VŠEOBECNÁ ZDRAVOTNÍ POJIŠŤOVNA ČESKÉ REPUBLIKY

Standardy a podmínky dodávek informačního systému Všeobecné zdravotní pojišťovny ČR

Informační architektura VZP ČR

Verze: 5.6
Datum: 1.1.2016

Obsah

Seznam obrázků

Historie dokumentu

Verze	Datum	Autor	Popis
1.00	1.8.2007	ÚICT VZP ČR	Vytvoření dokumentu
1.01	8.8.2007	VZP ČR	Zapracování připomínek
1.02	9.8.2007	VZP ČR	Formální úpravy
1.03	30.8.2007	VZP ČR	Doplnění kapitol Monitoring, Zálohování, Auditní stopa
1.04	31.8.2007	VZP ČR	Formální úpravy
1.05	1.10.2007	VZP ČR	Úprava kapitoly monitoring
1.06	5.10.2007	VZP ČR	Formální úpravy
1.07	17.9.2008	VZP ČR	Doplnění integračních standardů
2.00	24.4.2009	VZP ČR	Doplnění verze
3,00	25.1.2010	VZP ČR	Zapracování připomínek
3.1	9.4.2010	VZP ČR	Zapracování připomínek
4.00	1.9.2010	VZP ČR	Zapracování připomínek
4.1	1.6.2011	VZP ČR	Zapracování připomínek
5.0	1.12.2011	VZP ČR	Změna struktury standardů, zapracování připomínek
5.1	1.3.2012	VZP CŘ	Zapracování připomínek
5.2.	1.9.2012	VZP ČR	Zapracování připomínek, doplněna příloha
5.3.	1.12.2012	VZP ČR	Zapracování připomínek, úprava příloh
5.4.	1.6.2014	VZP ČR	Zapracování připomínek, úprava příloh
5.5.	1.9.2015	VZP ČR	Doplnění verze
5.6.	1.1.2016	VZP ČR	Doplnění verze

1. Popis standardů informačního systému

V této kapitole jsou popsány standardy informačního systému Všeobecné zdravotní pojišťovny České republiky.

1.1 Úvod

Dokument obsahuje sadu standardů pro vybudování a především další udržování a rozvoj informační architektury v souladu s požadavky uživatelů a vedení pojišťovny. Vytvořené standardy jsou základem pro další rozšiřování systému zaváděním nových komponent a to jak „standardních“, tak i vytvářených dle specifických požadavků VZP ČR. Zavedení úplného souboru standardů a jejich následná důsledná aplikace zajišťuje otevřenost systému na jedné straně a integrovatelnost na straně druhé. Ve chvíli, kdy pojišťovna optimalizuje svou informační architekturu včetně důsledného sdílení komponent IS je zavedení standardů nutnou podmínkou pro bezporuchový chod ICT.

Standardy pro informační architekturu VZP ČR jsou vytvářeny především v oblastech:

- technologická
- aplikační
- datová
- integrační
- komunikační
- bezpečnostní - základní rámec bezpečnostních standardů pro IS
- zálohovací a archivační
- monitorovací a auditní

V případě specifikace rozšíření informačního systému zaváděním nových komponent ve smlouvě s dodavatelem, má specifikace uvedená v této smlouvě přednost před Standardy. Tato nová komponenta musí projít schválením systémového integrátora a poté budou doplněny Standardy.

Přílohy uváděné v tomto dokumentu budou příslušnému dodavateli předány při podpisu smlouvy s VZP ČR.

1.2 Manažerské shrnutí

V dnešním světě informačních a komunikačních technologií, který stále prodělává bouřlivý vývoj, je standardizace jedním ze záchytných bodů, kterých se může organizace provozující a rozšiřující svůj informační systém zmírnit rozmanitost používaných technologii a tak přispět k homogenitě prostředí, stejně jak se z distribuovaných systémů směruje ke konsolidované a centralizované architektuře. V dalších kapitolách dokumentu je zachycena standardizace a doporučení využívání technologií tak jak je tomu ve většině případů již nyní v nepsané formě.

Cílem standardizace je především:

- kvalita
- bezpečnost
- kompatibilita
- interoperabilita
- úspora prostředků

Tento dokument si klade za cíl vymezit hlavní standardy, na jejichž bázi budou informační a komunikační technologie (ICT) VZP ČR dále rozvíjeny. Dokument zachycuje standardizaci procesů a technologií spojených jak s vývojem ICT, tak současně s jejich provozem.

Aplikací standardů dosáhne v rámci dalšího vývoje nejenom celistvosti ICT jako takových, ale i návaznost na standardy v komunikaci s okolním světem – bankami, státními institucemi, partnery, atd.

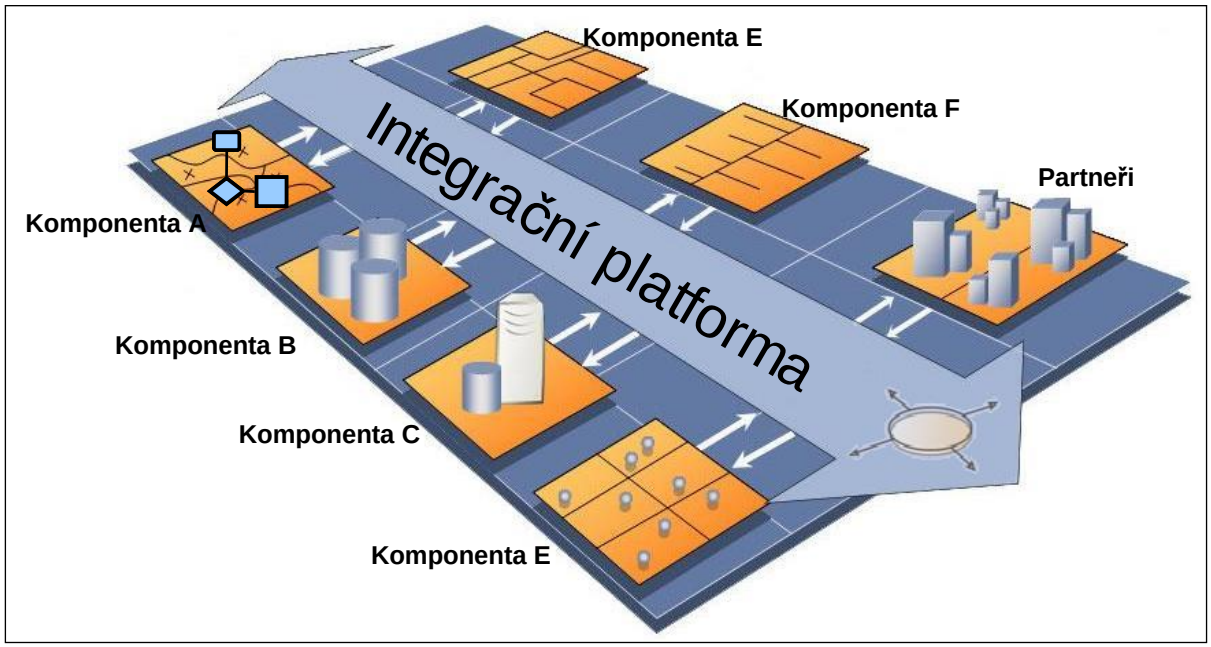
Tato standardizace přinese ve výsledku významné úspory právě v oblastech:

- komunikace – nebude nutné transformovat proprietární datová rozhraní do obecně používaných standardů a naopak
- správa – sjednocení platforem a zavedení standardizovaných postupů při správě IS přinesou značné zjednodušení a zmenší nároky na rozsah znalostí příslušných pracovníků
- flexibilita – díky standardizaci procesu vývoje a jednotlivých komponent systému lze rychle reagovat na aktuální trendy a obchodní potřeby organizace. Maximální možnost využití virtualizace

1.3 Architektura aplikací a jejich integrace

1.3.1 Základní teze architektury

Informační systém VZP ČR je založen na komponentní architektuře a architektuře orientované na služby tzv. SOA. Základním stavebním kamenem jsou služby poskytované z jednotlivých komponent směrem k Integrační platformě (IPF). IPF následně poskytuje tyto služby dalším komponentám, popřípadě vytváří orchestrací služby nové. IPF umožňuje vytvářet technologické i obchodní procesy a je centrálním prvkem mezi jednotlivými komponentami.

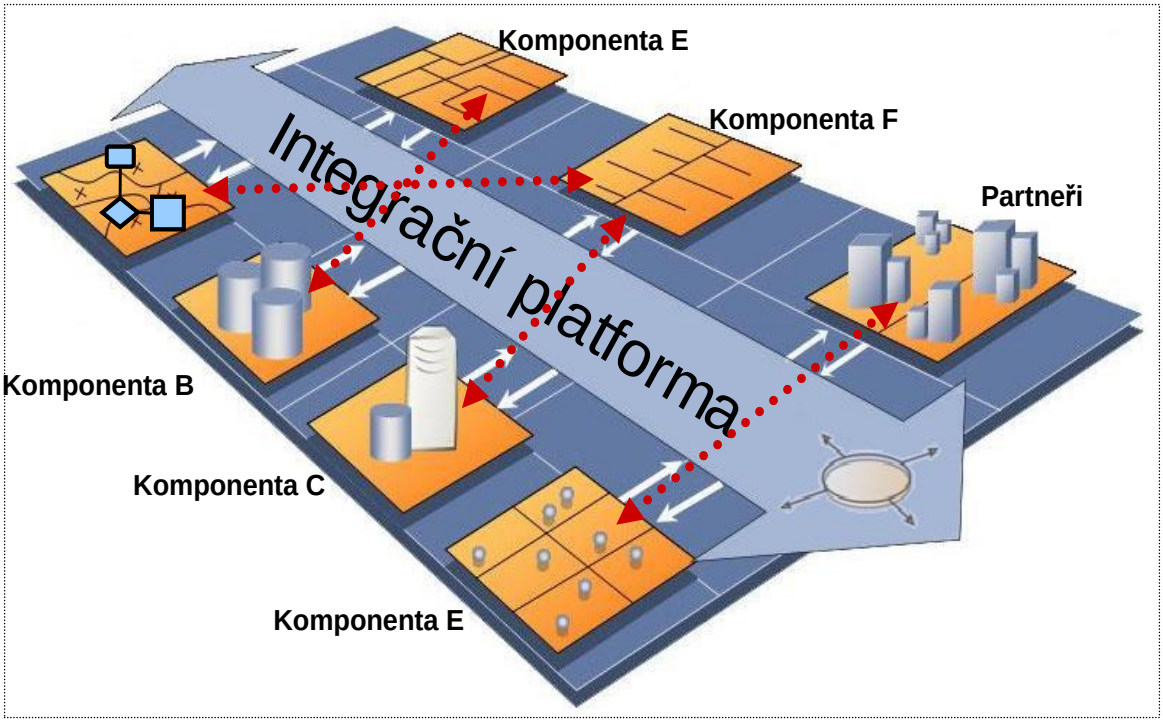


Obrázek 1.3-1: Cílová architektura IS VZP ČR

Mezi komponentami je vytvářena takzvaná volná vazba, kdy konzument služby je nezávislý na implementaci konkrétní služby, na prostředí, ve kterém je služba provozována, na programovacím jazyku, ve kterém je napsána. Pro konzumenta je důležité jen standardní rozhraní k této službě (v současné době nejlépe pomocí webových služeb).

Cílem je také používat omezenou množinu definovaných protokolů a datových formátů. Tyto protokoly a formáty jsou definovány dále.

Na následujícím obrázku je tečkovanou čarou označená chybně provedená integrace mezi komponentami bez použití IPF.



Obrázek 1.3-2: Chybně provedená integrace mezi komponentami bez použití IPF

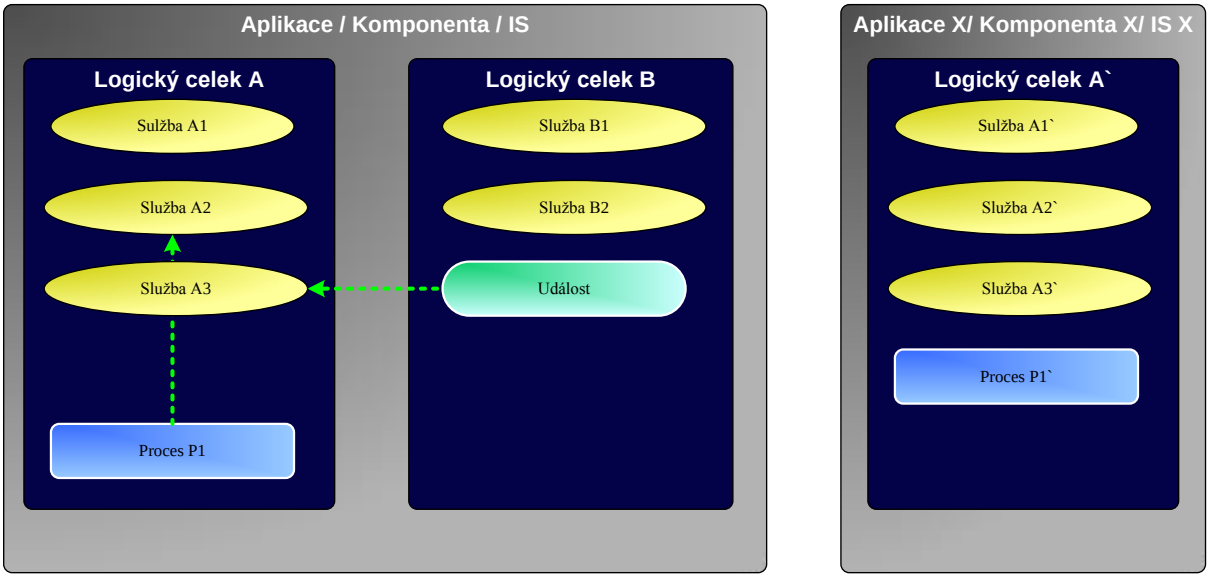
1.3.2 Integrace komponent

Každá ze současných nebo budovaných komponent nabízí své služby okolí. Protože systém IS VZP ČR je rozsáhlý, je žádoucí, aby všechny služby byly popisovány stejným způsobem. Stejně tak pro technologii musí být dodrženy dané standardy a koncepty. Popis uvedeného je v následujících kapitolách.

1.3.2.1 Popis služeb u jednotlivých komponent

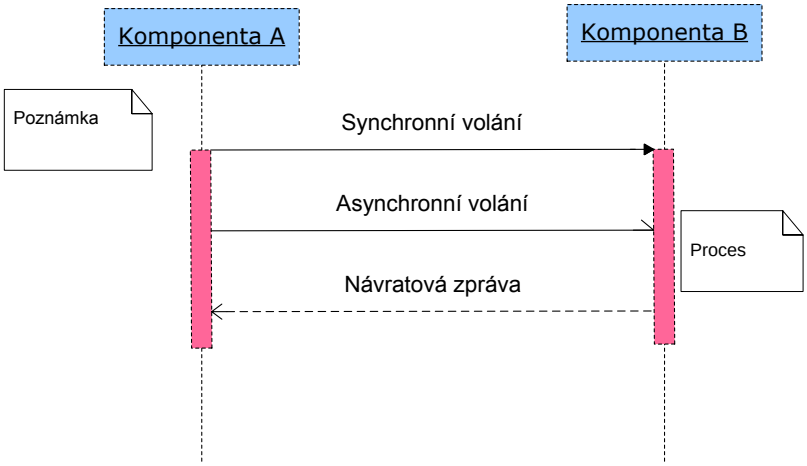
Společně s každou komponentou dodávanou do prostředí ICT VZP ČR musí být dodán i její popis. V úvodu každého popisu komponenty musí být zevrubně popsána funkcionalita komponenty. Následně musí být detailně rozepsány všechny služby, které komponenta nabízí. Snahou je udržet jednotné schéma, které by mělo čtenáři usnadnit orientaci v navrhovaných službách.

Popis služeb lze v rámci komponent nebo mezi komponentou a IPF schematicky znázornit tak, jak je uvedeno na následujícím obrázku. Barevně i tvarem jsou odlišeny tři druhy entit – služba, událost a proces. Událostí se rozumí obchodní nebo technologická událost, která následně může vyvolat proces nebo volání služby. Službou se rozumí základní jednotka SOA architektury – služba poskytovaná svému okolí. Jednotlivé služby a události mohou v rámci komponenty nebo i mezi komponentami tvořit proces. Tyto procesy musí být zřetelně popsány včetně například sekvenčního diagramu.



Obrázek 1.3-3: Schematické znázornění popisu služeb

Pak by měl následovat sekvenční diagram, který přehledně zobrazí probíhající interakce mezi zainteresovanými komponentami.



Obrázek 1.3-4:Vzor sekvenčního diagramu

Následuje tabulka se soupisem služeb, poskytovaných jednotlivými komponentami.

Název služby/ procesu	WSDL operace	Krátký popis
Toto je služba A	SlužbaA	Služba A umožňuje získání informaci o faktuře dodavatele včetně všech náležitostí.
Toto je služba B	SlužbaB	Služba B zakládá faktury. S těmito náležitostmi…. Atd.

A konečně v detailu musí být služby identifikovány jednak slovním „lidským“ popisem (např. Obsah číselníku zdravotních pojišťoven) a jednak *identifikátorem* neboli WSDL operací (např. ObsahCiselnikuZdravotnichPojistoven), jímž bude služba jednoznačně identifikována (identifikátor je konkrétní název technologický název služby uvedený ve WSDL popisu). V tabulce je též stručně popsán účel a obsah poskytované služby.

V odstavcích věnovaných jednotlivým službám musí být podrobněji rozepsáno:

- Cíl, účel, obsah a rozsah poskytované služby
- Pro které konzumenty je služba určena
- Jaký komunikační vzor služba používá (synchronní, asynchronní,…)
- Abstraktní datový typ požadavku (Integer, String, Compex, Enum)
- Abstraktní datový typ odpovědi, resp. slovní popis činnosti, která se odehraje jako reakce služby na příjem požadavku (např. použití služby IPF)

Abstraktní datové typy požadavků a odpovědí specifikují na nejvyšší úrovni abstrakce strukturu a obsah požadavků a odpovědí. Rozlišuje se pouze celočíselná hodnota (Integer), reálná hodnota (Float), řetězec znaků (String) nebo komplexní datový typ (Complex). Komplexním datovým typem se rozumí buď struktura (skupina přesně daného počtu položek různých datových typů) nebo pole (přesně nespecifikovaný počet položek téhož datového typu). Struktura elementů (nadřazený – podřazený element) je naznačena vizuálně:

ElementÚrovně1		Complex	1
ElementÚrovně2		Complex	1
ElementÚrovně3		String	1
JinýElementÚrovně3	Integer		1
JinýElementÚrovně2	Complex		1
…			
JinýElementÚrovně1	…		

U každého elementu abstraktních datových typů je uveden počet jeho výskytů. Většina elementů má výskyt právě jeden. Nepovinné elementy mají uveden výskyt 0-1. U polí je uveden počet výskytů elementů buď 1-n nebo 0-n.

U elementů, které mohou být sémanticky nejasné musí být uveden i jejich sémantický smysl.

Popis interakce mezi více komponentami, tedy komponentní služby, provádí dodavatel příslušné komponenty. Každá komponenta však popisuje interakce s integrační platformou bez ohledu na to, jak je služba na IPF realizována. V sekvenčních diagramech tedy bude na jedné straně dodávaná komponenta, na straně druhé IPF. Popisem uvedeným výše budou popisovány služby požadované od IPF jako součinnost i služby nabízené komponentou. V druhém kole, za účasti Kompetenčního centra integrace ICT budou požadované služby upřesněny. Tam kde je to možné bude použita popřípadě rozšířena stávající služba IPF.

V prvním kroku je však na dodavateli komponenty definovat jaké služby s jakými atributy a jakou souslednosti jsou požadovány. Ve druhém kroku musí být služby požadované od IPF, které budou zajišťovány jako součinnost, předloženy Kompetenčnímu centru integrace ke schválení.

Součástí implementace služeb IPF musí být analýza dopadu s ohledem na HW infrastrukturu integrační platformy s případným doporučením na její rozšíření.

1.3.2.2 Preferované architektonické a komunikační vzory

1.3.2.2.1 Asynchronní komunikace

Asynchronní komunikace je založena na principu pošli žádost, pokračuj v práci, odpověď dostaneš. Obvykle jedna strana sestaví žádost, pošle ji druhé straně pomocí dalšího prostředku (JMS, SOAP) a neočekává okamžitou odpověď, popřípadě jen očekává potvrzení příchodu zprávy. Druhá strana převezme příchozí zprávu, zpracuje ji dle svého načasování a eventuálně pošle odpověď. Mezi tím samozřejmě strana, která iniciovala požadavek pokračuje v další činnosti.

Tento typ komunikace přináší nutnost zaručit přenos zprávy – to lze implementovat různými způsoby. Těmi jsou například potvrzování příjmu zpráv na úrovni SOAPu nebo posílání zpráv pomocí jiných prostředků jakými jsou například JMS nebo AQ.

Asynchronní charakter zpráv s sebou nese nutnost takzvané korelace jednotlivých požadavků a vyřízených žádostí. Princip korelace a vzor zprávy jsou uvedeny dále v textu.

1.3.2.2.2 Komunikace řízená událostmi – Event driven

Událostí se rozumí obchodní událost (business event). Obchodní událost lze definovat jako smysluplnou změnu stavu relevantní pro obchodní logiku softwaru. Příkladem může být změna smlouvy se zdravotním zařízením. Základem tedy je umět zachytit důležitou změnu a publikovat ji. V našem případě publikovat ji do Integrační platformy pomocí definované webové služby. Integrační platforma je takto krátkou zprávou informována o důležité změně a pak může spustit potřebný koordinační proces. Je tedy na IPF, jak se změnou naloží. Tento proces je tedy již plně v režii Integrační platformy.

V komponentě jsou tedy implementovány 2 mechanizmy:

- Upozornění na změnu
- Umožnění „přečtení“ změny

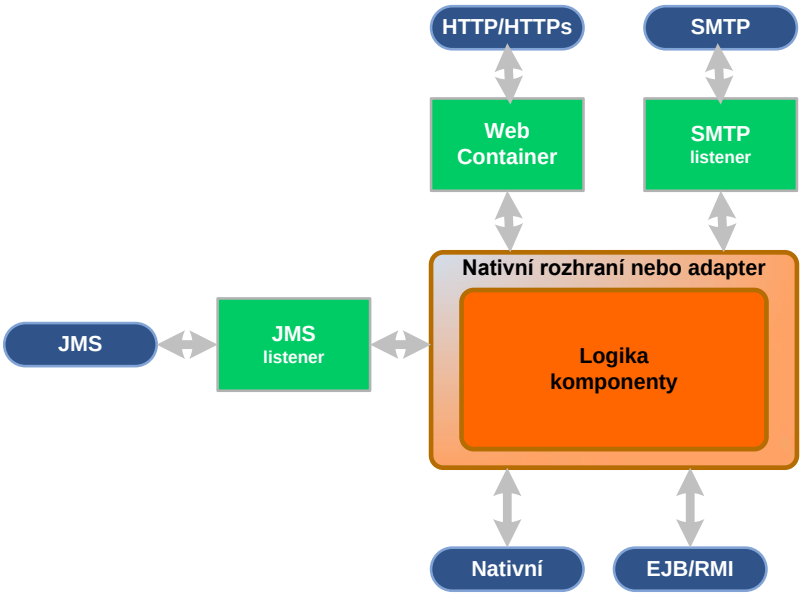
1.3.2.2.3 Fronty požadavků

Pro asynchronní komunikaci je možné a vhodné v prostředí VZP ČR použít komunikaci pomocí JMS/AQ, která vytváří i časově volnou vazbu mezi systémy. Fronty požadavků kromě vytvoření volné vazby mezi různě dostupnými systémy umožňují také překlenutí požadavků na zpracování většího než možného nebo přijatelného množství v daném systému. Je vysoce pravděpodobné, že vzniknou okamžiky, kdy bude zasíláno větší množství požadavků, než bude moci cílový systém nebo komponenta vyřídit – pomocí fronty požadavků může cílový systém řídit svůj takt zpracování.

1.3.2.3 Protokoly a datové formáty pro integraci

V následující tabulce jsou (sestupně dle preference použití) uvedeny varianty, které je při integraci systémů a aplikací možné využívat.

Transportní protokol	Druh komunikace	Formát dat	Popis
HTTP	Synchronní Asynchronní	SOAP XML	Pro vzdálený přístup, nezabezpečený, nezávislý na platformě, pro přístup k službám v rámci organizace, mimo organizaci pouze po důkladné analýze
HTTPS	Synchronní Asynchronní	SOAP XML Form (Get/Post)	Pro vzdálený přístup, zabezpečený, nezávislý na platformě, pro přístup k službám v rámci organizace nebo i mimo organizaci
JMS/AQ	Asynchronní	SOAP XML Java Objekty	Pro komunikaci s IPF, Peer to peer nebo publish/subscribe
SMTP	Asynchronní	SOAP XML Context Based	Pro vzdálený přístup s externími partnery
Daný konkrétním Standardním adapterem			Některé standardní produkty jsou dodávány s vlastními konektory pro různé integrační prvky (například BPEL Process Manager). Kvalitní produkty však již většinou obsahují standardní WS rozhraní.
CORBA, COM+, DCOM, COM, EJB/RMI, **NET Remoting**			Pro aplikační komunikaci



Obrázek 1.3-5: Obecné schéma komponenty

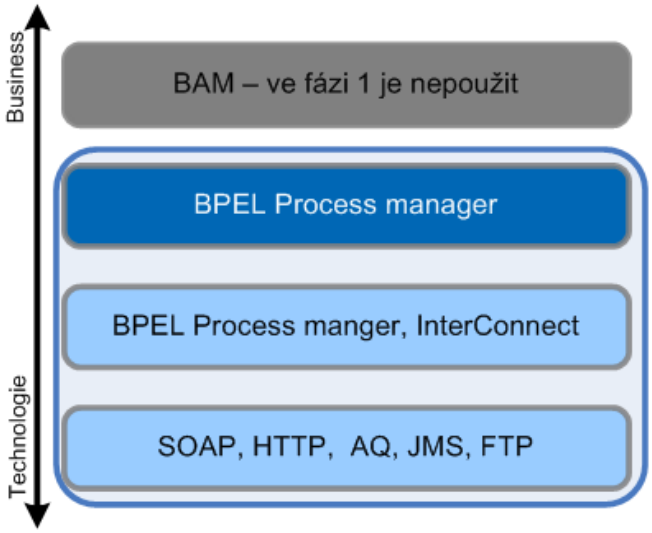
Komponenty systému nabízejí svoje služby svému okolí pomocí metod, které jsou zpřístupněny jedním z rozhraní nadefinovaným v předešlé tabulce. Samozřejmě komponenta nemusí implementovat pouze jedno z těchto rozhraní, ale může jich nabízet několik.

1.3.2.4 Technologické prostředí IPF

Integrační platforma (IPF) slouží k vytváření integračních vazeb mezi komponentami IS VZP ČR, jak bylo uvedeno výše. Architektura Integrační platformy vychází z nejnovějších poznatků v oblasti návrhu rozsáhlých podnikových řešení a zohledňuje snahu o zachování investic do informačních technologií, je to architektura orientovaná na poskytování služeb (SOA).

Softwarová infrastruktura je tvořena produkty firmy HP na úrovni operačních systémů (HP-UX) a produkty firmy Oracle na databázové a aplikační úrovni, konkrétně pro databázi Oracle DB Enterprise Edition , Aplikační server Weblogic, BPEL Process manager (dnes SOA Suite), který je součástí aplikačního serveru enterprise edition.

Namapování těchto produktů a technologií na jednotlivé vrstvy integrace je zobrazeno na následujícím obrázku.



Obrázek 1.3-6: Produkty a technologie

Hardwarovou infrastrukturu na databázové úrovni tvoří Oracle RAC cluster složený ze čtyř HP-UX serverů..Na aplikační úrovni jsou využívány farmy aplikačních serverů s Oracle iAS 11g R2, na kterých je instalován Oracle BPEL Process Manager. RAC clustery a farmy aplikačních serverů tvoří geografický cluster. BPEL Process manager je tak zvaně bezestavový, to znamená, že stavy jsou okamžitě ukládány do databáze (dehydratace). Tak je zajištěno, že při pádu jednoho z BPEL serverů zpracovávané procesy převezme server jiný, bez nutnosti vytváření Java clusteru na aplikační úrovni.

Poslední vrstvu, vrstvu load balancerů, tvoří dva Cisco ACE. Přes tyto komponenty přicházejí všechny požadavky na Integrační platformu. Požadavky jsou posléze předávány dostupnému, popřípadě méně zatíženému aplikačnímu serveru. Přesto, že jsou tyto prvky velmi spolehlivé, jsou pro zvýšení dostupnosti zdvojené.

1.4 Technologické standardy

1.4.1 Operační systémy obecně

1.4.1.1 Standardy

Operační systém	Verze	Použití	Poznámky
UNIX	HP-UX 11.31	Stěžejní aplikace, Aplikační i databázová vrstva A++, A+, A a B aplikace	1 x za rok Patchová analýza – termíny po dohodě dle potřeb VZP
MS Windows	2003, 2008, 2012, 7 enterprise)	Podpůrné aplikace, popřípadě aplikace třídy B. Aplikace, kde není možné použít UNIX, zejména balíkový SW. E-mailový systém v třídě A+	Aktuální hotfixy ověřené testováním
Linux	distribuce RHEL/CentOS 6 a vyšší	Podpůrné aplikace, popřípadě aplikace třídy B, A a A+	1 x za rok Patchová analýza – termíny po dohodě dle potřeb VZP

1.4.2 Serverová Infrastruktura

Oblast	Požadavky
Systémy	Enterprise systémy jsou centralizované a provozované v rámci datových center (DC)
Aplikace	Každé aplikaci musí být přidělena kategorie A++, A+, A nebo B Hlavní charakteristiky: A++ překlenutí výpadku serveru v rámci lokality a výpadku lokality A+ překlenutí výpadku jednoho serveru v rámci lokality A překlenutí výpadku lokality (aktiv/pasiv) B podpůrné, méně důležité aplikace
Společné použití SAN infrastruktury	V jednotlivých datových centrech jsou primární disková pole, která jsou zapojena do SAN infrastruktury. Potřebná kapacita je řešena rozšířením těchto poli nikoliv nákupem dalších polí.

1.4.2.1 Centrální vysoce dostupné serverové systémy

Jedná se o systémy pro které je vytvořena nebo vytvářena architektura s vysokou dostupností. Hostí převážně aplikace kategorií A++, A+ nebo A. Na každém z centrálních serverů může být provozována jedna nebo více aplikací. Aplikace sloužící jako komunikační kanály směrem ke klientům (portál, B2B) jsou provozovány mezi dvěma centry v režimu aktiv/aktiv. Aplikace pro vnitřní použití počínaje kategorií A jsou zálohovány na druhou lokalitu.

1.4.2.1.1 Standardy

Operační systém	Verze	Použití	Poznámky
HP-UX HP ServiceGuard HP ServiceGuard Cluster File Systém for RAC *	11.31 A.11.20.00 A.04.01.00. 11gR2	Active/Active– obě DC v aktivním módu Zálohováno mezi lokalitami Cluster,databáze, kategorie A,A+,A++ Testovací prostředí cluster Activ-Activ, kategorie A++,A+ Automatická správa úložiště pro databázové soubory Oracle.	Databáze, aplikační servery.
Windows	2003, 2008, 2012, 7 enterprise	Rozdělení mezi lokality Produkce/Záloha/Test	Pro podpůrné aplikace. Za určitých okolností, například pro aplikace vyžadující toto prostředí je možné tuto platformu využít i jinde. Tato platforma však není preferovaná pro enterprise aplikace.
distribuce RHEL/CentOS	6 a vyšší	Rozdělení mezi lokality Produkce/Záloha/Test	

* Pro nové aplikace s dodávkou nové infrastruktury se použije Oracle Automatic Storage Manager

1.4.3 Pracovní stanice

1.4.3.1 Standardy

Název	Verze	Použití	Poznámky
OS Windows	Windows 7 enterprise	Lokální pracovní stanice	

Název	Verze	Použití	Poznámky
Tiskárny	PCL, Postskript	Připojené přes tiskový server Výjimečně lokální	
MS Word	MS Office 2010	Na všech pracovních stanicích	
MS Excel	MS Office 2010	Na vybraných pracovních stanicích	
7Zip		Na všech pracovních stanicích	
Endpoint Protection Antivirová ochrana Kaspersky Endpoint Security	Centrálně řízený Endpoint Protection v aktuálních verzích zajišťující: AntiMalware, IDS/IPS, Firewall, Application control, Device control, Antispam	Na všech pracovních stanicích	
Endpoint Encryption Area Guard Neo	Centrálně řízený systém šifrování disků a souborů	Na vybraných pracovních stanicích	Notebooky
Vzdálený přístup	Remote Desktop, Support Assistant,	Na všech pracovních stanicích	
Data	E-Mail, Soubory	Na serverech, výjimečně na mobilních zařízeních – v tomto případě chráněná před zneužitím	Umístění dat na pracovní stanici je bez záruky.

Zobrazovač Adobe	Flash Player – aktuální verze. Reader 11.0.5	Na všech pracovních stanicích	
Prostředí pro provoz 3V aplikací	SUN JRE v.1.6.0_45 a 1.7.51 vyšší, IE v 11)	Na všech pracovních stanicích	
Distribuce Aplikačního SW	SCCM	Na všech pracovních stanicích	
Distribuce Patchů Operačního Systému	SCCM	Na všech pracovních stanicích	
Zálohování	%USERPROFILE%, C:\DATA	Mimo systémových souborů. Pracovní stanice se jako celek nezálohují	
Oprávnění		Uživatel není Administrátor	
Nastavení		Nastavení počítače i uživatele je řízeno a vynucováno centrálně doménovými politikami	
Jednotná adresářová struktura	APPL, Archiv Data Nezalohovano Program Files Temp TMP Users Windows	Root,Program Files, Windows – přístup pro čtení	
VPN klient	Cisco AnyConnect Secure Mobility Client	Na vybraných pracovních stanicích (notebook)	
.NET Framework	v. 4.0 a vyšší	Na všech pracovních stanicích	

1.5 Aplikační standardy

1.5.1 Používané aplikační servery

Druh AS	Použití
Oracle Fussion Middleware Forms&Reports 11gR2	Stávající aplikace programované v Oracle Forms a Reports
Oracle Fusion Middleware WebLogic Server 11gR2	Nově dodávané aplikace v Oracle Forms a Reports 11gR2
JBoss aplikační server 4.0.5	Aplikace vytvořené mimo prostředí Oracle Forms

1.5.2 Standardizovaný vzhled vyvíjených aplikací

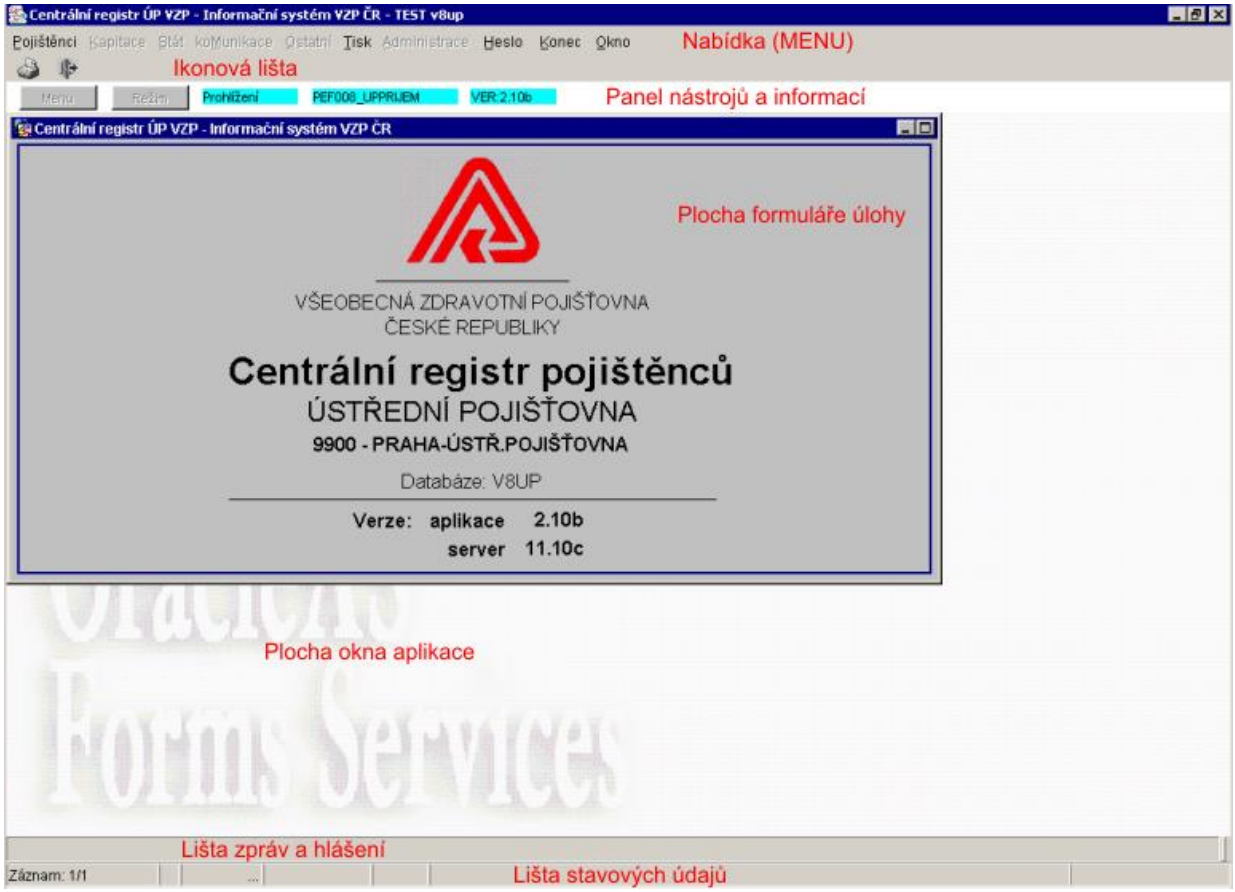
Standardním a preferovaným prostředím aplikací vyvíjených na zakázku je Oracle Forms. Dodávané aplikace mají jednotný vzhled, který je definovaný v příloze „Standardní design aplikace pro VZP a dodavatele“.

Tento dokument obsahuje design obrazovek, popis použitých stylů, barev, fontů a seznam ovládacích funkcí - „horkých kláves“.

1.5.2.1 Standardní design aplikace

Hlavní aplikační formulář se skládá z několika sekcí:

- **Záhlaví okna** – nachází se v horní části okna aplikace. Obsahuje následující údaje:
- **Menu aplikace** – nachází se těsně pod záhlavím okna. Je typu pull-down a je od zavedení systému IdM řízeno rolemi uloženými v autorizační databázi (ADB) – viz příloha Standardů „Integrace aplikace do IDM (identity management)“. Obsahuje nabídku spustitelných úloh (formulářů). Pokud uživatel má oprávnění ke spuštění úlohy, je možné nabídku vybrat pomocí levého tlačítka myši nebo kombinací klávesy ALT+písmeno.
- **Ikonová lišta** – obsahuje ikony pro rychlé volání funkcí pomocí myši.
- **Panel nástrojů a informací** – prostor pro zobrazení identifikačních informací a umístění aplikačních nástrojů.
- **Pracovní oblast** – prostor pro formulářová okna.
- **Lišta zpráv a hlášení** – obsahuje zprávy běžících úloh aplikace.
- **Lišta stavových údajů** – obsahuje další údaje, například počet vybraných záznamů, pořadí aktivního záznamů, atd.

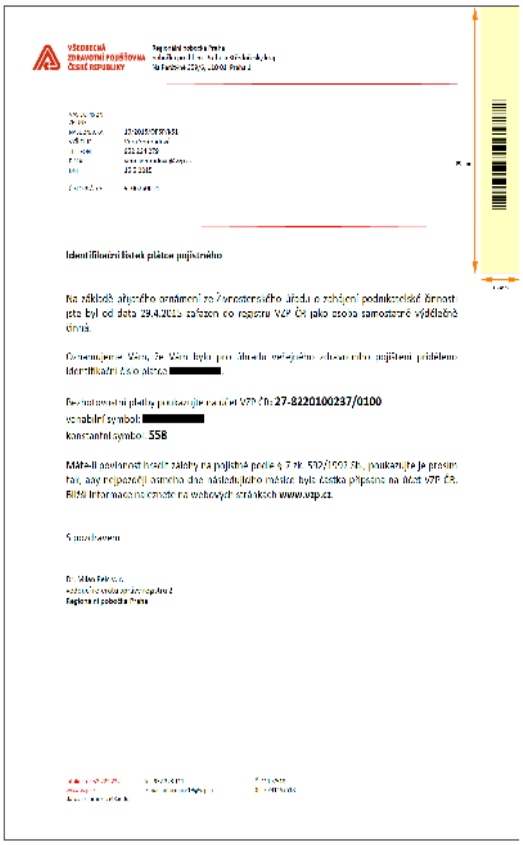


1.5.2.2 Výstupy generované aplikacemi

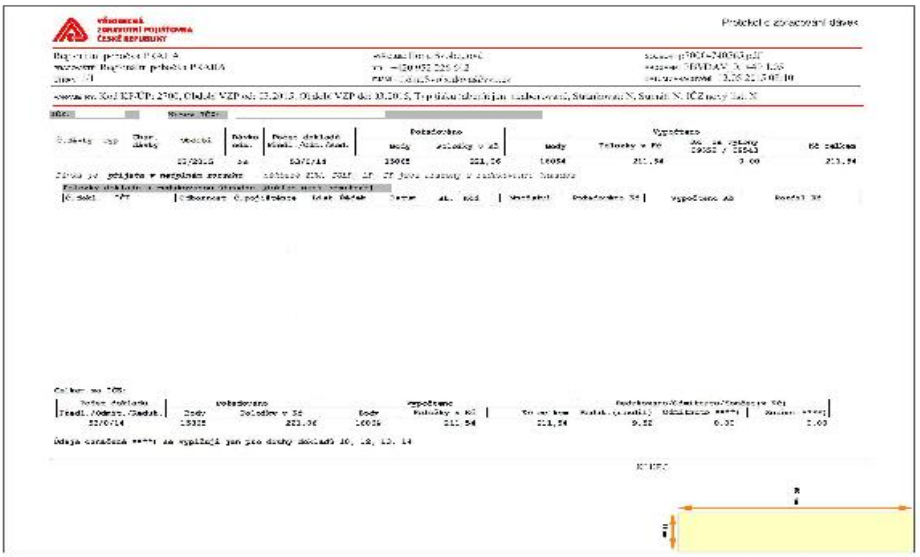
Výstupy generované aplikacemi musí být v souladu s Manuálem jednotného vizuálního stylu VZP ČR, zejména musí být použito správné logo, které je uvedeno v záhlaví tohoto dokumentu a které bude předáno ve formě gif, jpg na vyžádání.

Tisková sestava, která je určená na slučování s jinými sestavami a distribuci Hybridní poštou musí splňovat tyto požadavky:

1. povinný formát sestavy A4 (210 x 297) nebo (297x210) v rámci PDF souboru
2. povinné místo pro doplnění čárového kódu – párovácího znaku pro obálkovačku - vpravo nahoře, nebo vpravo dole obdélníkem o velikosti 15 x 90 mm. Názorné ukázky realizace jsou zde:



Identifikační list



1.5.3 Adresářové struktury pro ukládání aplikačních modulů a datových souborů

Aplikační moduly (upgrade, spustitelné programy) pro unixové servery se ukládají na databázovém serveru do následující adresářové struktury:

/appl/vzpcvon/cre pro upgrade

kde vzpcvon je unixový uživatel aplikace (vlastník)

cre je adresář, kde jsou v podadresářích uloženy upgrade programů a databázových objektů

/appl/vzpcvon/prg pro spustitelné programy v prostředí operačního systému

Dále jsou aplikační moduly uloženy na aplikačním serveru do následující adresářové struktury:

/appl3w/vzpcvon/prg pro spustitelné formuláře a reporty

Datové soubory a tiskové výstupy na unixových serverech se ukládají na databázovém serveru do následující adresářové struktury:

/vzpdata/data/vzpcvon/logs pro logovací soubory

kde vzpcvon je unixový uživatel aplikace (vlastník)

/vzpdata/data/vzpcvon/lst pro speciální soubory (drg, regulace) a tiskové výstupy

/vzpdata/data/vzpcvon/work<n> pro pracovní soubory

kde n je pořadové číslo

Pro nově vyvíjené aplikace se aplikační logika nachází na aplikačním serveru ve formě aplikačních modulů nezávislých na platformě hostujícího operačního systému.

Pro případné operace s daty na databázové vrstvě (v databázi) není aplikační kód umístěn mimo databázi. Aby byla zaručena jeho platformová nezávislost, je uložen ve formě programových modulů přímo v databázových procedurách a funkcích..

1.5.4 Jednotná správa identit

Správa identit je řešena prostřednictví Oracle identity manageru. Využívají se uživatelské účty v Active Directory, definované business role v Oracle identity manager a aplikační a typové role vedené v autorizační databázi. Konfigurace Oracle Virtual Directory v produkčním prostředí zajišťuje přístup k:

- ADB databázi
- Microsoft Active Directory
- Servisním účtům

Prostřednictvím rozcestníku aplikací (RAP) je řešeno jednotné přihlašování (SSO) k obchodním aplikacím.

Kroky a zodpovědnosti při řešení integrace aplikací do IDM jsou uvedeny v následující tabulce:

Fáze	Procesní krok	VZP - IDM	VZP - garant aplikace	Dodavatel aplikace	HP/GEM	Komentář
	Předání materiálů pro integraci s IDM					Dokumentace, knihovny, přístupová oprávnění
VÝVOJ	Implementace API (rozhraní) pro OIM komunikaci[1)]			X		
	Vhodnost LOGIN dialogu aplikace pro SSO			X		
	Integrace s ADB (ADB knihovna) [2)]			X		Případná změna modelu řízení oprávnění
	Podpora dodavatele při integraci s IDM				X	
	Seznam TR, AR (včetně mapování) pro nastavení ADB[2)]			X		
	Seznam TR pro nastavení OIM[1)]			X		
	Specifikace BR a schvalovacích procesů		X		X	
	Rozšíření konfigurace OIM (BR, konektor k aplikaci)				X	
TEST	Konfigurace ADB dle podkladů TR/AR[2)]	X				
	Konfigurace OIM včetně BR [1)]	X				
	Podklady pro RAP, eSSO			X	X	URL, test uživatel/heslo
	Konfigurace RAP, eSSO	X				
	Specifikace BR a schvalovacích procesů		X		X	
	Specifikace mapování „uživatelů VZP a BR“		X			
	Integrační testy (RAP, eSSO, OIM, ADB)	X		X	X	
PRODUKCE	Konfigurace ADB dle podkladů TR/AR[2)]	X				
	Konfigurace OIM včetně BR [1)]	X				
	Přiřazení BR v OIM dle mapování „uživatelů a BR“	X				
	Integrační testy (RAP, eSSO, OIM, ADB)					

	Podklady pro RAP, eSSO		X	X		
	Konfigurace RAP, eSSO	X	X			Zpřístupnění aplikace pro koncové uživatele

Poznámky:

1) *Jedná se o variantu integrace „vlastní“ úložiště / přímá integrace s OIM*

2) *Jedná se o variantu integrace „externí“ úložiště / integrace skrze ADB*

Po podpisu smlouvy s VZP ČR dostane dodavatel dokument „Integrace aplikace do IDM“, který je nedílnou součástí těchto standardů.

1.5.5 Centrální správa číselníků

Aplikace Centrální správa číselníků (CSČ) je základním nástrojem pro jednotnou správu číselníků z jednoho místa v rámci Centrálního informačního systému VZP ČR (CIS)

Zařazení číselníku do správy aplikace CSČ je podmíněno přidělením rolí:

- garant číselníku (GARANT),
- operátor obsahu číselníku (OPERATOR_OBSAHU),
- operátor struktury (OPERATOR_STRUKTURY),
- konkrétním uživatelům oprávněným pracovat s číselníkem v rozsahu platných uživatelských práv

Jedním ze základních úkolů aplikace CSČ je zajištění konzistence číselníků v rámci prostředí a mezi komponentami při zachování principu „pravda na jednom místě“

Po podpisu smlouvy s VZP ČR dostane dodavatel dokument „Integrace aplikace s CSČ“, který je nedílnou součástí těchto standardů.

1.5.6 Dokument management systém

Aplikace Dokument management systém (DMS) je nástrojem pro správu dokumentů ve VZP ČR, Jeho součástí je workflow schvalování dokumentů.

Po podpisu smlouvy s VZP ČR dostane dodavatel dokument „Integrace aplikace s DMS“, který je nedílnou součástí těchto standardů.

1.5.7 Tiskový subsystém

Aplikace Tiskový subsystém (TS) je nástrojem pro jednotné spouštění, vytváření, prohlížení a tisk tiskových výstupů v IS VZP ČR. TS má následující vlastnosti:

Jednotnost

evidence a registrace tiskových modulů, jejich atributů (.rdf) a parametrů

konfigurace (při registraci, při spuštění, u vygenerovaného výstupu)

volání Oracle Reports (http/GET na rwservlet)

řízení vyřizování požadavků (hodnoty parametrů, priorita, ihned/v budoucnu,…)

správa výstupů (stav generování, prohlížení, archivace, výmaz, obnovení)

Poskytované rozhraní - API

pro volání z Oracle DB

PBREP (PL/SQL)

Views (SQL; tvorba GUI)

pro volání z Oracle Forms

PBREPORT.pll (nadstavba - volá PBREP)

GUI (formuláře Oracle Forms) pro volání z Forms aplikace

pro integraci s IPF – AQ (Portál, abonované sestavy)

služba VytvorSestavu (spuštění sestavy s parametry, vrácení výstupu)

služba ObjednavkaPredplatneho (registrace abonenta na abo sestavu, výstupy do IPF)

Po podpisu smlouvy s VZP ČR dostane dodavatel dokument „Integrace aplikace s TS“, který je nedílnou součástí těchto standardů.

1.5.8 Business Inteligence

Aplikace Business Inteligence (BAM/BI) je nástrojem pro reportování, analyzování a poskytování přehledů nad daty informačního systému VZP ČR ve vytvořeném datovém skladu. Dodavatel dodávané komponenty IS VZP ČR poskytne součinnost autorům BI řešení pro získání potřebných údajů z dodávané komponenty.

1.5.9 Realizace integračních vazeb

Realizace integračních vazeb mezi komponentami informačního systému je prováděna prostřednictvím integrační platformy (IPF). Princip integračních vazeb je popsán v kapitole Architektura aplikací a jejich integrace. Podrobnější informace o realizaci integračních vazeb získá dodavatel z dokumentu „Popis integračních vazeb prostřednictvím IPF a metodika realizace integračních vazeb“ V uvedeném dokumentu je rovněž uvedena metodika realizace integračních vazeb.

Při podpisu smlouvy s VZP ČR dostane dodavatel dokument „Popis integračních vazeb prostřednictvím IPF a metodika realizace integračních vazeb“, který je nedílnou součástí těchto standardů.

1.5.10 Autentizační a autorizační služby

Oblast standardizace	Popis
Mechanismy asymetrické kryptografie	Autentizační mechanismy realizované na bázi asymetrické kryptografie jsou realizovány prostřednictvím algoritmů RSA, DSA popřípadě ECC elektronickým podpisem za současného využití prvků PKI, kde přiřazení veřejného klíče danému uživateli nebo procesu je stvrzeno ve formě certifikátu X.509v3 certifikační autoritou náležící k LAN. Při autentizaci se na aplikační/serverové straně využívá kontroly platnosti předkládaného certifikátu prostřednictvím kontroly CRL nebo pomocí OCSP. Autorizace navazující na zdařilou autentizaci je svázána s příslušnými atributy certifikátu, typem páru klíčů, popřípadě vynucením dalšího elektronického podpisu.
Kerberos5	Autentizační/Autorizační mechanismy na bázi systému Ker-

	beros5 vycházejí ze standardu RFC 1510. Pro realizaci klíčů příslušných principů se prioritně využívají tzv. silné symetrické šifry typu 3DES, RC2, RC4 apod. KDC pro MS doménu je z bezpečnostních důvodů oddělena od KDC pro autentizaci a autorizaci přístupu k UNIX systémům. Je přípustné realizovat v rámci VZP jednosměrné vztahy důvěry typu MS KDC důvěřuje KDC pro UNIX systémy nebo jinému MS KDC. Autentizace na bázi Kerberos5 je používána v režimu vynucené preautentizace, kde je dále možné využít tzv. mechanismu PKINIT. Autentizace a autorizace na bázi Kerberos5 je používána při autentizaci přístupu k OS nebo koncové aplikaci popřípadě databázi.
Radius/TACACS	V rámci VZP je RADIUS realizován prostřednictvím modulu FreeRadius a TACACS prostřednictvím modulu XTACACS. Autentizační a autorizační principy Radius/Tacacs protokolu jsou využívány v prostředí RAS a řízení přístupu k aktivním prvkům typu směrovač, switch apod. K řízení přístupu k aktivním síťovým prvkům se používá Cisco ACS (Access Control Server) - modul Cisco TACACS+ a RADIUS

1.5.10.1 Standardy jednotného přihlašování SSO na klientských stanicích

- Oracle Forms doplní název unikátní aplikace (název okno) v okamžiku zobrazení přihlašovacího formuláře.
  - Pro potřeby rozeznání aplikace na klientské stanici je nutné modifikovat Oracle Forms aplikace a pomocí triggeru „pre_logon“ nastavit název okna na unikátní hodnotu v rámci Oracle Forms aplikací provozovaných ve VZP.
- Java Helper Object (JHO) – knihovny
  - Java Helper Object představuje sadu souborů, které je nutné umístit do adresáře Java Runtime Environment (JRE). Obsah JRE adresáře je nutné rozšířit o následující soubory.
    Proměnná $JAVA_HOME například obsahuje hodnotu “C:\Program Files\Java\j2re1.6.0_45“.
    - $JAVA_HOME\lib\accessibility.properties soubor obsahující řádek s textem *assistive_technologies=com.passlogix.vgo.ho.jho*
    - $JAVA_HOME\lib\ext\jho.jar
    - $JAVA_HOME\lib\ext\jaccess.jar
    - $JAVA_HOME\bin\ssojho.dll
  - V případě, že není JRE adresáře správně upravený, nebude funkční automatické přihlášení do Java aplikací, tedy i do Oracle Forms aplikací.
- eSSO LM agent – pracovní stanice je rozšířena o SW modul realizující automatické přihlášení do spouštěných aplikací
- Autentizace do klientských aplikací – nesmí být automatická na základě přihlášení do Windows domény (např. prostřednictvím Kerberos ticket nebo NTLM)
- Podnikové aplikace budou spouštěny z prostředí rozcestníku, který dovoluje řídit oprávnění a zatížení serverů

1.5.11 Elektronická pošta

Oblast standardizace	Popis
SMTP brány	Příjem elektronické pošty z Internetu je realizován přes dedikované SMTP brány v perimetru. Před předáním emailu do interního poštovního systému je provedena jeho antivirová a antispamová kontrola.
Vnitřní elektronická pošta a messaging	Vnitřní elektronická pošta a messaging systém je realizován prostřednictvím MS Exchange 2010. Poštovní komunikace směrovaná mimo lokální poštovní doménu probíhá prostřednictvím protokolu SMTP a je směrována na SMTP brány. Z hlediska klientského vybavení je za standard považován MS Outlook 2010.

1.5.12 Virtualizace

Oblast standardizace	Popis
Platforma	Hostitelský systém je operační systém nebo HW, který umožní provoz Virtuálních serverů. Jako podporované platformy mohou být ve VZP nasazeny technologie HP VM, HP nPar či vPar, VMWare vSphere 5 + MS Hyper-V nebo Linux XEN..
Řízení Virtuálních serverů	Řízení HP virtuálních serverů vychází z koncepce jednotné konzole HP SIM, které pomocí modulu HP VMM umí pracovat s HP-UX hostitelským systémem Řízení pro Hyper-V je realizováno SCVMM konzolou a pro VMWare VMWare konzolou vCenter serveru.
Konfigurace vysoké dostupnosti	Pro zajištění vysoké dostupnosti a realizaci DRP plánu vybraných virtuálních serverů bude sloužit centrální konzole HP SIM. Pro realizaci vysoké dostupnosti v rámci x86 světa může sloužit VMware DRS a HA cluster.

1.5.13 LoadBalancing

Oblast standardizace	Popis
LoadBalancing	Pokud nebude součástí jiného dokumentu (smlouva, projektová dokumentace, …) přesný popis nastavení load balancingu, OTP nastaví load balancing na požadovaných serverech standardně používanou metodou round robin. Tato jednoduchá metoda poskytuje pouze základní nastavení a není optimalizována ve vztahu k balancované aplikaci, což může vést k vysoké až zásadní neoptimalitě. Stickyness nebude nastavena a kontrola dostupnosti serverů bude pouze minimální a to prostřednictvím pingu (ICMP).

	Minimální požadavky: • Port služby • URL služby • Keepalive URL

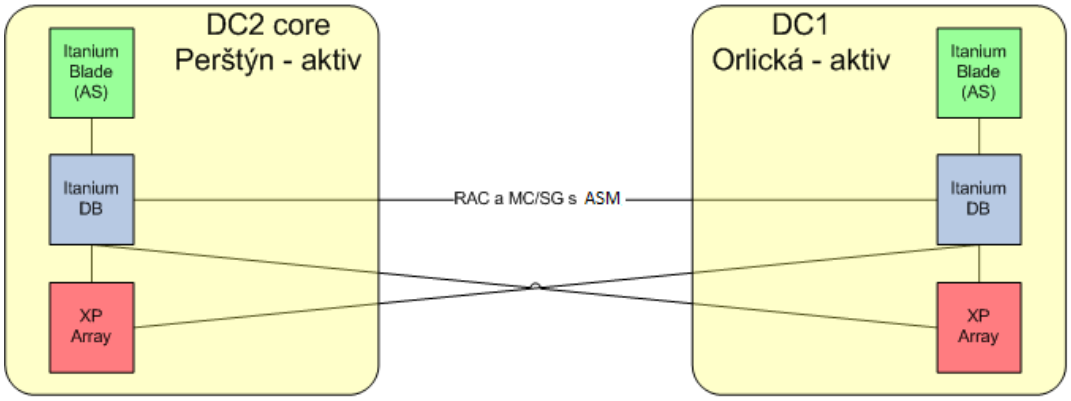
1.5.14 Druhy podporovaných aplikací dle tříd

1.5.14.1 Třída A++

Aplikace v této třídě pracují v režimu aktiv/aktiv na obou lokalitách současně. V případě výpadku jedné lokality aplikace automaticky funguje dál v druhé lokalitě. Výpadek jedné lokality nicméně může mít vliv na výkonnost aplikace.

Typickou konfigurací je geografický Oracle RAC cluster v kombinaci s HP ServiceGuard (dále jen SG) a Oracle ASM. Data jsou zrcadlena do záložní lokality prostřednictvím Veritas VM (Veritas Volume Manager).

Grafický obrázek zachycuje minimální konfiguraci, kdy pro případ A++ B2B je budován jako čtyřbodový geografický RAC cluster.

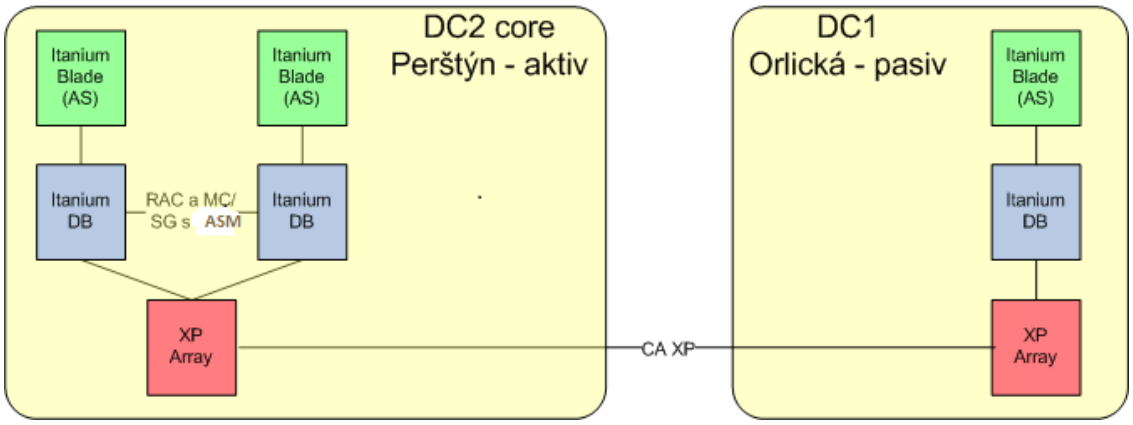


Obrázek 1.5-1 Příklad řešení HA aplikace ve skupině A++

1.5.14.2 Třída A+

Aplikace v této třídě pracují v režimu aktiv/aktiv v jedné lokalitě a mohou být manuálně přepnuty do záložní lokality. V případě výpadku jednoho serveru v primární lokalitě aplikace automaticky funguje dál na druhém serveru. Výpadek jednoho serveru může mít vliv na výkonnost aplikace. V případě výpadku primární lokality bude aplikace po dobu nutnou k manuálnímu přepnutí do záložní lokality dočasně nedostupná. Výpadek primární lokality bude mít vliv na výkonnost aplikace.

Typickou konfigurací je lokální Oracle RAC cluster v kombinaci s HP SG a Oracle ASM. Data jsou zrcadlena do záložní lokality prostřednictvím technologie HP Continuous Access XP (dále jen XP CA).



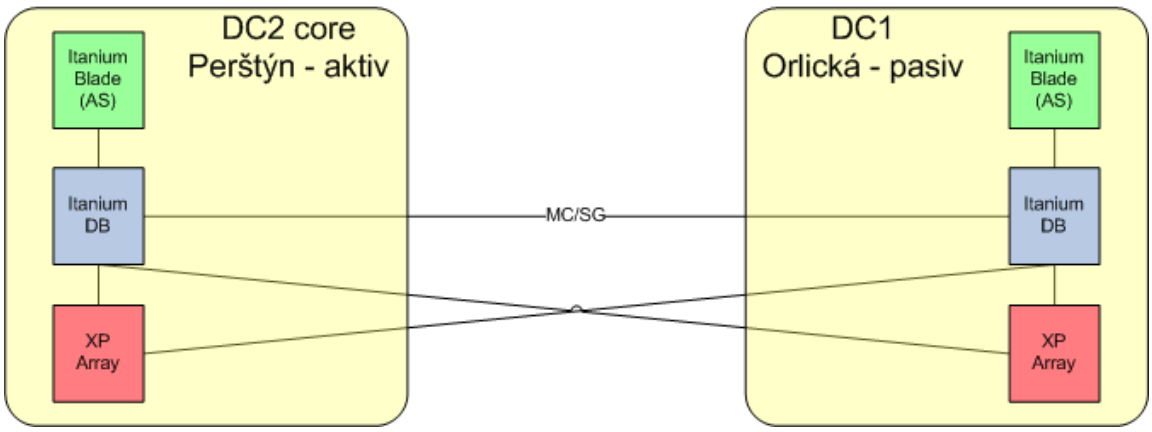
Obrázek 1.5-2 - Příklad řešení HA aplikace ve skupině A+

1.5.14.3 Třída A

Aplikace v této třídě pracují v režimu aktiv/pasiv mezi oběma lokalitami. V případě výpadku serveru v primární lokalitě nebo celé primární lokality bude aplikace po dobu nutnou k přepnutí do záložní lokality dočasně nedostupná. Přepnutí může být provedeno buď automaticky, poloautomaticky nebo manuálně, záleží na typu aplikace a možnostech jejího clusterování. Přepnutí do záložní lokality může mít vliv na výkonnost aplikace.

Typickou konfigurací je geografický HP SG cluster, kde je konfigurovaný failover aplikační balíček pro Oracle databázi (dále je DB).

Data jsou zrcadlena do záložní lokality prostřednictvím technologie HP Continuous Access XP, Veritas VM, MirrorUX (bude použit pro zrcadlení SAPu).



Obrázek 1.5-3 - Příklad řešení HA aplikace ve skupině A

1.5.14.4 Třída B

Aplikace v této třídě nepatří mezi kritické a nemají takové nároky na zajištění vysoké dostupnosti, proto pro ně nebude budováno clusterové řešení. Vysoká dostupnost je zajišťována na úrovni serveru, na kterém aplikace běží (technologie HP APA, Linux bonding, diskový RAID, vícenásobné připojení k SAN apod.).

1.5.15 Testování aplikací

Testování aplikací bude probíhat dle scénářů pro jednotlivé funkce a business procesy dodávaných aplikací. Seznam testovaných funkcí a procesů navrhne dodavatel, odběratelem může být doplněn a musí být odběratelem schválen. Testovací scénáře k funkcím / procesům včetně zátěžových testů zpracuje dodavatel a předá je

odběrateli před zahájením testů. Odběratel je oprávněn provádět testování procesů i nad rámec dodaných TS. Chyby vyskytující se při testování a retestování po jejich opravě budou evidovány v nástroji „Mantis“ až do uzavření akceptačních testů. Souhrnné údaje z nástroje Mantis budou sloužit pro vyhodnocování plnění akceptačních kritérií. Dodavatel bude mít do aplikace Mantis přístup po dobu provádění testů, komunikace mezi účastníky testování na straně odběratele a dodavatele bude probíhat v rámci tohoto nástroje. Obsluha aplikace a komunikace bude prováděna podle návodu k obsluze „Mantis“, který bude dodavateli rovněž k dispozici.

Při podpisu smlouvy s VZP ČR dostane dodavatel dokument „Test management VZP pro dodavatele“, který je nedílnou součástí těchto standardů.

1.5.16 Release management aplikací

Upgrade aplikačního programového vybavení se ve VZP provádí dle potřeby po dohodě s dodavatelem. Vlastní upgrade provádí pracovníci VZP dle dodaných instalačních průvodek a instalačních balíčků. Dodavatel umisťuje upgrade do sdíleného prostoru na serveru VZP a mailem informuje o umístění upgrade. Následně je upgrade pracovníky VZP otestován. Podrobný popis předávání upgrade do VZP je popsán v dokumentu „ Release management VZP pro dodavatele“.

Při podpisu smlouvy s VZP ČR dostane dodavatel dokument „Release management VZP pro dodavatele“, který je nedílnou součástí těchto standardů.

1.6 Datové a databázové standardy

Oblast standardizace	Popis
Minimum redundancí	Data jsou uložena na jednou databázi. Redundantní databáze v rámci lokality nejsou pro core business aplikace povoleny. Replikace se provádí pouze do dalších lokalit.
Dostupnost dat aplikací A++, A+	Aplikace v kategorii A++, A+ mají dostupné datové zdroje bez výpadku i v případě výpadku jednoho ze serveru v rámci lokality. Povolena je pouze ztráta spojení, které musí být okamžitě nahrazeno jiným. Databáze jsou provozovány na více než jednom serveru.
Replikace na záložní centra	Pro aplikace kategorií A++, A+ a A jsou data databáze replikována na záložní centrum (centra).
Jediný zdroj informací	Data jsou uložena v místě jejich vzniku, do ostatních systémů jsou poskytována prostřednictvím integrační platformy. Platí pravidlo minima duplicit.
Datová konzistence	Datová konzistence je zachovávána již v rámci databáze, tedy nikoliv pouze aplikačně.
Modelování DB pomocí ER diagramu	Jsou zachovány normálové formy. Pouze v případech, kdy je to nutné jsou možné výjimky – v dokumentaci však je explicitně uvedeno.
Návrh datového modelu	Návrh datového modelu je zodpovědností konkrétního vývojáře (dodavatele aplikace). Persistentní objekty vývojář definuje bez určení: • Názvu tablespace • fyzických atributů segmentu (pctused, pctfree, storage params,...) Databázové objekty jsou považovány za privátní součást aplikace, tj. aplikace nesmí přistupovat k databázovým objektům jiné aplikace.

1.6.1 Datové standardy

Aplikační kontext	Formát
Datová komunikace	XML
Web	XML, XHTML, HTML
Dokumenty	RTF, DOC, XLS, PDF, PDF/A,
Komprimace	ZIP, JAR, gz, bz2
Skenované dokumenty	TIFF, PDF, JPG
Obrázky	TIFF, JPEG, PNG
Kódování	UTF16, UTF8, ISO 8859-2, Windows 1250

1.6.2 Databázové standardy

Standard	Popis
Oracle DB 11g R2 1)	Pro aplikace tříd A++, A+ a A. Nebo i B.
MS SQL 2005, 2008, 2012, 2014 (x86 i X64)	Podpůrné služby a pro aplikace typu B.
Modelovaní pomocí ER diagramu	Fakta jsou vyjádřena pomocí tabulek v 5 NF. Entity (vyjádřeny tabulkami) jsou pojmenovány výstižným podstatným jménem v jednotném čísle. Mezi entitami je vytvořena relace typu 1:N a výstižně pojmenována slovesem nebo předložkou. Jsou-li čtena slova označující první entitu, relaci od ní a druhou entitu ve směru od N k 1, pak musí takto sestavená věta dávat smysl.
Zachování integrity na DB úrovni	Entitní integrita (jednoznačné určení každého řádku v rámci tabulky) Doménová integrita (každá hodnota atributu je vybrána z množiny přípustných hodnot) Referenční integrita (Atribut nebo skupina atributů tvořící v jiné tabulce (relaci) primární klíč nemůže nabývat nepřípustných hodnot)

Jmenné konvence databázových objektů

Všechna jména základních databázových objektů (tabulky, pohledy, balíky funkcí a procedur, fronty, sekvence, indexy, triggery apod.) začínají dvouznakovým prefixem dodavatele – GM (GEM System International s.r.o.), PB (PIKE ELECTRONIC s.r.o., Brno).

Názvy objektů, dále parametrů a sloupců jsou české, event. složené z českých zkratek.

Jména databázových tablespace začínají dvouznakovým prefixem dodavatele – např. GM (GEM System International s.r.o.), PB (PIKE ELECTRONIC s.r.o., Brno).

Dále je ve jménu tablespace použito CRE pro tabulkové tablespace, CIX pro indexové tablespace, TMP pro temporary tablespace. Jméno je doplněno jednoznačnou identifikací tablespace, např. PBCRE4.

Příslušné datafile pro jednotlivé tablespace jsou ukládány na databázovém serveru do následující adresářové struktury:

/oradata1/PVZP/PBcre41.dbf

kde oradata1 je příslušný datový adresář

PVZP je jméno databázové instance

PBcre41.dbf je příklad jména prvního datového souboru pro tablespace PBCRE4

Pro nově vytvářené databáze bude pro ukládání databázových souborů (Data,Indexy,Redology,Archlogy a Temporary) použito úložiště spravované prostřednictvím Oracle Automatic Storage Management.

1.6.3 Datová rozhraní

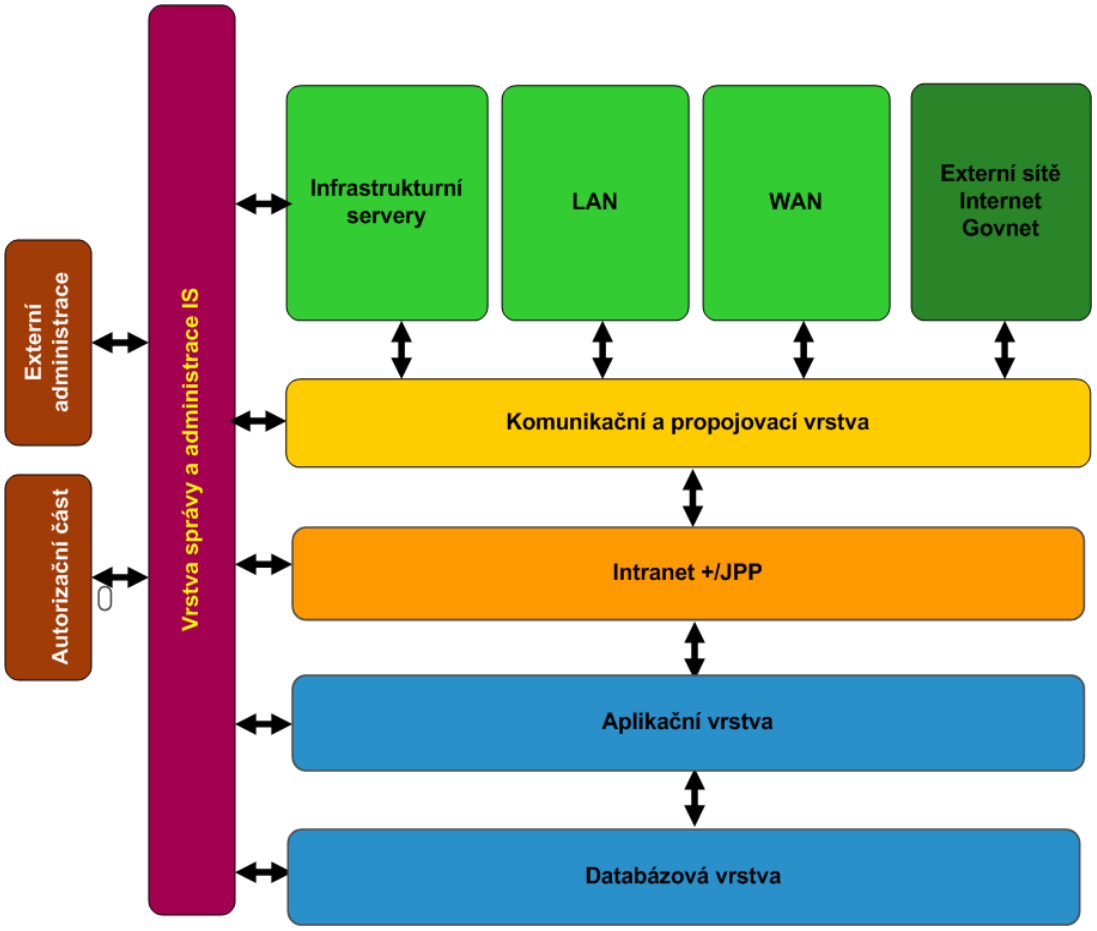
Pro komunikaci s externími partnery VZ ČR používá schválená datová rozhraní. Tato rozhraní jsou uvedena na Portále VZP ČR http://www.vzp.cz v sekcích dle jednotlivých kategorií partnerů.

Dodavatel nové komponenty IS bude respektovat zavedená datová rozhraní, popř. požádá VZP ČR o schválení nově navrhovaných rozhraní.

1.7 Komunikační standardy

1.7.1 Rozdělení do vrstev

Na následujícím obrázku je znázorněn požadovaný stav architektury síťového prostředí VZP (pro snadnější rozlišení celků s rozdílnou bezpečnostní úrovní je použito barevné odlišení).



Obrázek 1.7-1 Požadovaný stav architektury síťového prostředí VZP ČR

1.7.1.1 Standardy komunikace v datových centrech

Z vrstvy	Do vrstvy	Popis	Poznámky
Infrastrukturní servery	WAN	Komunikace je omezena na nezbytně nutné protokoly, porty a adresy.	
Infrastrukturní servery	LAN	Komunikace je omezena na nezbytně nutné protokoly, porty a adresy.	
Infrastrukturní servery	Vrstva správy a administrace IS	Komunikace směrem infrastrukturní servery -> Vrstva správy a administrace je omezena, opačná komunikace je založená na požadavcích nástrojů či aplikací určených pro monito-	

Z vrstvy	Do vrstvy	Popis	Poznámky
		rování a správu - např. SNMP, SYSLOG, RADIUS, terminálové služby…) a tomu odpovídá i povolená komunikace. Komunikace je zprostředkována Komunikační a propojovací vrstvou.	
Infrastrukturní servery	Externí sítě, Internet	Komunikace je zprostředkována Komunikační a propojovací vrstvou. Omezení pro komunikaci je specifikováno v popisu rozhraní „Komunikační a propojovací vrstva – Externí sítě, Internet“	
WAN	LAN	Komunikace je zprostředkována Komunikační a propojovací vrstvou. Komunikace je povolena pouze ve směru LAN ->WAN a to pro účely vzdálené administrace systémů.	
WAN	Vrstva správy a administrace IS	Komunikace směrem WAN -> Vrstva správy a administrace není povolena, opačná komunikace je založená na požadavcích nástrojů či aplikací určených pro monitorování a správu - např. SNMP, SYSLOG, RADIUS, terminálové služby...), a tomu odpovídá i povolená komunikace. Komunikace je zprostředkována Komunikační a propojovací vrstvou.	
WAN	Externí sítě, Internet	Komunikace je zprostředkována Komunikační a propojovací vrstvou. Omezení pro komunikaci je specifikováno v popisu rozhraní „Komunikační a propojovací vrstva – Externí sítě, Internet“.	
LAN	Vrstva správy a administrace	Komunikace směrem LAN -> Vrstva správy a administrace není povolena, opačná komunikace je založená na požadavcích nástrojů či aplikací určených pro monitorování a správu - např. SNMP, SYSLOG, RADIUS, terminálové služby...), a tomu odpovídá i povolená komunikace. Komunikace je zprostředkována Komunikační a propojovací vrstvou.	
LAN	Externí sítě, Internet	Komunikace je zprostředkována Komunikační a propojovací vrstvou. Omezení pro komunikaci je specifikováno v popisu rozhraní „Komunikační a propojovací vrstva – Externí sítě, Internet“	
LAN/WAN	Proxy vrstva	Komunikace je jednosměrně navazovaná uživateli z LAN/WAN • Komunikace je založená pouze na protokolu HTTPS,	

Z vrstvy	Do vrstvy	Popis	Poznámky
		• komunikace je na rozhraní filtrovaná („firewalling“) a jsou zde sledovány útoky („IDS/IPS“), • směrem do Proxy vrstvy se využívá content přepínačů (rozložení zátěže, přesměrování požadavků či zajištění vysoké dostupnosti), • směrem z Proxy vrstvy jsou prezentovány pouze jednotlivé služby JPP a struktura aplikační vrstvy je uživatelům skryta.	
Proxy vrstva	Vrstva správy a administrace	Komunikace směrem Komunikační a propojovací vrstva -> Vrstva správy a administrace není povolena, opačná komunikace je založená na požadavcích nástrojů či aplikací určených pro monitorování a správu - např. SNMP, SYSLOG, RADIUS, terminálové služby, ...) a tomu odpovídá i povolená komunikace. Komunikace je na rozhraní filtrovaná („firewalling“) a jsou zde sledovány útoky („IDS/IPS“).	
Proxy	Aplikační vrstva	Komunikace je jednosměrně navazovaná z Proxy vrstvy • Komunikace je založená na protokolu http, • uvnitř HTTP protokolu je předávána informace o uživateli pro autorizaci na aplikační vrstvě, • komunikace není na rozhraní filtrovaná, • směrem do aplikační vrstvy se využívá content přepínačů (rozložení zátěže, přesměrování požadavků či zajištění vysoké dostupnosti), • směrem z aplikační vrstvy jsou prezentovány pouze jednotlivé služby či aplikace (ne vlastní aplikační servery), struktura aplikační vrstvy je Proxy vrstvě skryta.	
Proxy vrstva	Externí sítě, Internet	Komunikace je omezena povolenými porty a komunikací na vrstvě „Externí sítě, Internet“, která zabezpečuje firewalling.	
Vrstva správy a	Aplikační vrstva	Komunikace je jednosměrně navazována z	

Z vrstvy	Do vrstvy	Popis	Poznámky
administrace		vrstvy správy a administrace. Jedinou výjimku tvoří: SNMP trap • komunikace je založená na požadavcích nástrojů či aplikací určených pro monitorování a správu aplikační vrstvy (např. SNMP, SYSLOG, RADIUS, terminálové služby, ...) • komunikace je na rozhraní filtrovaná („firewalling“) a jsou zde sledovány útoky („IDS/IPS“)	
Vrstva správy a administrace	Databázová vrstva	Komunikace je jednosměrně navazována z vrstvy správy a administrace IS. Jedinou výjimku tvoří : SNMP trap,... • komunikace je založená na požadavcích nástrojů či aplikací určených pro monitorování a správu aplikační vrstvy (např. služby - SNMP, SYSLOG, RADIUS, terminálové služby, ...) • komunikace je na rozhraní filtrovaná („firewalling“) a jsou zde sledovány útoky (IDS/IPS)	
Aplikační vrstva	Databázová vrstva	Komunikace je jednosměrně navazovaná aplikacemi (Aplikační vrstva ->Databázová vrstva), komunikace je založená na požadavcích aplikací – SQL link nebo SSH, na tomto rozhraní je preferována propustnost před bezpečností, proto zde není uvažováno nasazení firewallů, aplikace se odkazuje na virtuální adresu databázového clusteru.	

1.7.2 Komunikační pravidla zón DC

DC je rozděleno do několika bezpečnostních zón, mezi kterými platí určitá pravidla. Zóny představují zpravidla několik L3/L2 segmentů, která mají podobná bezpečnostní pravidla. Zóny jsou IP adresací příslušné k lokalitě DC. Výjimku tvoří zóna DC-DB, ta je L2 geograficky rozprostřena mezi lokalitami DC1 a DC2.

Rozdělení DC zón:

- **VZP NET**
  Zóna označuje síť VZP, která není součástí DC – tj. infrastrukturní část LAN/WAN včetně části koncových uživatelů.

- **DC-DMZ**
  Zóna je dostupná z obou stran jak pro VZP, tak pro DC. Slouží k zabezpečení a poskytování služeb. Typicky Management, DNS, MS AD DC nebo LDAP, ACS.
- **DC-VIP**
  Prezentační vrstva DC, Jedná se o virtuální IP adresy, které reprezentují jednotlivé aplikace pro přístup jak z VZP NET tak z ostatních aplikací DC.
- **DC-APP**
  Aplikační vrstva DC. Umístění aplikačních serverů.
- **DC-DB**
  Databázová vrstva DC. Umístění DB serverů. L2 vrstva rozprostřená geograficky mezi lokalitami DC1 a DC2. Pouze v databázové vrstvě je možné vytvářet clustery se společnou IP adresou mezi jednotlivými lokalitami.
- **DC-SERVIS**
  Zóna slouží jako prostředník pro výměnu dat mezi ostatními zónami a mezi prostředími.

Zóny DC-APP a DC-DB nejsou přímo dostupné z VZP NET a obráceně. Komunikace musí být zprostředkována přes některou ze zón:
DC-DMZ
DC-VIP
DC-SERVIS

Komunikační matice zobrazuje podporované komunikace mezi jednotlivými zónami.

Komunikační matice zón DC

Komunikace ze zóny ↓	Komunikace do zóny → VZP NET	DC-DMZ	DC-VIP	DC-APP	DC-DB	DC-SERVIS
VZP NET	ANO	ANO	ANO	⊖	⊖	ANO
DC-DMZ	ANO	ANO	ANO	ANO	ANO	ANO
DC-VIP	⊖	⊖	⊖	ANO	⊖	⊖
DC-APP	⊖	ANO	ANO	⊖	ANO	ANO
DC-DB	⊖	ANO	⊖	možné	možné	ANO
DC-SERVIS	ANO	ANO	⊖	ANO	ANO	ANO

1.7.3 Standardy síťového prostředí

Aspekt	Popis	Poznámky
Lokální pobočkové sítě	Za technologický standard je považována technologie Cisco pro přepínané i směrované prostředí. Klienti jsou odděleni od serverů, tiskáren a infrastrukturních prvků pomocí virtuálních LAN (VLAN). Jejich vzájemná komunikace je zajištěna směrováním na pobočkovém prvku včetně základního zabezpečení a pravidel definovaných pomocí accesslistů. Standardem pro připojení je 10/100 Mbit ethernet či 1000Mbit ethernet pro server. Redundance a kon-	

Aspekt	Popis	Poznámky
	vergence pobočkové LAN sítě je zajištěna protokolem Spanning tree.	
WAN sítě	WAN síť se dá rozdělit na přenosovou část a část šifrátorů. Pro přenosovou část je standardem IP MPLS konvergentní síť s definovanou a měřenou šířkou pásma. Tato síť je též vybavena QoS pro diferenciaci provozu v rámci VZP. Část šifrátorů zajišťuje autentikaci jednotlivých poboček pomocí certifikátů a dále pak šifrování celého datového toku mezi pobočkami s časově poměným klíčem. Za standard se dá považovat autentikace pomocí certifikátů, šifrování 3DES či AES, výměna klíčů pomocí Diffie-Helman. Šifrátory jsou též vybaveny access-listy zamezující průlomu do VZP sítě z MPLS-VPN.	VZP vyžaduje, aby se komunikace nových komunikačních komponent byla rozdělována do příslušných QoS tříd.
Připojení k internetu	Standardem je vícestupňový firewalling s definovanými DMZ. Každá bezpečnostní zóna je chráněna accesslisty proti útoku z Internetu včetně aplikační logiky. Pro větší granularitu odhalení útoku jsou v cestě též IPS sondy. Celý systém je spravován pomocí SW Cisco security manager jenž se stará o aktuálnost nastavení, nahrání posledních úprav SW či signatures. Pro vzdálené připojení klientů či organizací do VZP je standardem authentikace a authorizace pomocí veřejných certifikátů a navázání šifrovaného tunelu do VZP. Zde je na firewallech definován prostup dle platných směrnic VZP.	
Připojení klientů	Standardem pro připojení klientů přes drát či „bezdrát“ je technologie 802.1x. Tato technologie na síťové úrovni připojí pouze autentikované počítače či klienty (mající certifikát). .	
LAN datových center	Datová centra jsou propojena technologií DWDM přes jeden pár optického vlákna.. Standardem pro jednotlivé vrstvy (zóny) datového centra jsou modulární Cisco přepínače / směrovače s Service moduly. Jednotlivé vrstvy jsou Content přepínány a prostupy mezi nimi jsou definovány pomocí Firewall modulů. SSL komunikace směrem k serverům je zakončena SSL modulem a dále přeposlána v otevřené formě.	
IP telefonie	Standardem pro telefonii je IP Cisco telefonie s centrálním Call managerem clusterem v datových centrech. Provázanost na veřejnou PSTN a do sítě mobilních operátorů je přes Cisco VoIP hlasové brá-	

Aspekt	Popis	Poznámky
	ny.	
Služby DNS	Současným standardem pro poskytování služeb DNS je systém IPAM od firmy Infoblox, případně systém BIG-IP od firmy F5.	
Služby DHCP	Současným standardem pro poskytování služeb DHCP je systém IPAM od firmy Infoblox.	
VPN připojení	Standardem pro připojení klientů do sítě VZP pomocí VPN je protokol SSL. Podporovaným klientem je Cisco AnyConnect Secure Mobility Client v aktuální verzi, kterou lze instalovat z https://vpn.vzp.cz	

1.7.4 Loadbalancing

V IS VZP ČR existují následující 3 druhy loadbalancingu

- Loadbalancing v datových centrech, který zajišťují Application Content Engine (ACE) moduly a Global Site Selector (GSS)
- Loadbalancing v perimetru sítě, který zajišťuje F5-Local Traffic Manager (LTM) a F5-Global Traffic Manager (GTM)
- Loadbalancing ve VZP netu, který zajišťují Content switche

1.7.4.1 Loadbalancing v datových centrech

Pro loadblancing mezi datovými centry DC1-Orlická a DC2-Perštýn se používá loadbalancing na bázi DNS, který zajišťuje GSS. Standardně je loadbalancing konfigurován takto:

Sondy - Kal-Ap by VIP

Balance method - Hashed by Source Address

- Round Robin

Stickyness - Ano

DNS TTL - 300 s

Pro loadbalancing mezi jednotlivými servery v rámci jednoho datového centra se používají ACE moduly, které jsou standardně nakonfigurovány takto:

Sondy - http, metoda head

Balance method - Round Robin

Stickyness - Ano, source address, timeout 30 minut

Loadbalancing v DC je možné nakonfigurovat odlišně od těchto standardů. Zadání se provádí pomocí Excel souboru DC_ID_<jméno projektu>_v<číslo verze>.xls v sekci lokální aplikace. Vzor je uveden na obrázku níže.

Lokální aplikace									
Název aplikace	Stickiness	Keepalive URL	Protokol	Porty	URI	FQDN	Sezení (čas v sec)	Zdroj. IP adresy (odkud se komunikuje)	Nestandardní požadavky

1.7.4.2 Administrátorská sonda

Pro účely provádění údržby serveru je nutné zajistit automatické vyjmutí serveru ze server farmy. K tomuto účelu slouží tzv. administrátorská sonda, která pomocí metody http-head nebo http-get vrací stav serveru. Pokud je odpověď 200-O.K. server je zařazen do farmy a obsluhuje standardní klientské požadavky. Pokud je odpověď cokoliv jiného je server z farmy vyřazen. Metodou http-get je možné požadovat podrobnější testování stavu serveru..

Tato administrátorská sonda musí být dodána ke každému aplikačnímu serveru v datových centrech.

1.7.4.3 Loadbalancing v perimetru

Aplikace, které jsou umístěny v perimetru, jsou loadbalancovány prostřednictvím zařízení F5 BIG-IP. Tyto aplikace mohou být přístupné interním i externím uživatelům

Aplikace, které jsou umístěny pouze v jednom perimetru, je možné loadbalancovat mezi více servery prostřednictvím F5 BIG-IP Local Traffic Manager (LTM). Aplikace jsou standardně balancovány metodou round-robin. Jsou k dispozici i další metody. Kontrola dostupnosti je standardně prováděna prostřednictvím ICMP pingu na každý server a TCP CONNECT na portu specifickém pro danou aplikaci. Oproti standardu je možné na základě zadání provádět kontrolu dostupnosti i jiným způsobem např. http-get. Je rovněž možné definovat stickyness. Změna standardu loadbalincingu se provádí zadáním pomocí tabulky, jejíž vzor je totožný se vzorem uvedeným v kapitole 1.7.4.1.

Aplikace, které jsou umístěny v obou perimetrech, je možné loadbalancovat mezi více servery v obou perimetrech prostřednictvím F5 BIG-IP Global Traffic Manager (GTM). V tomto případě jsou aplikace nakonfigurovány v LTM v dané lokalitě jako v předchozím případě a platí pro ně vše, co bylo zmíněno v předchozím odstavci. LTM modul pak u aplikací dostupných v obou perimetrech poskytuje modulu GTM informace o tom zde je aplikace v daném perimetru dostupná – či nikoliv. GTM modul poskytuje pro tyto aplikace službu inteligentního DNS.

Rovněž loadbalancing v perimetru je nutné doplnit o „administrátorskou sondu“ – viz kapitola 1.7.4.2

1.7.4.4 Loadbalancing ve VZP-netu

Ve VZP-netu je loadbalancing prováděn prostřednictvím Cisco Content Service Switche 11503 (CSS). V specifických případech – kdy je třeba aplikaci provozovat active-active mezi oběma centrálními lokalitami – je použito GSS. Monitoring dostupnosti aplikace je u CSS možný pouze jednoduchým mechanismem (keepalive - probe) (ICMP, TCP/UDP ping nebo http-get apod.). U CSS není možné kombinovat více keppalive do jedné logické probe (např. ICMP a http-get). CSS umožňuje napsat si vlastní scriptovaný keepalive.

Provoz aplikace je směrován na VIP adresu v konkrétní lokalitě. CSS rozděluje provoz mezi servery standardně metodou round-robin. Oproti standardu je možné na základě zadání provádět kontrolu dostupnosti i jiným způsobem např. http-get. Je rovněž možné definovat stickyness. Změna standardu loadbalincingu se provádí zadáním pomocí tabulky, jejíž vzor je totožný se vzorem uvedeným v kapitole 1.7.4.1.

Pro případ výpadku jednoho CSS nebo výpadku připojení do jedné lokality jsou VIP adresy inzerovány do routovací tabulky na obou lokalitách – avšak s různou metrikou. V případě výpadku je možné k službě dále při-

stupovat za předpokladu, že servery a centrální switche nadále fungují a že je funkční DWDM propojení obou lokalit.

1.8 Bezpečnostní standardy

Požadavky	Popis
Zajistit definovanou úroveň bezpečnosti pro systémy a aplikace	Definováním standardů bude zajištěna jasně definovaná úroveň zabezpečení systémů.
Předejít neoprávněným přístupům, změnám, zničení a ztrátám společnosti	Dodržováním a kontrolou definovaných standardů se zajistí odolnost proti bezpečnostním incidentům a hlavně připravenost na ně.
Zabezpečit diskrétnost, integritu, dostupnost a závaznost IS VZP ČR	Zabezpečení ICT je vnímáno jako celek a zahrnuje a proniká do všech souvisejících oblastí. Požadované celistvosti je dosaženo definováním bezpečnostních pravidel.

1.8.1 Základní bezpečnostní pravidla

Aspekt	Popis	Poznámky
Respektování zákonných předpisů	Striktní dodržování zejména: • Zákon o ochraně osobních údajů (zákon č. 101/2000 Sb., o ochraně osobních údajů a změně některých zákonů, v platném znění.) • Autorský zákon (zákon č. 121/2000 Sb., o právu autorském, právech souvisejících s právem autorským a o změně některých zákonů, v platném znění.)	
Obecné pravidlo bezpečnosti	Vše co není výslovně povoleno bezpečnostní směrnicí je zakázáno. Toto pravidlo platí pro všechny systémy, aplikace, procesy a zaměstnance, uživatele, apod.	
Minimalizování běžících služeb	Na serverech jsou nainstalovány a běží pouze takové služby, které jsou nezbytné pro korektní běh aplikací nebo správy systému. Ostatní služby musí zůstat vypnuté.	
Nevyhovující služby nebo protokoly	Služby nebo protokoly, které nevyhovují minimálním bezpečnostním požadavkům pro přenos či zpracování definované kategorie citlivosti informace nesmí být pro přenos nebo zpracování informace použity.	Např. pro administraci použít protokol telnet, apod.
Klasifikace informací	Všechny informace mají definovanou kategorii citlivosti, která je odvozena od důležitosti informace pro společnost nebo zákonem. Kategorie citlivosti dále určuje jakým způsobem může být s informací nakládáno. Každá informace	

	musí mít určeného vlastníka, který je zodpovědný za definovaní pravidel přístupu a zacházení s informací a kontrolou dodržování těchto pravidel.	
Logování informací	Logované informace se udržují po dobu definovanou zákonem nebo určenou podle citlivosti informace, ke které se přistupovalo a o které je veden záznam. Logované informace musí vždy obsahovat kdo, kdy, kam a co provedl, resp. jak akce dopadla. Z logované informace musí být zřejmé, co se stalo a jak to dopadlo a jednoznačné určení kdo to provedl.	
Dodržování licenčních podmínek	Ve VZP je dodržování licenčních podmínek používaného systému, aplikace, SW, apod. striktně vyžadováno a kontrolováno.	
Projektová bezpečnostní dokumentace	Úvodní bezpečnostní studie informačního systému Zpráva o výsledcích analýzy rizik Návrh bezpečnostních opatření pro jednotlivé fáze projektu Plán implementace vybraných bezpečnostních opatření Dokumentace k testům bezpečnosti výsledku projektu	Schvaluje OBIT
Test zranitelnosti aplikace	Před nasazením komponenty IS do provozu IT musí být proveden test zranitelnosti aplikace nástrojem NESSUS, nebo v případě potřeby tento test realizovat nezávislým penetračním testem externím dodavatelem..	

1.8.2 Identifikace při přístupu k systémům a aplikacím

Aspekt	Popis	Poznámky
Identifikace uživatele	Identita uživatele je uchovávána v AD. Identita uživatele v systémech je řízena IDM.	
Hesla	Hesla musí mít minimální délku 8 znaků z kombinace alfanumerických znaků (a, b, …, 1, 2, …) a nesmí se vztahovat k práci nebo osobnímu životu (např. registrační značka vozidla, jméno manželky, manžela, části bydliště atp.) a nesmí používat samotná slova obsažená ve slovníku (vlastní jména, technické výrazy, atd.). Složitost hesla musí odpovídat citlivosti informace (citlivější informace = složitější heslo) ke které je přistupováno (u složitějších hesel se doporučuje kombinace alfanumerických a zvláštních znaků (a, b, …, 1, 2, …, *, @, #, …)). Heslo musí být uchováno v tajnosti a periodicky měněno. Hesla nesmí být uchovávána v čitelné podobě v dávkových souborech, automatických přihlašovacích skriptech, makrech, zkratkových klávesách, v nechráněných systémech a všude jinde, kde by mohlo dojít k jejich odhalení. Pokud	

Aspekt	Popis	Poznámky
	existuje jakékoli podezření, že heslo zná někdo jiný než oprávněný držitel, je nutno identifikaci (heslo, certifikát) okamžitě změnit.	
Expirace hesel	Všechny přístupové účty musí mít nastavenou časovou platnost hesel (expirační dobu) maximálně na 90 dní. Pokud v tomto časovém úseku nedojde ke změně hesla, účet se po uplynutí expirační doby automaticky uzamkne. O opětovné zprovoznění takto uzamčeného účtu je nutno požádat Administrátora systému nebo aplikace.	
Anonymní účty	Vytváření anonymních účtů, které nemají přímou vazbu na konkrétní zodpovědnou osobu, je zakázáno.	
Mechanismus obrany proti hádání přístupu do systému	Ve všech systémech nebo aplikacích musí být implementována kontrola proti pokusům o uhádnutí uživatelských jmen a hesel (např. prostřednictvím omezeného počtu pokusů o přihlášení a definované doby omezení přístupu do systému či aplikace). V případě několika neoprávněných přístupů musí dojít k automatickému uzamčení postiženého účtu. Opětovné odemknutí je v kompetenci Administrátora systému nebo aplikace. Navržený mechanismus musí být navržen tak, aby nedošlo k hromadnému zamykání a tím odepření služby. Schválení mechanismu podléhá OBIT.	
Požadavky na přístupy	Požadavky na udělení přístupových práv musí být písemně nebo pomocí e-mailu schváleny vlastníkem aplikace. K vybraným systémům je navíc vyžadován souhlas s udělením přístupového oprávnění od definované osoby.	
Požadavky na řízení přístupu do IS VZP ČR přes VPN	Pravidla provozování a podmínky udělování přístupu přes VPN pro interní zaměstnance i externí subjekty se řídí příslušnými interními normami a směrnicemi VZP ČR a podléhá schválení určenými osobami VZP.	

1.8.3 Bezpečnost infrastruktury

Aspekt	Popis	Poznámky
Připojení systémů do vnitřní sítě	Všechna zařízení, která jsou připojována, ať již trvale nebo dočasně, k vnitřní počítačové síti, musí být zabezpečena minimálně způsobem „uživatel/heslo“. Systémy obsahující citlivá data musí rovněž splňovat tuto minimální úroveň zabezpečení, a to bez ohledu na to, zda jsou připojeny k síti či nikoli. Připojení cizího zařízení k vnitřní počítačové sítí podléhá schválení OBIT.	
Komunikace z externích sítí	Všechna připojení, která směřují z/do externích sítí (internet, veřejné telefonní sítě, atd.) do/z vnitřní sítě, musí být schválena definovanou osobou a OBIT-em a kontrolována definovaným bezpečnostním prvkem. Externí přístup nesmí	

Aspekt	Popis	Poznámky
	snížit úroveň zabezpečení systému, aplikace nebo společnosti. Externí přístup musí zajistit silnou autentizaci přistupující strany a logování kdo kdy, kam a jak dlouho přistupoval.	
Zapojení nového systému do infrastruktury	Zavádět nové systémy nebo připojovat další datové sítě do lokální počítačové sítě bez písemného souhlasu definované osoby je zakázáno. Zapojení jakéhokoliv nového (i přeinstalovaného) systému do infrastruktury vyžaduje otestování systému, zda dodržuje odpovídající bezpečnostní požadavky. Akceptační testy zabezpečuje OŘZ v součinnosti s OBIT-em. Schválení za oblast bezpečnosti IT je plně v kompetenci OBIT-u.	
Změny v síťové infrastruktuře	Změny v počítačové síti zahrnují upgrade komunikačního softwaru, změny konfigurací IP adres, změny konfigurací routerů a jiných aktivních síťových prvků apod. S výjimkou řešení výpadku v sítové infrastruktuře musí být veškeré tyto změny: • zdokumentovány podle platného procesu Změnového řízení,, • současně schváleny bezpečnostním architektem a síťovým architektem.. Všechny změny týkající se řešení výpadku v síťové infrastruktuře mohou provádět pouze osoby pověřené prováděním změn v síťové infrastruktuře.	

1.8.4 Internet – důvěryhodnost a obezřetnost

Aspekt	Popis	Poznámky
Přenášení citlivých informací přes Internet	Je striktně zakázáno přenášet prostřednictvím Internetu informace klasifikované jako citlivé v otevřené (nešifrované) podobě. Jedná se např. o uživatelská jména a hesla pro vstup do systémů, čísla firemních kreditních karet a další informace mající pro společnost strategický význam.	
Kontrola vstupních informací aplikací	Jakýkoliv vstup do aplikace musí provádět kontrolu na typ a množství přijímaných dat. Kontroluje se dodržení definovaného formátu dat a výskyt nedovolených vstupních znaků či řetězců. Nevyhovující data nesmí být dále zpracovávána a zároveň tato informace musí být logována.	

1.8.5 Šifrování a citlivost informací

Aspekt	Popis	Poznámky
Přenášení citlivých informaci po síti	Pokud jsou citlivé informace přenášeny po síti, musí být respektována pravidla šifrování a klasifikace informací.	
Citlivé informace na nosičích	Pokud jsou citlivé informace uloženy na nosičích, ať již pro potřeby přenášení informací či z důvodu zálohy, musí být respektována pravidla šifrování a klasifikace informací.	
Dokumentace	V rámci dokumentace nesmí být použita osobní nebo citlivá data. Taková data musí být anonymizována. Anonymizací se rozumí taková úprava, po které nelze údaje vztáhnout k určenému nebo určitelnému subjektu údajů.	
Ochrana privátního klíče	Jakýkoliv privátní klíč musí být chráněn heslem. Privátní klíče musí být spolehlivě zálohovány pro případ jejich ztráty nebo poškození. Zároveň musí být definovány postupy pro obnovení klíče a postupy instalace nového klíče v případě nedůvěry ve starý aktuální klíč.	
Pravidla šifrování	Musí být dodrženy postupy a pravidla kdy a pro jaké kategorie citlivosti se musí dokumenty šifrovat, kdy podepisovat a kdy oboje najednou. Zároveň musí být používány pouze schválené nástroje.	

1.8.6 Fyzická bezpečnost

Aspekt	Popis	Poznámky
Kontrola vstupu do objektu s technologií	Každý objekt, ve kterém je umístěna technologie systému má na vstupu do objektu vrátnici, kde je prováděna kontrola oprávněnosti přístupu do objektu..	
Identifikační karty	Každá oprávněná osoba vlastní identifikační kartu a při vstupu do objektu a pohybu v něm používá identifikační kartu na prokázání identity a rozhodnutí o oprávněnosti vstupu. Identifikační karta je nošena na dobře viditelném místě.	
Neoprávněné přístupy	Opakované pokusy o neoprávněný fyzický přístup jsou bezodkladně řešeny bezpečnostní službou provádějící ostrahu objektu.	
Vstupy do místností s technologií	Pro vstup do místnosti s technologii je vyžadováno ověření oprávnění přístupu přes identifikační kartu. Vstup je vždy kontrolován bezpečnostní kamerou. Bezpečnostní technologie pro kontrolu fyzického přístupu jsou voleny podle důležitosti dat, které se v místnosti nalézají.	

Kamerový dohled serveroven	Veškeré prostory s technologií datových center jsou sledovány bezpečnostními kamerami, které přenášejí „on-line“ obraz na dohledové stanoviště s nepřetržitou službou. Jsou klasifikovány jako zabezpečené oblasti.	
Požární detektory a hlásiče v serverovnách	V serverovnách jsou instalovány detektory a hlásiče požáru. Serverovny jsou vybaveny samo hasicí technologií pro případ požáru. Informace o změně stavu musí být bezodkladně hlášeny na dohledové stanoviště.	
Dostupnost napájení	Každá serverovna je vybavena nepřerušitelným zdrojem napájení (UPS) a záložním generátorem napájení.	
Obecné podmínky objektové bezpečnosti v zabezpečených oblastech	Zabezpečené oblasti jsou situovány mimo prostory plynného a prašného znečištění tak, aby nebyly ohroženy záplavami, hladinou spodní vody a provozními haváriemi. Zabezpečené oblasti jsou stavebně řešeny jako uzavřené prostory. Stěny, podlahy a stropy jsou zděné nebo betonové stavební konstrukce. V zabezpečených oblastech jsou instalována zařízení upravující klimatické podpínky.	

1.8.7 Bezpečnost provozu systému

Aspekt	Popis	Poznámky
Provozní dokumentace	Ke každému systému musí existovat provozní dokumentace popisující každou činnost prováděnou na systému. Dokumentace bude obsahovat také kontakty na administrátory a vlastníky systému. Zároveň musí obsahovat postupy v případě neočekávaných problémů.	
Řízení změn	Jakékoliv změny, které mají vliv na nastavení systému, musí být zdokumentovány a projít procesem Řízení změn.	
Řešení a evidence incidentů	Při řešení jakékoliv nestandardního chování, které je v rozporu s definovaným chováním systému, musí být postupováno podle procesu Správy incidentů.	
Oddělení prostředí	Produkční, testovací a vývojové prostředí musí být od sebe odděleno tak, aby nebylo možné, že změny provedené v prostředí X ovlivní prostředí Y. Výjimečně musí být minimálně odděleno produkční prostředí od ostatních prostředí.	
Zálohování OS a dat	Všechny systémy musí být zálohovány. Pravidelnost a hloubka zálohování je určena kritičností systému či citlivostí informací uložených v systému.	
Definice práv na souborovém systému	U systémů, které umožňují uživatelům vlastní definici práv na souborovém systému, se mimo odůvodněných případů nesmí přidělovat všechna práva k danému objektu (read, write, execute, atd.).	
Elektronické zasílání	Možný obsah zprávy el. pošty vymezuje klasifikace infor-	

Aspekt	Popis	Poznámky
zpráv	mací. Pravidla pro možné způsoby použití systému el. pošty jsou dána příslušnými PŘ VZP ČR.	
Bezpečnost při zacházení s médii	Správa výměnných počítačových médií a jejich likvidace podléhají pravidlům popsaných v klasifikaci informací.	
Ochrana proti škodlivým programům a mobilním kódům	V prostředí pojišťovny jsou zavedena pravidla a opatření na ochranu proti škodlivým programům a mobilnímu kódu jež je nutné dodržovat a akceptovat.	

1.8.8 Nepovolené aktivity

Aspekt	Popis	Poznámky
Neoprávněné aktivity	Aktivity, které zahrnují neoprávněné přístupy k systémům, aplikacím, datům, neoprávněné dešifrování, neoprávněné pořizování kopií, zatěžování systémů, zneužití počítačových a síťových systémů, a dále aktivity, které nesouvisí s pracovní činností nebo vedou k porušování interních norem či jsou v rozporu s právním řádem ČR, nejsou povoleny a mohou být posuzovány jako porušení pracovní kázně zvláště hrubým způsobem. V této souvislosti si VZP ČR vyhrazuje právo na zrušení přístupů do systémů kterémukoliv uživateli v jakoukoliv dobu.	
Zrušení přístupu do systémů	Rozhodnutí o zrušení přístupu do systémů pro uživatele v případě neoprávněného přístupu k systémům, aplikacím, datům, neoprávněného dešifrování, neoprávněného pořizování kopií, zatěžování systémů, kompromitace počítačových a síťových systémů, podléhá schválení Manažerovi bezpečnosti.	

1.8.9 Porušování pravidel bezpečnosti IT

Aspekt	Popis	Poznámky
Hlášení incidentů	Jakékoli podezření na porušování bezpečnostních pravidel, pokusy o prolomení systémů, o šíření virové nákazy a další obdobné hrozby a incidenty, musí uživatel neprodleně ohlásit definovaným Administrátorům nebo zapsat do k tomuto účelu vytvořenému systému.	

1.9 Standardy monitorování provozu informačního systému

Dohled provozu informačního systému je centralizovaný a je zajišťován dohledovým centrem v pracovních dnech od 6:00 do 22:00 hod. (v režimu 5x16). V tom čase jsou drženy pohotovosti řešitelských skupin pro síťovou infrastrukturu, operační systémy Unix, Windows, Oracle databáze, provoz aplikací, Exchange a pro dohledové nástroje.

1.9.1 Nástroje monitoringu

Centrální systém dohledu provozu informačního systému je vybudován na platformě HP OpenView. Do dohledového centra HPOV (centrální konzole) jsou soustřeďovány všechny důležité zprávy z ostatních monitorovacích nástrojů. HP OpenView je propojen s nástrojem Service Manager.

Pomocí nástroje HP OpenView Operations Manager je sledován průběžný stav a výkon všech unixových systémů, které zajišťují provoz aplikací. U klíčových unixových systémů je pro detailnější sledování výkonnosti nasazen HP OpenView Performance Manager.

Všechny infrastrukturní komponenty Oracle jsou monitorovány pomocí agentů Oracle Enterprise Manager (OEM) / Oracle Grid Control. Nástroj je integrován do centrální konzole HP OpenView.

Sledování provozu, parametrů a funkčnosti služeb všech serverů Windows je zajištěno produktem MS System Center Operations Manager (SCOM) s integrací do HP OpenView.

Monitoring uživatelské dostupnosti (aplikační monitoring) aplikací je nasazován pomocí HP Business Availability Center (HP BAC). Tento nástroj je integrován do centrální konzole HP OpenView, a to obousměrně.

Monitoring datových sítí (LAN i WAN) je primárně prováděn pomocí HP OpenView Network Node Manageru. Jsou sledovány klíčové prvky sítí (směrovače, přepínače, WAN akcelerátory, GSS, Load balancery), v případě potřeby jsou sledovány i další důležité prvky, např. servery.

Klíčové síťové prvky jsou sledovány pomocí HP NNM. Vybrané události jsou integrovány do konzole HP OpenView. Kvalitativní parametry sítí jsou monitorovány pomocí nástrojů v CiscoWorks LMS. Nástroj není integrován s HP OpenView.

Sledování výkonnostních parametrů sítí je zajišťováno nástrojem HP Network Control Center.

Bez-agentní způsob sledování lze uskutečnit pomocí HP Sitescope.

1.9.2 Podrobný popis monitoringu

Podrobný popis monitoringu provozu IS VZP je popsán v dokumentu „Standardy pro monitoring IS“ Při podpisu smlouvy s VZP ČR dostane dodavatel dokument „Standardy pro monitoring IS“.

1.10 Zálohování informačního systému

Konfigurace zálohovacího serveru je konfigurací vysoce dostupnou. Vlastní koncept zálohování je založen na zálohovacím software schopném běhu ve všech datových centrech. Fyzicky jsou data ukládána na dvojici knihoven ve dvou datových centrech. Vlastní zálohování probíhá křížem vždy z datového úložiště v jedné lokalitě na pásku v lokalitě druhé. Případná třetí lokalita je zálohována jednou z knihoven.

Mechanismus zálohování je stejný pro všechny aplikace a OS:

- HP-UX, Windows, Linux filesystémy
- Oracle databáze
- MS SQL databáze,
- MS Exchange,
- další aplikace a systémy.

Poznámka: Zálohování Windows otevřených souborů pomocí VSS.

V případě HP-UX je zálohování doplněno o nástroj Ignite, který slouží k disaster recovery (DR) systémového disku. V případě platformy Windows je DR vyřešeno s pomocí DataProtectoru.

Každý provozovaný server, vyžadující zálohování musí umožnit instalaci aplikace DataProtector. Licence tohoto software při nových dodávkách zajišťuje VZP ČR, dodavatel však vždy musí v nabídkách a dalších dokumentech specifikovat počet zálohovaných serverů včetně pasivních nódů.

1.11 Auditní stopa

Každá z částí IS VZP ČR pracující s klientskými daty musí veškeré informace týkajících se styku s klientem zapisovat do komponenty nazvané auditní stopa.

Auditní stopa (AST) poskytuje tyto informace:

- Poskytnutí přehledu o uskutečněné komunikaci mezi VZP a klientem (tedy nezávisle na systému kde informace vznikla)
- podklady pro případnou reklamaci ze strany klienta,
- podpora tvorby statistik pro monitoring komunikace se zákazníky (spolupráce s analytickými nástroji a CRM),
- přehled o komunikaci s VZP pro potřeby klienta (pohled přes kanál Portálu, či B2B nebo další kanály),
- sledování konkrétního případu/procesu (zvláště přes více systémů),
- přehled komunikace konkrétního klienta,
- přehled komunikace konkrétního pracovníka VZP ČR.

Přístup k auditní stopě je možné přes IPF – pro čtení a zápis; nebo přes grafické rozhraní pro pracovníky VZP ČR.

Součástí každé analýzy a implementace systému je seznam událostí, které budou do auditní stopy předávány. Součástí analýzy je i vazba na implementované obchodní procesy.

1.11.1 Technické informace

Auditní stopa (AST) je úložiště, do kterého vkládají aplikace prostřednictvím služby IPF záznamy o vybraných událostech, spojených s komunikací mezi VZP a jejím klientem nebo partnerem.

Auditní stopa neuchovává přenášená data, součástí záznamu může být odkaz na data uložená v aplikaci hash záznamu, pomocí kterého je možné jednoznačně určit, zda nebylo se záznamem dodatečně manipulováno.

Záznam do Auditní stopy provádí aplikace prostřednictvím služby IPF v okamžiku, kdy proběhne výměna dat mezi VZP ČR a jejím klientem nebo partnerem, případně jiná událost, která má být v AST zachycena. Tato služba je realizována jako synchronní, v rámci jejího volání musí být dodány vstupní parametry (např. identifikátor aplikace, události, procesu, klienta nebo partnera apod...)

Čtení z Auditní stopy je v rámci IPF zpřístupněno jako další služba, poskytovaná IPF. Služba je realizována jako synchronní, prezentaci dat dle uživatelské role zajišťuje aplikace volající tuto službu.

Registr procesů je seznam spravovaný v podobě registru ve standardní aplikaci IS „Centrální správa číselníků (CSČ)“. Registr procesů obsahuje informace jako např. označení typu procesu a jméno procesu.

Registr typu klienta Tento registr typů klienta (např. fyzická osoba, právnická osoba apod.) je spravován v podobě registru ve standardní aplikaci IS „Centrální správa číselníků (CSČ)“.

Registr skupin událostí je seznam možných skupin (např. události typu telefonní komunikace, příjem podání, apod.). Tento registr je spravován v podobě registru ve standardní aplikaci IS „Centrální správa číselníků (CSČ)“.

Registr atributů. Každá událost může být spojena s atributy/metadaty, tyto atributy zároveň umožňují realizovat vazby mezi samostatnými procesy, u kterých je definována závislost konkrétního kroku v rámci dalšího procesu. K tomu, aby bylo možné používat atributy k dohledávání vazeb, musí existovat jednotný slovník/registr těchto atributů. Tento slovník atributů bude spravován v podobě registru ve standardní aplikaci IS „Centrální správa číselníků (CSČ)“.

Registrace aplikace. Každá aplikace, která bude do AST zapisovat, musí být v AST registrována se svým jednoznačným identifikátorem. Registrace se provádí voláním synchronní služby, poskytované IPF. Tato služba se bude volat v rámci deploymentu (instalačního skriptu) dané aplikace.

Registrace událostí. Aplikace sama musí zaregistrovat všechny typy událostí, se kterými bude pracovat. Tento seznam může aplikace postupně rozšiřovat, ale nemůže měnit již registrované typy. Aplikace nemůže zapsat typ události, který nebyl registrován. Každá událost je součástí právě jednoho procesu/úlohy.Události jsou do AST registrovány pomocí dedikované synchronní služby IPF. Součástí volání služby je ID aplikace a XML struktura s událostmi k registraci.

1.11.1.1 Pravidla pro aplikace využívající služeb AST

Aplikace využívající AST musí splňovat následující pravidla:

- Pokud bude aplikace využívat služeb AST, musí se nejprve u AST zaregistrovat. Tato registrace se provádí ručně spouštěným skriptem, ve chvíli deploymentu dané aplikace a její součástí je předání jednoznačného identifikátoru aplikace a případně parametry přístup k datům spojeným s aplikací.
- Dalším krokem, který již provádí sama aplikace, je povinná registrace aktuálního seznamu událostí. Spojením identifikátoru zdroje události (ID aplikace) a identifikátoru události vznikne jednoznačná identifikace typu události v rámci IS VZP ČR.
- Aplikace bude pro zápis události do AST využívat k tomu určenou synchronní službu „Zápis události do AST“. V rámci volání této služby musí být dodány všechny povinné parametry (viz zápis do AST).
- Pokud bude aplikace do AST zapisovat události, musí AST zároveň zprostředkovat přístup k datům, kterých se daný záznam týkal, případně zprostředkovat odpověď, že daná data již nejsou k dispozici. Aplikace tedy musí poskytovat jednu z následujících služeb, případně jejich kombinaci:
- Na základě předaných parametrů zobrazit uživateli formulář s poptávanými daty. Tyto parametry budou předány v příkazové řádce při spouštění aplikace. Tento způsob prezentace dat nepodporuje možnost ověření dat.

- Na základě předaných parametrů předat zpět poptávaná data ve formátu XML. AST musí mít k dispozici příslušnou šablonu pro zobrazení. Tato šablona je předávána v rámci registračního procesu. V rámci tohoto způsobu prezentace dat je možné v rámci prezentace dat ověřit jejich platnost.
- V případě, že nebude aplikace poskytovat ani jednu z výše uvedených služeb, pak může ZZAS zobrazit pouze záznam, bez vazby na konkrétní data události.
- Pokud bude aplikace zapisovat události, které budou součástí obchodních procesů, pak musí podporovat tzv. předávání identifikace obchodního procesu. Tato identifikace musí být obsažena v parametrech volání služby a zároveň v návratových parametrech. Aplikace musí zajistit, že si identifikaci procesu podrží v rámci svého běhu. Tuto identifikaci použije v případě zápisu do auditní stopy.

Po podpisu smlouvy s VZP ČR dostane dodavatel dokument „Integrace aplikace s AST“, který je nedílnou součástí těchto standardů.

2. Povinnosti dodavatele

V této kapitole jsou uvedeny základní povinnosti dodavatele při dodávkách komponent informačního systému do VZP ČR.

Přílohy uváděné v tomto dokumentu budou příslušnému dodavateli předány při podpisu smlouvy s VZP ČR.

2.1 Provozní dokumentace

Povinností dodavatele komponenty informačního systému VZP ČR je zpracování dokumentace popisující funkcionalitu dodané komponenty v minimálním členění:

- Popis navrženého řešení (analytický, prováděcí projekt)
- Instalační návod
- Provozní příručka
- Uživatelská příručka
- Administrátorská příručka
- Databázový model
- Zpracování dokumentace popisující služby poskytované komponentou ostatním komponentám informačního systémů
- Zdrojové kódy předaných programových modulů

2.1.1 Provozní příručka

Hlavní cíl dokumentu:

Provozní příručka je určena pro provozní útvary systému. Cílem provozní příručky je poskytnout nejen technické informace o podporovaném prostředí, popisu detailních nastavení daného řešení, popis souvislostí s okolním prostředím, popis logiky řešení, ale i pravidelných i nepravidelných činností, definování zodpovědností a návazností na procesy, definice kvality služby, monitoringu, reportingu, governance.

Míra detailu:

Dokumentace musí dávat ucelené přehled o daném řešení systému/služby. Předpokládá se hlubší znalost IT u budoucích uživatelů – ta však může být specificky zaměřená.

Příklad nebo typický obsah:

Osnova provozní dokumentace může vypadat např. následovně:

- Úvod (stručný popis, seznam zkratek)
- Popis aplikace (business pohled, kontext zasazení, popis komponent, adresářové struktury, databázových instancí, procesů, vstupů/výstupů, logů, přístupů…)
- Způsob integrace s okolím
- Popis aplikační logiky (logické komponenty, toky informací, chybové stavy)
- Popis technologie a infrastruktury (HW, disková pole, síťová infrastruktura, OS, servery, clustery, DB, aplikace, monitoring, dohled, zabezpečení…)

- Administrativní nástroje (detaily za jednotlivé komponenty)
- Diagnostika
- Pravidelná údržba a aktivity
- Upgrade a nasazování změn
- Řešení chyb a problémů (včetně typických chyb a způsobu řešení)
- Zálohování a obnovení
- Doporučení a omezení monitorování
- SLA
- Součinnost interních a externích dodavatelů (může být doplněno RACI tabulkou)
- Servisní okno
- Popis instalace a konfiguračních souborů
- Přílohy

Praktické poznámky:

Provozní příručku je potřeba udržovat aktuální během celého životního cyklu systému/služby. Obsah se může dynamicky měnit na základě změnových řízení, změnách dodavatelů, upgrade systému, instalování oprav, změně organizační struktury a ostatních změn okolního prostředí.

2.1.2 Administrátorská příručka

Hlavní cíl dokumentu:

Cílem je zdokumentovat postupy administrace a instalace systému/služby. Může jít o dokumentaci šitou na míru danému zákazníkovi i dokumentaci na typizovaná řešení.

Míra detailu:

Tato dokumentace popisuje hlavní administrátorské úkony potřebné pro provoz technologické části řešení. V podstatě jde o obdobu provozní příručky, ale pro technologie. Některé technologie mohou být standardizovány a popis jejich administrace bývá definován odkazem na patřičnou dokumentaci nebo zvyklosti.

Příklad nebo typický obsah:

Administrátorská příručka popisující administraci následujících oblastí:

- OS
- DB
- HW
- konfig.sítí
- apod.

Praktické poznámky:

Administrátorské příručky je potřeba udržovat aktuální. V praxi dochází nejčastěji k následujícím změnám:

- změna vlivem nasazení aplikace/služby (odkaz na existující standard, jeho úprava nebo rozšíření),

- změna vlivem nasazení aplikace/služby (nový individuální dokument pro tuto službu/aplikaci),
- změna vyvolaná změnovým řízením aplikace/služby (aktualizace dokumentace),
- změna vyvolaná změnovým řízením okolních technologií (změna standardu).

Rozsah administrátorské příručky je vymezen dokumentem Osnova administrátorské příručky, který dodavatel komponenty IS obdrží při podpisu smlouvy s VZP ČR.

2.1.3 Uživatelská příručka

Hlavní cíl dokumentu:

Cílem je ukázat koncovým uživatelům a pracovníkům podpory uživatelů způsob využití systému/služby. Prakticky jde o popsání způsobu, jak jednoduše dosáhnout původních cílů business zadání bez znalosti technických detailů řešení.

Míra detailu:

Dokumentace pro koncové uživatele má základní způsob práce s aplikací/službou např. formou nasnímaných obrazovek, instruktážních videí, interaktivních průvodců, atp. Dokumentace pro podporu uživatelů bývá obsáhlejší, často je budována znalostní databáze i v průběhu samotného provozu (typické dotazy uživatelů, wizardy, atp.).

Opět záleží případ od případu a distribuce znalostí v rámci jednotlivých vrstev. Při specifikaci specializací v dělbě práce používáme „klasickou pyramidu“:
1. Klíčoví zaměstnanci s detailní a technickou znalostí (relativně malý okruh lidí, v některých případech subdodavatelé)
2. Podpůrné vrstvy zaměstnanců s dílčí technickou znalostí nebo rozsáhlou dokumentací nebo subdodavatelé
3. Masa řadových zaměstnanců – flexibilní a operativní přístup, „unifikované“ kategorie pozic s poměrně jasně definovanými postupy.

V praxi může být tedy výhodnější „minimální“ znalost nutné funkcionality bez technických detailů (jak z pohledu uživatele, tak náročnosti správy dokumentace, klasifikace důvěrnosti informací, atd.). Reálně tedy stačí, když bude mít pracovnice na pobočce zdokumentován sub-proces vystavení příjmového/výdajového dokladu, případné náhradní řešení a jasně definované vstupně/výstupní body, ale již nemusí znát logiku cestování informací po systémech, detailní vazby na jiné systémy, apod.

Příklad nebo typický obsah:

Návod na používání aplikace, procesní postupy…

Praktické poznámky:

Provozní příručka pro koncové uživatele může být členěna tematicky (typické činnosti pro specifický profil uživatelů) nebo podle logického uspořádaní funkcionalit v daném systému/službě.

V některých případech nemusí uživatelská příručka prakticky existovat (například pro evidenci příchodů/odchodů zaměstnanců stačí zaměstnanci identifikační karta a jednotný eskalační bod pro případ technických problémů).

2.2 Tabulky předání komponent IS do provozu

Při předávání komponenty vytvořené dodavatelem do provozu pracovníkům informačního systému VZP ČR je povinností dodavatele spolupodílet se na vyplnění tabulek uvedených v samostatném dokumentu „Tabulky předání komponenty IS do provozu“, který obdrží dodavatel při podpisu

smlouvy.. Tabulky vyplňuje vedoucí projektu VZP ČR ve spolupráci s dodavatelem příslušné komponenty IS..

2.3 Popis dodané komponenty pro Enterprise Architecture

Architektura dodané komponenty informačního systému bude popsána dle konvencí jazyka Archimate. Bude obsahovat business, aplikační i technologickou architekturu. Architektura může být popsána v architektonickém nástroji, který je schopen předat navrhovanou architekturu ve formátu XMI. Popis architektury bude proveden v souladu s dokumentem „Metodika popisu a realizace architektury IS“. Dokument obdrží dodavatel při podpisu smlouvy.

2.4 Implementace služeb a jejich evidence

Pokud dodaná komponenta informačního systému bude obsahovat služby, které je možné využívat jinými komponentami informačního systému (integrační služby), je dodavatel povinen před implementací těchto služeb na IPF tyto služby popsat (včetně WSDL a vazeb) v aplikaci Evidence služeb. Povinností dodavatele je dodat komplexní popis služby XSD včetně AQ služeb požadavek/odpověď a to i položek DataC a DataB. Přístup do aplikace Evidence služeb získá dodavatel při podpisu smlouvy. Doporučuje se provádět popis v Evidenci služeb již v průběhu jejich vývoje s uváděním verzí služeb.

2.5 Archivace

Dodavatel komponenty informačního systému navrhne způsob archivace dat uložených v dodané komponentě v souladu s platnými právními předpisy a Archivačním řádem VZP ČR, který mu pro tento účel bude k dispozici. Návrh bude obsahovat archivaci dat v databázích na filesystému i papírových dokumentů. Při návrhu dodavatel přednostně využije systémy pro správu dokumentů využívané ve VZP ČR: dokument management systém, elektronické spisová služba a digitalizace.

2.6 Disaster recovery plán

Dodavatel komponenty informačního systému navrhne disaster recovery plan pro obnovu dodané komponenty při havárii informačního systému. Disaster recovery plán bude v souladu s plánem obnovy informačního systému VZP ČR.

2.7 Školení

Dodavatel zpracuje školení k dodané komponentě informačního systému v podobě Elearningového kurzu. Kurz bude dodán v jedné z následujících norem: AICC, SCORM 1.2 nebo LRN společnosti Microsoft.

2.8 Komunikace se service deskem VZP

Dodavatel komponenty informačního systému VZP ČR se zavazuje, že při řešení incidentů v jím dodané komponentě bude komunikovat se service deskem VZP ČR dle pravidel uvedených v dokumentu Komunikace se service deskem VZP ČR. Dokument obdrží dodavatel při podpisu smlouvy.

Minimální pravidla pro komunikaci s VZP:

Vzájemná komunikace mezi helpdeskovými pracovišti VZP a externí firmou se uskuteční na bázi nestrukturované komunikace mezi SD operátory na obou stranách.

VZP zasílá externí firmě emaily se servisními požadavky (SP). Externí firma tyto požadavky přijme a vyřeší nebo odmítne. Externí firma zašle informaci o stavu požadavku operátorům SD ve VZP.

Rámcový proces komunikace:

1. Zadání SP ze strany objednatele (VZP) - (zaslání MAILU externí firmě)
2. Potvrzení přijetí nového požadavku externí firmou – (zaslání MAILU do VZP)
3. Odmítnutí externí firmou - (MAIL do VZP)
4. Dotaz na stav řešení požadavku - (zaslání MAILU externí firmě), externí firma odpoví nestrukturovaným emailem na adresu odesílatele
5. Vyřešení externí firmou - (MAIL do VZP)

3. Seznam použitých zkratek

Zkratka	Význam
ACL	Access Control List, Seznamy přístupových práv
ActiveX	Microsoft technologie používaná ve webových prezentacích pro snížení nevýhod tenkého klienta
AD	Active Directory, Microsoft adresářová služba pro uložení identit
AIIM	Technologie, nástroje a metody sloužící k zachycení, správě, uložení, zabezpečení a dodání obsahu napříč organizací
AQ	Advanced queueing, Oracle technologie implementující a rozšiřující JMS
AS	Aplikační server
ASM	Archive and Storage Management
AST	Auditní stopa
CA	Certifikační autorita
CAC	Call Admission Control, komponenta řídící platformy Call manageru
CPU	Central processing unit, ústřední výkonná jednotka počítače, procesor
CSC	Centrální správa číselníků
DB	Databáze
DHCP	Dynamic Host Configuration Protocol, aplikační protokol, používá se pro automatické přidělování IP adres koncovým stanicím v síti
DMS	Document Management Systém, Systém pro správu dokumentů
DMZ	Demilitarizovaná zóna
DNS	Domain Name System, hierarchický systém doménových jmen
ebXML	Standard pro komunikaci mezi systémy, vytvořený firmou SUN
EDI	Standard pro komunikaci mezi systémy
EDI, EDIFACT EDIINT	Electronic Data Interchange, výměna strukturovaných zpráv mezi počítači
FTP	File Transfer Protocol, komunikační protokol, je určen pro přenos souborů mezi počítači
HA	High Availability, Vysoká dostupnost
HB	Heart Beat – mechanismus zajištění vysoké dostupnosti, kdy mezi dvěma a více komponentami probíhá kontrola jejich správného fungování.
http	Hyper Text Transfer Protocol, internetový protokol
iAS	Aplikační server firmy Oracle
ICT	Informační a komunikační technologie
IDM	Identity management
IPF	Integrační platforma
ISP	Poskytovatel internetového připojení
JDBC	Spojení z aplikace do databáze využívané jazykem Java
JMS	Java Message Service, JMS představuje API pro vytváření, čtení, posílání či obdržení zpráv. API je schopné poskytnout napojení na již existující MOM systémy (Messaging Oriented Middleware).
JPP	Jednotná přihlašovací plocha
JTS	Jednotná telefonní síť
JVM	Java virtual machine

OV	Open View
QoS	Quality of Service (QoS).Řízení kvality služby. V projektu myšleno, rozdělení aplikací dle důležitosti a její adekvátní nastavení na WAN.
RMI	Remote Method Invocation, umožňuje objektu z jednoho Javového Virtualního Stroje (JVM) vyvolávat metody na jiném objektu, který se může nacházet v jiném JVM
RPC	Remote procedure call je systém pro vzdálené volání procedur. Jedná se o silně typový způsob volání služeb bez možnosti přidávat parametry bez změny klienta.
RTO	Return to operate, návrat k funkčnosti
SAN	Storage Area Network, způsob jak uchovávat data ve velkých počítačových sítích
SI	Systémová integrace
SOA	„Service Oriented Architecture" – architektura orientovaná na služby. Jedná se o koncept architektury v IT, kde celý informační systém je složen z komponent, které nejlépe umí vykonávat jistou činnost – službu, a tu nabízí svému okolí k použití. Jedná se o moderní architektonický styl. IS vybudovaný tímto konceptem poskytuje vysokou flexibilitu.
SOAP	„Simple Object Access Protocol" – Standardní protokol pro komunikaci mezi systémy a aplikacemi. Jeden ze základních kamenů webových služeb. Někdy interpretována jako „Service Oriented Architecture Protocol".
SSH	Secure Shell, protokol, který umožňuje bezpečnou komunikaci mezi dvěma počítači
TS	Tiskový subsystém
UDDI	Universal Description, Discovery and Integration. Koncept, který se dá přirovnat ke zlatým stránkám pro webové služby
VLAN	Virtuální LAN
VM	Virtual machine, virtuální stroj
WAN	Rozlehlá počítačová síť (Wide Area Network - WAN). Počítače rozlehlé sítě jsou umístěny ve více městech, dokonce i ve více státech či kontinentech
WSDL	Web Services Description Language, přesný popis rozhraní webové služby dostupné přes SOAP
XML	Standard pro formát dat vytvořený sdružením OASIS a přijatý IT firmami.
XMI	XML Metadata Interchange – výměna metadatových informací prostřednictvím XML
ZIS	Základní informační systém VZP ČR
ZZ	Zdravotnické zařízení
ZZP	Zaměstnanecká zdravotní pojišťovna