilání e-mailů expirace certifikátů

Pro automatizované testování budou dodány skripty.

Typy certifikátů

Interní CA bude mít za úkol vydávat jak serverové certifikáty, tak certifikáty pro prvky infrastruktury a aplikace.

Interní CA bude mít za úkol vydávat uživatelské certifikáty.

Žádosti o certifikáty

Pro doménové stanice jak servery, tak i pracovní stanice bude nastaveno automatické vydávání a obnova certifikátů.

V rámci analýzy bude rozhodnuto, jak se bude přistupovat k jednotlivým typům certifikátů, procesů jejich schvalování operátory a způsobů vystavení.

Součástí řešení bude zdokumentování procesů správy a vydávání certifikátů.

Návrh životního cyklu certifikátů, vydávaných z interní CA

V rámci analýzy bude pro jednotlivé typy certifikátů navržen a zdokumentován životní cyklus.

Návrh správy a životního cyklu uživatelských certifikátů bude dodán jak v dokumentaci, tak bude dodán i formalizovaný do UML2.

Podpora stávajících karet

Stávající čipové karty tip Gemalto TOP IM GX4, Gemalto TOP HM GX4, v aktuálním prostředí zadavatele, budou využívány i v novém prostředí.

Zprovoznění Smartcard Logon do domény

V doménových Active Directory budou konfigurovány parametry, které v doméně aktivují podporu pro autentizaci čipovou kartou (Smartcard Logon).

Cílem nastavení prostředí s podporou smart karet je umožnit uživatelům autentizace do domény, s využitím certifikátu v kontaktní části čipu karty.

Další kroky:

V rámci analytické fáze budou navrženy:

- Šablony certifikátů - objekt v AD
- Návrh životního cyklu karet
- Návrh životního cyklu certifikátů, vydaných z externí CA
- Import držitelů karet do docházkového systému
- Integrace s ostatními systémy

Návrhy budou dodány jak v dokumentaci, tak budou dodány i formalizovaný do formátu UML2.

Monitoring / dohled

Monitoring bude sledovat dostupnost provozovaných služeb v rámci požadavků zadavatele v rozsahu ZD. V rámci analýzy bude Monitoring upřesněn.

Zálohování

V průběhu analýzy bude upřesněn mechanismus zálohování a ukládání záloh. Pro rozsah zálohování se počítá hlavně se zálohováním databáze certifikační autority.

Auditní záznamy o přístupech

Na servery s rolí ADCS bude aplikována politika zvýšeného logování událostí služby pomocí politik GPO řízených z AD.

Provoz systému

Dokončením funkčních testů a po akceptaci systému bude oprávněným pracovníkům předáno vše potřebné pro provoz prostředí. Potřebné účty, hesla, piny karet apod.

Akceptační testování systému

Seznam akceptačních bodů jako i testovací scénáře budou součástí dodávky.

Migrace dat informací Smart karet ze stávajícího prostředí

Do nového prostředí to systému správy karet budou přesunuta data ze stávající programu.

V rámci budování se počítá s minimální součinností zadavatele, pro migraci je tato součinnost však nezbytná.

- Zadavatel dodá informaci k tiskárnám vztahující se na podporu potisku Smart karet.
 - Zapůjčí dokumentaci k používaným tiskárnám.
 - Umožní provedení testů tiskáren – zkušební tisky
- Zajistí v digitální formě fotografie uživatelů nutné pro personifikace čipových karet, akceptován je i kontejner AD obsahující fotografie uživatelů.
- V průběhu analýzy bude upřesněn postup a časový plán migrace.

Ostatní požadavky na součinnost jsou v samostatné kapitole tohoto dokumentu „Požadavky na součinnost zadavatele“.

Produkční prostředí

Pro implementaci role AD CS je navrženo použít v produkčním prostředí deset virtuálních serverů, z důvodu nasazení jako Failover Clustering služeb pro vysokou dostupnost.

Server	Typ serveru	Umístění	Poznámka
CA01	Virtuální počítač	DC1	SHA2 Provoz
CA02	Virtuální počítač	DC1	SHA1 Provoz
CA03	Virtuální počítač	DC1	TSA
CA04	Virtuální počítač	DC1	Internal CA Services
CA05	Virtuální počítač	DC1	External CA Services
CA06	Virtuální počítač	DC2	SHA2 Provoz
CA07	Virtuální počítač	DC2	SHA1
CA08	Virtuální počítač	DC2	TSA
CA09	Virtuální počítač	DC2	Internal CA Services
CA10	Virtuální počítač	DC2	External CA Services

Údaje jsou uvedeny orientačně a budou upřesněny v etapě Návrh realizace – analýza.

Testovací prostředí

Pro implementaci role AD CS je navrženo použít v testovacím prostředí deset virtuálních serverů, z důvodu nasazení jako Failover Clustering služeb pro vysokou dostupnost odpovídající provoznímu prostředí.

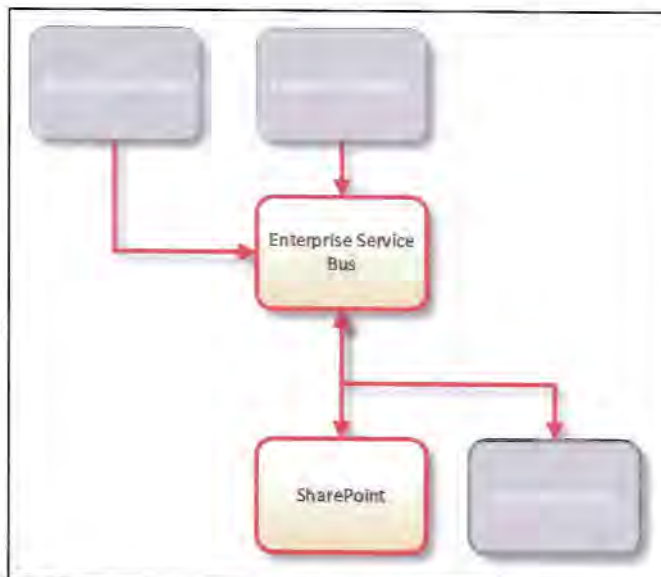
Server	Typ serveru	Umístění	Poznámka
CA01	Virtuální počítač	DC1	SHA2 Provoz
CA02	Virtuální počítač	DC1	SHA1 Provoz
CA03	Virtuální počítač	DC1	TSA
CA04	Virtuální počítač	DC1	Internal CA Services
CA05	Virtuální počítač	DC1	External CA Services

CA06	Virtuální počítač	DC2	SHA2 Provoz
CA07	Virtuální počítač	DC2	SHA1
CA08	Virtuální počítač	DC2	TSA
CA09	Virtuální počítač	DC2	Internal CA Services
CA10	Virtuální počítač	DC2	External CA Services

Údaje jsou uvedeny orientačně a budou upřesněny v etapě Návrh realizace – analýza.

2.3.5 ESB – ENTERPRISE SERVICE BUS

Kapitola obsahuje popis nasazení Microsoft BizTalk podle požadavku Přílohy č. 6 Zadávací dokumentace v kapitole 2.4.3.

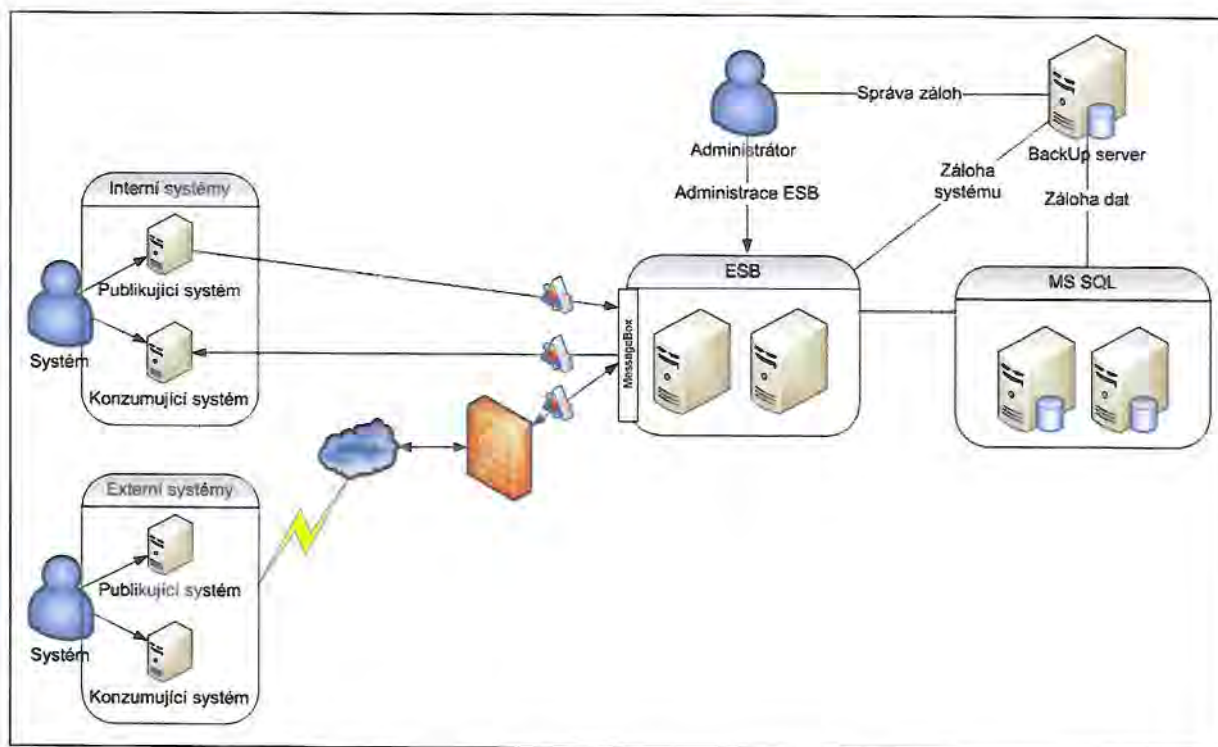


Obrázek 4 – Implementace ESB

2.3.5.1 Návrh funkčního řešení ESB

Cílová architektura JISPSV je postavena na oddělených systémech, které jsou mezi sebou propojeny prostřednictvím ESB. ESB má funkci centrální integrační platformy pro výměnu dat mezi jednotlivými systémy. Tato integrace bude pouze v odůvodněných případech doplněna dalšími způsoby komunikace (souborový přenos,...). ESB poskytuje jednotnou platformu pro integraci všech aplikací portfolia JISPSV. JISPSV-PIP ESB bude integrovat interní aplikace a bude také zajišťovat integraci s externími aplikacemi jiných úřadů, ministerstev a ostatních dotčených OVM.

- Navrhovaná integrační architektura bude umožňovat následující funkčnost:
 - Sdílení/výměnu dat, souborů a zpráv
 - v případě potřeby bude provádět též konverze protokolů
- Poskytování, sdílení, kompozici služeb
 - služby servisní sběrnice
 - integrace API
- Otevřenost
 - integrace stávajících interních a externích systémů (dle Návrhu realizace)
 - integrace nově vznikajících aplikací



Obrázek 5 – Návrh konceptu architektury ESB

ESB bude v rámci jedné lokality provozována na dvou serverech zapojených do balancovaného propojení (Microsoft Network Load Balancing), který zajistí jak rozložení zátěže, tak odolnost proti výpadkům (failover). Jako databáze bude použit MS SQL Server, který bude provozován v active/passive failover clusteru (Microsoft Cluster Services), který zajistí odolnost proti výpadkům. Jako workflow pro interakci s aplikacemi bude použita interní orchestrace MS BizTalk. S interními integrovanými systémy bude ESB komunikovat po síti napřímo, s externími systémy přes výstupní bránu. Druhá lokalita bude řešena analogicky.

ESB bude provedeno jako centrální uzel (integrační platforma), která zabezpečí výměnu dat mezi systémy (Publikující x Konzumující). Tyto integrované IS budou mít s vysokou pravděpodobností různé vstupní / výstupní formáty datových struktur, kódování, případně struktury samotné. ESB, tak jak bude postupně tvořeno, bude integrovat ty systémy, které projdou důkladnou analýzou požadavků a datových struktur. Pro jednotlivé typy dat bude navržen základní (normalizovaný) formát, který bude v rámci ESB ve všech výstupních strukturách definován jako defaultní. Tento formát bude možno pro vybrané systémy změnit, ale pouze po dohodě a potvrzení analýzou. Tím bude zachována opakovaná použitelnost datových formátů, jejich neměnnost v čase při interním zpracování v ESB a ESB bude tedy poskytovat univerzální šablonu pro každý formát.

Pokud bude integrovaný systém vyžadovat jiný formát (příkladem je typ Datum a čas, DateTime, který bude pravděpodobně požadován v různých formátech), při zpracování v ESB bude tento jiný formát v rámci vstupní/výstupní fronty konvertován do/z normalizovaného formátu. Interně bude ESB zpracovávat pouze normalizovaný formát. Při návrhu nového integračního propojení bude preferováno použití normalizovaného formátu.

Navržené řešení předpokládá existenci tzv. ESB farmy, ve které je sdruženo více na sobě nezávislých ESB uzlů (server BizTalk), které lze libovolně škálovat dle potřeby. Ty komunikují s frontou (MessageBox) do které jsou zapsány požadavky (zprávy) k vyřízení, které odeslaly Publikující systémy

a zároveň z ní získávají, odesílají, zprávy do Konzumujících systémů. Mezi přijetím a odesláním zprávy probíhá orchestrace veškerého procesního toku potřebného k zajištění správné funkcionality ESB.

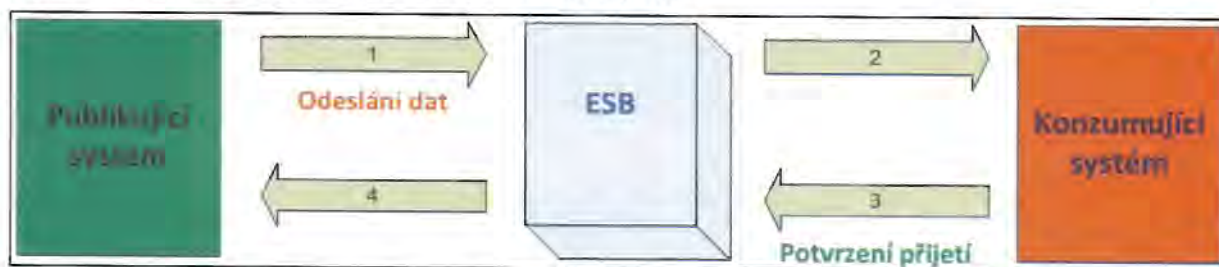
Databázové servery budou (dle nastavení) ukládat data, která jsou obsahem zpráv a to jak před překladem, tak i po překladu, před odesláním do Konzumujícího systému. Toto logování (protokolování dat) bude řešeno na základě výstupů fáze Návrh realizace pro každou integraci zvlášť.

Vlastní logování ESB lze rozdělit na logování systému (audit uživatelů, zdroje, obsazenost disků, počet aktivních zpráv ve frontě, atd.), logování jednotlivých služeb, zpráv (počet, čas volání, doba odezvy, velikost zprávy, atp.) a transakční logy (logování transakcí), které jsou nejnáročnější. Nastavení úrovně logování je pro každý typ logu jiné a bude řešeno v rámci dodávky samotné.

2.3.5.2 Principy komunikačních kontraktů

Pro celkové pochopení, jak modul ESB bude pracovat, je doplněn popis principů komunikačních kontraktů a životního cyklu zprávy, včetně jejího vyvolání uživatelem.

Z pohledu systému ESB převládají dva typy komunikace. První typ je založen na předpokladu, že akci vyvolá Publikující systém, který první zprávou pošle data Konzumujícímu systému. Konzumující systém přijatá data zpracuje a potvrdí jejich přijetí druhou zprávou



Obrázek 6 – Komunikační kontrakt I. typu

Druhý typ komunikace je založen na tom, že Konzumující systém vyšle první zprávu, kterou žádá o data. Publikující systém zprávu (žádost) přijme, a pokud je validní, oprávněná, odešle odpovídající data druhou zprávou do Konzumujícího systému.



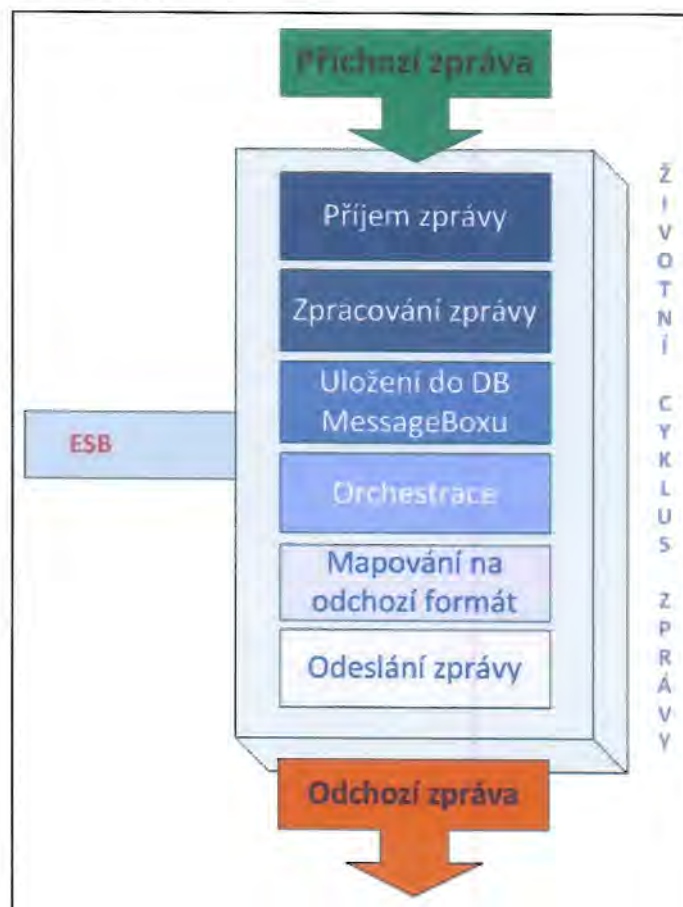
Obrázek 7 – Komunikační kontrakt II. typu

Životní cyklus zprávy po dobu průchodu ESB

Odesílající systém (konzumující nebo publikující) odesílá zprávu (informaci, data, soubor) jinému přijímajícímu systému. Za zprávu tedy považujeme i žádost o data, případně potvrzení přijetí.

1. Odesílající systém volá službu ESB, která je pro něj určena na předem známé adrese a s danou strukturou dat (rozhraní)
2. Systém ESB přijímá zprávu na předem známé adrese
3. ESB provede na svém vstupu tyto operace (*nemusí však nutně všechny*)
 - a) Datová normalizace – převod jiných datových formátů do XML

- b) Datová transformace – XSLT
 - c) Extrakce a vkládání vlastností
 - d) Agregace a rozdělování (např. součet dvou hodnot do jiné, sjednocení řetězců, transformace struktury do jemnější podoby, apod.)
 - e) Kódování a dekódování (změna znakové sady)
 - f) Šifrování a dešifrování
 - g) Podepisování a ověřování podpisů/časových razítek
4. Odeslání zpracované zprávy do zásobníku zpráv (SQL databáze – tzv. MessageBox)
 5. ESB si vyzvedne zprávu a provádí nad ní orchestraci workflow (odesílá maily, kontroluje, atp.)
 6. ESB provede konverzi na odchozí typ zprávy (např. do souboru, XML, atd.)
 7. ESB odesílá zprávu přijímajícímu systému na předem známou adresu s danou strukturou dat
 8. Přijímající systém zprávu zpracuje, případně odešle odpověď (odpověď pak může absolvovat stejný životní cyklus zprávy)



Obrázek 8 – Životní cyklus zprávy

Systém ESB takto provedl přesun zprávy ze systému A do systému B včetně její transformace do odpovídající struktury. Takto lze přenášet i soubory ze systému SharePoint do jiného systému.

Navržené řešení, jeho modularita a celistvost vychází z technologií, které jsou dodávány jedním výrobcem. Tím je minimalizována hrozba nekonzistence mezi jednotlivými částmi – ESB, aplikační server, databáze.

2.3.5.3 Technologický pohled na řešení ESB

Navržené řešení je založeno na postupném doplňování jednotlivých integrovaných systémů po jejich důkladné analýze. Z tohoto konstatování vyplývá, že se ihned od návrhu počítá s modulárním systémem, který bude nejen postupně růst, ale který bude umět využívat již existující služby a business řešení k pokrytí nových integrací a požadavků z nich plynoucích.

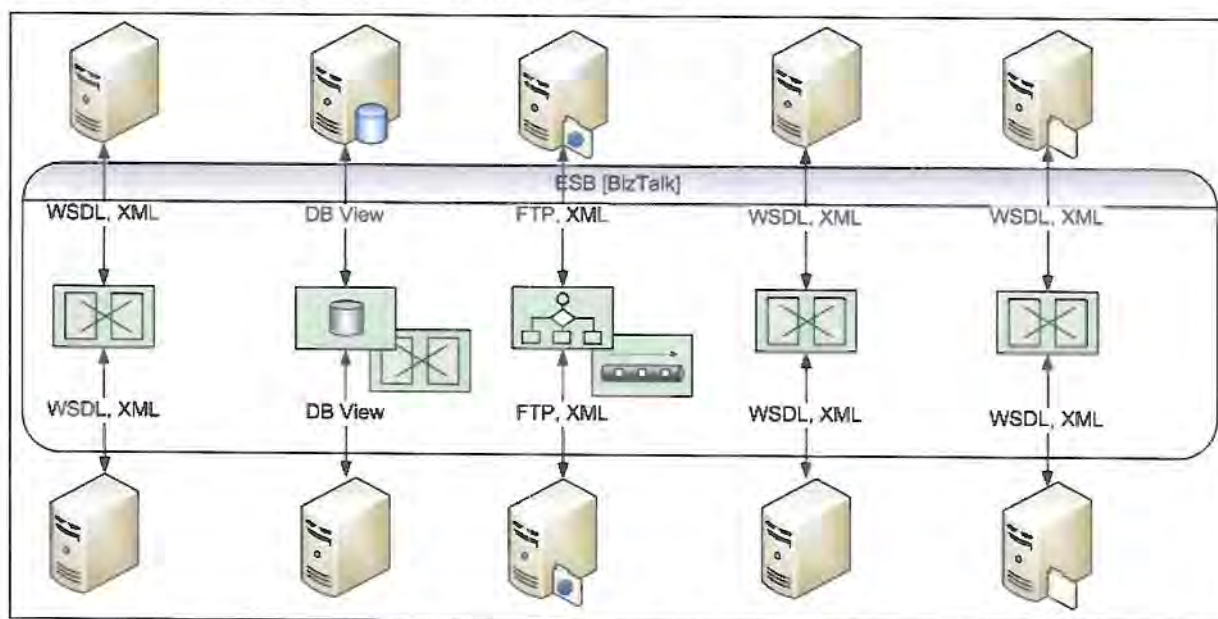
Z technologického pohledu jsou systémy integrované založeny na následujících platformách:

Druh integrace	Formát dat
Web services	WSDL, XML na HTTPs
Přístup do DB pomocí PL SQL	DB View data
FTP	XML na FTPs protokolu

Tabulka 8 – Seznam druhů integrací

Z pohledu jednotlivých druhů bude každý integrovaný systém proveden pomocí samostatného rozhraní, které bude pomocí ESB komunikovat s oběma integrovanými systémy (Publikující a Konzumující systém). Přenášená data, datové struktury, soubory se budou v rámci logování ukládat před samotnou transformací do cílové aplikace pro možnost zobrazení výchozích dat.

Na následujícím obrázku je uvedeno blokové schéma řešení.



Obrázek 9 – Konceptuální model ESB

Pro každou novou integraci se předpokládá analýza stávajícího řešení, procesů, struktur dat určených pro přenos a vytvoření nových integračních rozhraní umožňujících přenos dat mezi spolupracujícími systémy.

2.3.5.4 Integrované systémy

Na základě informací dostupných v době odevzdání nabídky bude integrováno prostřednictvím ESB 10 systémů. Další pak budou řešeny v rámci správy systému.

Pro každý integrovaný systém bude v rámci fáze Návrh realizace provedena detailní analýza požadavků na proces toku požadavků a dále na strukturu požadovaných dat a jejich formátů. Po této fázi bude zahájena realizace integrační části, které bude implementována do prostředí JISPSV-PIP.

2.3.5.5 Serverové prostředí ESB

Prostředí v této kapitole nezahrnuje MS SQL Server, ten je specifikován centrálně v kapitole 2.3.9. Veškeré údaje jsou uvedeny orientačně a budou upřesněny v etapě Návrh realizace.

Produkční prostředí

Server	Typ serveru	Umístění	Poznámka
ESB11	Virtuální počítač	DC1	MS BizTalk Node 1 DC1
ESB12	Virtuální počítač	DC1	MS BizTalk Node 2 DC1
ESB21	Virtuální počítač	DC2	MS BizTalk Node 1 DC2
ESB22	Virtuální počítač	DC2	MS BizTalk Node 3 DC2

Testovací prostředí

Server	Typ serveru	Umístění	Poznámka
ESB11	Virtuální počítač	DC1	MS BizTalk DC1
ESB21	Virtuální počítač	DC2	MS BizTalk DC2

Vývojové prostředí

Server	Typ serveru	Umístění	Poznámka
ESBDev	Virtuální počítač	–	MS BizTalk MS Visual Studio Professional

2.3.5.6 Cena připojení jednoho každého dalšího systému

Cena připojení jednoho každého dalšího systému je 550 000,- Kč bez DPH.

2.3.6 MICROSOFT SHAREPOINT SERVER (DMS)

Kapitola obsahuje popis nasazení Microsoft SharePoint podle požadavku Přílohy č. 6 Zadávací dokumentace v kapitole 2.4.1.

DMS úložiště bude použito pro ukládání digitálních dokumentů a dat z dalších aplikací jako je např. spisová služba. SharePoint budou na základě oprávnění využívat i koncoví uživatelé. DMS zajistí jak uložení, tak přístup k dokumentům, a to včetně zachování jejich důvěryhodnosti. DMS zajistí pro elektronické systémy spisové služby službu fyzického úložiště datových souborů s digitálními dokumenty, tak služby pro uložení dokumentů, jež nejsou spravovány v rámci ESS

DMS bude obsahovat **integrační rozhraní** pro komunikaci se systémy JISPSV přímo nebo prostřednictvím ESB pomocí specializované integrační komponenty viz kapitola Integrace na okolní systémy.

Předpokladem naší nabídky je řešení postavené na platformě SharePoint 2013 server, která bude poskytovat následující klíčové funkčnosti:

- systémové řízení dokumentů,
- uživatelské řízení dokumentů,
- řízení práv přístupu,
- audit přístupu,
- archivace dokumentů,
- razítkování dokumentů časovou značkou,
- podepisování dokumentů elektronickým podpisem.
- služby sdíleného úložiště poskytujícího technologické prostředky pro ukládání binárních dat dokumentové povahy,
- Office Web Apps,
- Indexování (podporovány budou dokumenty MS Office a PDF) a vyhledávání v obsahu nebo dokumentů,
- Workflow 2010, Workflow 2013

Veškeré výše popsané funkčnosti budou využívat v maximální míře standardní funkcionalitu platformy SharePoint. Pouze v případech, kdy platforma tuto funkcionalitu neobsahuje, bude tato doplněna vyvinutou komponentou, která bude do SharePointu doplněna jako samostatný funkční balíček.

Prostředí v této kapitole nezahrnuje MS SQL Server, ten je specifikován centrálně v kapitole 2.3.99. Veškeré údaje jsou uvedeny orientačně a budou upřesněny v etapě Návrh realizace.

2.3.6.1 Produkční prostředí

Pro zajištění vysoké dostupnosti a potřebného výkonu bude SharePoint nasazen jako farma složená z více serverů ve čtyřvrstvé architektuře:

- Front end pro obsluhu primárních uživatelských dotazů s nastaveným load balancingem.
- Aplikační front end pro napojené systémy, které budou používat SharePoint jako úložiště dokumentů.
- Search Front end dedikované pro vyhledávání.
- Search Back end pro provoz vyhledávacího subsystému.
- Back end pro provoz podpůrných služeb.

Data budou uložena v SQL databázi v oddělených instancích s alokovaným diskovým prostorem. Diskový prostor každé instance bude rozdělen na tři části:

- Data – soubory MDF uživatelských a systémových databází.
- TempDB – soubory MDF TempDB databázi.
- Logy – Soubory LDF všech databází

Vzhledem k požadavkům dle zadávací dokumentace bude SharePoint farma provozována na 10 serverech ve čtyřvrstvé architektuře. Toto prostředí bude doplněné o 2 servery Office web apps.

Na základě požadavků na kapacitu a vysokou dostupnost v klíčových komponentách včetně workflow a vyhledávání, navrhujeme následující serverovou konfiguraci:

SharePoint Farma:

- 2x SharePoint Web Front End
- 2x SharePoint Application Web Front End
- 2x SharePoint Search Front End
- 2x SharePoint Search Back End
- 2x SharePoint Back End

Důvěryhodné úložiště:

- 2x Front End důvěryhodný archiv

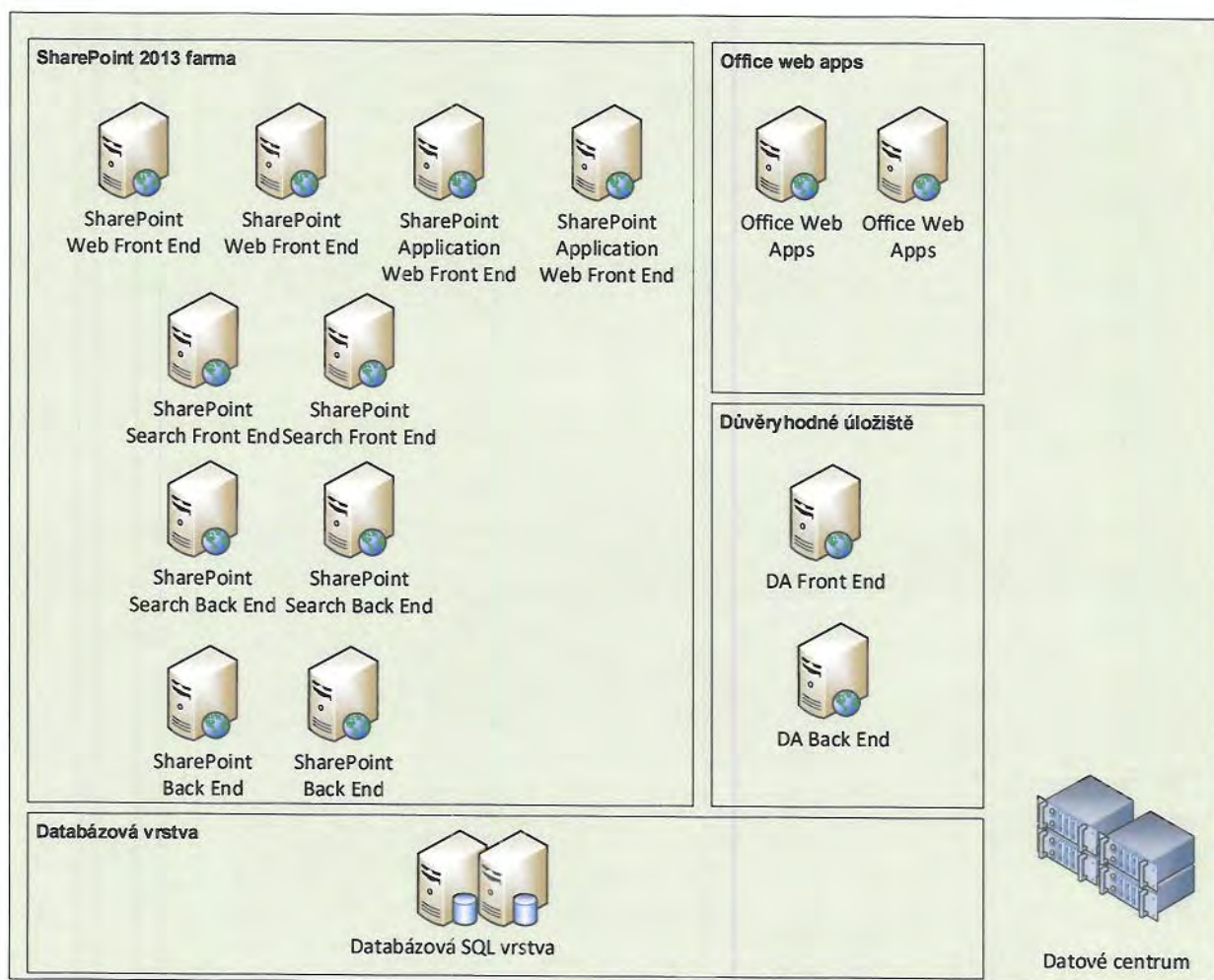
Office Web Apps (OWA) farma:

- 2x Office Web Apps 2013 Server

Servery SharePoint a Office Web Apps navrhujeme jako virtualizované na virtualizační platformě v následující konfiguraci:

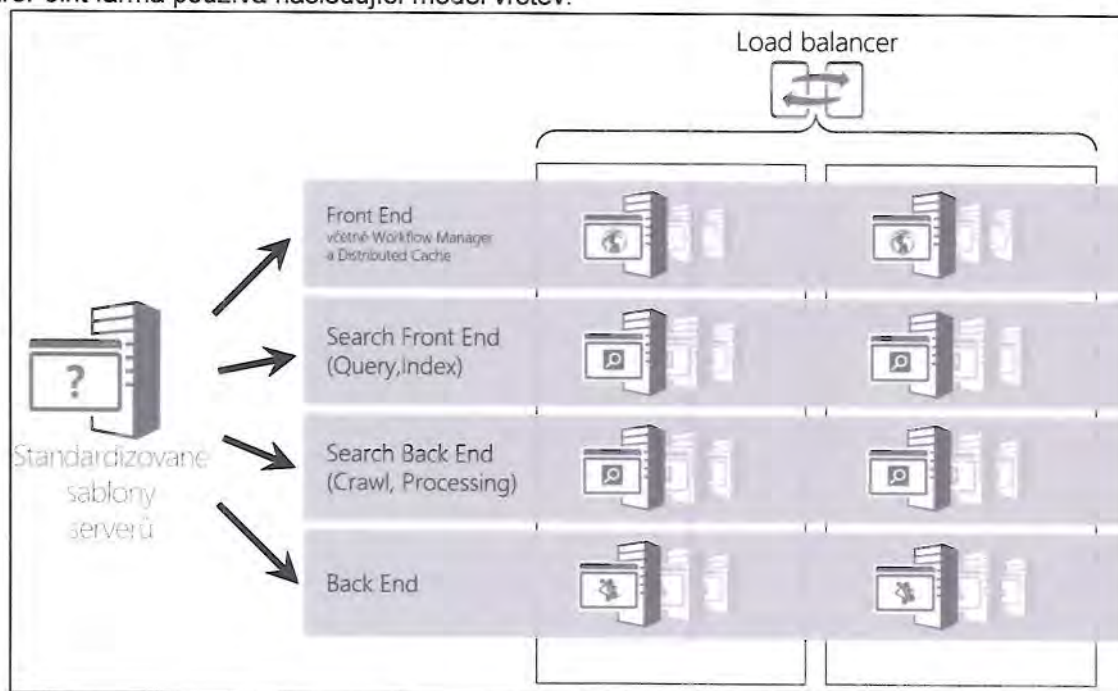
- OS: Windows Server 2012 R2
- CPU: 8 jader
- RAM: 24 GB
- Disk: 200 GB
- Disk 2:
 - role SharePoint Search Front End: 250 GB
 - role SharePoint Search Back End: 150 GB

Navrhovaná architektura produkčního prostředí je shrnuta na následujícím obrázku.



Obrázek 10 – DMS architektura produkčního prostředí

SharePoint farma používá následující model vrstev:



Obrázek 11 – Vrstvy SharePoint farmy

Vrstva Front End a Application Front End

Téma	Popis
Popis vrstvy	Servery v této vrstvě odpovídají na webové dotazy uživatelů a služeb a poskytují služby Distributed Cache.
Služby na serveru	Následující služby běží na serverech této vrstvy: Access Database Service 2010* App Management Service Application Discovery and Load Balancer Service Business Data Connectivity Service Claims to Windows Token Service Excel Calculation Service* Performance Point Service* Managed Metadata Service Microsoft SharePoint Foundation Sandboxed Code Service Microsoft SharePoint Foundation Subscription Settings Service Microsoft SharePoint Foundation Workflow Timer Service Microsoft SharePoint Foundation Web Application Search Query and Site Settings Service Secure Store Service User Profile Service Visio Graphics Service (pouze v případě SharePoint Enterprise verze) Distributed Cache
Komponenty na serveru	Následující komponenty běží na serverech této vrstvy: Workflow Manager Workflow Client

Tabulka 9 – Vrstva Front End a Application Front End

Vrstva Search Front End

Téma	Popis
Popis vrstvy	Servery v této vrstvě provozují vyhledávací komponenty Query Processing a Index.
Komponenty na serveru	Následující komponenty běží na serverech této vrstvy: Query Processing Index
Služby na serveru	Následující služby běží na serverech této vrstvy: Search Host Controller Service Search Query and Site Settings Service SharePoint Server Search

Tabulka 10 – Vrstva Search Front End

Vrstva Search Back End

Téma	Popis
Popis vrstvy	Servery v této vrstvě provozují vyhledávací komponenty Admin, Crawl, Analytical Processing a Content Processing.
Komponenty na serveru	Následující komponenty běží na serverech této vrstvy: Admin Crawl Analytical Content Processing
Služby na serveru	Následující služby běží na serverech této vrstvy: Search Host Controller Service Search Query and Site Settings Service SharePoint Server Search

Tabulka 11 – Vrstva Search Back End

Vrstva Back End

Téma	Popis
Popis vrstvy	Aplikační vrstva se servery hostujícími servisní aplikace.
Služby na serveru	Následující služby běží na serverech této vrstvy: User Profile Synchronization Central Administration Word Automation Services Work Management Service Machine Translation Service Microsoft SharePoint Foundation Incoming E-Mail Microsoft SharePoint Foundation Workflow Timer Service Search Host Controller Service (pro účely konfigurace) SharePoint Server Search (pro účely konfigurace) Document Conversions Launcher Service Document Conversions Load Balancer Service

Tabulka 12 – Vrstva Back End

Server	Typ serveru	Umístění	Poznámka
SPWFE1	Virtuální počítač	DC1	SharePoint Web Front End
SPWFE2	Virtuální počítač	DC2	SharePoint Web Front End
SPWFE3	Virtuální počítač	DC1	SharePoint Application Web Front End
SPWFE4	Virtuální počítač	DC2	SharePoint Application Web Front End

Server	Typ serveru	Umístění	Poznámka
SPSFE1	Virtuální počítač	DC1	SharePoint Search Front End
SPSFE2	Virtuální počítač	DC2	SharePoint Search Front End
SPSBE1	Virtuální počítač	DC1	SharePoint Search Back End
SPSBE2	Virtuální počítač	DC2	SharePoint Search Back End
SPBE1	Virtuální počítač	DC1	SharePoint Back End
SPBE2	Virtuální počítač	DC2	SharePoint Back End
SOWA1	Virtuální počítač	DC1	Office Web Apps 2013 Server
SOWA2	Virtuální počítač	DC2	Office Web Apps 2013 Server
SDAFE1	Virtuální počítač	DC1	Front End důvěryhodný archiv
SDABE1	Virtuální počítač	DC2	Back End důvěryhodný archiv

Detailní popis požadavků na infrastrukturu bude vypracován v rámci analytické fáze projektu a bude vycházet z výše uvedeného návrhu.

2.3.6.2 Testovací prostředí

Testovací prostředí navrhujeme jako testovací prostředí správy obsahu a aplikací, nikoli jako infrastrukturní kopii produkčního prostředí. Navrhujeme tedy následující zjednodušenou architekturu:

SharePoint Farma:

- 2x SharePoint Web Front End
- 1x SharePoint Application Web Front End
- 1x SharePoint Search
- 1x SharePoint Back End

Důvěryhodné úložiště:

- 1x Server důvěryhodný archiv

Office Web Apps (OWA) farma:

- 1x Office Web Apps 2013 Server

Servery navrhujeme jako virtualizované v následující konfiguraci:

- OS: Windows Server 2012 R2
- CPU: 4 jádra
- RAM: 16 GB
- Disk: 150 GB
- Disk 2:
 - role SharePoint Search: 200 GB

Detailní popis požadavků na infrastrukturu bude vypracován v rámci analytické fáze projektu a bude vycházet z výše uvedeného návrhu.

Server	Typ serveru	Umístění	Poznámka
SPTWFE1	Virtuální počítač	DC1	SharePoint Web Front End
SPTWFE2	Virtuální počítač	DC1	SharePoint Application Web Front End
SPTSFE1	Virtuální počítač	DC1	SharePoint Search Front End
SPTSBE1	Virtuální počítač	DC1	SharePoint Search Back End
SPTBE1	Virtuální počítač	DC1	SharePoint Back End
SPTOWA1	Virtuální počítač	DC1	Office Web Apps 2013 Server
SDAT1	Virtuální počítač	DC1	Důvěryhodný archiv

2.3.6.3 Vývojové prostředí

Vývojové prostředí navrhujeme jako prostředí pro vývoj aplikací pro SharePoint. Navrhujeme tedy následující zjednodušenou architekturu:

SharePoint Farma:

- 1x SharePoint Web Front End
- 1x SharePoint Application Web Front End
- 1x SharePoint Search
- 1x SharePoint Back End

Office Web Apps (OWA) farma:

- 1x Office Web Apps 2013 Server

Servery navrhujeme jako virtualizované v následující konfiguraci:

- OS: Windows Server 2012 R2
- CPU: 4 jádra
- RAM: 16 GB
- Disk: 150 GB
- Disk 2:
 - role SharePoint Search: 200 GB

Server	Typ serveru	Umístění	Poznámka
SPDWFE1	Virtuální počítač	DC1	SharePoint Web Front End
SPDSFE1	Virtuální počítač	DC1	SharePoint Search Front End
SPDSBE1	Virtuální počítač	DC1	SharePoint Search Back End
SPDBE1	Virtuální počítač	DC1	SharePoint Back End
SPDOWA1	Virtuální počítač	DC1	Office Web Apps 2013 Server

Detailní popis požadavků na infrastrukturu bude vypracován v rámci analytické fáze projektu a bude vycházet z výše uvedeného návrhu.

2.3.6.4 Webové Aplikace

Na SharePoint farmě budou provozovány následující webové aplikace na portu 443 popř. 80 (HTTPS, HTTP):

- Služby hlavního DMS portálu a SharePoint aplikací provozované na specifických URL adresách. Jednotlivé části portálu budou dělené do samostatných kolekcí webů, kdy každá jednotlivá kolekce bude mít svou alespoň jednu obsahovou databázi.
- Služba centrální administrace

Detailní nastavení a počet webových aplikací může být upřesněn v rámci analytické fáze.

2.3.6.5 Důvěryhodné úložiště

Důvěryhodné úložiště bude zajišťovat funkci zachování důvěryhodnosti dokumentů. Navržené řešení zajistí uložení dokumentů přímo z prostředí SharePoint do důvěryhodného úložiště (dále jen DÚ). DÚ se pak stará o naplnění všech postupů nutných k dlouhodobému zajištění relevance uložených dokumentů. Prostředí SharePoint následně umožní stažení jak souboru originálu, tak souboru balíčku vytvořených elektronických důkazů.

Základním stavebním kamenem nabízeného řešení je produkt O2STA (O2 Smart Trusted Archive – „Důvěryhodné úložiště“), který zajišťuje naplnění všech postupů nutných k dlouhodobému zajištění právní relevance uložených dokumentů. Dále pro ovládání DÚ už slouží funkcionality, které se nainstalují na SharePoint a uživatelé je používají jako ostatní standardní funkce.

O2STA vyžaduje pro svůj běh 2 serverové zapojení a to pro komunikaci se SharePointem, tak pro ukládání dokumentu tedy DB.

Servery navrhujeme jako virtualizované v následující konfiguraci:

OS: Windows Server 2012 R2
CPU: 4 jádra
RAM: 16 GB
Disk: 150 GB

Produkt důvěryhodného úložiště s okolím komunikuje pomocí rozhraní SharePointu jim poskytovaných webových služeb. Každý požadavek na DÚ vyžaduje, aby požadavek byl digitálně podepsán. Pro vkládání souborů musí být vždy zaregistrován na serveru SharePointu certifikát pro ověření podpisu požadavků.

2.3.6.6 Architektura vyhledávání

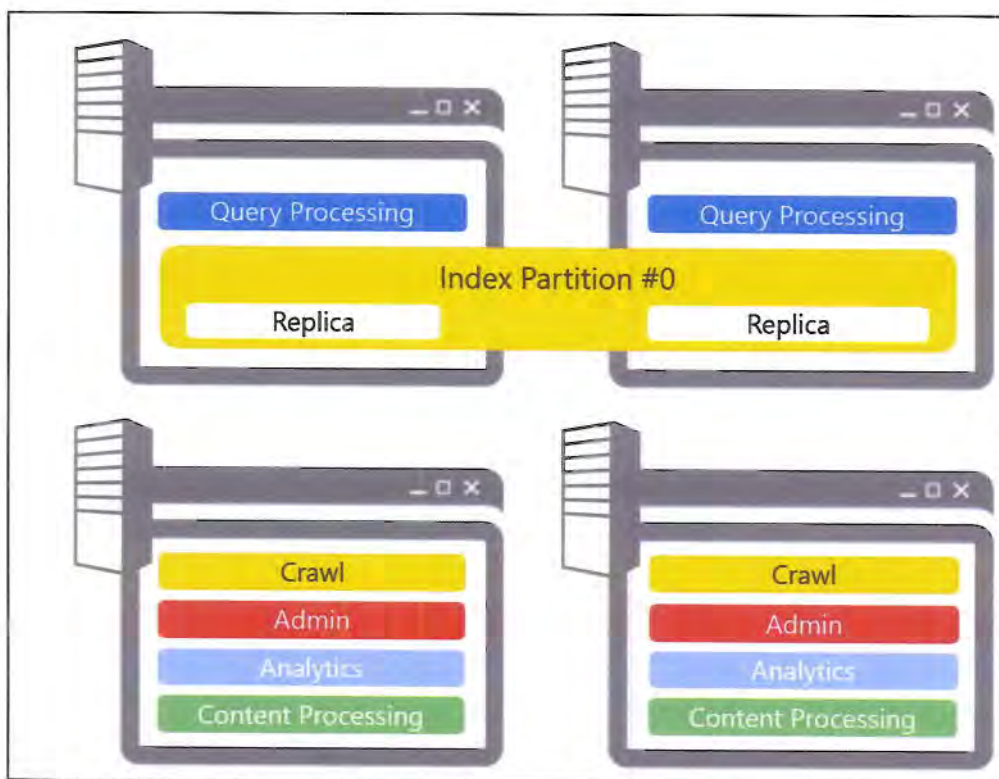
Architektura vyhledávání v produkčním prostředí bude navržena pro až cca 10 milionů položek. Používá 2 servery Search Front End a 2 servery Search Back End.

Předpokládáme indexování následujících typů dokumentů:

- Dokumenty MS Office
- Dokumenty PDF.

V rámci konfigurace bude indexování konfigurováno pro data uložená v rámci SharePoint 2013 portálu.

Index bude implementován jednou „index partition“, která má repliky na dvou serverech (primární a sekundární):

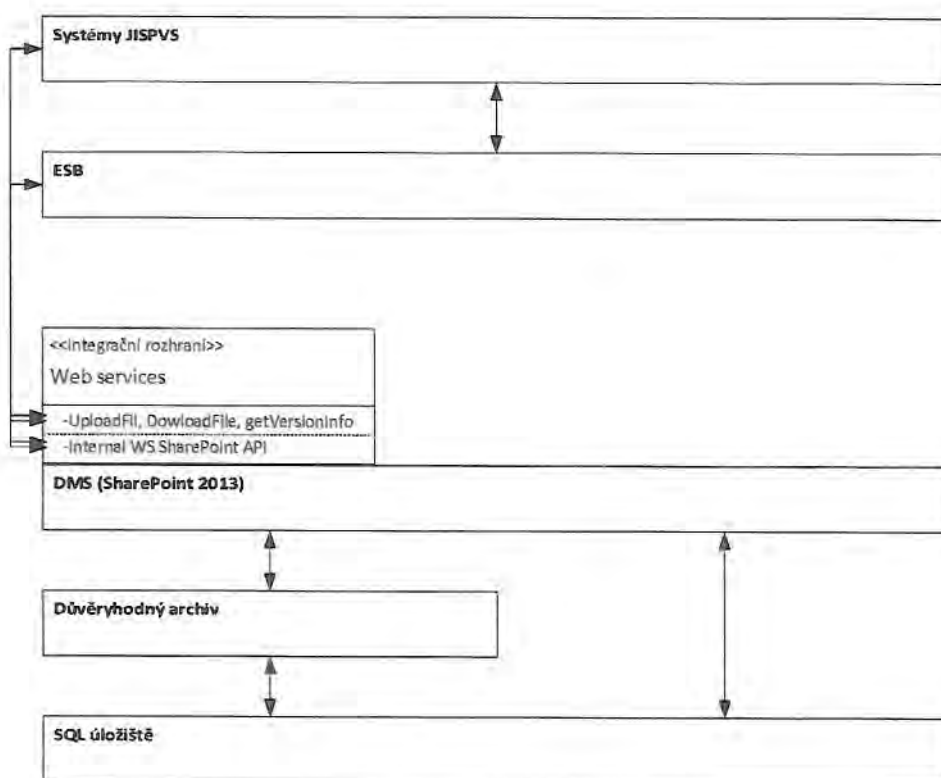


Obrázek 12 – Index partition

2.3.6.7 Integrace na systémy JISPSV

Implementace SharePoint 2013 farmy do interní infrastruktury zadavatele bude detailně specifikována v Návrhu realizace. Navržené řešení bude postavené z části na standardní customizaci platformy SharePoint, která bude doplněna o vyvinuté komponenty umožňující jednoduchou integraci pomocí **Integračního rozhraní** mezi systémy JISPSV napřímo nebo zprostředkovaně přes ESB a úložištěm v SharePointu, které bude poskytovat požadované služby.

Návrh rozhraní je zobrazen na obrázku:



Obrázek 13 – Schema integračního rozhraní

DMS bude dle navrženého schématu fungovat jako úložiště dokumentů se specifickými procesy pro výměnu dat mezi JISPSV a SharePointem prostřednictvím integrační vrstvy. Jeho konfigurace vyplývá z principů vlastní platformy SharePoint, kde na základě změn významných atributů (např. změna Statusu dokumentu) v SharePointu bude provedena synchronizace dat mezi DMS a systémy JISPSV, tj. dojde k předání aktuální datové věty a podkladů přes ESB do JISPSV.

DMS bude strukturovat data tak, aby eliminovalo případná technologická omezení platformy MS SharePoint. Detailně bude upřesněno v rámci analytické části projektu, kde bude upřesněn i návrh na vytvoření/úpravu cílové struktury aplikace na straně SharePointu.

Navržené řešení bude koncipováno tak, aby v maximální míře splňovalo následující předpoklady:

- Cílové řešení splňuje minimálně stávající provozní parametry všech projektem ovlivněných systémů.
- Řešení splňuje požadavky na bezpečnost.
- Řešení splňuje požadavky na zaznamenávání událostí v řešení (logování).

Ostatní integrace předpokládáme s následujícími systémy:

- **Active Directory** – za účelem synchronizace profilů uživatelů z AD. SharePoint farma bude pouze číst data z AD, nebude probíhat žádný zápis do AD. Importovány budou výchozí vlastnosti (properties) uživatelů z AD.
- **SMTP server** – odchozí emaily z SharePoint farmy budou využívat SMTP server.

2.3.6.8 Ostatní nastavení

SharePoint farma bude nastavena následovně:

- Jako šablona webu bude použita standardní šablona Týmového webu
- Bude použita výchozí šablona MasterPage
- Uživatelské profily budou synchronizovány s jedním Active Directory
- Bude použito výchozí téma SharePoint webu
- Základní instalace farmy bude provedena z primární anglické jazykové verze. Do prostředí bude doinstalován český jazykový balíček.

2.3.6.9 Migrace dat

Současné aplikace provozované na existujícím SharePointu budou migrované v rámci Rozvoje dle čl. 3.3 Smlouvy. Předpokládáme:

- migraci stávajících SharePoint aplikací provozovaných v rámci stávající platformy, včetně případné optimalizace, např. stávající spisové služby nebo oběhu dokumentů,
- provedení kompletní migrace dat uložených ve stávajících systémech. Migrace dat stávajícího úložiště bude provedena takovým způsobem, aby zajistila pokračování funkčnosti datového úložiště pro všechny původní aplikace, které SharePoint jako své datové úložiště používaly,
- poskytnutí součinnosti při implementaci a integraci nových business aplikací, např. nové spisové služby. Tyto nové aplikace budou používat nový SharePoint jako své datové úložiště.

Detailní popis řešení migrace a její kalkulace není předmětem této části nabídky a bude případně upřesněn na základě analýzy až v rámci Rozvoje dle čl. 3.3 Smlouvy.

2.3.7 SCCM A WSUS

Kapitola obsahuje popis nasazení System Center a WSUS podle požadavku Přílohy č. 6 Zadávací dokumentace v kapitole 2.4.6.

Produkční prostředí

Návrh realizace – část analýza – SCCM, WSUS, antivirové řešení

Analýza předpokládá zhodnocení současného stavu infrastruktury stávajících a nových koncových stanic z pohledu konfiguračního managementu:

- SCCM – analýza použití dřívějších nástrojů pro správu a jejich možnost odstranění, možnosti koncových stanic do nové AD struktury a do nové management struktury. Analýza požadavků zadavatele a jednotlivých rolí správy (administrátoři, správci aplikací, lokální správci atd.). Analýza topologie sítě.
- WSUS – analýza požadavků zadavatele na SW aktualizace, porovnání s doporučenými postupy. Analýza požadavků z pohledu bezpečnosti.
- Distribuce aplikací – analýza stávajících aplikací, současná inventarizace.
- Monitorování – analýza požadavků zadavatele na inventarizaci SW a HW koncových stanic.
- Antivirové řešení – analýza stávajícího stavu, primární inventura verzí současného antivirového řešení, možnosti migrace na navrhované řešení integrované do SCCM. Analýza požadavků na zabezpečení stanic.

Návrh realizace – detailně technická specifikace – SCCM, WSUS, antivirové řešení

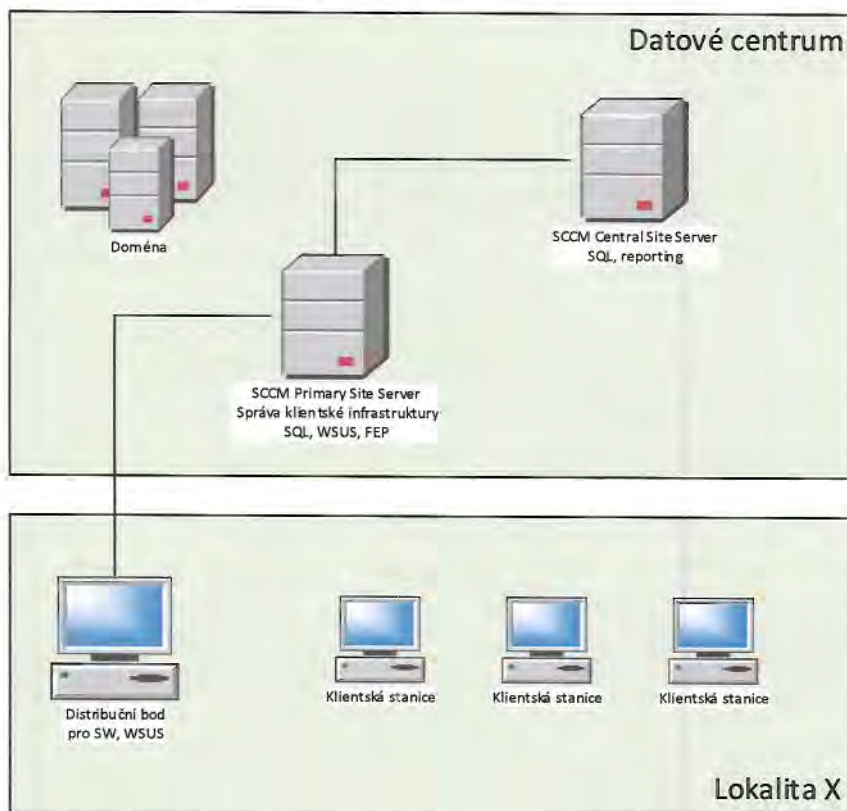
Výstupem bude návrh technické specifikace a postupy pro migraci do nového prostředí. Pro splnění požadavků podle kapitoly 2.4.6 zadávací dokumentace navrhujeme všechny funkce integrovat do SCCM – WSUS, distribuce aplikací, monitorování stavu HW a SW a antivirové řešení s centrálním managementem. Integrace má výhody zejména pro zjednodušení správy z pohledu topologie sítě. Díky integraci WSUS do SCCM není nutné provozovat WSUS servery na lokalitách. Postačí jediný WSUS server a v lokalitách obslouží klienty distribuční body, které musí být zřízeny mimo jiné z důvodu distribuce aplikací. Management bude integrován s Active Directory. Jako antivirovou ochranu navrhujeme Forefront Endpoint Protection, jehož správa bude integrovaná do SCCM. Klientská licence FEP je součástí klientské licence System Center CAL.

Návrh bude řešit tyto oblasti:

- Design SCCM sites, SQL a distribučních bodů
- Security mód
- Extenze AD, zdůvodnění
- Návrh řešení vysoké dostupnosti
- Databázový pohled, SCCM provider, SQL autentizace.
- Předinstalační požadavky.
- Doménové a bezpečnostní požadavky, SPN.Jmenná konvence.
- Definice boundaries. Definice komunikačních portů.
- Požadavky na účty, přístupová práva a security skupiny
- Discovery
- Kapacitní plán, performance
- Definice požadavků na IIS

- Zatížení datové sítě
- Maintenance site, backup.
- Plánování SCCM klientů
- Design Client Status Reporting
- Design administrace, SCCM konzoly
- Design Distribuce SW
- Design Integrace WSUS
- Design HW Inventory
- Design WWW reporting
- Design SQL dotazů – customizace dotazů
- Design SCCM collection – customizace
- Design Forefront Endpoint Protection
- Návrh testovacích scénářů
- Návrh akceptačních protokolů

Předpokládaný návrh SCCM topologie:



Implementace – část instalace jednotlivých systémů, včetně konfigurace v prostředí MPSV

V této části budeme postupovat podle vytvořeného Návrhu realizace a připraveného harmonogramu. Implementace SCCM, WSUS a FEP je závislá na primární implementaci Active Directory, DNS a na přípravě virtuálního prostředí.

Implementace – část funkční testování jednotlivých systémů

Testování bude probíhat podle připravených testovacích scénářů a podle harmonogramu testování. Pro testování na klientech navrhujeme pilotní ověřovací provoz.

Implementace – část migrace dat nebo aplikací ze stávajícího prostředí jednotlivých systémů

Současně s migrací koncových stanic do nové struktury AD dojde i k migraci SCCM klienta, WSUS nastavení klientů. Migraci klientů je možné provést až po ukončení testů serverové části a po ukončení pilotního provozu.

Implementace – část akceptační procedura (akceptační řízení) jednotlivých systémů

Akceptaci je možné provést na základě vyhodnocení pilotního provozu, který ověří funkčnost a postupy potřebné pro zahájení produktivního provozu v produkčním prostředí.

Implementace – část integrační testování

Zahájení produktivního provozu v produkčním prostředí

V klientské části musí nejprve dojít k migraci koncových stanic do nové AD struktury, pak je možné migrovat SCCM klienty, hromadně odinstalovat klienty antiviru a instalovat nové klienty.

Podpora provozu implementovaného systému

Předpokládáme podporu v těchto oblastech:

- Příprava SW balíčků
- Úpravy výstupů z SCCM reportů a queries:
 - Inventury HW a SW (programového vybavení)
 - Stavy distribucí balíčků
 - Stavy aktualizací WSUS
 - Stavy zabezpečení koncových stanic
- Metodická pomoc s aktualizacemi WSUS
- Metodická pomoc se změnami konfigurací FEP podle aktuálních potřeb zabezpečení

Server	Typ serveru	Umístění	Poznámka
SCCM01	Virtuální počítač	DC1 / DC2	SCCM Central Site, vlastní SQL
SCCM03	Virtuální počítač	DC1 / DC2	SCCM Primary Site pro stanice, vlastní SQL
SCCMxxx	Fyzický HW nebo Virtuální počítač	Lokality	Distribuční bod pro lokalitu Počet není známý, bude stanoven v průběhu etapy Návrh realizace

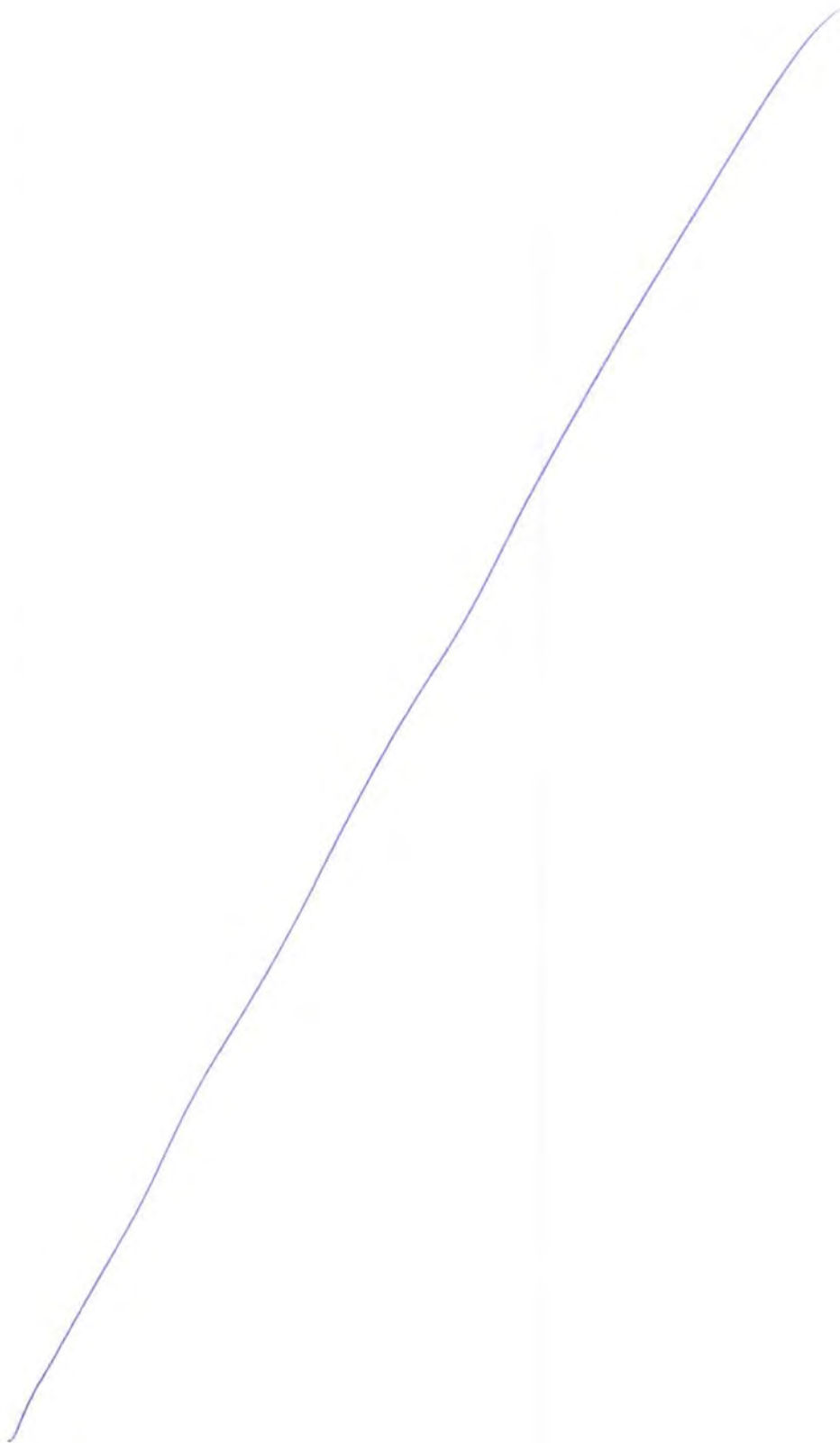
Údaje jsou uvedeny orientačně a budou upřesněny v etapě Návrh realizace – analýza.

Testovací prostředí

V testovací části navrhujeme jednu SCCM site, není potřeba testovat komunikaci mezi SCCM sites. Pro účely testování požadovaných vlastností není nutné oddělit centrální reporting. Všechny požadované SCCM, WSUS a antivirové funkce bude možné v testovacím prostředí testovat, ověřovat postupy a přenášet do produkčního prostředí.

Server	Typ serveru	Umístění	Poznámka
SCCMTEST01	Virtuální počítač	DC1/DC2	SCCM Primary Test Site, vlastní SQL

Údaje jsou uvedeny orientačně a budou upřesněny v etapě Návrh realizace – analýza.



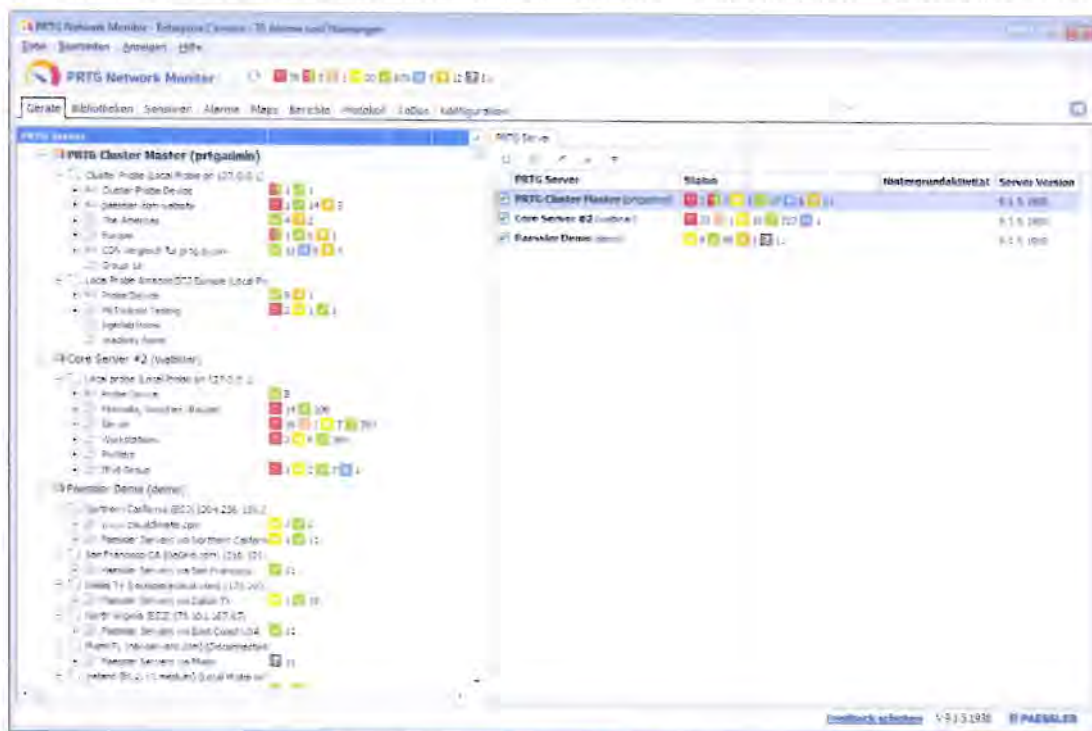
2.3.8 PROVOZNÍ DOHLED

Pro provozní monitoring serverů (myšleno pouze serverů, nikoli koncových stanic) navrhujeme z licenčních důvodů produkt PRTG. V případě, že by pro servery byla Zadavatelem pořizována licence MS System Center např. z důvodu implementace další MS System Center komponenty, je možné implementovat bez dodatečných nákladů MS SCOM (náklady by se snížily o cenu licencí PRTG).

PRTG je nástroj pro monitorování sítí a systému, zařízení, aplikací, přenosu dat a dostupnosti. Je funkční v systémech Windows Server 2003, 2008, 2012 a také v XP, Vista a Windows 7 a monitoruje Systémy Windows, Linux, Unix a MacOS. Instalace má vlastní, integrovanou databázi, webový server. PRTG Network Monitor podporuje monitorování SNMP, WMI, Flow, stejně tak jako sledování paketů (packet sniffing) a nabízí 80 speciálních senzorů pro monitorování VoIP, webových stránek, e-mailů, aplikací, databází, virtuálního prostředí a mnoho dalšího. PRTG Network Monitor využívá klienty - sondy, které lze instalovat do lokálních sítí, a poté data monitorování na centrální server. Data lze šifrovat.

PRTG Network Monitor obsahuje kompletní sadu funkcí pro monitorování sítí v každé licenci. S jedním clusterem s podporou převzetí služeb při selhání zajišťuje, že monitorování nebude přerušeno v případě poruchy serveru ani při aktualizacích.

Navrhujeme nasazení dvou serverů v clusteru pro monitoring serverové infrastruktury v produkčním prostředí i testovacím prostředí. Oba servery v clusteru lze propojit pomocí enterprise konzoly.



- Monitoring informačních systémů jednotlivých agend zadavatele
- PRTG bude monitorovat systémy včetně infrastrukturních, např. ESB, DMS
- V nové infrastruktuře bude PRTG monitorovat:
 - MS Active Directory
 - MS Exchange
 - MS SQL servery
 - SharePoint
 - WSUS

- FEP

Monitoring protokoly

PRTG může být konfigurován jako agent-less monitoring, pro dohled infrastruktury nepotřebuje instalaci lokálních agentů na serverech, či spouštět v systému separátní skripty k získání sledovaných informací a veličin. PRTG bude konfigurováno přesně tak, aby sledované informace a veličiny získávalo ze všech systémů výhradně skrze níže jmenované management protokoly.

- **WMI** protokol - pro sledování Microsoft platform a aplikací vč. SQL, Exchange
- **WBEM, SOAP**
- **SSH**
- **SNMP get** - pro získání networking informací o zařízeních a přenosech
- **ADO** - pro komunikaci s DB systémy, jež nejsou přímo podporované
- **TCP** protokoly (http, snmp, ftp, cifs ... port), pro dohled komunikačních protokolů a serverů
- **Syslog s SNMP Trap receiver** - pro příjem notifikací od vybraných prvků

PRTG server může být zároveň konfigurován jako SYSLOG server.

Notifikace a eskalace

PRTG server může pro notifikace a eskalace použít řadu komunikačních kanálů. Konfigurace bude obsahovat eskalační upozornění na skupinu administrátorů. Eskalace bude vyvolána, pokud chybový stav nebude řešen (acknowledged), nebo nebude stav změněn zpět na Ok. Konkrétní nastavení notifikací a eskalací bude upřesněno během implementačního procesu na základě předcházející analýzy.

Operační systémy a aplikace

Základní operační platformou bude Microsoft Windows, který díky instrumentaci WMI poskytuje dostatečný velký rozsah informací pro dohled operačních systémů. Pomocí WMI bude prováděn i dohled nadstavbových serverů a SQL uvedených samostatně níže.

Windows servery

Níže je uvedena sada minimálních veličin, které budou konfigurovány a sledovány na úrovni operačního systému:

- Dostupnost (ping)
- CPU vytižení
- MEM využití
- HDD využití (multi, nebo jednotlivě)
- NIC bandwidth
- RDP
- SWAP
- Uptime
- Last update

Dále bude nutné monitorovat stav jednotlivých služeb běžících na jednotlivých serverech a v případě pádu služby PRTG provede její automatický restart. Stejně tak v případě, kdy nenastartuje automaticky.

Bude sledován nejen stav zvolené služby, ale také konkrétní systémový proces odpovídající této službě z hlediska jeho konzumace systémových prostředků.

Doménové řadiče

Na doménových řadičích budou navíc sensory pro kontrolu replikací Active Directory a DNS Resolve checker, který bude překládat DNS jméno AD na IP adresy kontrolérů, které bude porovnávat s referenčními, typicky NS servery domény. Dále budou sledovány kritické služby jako DNS, DHCP a sledovány hodnoty NTP zdroje času.

Clustery

V případě MS clusterů budou hodnoty vyčítány přes cluster instanci, jejíž IP adresa se nebude měnit, virtuální instance. Kontrola parametrů diskového systému vč. sledování místa bude jen na vybraných discích, tak aby se předešlo chybně odesílaným notifikacím, případně budou adekvátně konfigurovány Dependenci, tak aby se tomuto false-positive efektu co nejvíce zamezilo.

SQL servery

Microsoft SQL Server je přímo podporován na straně PRTG a není tedy nutná manuální konfigurace ADO dotazů.

SQL server bude monitorován nejen z hlediska dostupnosti, běžících služeb, dostupnosti tcp portů, ale i z hlediska jeho vlastní výkonosti.

2.3.9 MICROSOFT SQL SERVER

Pro potřeby databázové vrstvy pro některé aplikace bude využito dvou Microsoft SQL Server. Parametry vlastní implementace budou upřesněny při návrhu realizace.

Zálohování dat bude realizováno nativními prostředky SQL Serveru v podobě zálohy do souboru, který bude dále zpracován systémem zálohování Zadavatele.

2.3.9.1 SQL server IdM

Pro potřeby IdM je navržen kvůli kompatibilitě s FIM a požadavkům na výkon samostatný Microsoft SQL Server 2012R2.

Produkční prostředí

V produkčním prostředí je navrženo nasazení dvojice serverů s technologií vysoké dostupnosti.

Server	Typ serveru	Umístění	Poznámka
SQL01	Virtuální počítač	DC1	
SQL02	Virtuální počítač	DC2	

Údaje jsou uvedeny orientačně a budou upřesněny v etapě Návrh realizace – analýza.

Testovací prostředí

V testovacím prostředí bude použit jeden server

Server	Typ serveru	Umístění	Poznámka
SQL01	Virtuální počítač	DC1/DC2	

Údaje jsou uvedeny orientačně a budou upřesněny v etapě Návrh realizace – analýza.

2.3.9.2 SQL Server DMS a další

Pro SharePoint a další aplikace je navrženo použít pro produkční i testovací prostředí Microsoft SQL Server 2014 Enterprise s několika samostatnými instancemi. Implementace bude navržena tak, aby byla zajištěna vysoká dostupnost poskytovaných služeb.

Zálohování dat bude realizováno nativními prostředky SQL Serveru v podobě zálohy do souboru, který bude dále zpracován systémem zálohování Zadavatele.

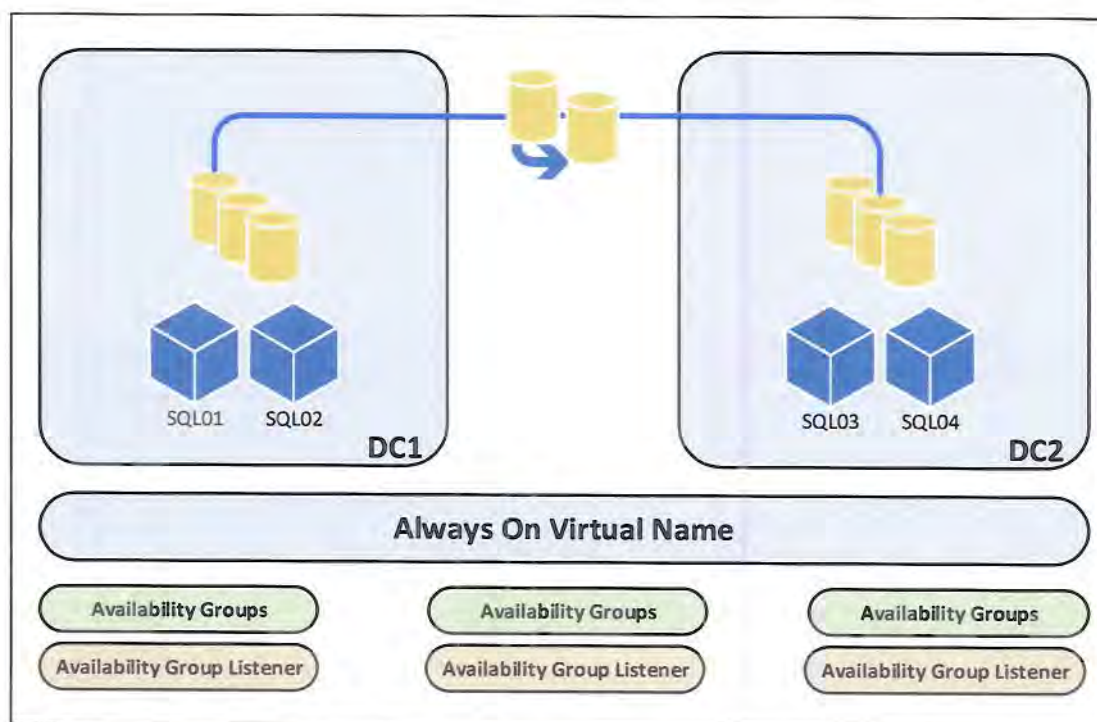
Produkční prostředí

Pro produkční prostředí je navrženo využití celkově čtyř serverů. Všechny servery budou virtualizované.

Vysoká dostupnost

Vysokou dostupnost databází bude zajišťovat technologie Windows Failover Clustering a SQL AlwaysOn. Na obou lokalitách budou vždy dva servery. Vybrané databáze budou synchronizovány mezi lokalitami. Navržené řešení umožňuje zpracování v active - passive nebo active - active databázovém režimu, volba vhodného režimu bude součástí dokumentu Návrh realizace – analýza.

Aplikace pracují vždy s daty jednoho (aktivního) datového centra. Záložní databáze v druhém datovém centru je synchronizována s primární databází pomocí technologie Always On Availability Groups. V případě výpadku aktivního datového centra je aktivována záložní databáze a stává se primární databází.



Replikace mezi datovými centry

Microsoft SQL Server 2014 Enterprise podporuje funkcionalitu AlwaysOn Availability Groups, která nabízí funkce vysoké dostupnosti a mirroring skupin databází, podporuje jednu read-write primární a až osm odpovídajících sekundárních read-only databází. Zrcadlení může probíhat v Asynchronous-commit režimu pro replikace s menší průchodností sítě, ale pro řešení je navrženo využít Synchronous-commit režimu pro zajištění nejvyšší úrovně vysoké dostupnosti. Díky těmto technologiím je řešení připraveno na škálování jak z hlediska výkonu jednotlivých uzlů (navýšením kapacit virtuálního serveru), tak z hlediska zvýšení dostupnosti při nárůstu počtu datových center.

Interní konektivita databázového clusteru

Servy zařazené v clusteru budou navzájem spojeny privátní sítí, tzv. „cluster interconnect“, která umožňuje interní komunikaci mezi uzly clusteru. Předpokládáme pro tuto komunikaci využít vyhrazené virtuální adaptéry ve virtuálních SQL serverech. Propojení mezi hostitelskými virtualizačními servery předpokládáme realizovat po vyhrazené VLAN.

Navržené instance SQL:

- Microsoft SharePoint (3 instance)
- Ostatní aplikace

Server	Typ serveru	Umístění	Poznámka
SQL01	Virtuální počítač	DC1	
SQL02	Virtuální počítač	DC1	
SQL03	Virtuální počítač	DC2	

SQL04	Virtuální počítač	DC2	
-------	-------------------	-----	--

Údaje jsou uvedeny orientačně a budou upřesněny v etapě Návrh realizace – analýza.

Testovací prostředí

Pro testovací prostředí je navrženo nasazení dvou serverů s technologií AlwaysOn cluster v režimu Active – Passive. Podobně jako v produkčním prostředí a v testovacím navrhujeme použít samostatné instance.

Server	Typ serveru	Umístění	Poznámka
SQL01	Virtuální počítač	DC1	
SQL02	Virtuální počítač	DC2	

Údaje jsou uvedeny orientačně a budou upřesněny v etapě Návrh realizace – analýza.

2.3.10 SÍŤOVÉ SLUŽBY DNS, DHCP A WINS

Kapitola obsahuje popis nasazení síťových služeb DNS, DHCP a WINS podle požadavku Přílohy č. 6 Zadávací dokumentace v kapitole 2.4.1.

Služby DNS, DHCP a WINS budou nasazeny na řadičích domény.

Postup implementace a migrace bude upřesněn v průběhu etapy Návrh realizace – analýza. Součástí návrhu bude zejména:

- Postup a architektura implementace
- Identifikace a seznam nezbytných dat, migrovaných z původních systémů
- Postup migrace nezbytných dat z původních systémů

3 ARCHITEKTURA A NÁVRH ŘEŠENÍ

Kapitola obsahuje popis nasazení síťových služeb DNS, DHCP a WINS podle požadavků Zadavatele v kapitolách 2.3.1 – 2.3.3 Přílohy č. 6 Zadávací dokumentace.

3.1.1 OBECNÉ POŽADAVKY

Kapitola obsahuje popis splnění požadavků Přílohy č. 6 Zadávací dokumentace v kapitole 2.3.1.

Pro instalaci serverů bude použito operačního systému Microsoft Windows Server 2012R2 a odpovídajících verzí aplikace s použitím licencí, které dá u vyjmenovaných produktů k dispozici Zadavatel. U stávajících serverů, které budou definovány v průběhu etapy Návrh realizace, bude proveden upgrade.

Projekt bude rozdělen do několika samostatných částí podle implementovaných produktů. Tyto části budou každá sama za sebe dodržovat také nefunkční požadavky (dokumentace, dostupnosti, školení aj.) uvedené v Příloze č. 6 Zadávací dokumentace.

Každá z částí projektu bude mít následující fáze:

- a) Návrh realizace – část analýza: výstupem bude analytická dokumentace a návrh technického řešení implementace celého Systému (všech systémů),
- b) Návrh realizace – část detailní technická specifikace celého Systému (všech systémů): popisuje pro vybranou variantu detailně technické a projektové provedení implementace a migrace. Tato technické specifikace bude obsahovat i harmonogram prací a podrobný popis jednotlivých fází projektu,
- c) Implementace – část instalace jednotlivých systémů, včetně konfigurace v prostředí MPSV,
- d) Implementace – část funkční testování jednotlivých systémů,
- e) Implementace – část migrace dat nebo aplikací ze stávajícího prostředí jednotlivých systémů,
- f) Implementace – část akceptační procedura (akceptační řízení) jednotlivých systémů,
- g) Implementace – část integrační testování,
- h) Zahájení produktivního provozu v produkčním prostředí,
- i) Podpora provozu implementovaného systému.

Každá část projektu bude mít samostatně kompletní sadu dokumentace, vyhovující požadavkům popsaných v požadavcích na dokumentaci.

3.1.2 POŽADAVKY NA ARCHITEKTURU SYSTÉMU

Kapitola obsahuje popis splnění požadavků Přílohy č. 6 Zadávací dokumentace v kapitole 2.3.2.

Dodávané systémy budou umístěny ve stávajícím prostředí MPSV a budou poskytovat služby infrastrukturního charakteru, a to ostatním systémům v rámci JISPSV ev. přímo koncovým uživatelům a jejich stanicím.

Pro implementaci Systému budou zvoleny takové technologie, které umožní zajistit škálovatelnost a vysokou dostupnost bez ztráty kontextu v případě výpadku všude tam, kde je to technologicky možné. Aplikační logiky budou realizovány s využitím souběžného zpracování požadavků (volání) více vláken (multithreading).

Veškeré systémy budou provozovány ve virtuálním prostředí MPSV provozovaném na virtualizační technologii Microsoft Hyper-V, kterými Zadavatel disponuje,

Některé služby není ze své podstaty vhodné provozovat ve virtuálním prostředí a pro ně bude využito dedikovaných serverů v nezbytné kapacitě s nezbytným výkonem. Nezbytné požadavky na kapacitu a výpočetní výkon dedikovaných serverů stanoví Uchazeč v Návrhu realizace.

Součástí dodávky je i implementace potřebných serverových operačních systému (vždy platforma Microsoft) a databází. Použité databáze budou Microsoft SQL Server v nejnovější verzi, kterou podporuje implementovaný produkt. Použity budou pouze ty produkty, které jsou kompatibilní s uvedenou virtualizační platformou.

Systémy budou provozovány v testovacím a produkčním prostředí. Testovací prostředí budou disponovat nižším požadovaným výkonem a v odůvodněných případech omezením v oblasti vysoké dostupnosti, jinak budou shodné jako produkční prostředí. Mimo trvalá provozní a testovací prostředí mohou být zřizována dočasná testovací prostředí pro specifické účely ověřování a testování podle potřeby z dodaných obrazů virtuálních serverů testovacího prostředí.

Systém budou mít jednotné administrační rozhraní pro správu parametrů systémů JISPSV - konfiguraci, správu potřebných workflow, správu úloh a jejich plánování, správu integračních rozhraní umožňujících konfigurovat API na další systémy, správu reportů a správu oprávnění.

Celé řešení bude podporovat používání národních znakových sad minimálně v rozsahu UTF8, win1250-1251, ISO 8859-1 a 8859-2. Všechny webové přístupy k implementovaným produktům pro koncového uživatele budou v českém jazyce. V českém jazyce nebo s českou sadou Language Pack budou i OS a implementované systémy u kterých je to technologicky možné.

Systém bude zajišťovat vypořádání uživatelských požadavků zejména následujícího charakteru:

- a) koncové uživatelské požadavky na uložení a přístup k dokumentům,
- b) na zajištění infrastrukturních služeb z uživatelského PC,
- c) mailové služby,
- d) žádosti o služby infrastruktury (certifikát, role,...),
- e) administrátorské požadavky přicházející na administrátorská rozhraní jednotlivých služeb.

Systém bude zajišťovat služby pro JISPSV zejména následujícího charakteru:

- a) doménové,
- b) integrační,
- c) autentizační,
- d) autorizační.

3.1.3 POŽADAVKY NA BEZPEČNOST

Kapitola obsahuje popis splnění požadavků Přílohy č. 6 Zadávací dokumentace v kapitole 2.3.3.

Systém bude využívat standardní technologie k zabezpečení podle doporučení výrobce všude tam, kde je to technologicky možné. Upřesnění bude provedeno v etapě Návrh realizace.

Systém bude pro síťovou komunikaci využívat přednostně protokolu TCP, přičemž na straně komponenty poskytující služby (server) bude preferovaně využívat statických, předem známých portů. Volitelně bude umožňovat použití šifrované komunikace. Pokud bude z technologického a provozního hlediska výhodnější použít pro některé komponenty dynamického přidělování portů, bude zaručena kompatibilita takovéto komponenty, která je součástí subsystému v prostředí MPSV a její bezproblémový chod.

Systém bude umožňovat přihlášení uživatele pomocí SSO s možností přihlášení pomocí Microsoft Windows AD protokolem Kerberos. V případě, že nedojde k ověření pomocí mechanismu SSO, bude

umožněno přihlášení pomocí jména a hesla nebo klientského certifikátu X.509 v rámci protokolu SSL / TLS. Ověření bude provedeno opět vůči Microsoft AD. Systém / aplikace umožní pouze na základě změny konfigurační položky přihlášení (ověření) uživatelů jednotlivě jedním z výše zmíněných způsobů či oběma způsoby naráz (více faktorová autentizace) všude tam, kde to konkrétní produkt umožňuje. Uživatelské účty budou uloženy a spravovány v rámci Microsoft AD, ze které bude Systém / aplikace v okamžiku přihlášení přebírat identitu uživatele. Uživatelské rozhraní bude také poskytovat možnost úplného a bezpečného odhlášení uživatele ze systému.

Všechny přístupy k poskytované službě budou jednotné bez ohledu na to, jestli přistupuje uživatel pomocí uživatelského rozhraní nebo aplikace pomocí webové služby. Vždy je nezbytné provést ověření uživatele a jeho oprávnění přístupu k datům na základě role nebo oprávnění a provést auditní záznam o tomto přístupu (ev. zamítnutí přístupu) a činnosti, kterou s daty uživatel provádí. Každý přístup ke službě musí být jednoznačně identifikován a přiřazen ke koncovému uživateli, který s daty pracuje.

Implementace produktů bude využívat všech možností pro používání certifikátů a to jak pro přihlášení uživatele, tak pro podpis dokumentů, zabezpečení - šifrování dokumentů, zabezpečené spojení nebo při použití elektronické pošty. Všechny certifikáty budou při každém použití kontrolovány na jejich platnost i proti CRL.

Součástí správy aplikačních rolí bude vytváření, údržba a rušení aplikačních rolí. Uchazeč dodá návrh aplikačních rolí tak, aby respektovali požadavky na zajištění odděleného přístupu k datům nebo prostředkům MPSV na základě pracovní pozice, organizační struktury, lokality a činností vykonávaných jednotlivými uživateli. Aplikační role budou dále nadefinovány v Microsoft AD jako skupiny a přiřazení rolí uživatelům bude probíhat administrací v Microsoft AD zařazením uživatele do příslušné skupiny, resp. ve FIM, který bude sloužit pro správu Microsoft AD. Jednotlivé aplikace budou role uživatele přebírat z Microsoft AD, pokud je budou potřebovat. Součástí nabídky bude základní autorizační koncept. Detailní autorizační koncept bude vypracován a předán uchazečem v rámci etapy Návrh realizace - analýza. Vzhledem ke specifickému prostředí správy MPSV a silné provázanosti v rámci celkové architektury bude uchazeč při tvorbě detailního autorizačního konceptu úzce spolupracovat s pracovníky MPSV nebo pověřenými informatiky detašovaných pracovišť a přihlédne v návrhu k požadavkům, které budou pro jednotlivé role požadovány.

Systém o sobě bude poskytovat informace důležité pro audit prováděných činností. Každá činnost každého uživatele bude evidována, součástí evidence bude minimálně operace, identita uživatele a čas. Součástí projektu bude ve fázi Návrh realizace – detailní technická specifikace celého Systému (všech systémů) zpracování návrhu auditního modelu a na jeho základě po schválení MPSV zavedení auditního logování pro všechny implementované produkty.

Systém o sobě bude poskytovat také informace důležité pro provozní a bezpečnostní monitoring. Bude mimo jiné logovat veškeré operace ohledně přístupu a oprávnění uživatelů a to jak úspěšné, tak neúspěšné pokusy o přístup do aplikace a na jednotlivá API a veškeré provozní stavy aplikace a použitých frameworků.

Implementace produktů bude využívat jejich možností pro zajištění šifrování záznamů.

Implementace produktů bude využívat možnosti automatického zjišťování a stahování bezpečnostních záplat s upozorněním na tyto záplaty pro administrátora systému. Implementace záplat musí probíhat až po předchozím souhlasu administrátora v předem naplánovaném čase.

Systém bude integrován do zálohovacího prostředí zadavatele a to jak instalace, tak data. Zálohovací systém může zálohovat jak data, tak celé virtuální servery.

4 HARMONOGRAM PLNĚNÍ VEŘEJNÉ ZAKÁZKY

Kapitola obsahuje podle požadavku Zadávací dokumentace harmonogram plnění. Dále jsou zde uvedeny základní informace o metodice projektového řízení, aplikované Uchazečem při realizaci podobných projektů.

4.1 HARMONOGRAM PLNĚNÍ

Harmonogram plnění veřejné zakázky plně respektuje závazné požadavky Zadavatele na plnění jednotlivých milníků v souladu se Zadávací dokumentací. Milníky jsou rekapitulovány v následující tabulce.

ID	Milník	Termín
1.	Uzavření Smlouvy	T
2.	Vytvoření Návrhu realizace ve smyslu odst. 3.1.1 Smlouvy.	T + 3 měsíce (=T1)
3.	Ukončení akceptace Implementace ve smyslu odst. 3.1.2 Smlouvy a Dokumentace v souladu s odst. 3.1.3 Smlouvy vč. naplnění daty a migrace dat	T1 + 4 měsíce (=T2)
4.	Zahájení poskytování Služeb podpory provozu v souladu s odst. 3.2 Smlouvy	T2 + 1 den

Tabulka 13 – Milníky plnění veřejné zakázky

Na následujícím obrázku je patrný celý harmonogram v měsících rozdělený po jednotlivých etapách.



Obrázek 14 – High-Level pohled na harmonogram

Legenda k harmonogramu:

- **Zelená** oblast zajištění kontinuitního projektového řízení realizace dané etapy
- **Žlutá** oblast předpokládaný časový úsek realizace dané činnosti v rámci etapy
- **Červená** oblast akceptační milník v souladu požadavky na milníky

Na následující stranách jsou zobrazeny jednotlivé detailní výseky odpovídající konkrétní etapě.

	Návrh realizace (T + 3 měsíce)											
	1. měsíc				2. měsíc				3. měsíc			
	1. t.	2. t.	3. t.	4. t.	1. t.	2. t.	3. t.	4. t.	1. t.	2. t.	3. t.	4. t.
T = Datum podpisu Smlouvy												
Vytvoření Návrhu realizace ve smyslu odst. 3.1.1 Smlouvy												
Řízení projektu "Návrh realizace"												
Zpracování dokumentu Návrh realizace												
Prezentace Návrhu realizace a schvalovací proces												
Akceptace Návrhu realizace												

Obrázek 15 – Harmonogram - Etapa Návrh realizace

T = Datum podpisu Smlouvy	Implementace & Dokumentace (T + 7 měsíců)																				
	4. měsíc				5. měsíc				6. měsíc				7. měsíc								
	1.t.	2.t.	3.t.	4.t.	1.t.	2.t.	3.t.	4.t.	1.t.	2.t.	3.t.	4.t.	1.t.	2.t.	3.t.	4.t.	1.t.	2.t.	3.t.	4.t.	
Implementace ve smyslu odst. 3.1.2 Smlouvy a Dokumentace v souladu s odst. 3.1.3 Smlouvy vč. naplnění daty a migrace dat																					
Řízení projektu "Implementace a Dokumentace"																					
Příprava Implementace																					
Implementace Systému																					
Technická dokumentace k Systému																					
Školení - příprava podkladů																					
Školení 80 administrátorů																					
Školení 200 správců																					
E-learning pro 20.000 koncových uživatelů																					
Migrace dat - příprava detailního plánu a vývoj migračních nástrojů																					
Provedení zkušební a ostré migrace dat a kontrola integrity dat																					
Zpracování plánu obnovy Systému																					
Příprava akceptačních podkladů (scénáře, atp.)																					
Příprava funkčních testů																					
Příprava zátěžových testů a testování																					
Příprava penetračních testů a testování																					
Akceptační testování																					
Akceptace Implementace a Dokumentace																					
Dokumentace v souladu s odst. 3.1.3 Smlouvy																					
Administratorská dokumentace																					
Školící dokumentace																					
Uživatelská dokumentace																					
Dokumentace pro operátora Monitoringu																					
Dokumentace pro správce Systému																					
Dokumentace pro správce datového modelu a dat																					
Ostatní provozní dokumentace																					

Obrázek 16 – Harmonogram - Etapa Implementace & Dokumentace

T = Datum podpisu Smlouvy	7. měsíc				1. měsíc podpory			
	1.t.	2.t.	3.t.	4.t.	1.t.	2.t.	3.t.	4.t.
Zahájení poskytování Služeb podpory provozu v souladu s odst. 3.2 Smlouvy								
Řízení projektu "Služby podpory IS JISPSV-pip"								
Implementace a propojení Service Desku								
Nastavení služeb								
Implementace monitoringu								
Zaškolení operátorů								
Zahájení poskytování Služeb podpory provozu								
Poskytování služb podpory								

Obrázek 17 – Harmonogram zahájení poskytování Služeb podpory provozu

4.2 APLIKOVANÁ METODIKA ŘÍZENÍ DODÁVKY DÍLA

4.2.1 PROJEKTOVÁ PŘÍPRAVA, ŘÍZENÍ PROJEKTU

Vlastním řízením realizace dodávky bude pověřen tým odborníků, kteří budou stavět na svých dosavadních zkušenostech z obdobných projektů. Tento tým bude v průběhu celého projektu úzce spolupracovat s projektovým týmem Zadavatele a dalšími relevantními pracovníky na straně Zadavatele tak, aby zajistil maximální úspěšnost dodávky a minimalizoval všechna potenciální rizika spojená s realizací projektu.

Základní principy řízení projektu mezi Uchazečem a Zadavatelem určuje Metodika PRINCE2®, která byla vyvinuta a je vlastněna Office of Government Commerce (OGC) jako odpovědnou autoritou vlády Spojeného království Velké Británie a Severního Irska. Z této metodiky budou převzaty techniky a pracovní postupy užívané při vykonávání činností prováděných v rámci řízení projektu.

Cílem uplatnění Metodiky PRINCE2® v praxi je bezpečně řídit a realizovat projekt „On time, In full, On budget“, neboli tak, aby byla dodávka předmětu realizace uskutečněna v dohodnutém termínu, rozsahu a v rámci daného finančního rozpočtu.

Metodika PRINCE2® pokrývá všechny základní fáze životního cyklu projektu od okamžiku podpisu smlouvy se Zadavatelem, přes zahájení projektu, jeho naplánování, realizaci, až po jeho ukončení a předání do režimu podpory.

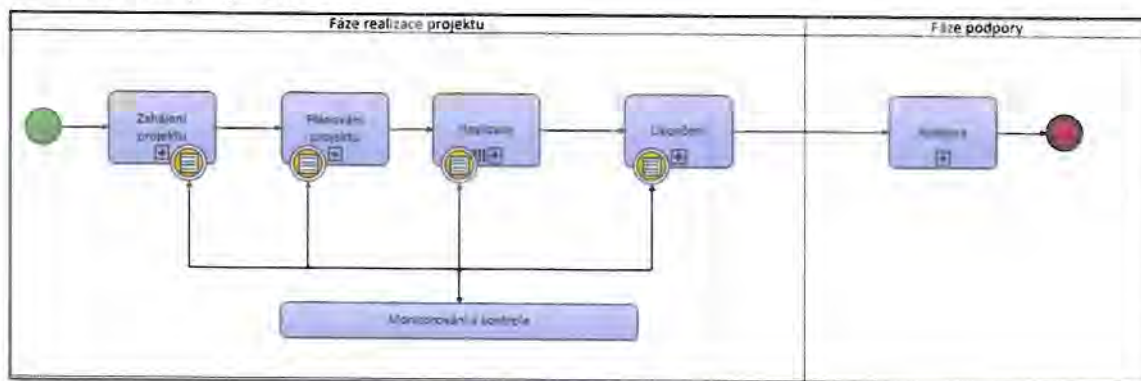
Postup řízení projektu podle Metodiky PRINCE2® je stručně popsán v následujících podkapitolách a jedná se o metodiku navrženou Uchazečem. Po dohodě se Zadavatelem může být metodika upravena tak, aby respektovala konkrétní prostředí zadavatele a jeho případná specifika.

4.2.2 PROCESY ŘÍZENÍ PROJEKTU A HLAVNÍ VÝSTUPY

V rámci přípravné fáze zahájení projektu musí být provedena příprava, nadefinování a následné odsouhlasení pravidel řízení průběhu projektu a nástrojů pro řízení realizace projektu.

Vlastní řízení projektu bude pro zajištění řízeného průběhu realizace rozděleno do pěti procesních skupin (oblastí), a to:

- zahájení projektu,
- plánování projektu,
- realizace,
- monitorování a kontrola,
- ukončení projektu.



Obrázek 18 – Řízený průběh realizace

4.2.2.1 Zahájení a plánování projektu

Projektová dokumentace

Na začátku je na úrovni Vedení projektu předložen a schválen seznam projektové dokumentace. Není-li dohodnuto jinak, jsou dokumenty předávány v elektronické podobě, ve standardních formátech MS Office, MS Project a MS Visio ve schválených verzích. Dále je možné využít i formát PDF. Rovněž je standardně využívána e-mailová komunikace.

Vedoucí projektu jsou zodpovědní za předávání aktuálních dokumentů i za zajištění jejich připomínkování a následného schválení. Zpravidla jsou připomínky k předaným dokumentům očekávány formou revizí, či komentářů.

Základní dokumenty vztahující se k řízení projektu:

Zakládací listina projektu – v průběhu přípravy projektu bude vytvořena Zakládací listina projektu (ZLP). Zakládací listina projektu je základní dokument, který bude po celou dobu trvání projektu zdrojem informací o tom, jak je projekt naplánován, prováděn, sledován, řízen a jak bude ukončen. V tomto dokumentu dojde k praktickému propojení zvolené metodiky řízení projektu s konkrétním projektem a jeho potřebami. Budou připraveny šablony vybraných dokumentů stanovených metodikou a určených pro sledování a vykazování stavu, průběhu a řízení projektu.

Vytvoření Zakládací listiny projektu musí proběhnout ve třech krocích:

- vypracování návrhu ZLP,
- předložení návrhu ZLP k oponentuře Zadavateli a následné zapracování jeho připomínek,
- schválení ZLP Řídícím výborem projektu jakožto nejvyšším orgánem projektu.

Zakládací listina projektu bude vytvořena jako dokument v MS Word a po schválení Řídícím výborem se stane dokumentem závazným pro všechny účastníky zapojené do realizace projektu. Dokument připravuje vedoucí projektu za AC ve spolupráci s technickými specialisty.

Harmonogram projektu – definuje jednotlivé činnosti a průběh jejich realizace. Vedoucí projektu za stranu Uchazeče harmonogram průběžně aktualizuje na základě postupu projektu a získaných upřesnění.

Komunikační plán – slouží jako seznam osob (vč. kontaktů) zúčastněných na projektu s upřesněním jejich týmu a role na projektu. V případě potřeby může být doplněna i popis schvalovacích pravomocí. Za přípravu jsou odpovědní Vedoucí projektu za zúčastněné strany.

Zápis z jednání – vzniká z každého jednání v rámci realizace projektu. Dle dohody zápis tvoří Vedoucí projektu, nebo případně jiný stanovený pracovník. Výjimkou mohou být technická jednání, jejichž závěry jsou zapracovány do samostatných projektových dokumentů.

Zpráva o stavu projektu – jedná se o pravidelně zpracovávané informace o průběhu projektu za dané období, které jsou předkládány členům ŘV. Za zpracování odpovídají Vedoucí projektu.

Registr rizik - ošetření projektových rizik je předmětem procesu řízení rizik projektu, který bude nedílnou součástí řízení celého projektu. V rámci něho proběhne analýza rizik, jejímž výsledkem bude identifikace negativních jevů, či odchylek od schváleného plánu, které mohou mít dopady do realizace projektu a zajištění jejich eliminace, nebo alespoň minimalizace dopadů.

Hlavním výstupem výše uvedených činností je dokument Registr rizik projektu. V průběhu realizace shromažďují vedoucí projektu informace a údaje potřebné ke zhodnocení aktuálního stavu a vývoje rizik projektu. Na základě získaných informací je zpracována a průběžně aktualizován Registr rizik (na jednáních vedení projektu). Registr rizik slouží k identifikaci, analýze a vlastnímu řízení jednotlivých rizik. Rovněž obsahuje informace o dopadu a

pravděpodobnosti rizik, plán jejich eliminace a plán postupu pro případy, že skutečně nastanou.

Registr rizik projektu bude udržován formou pracovního sešitu aplikace MS Excel.

Akceptační / Předávací protokoly – slouží k formálnímu předání, či akceptaci výstupů projektu. Návrh protokolu připravuje vedoucí projektu za Zhotovitele.

Další projektové dokumenty – jedná se o veškeré dokumenty předávané v rámci realizace projektu dle seznamu projektové dokumentace (Issue log a Změnové požadavky).

Nastavení organizační struktury projektu

V rámci tohoto procesu bude nastavena organizační struktura projektu, popsány jednotlivé orgány projektu a jejich konkrétní zodpovědnosti a činnosti.

Jako součást organizační struktury bude vypracován základní popis rolí jednotlivých účastníků projektu a komunikační plán projektu.

Vypracování harmonogramu projektu

Rámcový harmonogram projektu, který je součástí nabídky, byl zpracován pro potřeby nabídky na méně podrobné úrovni a detailně bude dopracován po formálním zahájení projektu v rámci procesu plánování projektu.

Harmonogram projektu bude zpracován v aplikaci MS Project a bude schválen na úrovni Vedení projektu.

Organizační struktura projektu

U realizovaných projektů je standardně využívána tříúrovňová organizační struktura v souladu s požadavky Kapitoly 3 Přílohy č. 6 Zadávací dokumentace s tím, že může být upravena dle potřeby (rozsahu) projektu. Na zahájení projektu bude potvrzena organizační struktura projektu včetně jmenování konkrétních osob pro stanovené řídicí pozice.



Obrázek 19 – Organnizační struktura projektu

Řídicí výbor (ŘV)

Řídicí výbor představuje nejvyšší orgán projektu, který formálně akceptuje výstupy projektu, kontroluje a sleduje průběh realizace projektu a schvaluje případné změny

projektu. Členy ŘV jsou zpravidla členové vrcholného vedení zúčastněných organizací, kteří mají dostatečné rozhodovací pravomoci ohledně řešení projektu.

Jednání ŘV se zpravidla účastní Sponzor projektu za stranu Objednatele, člen vedení za Zhotovitele a vedoucí projektu za obě zúčastněné strany. V případě potřeby jsou přizváni další účastníci. Periodicita schůzek je stanovena dle potřeby projektu, zpravidla 1x za měsíc.

Vedení projektu (VP)

Vedení projektu je řídicím a rozhodovacím orgánem, který průběžně koordinuje jednotlivé kroky realizace projektu a rozhoduje o dalším postupu v mezích stanovených smlouvou, či rozhodnutími ŘV.

Jednání VP se mohou podle vlastního rozhodnutí účastnit také členové ŘV. Na jednání mohou být přizváni další pracovníci, bude-li jejich účast potřebná pro řešení dané problematiky. Periodicita schůzek je stanovena dle potřeby projektu, zpravidla 1x za týden.

Realizační týmy (RT)

Realizační týmy jsou výkonným orgánem projektu, jejich členy jsou pracovníci Zhotovitele a Objednatele. Realizační týmy zpracovávají problematiku rozhodnutou na vedení projektu a za práci realizačních týmů zodpovídá příslušný vedoucí realizačního týmu. Členové realizačních týmů se aktivně účastní na realizaci jednotlivých projektových úkolů.

Složení realizačního týmu je obvykle následující:

- Vedoucí projektu za stranu Zadavatele a Uchazeče
- Architekt řešení Zadavatele a Uchazeče
- Vedoucí odpovídajícího RT
- Členové odpovídajícího RT

Pravomoci a odpovědnosti RT jsou obvykle následující:

- Plnění úkolů daných VP a harmonogramem Projektu
- Poskytování součinnosti mezi RT Uchazeče a Zadavatele
- Reportování průběhu, problémů, rizik vč. předkládání návrhů jejich řešení
- Připomínkování dokumentace dle pravidel a směrnic vztahujících se k dané oblasti

Seznam a popis klíčových rolí na projektu

Sponzor projektu

Je reprezentován některým z klíčových představitelů Objednatele, který má dostatečné rozhodovací pravomoci ohledně způsobu řízení Projektu v rámci předmětu Smlouvy. Sponzor Projektu je obvykle předsedou ŘV Projektu. Mezi hlavní úkoly sponzora Projektu patří např. následující aktivity:

- rozhodování ve sporných případech a eskalacích předaných ŘV.
- zajišťování nezbytné podpory Projektu ze strany vedoucích složek Zadavatele
- rozšiřování povědomí o Projektu na straně Zadavatele

- odpovídá za určení globálních cílů projektu a zabezpečení podmínek pro jejich dosažení
- odpovídá za dohled nad celkovými (business) výsledky projektu
- další aktivity, které souvisejí s působností ŘV

Člen řídicího výboru

Řídicí výbor představuje nejvyšší orgán Projektu, který formálně akceptuje projektové výstupy, kontroluje a sleduje průběh Projektu a schvaluje změny Projektu. Je vrcholným rozhodovacím orgánem s primární úlohou udávat směr a zajišťovat rozhodování o Projektu. Členy ŘV jsou zástupci Objednatele i Zhotovitele.

Vedoucí projektu

Vedoucí projektu zodpovídají za průběh realizace celého projektu. Mezi vedoucím projektu za Zhotovitele a Objednatele probíhá úzká spolupráce.

Vedoucí projektu za Zhotovitele především

- zodpovídá za celkovou koordinaci, průběh projektu a eskalaci případných problémů
- zodpovídá za řízení veškerých činností na straně Zhotovitele
- zpracovává veškeré plány realizace projektu a zodpovídá za jejich dodržení spolu s vedoucím za stranu Objednatele
- koordinuje přípravu dílčích zadání pro realizační týmy
- stanovuje pravidla pro řízení projektu (pracovní postupy, řízení změn, kvality atd.)
- zajišťuje správu projektové dokumentace v průběhu celého projektu
- svolává všechna oficiální setkání konaná na úrovni projektu
- připravuje podklady pro jednání Řídicího výboru projektu
- řeší připomínky a posuzuje podněty od všech osob zařazených do projektu;
- má právo navrhnout Řídicímu výboru projektu změnu smlouvy
- připravuje Předávací protokoly a Akceptační protokoly za Zhotovitele

Vedoucí projektu za Objednatele především zodpovídá za

- řízení veškerých činností na straně Objednatele
- eskalaci problémů, které je třeba řešit na úrovni ŘV
- zajištění a koordinaci účasti uživatelů na projektu a zabezpečení plynulého chodu
- vypracování specifikace požadavků od uživatelů, za dodání potřebných podkladů pro zpracování projektu a řešení protichůdných požadavků uživatelů
- kvalitu výstupů a dodržování zásad pro práci na projektu ze strany svého týmu
- schvaluje Předávací protokoly a Akceptační protokoly za Objednatele

Architekt řešení

Architekt řešení je role, která je obsazena odborníkem s patřičnými zkušenostmi a znalostmi za stranu Zadavatele i Uchazeče, který bude plně odpovědný za dvě oblasti projektu:

- vytvoření Technické a procesní specifikace (v rámci fáze projektu analýza a návrh řešení)
- prosazení navržené Technické a procesní specifikace (v rámci fáze realizace projektu)

Hlavní konzultant/Analytik senior

Role Analytik senior bude obsazena odborníkem s patřičnými zkušenostmi a znalostmi v dané oblasti. Odpovědný pracovník v této roli bude v průběhu realizace projektu provádět následující aktivity:

- analýza problematiky a vytvoření dokumentů Analýza a návrh řešení

- řízení interview se zástupci Objednatele, a to jak obsahově, tak koncepčně
- spolupráce s Architektem řešení při vytváření návrhu řešení
- spolupráce při průběžné revizi implementovaného řešení za účelem kontroly kompatibility vyvíjeného řešení s dokumentem Technická a procesní specifikace
- zabezpečení komunikace s technickým a vývojovým týmem

Vedoucí pracovník vývoje/Vývojář Senior

Pozice Hlavní pracovník vývoje bude obsazena odborníkem s patřičnými zkušenostmi a znalostmi, který bude plně odpovědný za následující oblasti Projektu:

- vývoj řešení, včetně jeho kompletního otestování a zdokumentování
- podpora pilotního provozu
- podpora uživatelských akceptačních testů (UAT)

V průběhu realizace Projektu bude osoba v této roli provádět následující aktivity:

- spolupráce s Architektem řešení při vytváření návrhu celkové architektury řešení
- řízení procesů nezbytných pro úspěšný průběh vývoje, a to zejména:
 - řízení vývoje a řízení změn zdrojového kódu (Source code management)
 - podpora realizace a vyhodnocování průběhu testování (Test management)
 - kontrola vytvoření kompletní dokumentace (Document management)
- spolupráce na vývoji řešení, včetně jeho zdokumentování a předání k testům

Vývojář

V průběhu realizace Projektu bude osoba v této roli provádět následující aktivity:

- spolupráce na vývoji řešení, včetně jeho zdokumentování a předání k testům
- podpora uživatelských akceptačních testů (UAT)
- podpora pilotního provozu

Analytik testů

Na pozici Analytik testů bude obsazen odborník s patřičnými zkušenostmi a znalostmi, který bude plně odpovědný za:

- tvorbu test analýzy
 - test case
 - test script
- během psaní scénářů zaznamenává požadavky na testovací data
- po dokončení přípravy testů pro danou aplikaci/část aplikace připraví detailnější plán testů pro další fázi testování softwaru a stanoví hodnotící kritéria
- spolupráce exekuci testů

Tester

V rámci realizace Projektu bude pracovník v této roli provádět následující aktivity:

- provádí manuální testy podle předem připravených testovacích scénářů,
- zaznamenává a vede evidenci výsledků (bug tracking) jednotlivých testů podle scénářů.

4.2.2.2 Realizace projektu

Sledování vývoje projektu

V průběhu realizace projektu je třeba sledovat jeho vývoj a tyto údaje porovnávat s plánovanými výsledky a provádět vyhodnocení rozdílu mezi plánovaným a reálným průběhem projektu.

Jedná se o proces prováděný kontinuálně po celou dobu Projektu, při kterém PM neustále monitoruje a kontroluje aktuální stav Projektu a průběžně jej porovnává s Plánem Projektu (včetně časového harmonogramu a počítanými náklady na projekt). Následně PM přijímá relevantní opatření a zajišťuje provedení relevantních činností k tomu, aby mohl být Projekt ukončen v naplánovaném rozsahu a čase a v rámci naplánovaného rozpočtu.

Činnosti vykonávané v průběhu tohoto procesu zahrnují zejména:

- Přidělování práce jednotlivým členům realizačního týmu.
- Kontrola skutečně odvedené práce a porovnání s plánovaným vývojem prací na Projektu.
- Kontrola dodržování časového harmonogramu Projektu.
- Porovnání skutečných rizik Projektu a jejich skutečného vývoje s Registrem rizik.
- Kontrola průběžných ekonomických výsledků Projektu a porovnávání se schválenou kalkulací projektu.
- Odhad činností nutných k dokončení Projektu.
- Odhad zdrojů nutných k dokončení Projektu.
- Odhad zbývajících časového rámce Projektu.

Sledování rizik a trendů projektu

V průběhu tohoto procesu shromažďuje PM informace a údaje potřebné k určení trendů v jednotlivých oblastech Projektu a zhodnocení stavu a vývoje aktuálních rizik. Na základě těchto údajů poté průběžně kontroluje Projekt a adekvátně reaguje na momentální situaci.

Oblasti sledované a hodnocené v průběhu tohoto procesu zahrnují zejména:

- Doposud vyčerpané zdroje (finanční, lidské a materiálové).
- Doposud odvedená práce.
- Kvalita doposud odvedené práce.
- Efektivita použitých projektových procesů a postupů.
- Dodržování časového harmonogramu.
- Stav rizik a efektivita (použitých) plánovaných opatření.
- Stav vztahu s Objednatelem

Kontrola projektu

Tento proces vychází z výsledků procesů Sledování rizik a trendů Projektu a s ohledem na tyto výsledky jsou v jeho rámci připraveny veškeré nutné úpravy/změny Projektu a jeho řízení. Změny mohou být nutné zejména z důvodu zachování:

- Konečného termínu dodávky.
- Načasování jednotlivých milníků Projektu.
- Kritické cesty/kritického řetězu.
- Organizační struktury Projektu.
- Složení a množství zdrojů.

Pokud je možné vyhnout se posunu konečného termínu dodávky či jednotlivých milníků cestou změn v projektových aktivitách, může být výsledkem tohoto procesu pouze vydání nových Pracovních instrukcí pro jednotlivé členy realizačního týmu. Pokud jsou ale naopak nutné zásadní změny jako např. zrušení či sloučení některých milníků Projektu, může být výsledkem tohoto procesu změna/aktualizace projektových plánů definovaných v Plánu Projektu a/nebo Plánu řízení kvality Projektu.

Vykazování projektu

V rámci tohoto procesu je vystavována pravidelná měsíční Zpráva o stavu Projektu

Obsah Zprávy musí vždy odpovídat rozsahu a komplexnosti Projektu a také rozsahu rizik s Projektem spojených. Je v zájmu PM, aby do Zpráv zahrnul maximum relevantních informací

tak, aby bylo eliminováno riziko případných chybných či pozdních rozhodnutí kterékoliv ze zúčastněných stran, ke kterým by mohlo dojít (mimo jiné i) z důvodu nedostatečné nebo nevčasné informovanosti.

Zpráva pro Zadavatele o stavu Projektu

Slouží k poskytnutí nejdůležitějších informací o stavu Projektu Objednateli, a to formální cestou. Přesný formát Zprávy se může lišit Projekt od Projektu a může se pohybovat v rozmezí od jednostránkového přehledu nejdůležitějších oblastí Projektu až po mnohastránkový dokument detailně popisující pokrok dosažený na Projektu od počátku Projektu do konce sledovaného období. Konkrétní forma vždy musí odpovídat potřebám a požadavkům Objednatele a také podmínkám Smlouvy uzavřené s Objednatelem.

Na podkladě vystavené Zprávy zorganizuje PM (měsíční) Kontrolní schůzku Projektu, které se zúčastní, není-li stanoveno jinak (např. Smlouvou), on sám a jeho liniový manažer a pověření pracovníci za stranu Objednatele. Ze schůzky, na níž se detailně prochází pokrok dosažený do konce sledovaného období na Projektu a výhled do konce Projektu, pořídí PM Zápis, včetně seznamu úkolů, které z Kontrolní schůzky Projektu vyplynuly.

4.2.2.3 Ukončení projektu

Dokončení projektu

Tento proces plynule navazuje na procesy probíhající ve Realizace Projektu, kdy je Projekt průběžně monitorován a kontrolován. Když se Projekt blíží ke svému konci, soustředí se PM (v rámci procesu Dokončení Projektu) na aktivity spojené s ujištěním se, že byly splněny všechny milníky Projektu, dodrženy všechny povinnosti dané Smlouvou, dílo jako celek bylo předáno a Objednatelem písemně akceptováno.

Mezi nejdůležitější aktivity tohoto procesu patří zejména:

- Kontrola dodávky proti Plánu Projektu.
- Kontrola dodávky proti Smlouvě s Objednatelem a revize všech oblastí, které by mohly být předmětem reklamací či vymáhání škod.
- Řízení procesu Akceptace dodávky Objednatelem a zajištění Objednatelem podepsaného Akceptačního protokolu na celé dílo.
- Revize projektových dokumentů a zajištění jejich archivace.
- Příprava a distribuce hodnocení jednotlivých členů realizačního týmu.

Uzavření projektu

Během tohoto procesu dochází k formálnímu ukončení a uzavření Projektu a k revizi a zhodnocení jeho průběhu. Tato fáze začíná někdy již po předání Projektu Objednateli do živého provozu a faktickém ukončení dodávky Projektu (tj. po podpisu Akceptačního protokolu a (do)vyfakturování Projektu), často však až po skončení záruční lhůty.

PM uzavře rozpočet Projektu, vypořádá zbývající WIP a vystaví finální fakturu pro Objednatele. Je vystavena závěrečná Zpráva o stavu Projektu.

4.3 APLIKACE SLUŽEB PODPORY PROVOZU

Každý provozní prvek podpory provozu v projektu plní svou roli. Tyto prvky jsou provázány a spolupracují dle nastavených procesů ISO 20000.

Service Desk

Service desk (dále SD) zajišťuje zejména tyto činnosti:

- Hlavní vstupní bod pro pracovníky Zadavatele
- Příjem všech požadavků pracovníků Zadavatele
- Distribuce požadavků na jednotlivé řešitele
- Vzdálené správy, telefonické nebo mailové konzultace
- Procesní dohled a sledování plnění zadaných požadavků nad provozními prvky (pobočky, dohledové centrum, 3. strany) a dohled nad plněním SLA
- Řešení eskalací požadavků uživatele
- Shromažďování podkladů pro měření služby, statistické výstupy
- Pracuje v non-stop režimu – zadávat požadavky anebo hlásit poruchy je možné 24 hodin denně 7 dnů v týdnu.

Service Desk uchazeče bude zajišťovat

- Jednotné kontaktní místo pro příjem požadavků v požadovaném pracovním kalendáři s využitím následujících komunikačních kanálů – telefon, e-mail, web
- Procesní dohled nad plněním zadaných požadavků nad provozními prvky (dohledové centrum, 3tí strany) a dohled nad plněním SLA
- Monitoring
- Řešení incidentů prostřednictvím vzdáleného přístupu na zařízení s garantovanou dobou odezvy řešení (SLA)
- Řešení eskalací požadavků uživatele
- Statistické výstupy z hlediska plnění smluv

Technologická podpora

Uchazeč definuje pracoviště pro podporu provozu, kde se tým specialistů stará o optimalizaci provozu, kvalitu technologií služeb, průběžné zlepšování technologií, technologickou dokumentaci a udržení kontinuity nasazených technologií.

Pracoviště rovněž poskytuje podporu technikům při nestandardních incidentech a řešení problémů. Provádí rovněž posouzení dopadů chystaných technologických změn na provozované systémy. Pracoviště společně s SD a techniky řeší technologicky procesy problem managementu.

Další případná technologická podpora je také zajišťována v odborných divizích Uchazeče, které disponují řadou specialistů vybavených potřebnými certifikáty.

Projektová kancelář

Projektová kancelář je řídicí prvek odpovědný za realizaci a plnění smluvních podmínek, je zastoupena na výkonném výboru projektovým manažerem a má tyto úkoly:

- Plánuje postup prací v provozu a plánuje změnové projekty

- Nastavuje procesy provozu a řídí změnové projekty
- Sleduje a vyhodnocuje rizika vzešlé z provozu
- Kontroluje a řídí postup prací
- Komunikuje o jednotlivých nebo globálních problémech se Zadavatelem
- Předkládá reporty a vyhodnocení služeb za smluvně dané období
- Spolu s technologickou podporou řídí procesy „problem managementu“
- Zpracovává dokumentaci provozu

Projektová kancelář bude zajišťovat:

- vyhodnocování kvality služeb;
- pravidelné měsíční schůzky;
- pravidelný měsíční reporting objemu řešených výpadků v elektronické podobě;
- pravidelný měsíční reporting plnění kvalitativních parametrů SLA v elektronické podobě.

5 POŽADAVKY NA SOUČINNOST ZADAVATELE

Kapitola uvádí podle požadavků kapitoly 3 Přílohy č. 6 Zadávací dokumentace popis potřebné součinnosti Zadavatele.

5.1 SOUČINNOST ZADAVATELE PRO ANALÝZU A NÁVRH

Vzhledem k faktu, že pro provedení detailní analýzy a návrhu systému JISPSV-PIP dle kapitoly 3.1.1 Přílohy č. 6 Zadávací dokumentace, bude k dispozici omezený počet klíčových uživatelů (4) s maximální kapacitou 20 %, bude nezbytně nutné zajistit následující:

- nominovat klíčové uživatele tak, aby měli dostatečně delegovanou pravomoc k odpovědnému a zodpovědnému rozhodování o obsahu analýzy a návrhu řešení;
- nominovat klíčové uživatele tak, aby měli maximálně možný přehled a znalosti o celém systému JIPSPV pro zajištění integrity řešení JISPSV-PIP v kontextu ostatních částí JIPSPV;
- zajistit jejich dostupnost i po celou dobu další realizace s minimální kapacitou 10 %, tj. i v průběhu implementace a provozu, aby byla zajištěna informační kontinuita, popř. s dostatečným předstihem zajistit výměnu a v rámci projektového řízení a dle dohodnutých pravidel ji aplikovat;
- zajistit dostupnost odborných pracovníků třetích stran, pokud nebude možné odborné podklady dodat vlastními silami;
- zajistit dostupnost a koordinaci pracovníků třetích stran, kteří budou implementovat další části celého systému JIPSPV;
- před zahájením fáze Návrh realizace provést v kooperaci s Uchazečem detailní plán rozložení času a místa na jednotlivé schůzky a činnosti spojené s přípravou podkladů pro Uchazeče, revizemi výstupů fáze a také akceptaci analýzy a návrhu řešení;
- pro všechna setkání zajistit rezervace zasedacích místností odpovídající velikosti, vybavenou projektorem a magnetickou tabulí s funkčními barevnými fixy (min. 4 různé barvy) a/nebo flipchartem s dodatečnou zásobou (min. 10 ks) oboustranně čistých papírů a funkčními barevnými fixy (min. 4 různé barvy).

Dále je pro účely analytických a návrhových prací zajistit:

- platné interní předpisy a nařízení týkající se pravidel práce se systémy v rámci Ministerstva práce a sociálních věcí, Generálního ředitelství úřadu práce a Úřadů práce České Republiky;
- stávající platná bezpečnostní dokumentace.

Pro všechny pracovníky Uchazeče, kteří budou provádět odborné činnosti, bude třeba zajistit přístup k modelovacímu nástroji a jeho úložišti následovně:

- Při zahájení fáze Návrh realizace dodat šablonu písemné žádosti o přístup k modelu
- Zajištění přístupu pracovníkům Uchazeče k modelu v souladu s dodanými písemnými žádostmi
- Zajištění přístupu pracovníkům Uchazeče k modelu i formou vzdáleného přístupu, pokud to bezpečnostní politika dovoluje, popř. dodat další potřebné podklady Uchazeči, aby bylo vyhověno všem bezpečnostním požadavkům Zadavatele.
- Zajistit řádnou a bezpečnou správu modelů včetně jejich pravidelného zálohování.
- V následných fázích zajistit přístup pro další pracovníky Uchazeče, kteří pro svoji činnost budou nezbytně nutně potřebovat informace z modelů, popř. je mohli aktualizovat dle reality implementace nebo změnových požadavků.

5.2 SOUČINNOST ZADAVATELE PRO TESTOVÁNÍ

V souladu s kapitolou 3.1.2 Přílohy č. 6 Zadávací dokumentace za účelem provedení akceptačních testů, je třeba, aby v rámci toho bylo v součinnosti zajištěno následující:

- Všichni pověření pracovníci musí mít delegovanu pravomoc a plnou zodpovědnost za konečné kvalifikované a svobodné rozhodování v průběhu akceptačních testů a též za jejich výstupy.
- Všichni pověření pracovníci musí mít maximálně možný přehled a znalosti o celém systému JIPSPV pro zajištění integrity řešení JIPSPV-PIP v kontextu ostatních částí JIPSPV a to v rozsahu, který odpovídá příslušné části, za kterou budou přebírat zodpovědnost za akceptační testy.
- Zajistit v definovaných termínech součinnost s dodavateli nebo provozovateli systémů třetích stran při realizaci testů.

Za účelem provedení zátěžových testů je třeba, aby v rámci toho bylo v součinnosti zajištěno pomocné testovací prostředí s výkonnostními parametry produkčního prostředí.

Za účelem provedení bezpečnostních testů je třeba, aby v rámci toho bylo v součinnosti zajištěno pomocné testovací prostředí.

5.3 SOUČINNOST ZADAVATELE PRO MIGRACI DAT

V rámci součinnosti migrace popsané v kapitole 3.1.3 Přílohy č. 6 Zadávací dokumentace dat je nezbytně nutné, aby byly detailně zmapovány všechny datové prvky, jejich data, validita, platnost a také vztahy mezi nimi. V této souvislosti v rámci součinnosti bude třeba, aby Zadavatel:

- zajistil vlastními silami nebo prostřednictvím třetích stran detailní aktuální struktury a popisy datových struktur všech systémů, které budou předmětem migrace;
- zajistil, koordinoval a řídil součinnost třetích stran tam, kde to nebude sto zvládnout vlastními silami či prostředky;
- zajistil pro etapu Implementace všechny podklady a to nejpozději do dvou (2) měsíců od začátku zahájení realizace etapy;
- zajistil kvalifikované a znalé pracovníky pro všechny datové struktury (vlastní či třetí strany), kteří budou spolupracovat s pracovníky Uchazeče na konzultacích k vlastnostem migrovaných dat a jejich relevanci pro migrování v kontextu výstupů fáze Návrh realizace;
- zajistil kvalifikované a znalé pracovníky, kteří zajistí, že navržená struktura dat pro migraci včetně formátů bude při přípravě datového vzorku a produkčních dat ze stany Zadavatele dodržena.

Zadavatel poskytne data dle vzájemné dohody tak, aby migrace dat mohla proběhnout co nejefektivněji s minimálním množstvím nezbytně nutných datových transformací nebo dohledávání integritních vztahů. V této souvislosti pro vybrané migrované struktury bude třeba dodat výstupy v některém z uvedených formátů:

- strukturovaný XML soubor ve struktuře, která bude vzájemně na projektové úrovni odsouhlasena;
- jednoduchý CSV soubor s datovými větami každá na jednom řádku oddělené na projektové úrovni dohodnutým validním oddělovačem;
- formát nekomerční volně dostupné databáze tak, aby jednotlivé tabulky udržovaly mezi sebou veškeré integritní datové vazby.

Zadavatel poskytne datový vzorek pro ověření migrace a správnosti migrovaných dat a to v termínu nejméně jednoho (1) měsíce před zahájením migrace. Datový vzorek bude dodán v dohodnutém formátu a struktuře. Současně s datovým vzorkem bude Zadavatelem dodán podklad pro možnost zajištění přípravy a provedení kontroly správnosti a úplnosti migrovaných dat.

Zadavatel poskytne uchazeči celková produkční data v dohodnutém formátu a struktuře nejpozději dva (2) týdny před zahájením přechodu na nový systém JISPSV-PIP pro účely finálních testů migrace.

Data pro přechod na nový systém JISPSV-PIP budou poskytnuta Zadavatelem v dohodnutém formátu a struktuře ke dni odstávky systému stávajícího. Zadavatel musí zajistit neměnnost dat od dne odstávky.

Současně zajistí vlastními silami nebo prostřednictvím třetích stran konzultanty, kteří budou k dispozici na technické řešení problémů vzniklých v souvislosti s migrovanými daty a to zejména z pohledu:

- | | |
|--------------|--------------|
| – struktury, | – validity, |
| – formátu, | – integrity. |

Dále s daty jak pro finální testy migrace, tak i pro ostrou migraci bude Zadavatelem dodán podklad pro možnost zajištění přípravy a provedení kontroly správnosti a úplnosti migrovaných dat.

5.4 SOUČINNOST ZADAVATELE PRO NASAZENÍ

V souladu s kapitolou 3.1.4 Přílohy č. 6 Zadávací dokumentace pro nasazení je třeba, aby bylo součinností Zadavatele zajištěno:

- Pověření pracovníci Zadavatele musí mít dostatečná oprávnění pro odsouhlasení a realizaci implementačních kroků;
- Pověření pracovníci Zadavatele musí mít delegovánu pravomoc zajistit součinnost s dodavateli nebo provozovateli souvisejících systémů;
- Poskytnutí výpočetní platformy v obou datových centrech Zadavatele pro produkční a testovací prostředí (pokud nebude v době implementace k dispozici platforma v obou datových centrech, bude na přechodnou dobu použito prostředků pouze jedno datové centrum);
- Poskytnutí dočasných prostředků výpočetní platformy pro provádění integračních a zátěžových testů;
- Zajištění provozní konfigurace výpočetní platformy podle primárních požadavků po úpravách na základě výsledků zátěžových testů apod., odsouhlasených oběma stranami;
- Poskytnutí licenčních klíčů pro produkty, jejichž licence jsou Zadavatelem poskytovány pro realizaci řešení;
- Poskytnutí přístupu k předmětným prostředkům Zadavatele pro pracovníky Uchazeče;
- Poskytnutí síťové a komunikační infrastruktury LAN / WAN pro potřeby provozu Systému a zajištění potřebných a Zadavatelem schválených úprav konfigurace sítí.

5.5 SOUČINNOST ZADAVATELE PRO ŠKOLENÍ

V souladu s kapitolou 3.1.5 Přílohy č. 6 Zadávací dokumentace je třeba zajistit následující:

Školící prostory

Školící prostory a učebny musí být s dostatečným předstihem v souladu s dohodnutým termínovým plánem školení rezervovány. Školitelé Uchazeče musí mít zajištěn vstup minimálně jeden (1) den před zahájením školení, za účelem ověření funkční techniky. V den školení je nezbytné, aby školitelé Uchazeče měli přístup minimálně dvě (2) hodiny před zahájením školení a minimálně dvě (2) hodiny po jeho skončení.

Velikost a vybavení školících prostor

Pro školící učebny je třeba v rámci součinnosti Zadavatele zajistit následující:

- vybavení každé školící učebny prezentační a školící technikou minimálně v rozsahu:
 - funkční projektor a nepoškozené projekční plátno, popř. volná bílá zeď;
 - magnetická tabule s funkčními barevnými fixy (min. 4 různé barvy) a/nebo flipchart s dodatečnou zásobou (min. 50 ks) oboustranně čistých papírů a funkčními barevnými fixy (min. 4 různé barvy);
 - funkční pracovní PC stanice vyhovující minimálním standardům pro práci uživatelů ministerstva nebo úřadů ideálně pro každého jednotlivého školeného pracovníka a jednu stanici pro školitele (**Poznámka:** Případně lze k proškolení využít mobilní pracoviště, jenž bude dodané v rámci plnění.);
 - pracovní stanice musí mít nainstalovanou aktuálně uvolněnou verzi MS Office (zejména pak MS PowerPoint) ke dni, kdy bude předána školící dokumentace;
 - pracovní stanice musí vyhovovat nárokům na školenou problematiku včetně nainstalovaných funkčních a aplikačních rozšíření dle specifikace dodané Uchazečem;
 - pracovní stanice musí být připojené do LAN/WAN sítě s přístupem k testovacímu a školícímu prostředí a též k portálu s uživatelskou a školící dokumentací;
 - zajištění jedné funkční černobílé laserové tiskárny připojené přímo ke stanici školitele, popř. prostřednictvím síťového sdílení s nastavenými oprávněními k tisku;
 - zajištění přístupu k internetu pro školitele Uchazeče;
- zajištění oprávnění přístupu k testovacímu a školícímu prostředí a též k portálu s uživatelskou a školící dokumentací pro všechny účastníky školení včetně školitelů Uchazeče;
- zajištění místností tak, aby každý školený pracovník měl dostatečný osobní prostor nejen pro práci na pracovní stanici, ale i na samotném stole pro případnou tvorbu poznámek do školících materiálů;
- zajištění místností tak, aby byla vybavena funkční vzduchotechnikou;
- zajištění dvou (2) samostatných stolů (dle dispozice místa uvnitř nebo v těsné blízkosti školící místnosti) pro uložení občerstvení (přesnídky a nápojů) a dále pak dostupnost odpadkového koše a také nádobí (talíře, hrnky a skleničky);
- jestliže to místo umožňuje, je třeba zajistit přístup do kuchyňky a/nebo ledničky.

Termíny

Jelikož Zadavatel vypracuje termínový plán školení a seznámí s ním uchazeče nejpozději do dvou (2) týdnů před zahájením školení, je nutné, aby:

- termín zahájení vypracovávání termínového plánu v rámci projektového řízení nahlásil nejpozději dva (2) týdny před jeho zahájením, aby byl zapracován do projektového harmonogramu;

- Zadavatel v průběhu vypracovávání termínového plánu spolupracoval s pověřeným školitelem Uchazeče, který bude znát detaily implementovaného systému JISPSV-PIP z pohledu náplně, organizace, kapacity a jiných záležitostí školení;
- Zadavatel stanovil počáteční termín školení v souladu s projektovým plánem, skutečným stavem realizace a vždy po vzájemné dohodě obou stran;
- Zadavatel plánoval počty školených uživatelů v termínech maximálně efektivně tak, aby vždy byla bezpečně naplněna kapacita školící místnosti v rozsahu z 85-100 % ne méně;
- Zadavatel zajistil všem školeným pracovníkům v souladu s termínovým plánem časový prostor v rozsahu jeden (1) den na účast na školení, a to s dostatečným předstihem před jeho zahájením, minimálně však alespoň deset (10) pracovních dní;
- Zadavatel zajistil, že všichni školení pracovníci budou v den školení v učebně minimálně třicet (30) minut před zahájením školení;
- všichni školení pracovníci bez výjimky byli počítačově gramotní minimálně na úrovni základní práce s PC, kancelářskými balíky MS Office (Outlook, Word, Excel, PowerPoint), práce v internetovém prohlížeči a v dostatečné míře ovládat práci s klávesnicí, myší a tiskárnou.

5.6 SOUČINNOST PRO PROJEKTOVÉ ŘÍZENÍ

V souladu s kapitolou 3.1.6 Přílohy č. 6 Zadávací dokumentace je třeba zajistit součinnost nebytnou pro realizaci projektu a to jak na organizační úrovni, tak i na úrovni řízení.

V případě, že vznikne odůvodnitelný požadavek na straně Uchazeče na kanceláře a přístupy do budov, je třeba zajistit pro dohodnutý počet pracovníků Uchazeče dle aktuálně realizované fáze projektu, též přístup do budov Ministerstva práce a sociálních věcí, Generálního ředitelství úřadu práce. A dále pak v rozsahu dle součinnosti pro analýzu a návrh (viz kapitola 5.1) též i poboček či kontaktních pracovišť Úřadu práce v rámci celé České republiky.

Pro vybraný počet pracovníků Uchazeče, jako jsou např. Projektový manažer, Architekti a další pracovníci pravidelně docházející na Ministerstvo práce a sociálních věcí či Generální ředitelství úřadu práce, též vstupní kartičky do objektů, pokud to bezpečnostní politika dovoluje, popř. dodat další potřebné podklady Uchazeči, aby bylo vyhověno všem bezpečnostním požadavkům Zadavatele.

Bude-li v rámci poskytnutých kanceláří poskytnuto i připojení k internetu, které bude autentizováno, je v rámci součinnosti nezbytné, aby Zadavatel zajistil pro všechny dohodnuté pracovníky Uchazeče přístupová oprávnění, dle politik a pravidel bezpečnosti resortu.

Protože přidělené kanceláře mohou být nejen na Ministerstvu práce a sociálních věcí, ale i v jiných částech, jako je Generální ředitelství úřadu práce, popř. též i pobočky či kontaktní pracoviště Úřadu práce v rámci celé České republiky, je třeba i zde autentizované připojení k internetu zajistit, bude-li to povaha vykonávané pracovní činnosti vyžadovat. A to vždy po vzájemné dohodě obou stran na úrovni projektového vedení, nebude-li možné připojení zajistit operativně ze strany Zadavatele jinak.

6 SEZNAM POTŘEBNÉHO HW

Následující seznam sumarizuje předpokládané požadavky na servery pro realizaci zakázky, uvedené v předchozích kapitolách.

Produkční prostředí

Typ serveru	Počet	Poznámka
Fyzický HW	11	
Virtuální počítač	55	

Testovací prostředí

Typ serveru	Počet	Poznámka
Fyzický HW	0	
Virtuální počítač	47	

7 POUŽITÉ ZKRATKY

Zkratka	Význam
AD	Active Directory
AD CS	Active Directory Certificate Services
ADO	ActiveX Data Objects
API	Application Programming Interface
BPMN	Business Process Model and Notation
CA	Certifikační autorita
CAL	Klientská licence Microsoft (Client Access License)
CAS	Exchange role Client Access Server
DAG	Exchange Database Availability Group
DHCP	Správa adresního prostoru IP protokolu
CRL	List odvolaných certifikátů
CSV	Comma separated value
DB	Databáze
DC1 / DC2	Datové centrum 1 / Datové centrum 2
DMS	Systém správy dokumentů (Document Management System)
DNS	Domain Name Service
ECMA	Extensible Connectivity Management Agent
ESB	Enterprise Service Bus, MS BizTalk
FEP	Forefront Endpoint Protection
FIM	Forefront Identity Manager
FSMO	Flexible Single Master Operations
GPO	Group Policy Object
HW	Hardware
ICT	Informační a komunikační technologie
IdM	Identity Management
IIS	Internet Information Server
IS	Informační systém
IT	Informační technologie
JBOD	Diskové úložiště „Just a Bunch Of Disks“

JIP	Jednotný identitní prostor
JISPSV	Jednotný informační systém práce a sociálních věcí
JISPSV-PIP	Jednotný informační systém práce a sociálních věcí – Provozní integrační prostředí
KAAS	Katalog autentizačních a autorizačních služeb
KDC	Key distribution center
LDAP	Lightweight Directory Access Protocol
MBS	Exchange role Mailbox Server
MS	Microsoft
O2STA	O2 Smart Trusted Archive – „Důvěryhodné úložiště“
OS	Operační systém
OVM	Orgán veřejné moci
PC	Osobní počítač (Personal Computer)
PKI	Infrastruktura správy a distribuce veřejných klíčů z asymetrické kryptografie (Public Key Infrastructure)
RBAC	Řízení oprávnění na bázi role (Role-Based Access Control)
SC	Systém Center
SCCM	Systém Center Configuration Manager
SCORM	Referenční model pro e-learning (Shareable Content Object Reference Model)
SHA1	Secure Hash Algorithm 1
SHA2	Secure Hash Algorithm 2
SID	Security Identifier
SLA	Service Level Agreement
SNMP	Simple Network Management Protocol
SOAP	Simple Object Access protocol
SPN	Service Principal Name
SSH	Secure Shell
SSO	Single Sign-On
SW	Software
TSA	Autorita časového razítka (Time Stamp Authority)
UML	Unified Modeling Language
WBEM	Web-Based Enterprise Management

VM	Virtuální počítač
WINS	Windows Internet Name Service
WMI	Windows Management Instrumentation
WSUS	Služba zajišťující aktualizaci softwaru pro operační systémy Microsoft Windows (Windows Server Update Services)
XML	Extensible Markup Language
XSD	XML Schema Definition
XSLT	eXtensible Stylesheet Language Transformations