

# Standardy IS VZP – NIS

## **UPOZORNĚNÍ:**

Tento dokument je zpracován Všeobecnou zdravotní pojišťovnou České republiky (dále též jen „VZP ČR“ nebo „VZP“). Všeobecná zdravotní pojišťovna České republiky jej uveřejňuje v rámci zadávací dokumentace jí zadávaných veřejných zakázek. Tento dokument umožňuje utvořit si představu o standardech informační architektury ICT VZP ČR. Účelem jeho uveřejnění je poskytnout informace nezbytné pro integraci dodávané komponenty se stávajícím informačním systémem v souladu se Standardy ICT- VZP- NIS.

Uveřejněním tohoto dokumentu není dotčena právní odpovědnost spojená s jeho zneužitím.

V tomto dokumentu bylo použito názvů subjektů a názvů produktů, které mohou být chráněny příslušnými právními předpisy.

**Otevřením tohoto dokumentu berete výše uvedené skutečnosti na vědomí.**

## Verze dokumentu

Verze	Datum	Autor	Popis
1.06	11. 10. 2017	ÚICT VZP ČR	
1.07	23. 02. 2018	██████████	Úprava 3. kapitoly
1.08	7. 9. 2018	██████████	Revize integračních částí - pro účely CIS
1.09	26. 2. 2019	██████████	Revize kapitoly Bezpečnostní standardy
1.10	11. 3. 2019	██████████	Úpravy v dokumentu, upřesnění logování
1.10.1	23. 5. 2019	██████████	Sloučeny změny s revizemi od OTP
1.10.2	12.6.2019	██████████	Úprava formátu
1.11	30.7.2019	██████████	Další revize k zapracování změn
1.11.1	18.10.2019	██████████	Doplněna autentizace a autorizace
1.11.2	8.11.2019	██████████	Finálizace změn v kapitolách kde je garantem OIKB

## Obsah

1	Úvod .....	8
2	Architektonické a QA standardy.....	9
2.1	Aplikační – obecné standardy .....	9
2.1.1	Třídy Aplikací .....	9
2.2	Integrační a komunikační standard .....	9
2.2.1	Integrace se stávajícím IS .....	10
2.3	Vývojové standardy .....	10
2.3.1	Použité vývojové nástroje pro interní vývoj aplikací:.....	10
2.3.2	Vývojová a testovací prostředí .....	10
2.4	Testovací standardy.....	11
2.5	Dokumentační standard .....	12
3	Infrastrukturní standardy .....	18
3.1	Obecné zásady.....	18
3.2	HW .....	18
3.2.1	On Premise Serverová infrastruktura.....	18
3.3	Sítě.....	19
3.3.1	VLAN .....	19
3.3.2	QoS (QUALITY OF SERVICE).....	19
3.3.3	Datová centra .....	20
3.3.4	Perimetr.....	21
3.3.5	Síťové služby .....	22
3.4	OS .....	22
3.4.1	OS pro aplikace třídy A .....	22
3.4.2	OS pro aplikace třídy B .....	22
3.4.3	Prostředí pro virtualizaci .....	22
3.4.4	Požadavky na linuxové účty.....	22
3.5	Middleware .....	23
3.5.1	Aplikační servery.....	23
3.5.2	Webové servery.....	23
3.6	Virtualizovaná infrastruktura pro hostování aplikací .....	23

3.7	Deployment aplikací provozovaných on-Premise do prostředí v DC VZP .....	24
3.8	Datové a databázové služby .....	25
3.8.1	Databázové technologie .....	25
3.8.2	Datové a databázové standardy .....	25
4	Bezpečnostní standardy .....	27
4.1	Dodržování legislativních požadavků .....	27
4.1.1	Autorský zákon .....	27
4.1.2	ZOKB .....	27
4.1.3	GDPR .....	27
4.2	Dodržování obecných standardů a doporučení .....	27
4.3	Minimum běžících a instalovaných služeb .....	28
4.4	Nevyhovující služby nebo protokoly .....	28
4.5	Synchronizace času .....	28
4.6	Kryptografie .....	28
4.6.1	Požadavky na kryptografické algoritmy .....	28
4.6.2	Požadavky na ochranu privátního klíče .....	28
4.6.3	Požadavky na CA / PKI .....	28
4.7	Komunikace s veřejnou sítí .....	29
4.7.1	Systémy, nebo aplikace, které publikují služby do veřejné sítě (inbound) .....	29
4.7.2	Komunikace do veřejné sítě (outbound) .....	29
4.7.3	SMTP komunikace s veřejnou sítí .....	29
4.8	Řízení přístupu .....	29
4.8.1	Autentizace a autorizace při přístupu k systémům, nebo aplikacím VZP ČR z interní sítě VZP ČR	29
4.8.2	Autentizace a autorizace při přístupu k systémům, nebo aplikacím VZP ČR z veřejné sítě	30
4.8.3	viz. 4.8.1.1 Propagace identity uživatele ke koncovým službám .....	31
4.8.4	Ochrana hesel a politika hesel .....	31
4.8.5	Mechanismus obrany proti hádání přístupu do systému .....	31
4.8.6	Omezení přístupů ke službám ve vnitřní síti VZP ČR .....	32
4.8.7	Zobrazení varovného hlášení .....	32
4.9	Ochrana informačních aktiv .....	32
4.9.1	Klasifikační schéma informačních aktiv .....	32
4.9.2	Data v klidu (Data at Rest) .....	33

4.9.3	Data v pohybu (Data in Transfer) .....	33
4.9.4	Data při zpracování použití (Data in Use) .....	33
4.9.5	Antimalware ochrana .....	33
4.9.6	Plán obnovy (Disaster Recovery) .....	33
4.10	Bezpečnostní testy .....	33
4.10.1	Systémy, nebo aplikace, které nepublikují služby do veřejné sítě .....	33
4.10.2	Systémy, nebo aplikace, které publikují služby do veřejné sítě .....	34
5	Logování .....	35
5.1	Požadavky .....	36
5.1.1	Formát a encoding logu .....	36
5.1.2	JSON - doporučené pojmenování klíčů a identifikace datové struktury .....	36
5.1.3	Obecně platné zásady pro logování .....	36
5.1.4	Technické zajištění logování .....	36
5.1.5	Retence logů .....	37
5.1.6	Dokumentace .....	37
5.2	Základní úroveň logování z pohledu bezpečnosti .....	37
5.2.1	Logování procesu autentizace .....	37
5.2.2	Činnosti provedené administrátorem .....	38
5.2.3	Změny přístupových oprávnění a změny údajů, které slouží k přihlášení .....	38
5.2.4	Neprovedení činnosti v důsledku nedostatku přístupových oprávnění .....	38
5.2.5	Přístupy k záznamům o činnostech .....	38
5.2.6	Operace se soubory .....	39
5.2.7	Vybrané JSON klíče pro záznam události .....	39
5.3	Logování transakcí při zpracování osobních a zvláštní kategorie osobních údajů .....	40
5.3.1	Vybrané JSON klíče pro záznam události .....	40
5.3.2	Příklad logu činnosti nahlížení .....	41
5.3.3	Příklad logu činnosti změna .....	41
5.4	Základní požadavky na logování komunikace a business logiky- Transakční log .....	41
5.4.1	Informační obsah události zaznamenávané v transakčním logu .....	41
5.4.2	Vybrané JSON klíče pro záznam události .....	42
5.4.3	Příklad transakčního logu .....	43
5.5	Provozní log .....	43
5.5.1	Základní požadavky na provozní logování – Provozní log .....	43
5.5.2	Formát logovacího souboru provozního logu .....	43

---

6	Provozní standardy.....	44
6.1	Monitoring.....	44
6.1.1	Rozsah monitoringu a používané nástroje .....	44
6.1.2	Používané dohledové nástroje pro On premise řešení .....	44
6.1.3	Požadavky na procesy z hlediska monitoringu.....	45
6.1.4	Požadavky na návrh monitoringu.....	45
6.1.5	Požadavky na rozhraní pro monitoring .....	45
6.2	Zálohování a archivace .....	46
6.2.1	Zálohovací systém .....	46
6.2.2	Požadavky na aplikační celky z pohledu jejich zálohování: .....	46
6.3	Definice provozních parametrů služby/aplikace (SLA).....	47
6.4	Podmínky převzetí do rutinního prostředí a aplikační podpory.....	47
6.5	Vazba na ITIL procesy .....	48
6.5.1	Definování veškerých eskalačních procedur u aplikace - správa HelpDesku/ServiceDesku 48	
6.5.2	Zavedení aplikace do incident managementu.....	48
6.5.3	Zavedení aplikace pod standardní řízení změn - change management .....	48
6.5.4	Zavedení aplikace do release plánů - release management .....	48
7	Seznam příloh.....	49
8	Výjimky ze standardu .....	49
8.1	Integrace se stávajícím IS .....	49

## 1 Úvod

### STANDARDY IS VZP - NIS

- **Představují** - soubor pravidel určených pro vytváření, rozvoj a využívání IS VZP ČR.
- **Obsahují** - charakteristiky, metody, postupy a podmínky, které musí IT komponenty naplnit či dodržet, zejména pokud jde o bezpečnost a integrovatelnost s jinými informačními komponenty a systémy.
- **Jsou určeny** - pro všechny dodavatele řešení/služeb/komponent jako pravidla dodávek IS/IT a k vývoji aplikací a jejich releasů.
- **Všichni dodavatelé komponent IS do VZP** jsou povinni po akceptaci standardu ho respektovat ve znění, v jakém ho přijali.
- **Od standardu se lze odchýlit pouze na základě výjimky.** Výjimky zpracovává oddělení architektury, posuzuje je vlastník příslušného standardu VZP ČR, který je uveden u příslušné kapitoly. Schválení výjimky na základě posouzení schvaluje náměstek pro IT VZP ČR.
- **Při vydání nové verze standardu dodavatelé jsou vyzváni k přistoupení k nové verzi standardu** pro další dodávky. Pokud není poskytované řešení kompatibilní s novou verzí standardu, požádají VZP o výjimku.
- **Jejich účelem je** nasazení a následné provozování řešení/komponent v rutinním prostředí VZP s požadovanými garancemi, s požadovanými provozními parametry, s požadovanou odbornou aplikační a provozní podporou provozu IT při optimalizaci řešení IT.



## 2 Architektonické a QA standardy

### 2.1 Aplikační – obecné standardy

Vlastník kapitoly: oddělení Architektury

- Aplikace má být navržena jako vícevrstvá, tyto vrstvy musí být jasně definovány a jejich rozdělení striktně dodržováno. Obvykle se aplikace skládá z těchto vrstev:
  - Webová / presentační vrstva - uživatelské rozhraní -
    - Aplikační vrstva
    - Databázová vrstva
- Aplikační řešení musí být složeno z jednotlivých komponent s definovanými a oddělenými funkčnostmi, včetně rozhraní (API) jež funkčnosti zpřístupňují, bez duplicit a distribuované funkční logiky.
- Aplikační řešení by má být tvořeno ze sady relativně nezávislých modulů, aby změna v jednom z nich neznamenal (podstatný) zásah do zbývajících modulů. Moduly jsou v ideálním případě samostatně (autonomně) nasaditelné (upgradovatelné).
- Aplikace musí mít deklarovatelným způsobem ošetřeny architektonické aspekty: škálovatelnost a flexibilita a to zejména **umožněním horizontálního škálování**;
- Součástí návrhu aplikačního řešení a realizace je požadován kapacitní a výkonnostní sizing systému s výhledem na 5 let.
- Aplikace musí splňovat požadavky na zálohování a obnovu popsané níže.
- Aplikace/ Řešení musí podporovat mechanismy pro archivaci dat a jejich případnou obnovu
- Aplikace musí respektovat již v návrhu požadavky na bezpečnost a soulad (compliance), viz kapitola [4 Bezpečnostní standardy](#).

#### 2.1.1 Třídy Aplikací

Aplikace a aplikační řešení jsou z pohledu kritičnosti provozu kategorizovány do následujících tříd:

##### Třída A

Jedná se o business kritické a technologické aplikace, jejichž výpadek má zásadní charakter. Garantovaná dostupnost těchto aplikací je 99,4% v požadovaném režimu provozu (standardně 7x24 nebo 5x16).

##### Třída B

Jedná se o aplikace, které nepatří mezi business kritické a mají nižší nároky na zajištění jejich dostupnosti. Požadovaná dostupnost je 98,1% v požadovaném režimu provozu 5x8 nebo 5x16.

### 2.2 Integrační a komunikační standard

Vlastník kapitoly: oddělení architektury

- Komunikace mezi aplikacemi a integrace musí respektovat následující pravidla: Komunikace je v zásadě asynchronní (synchronní komunikace pouze ve výjimečných odůvodněných případech);
- Komunikace musí být odolná proti výpadku jedné strany
- Komunikace maximálně omezuje využívání mechanismů:

- distribuovaná transakce
- dvoufázové potvrzení transakce (two-phase- commit);
- Komunikace dodržuje zásady idempotence<sup>1</sup>, tam kde je to možné.
- Veškeré vazby systému na ostatní systémy jsou formou volné vazby (loosely coupled), doporučeným mechanismem aplikační komunikace je využití messagingu, případně synchronních REST služeb.
- Pro přenos souborů (MFT) a datových objektů větších než 2MB se využije souborový přenos.
- Pro datovou integraci se využijí nástroje ETL, případně nástroje pro Event Streaming .
- Pro implementaci nových veřejných rozhraní (API) upřednostňovat REST v3.0 (HATEOAS<sup>2</sup>).
- Spojení mezi stávajícími systémy VZP provádět přes integrační platformu (ESB).
- V maximální možné míře je nutno využívat stávajících již implementovaných aplikačních služeb nabízených v infrastruktuře VZP.
- Není povoleno využívat integraci aplikací na úrovni databází (link mezi databázemi);
- V rámci aplikace musí být zajištěna kontrola vstupů a výstupů (formátů dat), automatické přenosy obsahují kontrolní součty a zabezpečení, manuální přenosy jsou nepřístupné;
- Proces zpracování dávek (batch, ETL, MFT) musí obsahovat dílčí kontrolní body a kontrolní mechanismy.

### 2.2.1 Integrace se stávajícím IS

Ke dni vzniku tohoto standardu VZP provozuje stávající IS řízený historickou verzí standardu. Způsob integrace s tímto IS je proto prováděn odchylně od tohoto standardu. Tato výjimka je zachycena v kapitole [8.1 Integrace se stávajícím IS](#).

## 2.3 Vývojové standardy

Vlastník kapitoly: OAVRZ

### 2.3.1 Použité vývojové nástroje pro interní vývoj aplikací:

- Funkční analýza a design: Enterprise Architekt, MS Word, Balsamiq Mockups
- Technický design-aplikační logika: Visual Studio 2015/2017
- Technický design-datový design: Visual Studio 2017 Database Tools (MSSQL / Oracle)
- Technický design-integrační procesy: OpenAPI / AutoRest (Enterprise Architect, MS Word)
- Správa verzí: Visual Studio Team Services (Git), Gitlab
- Vývoj aplikací: Visual Studio 2015/2017, Visual Studio Code, SQL Server Management Studio, XCode / Android Studio, SOAP UI, Postman
- Migrace a deployment aplikací: Azure DevOps

### 2.3.2 Vývojová a testovací prostředí

Vyvíjená aplikace musí mít definována minimálně prostředí:

- Samostatné prostředí určené konkrétnímu vývojáři
- prostředí určené pro ověřovací testy v rámci vývoje, preferované je, aby nasazování na tato prostředí probíhá automaticky
- prostředí určené pro akceptační test garanty aplikací, nasazení na tato prostředí je řízeno pověřeným vedoucím testování (určeným vedoucím testovacího oddělení)
- Verzování vývoje

<sup>1</sup> (<https://en.wikipedia.org/wiki/Idempotence>)

<sup>2</sup> <http://restcookbook.com/Basics/hateoas/>

- Vytvářená aplikace bude verzována pomocí tzv. sémantického verzování<sup>3</sup>

## 2.4 Testovací standardy

Vlastník kapitoly: OTP Oddělení testování

- Součástí každého řešení/ komponenty je testovací dokumentace (viz dokumentační standard)
- Součástí každého řešení jsou provedené testy dle dokumentace příslušné aplikační komponenty
- Testování se provádí na anonymizovaných/pseudonymizovaných datech (součástí řešení jsou nástroje pro anonymizaci/pseudonymizaci testovacích dat)
- Musí být zajištěna jednotná anonymizace/pseudonymizace dat integrovaných aplikací v rámci testovacího prostředí

### Typy požadovaných testů pro předání do provozu IT

<b>Vývojové testování</b>			
<b>Název testu</b>	<b>Provádí</b>	<b>Vstupy</b>	<b>Výstupy</b>
unit test	vývojoví pracovníci a testeři dodavatele komponenty	Návrh architektury testování	Odsouhlasené testovací scénáře a testovací případy Odsouhlasená specifikace testovacích dat Záznam výsledků testů Protokol o provedení vývojových testů
assembly test		Plán testů	
funkční test		Testovací scénáře a testovací případy	
test výjimek		Specifikace testovacích dat Testovací data	
<b>Systémové testování</b>			
<b>Název testu</b>	<b>Provádí</b>	<b>Vstupy</b>	<b>Výstupy</b>
smoke test	testeři dodavatele komponenty společně s testery VZP ČR <sup>4</sup>	Testovací scénáře a testovací případy	Odsouhlasené testovací scénáře a testovací případy Odsouhlasená specifikace testovacích dat Záznam o výsledku testů Protokol o provedení systémových testů
funkční test		Specifikace testovacích dat	
test výjimek		Testovací data	
integrační test		Protokol o provedení vývojových testů	
<b>Nefunkční testy</b>			

<sup>3</sup> <https://semver.org/lang/cs/>

<sup>4</sup> Společně s testery VZP znamená poskytnutí přiměřené součinnosti VZP k provedení a přípravě testu tam kde je to věcně nezbytné.

Název testu	Provádí	Vstupy	Výstupy
zátěžový test <sup>5</sup>  stress test	testeři dodavatele komponenty společně s testery VZP ČR	Projektová dokumentace Plán testů Analýza pro výkonnostní test Testovací data Testovací scénáře Protokol o provedení systémových testů	Výsledky výkonnostního testu Zpráva o výkonnostním testu
Backup a recovery test	Administrátoři VZP ČR	Postup zálohy a postup obnovení. Testovací scénáře ověřující základní funkčnosti po záloze a obnovení	Záznam ověření provedení obnovy ze zálohy.
<b>Bezpečnostní testy</b>			
Název testu	Provádí	Vstupy	Výstupy
bezpečnostní test	testeři OBIT VZP ČR	Identifikace komponent k testování (dodavatel a VZP ČR)	Výsledky testu
penetrační test (u Internet facing aplikací / systémů)	penetrační testování zajišťuje nezávislý subjekt (subdodávka), náklady nese dodavatel	Identifikace komponent k testování (dodavatel a VZP ČR), návrh rozsahu penetračního testu (dodavatel, VZP ČR)	Výsledky testu
<b>Akceptační uživatelské testy - strana odběratele (VZP ČR)</b>			
Název testu	Provádí	Vstupy	Výstupy
akceptační uživatelský test	testeři VZP ČR	Protokol o provedení systémových testů Testovací scénáře, testovací případy Data ze systémových testů	Záznam výsledků testu Akceptační protokol za testování

## 2.5 Dokumentační standard

Vlastník kapitoly: OAVRZ

<sup>5</sup> Pro zátěžové testy preferuje VZP ČR nástroj jMeter (<https://jmeter.apache.org/>)

Dokumentace systému se skládá z:

- Celková – úplná dokumentace. Popisuje úplně systém v jeho aktuální podobě.
- Přírůstek dokumentace – dokumentace konkrétní změny provedené oproti celkové dokumentaci.
- Celková dokumentace k dodanému řešení musí být dodavatelem pravidelně aktualizovaná a to při významných změnách / velký release .
- Dokumentace musí být min. 1 x ročně konsolidována, všechny dílčí změny zapracovány do úplné verze a předány VZP.
- Kromě odůvodněných a schválených a smysluplných výjimek (např. zdrojový kód) je dokumentace vedena v nástroji Sparx Enterprise Architect.

Níže uvedený seznam dokumentů je volitelný. Dle předmětu specifikace zakázky na dodávku do IS VZP bude proveden výběr povinně požadovaných dokumentů od dodavatele řešení.

Dokumentační oblast	Podrobnější popis	Dokumenty
Funkční dokumentace	<p>Funkční dokumentace definuje funkčnosti systému a jejich chování v souvislosti s řešením služeb pro podporu business procesu. Představuje detailní popis, jak software funguje, bez vazby na konkrétní technologii či detailní architekturu systému.</p> <p>Zabývá se proto business elementy, jako jsou: business entity, schopnosti, procesy, role, cíle, lokality a taky vnější omezení (např. legislativní) a jiné vlivy, které je třeba při návrhu řešení brát v potaz.</p> <p>Funkční a nefunkční požadavky na řešení jsou definovány v katalogu požadavků.</p> <p>Popis požadavku na změnu definuje klíčové potřeby uživatelů na IS, podporované procesy.</p> <p>Při velkých změnách obsahuje funkční dokumentace i návrh nového</p>	<p>Katalog požadavků na dodané řešení do IS VZP</p> <p>Účastníci řešení</p> <p>Pojmy a artefakty řešení</p> <p>Statický model</p> <p>Doménový model</p> <p>Statický model</p> <p>Logická architektura</p> <p>Konceptuální datový model</p> <p>Procesy podporované dodaným řešením</p> <p>Dynamický model</p> <p>Funkční předpoklady, omezení</p> <p>Katalog služeb komponenty</p> <p>Postup implementace a migrace</p>

	řešení a způsob, jak nového řešení dosáhnout ve vazbě na stávající stav.	
Technická dokumentace	<p>Technická dokumentace obsahuje návrh IT řešení business problémů specifikovaných na úrovni business analýzy a obsažené ve funkční dokumentaci. Navrhuje funkčnost jednotlivých technických komponent IT systémů, místo řešení požadavků v rámci vrstev nebo jiných částí IT architektury.</p> <p>Zpodrobňuje požadavky z funkční dokumentace na implementační úroveň.</p> <p>Obsahuje popis aplikační architektury, front end komponenty, validace, popis business logiky, orchestrace, popis datové vrstvy, deployment, konzumované služby IS, napojení na integrační komponenty...</p> <p>Provádí přiřazení funkčních služeb do IT komponent / domén.</p> <p>Provádí přiřazení business objektů do IT komponent / domén.</p> <p>Při velkých změnách architektury (náhrady komponent) obsahuje návrh nového řešení a způsob, jak nového řešení dosáhnout ve vazbě na stávající stav.</p>	<p>Aplikační architektura</p> <p>Integrační architektura</p> <p>Datová architektura</p> <p>Technologická architektura</p> <p>Technické předpoklady, omezení</p> <p>Postup implementace a migrace</p>
Bezpečnostní dokumentace <sup>6</sup>	Popis integrace do sítě VZP ČR s ohledem na umístění komponent v rámci segmentace komunikační sítě (dle DC zón a zón Perimetru). Popis potřeb a návrh řešení s ohledem na	Síťová bezpečnost

<sup>6</sup> Pokud informace požadované bezpečnostní dokumentací uvedl zpracovatel v rámci jiné dokumentační oblasti, pak je v bezpečnostní dokumentaci řešeno odkazem.

	komunikaci mimo síť VZP ČR. Výčet služeb poskytovaných do veřejné a vnitřní sítě.	
	Popis mechanismu autentizace a autorizace uživatelů. Napojení na centrální autoritu autentizace a autorizace. Napojení na IDM/EIM.	Autentizace a Autorizace uživatelů
	Výčet použitých účtů a rolí (včetně účtů a rolí dodaných s aplikací nebo systémem nebo vytvořených na základě zadání VZP ČR). Identifikace, zda je účet nebo role vytvořena lokálně, nebo převzata z centrální autority, zda se jedná o privilegovaný účet nebo roli, popis využití účtu nebo role. Matice rolí, která identifikuje nežádoucí kombinace systémových rolí (kombinace, které mohou zapříčinit zneužití přidělených oprávnění při kumulaci rolí)	Uživatelské a servisní účty
	Identifikace a popis informačních aktiv se kterými systém nebo aplikace pracuje a klasifikace informačních aktiv. V případě osobních a citlivých údajů popis kategorií subjektů údajů a kategorií osobních údajů, plánované lhůty pro výmaz jednotlivých kategorií údajů, účelu zpracování a právního důvodu zpracování.	Výčet primárních aktiv typu informace
	Při zpracování osobních informací je součástí bezpečnostní dokumentace analýza „Vliv zamýšlených operací zpracování na ochranu osobních údajů“, tedy analýza rizik a dopadů zpracování dat a dokumentů.	Vliv zamýšlených operací zpracování na ochranu osobních údajů
	Popis integračních vazeb (vazby na další komponenty IS VZP ČR nebo státní správy) z pohledu bezpečnosti a to specificky se zaměřením na využitý komunikační framework, popis a klasifikaci přenášených informačních aktiv, mechanismy autentizace, autorizace a auditu, způsobu zabezpečení vč. specifikace použitých šifrovacích mechanismů.	Integrační vazby

	<p>V případě, že systém nebo aplikace využívá v rámci kryptografických opatření privátních klíčů, pak jsou součástí dokumentace informace o uložení a zabezpečení privátních klíčů. Z provozní dokumentace musí být zřejmé, kde a za jakým účelem jsou privátní klíče využity.</p> <p>V případě, že systém, nebo aplikace využívá v rámci kryptografických opatření certifikátů vydaných CA VZP ČR (technologický certifikát), pak je nutné zajistit, aby byl dokumentován postup výměny certifikátu v provozní dokumentaci. Rovněž musí být popsáno, jakým způsobem je procesně zajištěno, že nedojde k přerušení činnosti aplikace nebo systému díky expiraci certifikátu. Z provozní dokumentace musí být zřejmé, kde a za jakým účelem jsou certifikáty využity.</p>	Kryptografická opatření
	Výčet zaznamenávaných bezpečnostních událostí, včetně popisu formátu, místa uložení a retence.	Bezpečnostní logování
	Podrobný plán obnovy systému. V případě, že systém využívá asymetrické kryptografie, pak jsou součástí dokumentace informace o zajištění zálohování a obnovy privátních klíčů.	Plán kontinuity činností
Testovací dokumentace	Dokumentuje průběh testování pro danou komponentu. Rozsah povinné dokumentace se stanoví dle metodiky testování VZP v závislosti na charakteru komponenty, typu vývoje a správy systému, včetně postupů pro obnovu dat, jak z produkčního prostředí, tak mezi testovacími prostředími. Dále bude dokumentace popisovat návrhy řezů dat a možnosti pseudonymizace a anonymizace.	Testovací strategie Testovací plán Test scope - rozsah testů Testovací scénáře Testovací případy Testovací skripty Testovací data Záznam o provedení testu



		<p>Postup na obnovu dat v testovacím prostředí</p> <p>Postup pro vytváření řezů dat a anonymizaci/pseudonymizaci dat</p> <p>Akceptační protokol</p>
Provozní dokumentace	Provozní dokumentace potřebná k provozování a správě dodaného řešení v prostředí VZP.	<p>Zálohování a archivace, odklady dat, obnova dat – provozní příručka</p> <p>Monitoring – provozní příručka</p> <p>Administrátorská příručka</p> <p>Uživatelská příručka</p> <p>Instalační postup</p> <p>Konfigurační příručka</p> <p>Tabulky předávání do provozu IT</p> <p>Migrační dokumentace</p> <p>Licenční politika, certifikáty</p> <p>Řešení typických chyb a problémů</p> <p>Administrační nástroje</p> <p>Pravidelná údržba, profylaxe</p> <p>Popis infrastruktury</p> <p>Datový model</p> <p>Kapacitní nároky – disky, HW</p> <p>Popis síťového řešení</p>
Zdrojové kódy	<p>Obecné požadavky na kód:</p> <ul style="list-style-type: none"> <li>- Snadná udržitelnost</li> <li>- Vnitřní integrita</li> <li>- Efektivita návrhu a zápisu</li> <li>- Snadné další použití</li> </ul> <p>Veškerý konfigurační kód musí být řádně okomentován tak, aby pro každý funkční modul bylo zřejmé:</p> <ul style="list-style-type: none"> <li>- Název modulu</li> <li>- Účel modulu</li> <li>- Původní autor</li> <li>- Provedené změny (datum, autor, účel změny)</li> </ul> <p>Veškeré názvy použité v konfiguračním kódu musí být uvedeny tak, aby byl odborným specialistům zřejmý účel pojmenovaného prvku v daném kontextu.</p>	

	<p>Názvy musí odpovídat jmenné konvenci jednotné pro veškerý konfigurační kód v rámci dodávky. VZP preferuje standardizovanou konvenci CamelCase.</p> <p>Veškerý konfigurační kód musí být navržen v co nejjednodušší struktuře, která je zároveň čitelná a pochopitelná odborným specialistou.</p> <p>Odborným specialistou se myslí pracovník, který může být získán na běžném pracovním trhu a po absolvování běžně dostupného odborného výcviku může pracovat na dalších úpravách a rozvoji dodaného informačního systému.</p>
--	--

## 3 Infrastrukturní standardy

### 3.1 Obecné zásady

Standardem pro provoz aplikací je virtualizovaná infrastruktura. Virtualizace může být realizována formou virtuálních serverů, kontejnery či přímým hostingem funkcí.

Instalace aplikace na bare-metal HW je možná pouze po schválení výjimky ze strany OTP a Oddělení architektury.

Infrastruktura provozovaná formou služby (public cloud) není povolena.

### 3.2 HW

Vlastník kapitoly: OTP OSI

#### 3.2.1 On Premise Serverová infrastruktura

Základem serverové infrastruktury, centralizované a provozované v rámci datových center (DC), jsou servery nebo serverovými systémy založené na architektuře procesoru x86. Serverová infrastruktura je postavena na neproprietárních základech (bez vazby na jediného konkrétního výrobce). Servery jsou certifikovány na operační systémy uvedené v kapitole 3. 3., musí být rozšířitelné, maximálně flexibilní a vysoce dostupné. Jednotlivé servery nebo serverové systémy jsou připojeny do sítě LAN a v případě komunikace s diskovými poli i do sítě SAN a vybaveny kvalitními nástroji pro správu. V případě používání virtualizace uvedené v kapitole 3. 3. je hardware management propojen s virtualizační vrstvou. Servery nebo serverové systémy jsou v provedení rackmount a v datových centrech jsou umístěny v rackových skříních velikosti 42U. Napájení rackových skříní se odvíjí od spotřeby zařízení, která jsou v něm umístěna.

Standardem pro připojení fyzických serverů do sítě LAN v datových centrech je:

- Management console konzole, 1x1GE, access
- Management interface, 2x1GE, acces, active-standby
- Datový interface, 2x10GE, trunk, active LACP

#### On Premise SAN infrastruktura

V jednotlivých datových centrech jsou disková enterprise a midrange pole, která jsou zapojena do SAN infrastruktury pomocí SAN prepínačů. Potřebná kapacita diskových polí je řešena rozšířením těchto polí nikoliv nákupem dalších polí. Do této SAN infrastruktury jsou z důvodu vysoké propustnosti a kvalitního zabezpečení (využití alternativních cest) zapojeny všechny významné servery, zálohovací zařízení (páskové knihovny, B2D zařízení) a zmíněná disková pole. Tato SAN síť využívá u všech významných komponent minimálně 2 FC rozhraní pro zajištění vysoké dostupnosti.

#### 3.2.1.1 Podmínky pro on – premise infrastrukturu podle Třídy Aplikací

##### **Třída A**

Aplikace v této třídě pracují v režimu aktiv/pasiv mezi oběma lokalitami. Jsou provozované na infrastruktuře, která eliminuje dopady výpadků fyzických komponent HW. V případě výpadku celé primární lokality bude aplikace po dobu nutnou k přepnutí do záložní lokality dočasně nedostupná. Přepnutí může být provedeno buď automaticky, nebo poloautomaticky. V záložní lokalitě je připravena infrastruktura primárně využívána pro testovací prostředí, které bude v případě přepnutí produkčních aplikací omezeno, nebo vypnuto. Přepnutí do záložní lokality může mít vliv na výkonnost aplikace. Data jsou zrcadlena do záložní lokality prostřednictvím vhodné technologie.

##### **Třída B**

Aplikace nemusí být provozované na infrastruktuře, která eliminuje dopady výpadků fyzických komponent HW.

V případě nedostupnosti není počítáno s automatickým nebo poloautomatickým převodem do záložní lokality. Data nejsou zrcadlena do záložní lokality.

Veškeré nově implementované nebo upravované aplikace obou tříd musí umožňovat odklad dat a vytváření archivů a to jak z databázových objektů, tak z nedatabázových oblastí (z filesystémů).

### **3.3 Síť**

Vlastník kapitoly: OTP OSS

#### **3.3.1 VLAN**

VLANy jsou implementované v přístupové vrstvě. Uživatelé z různých oddělení, rozdělení do určených VLAN, mohou přistupovat do sítě určenými přístupovými prepínači, které jsou umístěny v různých podsítích. V hraniční, případně distribuční, vrstvě je nakonfigurované směrování těchto podsítí mezi sebou a také případné omezení provozu mezi VLANami pomocí ACL – Access Control List (přístupových listů).

#### **3.3.2 QoS (QUALITY OF SERVICE)**

QoS zajišťuje rovnoměrné vyvažování zátěže sítě s ohledem na druh přenášených dat, spravedlivě rozděluje konektivitu mezi jednotlivé aplikace dle nastavených priorit a zabraňuje přetížení sítě.

Ve VZP ČR jsou použity následující **QoS** třídy, které jsou řazeny dle priority – od nejvyšší priority po nejnižší priority.

- Třída – Network support
- Třída – Real time (VoIP RTP, VoIP Signalizace)
- Třída – 3B: Interaktivní provoz (terminálová třída) – (Aplikace Interaktivní)
- Třída – 3A: Web provoz (webová třída)

- Třída – 3D: Scavenger třída (DoS, P2P, ...) – Služby UDP (Bulk)
- Třída – Zbytková třída – ostatní provoz

### 3.3.3 Datová centra

Fyzická topologie síťové vrstvy v každém z datových center VZP ČR je tvořena dle architektury Spine and Leaf. Logická síťová vrstva je centrálně řízena pomocí clusteru controllerů. Jedná se o aplikačně řízenou infrastrukturu (Application Centric Infrastructure - ACI), která umožňuje integrovat do řízení síťového provozu datového centra vlastní logiku jednotlivých aplikací z pohledu jejich požadavků na síťovou konektivitu, bezpečnost a L4-L7 služby (load balancing, firewalling atd.).

VZP ČR používá technologii Cisco ACI.

#### 3.3.3.1 Architektura datových center

Z pohledu architektury se obě datová centra chovají jako jedno logické datové centrum, dále jen NDC – Nové Datové Centrum. NDC je v prostředí ACI vytvořeno několika tenanty (virtuálními prostředími). Pro zajištění sdílení infrastrukturních a společných služeb je využit tenant common.

Přehled použitých tenantů (prostředí):

- Sdílené služby (common) – služby sítě, AAA, management, dohled, ostatní společné síťové služby, propojení do uživatelské sítě VZP net.
- Administrativní/Management prostředí (ADM) – out-of-band management připojení, management rozhraní
- Produkční prostředí (PRO) – produkční aplikační celky
- Testovací prostředí (TSTxx) – testovací prostředí TST01 – TST12. Každé testovací prostředí je samostatným tenantem, tedy až 12 tenantů.

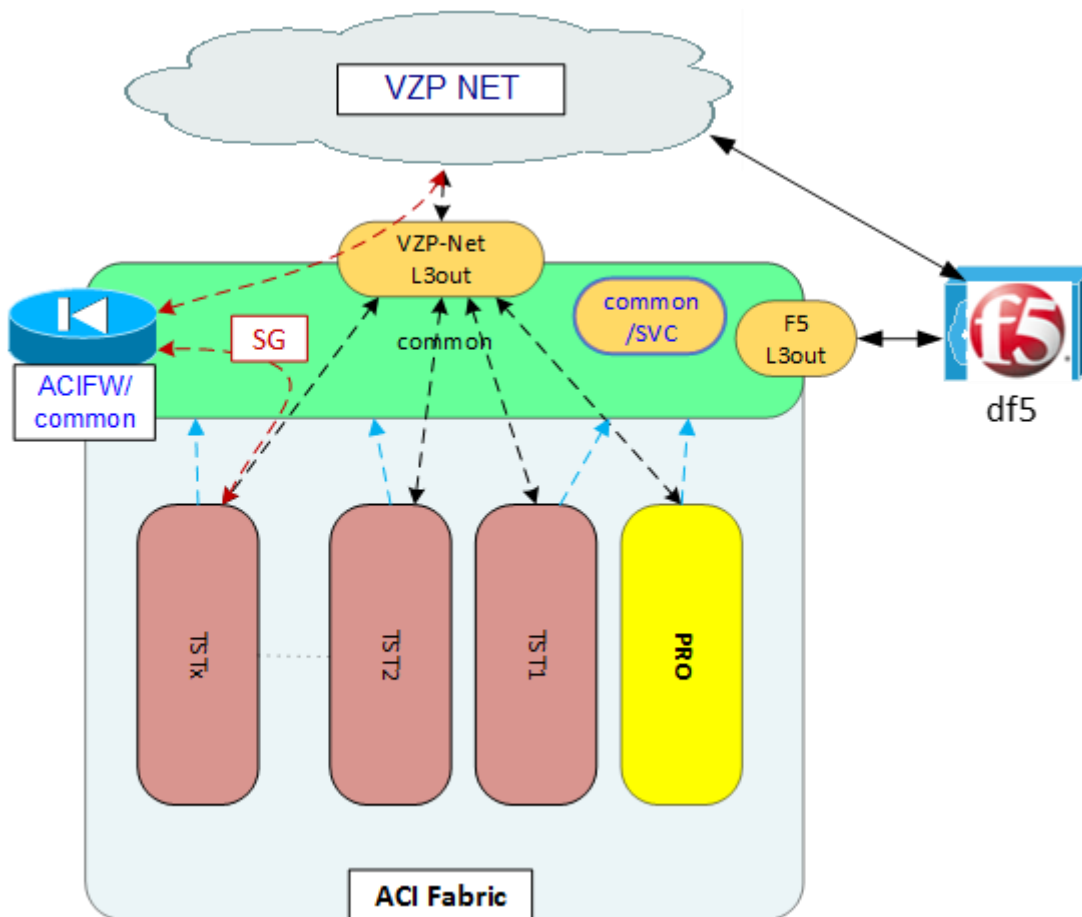
Produkční a testovací prostředí NDC je rozděleno do aplikačních celků. Každý aplikační celek je tvořen samostatným aplikačním profilem. Aplikační celek se typicky skládá z jednotlivých EPG (End Point Group) reprezentujících vrstvu aplikace:

- Webová (Prezentační) vrstva
- Aplikační vrstva (APP EPG)
- Databázová vrstva (DB EPG)
- HeartBeat vrstva
- Aplikační profil (Application Profile) je množina EPG a kontraktů/filtrů, které dohromady tvoří pravidla pro komunikaci v rámci vybrané aplikace.
- EPG je logická skupina serverů/aplikací/koncových zařízení, pro kterou jsou definovány jednotlivé politiky. V rámci EPG je standardně povolena veškerá komunikace. Mezi jednotlivými EPG je standardně veškerá komunikace zakázána a povolená komunikace je stanovena pomocí kontraktů (contracts).
- Kontrakty (contracts) je skupina politik, která definuje potencionální komunikaci mezi jednotlivými EPG. Kontrakt je tvořen filtry (filters), které definují specifické protokoly a porty, které jsou povoleny v komunikaci mezi EPG.

Bezpečnostní oddělení (řízení provozu) na síťové vrstvě je zajištěno následujícími prostředky:

- East-West provoz – komunikace v rámci tenanta uvnitř ACI prostředí – je řízena pomocí standardních contractů mezi jednotlivými EPG.

- East-West provoz – komunikace mezi tenanty uvnitř ACI prostředí –probíhá výjimečně a je řízena pomocí standardních kontraktů mezi jednotlivými EPG nebo ve specifických odůvodněných případech je využít servisní graf obsahující firewall.
- North-South provoz – komunikace ze sítě VZP (administrátoři) do tenantů NDC –probíhá přes L3 out spojení, kde bude vytvořen servisní graf se zařazením firewallu pomocí PBR (Policy Based Redirect).
- North-South provoz – komunikace ze sítě VZP (uživatelé) do tenantů NDC –probíhá přes L3 out spojení přes loadbalancer F5 bez servisního grafu, tj. bez firewallu.



Obrázek: Tenanti a komunikace v ACI a mimo ACI

### 3.3.4 Perimetr

Perimetr je zabezpečená oblast podnikové sítě, která leží mezi internetem a vnitřní sítí VZP ČR. Perimetr je rozdělen pomocí bezpečnostních bran (firewallů) do několika oddělených bezpečnostních zón:

- vnější perimetr – bezpečnostní oddělení externích sítí (Internetu) od sítě VZP
- vnitřní perimetr – bezpečnostní oddělení veřejně vystavených služeb VZP od vnitřní (uživatelské) sítě VZP

Součástí řešení je i VPN přístup do VZP ČR. VPN slouží pro vzdálený přístup zaměstnanců a externích kontraktorů do sítě VZP ČR z Internetu.

### 3.3.5 Síťové služby

Síť VZP ČR poskytuje pro koncová zařízení, aplikace a uživatele následující služby:

- Časová synchronizace (NTP)
- Kvalita služby (QoS)
- DNS, DHCP, IPAM (DDI)
- Loadbalancing

## 3.4 OS

Vlastník kapitoly: OTP OSSM

V době instalace musí mít všechny implementované verze OS zajištěnu podporu ještě minimálně dalších 5 let.

### 3.4.1 OS pro aplikace třídy A

- Red Hat Enterprise Linux, Oracle Linux, CentOS (verze 7 a vyšší)
- MS Windows Server 2016

### 3.4.2 OS pro aplikace třídy B

- Red Hat Enterprise Linux, Oracle Linux, CentOS (verze 7 a vyšší)
- MS Windows Server 2016

### 3.4.3 Prostředí pro virtualizaci

Hostitelský systém je hypervizor nebo operační systém s hypervizorem , který umožní provoz Virtuálních serverů. Podporované platformy jsou a ve VZP mohou být nasazeny technologie, VMWare vSphere 6.5 Enterprise a vyšší, Oracle VM 3.4 a vyšší.

Řízení Virtuálních serverů - správa VMs na VMWare nástrojem VMWare vCenter Server 6.5 Standard a vyšší.

Pro zajištění vysoké dostupnosti aplikací třídy A pro a realizaci DRP plánu slouží technologie VMware DRS a HA cluster, případně VMware SRM.

Pro aplikace třídy A využívající softwarové produkty Oracle bude použita virtualizace Oracle VM.

U aplikací třídy B lze použít i další virtualizační technologií:

- KVM (Kernel-based Virtual Machine)

### 3.4.4 Požadavky na linuxové účty

Uvedené požadavky jsou se zdůrazněním požadavků na aplikace ve vztahu k administraci.

- Na linuxových systémech se rozlišují 2 typy účtů: uživatelské a servisní účty.
- Uživatelské účty jsou centralizované, autentizace protokolem Kerberos, autorizace protokolem LDAP. Autentifikace i autorizace je nezávislá na aplikačním IDM. Zřizovány jsou

pouze za účelem správy systému, subsystémů a aplikací. Je zakázáno přidělovat uživatelské účty kvůli aplikačním přístupům (např. pro přenosy dat do/z aplikace). Na uživatelské účty se vzdáleně přistupuje protokolem ssh, autentizace heslem (možno GSSAPI).

- Servisní účty, to jsou účty dedikované pro správu, instalaci, provoz systému, subsystémů (např. Oracle db, aplikační servery, aj.) a aplikací, jsou lokální. Servisní aplikační účty (a skupiny) jsou alfabetické malými písmeny, začínají znaky ‚vzp‘, dále identifikace aplikace. Primární skupinou servisního aplikačního účtu je skupina stejného jména. S omezením na 16 znaků. UID a GID pro subsystémy a aplikace jsou přidělovány jednotně centrální autoritou VZP. Na servisní účty za účelem administrace se přistupuje pomocí sudo z běžného uživatelského účtu na základě přidělené administrátorské role (dedikovaný administrátorský LDAP). Přístup na servisní účty není povolen s autentifikací heslem.
- Instalace dané aplikace včetně tvorby unixové adresářové struktury (vlastnictví, skupiny uživatelů, práva) se provádí na základě aplikační dokumentace pomocí dodané instalační úlohy. Aplikační dokumentace musí obsahovat seznam veškerých aplikačních trustů vytvářených na úrovni systému (ssh public key trusty pro vzájemnou komunikaci, aj.). Aplikace obsahuje úlohu, která kontroluje správnost nasazení, tedy mj. i nastavení vlastnictví, skupiny uživatelů, práva v adresářových stromech aplikace. Zjištěné chyby jsou protokolovány, a pokud je to možné, automaticky opravovány.
- Veškeré aplikační struktury jsou uchovávány v dedikovaných aplikačních adresářových stromech. Pokud aplikace využívá obecné subsystémy (např. java, http server, openssl, ...), musí být rovněž veškerá konfigurace a data těchto subsystémů v adresářových stromech aplikace a nezávislá na případném použití komponenty jinou souběžnou aplikací (dedikovaný port pro http server, ...). Pokud nelze zajistit nezávislost použití dané komponenty, musí aplikace použít vlastní instalaci komponenty ve svém aplikačním stromě.

### 3.5 Middleware

Vlastník kapitoly: OTP OSAD

#### 3.5.1 Aplikační servery

Výčet typů AS využívaných v IS VZP:

Druh AS	Použití
Oracle Fusion Middleware WebLogic Server v nejnovější podporované verzi	Aplikace deployované v J2EE, vhodné pro aplikace třídy A
JBoss aplikační server v nejnovější podporované verzi	Pro J2EE aplikace třídy B nebo v odůvodněných případech, kde není vhodné použití Oracle Weblogic J2EE.

#### 3.5.2 Webové servery

Výčet typů WS využívaných v IS VZP:

- Oracle Web Tier v nejnovější podporované verzi
- Apache v nejnovější podporované verzi
- IIS

### 3.6 Virtualizovaná infrastruktura pro hostování aplikací

Vlastník kapitoly: OTP OSAD

Aplikační služby jsou hostovány na virtuálních prostředí / serverech následujících parametrů:

Název služby	Popis
Server s OS	OS Windows nebo Linux (viz kap. 3.3 OS)
Aplikační server	OS Windows nebo Linux aplik. serveru Oracle Weblogic Suite
Databázový server Oracle	OS Linux, Oracle dB EE + RAC + partitioning
Databázový server MS SQL	OS MS Windows, MS SQL Server v edici Enterprise

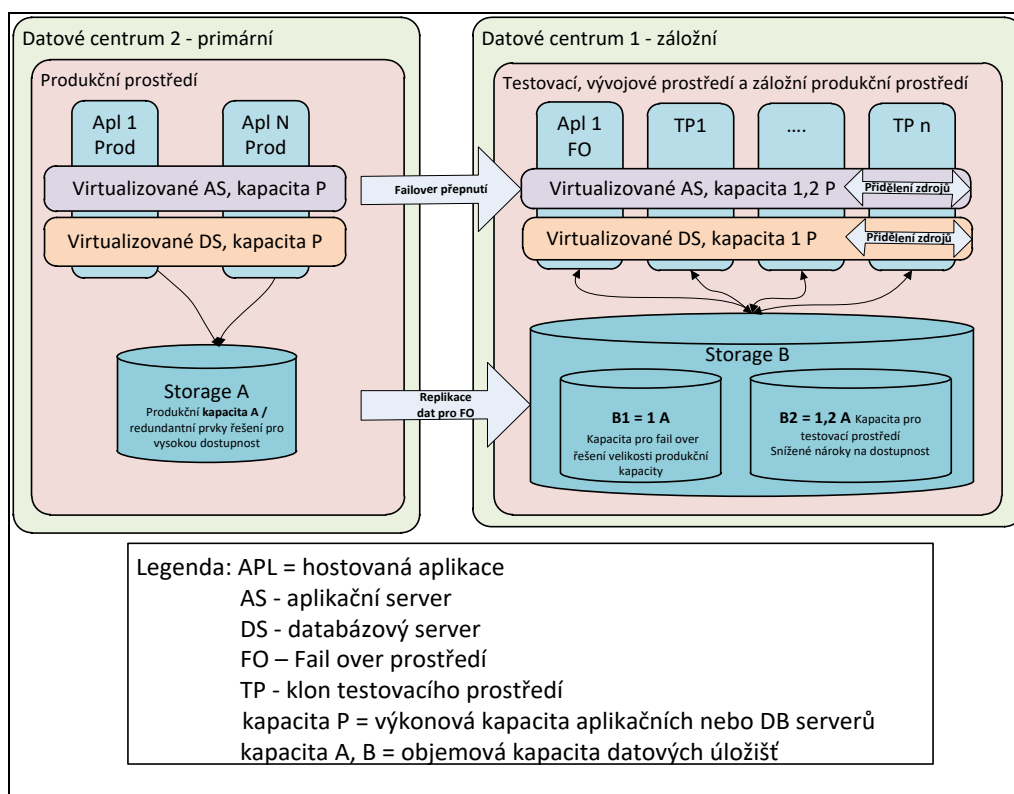
### 3.7 Deployment aplikací provozovaných on-Premise do prostředí v DC VZP

Vlastník kapitoly: OTP OSAD

Pro zabezpečení provozu aplikací v prostředí datových center je používán standardizovaný deployment aplikací:

- Produkční instance aplikací a jejich odpovídajících dat je hostována v primárním datovém centru na zařízeních s vysokou dostupností a redundancí na virtualizované infrastruktuře.
- Záložní instance aplikací je hostována ve virtualizované infrastruktuře v záložním datovém centru s dedikovanou kapacitou úložiště o velikosti produkčních dat pro fail over primárního DC.
- Virtualizovaná infrastruktura serverů záložního centra je dimenzována jako výkonový ekvivalent zařízení v primárním datovém centru. Požadavek na dostupnost je nižší, tomu odpovídá nižší redundance prvků.
- Virtualizovaná infrastruktura záložního centra je sdílena s testovacími prostředími.
- Produkční data z primárního DC jsou asynchronně replikována do záložního DC.
- Pro účely testování je v záložním DC dedikována obecně kapacita virtualizované úložné kapacity až v rozsahu 1,2 velikosti produkčních dat sdílená pro všechny instance testovacích prostředí. Tato kapacita je alokována individuálně při návrhu systému.
- Kapacita úložiště Storage B musí být 2,2 násobkem kapacity úložiště produkčního prostředí Storage A
- Kapacita HW serverů pro databázovou a aplikační vrstvu musí být výkonově dimenzována jako 1,2 násobek produkčního prostředí (měřeno součtovým počtem jader, velikostí operační paměti virtuálních serverů a diskových úložišť pro aplikační a databázovou vrstvu). Redundance komponent není nutná.





### 3.8 Datové a databázové služby

Vlastník kapitoly: OTP OSAD

#### 3.8.1 Databázové technologie

Standard	Popis
Oracle DB EE v nejnovější podporované verzi, včetně databázových options	Pro aplikace třídy A nebo B.
MS SQL EN/STD min. verze 2014, X64bit, standalone/cluster	Podpůrné služby a pro aplikace v třídě B. V odůvodněných případech je možné použít i pro aplikace třídy A.

#### 3.8.2 Datové a databázové standardy

Oblast standardizace	Popis
Minimum redundancí	Data jsou uložena v jediné databázi. Redundantní databáze v rámci lokality nejsou pro core business aplikace povoleny. Replikace se provádí pouze z důvodu realizace DR plánu.
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 DB musí být akceptován datovým architektem VZP ČR. Persistentní objekty vývojář definuje bez určení: <ul style="list-style-type: none"> <li>• Názvu tablespace</li> <li>• fyzických atributů segmentu (pctused, pctfree, storage params,...)</li> </ul> Databázové objekty jsou považovány za privátní součást aplikace, tzn. aplikace může přistupovat k databázovým objektům jiné aplikace pouze prostřednictvím dedikovaných služeb.
Jmenné konvence databázových objektů	Všechna jména základních databázových objektů (tabulky, pohledy, balíky funkcí a procedur, fronty, sekvence, indexy, triggeru apod.) začínají dvouznačným prefixem dodavatele
Kódování	Preferované UTF16, UTF8, Definici collation – preferována Czech CI AS (case insensitive a accent sensitive) Na výjimku: ISO 8859-2, Windows 1250
Podpora anonymizace / pseudonymizace osobních údajů	Datová vrstva musí podporovat možnost anonymizace a pseudonymizace osobních údajů bez nežádoucího vlivu na chování datového engine a aplikace. Využívá se pro účely příslušné legislativy a vytváření datového derivátu pro testování z produkčních dat. Součástí dodávek je nástroj pro vytváření anonymizovaných derivátů produkčních dat (scrambling tool). Toto musí být zohledněno i v dokumentaci.
Podpora řezů dat	Datový model musí být navržen tak, aby pro účely testování bylo možno oddělit testovací derivát – vzorek dat z produkčních dat. Součástí dodávek je nástroj pro vytváření takových derivátů. Toto musí být zohledněno i v dokumentaci.
Zakázané vazby	Data v relačních databázích nesmí být provazována technologicky přes významové klíče, povolena je relační vazba pouze přes nezávislé technologické klíče záznamů. Nejsou dovoleny přímé datové vazby mezi datovými doménami.

## 4 Bezpečnostní standardy

Vlastník kapitoly: OKIB

### 4.1 Dodržování legislativních požadavků

Dodávaný systém, nebo aplikace, je v souladu (po technické / procesní stránce poskytuje takové funkcionality, které VZP ČR umožní být v souladu) s níže uvedenými zákony a nařízeními:

#### 4.1.1 Autorský zákon

Zákon č. 121/2000 Sb., o právu autorském, právech souvisejících s právem autorským a o změně některých zákonů, v platném znění.

#### 4.1.2 ZOKB

Zákon č. 181/2014 Sb. (Zákon o kybernetické bezpečnosti a o změně souvisejících zákonů (Zákon o Kybernetické bezpečnosti) v platném znění (zkratka ZoKB) a související Vyhláška o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti) a to především v oblastech:

- zajištění průběžného a včasného odstraňování zranitelností systému, nebo aplikace po celou dobu podpory (subjekt odpovědný za správu systému, nebo aplikace vždy zajišťuje odstraňování zranitelností dle PŘ 2018/13 čl. 7);
- implementace vhodného způsobu řízení přístupu k informačním aktivům na základě rolí vč. autentizačních a autorizačních procesů;
- implementace logování systému, nebo aplikace.

#### 4.1.3 GDPR

„Nařízení Evropského parlamentu a Rady č. 679/2016 ze dne 27. 4. 2016“ (zkratka GDPR) a to především v oblastech:

- implementace procesů / datových modelů umožňujících a podporujících zajištění omezení doby zpracování (odstranění osobních údajů fyzických osob, které již nemají z hlediska VZP ČR další účel zpracování a kterým současně již uplynula stanovená doba pro uchování osobních údajů)
- implementace logování přístupu k příslušným informačním aktivům na aplikační úrovni
- implementace podpory mechanismů umožňujících snadné předání údajů zpracovávaných v příslušné aplikaci ve strojově čitelné podobě jinému správci
- ve spolupráci s VZP ČR zajistit provedení analýzy „Vliv zamýšlených operací zpracování na ochranu osobních údajů“ (Data Protection Impact Assessment - DPIA)

### 4.2 Dodržování obecných standardů a doporučení

V rámci dodávky/vývoje je doporučeno dodržování obecně platných standardů uvedených níže. Výjimky nebo odchylky od uvedených standardů musejí být předem schváleny VZP.

- Center for Internet Security Benchmark;
- Application Security Verification Standard;
- ISO/IEC 2700x (ISMS);
- ISO/IEC 12207 (Systems and software engineering – Software life cycle processes);
- ISO/IEC 15504 (Software Process Improvement and Capability Determination (SPICE)).

### 4.3 Minimum běžících a instalovaných služeb

Jsou nainstalovány a spuštěny pouze takové služby, které jsou pro provoz systému / aplikace nezbytné.

### 4.4 Nevyhovující služby nebo protokoly

Služby nebo protokoly, které nevyhovují bezpečnostním požadavkům pro přenos či zpracování definované kategorie citlivosti informace nesmí být pro přenos nebo zpracování informace použity.

Nevyhovuje zejména:

- použití nešifrovaných protokolů pro vzdálenou administraci (TELNET, http, atd ...);
- použití nešifrovaných protokolů pro přenos dat (FTP, http, atd ...);
- použití slabých a již nevyhovujících metod šifrování (SSL2, SSL3, SHA1, atd...);
- použití služeb se známou zranitelností, která není výrobcem opravena nebo je neopravitelná;
- použití služeb bez podpory výrobce (Out Of Life).

### 4.5 Synchronizace času

Systém provádí synchronizaci času s NTP servery VZP ČR (ntp1.vzp.cz, ntp2.vzp.cz, ntp3.vzp.cz) nejméně jednou za 24 hodin.

### 4.6 Kryptografie

#### 4.6.1 Požadavky na kryptografické algoritmy

Kryptografické algoritmy musí splňovat doporučení NÚKIB platné ke dni 28. 11. 2018. Dokument lze získat ze stránek <https://www.govcert.cz/cs/doporuceni-v-oblasti-kryptografickych-prostredku/>.

#### 4.6.2 Požadavky na ochranu privátního klíče

- Jakýkoliv privátní klíč uživatele musí být chráněn heslem;
- Privátní klíče musí být spolehlivě zálohovány pro případ jejich ztráty nebo poškození;
- Musí být definovány postupy pro obnovení klíče a postupy instalace nového klíče v případě nedůvěry ve starý aktuální klíč.

#### 4.6.3 Požadavky na CA / PKI

- Služba, které přísluší v roli interní certifikační autority VZP ČR vydávat na základě, certificate signing request' (CSR) certifikáty (technologické nebo osobní) musí být schopna kromě věcí obvyklých, jako je zajištění bezpečného vydávání těchto certifikátů, jejich bezpečná distribuce, omezení platnosti na max. 2 roky umožnit i jejich zneplatnění za pomoci vystavení tzv. ‚certificate revocation list' (CRL);
- systémy, nebo aplikace využívající certifikátů vydaných touto certifikační autoritou musí být schopny reagovat na změny v CRL;
- pro každé řešení v roli CA / PKI VZP ČR musí být zajištěno, že jsou vydané certifikáty evidovány a před dobou expirace certifikátu je vlastník upozorněn na blížící se expiraci certifikátu, toto platí **zejména pro certifikáty technologické** (upozornění musí být odesíláno min. tři měsíce předem vlastníkovvi aplikace a procesně musí být vynuceno ověření, že došlo k výměně certifikátu);
- dodavatel nemůže bez svolení pro svoje řešení využívat neschválenou CA / PKI, případně řešit zabezpečení tzv. ‚self-signed certifikáty' a preferenčně musí využít centrální CA / PKI VZP ČR.

## 4.7 Komunikace s veřejnou sítí

### 4.7.1 Systémy, nebo aplikace, které publikují služby do veřejné sítě (inbound)

Všechny On-Premise systémy, nebo aplikace, které publikují služby do veřejné sítě (např. poskytující B2B API, webové prezentace apod.) jsou:

- umístěny ve vyhrazeném síťovém segmentu (vnitřní perimetr), který je dohledován IDS/IPS řešením a má omezené možnosti komunikace do vnitřní sítě;
- zapojeny tak, že je aplikačními firewally prováděna inspekce provozu.

### 4.7.2 Komunikace do veřejné sítě (outbound)

Všechny On-Premise systémy, nebo aplikace, které potřebují pro zajištění svého provozu komunikovat s veřejnou sítí, kromě systémů, nebo aplikací poskytujících základní infrastrukturní služby typu DNS, NTP, e-mail gw pro veřejnou síť, Proxy (vč. schválených výjimek) s veřejnou internetovou sítí nekomunikují přímo, ale pro komunikaci s veřejnou sítí využívají proxy server (proxy server zajišťuje terminaci šifrovaného kanálu a inspekci provozu).

### 4.7.3 SMTP komunikace s veřejnou sítí

- SMTP brána, která komunikuje s veřejnou sítí, musí:
- být umístěna ve vyhrazeném síťovém segmentu (vnitřní perimetr), který je dohledován IDS/IPS řešením a má omezené možnosti komunikace do vnitřní sítě;
- identifikovat nevyžádané emaily (pomocí heuristiky, RBL, reputace odesílatele, nebo kombinací těchto mechanismů) a aplikovat na ně příslušné politiky (např. odmítnutí doručení, označení zprávy jako nevyžádané apod.);
- podporovat šifrování emailové komunikace mezi emailovými servery (SMTPS);
- zabránit potenciálnímu spoofingu emailové komunikace (SPF);
- Identifikovat malware a zabránit jeho doručení (využívat sandboxingu, nebo antivirového řešení).

## 4.8 Řízení přístupu

### 4.8.1 Autentizace a autorizace při přístupu k systémům, nebo aplikacím VZP ČR z interní sítě VZP ČR

4.8.1.1 V případě koncových uživatelů (pracovníků VZP ČR, kontraktorů VZP ČR):

- správa identit koncových uživatelů je uchovávána v nástroji pro správu a ověřování identit uživatelů, administrátorů a aplikací, kterým je centrální AD VZP ČR;
- musí být zajištěno řízení přístupových oprávnění k jednotlivým IS VZP ČR **na základě přístupových skupin a rolí** v nástroji pro řízení přístupových oprávnění, kterým je IDM (Identity Management System) VZP ČR;
- koncový uživatel (v rámci vnitřní sítě VZP ČR) musí vždy prokazovat svoji identitu směrem k aplikačnímu uživatelskému front-endu principem SSO, kdy **autentizace je zajištěna transparentně** (bez interakce uživatele);
- interaktivní autentizace koncového uživatele probíhá pouze do operačního systému;
- **Autentizace** koncového uživatele:
  - musí probíhat proti centrálnímu AD VZP ČR.
- **Autorizace** koncového uživatele:
  - je řízena IDM, ve kterém jsou přístupová oprávnění a skupiny definovány.

#### 4.8.1.2 V případě komponent IS VZP ČR (API a dalších technologických rozhraní):

- Musí být zajištěno řízení přístupů k jednotlivým IS VZP ČR.
- Autentizace** komponent IS v rámci SOA (v souvislosti s prokázáním identity komponenty IS musí být využito alespoň jednoho z níže uvedených způsobů:
- PKI VZP ČR. Všechny komunikující komponenty IS musí při ustanovení komunikace využít certifikát vydaný centrální certifikační autoritou VZP ČR (CA VZP ČR). Ověření platnosti certifikátu (podpis CA, rozsah platnosti, identita serveru/klienta) je prováděno na obou stranách, resp. klientem služby i konzumentem služby (mutual authentication);
  - případně s využitím podpůrné infrastruktury IdP a IdS (tiketů/tokenů, SAML/JWT) existující v době realizace zakázky.
- **Autorizace** komponenty IS v rámci SOA (musí být zajištěna alespoň jedním z níže uvedených způsobů):
    - Využitím atributu „DN“ certifikátu využitého pro autentizaci komponenty, na základě předaného „DN“ volaný systém ověří (LDAP nebo lokální úložiště), zda volající systém má autorizaci pracovat s API systému volaného (preferovaná varianta);
    - API key (tato varianta musí být schválena VZP ČR);
    - srovnáním fingerprintu konkrétního certifikátu klienta služby (import veřejného certifikátu klienta služby), tato varianta musí být schválena VZP ČR;
    - podepsáním zprávy (výměna veřejných klíčů mezi komunikujícími aplikacemi), tato varianta musí být schválena VZP ČR;
    - získáním informace o autorizaci pro danou operaci z externího pro to určeného řešení (LDAP/AD apod), tato varianta musí být schválena VZP ČR.

#### 4.8.2 Autentizace a autorizace při přístupu k systémům, nebo aplikacím VZP ČR z veřejné sítě

##### 4.8.2.1 V případě koncových uživatelů (klientů VZP ČR):

- správa identit koncových uživatelů musí být uchovávána a řízena v nástroji pro správu a ověřování identit uživatelů (EIM – Externí Identity Management), tj. není jím centrální AD VZP ČR;
- musí být zajištěno řízení přístupových oprávnění k jednotlivým IS VZP ČR na základě přístupových skupin a rolí v nástroji pro řízení přístupových oprávnění – IDM (Identity Management Systém) .
- **Autentizace** koncového uživatele.
  - musí probíhat proti EIM.
- **Autorizace** koncového uživatele:
  - je řízena IDM, ve kterém jsou přístupová oprávnění a skupiny definovány.

##### 4.8.2.2 V případě koncových uživatelů (pracovníků VZP ČR, kontraktorů VZP ČR):

- Koncový uživatel VZP ČR přistupuje do vnitřní sítě VZP ČR z veřejné sítě Internet vždy prostřednictvím VPN VZP ČR. Není proto důvod, aby byly služby pro tento typ koncové uživatele vystaveny přímo do Internetu. To platí rovněž pro služby využívané uživateli s privilegovanými oprávněními - administrátory.
- **Autentizace:**
  - uživatelským účtem spravovaným v AD VZP ČR a osobním certifikátem vydaným CA VZP ČR.
- **Autorizace:**

#### 4.8.3 viz. 4.8.1.1 Propagace identity uživatele ke koncovým službám

- Identita konkrétního uživatele je ověřena z front-endu nebo API aplikace a **vždy** propagována až ke koncovým službám přes všechny technologické vrstvy IS VZP ČR a to především z důvodu určení původce transakce a jeho pozdější identifikaci v příslušném aplikačním logu.

##### 4.8.3.1 Propagace identity pro SOAP Webové služby:

Bude využit standardní Username token s uživatelským jménem koncového uživatele. Token nebude obsahovat žádné heslo a bude odesílán v rámci WS-Security hlaviček SOAP požadavku. Viz následující příklad:

```
<?xml version="1.0" encoding="UTF-8"?>

<soap:Envelope xmlns:soap="http://.../soap/envelope/">

  <soap:Header xmlns:wssse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd" xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd">

    <wsse:Security>

      <wsse:UsernameToken wsu:Id="UsernameToken-484-624e-938a-a986-a5e8717dcb3d">

        <wsse:Username>melich99</wsse:Username>

      </wsse:UsernameToken>

    </wsse:Security>
    . . . . .
  </soap:Header>

  <soap:Body>
    . . . . .
  </soap:Body>

</soap:Envelope>
```

##### 4.8.3.2 Propagace identity pro RESTové služby

Pro propagaci identity na REST API bude využita hlavička aplikačního protokolu HTTP. Vzhledem k tomu, že využití standardní hlavičky *Authorization* pro čistou propagaci identity bývá matoucí, bude využita custom hlavička *iv-user*. Viz následující příklad:

```
GET /serverapi/v1/documents/1233222777/content http 1.1

host: esb.ecm.vzp.cz

iv-user: melich99
```

#### 4.8.4 Ochrana hesel a politika hesel

- Hesla nesmí být uchovávána v čitelné podobě v dávkových souborech, automatických přihlašovacích skriptech, makrech, v nechráněných souborech a všude tam, kde by mohlo dojít k jejich odhalení.
- Systém, nebo aplikace, musí zajistit ochranu hesel a vynucovat politiku hesel v souladu s požadavky ZoKB, resp. Vyhlášky 82/2018.

#### 4.8.5 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).

- Po definovaném počtu neúspěšných pokusů (5 pokusů) o přístup musí dojít k automatickému uzamčení příslušného účtu. Tento požadavek se nevztahuje na systémové účty, kde by mohlo uzamčení účtu způsobit provozní problémy. Opětovné odemknutí je v kompetenci Administrátora systému nebo aplikace. Mechanismus musí být navržen tak, aby nedošlo k hromadnému zamykání a tím odepření služby.

#### 4.8.6 Omezení přístupů ke službám ve vnitřní síti VZP ČR

Systémy, nebo aplikace, publikují do sítí, ze kterých k němu přistupují koncoví uživatelé, výhradně služby, které jsou koncovým uživatelům určené. Jiné služby (např. služby zajišťující integraci s jinými systémy) nesmí být nikdy ze sítí, ve kterých pracují koncoví uživatelé, dostupné.

#### 4.8.7 Zobrazení varovného hlášení

V případě systému, nebo aplikace, kdy uživateli jsou pracovníci VZP a systém, nebo aplikace obsahuje chráněné informace, musí být uživatelům před dokončením procesu autentizace zobrazeno varovné hlášení, které je informuje o důsledcích jejich aktivit. Toto hlášení musí uživatele varovat, že neoprávněný pokus o přihlášení, nebo zneužití takového přístupu může vést k pracovně právnímu postihu a/nebo trestnímu stíhání a dát jim možnost proces autentizace ukončit.

Varovné hlášení musí obsahovat následující text: *“Veškerá práva k systému a údajům v něm obsažených jsou vyhrazena ve prospěch VZP ČR. Vstup do tohoto systému je umožněn pouze na základě autorizovaného přístupu a při dodržování příslušných bezpečnostních pravidel. Jakékoli nakládání, přenášení nebo jiné zpracování údajů obsažených v tomto systému v rozporu s pokyny nebo souhlasem VZP ČR jsou zakázány. Aktivita v tomto systému jsou monitorovány.”*

### 4.9 Ochrana informačních aktiv

Systém, nebo aplikace, musí zajistit:

- kompletnost a platnost dat při zaručeném zpracování pouze autorizovanými systémy a uživateli;
- nesmí umožnit neautorizovaný zásah do evidovaných informací / dat.

#### 4.9.1 Klasifikační schéma informačních aktiv

Pro účely klasifikace informací VZP ČR je stanoveno následující klasifikační schéma informací:

- **chráněné informace** – informace, jejichž ochrana vyplývá ze zákona, nebo informace vyžadující zvýšenou úroveň ochrany na základě obchodních nebo vnitřních požadavků z hlediska dostupnosti, důvěrnosti nebo integrity,
- **interní informace** – informace související s běžným provozem VZP ČR a jednotlivých organizačních celků, které nejsou určeny ke zveřejnění a nesmějí být volně přístupné externím subjektům,
- **veřejné informace** – informace, které nevyžadují žádný zvláštní stupeň ochrany ve vztahu k zachování důvěrnosti, dostupnosti a integrity. Tyto informace mohou být volně zveřejněny i mimo VZP ČR.

Mezi **chráněné informace** patří:

- **osobní údaje** - jakákoliv informace týkající se určeného nebo určitelného subjektu údajů. Subjekt údajů se považuje za určený nebo určitelný, jestliže lze subjekt údajů přímo či nepřímo identifikovat zejména na základě čísla, kódu nebo jednoho či více prvků, specifických pro jeho fyzickou, fyziologickou, psychickou, ekonomickou, kulturní nebo sociální identitu.
- **zvláštní kategorie osobních údajů** - osobní údaj vypovídající o národnostním, rasovém nebo etnickém původu, politických postojích, členství v odborových organizacích, náboženství a filozofickém přesvědčení, odsouzení za trestný čin, zdravotním stavu a sexuálním životě



subjektu údajů a genetický údaj subjektu údajů; do zvláštní kategorie osobních údajů spadá biometrický údaj, který umožňuje přímou identifikaci nebo autentizaci subjektu údajů. Tam, kde je to možné, je provedena anonymizace subjektů přiřazením jedinečného identifikátoru, který s sebou nenesou žádná osobní data.

#### 4.9.2 Data v klidu (Data at Rest)

- Pokud data obsahují chráněné informace, pak musí být při uložení šifrovány (v databázích a datových skladech, na souborovém systému, na páskách a dalších výměnných médiích, v mobilních zařízeních apod.).
- Pro případ zničení primárních dat musí být data zálohována a archivována. Záložní kopie musí být umístěny v geograficky vzdálené lokalitě, nebo tak, aby nehrozilo současné zničení medií a zdrojových dat.
- Zálohovaná data se musí podepisovat a používat mechanismus kontrolního součtu.
- Musí být nastaven proces pro bezpečnou likvidaci již nepotřebných dat a to tak, aby informace nešlo obnovit.

#### 4.9.3 Data v pohybu (Data in Transfer)

- Pokud data obsahují chráněné informace, pak musí být během přenosu po síti šifrovány.
- je doporučeno data obsahující chráněné informace podepisovat.

#### 4.9.4 Data při zpracování použití (Data in Use)

- Přístup k informacím musí být řízen na základě přístupových oprávnění pro jednotlivé uživatele a jednotlivá aktiva.
- Je uplatňován princip *“need to know”*, do produkčních prostředí, která obsahují chráněné informace nemají např. přístup pracovníci vývoje.
- V případě, že informace obsahují osobní, nebo zvláštní kategorie osobních údajů, musí být operace (přístup a změna) nad těmito informacemi logovány.
- V neprodukčních prostředích (vývojová a testovací prostředí) nesmí být využívány chráněné informace.
- Informace v neprodukčních prostředích jsou anonymizovány, kdy Anonymizací se rozumí taková úprava, po které nelze údaje vztáhnout k určenému nebo určitelnému subjektu údajů.

#### 4.9.5 Antimalware ochrana

Ukládané dokumenty jsou testovány pomocí antiviru (systému na ochranu proti malware).

#### 4.9.6 Plán obnovy (Disaster Recovery)

Dokumentace musí obsahovat stanovení procesů, postupů a opatření pro zajištění obnovy provozu a testování DR plánů.

### 4.10 Bezpečnostní testy

#### 4.10.1 Systémy, nebo aplikace, které nepublikují služby do veřejné sítě

Systémy, nebo aplikace, které nepublikují služby do veřejné sítě, musí být ve spolupráci s dodavatelem podrobeny internímu bezpečnostnímu testování. Toto testování provádí VZP v součinnosti s dodavatelem.

#### 4.10.2 Systémy, nebo aplikace, které publikují služby do veřejné sítě

- a) V případě, že je systém, nebo aplikace bude dostupná z veřejné sítě, musí dodavatel zajistit, aby byl v rámci dodávky proveden nezávislý penetrační test aplikace v rozsahu, který je v souladu s nejlepší praxí.
- b) Minimálně jsou provedeny testy v těchto oblastech:

Oblast	Testy
Brute Force Prevention	Lack of account lockout, Different login failure message, Insufficient authentication, Weak password recovery, Lack of SSL on login pages, Auto-complete enabled on pass parameters
Credential/Session prediction	Sequential session token, Non-Random session token,
Insufficient Authorization	Forcefully browse to logged in URL, Forcefully browse to high privilege URL, HTTP verb tampering, Insufficient session expiration
Session Fixation	Failure to generate new session ID, Permissive session management
Session Weaknesses	Session token passed in URL, Session cookie not set with secure attribute, Session cookie not set with HTTPOnly, Session cookie not sufficiently random,  Site does not force SSL connection, Site uses SSL but references insecure objects, Site supports weak SSL ciphers
Cross-Site Scripting	Reflected cross-site scripting, Persistent cross-site scripting, DOM-based cross-site scripting, Cross-frame scripting, HTML injection, Cross-site request forgery, Clickjacking
Injection Attacks	Format string attack, LDAP injection, OS command injection, SQL injection, Blind SQL injection, SSL injection, XPath injection, HTTP header injection/response splitting, Remote file includes, Local file includes, Potential malicious file uploads
Information Disclosure	Directory indexing, XML External Entity
Information Leakage	Detailed application error messages, Include file source code disclosure, Path traversal, Predictable resource location, Insecure HTTP methods enabled, WebDAV enabled, Default web server files, Testing and diagnostics pages, Internal IP address disclosure, Server-Side Request Forgery (SSRF)

- a) Do doby provedení penetračních testů a odstranění nálezů plynoucích z těchto testů nesmí být aplikace veřejně dostupná (technickými prostředky je zajištěno, že je aplikace dostupná pouze subjektu, který provádí testování). Protokol s výsledky testů předkládá dodavatel VZP ČR. Protokol obsahuje metodiku testů, výčet použitých nástrojů při

provedení testů, výčet dílčích testů (dokladuje, které testy byly provedeny) a výsledky testů.

- b) Na základě výsledků testů VZP ČR rozhoduje o akceptaci testovaných komponent IS a jejich uvedení do provozu;
- c) tento test musí být opakován při každé významné změně systému, nebo aplikace, zejména pokud dochází ke změnám v přístupu k autentizaci a autorizaci systému, nebo aplikace (pokud je systém pod podporou dodavatele, tyto testy provádí dodavatel v rámci režie služby).

Na základě výsledků testů VZP ČR rozhoduje o akceptaci testovaných komponent IS a jejich uvedení do provozu.

## 5 Logování

Tato kapitola definuje požadavky na logování v oblastech:

- a) **Bezpečnosti:**
  - a. Základní úroveň logování z pohledu bezpečnosti;
  - b. Logování transakcí při zpracování osobních a zvláštních kategorií osobních údajů.
- b) **Komunikace a Business logiky:**
  - a. Transakční logy.
- c) **Provozu:**
  - a. Provozně-aplikační logy.

Pro zalogování událostí do správného logu nebo i do více logů se použije následující logika zařazení události:

Událost související s:	Oblast logování
Autentizací	Bezpečnost
Přístupovými oprávněními	Bezpečnost
Privilegované přístupy	Bezpečnost
Operace se soubory	Bezpečnost
Exporty dat	Bezpečnost
Operace s auditními záznamy	Bezpečnost
Operace s osobními daty	Bezpečnost
Stavem aplikace (chyby, výjimky)	Provoz
Stavem infrastruktury	Provoz
Výkoností aplikace	Provoz
Komunikace s dalšími aplikacemi, použití datových rozhraní	Komunikace

Událost může patřit do více než jednoho logu, tedy bude zalogována do více logů.

## 5.1 Požadavky

### 5.1.1 Formát a encoding logu

- a) Preferovaný formát logu je v případě vývoje aplikace specificky pro VZP ČR JSON (JavaScript Object Notation), **v ostatních případech je formát dán výrobcem** a jeho použití musí být schváleno VZP ČR.
- b) Doporučený encoding logu je [UTF-8](#), v ostatních případech je nutné schválení encodingu VZP ČR.

### 5.1.2 JSON - doporučené pojmenování klíčů a identifikace datové struktury

- a) Každý záznam musí obsahovat klíč "src\_type", který identifikuje datovou strukturu události (přiřazení záznamu příslušné doméně zájmu).
- b) Pokud je nutno zaznamenat informace, pro které není vhodné použít žádného z níže uvedených klíčů, pak dodavatel vytváří vlastní klíč:
  - i. Klíče jsou pojmenovávány v angličtině.
  - ii. Informace o nově vzniklém klíči a jeho účelu je součástí příslušné dokumentace.

### 5.1.3 Obecně platné zásady pro logování

- a) Každý záznam je označen časovým razítkem vytvoření / modifikace záznamu.
- b) Logované informace musí odpovídat aktuálnímu stavu systému, interpretace logů musí proveditelná bez dodatečných datových zdrojů. Pokud je logovaná hodnota z číselníku loguje se jak klíč tak i odpovídající hodnotu, které se vždy vztahují k danému časovému okamžiku.
- c) Každá komponenta, která se podílí na zpracování transakcí (včetně volání integračních služeb a rozhraní) bude logovat do lokálního transakčního logu. Do transakčního logu se zaznamenávají minimálně události volání a ukončení služby.

#### 5.1.3.1 Časové razítko

- a) Každý záznam obsahuje časové razítko vzniku události.
- b) Preferovaný formát časového razítka je: "YYYY-MM-DD hh:mm:ss", pokud není požadováno jinak, je uvedený čas vždy platný v zóně Europe/Prague. Příklad: "2019-03-14 11:02:39".
- c) Další možný formát časového razítka je ve formátu, ve kterém jej do logu zapisuje operační systém, na kterém je aplikace spuštěna (UNIX/Linux: "Mar 12 13:31:45", Windows "15.03.2019 9:31:40").
- d) Ostatní formáty zápisu časového razítka musí být v souladu s ISO 8601 a jejich použití musí být schváleno VZP ČR.

### 5.1.4 Technické zajištění logování

#### 5.1.4.1 On-Premise

- a) Logový soubor musí být lokální, tj. agent nemůže k logu přistupovat pomocí síťového protokolu na sdíleném prostředí. To nevylučuje vzdálené plnění logu. Nepřípustný je log v podobě průběžné databázové tabulky nebo pohledu.
- b) Pokud je aplikace nasazena na OS Unix/Linux, pak musí logovat s využitím souborového systému a musí zajistit rotaci logů, nebo využívá mechanismu syslog.
- c) Pokud je aplikace nasazena na OS Windows, pak musí logovat s využitím souborového systému a musí zajistit rotaci logů, nebo používá mechanismu Windows Event logu.
- d) Musí být zajištěno, aby velikost jedné zprávy nepřekročila 65507 bajtů.

- e) Preferovaný mechanismus pro zajištění persistence logů generovaných kontejnery Docker je využití [Docker Volumes](#).

### 5.1.5 Retence logů

Logy jsou předávány do Centrálního úložiště logů VZP ČR. V ostatních případech (udělena výjimka) musí být zajištěna kapacita pro dostatečně dlouhé uložení logů na příslušných aplikačních serverech, to znamená:

- všechny logy jsou online uchovány minimálně po dobu 30 dní;
- logy, které obsahují informace v souladu s požadavky ZoKB, resp. Vyhlášky 82/2018 jsou k dispozici minimálně po dobu 18 měsíců;
- logy, které obsahují informace o přístupech k osobním údajům nebo k zvláštní kategorii osobních údajů, jsou k dispozici minimálně po dobu 36 měsíců.

### 5.1.6 Dokumentace

Dodavatelem je předána dokumentace, která obsahuje:

- výčet auditovaných událostí;
- vzorky událostí;
- při použití JSON formátu názvy použitých klíčů vč. jejich popisu;
- způsob uložení (místo uložení na souborovém systému);
- zajištění retence a rotace;
- nastavení přístupových práv.

## 5.2 Základní úroveň logování z pohledu bezpečnosti

Vlastník kapitoly: OIKB

Pokud jsou záznamy ve formátu JSON, pak každý záznam musí obsahovat následující klíč a hodnotu: "src\_type": "security".

### 5.2.1 Logování procesu autentizace

Požadavek zaznamenat proces autentizace se týká všech komponent IS VZP ČR, které v jakékoli formě implementují proces autentizace (včetně API).

Auditovaná operace	action	Popis
Přístup do systému nebo aplikace	logon	Jsou zaznamenány všechny oprávněné i neoprávněné pokusy o přístup.
Ukončení práce v systému nebo aplikaci	logout	Je zaznamenáno, kdy byla ukončena práce se systémem - včetně situace, kdy bylo provedeno automatické odhlášení po uplynutí stanovené doby nečinnosti.

#### 5.2.1.1 Příklad logu procesu autentizace u aplikace

Příklad logu procesu autentizace u aplikace, která implementuje vlastní logování a log ukládá do souboru:

```
{ "time_stamp": "2019-03-14 11:02:39", "host_fqdn": "server1.vzp.cz", "host_ip": "172.16.0.1",
"src_type": "security", "application": "my_app1", "environment": "prod", "src_class": "VZP_USER",
"src_user": "user1", "src_fqdn": "client1.kz.vzp", "src_ip": "172.16.1.1", "src_interface": "UI",
"action": "logon", "auth_method": "password", "auth_provider": "ldap", "result": "false", "err_descr":
"invalid user" }
```

### 5.2.2 Činnosti provedené administrátorem

Komponenty IS VZP ČR, které zpracovávají, ukládají, nebo přenášejí informace s klasifikací interní a vyšší, musí zaznamenávat:

Auditovaná operace	action	Popis
Činnost administrátora	activity	Jsou zaznamenány činnosti administrátora.

#### 5.2.2.1 Příklad logu činnosti provedené administrátorem

Příklad logu činnosti provedené administrátorem v systému, který implementuje vlastní logování a pro uložení logu využívá syslog:

```
Mar 14 11:02:39 server1 user1: { "time_stamp": "2019-03-14 11:02:39", "origin_fqdn": "server1.vzp.cz",
"origin_ip": "172.16.0.1", "src_type": "security", "application": "os_linux", "src_user": "user1",
"event_type": "activity", "uid": "root", "gid": "root", "groups": "root", "pid": "17783", "shell":
"bash", "action": "tail -f /var/log/messages", "result": "true" }
```

### 5.2.3 Změny přístupových oprávnění a změny údajů, které slouží k přihlášení

Komponenty IS VZP ČR poskytující služby autentizace nebo autorizace musí zaznamenávat:

Auditovaná operace	Popis
Změny stavu účtu	Přidání, odebrání, zneplatnění, povolení, nebo uzamčení účtu administrátorem (včetně uzamčení účtu po několika neúspěšných pokusech o autentizaci).
Změny rolí přiřazených účtu	Přidání, nebo odebrání role uživatelskému účtu.
Přidání, změna nebo odebrání <i>definice</i> role	Jsou zaznamenány všechny aktivity související s přidáním, změnou, nebo odebráním definice role.

### 5.2.4 Neprovedení činnosti v důsledku nedostatku přístupových oprávnění

Komponenty IS VZP ČR, které zpracovávají, ukládají, nebo přenášejí informace s klasifikací interní a vyšší, musí zaznamenávat:

Auditovaná operace	Popis
Neprovedení činnosti	Je zaznamenáno, pokud aktivitu nebylo možno provést v důsledku nedostatečných přístupových oprávnění.

### 5.2.5 Přístupy k záznamům o činnostech

Komponenty IS VZP ČR, které zpracovávají, ukládají, nebo přenášejí informace s klasifikací interní a vyšší, musí zaznamenávat:

Auditovaná operace	Popis
Operace nad auditními záznamy	Komponenty IS VZP ČR musí zaznamenávat pokusy o manipulaci s auditními záznamy a konfigurací auditní služby (v rámci logování přístupu k souborům), včetně zastavení a spuštění mechanismů sloužících pro záznam těchto činností.

### 5.2.6 Operace se soubory

Pokud soubor obsahuje chráněné informace, pak musí být zaznamenány operace vytvoření, smazání, čtení a zápisu, včetně identifikace uživatele, který operace vykonal.

Auditovaná operace	Popis
Operace se soubory	Jsou zaznamenány operace vytvoření, smazání, čtení a zápisu souboru včetně výsledku operace.
Exporty	Pokud aplikace umožňuje exportovat chráněné informace prostřednictvím UI, pak jsou zaznamenány události exportu dat (uložení dat mimo určenou aplikaci).

### 5.2.7 Vybrané JSON klíče pro záznam události

Název	Typ	Popis
src_type	VARCHAR2	Identifikuje datovou strukturu události.
time_stamp	DATETIME	Datum a čas zpracování transakce.
origin_fqdn	VARCHAR2	FQDN zařízení, na kterém událost vznikla.
origin_ip	VARCHAR2	IP zařízení, na kterém událost vznikla.
application	VARCHAR2	Jednoznačný identifikátor aplikace, pro kterou záznam vznikl, dle katalogu aplikací (např. application = "crp").
environment	VARCHAR2	Identifikace prostředí (prod dev test).
src_class	VARCHAR2	Typ původce, který inicioval transakci. Může to být například zaměstnanec VZP (VZP_USER), automatická úloha (VZP_JOB), zdravotnické zařízení (ZZ), zdravotní pojišťovna (ZP) atd.
src_user	VARCHAR2	V případě zaměstnance VZP ČR uživatelské jméno, v případě zdravotnického zařízení kód IČZ, v případě zdravotní pojišťovny kód ZP.
dst_user	VARCHAR2	V případě zaměstnance VZP ČR uživatelské jméno, v případě zdravotnického zařízení kód IČZ, v případě zdravotní pojišťovny kód ZP.
src_fqdn	VARCHAR2	Identifikace zařízení (prostředku), ze kterého byla transakce iniciována (FQDN PC nebo serveru, případně reference požadavku IPF).
src_ip	VARCHAR2	Pokud je zařízení (prostředek) PC, nebo server, je uvedena IP adresa prostředku.

dst_fqdn	VARCHAR2	Identifikace zařízení (prostředku), pro který která byla transakce iniciována (FQDN PC nebo serveru, případně reference požadavku IPF).
dst_ip	VARCHAR2	Pokud je zařízení (prostředek) PC, nebo server, je uvedena IP adresa prostředku.
detail	VARCHAR2	Pole pro doplňující komentář nebo jiné informace.
src_interface	VARCHAR2	Identifikace volajícího rozhraní (např. UI, IPF, CRON).
action	VARCHAR2	Typ události / akce.
result	BOOLEAN	Výsledek operace (true == provedeno   false == selhalo).
error_descr	VARCHAR2	Upřesnění chyby v případě selhání.

### 5.3 Logování transakcí při zpracování osobních a zvláštní kategorie osobních údajů

Vlastník kapitoly: OKIB

Pokud transakce provádí operace, které lze vztáhnout k určenému nebo určitelnému subjektu údajů, jsou vždy zaznamenávány auditní informace, které umožní určit a ověřit, kdy, kým a z jakého důvodu byly osobní nebo zvláštní kategorie osobních údajů, zaznamenány nebo jinak zpracovány. Vždy je rovněž zaznamenán výčet primárních aktiv typu informace, které se transakce účastní.

Nad rámec transakcí zpracování osobních údajů a zvláštní kategorie osobních údajů údajů jsou zaznamenávány náhledy a změny zdravotní pojišťovny vzhledem k přímé vazbě na zpracování OÚ a pro možné prošetřování zejména neoprávněné přeregistrace ke zdravotní pojišťovně, případně provedené změny bez vědomí a souhlasu pojištěnce.

Záznamy transakcí při zpracování osobních údajů ve formátu JSON musí obsahovat identifikaci datové struktury "src\_type": "data\_access" a identifikaci události "action": s výčtovou hodnotou "data\_create" OR " data\_read" OR "data\_update" OR "data\_delete" ([CRUD](#)).

- Logování zajistí komponenta, která je původcem transakce.
- Vždy je zajištěna jednoznačná identifikace iniciátora transakce a to i při zřetězení transakce.
- Ze zaznamenané transakce musí být zjevné, zda je událost vyvolána interakcí uživatele s UI, nebo zda se jedná o automatizovaný proces.
- Pro zaznamenání, z jakého důvodu byly osobní údaje zaznamenány nebo jinak zpracovány, je využit číselník důvodů.

#### 5.3.1 Vybrané JSON klíče pro záznam události

Název	Typ	Popis
detail	VARCHAR2	Z jakého důvodu byly osobní údaje, nebo zvláštní kategorie osobních údajů zaznamenány, nebo jinak zpracovány.
subject_id	VARCHAR2[]	Identifikátor subjektu, nebo subjektů tak, jak jej využívá aplikace.
subject_attr	VARCHAR2[]	Výčet konkrétních informačních aktiv, které se účastní transakce.
file_name	VARCHAR2	Jméno souboru, pokud se účastní transakce.



### 5.3.2 Příklad logu činnosti nahlížení

Příklad logu nahlížení údaje subjektu z UI aplikace:

```
{ "time_stamp": "2019-03-14 11:02:39", "origin_fqdn": "server1.vzp.cz", "origin_ip": "172.16.0.1",
"src_type": "data_access", "application": "my_app1", "environment": "prod", "src_class": "VZP_USER",
"src_user": "user1", "src_fqdn": "client1.kz.vzp", "src_ip": "172.16.1.1", "src_interface": "UI",
"action": "data_read", "result": "true", "detail": "kontrola údajů klienta, žádost klienta", "subject_id":
": "54a2ca2e4f47e95870cdcd9b216588d7", "subject_attr": { "pojistenec": [ "cisloPojistence", "jmeno",
"prijmeni", "datumNarozeni" ], "aktualniAdresa": [ "ulice", "obec", "psc", "stat" ] } }
```

### 5.3.3 Příklad logu činnosti změna

Příklad logu změny zdravotní pojišťovny z UI aplikace:

```
{ "time_stamp": "2019-03-14 11:02:39", "origin_fqdn": "server1.vzp.cz", "origin_ip": "172.16.0.1",
"src_type": "data_access", "application": "my_app1", "environment": "prod", "src_class": "VZP_USER",
"src_user": "user1", "src_fqdn": "client1.kz.vzp", "src_ip": "172.16.1.1", "src_interface": "UI",
"action": "data_write", "result": "true", "reason": "přeregistrace klienta k jiné ZP", "subject_id":
": "54a2ca2e4f47e95870cdcd9b216588d7", "subject_attr": { "zdravotniPojistovna": [ "kod", "nazev" ] } }
```

## 5.4 Základní požadavky na logování komunikace a business logiky- Transakční log<sup>7</sup>

Vlastník kapitoly: OAVRZ

Každá komponenta, která se podílí na zpracování transakcí včetně volání služeb ESB bude logovat do lokálního transakčního logu. Do logu se zaznamenávají minimálně události volání a ukončení služby. Výčet zaznamenávaných událostí odpovídající business logice je povinnou součástí návrhu a dokumentace systému.

### 5.4.1 Informační obsah události zaznamenávané v transakčním logu

Pokud jsou záznamy ve formátu JSON, pak každý záznam musí obsahovat následující klíč a hodnotu: "src\_type": "transaction".

Auditovaná událost /operace	Popis
Volání rozhraní aplikační komponenty	Komponenty IS VZP ČR musí zaznamenávat volání svého aplikačního rozhraní.
Zápis a čtení zpráv do/z fronty zpráv	Komponenty IS VZP ČR musí zaznamenávat předávání dat pomocí front (mesagingu)
Synchronizace dat pomocí rozhraní pro dávkové zpracování	Komponenty IS VZP ČR musí zaznamenávat výměnu dat pomocí dávkového zpracování dat (ETL, file sync apod.)
Směrování zpráv v rámci integrační platformy	Komponenty IS VZP ČR musí zaznamenávat případné podmíněné směrování zpráv, případně volání. Relevantní zejména pro integrační vrstvu (ESB, BPEL engine apod.)

<sup>7</sup> Pro vyhodnocení Transakčních logů je nezbytnou podmínkou zapnutí logování ESB, kdy vlastní vyhodnocení bude probíhat technologicky v nástroji, který propojí informace z Aplikačního auditního logu a logování ESB.

Transformace zpráv	Komponenty IS VZP ČR musí zaznamenávat transformace zprávy na jiný formát. Relevantní zejména pro integrační a proxy komponenty.
--------------------	--

#### 5.4.2 Vybrané JSON klíče pro záznam události

Název	Typ	Popis
src_type	VARCHAR2	Identifikuje typ události.
time_stamp	DATETIME	Datum a čas zápisu záznamu
origin_fqdn	VARCHAR2	FQDN zařízení, na kterém událost vznikla.
origin_ip	VARCHAR2	IP zařízení, na kterém událost vznikla.
application	VARCHAR2	Jednoznačný identifikátor aplikace, pro kterou záznam vznikl, dle katalogu aplikací (např. application = "crp").
environment	VARCHAR2	Identifikace prostředí (prod dev test).
app_interface	VARCHAR2	Identifikace použitého rozhraní, zahrnuje typ rozhraní
service_id	VARCHAR2	Identifikátor použité služby – tím je myšleno ID(uri) rozhraní / ID fronty zpráv apod.
instance_id	VARCHAR2	Jednoznačný identifikátor instance dané transakce/služby přidělovaný zapisující službou / aplikací
com_partner	VARCHAR2	Jednoznačný identifikátor protistrany komunikace podle katalogu aplikací (pokud je znám)
transaction_id	VARCHAR2	Identifikátor primární business transakce – události předávaný přes všechna volání podřízených služeb
partner_id <sup>8</sup>	VARCHAR2	Technologický identifikátor partnera, kterého se volání

<sup>8</sup> ID\_PARTNER slouží k logování pro GDPR, 101/2000 Sb. a ZoKB jako zdroj informací o žádajícím subjektu

		služby týká, předávaný přes všechna volání podřízených služeb.
src_user	VARCHAR2	Identifikace uživatele, který spustil primární službu. Předávaný přes všechna volání podřízených služeb.
result	BOOLEAN	Výsledek operace (true == provedeno   false == selhalo).
result_code	VARCHAR2	Výstupní stav dané instance transakce/služby kód stavu

### 5.4.3 Příklad transakčního logu

Příklad záznamu volání aplikace přes webové rozhraní

```
{ "time_stamp": "2019-03-14 11:02:39", "origin_fqdn": "server1.vzp.cz", "origin_ip": "172.16.0.1",
"src_type": "transaction", "application": "my_app1", "environment": "prod", "app_interface": "SOAP",
"service_id": "soa-infra/services/ZakladniRegistry/AiscCtiAifo/client", "instance_id":
"a4567gdsfx4460", "com_partner": "B2B_proxy", "transaction_id": "a02546456fd464d45s46z1x", "partner_id":
" client1.kz.vzp ", "src_user": " user1 ", "result": "true", "result_code": "200 OK" }
```

## 5.5 Provozní log

### 5.5.1 Základní požadavky na provozní logování – Provozní log

#### 5.5.2 Formát logovacího souboru provozního logu

Formát provozních logů je specifický z důvodu specifických požadavků na rychlé a automatizované zpracování:

- Formát souboru je v podobě cleartext souboru operačního systému v některém z obecně používaných formátů (Syslog, Common / Combined Log Format,...), resp. ve formátu Windows Event Log, případně lze použít dohodnutý formát.
- Oddělovačem je svislé lomítko „|“ (vertical bar, ASCII 124);
- Žádné z polí zprávy by nemělo obsahovat diakritiku, pokud to není nutné např. z důvodu přenosu textu chybové zprávy z programu a jeho prostředí.

Popis polí provozního logu:

Název	Popis
time_stamp	Datum a čas zápisu záznamu ve formátu dle kapitoly <a href="#">5.1.3.1 Časové razítko</a>

při zpracování. Vlastní logování zpracovávaných osobních údajů (subjektů), kterých se daná transakce týká zajistí komponenta, která je původcem dané transakce

severity	Hodnocení závažnosti události viz níže.
Proces	Proces, ke kterému se vztahuje událost, nepovinné
object	objekt, který je zdrojem zprávy (např. program, název certifikátu, apod.), nepovinné
text	text zprávy, obsahující popis události a případné chyby

#### 5.5.2.1 Závažnost provozní události podle výsledku operace

Závažnost	Popis
Critical	Fatální chyba, např. nemožnost spustit operaci, kdy je nutný zásah v co nejkratší době.
Major	Výsledek operace je selhání operace, např. neúspěchu posledního z pokusů o přenos, kdy je nutný zásah, např. manuální zpracování.
Minor	Neúspěch běhu operace, operace bude opakována, nebo nastala dílčí chyba, která nemusí znamenat neúspěch celé akce. Je žádoucí kontrola průběhu.
Warning	Zjištění problémů u operace s úspěšným výsledkem nebo jiná upozornění, která vyžadují příležitostné prověření.
Normal	Úspěšné dokončení operace.

## 6 Provozní standardy

### 6.1 Monitoring

Vlastník kapitoly: OTP OCD

#### 6.1.1 Rozsah monitoringu a používané nástroje

Rozsah monitoringu a používané monitorovací nástroje jsou popsány v dokumentu Stav IS VZP.

#### 6.1.2 Používané dohledové nástroje pro On premise řešení

Centrální systém dohledu provozu informačního systému je vybudován na platformě **HP Operations Manager** (HP OM). Do dohledového centra HP OM (centrální konzole) jsou soustředovány všechny důležité zprávy z ostatních monitorovacích nástrojů.

**HP OM** – agent na úrovni OS, centrální konzole

**HP OM Performance Manager (PM)** – sledování vytíženosti systémů

**Oracle Enterprise Manager Cloud Control (OEM)** – agent, integrace vybraných událostí do HP OM

**Microsoft System Center 2012 Operations Manager (SCOM)** – agent na úrovni OS, integrace vybraných událostí do HP OM

**Nagios** – bezagentní, s integrací vybraných zpráv do HP OM

**HP Business Service Management (HP BSM)** – integrace do HP OM

- **Business Process Monitor (BPM)** – aktivní aplikační monitoring

**HP Network Node Manager i (HP NNMi)** – aktivní SNMP poll, pasivní SNMP trap, je integrován s HP OM

**HP SiteScope** – bezagentní, integrace do HP OM a HP BSM

Není-li možné nasadit monitoring pomocí zavedených nástrojů, poskytne dodavatel v rámci dodávky aplikace monitorovací nástroj (například skript), jehož výstup lze integrovat do HP OM.

### 6.1.3 Požadavky na procesy z hlediska monitoringu

Aplikační monitoring musí být součástí nasazovaného systému.

Kritické a závažné chybové stavy procesů/aplikací, které brání jejich provozu, dále chyby automatizovaných a dávkových zpracování musejí být zapisovány do aplikačního logu. Formát logu je popsán v kapitole 5.5 Provozní log.

Obchodně kritické procesy by měly mít implementovanou striktně čtecí roli pro technologického uživatele monitoringu, pokud tomu nebrání samotná povaha procesu (např. plně aktivní operace). Tato role musí umožnit i odstraňování případných sestav vytvářených uživatelem.

Součástí akceptačních testů musí být ověření funkčnosti monitoringu.

### 6.1.4 Požadavky na návrh monitoringu

Každá nově dodávaná aplikace nebo komponenta infrastruktury musí být monitorována, a to před nasazením do provozu. Návrh sledování dostupnosti, resp. chybovosti, jakož i výkonnosti musí být součástí projektových dokumentů (analýzy, technického designu, funkčního designu, implementační dokumentace) a zejména administrátorské a provozní dokumentace.

Návrh monitoringu vychází z doporučení dodavatele a je vypracován v součinnosti s VZP. Musí vycházet z popisu systémů, služeb a procesů aplikace, včetně návazností na ostatní systémy, a musí obsahovat zejména:

- způsob zjišťování stavu každé důležité komponenty / služby aplikace,
- návrh prahových hodnot nebo ukazatelů stavu,
- závažnost zjištěné události,
- prioritu řešení události,
- instrukce k řešení události.

Řešení monitoringu musí být navrženo tak, aby sledovaných událostí bylo co nejméně a sledování bylo proaktivní; události musejí včas upozornit na mezní stavy, aby bylo možné s předstihem zabránit výpadku služby, avšak nikoli za cenu inflace nevýznamných zpráv.

V HA aplikacích je nutné popsat režim, v němž jsou redundantní komponenty konfigurovány (loadbalance / failover) a určit závažnosti výpadků komponent a souvislosti kombinací těchto výpadků.

### 6.1.5 Požadavky na rozhraní pro monitoring

Všechny servery musejí na úrovni operačního systému umožňovat nasazení některého z agentů používaných dohledových nástrojů; spolu s agentem budou implementovány standardizované šablony s nastavenými prahovými hodnotami, které je možné na základě doporučení dodavatele upravit.

Všechna klíčová síťová zařízení musejí mít implementován protokol SNMP v. 3+ s možností hlášení událostí pomocí SNMP TRAP i GET, a s dostupnou MIB.

V případě monitorování pomocí logů (systémových, aplikačních apod.) musí být log vytvořen podle kapitoly [5.5 Provozní log](#)

## 6.2 Zálohování a archivace

Vlastník aplikace: OTP OSSU

Všechna DC jsou zálohována jedním společným zálohovacím subsystémem (dále jen ZS).

### 6.2.1 Zálohovací systém

ZS je tvořen těmito komponentami:

- Řídící SW „Data Protector“.
- Cluster dvou serverů v oddělených lokalitách, na nichž je řídicí SW provozován.
- HW pro ukládání zálohovaných dat, umístěný rovněž ve dvou různých lokalitách (DC), dostupný pomocí LAN a SAN infrastruktury. Jsou používány robotické páskové knihovny, které mohou být v případě potřeby doplněny o jiný HW (např. typu B2D), připojitelný pod řídicí zálohovací software.

Zálohování probíhá tak, aby byla respektována bezpečnostní zásada „3-2-1“ (tj. „důležitá data musí existovat 3x, ve 2 různých datových formátech, 1 kopie ve druhé lokalitě“) dle příslušné třídy aplikace.

### 6.2.2 Požadavky na aplikační celky z pohledu jejich zálohování:

Aplikace musí být navržena tak, aby:

- SW a HW komponenty aplikačních celků byly zálohovatelné technologiemi, které má VZP ČR v době nasazení aplikace a během jejího provozování k dispozici, v souladu s bezpečnostními standardy VZP ČR. Zálohovatelné musí být všechny SW komponenty a datové objekty potřebné pro činnost aplikace, a to s ohledem na předpokládané datové objemy, případné odstávky, propustnost potřebné infrastruktury a dobu potřebnou pro provedení záloh. Součástí dodávky aplikace musí být i analýza vývoje předpokládaných zálohovaných datových objemů.
- Umožňovala a podporovala datové odklady na jiná úložiště nebo zálohovací média. Musí tedy umět připravit data určená k odkladu/archivaci (např. umístit je do dohodnuté lokace, vhodně je pojmenovat, ...) a vést o nich potřebnou evidenci po provedení odkladu. Musí být také možné v případě potřeby takto odložená data po jejich obnově aplikaci opět zpřístupnit.
- Bylo možné omezit pravidelně zálohovaný datový objem (uspořádání dat do read-only datových objektů, které po jejich finální záloze sice mohou ležet na discích, ale již se dále nezálohují).
- Bylo možné identifikovat změny v datech, provedené od poslední zálohy
- Hodnoty parametrů RTO a RPO pro aplikační celky byly v souladu s platnými D+R a BC plány VZP ČR, a to i s ohledem na budoucí očekávané zálohované/obnovované datové objemy a datovou propustnost příslušné infrastruktury.
- Je-li pro tvorbu záloh třeba odstávka, součástí dodávky musí být potřebné nástroje, které umožní takové zálohy provádět automatizovaně.
- Jsou-li pro zálohování třeba nějaké další SW komponenty (přípravné scripty, programy třetích stran, ...), musí být také součástí dodávky aplikace.
- Je-li pro zálohování některé části aplikačního celku potřeba příslušná zálohovací licence pro požadovaný typ zálohy (typicky pro online zálohy DB, Exchange, ...), při nových dodávkách aplikačních celků ji zajišťuje VZP ČR, dodavatel aplikace však vždy musí v nabídkách a dalších dokumentech specifikovat, jaké typy záloh (s ohledem na námi používané technologie) budou požadovány.

Vysvětlivky:

*RTO = Recovery Time Objective ... doba výpadku postižených služeb v případě obnovy*

*RPO = Recovery Point Objective ... k jakému času lze data obnovit, která data bude třeba po obnově nahradit (datové změny od poslední zálohy), případně která nahradit nepůjdou*

### 6.3 Definice provozních parametrů služby/aplikace (SLA)

Vlastník kapitoly: OTP OSAD

SLA a provozní parametry příslušné aplikace/domény budou součástí v technické specifikace příslušné komponenty (definované smluvně).

Využívané hodnoty:

**Provozní doba aplikace** – doba, kdy běží servery a aplikace

Režim provozní doby (7x24, 7x16, 5x16, 5x8)

**Podporovaná provozní doba** - doba, kdy provozní oddělení IT VZP zajišťuje personálně provoz aplikace

Režimy podporované provozní doby: 7x24, 7x16, 5x16, 5x8

**Doba podpory externím dodavatelem** - doba, po kterou je dostupná podpora dodavatele

Režim doby podpory externím dodavatelem (7x24, 7x16, 5x16, 5x10, 5x8)

**Servisní okno** - servisním oknem se rozumí vymezený časový rámec mimo provozní dobu služby na údržbu systému.

Režim servisních oken

1. Po 18:00 - 24:00 HW údržba
2. Út 18:00 - 24:00 SW údržba
3. St 18:00 - 24:00 HW údržba
4. Čt 18:00 - 24:00 SW údržba

**Podpora Helpdesk** - standardní doba Helpdesku pro uživatele a řešitele -

Režim podpory Helpdesku

5. Po – Čt 07:00 - 17:00
6. Pá - 07:00 – 15:00

**Požadovaná dostupnost aplikace** – Dostupnost aplikace/služby koncovým uživatelům v procentech.

**Požadovaná doba odezvy** - časový interval mezi akcí uživatele a odezvou systému.

**Požadovaná spolehlivost** - střední doba mezi výpadky

Střední doba mezi obnovením služby po výpadku a vznikem nového výpadku dané služby. Uvádí se ve dnech.

### 6.4 Podmínky převzetí do rutinního prostředí a aplikační podpory

- Aplikace/služba je řádně otestovaná s příslušnou testovací dokumentací a akceptačními protokoly za jednotlivé druhy testů.
- Rutinní operace jsou plně automatizované (vyžadují pouze prvotní nastavení a následnou pravidelnou kontrolu), manuální operace jsou max. eliminovány (např. manuální kopírování dat v případě provozní chyby).

- Aplikace/služba je připravena k monitoringu všech funkcionalit, veškerého HW, SW a DB a je připravena k využití stávajících monitorovacích nástrojů.
- Aplikace/služba musí být předána dle standardního procesu předání aplikací do provozu včetně kompletní provozní dokumentace dle požadované struktury
- Aplikace/služba je dodána s kompletní dokumentací provozní i uživatelskou, včetně „Předávacích tabulek“ (přílohou standardů). K aplikaci/službě je dodán instalační postup a konfigurační příručka, podle kterých je možné jednoznačně aplikaci/službu instalovat a konfigurovat, bez jakýchkoliv manuálních zásahů.
- Po provedení instalace aplikace/služby dle dokumentace a instalačních postupů je stav aplikace/služby plně funkční, dle požadavků odběratele.
- Aplikace/služba je v době 1 měsíce od nasazení do produkčního prostředí v pilotním provozu, kdy se vyžaduje zvýšená podpora dodavatele
- Aplikaci/službu je po splnění a dodání výše uvedených bodů možné převzít do plného rutinního prostředí a následné aplikační podpory.

viz přílohy:

P5\_předávací\_Tabulky\_produkčního prostředí

P5a\_předávací\_Tabulky\_testovací\_prostředí

## 6.5 Vazba na ITIL procesy

Vlastník kapitoly: OKP

Aplikace musí být zařazena ve VZP do standardních ITIL procesů.

### 6.5.1 Definování veškerých eskalačních procedur u aplikace - správa HelpDesku/ServiceDesku

- Kritičnost aplikace
- Obnovení provozu
- Rozpoznání nestandardní situace
- Eskalační procedura

### 6.5.2 Zavedení aplikace do incident managementu

Aplikace musí být zavedena do procesu Incident Managementu.

### 6.5.3 Zavedení aplikace pod standardní řízení změn - change management

Aplikace musí být zavedena do procesu Change Managementu, který má následující části:

- Požadavek a zadání změny
- Schvalovací proces změny
- Realizace změny a předání úpravy aplikačního softwarového vybavení (dále zkratkou ASW) podle pravidel release managementu (uvedeno v následující kapitole)
- Nasazení změny ASW a akceptace v rámci procesu test managementu
- Podle objemu a závažnosti zakázky je může být celý proces projektově řízen.

### 6.5.4 Zavedení aplikace do release plánů - release management

Aplikace musí být zavedena do procesu Release Managementu.

Ve VZP používáme toto rozdělení release:

- malý - malé změny, bez dopadu do integrace
- velký - velké funkční změny
- mimořádný – mimo termín release plánu – např. legislativou vynucené změny...



Pro každou komponentu ASW se v rámci dohody mezi dodavatelem a ICT VZP ČR nastaví release plán.

## 7 Seznam příloh

- Příloha 1: Vzor\_Predavaci\_tabulky\_PP (produkční prostředí)
- Příloha 2: Vzor\_Predavaci\_tabulky\_TP (testovací prostředí)
- Příloha 3: Integrace aplikace do IDM (Identity management)
- Příloha 4: Integrace aplikace s CSČ (Centrální správa číselníků)
- Příloha 5: Popis integračních vazeb prostřednictvím IPF a metodika realizace integračních vazeb

## 8 Výjimky ze standardu

### 8.1 Integrace se stávajícím IS

- Příloha 3: Integrace aplikace do IDM (Identity management)
- Příloha 4: Integrace aplikace s CSČ (Centrální správa číselníků)
- Příloha 5: Popis integračních vazeb prostřednictvím IPF a metodika realizace integračních vazeb

# Stav IS VZP

**UPOZORNĚNÍ:**

Tento dokument je zpracován Všeobecnou zdravotní pojišťovnou České republiky (dále též jen „VZP ČR“ nebo „VZP“). Všeobecná zdravotní pojišťovna České republiky jej uveřejňuje v rámci zadávací dokumentace jí zadávaných veřejných zakázek. Tento dokument umožňuje vytvořit si představu o standardech informační architektury ICT VZP ČR. Účelem jeho uveřejnění je poskytnout informace nezbytné pro integraci dodávané komponenty se stávajícím informačním systémem v souladu se Standardy ICT- VZP- NIS.

Uveřejněním tohoto dokumentu není dotčena právní odpovědnost spojená s jeho zneužitím.

V tomto dokumentu bylo použito názvů subjektů a názvů produktů, které mohou být chráněny příslušnými právními předpisy.

**Otevřením tohoto dokumentu berete výše uvedené skutečnosti na vědomí.**

## Verze dokumentu

Verze	Datum	Autor	Popis
0.9	11.3.2019	Juraj Boldiš	Založení dokumentu ze Standardu verze 1.09
1.0	22.5.2019	Roman Palkovič (OTP)	Připomínkování a zpracování úprav dokumentu
1.0.1	14.6.2019	Juraj Boldiš	Zpracovány připomínky M. Škopa

# Obsah

<b>1. ÚVOD .....</b>	<b>6</b>
<b>2. APLIKAČNÍ KOMPONENTY .....</b>	<b>7</b>
2.1.1. Integrace se stávajícím IS.....	7
<b>3. INFRASTRUKTURA VZP .....</b>	<b>8</b>
3.1. HW.....	8
3.1.1. On Premise Serverová infrastruktura .....	8
3.1.2. Cloudová infrastruktura .....	8
3.1.2.1. IAAS - využívané služby.....	8
3.1.2.2. PAAS využívané služby.....	8
3.2. Sítě.....	9
3.2.1. Celkové schéma sítě VZP ČR .....	9
3.2.2. LAN RP a KLIPRů .....	10
3.2.3. Bezdrátová síť (WIFI).....	11
3.2.5. Datová centra On premise.....	12
3.2.6. Perimetr .....	13
3.2.7. Síťové služby.....	14
3.2.8. Sjednocená komunikace.....	14
3.3. OS .....	14
3.3.1. OS pro aplikace třídy A .....	14
3.3.2. OS pro aplikace třídy B .....	14
3.3.3. Prostředí pro virtualizaci .....	14
3.4. Middleware .....	15
3.4.1. Integrovaná platforma .....	15
3.4.2. Aplikační servery .....	15
3.4.3. Webové servery .....	15
3.5. Virtualizovaná infrastruktura pro hostování aplikací.....	16
3.6. Deployment aplikací provozovaných on-Premise do prostředí v DC.....	16
3.7. Datové a databázové služby .....	17
3.6. Popis standardního koncového zařízení .....	18
3.7. Elektronická pošta .....	19
3.8. Active Directory .....	20
3.9. PKI .....	20
<b>6. PROVOZNÍ PROSTŘEDÍ .....</b>	<b>21</b>
6.1. Monitoring .....	21
6.1.1. Rozsah monitoringu .....	21
6.1.2. Používané dohledové nástroje pro On premise řešení.....	21

---

<b>6.2. Zálohování a archivace .....</b>	<b>22</b>
<b>6.2.1. Zálohovací systém.....</b>	<b>22</b>
<b>6.2.2. Zálohovací architektura.....</b>	<b>22</b>

## Seznam obrázků

Obrázek 1 - Celkové schéma sítě VZP ČR.....	10
Obrázek 2 - Schéma propojení datových center .....	12
Obrázek 3 – Schéma deploymentu datových center .....	17
Obrázek 4 - Schéma zálohovacího systému VZP ČR .....	22

## 1. Úvod

# STAV IS VZP

- **Shrnuje aktuální stav aplikačních komponent** – poskytuje přehled o aplikačních komponentách, které jsou možné využít pro, rozvoj a budování IS VZP ČR.
- **Popisuje aktuální stav infrastruktury** – dává přehled o infrastruktuře, kterou v současnosti VZP využívá

## 2. Aplikační komponenty

### 2.1.1. Integrace se stávajícím IS

Ke dni vzniku tohoto dokumentu VZP provozuje stávající IS řízený historickou verzí standardu. Způsob integrace s tímto IS je proto prováděn dle původního standardu, stav je popsán v následujících přílohách.

- Příloha 3: Integrace aplikace do IDM (Identity management)
- Příloha 4: Integrace aplikace s CSČ (Centrální správa číselníků)
- Příloha 5: Popis integračních vazeb prostřednictvím IPF a metodika realizace integračních vazeb



### 3. Infrastruktura VZP

#### 3.1. HW

##### 3.1.1. On Premise Serverová infrastruktura

Základem serverové infrastruktury, centralizované a provozované v rámci datových center (DC), jsou servery nebo serverovými systémy založené na architektuře procesoru Intel Itanium a x86. Servery jsou certifikovány na operační systémy uvedené v kapitole 3. 3., jsou rozšiřitelné, maximálně flexibilní a vysoce dostupné. Jednotlivé servery nebo serverové systémy jsou připojeny do sítě LAN a v případě komunikace s diskovými poli i do sítě SAN a vybaveny kvalitními nástroji pro správu. V případě používání virtualizace uvedené v kapitole 3. 3. je hardware management propojen s virtualizační vrstvou. Servery nebo serverové systémy jsou v provedení blade nebo rackmount a v datových centrech jsou umístěny v rackových skříních velikosti 42U. Napájení rackových skříní se odvíjí od spotřeby zařízení, která jsou v něm umístěna.

Standardem pro připojení fyzických serverů do sítě LAN v datových centrech je:

- Management konzole, 1x1GE, access
- Management interface, 2x1GE, acces, active-standby
- Datový interface, 2x10GE, trunk, active LACP

##### On Premise SAN infrastruktura

V jednotlivých datových centrech jsou disková enterprise a midrange pole, která jsou zapojena do SAN infrastruktury pomocí SAN přepínačů. Potřebná kapacita diskových polí je řešena rozšířením těchto polí nikoliv nákupem dalších polí. Do této SAN infrastruktury jsou z důvodu vysoké propustnosti a kvalitního zabezpečení (využití alternativních cest) zapojeny všechny významné servery, zálohovací knihovny a zmíněná disková pole. Tato SAN síť využívá u všech významných komponent minimálně 2 FC rozhraní pro zajištění vysoké dostupnosti.

##### 3.1.2. Cloudová infrastruktura

Je využíván jeden cloudový poskytovatel - Microsoft a tedy spravujeme a využíváme jedno cloudové prostředí - Azure. Do listopadu 2019 můžeme využívat pouze služby, které jsou definovány smlouvou, není tedy možné využít jakoukoliv službu, následně bude možné využívat vše. Níže jsou vyjmenovány služby, které využíváme pro provoz e-VZP aplikací a veřejného webu.

###### 3.1.2.1. IAAS - využívané služby

Azure Virtual machine

Azure Virtual machine scale set

###### 3.1.2.2. PAAS využívané služby

Azure Storage – blob, queue, table, files

Azure SQL database

Azure Appservice

Azure CDN

Redis Cache

Service Bus

Key Vault

Notification HUB

Log Analytics

Service Fabric

Sendgrid

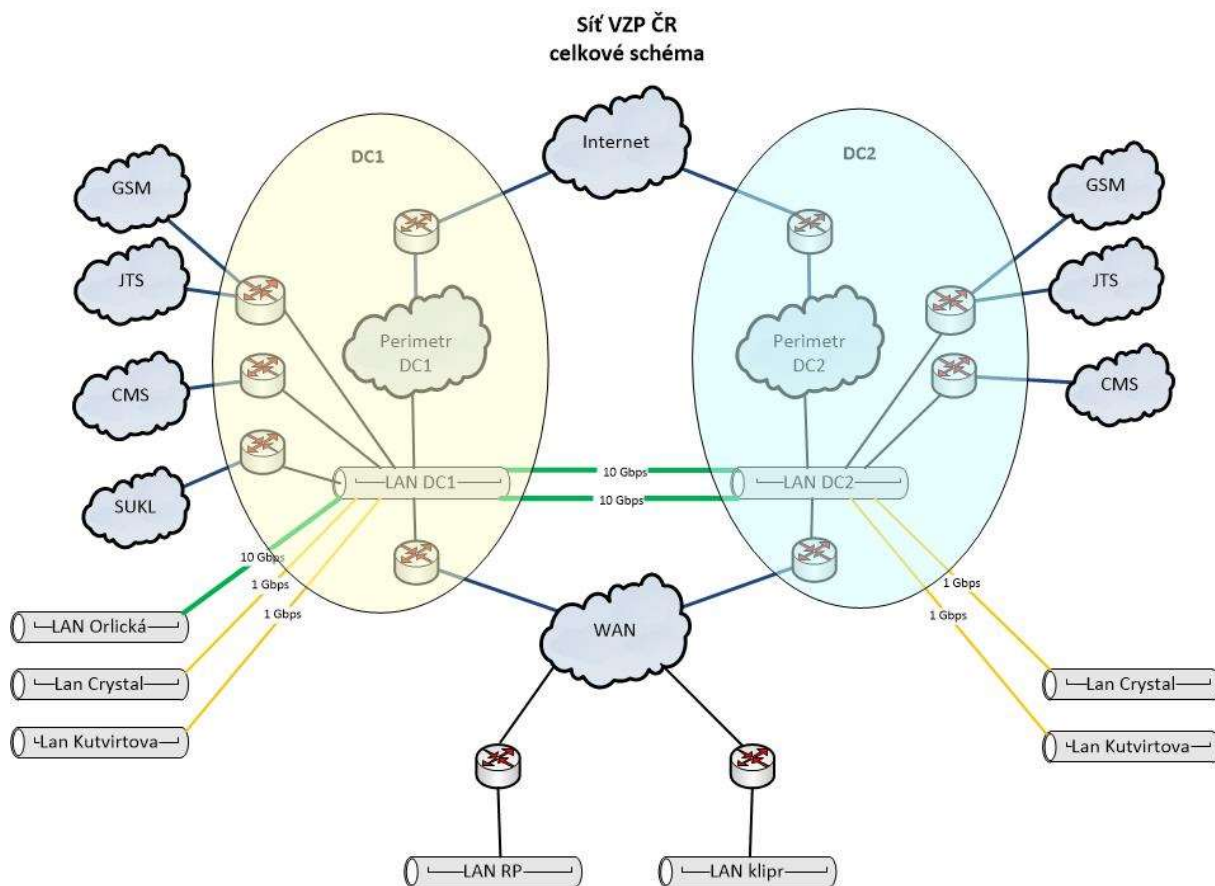
### 3.2. Síť

#### 3.2.1. Celkové schéma sítě VZP ČR

Z hlediska vztahu k uživatelům a k okolnímu světu je možné počítačovou síť VZP ČR rozdělit do několika funkčních celků:

- **Perimetr**
- **Datová centra**
- **WAN síť**
- **LAN sítě ústředí, regionálních poboček a kliprů(klientských pracovišť)**

Schematicky je síť VZP ČR znázorněna na následujícím obrázku:



Obrázek 1 - Celkové schéma sítě VZP ČR

<b>CMS</b>	Centrální místo služeb
<b>GSM</b>	Globální Systém pro Mobilní komunikaci
<b>JTS</b>	Jednotná telefonní síť
<b>SUKL</b>	Státní úřad pro kontrolu léčiv
<b>RP</b>	Regionální pobočka
<b>KLIPR</b>	Klientské pracoviště
<b>DC1</b>	Datové centrum 1 na adrese Orlická 4/2020, 130 00 Praha 3
<b>DC2</b>	Datové centrum 2 na adrese ČD Telematika, Pod Táborem 369/8a, 190 00 Praha 9
<b>LAN Orlická</b>	Ústředí na adrese Orlická 4/2020, 130 00 Praha 3
<b>LAN Crystal</b>	budova Crystal na adrese, Vinohradská 2577/178, 130 00 Praha 3
<b>LAN Kutvirtova</b>	Call Centrum a klipr na adrese Kutvirtova 339/5, 150 00 Praha 5

### 3.2.2. LAN RP a KLIPRů

LAN ve VZP ČR je rozdělena do vrstev podle hierarchického modelu:

- **Access (přístupová) vrstva** – zajišťující konektivitu koncových uživatelů
- **Distribution (distribuční) vrstva** – zajišťující vysokou dostupnost
- **Edge (hraniční) vrstva** – slouží pro připojení LAN do WAN

## SLUŽBY A TECHNOLOGIE LAN

- VLAN
- QoS

### VLAN

VLANy jsou implementované v přístupové vrstvě. Uživatelé z různých oddělení, rozdělení do určených VLAN, mohou přistupovat do sítě určenými přístupovými přepínači, které jsou umístěny v různých podsítích. V hraniční, případně distribuční, vrstvě je nakonfigurované směrování těchto podsítí mezi sebou a také případné omezení provozu mezi VLANami pomocí ACL – Access Control List (přístupových listů).

### QoS (QUALITY OF SERVICE)

QoS zajišťuje rovnoměrné vyvažování zátěže sítě s ohledem na druh přenášených dat, spravedlivě rozděluje konektivitu mezi jednotlivé aplikace dle nastavených priorit a zabraňuje přetížení sítě.

Ve VZP ČR jsou použity následující **QoS** třídy, které jsou řazeny dle priority – od nejvyšší priority po nejnižší prioritu.

- Třída – Network support
- Třída – Real time (VoIP RTP, VoIP Signalizace)
- Třída – 3B: Interaktivní provoz (terminálová třída) – (Aplikace Interaktivní)
- Třída – 3A: Web provoz (webová třída)
- Třída – 3D: Scavenger třída (DoS, P2P, ...) – Služby UDP (Bulk)
- Třída – Zbytková třída – ostatní provoz

#### 3.2.3. Bezdrátová síť (WIFI)

Bezdrátová síť ve VZP ČR je provozována na standardních zařízeních a technologii firmy Cisco. Bezdrátová síť poskytuje několik variant připojení:

- **WLAN\_DATA** – síť určená pro standardní uživatele interní sítě VZP, je veřejně inzerovaná. Tato síť je určená pro běžného uživatele a jsou na ni implementována bezpečnostní omezení.
- **WLAN\_ADMIN** – síť určená pouze pro administrátory sítě. Síť není veřejně inzerovaná (má vypnuto vysílání SSID).
- **WLAN\_PHONE** – síť určená pro připojení mobilních telefonů a pro volání po bezdrátové síti. Síť není veřejně inzerovaná (má vypnuto vysílání SSID). Přístup do sítě je ověřen pomocí MAC adresy zařízení.
- **WLAN\_GUEST** – síť určená pro připojení externích uživatelů s přístupem pouze do Internetu pomocí protokolu HTTP (S). Tato síť je veřejně inzerovaná.
- **WiredGuest** – jedná se o drátovou síť, která je řízená prostředky bezdrátové sítě a funguje obdobně jako síť WLAN\_GUEST s tím rozdílem, že klient se místo k bezdrátové síti připojuje do portu přepínače.  
Tuto síť je možno využívat pouze v centrálních lokalitách – Orlická, Perštýn.  
Tato síť určená pro připojení externích uživatelů s přístupem pouze na Internet.

#### 3.2.4. WAN

VZP ČR provozuje privátní datovou síť WAN na přenosových prostředcích poskytovatele datového připojení pomocí technologie MPLS. Pro zajištění bezpečnosti přenášených dat je použito šifrování na

síťové vrstvě mezi koncovými zařízeními pomocí protokolu IPSec. Pro navazování šifrované komunikace mezi směrovači v síti VZP ČR je použita technologie GET (Group Encrypted Transport) VPN.

### Šířka pásma

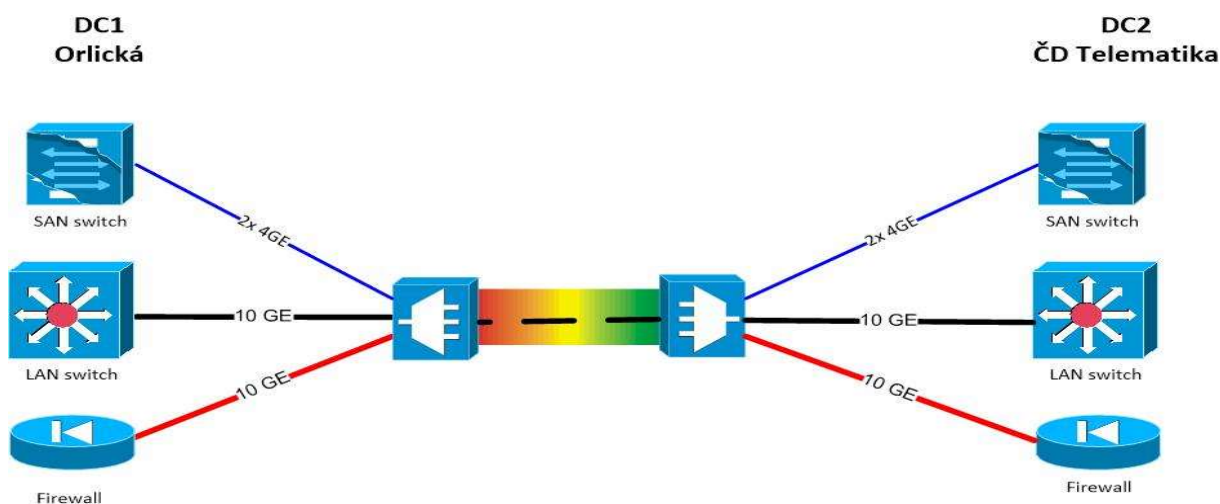
Typ pobočky	Počet uživatelů	Šířka pásma
1	1-5	0,5 Mbps
2	6 -50	4 Mbps
3	51 a více	8 Mbps

### 3.2.5. Datová centra On premise

VZP ČR provozuje dvě geograficky oddělená datová centra:

- DC1 na adrese Orlická 4/2020, 130 00 Praha 3
- DC2 na adrese ČD Telematika a.s., Pod Tábořem 369/8a, 190 00 Praha 9

Obě datová centra jsou propojena dvěma nezávislými optickými trasami technologií DWDM. Jedna vlnová délka o kapacitě 10 Gbps je použita pro LAN provoz a druhá 10 Gbps pro propojení firewall clusteru. Pro propojení SAN přepínačů jsou multiplexovány dva kanály, každý o kapacitě 4 Gbps.



Obrázek 2 - Schéma propojení datových center

Každé z datových center VZP ČR je vytvořeno na technologii firmy Cisco Nexus dle architektury Spine and Leaf a patří mezi tzv. aplikačně řízené infrastruktury (Application Centric Infrastructure (ACI)), které umožňují integrovat do řízení síťového provozu datového centra vlastní logiku jednotlivých aplikací z pohledu jejich požadavků na síťovou konektivitu, bezpečnost a L4-L7 služby (load balancing, firewalling atd.). Fyzické nebo virtuální aplikační servery sdílející stejnou bezpečnostní a síťovou politiku jsou konsolidovány do logických skupin a současně je definována jejich vzájemná komunikace (která aplikační komunikace je povolena, jaké vyžaduje QoS parametry a jaké vyžaduje L4-L7 služby).

Veškeré aplikační politiky jsou definovány na centrálním kontroleru (Application Policy Infrastructure Controller - APIC), který je s využitím otevřených aplikačních rozhraní automaticky distribuuje na jednotlivé komunikační prvky a systémy, které následně podle těchto aplikačních politik řídí síťový provoz.

## Logická infrastruktura

Provoz datového centra je z pohledu toku dat směrem od uživatele k vlastním datům rozdělen do jednotlivých funkčních modulů neboli zón. Rozhodujícím hlediskem pro sledování toku dat je „kdo inicializuje komunikaci“.

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:

#### – Síť VZP ČR (VZP NET)

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

#### – Demilitarizovaná zóna (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. Do této zóny patří vrstva správy a administrace a vrstva infrastrukturních serverů.

#### – Prezentační vrstva (DC-VIP)

Jedná se o vrstvu, v které jsou umístěné servery zajišťující komunikaci s uživateli. Patří sem i virtuální IP adresy, které reprezentují jednotlivé aplikace pro přístup jak z VZP NET, tak z ostatních aplikací DC.

#### – Aplikační vrstva (DC-APP )

Zde jsou umístěny aplikační servery zajišťující business logiku jednotlivých aplikací.

#### – Databázová vrstva DC (DC-DB)

Umístění DB serverů. L2 vrstva rozprostřená geograficky mezi lokalitami DC1 a DC2. V databázové vrstvě je možné vytvářet clustery se společnou IP adresou mezi jednotlivými lokalitami.

#### – Servisní zóna (DC-SERVIS)

Zóna slouží jako prostředník pro výměnu dat mezi ostatními zónami a mezi prostředím produkce a test.

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.

	Komunikace do zóny →					
Komunikace ze 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

### 3.2.6. Perimetr

Perimetr je zabezpečená oblast podnikové sítě, která leží mezi internetem a vnitřní sítí VZP ČR. Perimetr je rozdělen pomocí bezpečnostních bran (firewallů) do několika oddělených bezpečnostních zón:

- vnější perimetr – bezpečnostní oddělení externích sítí (Internetu) od sítě VZP
- vnitřní perimetr – bezpečnostní oddělení veřejně vystavených služeb VZP od vnitřní (uživatelské) sítě VZP

Součástí řešení je i VPN přístup do VZP ČR. VPN slouží pro vzdálený přístup zaměstnanců a externích kontraktorů do sítě VZP ČR z Internetu.

### 3.2.7. Síťové služby

Síť VZP ČR poskytuje pro koncová zařízení, aplikace a uživatele následující služby:

- Časová synchronizace (NTP)
- Kvalita služby (QoS)
- DNS, DHCP, IPAM (DDI)
- Loadbalancing

### 3.2.8. Sjedená komunikace

Sjedená komunikace je ve VZP ČR tvořena následujícími součástmi:

- **Hlasová komunikace**
  - IP Telefonie
  - Integrované nadstavbové funkcionality
  - Spolupracující systémy
    - Call Centrum Atlantis
    - Cisco Paging
- **Elektronická komunikace**
  - Instant messaging - Cisco Jabber
  - Webová konference – Cisco WebEx

## 3.3. OS

### 3.3.1. OS pro aplikace třídy A

- HP-UX 11.31, Red Hat Enterprise Linux, Oracle Linux, CentOS (verze 6.x a 7.x)
- MS Windows Server 2012R2 EN a novější

### 3.3.2. OS pro aplikace třídy B

HP-UX 11.31, Red Hat Enterprise Linux, Oracle Linux, CentOS (verze 6.x a 7.x)

MS Windows Server 2012R2 EN a novější

### 3.3.3. Prostředí pro virtualizaci

Hostitelský systém je hypervizor nebo operační systém s hypervizorem, který umožní provoz Virtuálních serverů. Podporované platformy jsou a ve VZP mohou být nasazeny technologie, VMWare vSphere 5.5 Enterprise a vyšší, HPVM, Oracle VM 3.4 a vyšší a MS Hyper-V 2012R2 a vyšší.

Řízení Virtuálních serverů - správa VMs na VMWare nástrojem VMWare vCenter Server 5.5 Standard a vyšší. Správa VMs na Hyper-V je realizována nástrojem SCVMM 2012R2 a vyšší.

Pro zajištění vysoké dostupnosti aplikací třídy A pro a realizaci DRP plánu slouží technologie VMware DRS a HA cluster, případně VMware SRM, VMware vSAN nebo MS Hyper-V Clustering, MS Storage Spaces Direct v aktuálních verzích.

Pro aplikace třídy A využívající softwarové produkty Oracle bude použita virtualizace Oracle VM.

U aplikací třídy B lze použít i další virtualizační technologií:

KVM (Kernel-based Virtual Machine)

### 3.4. Middleware

#### 3.4.1. Integrační platforma

- je založená na koncepci ESB (Enterprise Service Bus) jako podnikové sběrnice služeb
- pro realizaci integrace aplikací a služeb
- využívá centrální business rule repozitory a Business rule engine
- využívá principy servisně orientované architektury (SOA)
- využívá MOM architekturu (Message Oriented Middleware) jako podmnožinu ESB kde prostřednictvím Message brokera zajišťuje spolehlivé doručení zprávy nesoucí informaci (Message) mezi jednotlivými systémy (prostřednictvím front).
- využívá model řízení událostmi

#### Integrační platforma poskytuje tyto typy služeb:

- centrální řízení komunikaci mezi systémy realizované prostřednictvím ESB služeb,
- kompozice vlastních služeb a jejich publikace konzumentům
- zprostředkování a publikace sdílených služeb konzumentům,
- orchestraci služeb vnitřních i vnějších s ostatními integračními technologiemi (BPEL)
- směrování a předávání dat mezi jednotlivými službami
- transformaci formátů dat,
- konverze protokolů mezi jednotlivými službami,
- centrální business rule repozitory
- centrální repozitory služeb

#### 3.4.2. Aplikační servery

Výčet typů AS využívaných v IS VZP:

Druh AS	Použití
Oracle Fusion Middleware WebLogic Server v nejnovější podporované verzi	Aplikace deployované v J2EE, vhodné pro aplikace třídy A
JBoss aplikační server v nejnovější podporované verzi	Pro J2EE aplikace třídy B nebo v odůvodněných případech, kde není vhodné použití Oracle Weblogic J2EE.

#### 3.4.3. Webové servery

Výčet typů WS využívaných v IS VZP:

- Oracle Web Tier v nejnovější podporované verzi



- Apache v nejnovější podporované verzi
- IIS

### 3.5. Virtualizovaná infrastruktura pro hostování aplikací

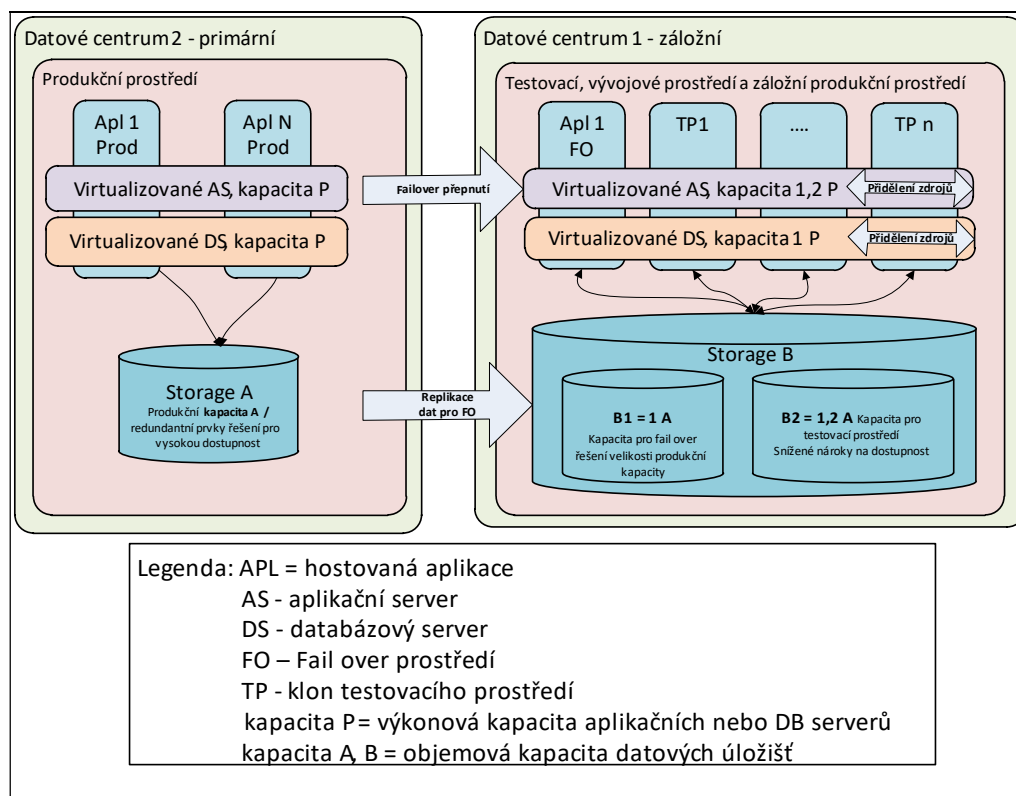
Aplikační služby jsou hostovány na virtuálních prostředí / serverech následujících parametřů:

Název služby	Popis
Server s OS	OS Windows nebo Linux (viz kap. 3.3 OS)
Aplikační server	OS Windows nebo Linux aplik. serveru Oracle Weblogic Suite
Databázový server Oracle	OS Linux, Oracle dB EE + RAC + partitioning
Databázový server MS SQL	OS MS Windows, MS SQL Server v edici Enterprise

### 3.6. Deployment aplikací provozovaných on-Premise do prostředí v DC

Pro zabezpečení provozu aplikací v prostředí datových center je používán standardizovaný deployment aplikací :

- Produkční instance aplikací a jejich odpovídajících dat je hostována v primárním datovém centru na zařízeních s vysokou dostupností a redundancí na virtualizované infrastruktuře.
- Záložní instance aplikací je hostována ve virtualizované infrastruktuře v záložním datovém centru s dedikovanou kapacitou úložiště o velikosti produkčních dat pro fail over primárního DC.
- Virtualizovaná infrastruktura serverů záložního centra je dimenzována jako výkonový ekvivalent zařízení v primárním datovém centru. Požadavek na dostupnost je nižší, tomu odpovídá nižší redundance prvků.
- Virtualizovaná infrastruktura záložního centra je sdílena s testovacími prostředími.
- Produkční data z primárního DC jsou asynchronně replikována do záložního DC.
- Pro účely testování je v záložním DC dedikována obecně kapacita virtualizované úložné kapacity až v rozsahu 1,2 velikosti produkčních dat sdílená pro všechny instance testovacích prostředí. Tato kapacita je alokována individuálně při návrhu systému.
- Kapacita úložiště Storage B musí být 2,2 násobkem kapacity úložiště produkčního prostředí Storage A
- Kapacita HW serverů pro databázovou a aplikační vrstvu musí být výkonově dimenzována jako 1,2 násobek produkčního prostředí (měřeno součtovým počtem jader, velikostí operační paměti virtuálních serverů a diskových úložišť pro aplikační a databázovou vrstvu). Redundance komponent není nutná.



Obrázek 3 – Schéma deploymentu datových center

### 3.7. Datové a databázové služby

#### 3.5.1. Databázové technologie

Standard	Popis
Oracle DB EE v nejnovější podporované verzi, včetně databázových options	Pro aplikace třídy A nebo B.
MS SQL EN v nejnovější podporované verzi, X64bit	Podpůrné služby a pro aplikace v třídě B. V odůvodněných případech je možné použít i pro aplikace třídy A.

#### 3.5.2. Datové a databázové standardy

Oblast standardizace	Popis
Minimum redundancí	Data jsou uložena v jediné databázi. Redundantní databáze v rámci lokality nejsou pro core business aplikace povoleny. Replikace se provádí pouze z důvodu realizace DR plánu..
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	<p>Návrh datového modelu DB musí být akceptován datovým architektem VZP ČR.</p> <p>Persistentní objekty vývojář definuje bez určení:</p> <ul style="list-style-type: none"> <li>• Názvu tablespace</li> <li>• fyzických atributů segmentu (pctused, pctfree, storage params,...)</li> </ul> <p>Databázové objekty jsou považovány za privátní součást aplikace, tzn. aplikace může přistupovat k databázovým objektům jiné aplikace pouze prostřednictvím dedikovaných služeb.</p>
Jmenné konvence databázových objektů	Všechna jména základních databázových objektů (tabulky, pohledy, balíky funkcí a procedur, fronty, sekvence, indexy, trigger apod.) začínají dvouznačným prefixem dodavatele
Kódování	<p>Preferované UTF16, UTF8,</p> <p>Definici collation – preferována Czech CI AS (case insensitive a accent sensitive)</p> <p>Na výjimku: ISO 8859-2, Windows 1250</p>
Podpora anonymizace / pseudonymizace osobních údajů	<p>Datová vrstva musí podporovat možnost anonymizace a pseudonymizace osobních údajů bez nežádoucí vlivu na chování datového engine a aplikace.</p> <p>Využívá se pro účely příslušné legislativy a vytváření datového derivátu pro testování z produkčních dat.</p> <p>Součástí dodávek je nástroj pro vytváření anonymizovaných derivátů produkčních dat (scrambling tool).</p> <p>Toto musí být zohledněno i v dokumentaci.</p>
Podpora řezů dat	<p>Datový model musí být navržen tak, aby pro účely testování bylo možno oddělit testovací derivát – vzorek dat z produkčních dat.</p> <p>Součástí dodávek je nástroj pro vytváření takových derivátů.</p> <p>Toto musí být zohledněno i v dokumentaci.</p>
Zakázané vazby	<p>Data v relačních databázích nesmí být provazována technologicky přes významové klíče, povolena je relační vazba pouze přes nezávislé technologické klíče záznamů.</p> <p>Nejsou dovoleny přímé datové vazby mezi datovými doménami.</p>

### 3.6. Popis standardního koncového zařízení

- Koncová pracovní zařízení počítače a notebooky
  - Instalován OS Windows enterprise 7 x32 /Windows 10 enterprise x64
  - Nastavení OS systému a uživatelského prostředí řízeno centrálně doménovou politikou.
  - Uživatel nemá na koncové zařízení administrátorské práva
  - Vzdálený přístup je zajištěn Remote Desktop, Support Assistant
  - Bezpečnostní aktualizace OS v 6 měsíčním cyklu
- Programové vybavení koncových pracovních zařízení
  - MS Office 2010/2016 /2019 Profesionál plus
  - Google Chrome, nastavení řízené centrální doménovou politikou

- IE aktuální verze 11, nastavení řízené centrální doménovou politikou
- 7ZIP
- Cisco AnyConnect Secure Mobility Client (Notebooky)
- Adobe Reader 11/DC
  
- Centrální distribuce programového vybavení na pracovní stanice
  - Distribuce SW je použitím SCCM
  
- Zabezpečení koncových pracovních zařízení
  - Endpoint Protection , Antivirová ochrana Kaspersky Endpoint Securit (centrálně řízený)
    - AntiMalware, IDS/IPS,
    - Firewall,
    - Application control,
    - Device control,
    - Antispam
  
- Jednotná adresářová struktura
  - Root:  
APPL  
Archiv  
Data  
Nezalohovano  
Program Files  
Temp  
TMP  
Users  
Windows
  - Pro Root, Program Files, Windows má běžný uživatel práva pouze pro čtení
  
- Ostatní programové vybavení
  - JAVA 1.6.045 ,1.7.51 , 1.8. a vyšší
  - NET Framework ver. 4.0 a vyšší
  
- Tisková koncová zařízení
  - Tisková a multifunkční zařízení připojená přes tiskový server, výjimečně lokální připojení
  - Follow me printing se zabezpečeným tiskem.
  - Ověřování pomocí bezkontaktních karet
  - (embedded čtečka v MFDnebo externí terminál, možnost ověření PINem).
  - Scan to me (možnost naskenovat z jakékoli MFD a obdržet sken v personální složce nebo emailem).
  
- Ostatní koncová zřízení
  - Mobilní telefony s OS : Android 5.0 a vyšší, Windows 10 mobile

### 3.7. Elektronická pošta

- Elektronická pošta ve VZP ČR je realizována prostřednictvím Microsoft Exchange server 2016. enterprise. Příjem elektronické pošty z Internetu zajišťují dedikované SMTP brány v perimetru, před předáním zpráv do interního poštovního systému je provedena jejich antivirová a antispamová kontrola. Odesílání pošty mimo lokální poštovní doménu probíhá pomocí SMTP protokolu s využitím poštovních bran.

- Klientský přístup k poštovnímu systému je zajištěn pomocí MS Outlook verze 2010 nebo vyšší, případně prostřednictvím internetového prohlížeče (Outlook Web App). Poštovní systém podporuje kromě SMTP i protokoly POP3 a IMAP.

Poštovní systém je využíván pro strategické řízení firmy, a proto je implementován jako vysoce dostupný.

### **3.8. Active Directory**

VZP ČR využívá pro ověřování uživatelů a pracovních stanic Microsoft Active Directory (dále AD). Služby AD jsou realizovány na serverech s MS Windows Server 2012 R2. V AD má každý uživatel i každá pracovní stanice svůj účet. Účty uživatelů jsou spravovány prostřednictvím Identity Managementu na základě údajů uložených v personálním systému. AD zajišťuje pomocí skupinových politik i nastavení pracovních stanic v souladu s platnými bezpečnostními standardy.

### **3.9. PKI**

VZP ČR využívá systém interních certifikačních autorit (PKI) založený na Microsoft Windows Server 2016. Vystavované certifikáty slouží pro identifikaci pracovních stanic a serverů v interní síti VZP ČR a dále pro podpis a šifrování elektronické pošty a pro vzdálený VPN přístup uživatelů do VZP ČR.

## 6. Provozní prostředí

### 6.1. Monitoring

#### 6.1.1. Rozsah monitoringu

Služba dohledu provozu informačního systému je centralizovaná a je zajišťována dohledovým centrem s dvousměnným provozem v pracovních dnech od 6:00 do 22:00 hod. (v režimu 5x16). V těchto časových úsecích jsou drženy pohotovosti řešitelských skupin pro síťovou infrastrukturu, operační systémy Unix, operační systémy Windows, Oracle infrastrukturu (databáze a middleware), provoz aplikací, Exchange, a pro dohledové nástroje.

Z hlediska teorie spolehlivosti IT systémů a služeb jsou sledovány a vyhodnocovány:

- chybovost, resp. dostupnost systémů a služeb (Availability) a jejich vytížení (Utilization),
- výkonnost služeb (Performance).

Z technicko-provozního hlediska je monitoring provozován ve dvou hlavních úrovních – infrastrukturní a aplikační.

- Infrastrukturní monitoring pokrývá všechny prvky produkční IT infrastruktury ZIS od síťových prvků přes servery, databáze až po middleware. Je vyhodnocována dostupnost, resp. chybovost, jakož i vytíženost sledovaných prvků.
- Aplikační monitoring je zaměřen na sledování klíčových služeb produkčních aplikací. Probíhá aktivně pravidelným spouštěním aplikačních úloh, simulujícím uživatelské akce. Zároveň jsou pasivně vyhodnocovány vybrané úlohy reálných uživatelů. Je vyhodnocována dostupnost úloh a služeb, a současně jsou zaznamenávány a vyhodnocovány odezvy takto měřených transakcí, tedy výkonost aplikací. Výstupy pasivního monitoringu jsou využitelné pro sledování vytíženosti sledovaných oblastí.

#### 6.1.2. Používané dohledové nástroje pro On premise řešení

Centrální systém dohledu provozu informačního systému je vybudován na platformě **HP Operations Manager** (HP OM). Do dohledového centra HP OM (centrální konzole) jsou soustřeďovány všechny důležité zprávy z ostatních monitorovacích nástrojů.

**HP OM** – agent na úrovni OS, centrální konzole

**HP OM Performance Manager (PM)** – sledování vytíženosti systémů

**Oracle Enterprise Manager Cloud Control (OEM)** – agent, integrace vybraných událostí do HP OM

**Microsoft System Center 2012 Operations Manager (SCOM)** – agent na úrovni OS, integrace vybraných událostí do HP OM

**Nagios** – bezagentní, s integrací vybraných zpráv do HP OM

**HP Business Service Management (HP BSM)** – integrace do HP OM

- **Business Process Monitor (BPM)** – aktivní aplikační monitoring

**HP Network Node Manager i (HP NNMi)** – aktivní SNMP poll, pasivní SNMP trap, je integrován s HP OM

**HP SiteScope** – bezagentní, integrace do HP OM a HP BSM

Není-li možné nasadit monitoring pomocí zavedených nástrojů, poskytne dodavatel v rámci dodávky aplikace monitorovací nástroj (například skript), jehož výstup lze integrovat do HP OM.

## 6.2. Zálohování a archivace

Všechna DC jsou zálohována jedním společným zálohovacím subsystémem (dále jen ZS).

### 6.2.1. Zálohovací systém

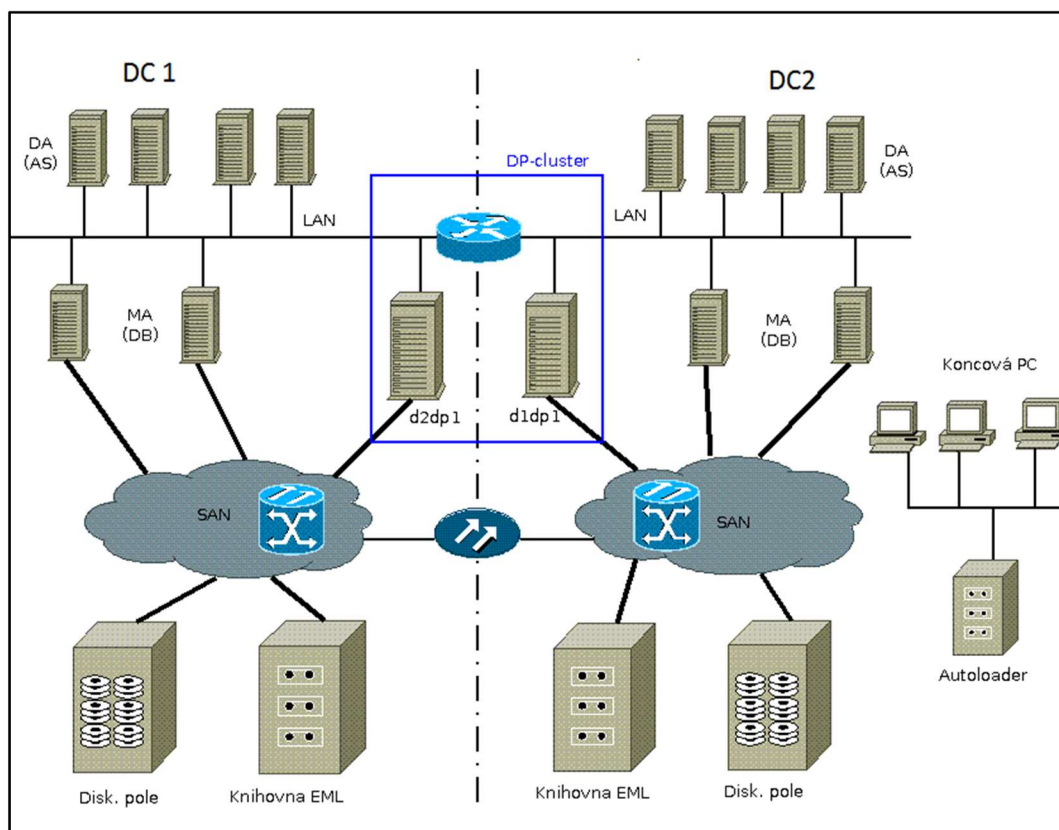
ZS je tvořen těmito komponentami:

- Řídící SW „Data Protector“.
- Cluster dvou serverů v oddělených lokalitách, na nichž je řídicí SW provozován.
- HW pro ukládání zálohovaných dat, umístěný rovněž ve dvou různých lokalitách (DC), dostupný pomocí LAN a SAN infrastruktury. Jsou používány robotické páskové knihovny, které mohou být v případě potřeby doplněny o jiný HW (např. typu B2D), připojitelný pod řídicí zálohovací software

Zálohování probíhá tak, aby byla respektována bezpečnostní zásada „3-2-1“ (tj. „důležitá data musí existovat 3x, ve 2 různých datových formátech, 1 kopie ve druhé lokalitě“) dle příslušné třídy aplikace.

### 6.2.2. Zálohovací architektura

Pro zálohování IS má VZP ČR k dispozici vysoce dostupný zálohovací systém s řídicím SW Micro Focus Data Protector. V každém datovém centru je k dispozici jedna pásková knihovna. Obě páskové knihovny jsou osazeny 8 kusy páskových mechanik (4x LTO4 + 4x LTO5, v budoucnu předpokládáme LTO7 a LTO8 a využití technologie B2D).



Obrázek 4 - Schéma zálohovacího systému VZP ČR

# **Integrace aplikace do IDM**

Příloha standardů a podmínek dodávek  
informačního systému VZP ČR



## UPOZORNĚNÍ:

Tento dokument je zpracován Všeobecnou zdravotní pojišťovnou České republiky (dále též jen „VZP ČR“ nebo „VZP“). Všeobecná zdravotní pojišťovna České republiky jej uveřejňuje v rámci zadávací dokumentace jí zadávaných veřejných zakázek. Tento dokument umožňuje utvořit si představu o standardech informační architektury ICT VZP ČR. Účelem jeho uveřejnění je poskytnout informace nezbytné pro integraci dodávané komponenty se stávajícím informačním systémem v souladu se Standardy ICT- VZP- NIS.

Uveřejněním tohoto dokumentu není dotčena právní odpovědnost spojená s jeho zneužitím.

V tomto dokumentu bylo použito názvů subjektů a názvů produktů, které mohou být chráněny příslušnými právními předpisy.

**Otevřením tohoto dokumentu berete výše uvedené skutečnosti na vědomí.**

## Obsah

1. Úvod .....	7
2. Integrace aplikace .....	7
2.1 Varianty integrace s IDM/OIM .....	9
2.1.1 Externí úložiště uživatelských dat (integrace s ADB nebo AD) .....	9
2.1.2 Vlastní úložiště uživatelských dat .....	10
2.2 OIM .....	12
2.3 ADB .....	13
2.3.1 Výhody použití ADB .....	14
2.3.2 Knihovna .....	15
2.3.3 Role .....	16
2.3.4 Lokality .....	16
2.4 Role .....	16
2.4.1 Metodika definování rolí .....	18
2.4.2 Kombinace „Role“ a „Pracovní úsek“ .....	19
2.5 ESSO LM .....	20
2.5.1 Spolupráce systémů OIM a eSSO .....	21
2.6 RAP .....	22
2.6.1 Integrace aplikace s RAP .....	23
2.7 GMUSERS – Katalog uživatelů .....	23
3. Fáze integrace aplikace .....	23
3.1 Kroky a zodpovědnosti během integrace aplikace do IDM řešení .....	25
4. PL/SQL API – komunikační rozhraní .....	26
4.1 Procedura Create User .....	26
4.2 Procedura UpdateUser .....	27
4.3 Procedura ChangePassword .....	27
4.4 Procedura LockUser .....	28
4.5 Procedura UnlockUser .....	28
4.6 Procedura DeleteUser .....	28
4.7 Procedura AddRole .....	29
4.8 Procedura RemoveRole .....	29
4.9 Návrátové kódy .....	29
5. Reference .....	30

## Seznam obrázků

Obrázek 1 - Přehled IDM komponent .....	9
Obrázek 2 – Integrace aplikace - externí úložiště.....	10
Obrázek 3 – Integrace aplikace - vlastní úložiště .....	11
Obrázek 4 - Schéma správy identity pomocí OIM .....	12
Obrázek 5 - Relační model ADB.....	13
Obrázek 6 - Řešení ADB .....	14
Obrázek 7 - Ukázka GUI ADB aplikace - seznam uživatelů.....	15
Obrázek 8 - Schéma využití knihovny ADLib.....	16
Obrázek 9 - Pyramida rolí .....	17
Obrázek 10 – Role v nepřímé integraci .....	18
Obrázek 11 - Role v přímé integraci .....	18
Obrázek 12 Příklad Business role a vazby na typové role.....	19
Obrázek 13 Princip Oracle eSSO LM .....	21
Obrázek 14 - Schéma zobrazení aplikace RAP .....	22

---

## Historie dokumentu

Verze	Datum	Autor	Popis
1.06	17.10.2017	ÚICT VZP ČR	Vytvoření dokumentu



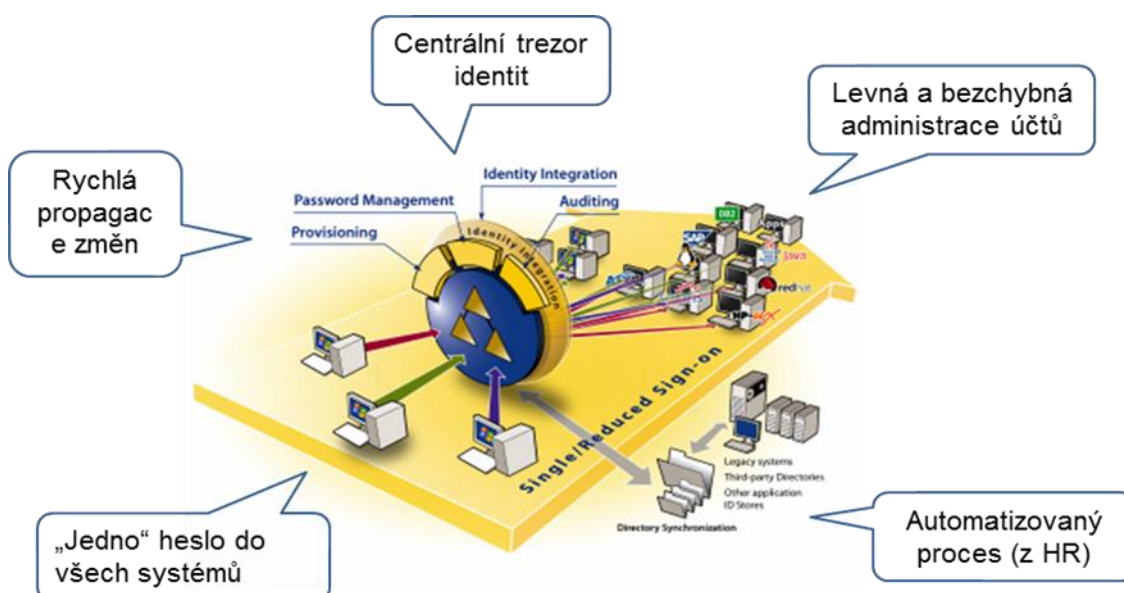
## 1. Úvod

Dokument obsahuje sadu standardů pro vybudování integračních vazeb nově dodávaných komponent informačního systému se stávajícími komponentami prostřednictvím integrační platformy v souladu se Standardy ICT VZP ČR. Vytvořené standardy jsou základem pro další rozšiřování systému zaváděním nových komponent a to jak „standardních“, tak i vytvářených dle specifických požadavků VZP ČR. Tento dokument je součástí výše uvedených Standardů ICT.

V případě specifikace rozšíření informačního systému zaváděním nových komponent ve smlouvě s dodavatelem, má specifikace uváděná v této smlouvě přednost před Standardy.

## 2. Integrace aplikace

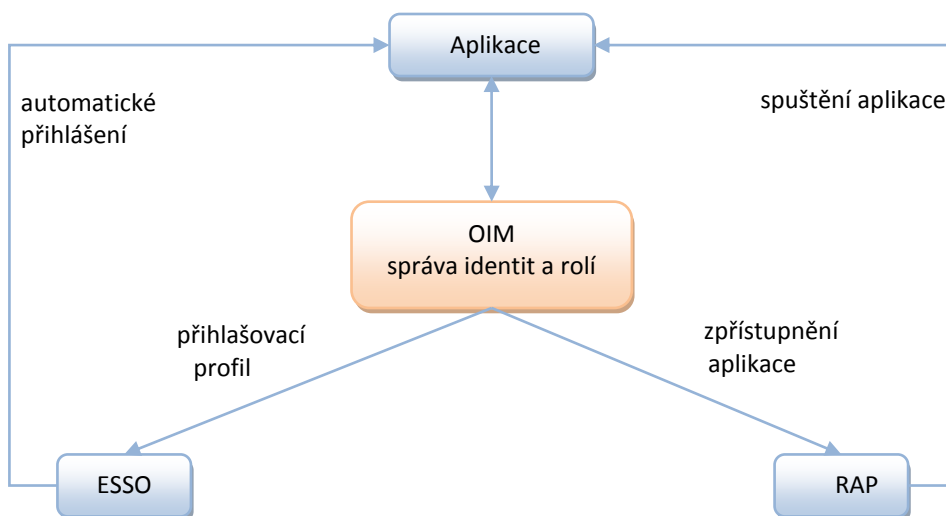
Dokument si klade za cíl seznámení s principy integrace aplikace do řešení IDM (Identity Management). Detailní informace o IDM řešení lze získat z dokumentace, která je uvedena v kapitole Reference.



Co nabízí integrace aplikace s řešením IDM?

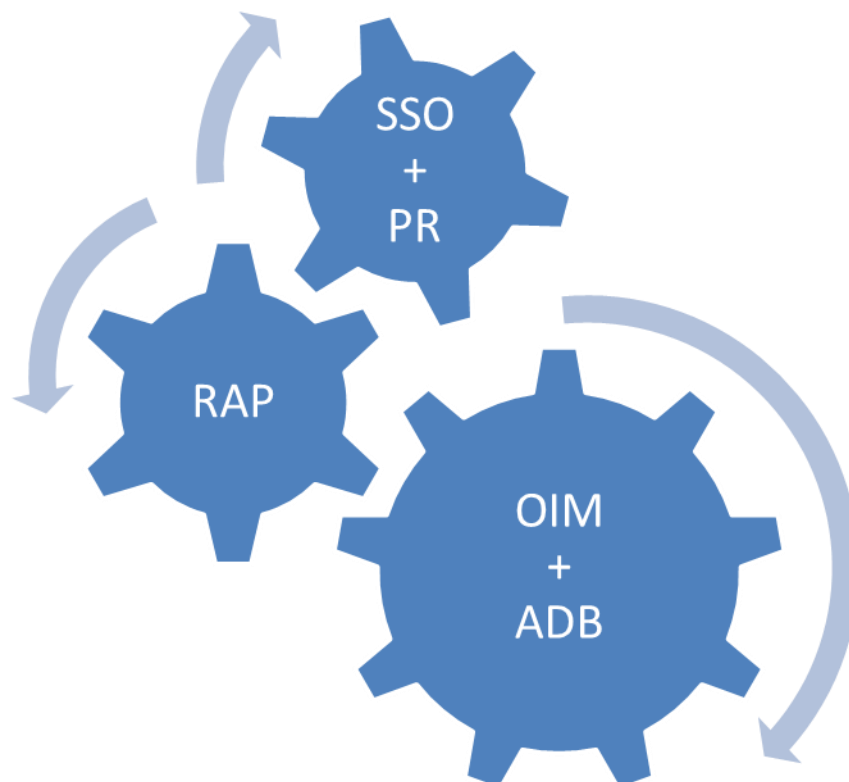
- Centrální správa uživatelských účtů a rolí pomocí Oracle Identity Manager (viz kapitola 2.1)
  - Správa identit uživatelů (jméno / heslo)
  - Správa oprávnění uživatelů pro přístup do aplikace (role, práva)
- Metodicky řešená podpora řízení oprávnění na základě rolí resp. hierarchie rolí
- Externí, konsolidované repozitory autentizačních a autorizačních dat s podporou specifik VZP – komponenta ADB (Autorizační Databáze)
- Řízené zpřístupnění aplikace (odkazu) cílovým uživatelům pomocí Rozcestníku aplikací (viz kapitola 2.6)

- Podporu Single Sign On (SSO) - automatické přihlášení cílových uživatelů do aplikace pomocí produktu Oracle Enterprise Single Sign-On Logon Manager (viz kapitola 2.5). Přihlašovací údaje do integrovaných aplikací pak spravuje OIM a vlastní přihlašování provádí Oracle eSSO LM.



Další kapitoly jsou členěny dle nabízených funkcí IDM řešení:

- Volba formy integrace s IDM (OIM)
- OIM – správa identit
- Řízení oprávnění na základě rolí
- ADB - externí, konsolidované úložiště uživatelských oprávnění
- eSSO – automatické přihlášení uživatele
- RAP – rozcestník aplikací



Obrázek 1 - Přehled IDM komponent

## 2.1 Varianty integrace s IDM/OIM

Aby bylo možné připojit aplikaci OIM a vyžít tak všech možností z toho plynoucích, je nejdříve nutné zvolit způsob integrace.

Způsob se volí dle druhu úložiště dat o uživateliích a jejich rolích:

1. **Externí úložiště dat** – jedná se o preferovaný způsob integrace. Aplikace využívá externí úložiště uživatelů aplikace a jejich rolí. Úložištěm dat je Autorizační databáze ADB, která je již s OIM integrována a zajišťuje tedy plnou spolupráci s OIM. Z pohledu OIM se jedná o nepřímou integraci.
2. **Vlastní úložiště dat** – pokud aplikace buď neumožňuje použít externí úložiště dat, nebo je tento způsob z nějakého důvodu nevhodný, lze nadále využívat vlastní úložiště dat provést takzvanou přímou integraci s OIM.

### 2.1.1 Externí úložiště uživatelských dat (integrace s ADB nebo AD)

V rámci nepřímé integrace je třeba připravit aplikaci pro oddělení svého úložiště autentizačních a autorizačních dat a jeho nahrazení autorizační databází ADB pomocí ADBLib knihovny (podrobné informace viz dokumentace ADB API uvedená v kapitole Reference. Podle typu aplikace se zvolí formát dodané knihovny ADB.

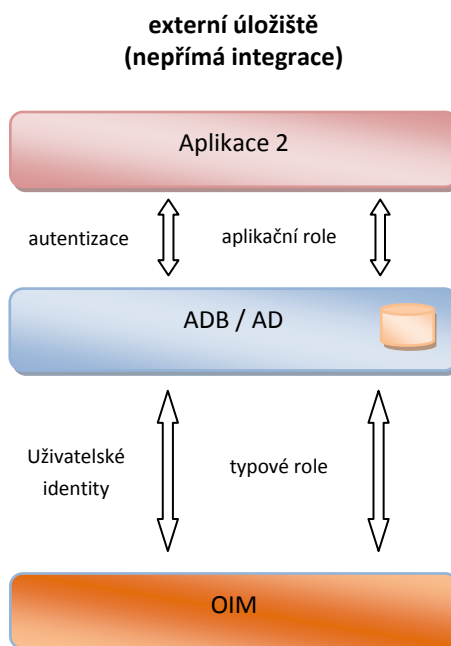
- Knihovna „jar“ – aplikace využívající technologii java
- Knihovna „pll“ – aplikace vytvořené v technologii Oracle Forms

Dále je třeba připravit seznam aplikačních rolí a jmenování zástupce, který se bude účastnit jednání o mapování typových a business rolích.



Pro vývojáře je k dispozici:

- Dokumentace ADB knihovny
- Knihovna ADB pro vývoj (verze XML) a integrační testy v TVS (verze WS)
- Podpora knihovny ADB ze strany dodavatele ADB



Obrázek 2 – Integrace aplikace - externí úložiště

## 2.1.2 Vlastní úložiště uživatelských dat

V případě, že aplikace preferuje použití vlastního úložiště dat, je nutné implementovat přímou integraci se systémem OIM – Oracle Identity Manager. Integrační rozhraní dovoluje obousměrnou komunikaci, v terminologii OIM / IDM se jedná o tzv.:

- Provisioning – poskytování údajů z IDM do integrované aplikace, tj. směr komunikace je z OIM do integrované aplikace
- Reconciliation – sjednocení údajů v IDM dle stavu dat v integrované aplikaci, tj. směr komunikace je z integrované aplikace do OIM

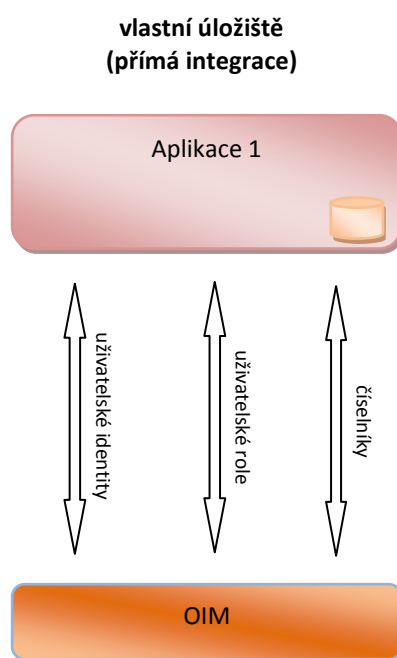
Pro implementaci integrace je nutné provést následující:

- Implementovat PL/SQL rozhraní na straně integrované aplikace (viz příloha), které slouží pro účely „provisioningu“

- Připravit tabulky/view na straně integrované aplikace pro účely „reconciliation“. Tabulky obsahují následující typy dat:
  - tabulka uživatelů (identit)
  - tabulka rolí přiřazených k uživatelům
  - tabulky číselníky, mezi které například patří číselník rolí

Pro možnost inkrementální „rekonciliace“, tj. přenosu pouze části dat, u kterých nastala změna od poslední „rekonciliace“, je nutné, aby tabulky (view) obsahovaly sloupec s datem poslední aktualizace.

Pro integrační testy je nutné předat IDM týmu přihlašovací údaje k databázi, tj. IP adresa a port, verze DB, SID DB, username, heslo atd.



Obrázek 3 – Integrace aplikace - vlastní úložiště

### 2.1.2.1 Přenosu dat z aplikace do OIM

Pro umožnění přenosu z aplikace do OIM stačí v databázi definovat tabulku nebo view. Každá taková tabulka nebo view by měly obsahovat sloupec určující datum a čas poslední změny daného řádku. OIM se pak snadno do takového databázového objektu podívá a získá údaje o posledních provedených změnách.

Přenášená data:

- Uživatelské identity (například přihlašovací jméno, heslo, jméno, příjmení, telefon, ...)
- Uživatelské typové role (například administrátor aplikace, evidence uživatelů, ...)
- Číselníky (například seznam pracovišť, seznam skupin, ...)

### 2.1.2.2 Přenos dat z OIM do aplikace

Pro zajištění funkcionality OIM vzhledem k uživatelům a jejich rolím v aplikaci, je definováno komunikační rozhraní PL/SQL API, které umožňuje základní operace s uživatelskými účty a jejich rollemi:

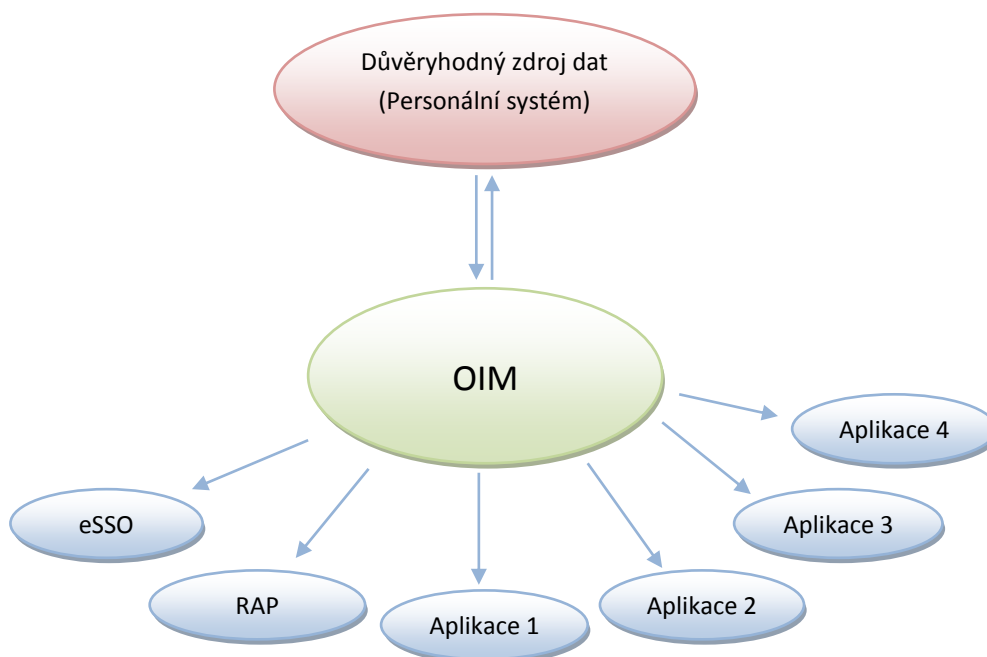
- **CreateUser** – Vložit uživatelský účet
- **UpdateUser** – Aktualizovat údaje o uživatelském účtu
- **LockUser** – Pozastavení uživatelského účtu
- **UnlockUser** – Obnovení uživatelského účtu
- **DeleteUser** – Smazání uživatelského účtu
- **ChangePassword** – Změna hesla uživatelského účtu
- **AddRole** – Přidání role
- **RemoveRole** – Odebrání role

Podrobnější informace o komunikačním rozhraní viz příloha PL/SQL API.

## 2.2 OIM

Oracle Identity Manager (OIM) zajišťuje centralizaci správy identit integrovaných aplikací a práv identit (rolí). Informace o uživateli jsou uloženy na jednom místě a odtud automaticky propagovány do integrovaných aplikací (viz Obrázek 4 - Schéma správy identity pomocí OIM). Například pokud se uživatelka vdá a změní příjmení, je tato změna propagována do všech integrovaných aplikací. Zároveň OIM může z integrovaných aplikací získávat aktuální data (například změny v číselnících) a případně je propagovat dále.

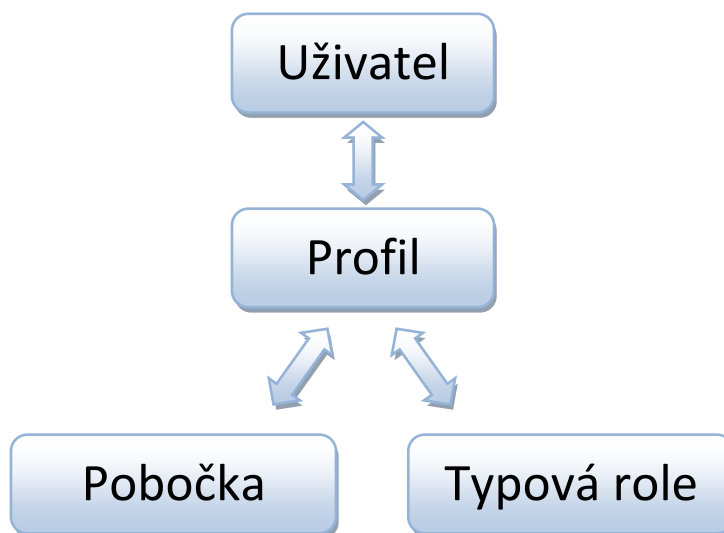
V rámci celé společnosti je tedy uživatel vždy zastoupen jednou identitou v OIM. Tato identita obsahuje všechny potřebné údaje o uživateli (v případě VZP jsou získávány z personálního systému VEMA). OIM řídí, do kterých aplikací má daná identita přístup a jaké má oprávnění (role) v aplikaci.



Obrázek 4 - Schéma správy identity pomocí OIM

## 2.3 ADB

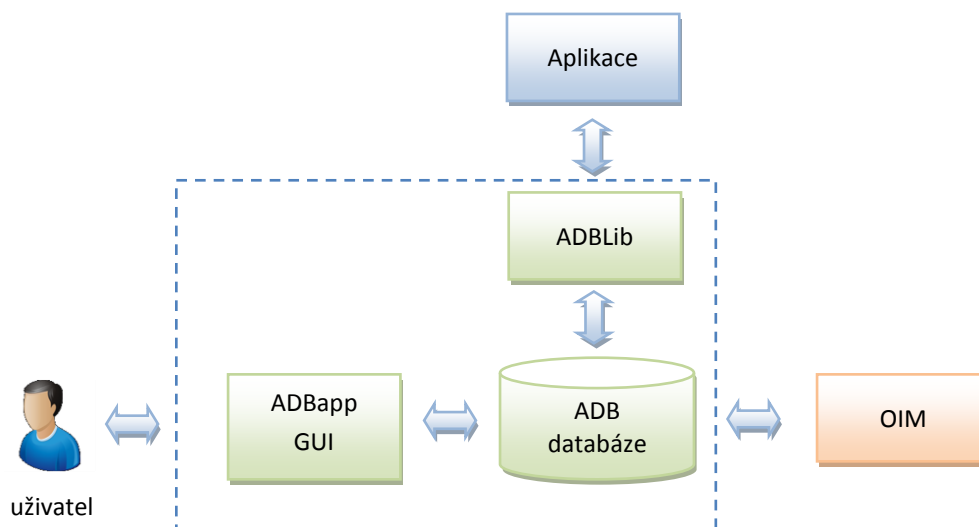
Autorizační databáze (ADB) je centrálním a konsolidovaným úložištěm dat určeným pro správu uživatelů a jejich rolí vzhledem k aplikacím. K vytvoření ADB vedly specifické požadavky v prostředí VZP. Každý uživatel ve VZP má přiřazené své typové role (každá typová role může obsahovat jednu a více aplikačních rolí), které jsou ale zároveň vázány na konkrétní pracoviště. Vzhledem k velkému množství uživatelů, pracovišť a rolí tak vznikla ADB, která ukládá tyto údaje v jednoduchém relačním modelu (viz Obrázek 5 - Relační model ADB).



Obrázek 5 - Relační model ADB

Následující schéma zobrazuje komponentový pohled na ADB řešení. ADB data jsou přístupná 3 způsoby:

1. Uživatelským rozhraním (GUI), které dovoluje plnou kontrolu na ADB daty.
2. Aplikace využívající ADB jako externího úložiště – pomocí API (ADBLib) dovolují číst data z ADB.
3. Řídící IDM systém (OIM) má plnou kontrolu nad ADB daty. Přístup je realizován skrze dedikované API pro OIM.



Obrázek 6 - Řešení ADB

### 2.3.1 Výhody použití ADB

Externí úložiště uživatelských dat v podobě ADB má následující výhody:

- Již vytvořená aplikace pro kompletní správu údajů, vytvořená v technologii Oracle Forms. Odpadá tedy nutnost vytváření vlastní správy uživatelů a jejich oprávnění v aplikaci.
- K dispozici jsou různé verze knihoven s jednotným rozhraním pro komunikaci s ADB. Stačí tedy odladit aplikaci, například s použitím XML verze knihovny, bez potřeby mít přístup k celé ADB, a po dokončení úprav jen vyměnit knihovnu a připojení s ADB bude fungovat.
  - Knihovna určená primárně pro vývoj, která umožňuje používat XML zdroj dat.
  - Knihovna určená pro komunikace s ADB prostřednictvím webových služeb.
  - V dohledné době bude k dispozici verze knihovny pro komunikaci s ADB prostřednictvím LDAP protokolu.
- Možnost zjednodušení práce s aplikačními rolemi pomocí typových rolí, které sdružují více aplikačních rolí dohromady, podle typu práce s aplikací. Typové role se pak snadněji u uživatelů spravují a mapují na business role.
- Aplikace nepotřebuje provádět žádnou správu svých uživatelů. To obstará ADB. Aplikace se pouze ptá (nepotřebuje provádět žádný zápis do oprávnění):
  - Existuje přihlašovaný uživatel?
  - Je heslo přihlašovaného uživatele správné?
  - Jaká oprávnění (aplikační role) má daný uživatel v aplikaci?
- Jednotný / konsolidovaný systém evidence uživatelů a oprávnění.
- Připravené GUI pro práci s ADB daty.

Aplikace	Uživatelé	Role	Práva
<b>Seznam uživatelů</b>			
Jméno	Příjmení	Login	Stav
Adam	Adamec	admin	AKTIVNI
Adam	Adamec	admin1	AKTIVNI
Jan	Jan	HONZA	AKTIVNI
Ferda	Mravenec	ferda	AKTIVNI
Petr	Pavel	1000001	AKTIVNI
test	test	1000000	NEAKTIVNI
OIM	USR1	OIMUSR1	AKTIVNI
		abrai72	AKTIVNI
		adame72	AKTIVNI
		allpohl	AKTIVNI
		allrpokl	AKTIVNI
		bacj71	AKTIVNI
		bazae72	AKTIVNI
		bernt72	AKTIVNI
		betad99	AKTIVNI
<input type="button" value="Nový uživatel"/> <input type="button" value="Smazat uživatele"/> <input type="button" value="Uložit změny"/>			
<b>Uživatel</b>			
Login	OIMUSR1	Jméno	OIM
Heslo		Příjmení	USR1
Heslo znovu		Telefon	123
Stav	AKTIVNI	Email	123
Pracoviště	2100	Územní pracoviště	BEROUN
<input type="button" value="Výběr"/>			
<b>Profil uživatele</b>			
Aplikace	Název role	Kód a název oprávněného pracoviště / aplikace	
ADB	Aplikační analytik	CSC	Centrální správa číselníků
ADB	Aplikační vývojář	CSC	Centrální správa číselníků
CSC	Administrátor CSČ	0	Celo VZP
CSC	Správce paketů a exportu CS	0	Celo VZP
CSC	Garant číselníku CSČ	0	Celo VZP
CSC	Super uživatel CSČ	0	Celo VZP
CSC	Uživatel CSČ	0	Celo VZP
<input type="button" value="Přidat profil"/> <input type="button" value="Upravit profil"/> <input type="button" value="Odstranit"/>			

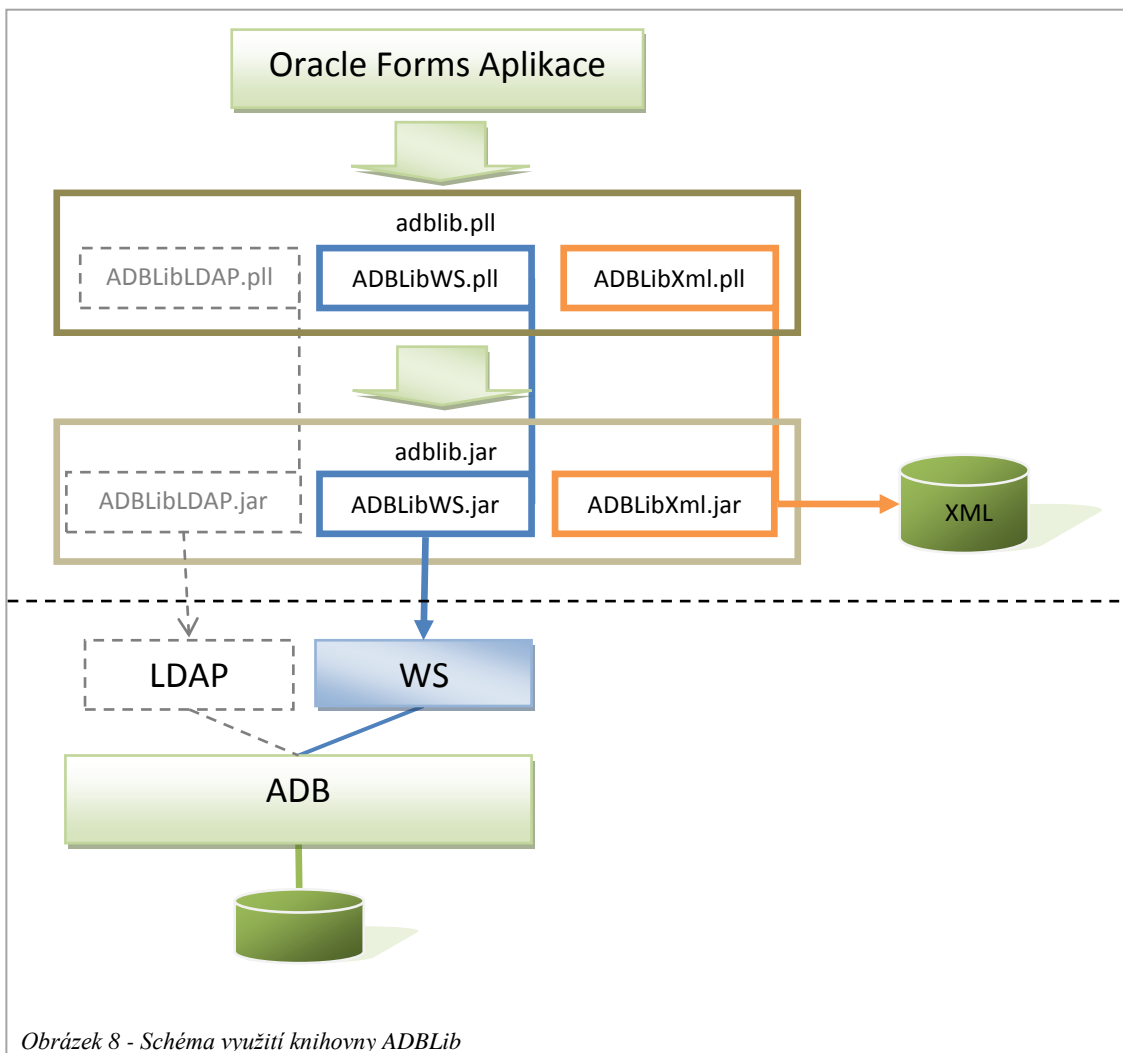
Obrázek 7 - Ukázka GUI ADB aplikace - seznam uživatelů

## 2.3.2 Knihovna

Knihovna ADBLib slouží ke komunikaci s autorizační databází ADB. V současné době jsou k dispozici 2 verze této knihovny (třetí verze, určená pro komunikaci prostřednictvím LDAP protokolu, bude dostupná později):

- Verze XML určená hlavně pro usnadnění vývoje, protože pro úpravu stávající či vývoj nové Oracle Forms aplikace není potřeba mít k dispozici celý systém autorizační databáze, ale stačí vytvořit si pouze data pomocí XML souborů.
- Verze WS, která v současné představuje dočasné řešení komunikace s vlastní Autorizační databází, než bude k dispozici rozhraní LDAP

Jednotné rozhraní knihovny ADBLib umožňuje vývoj Oracle Forms aplikace například na XML verzi, její odladění a poté prostou výměnou dvou souborů na aplikačním serveru Oracle Forms lze docílit výměny verze ADBLib knihovny.



### 2.3.3 Role

ADB nabízí možnost vytvoření typových rolí, které obsahují více aplikačních rolí. Více informací o rolích je k dispozici v následující kapitole.

### 2.3.4 Lokality

Typové role jsou vázány na pracoviště – lokality. Daná typová role uživatele může být na různých lokalitách a zároveň může mít uživatel v jedné lokalitě mít více typových rolí.

## 2.4 Role

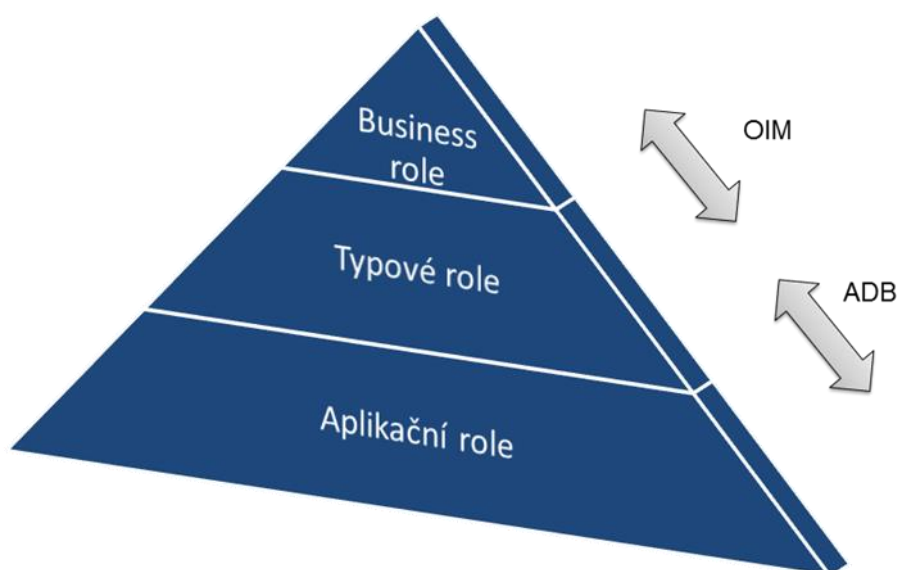
Role představují realizaci řízení oprávnění v aplikacích. Přiřazení role uživateli může být založeno na základě různých atributů uživatele: pracovního zařazení, pracoviště, dočasné potřeby, atd. . . Cílem je umožnit uživateli přístup pouze k informacím, ke kterým přístup má mít a umožnit mu s informacemi pracovat je tak, jak mu přísluší. K realizaci řízení bezpečnosti slouží 3 úrovně rolí.

Význam jednotlivých úrovní řízení bezpečnosti:

- AR - Aplikační role představuje zabezpečení na úrovni aplikace. Povoluje či zabraňuje tak vykonání konkrétní funkce aplikace. V případě vlastního úložiště dat se o správu aplikačních rolí stará sama

aplikaci. V případě použití externího úložiště ADB se o aplikační role stará ADB a na požádání aplikační role předává aplikaci.

- TR - Typové role představují seskupení oprávnění do logických (nedělitelných) celků. Umožňují usnadnění správy oprávnění v rámci jedné aplikace. K mapování aplikačních rolí na typové role dochází buď v ADB, tedy v případě využití externího úložiště dat anebo přímo v aplikaci, pokud to aplikace podporuje. V případě, že aplikace je aplikace integrována přímo, typové role nepodporuje a aplikačních rolí je málo, je možné prohlásit aplikační role za typové a provést tedy přímé mapování business rolí na role typové.
- BR - Business role seskupují typové role (tedy jednu a více aplikačních rolí) napříč více aplikacemi a odpovídají tak přiděleným zodpovědnostem (rolím) v rámci podnikových procesů. Například  $BR1=TR1+TR4+TR6\dots$  K mapování BR na TR dochází v OIM.



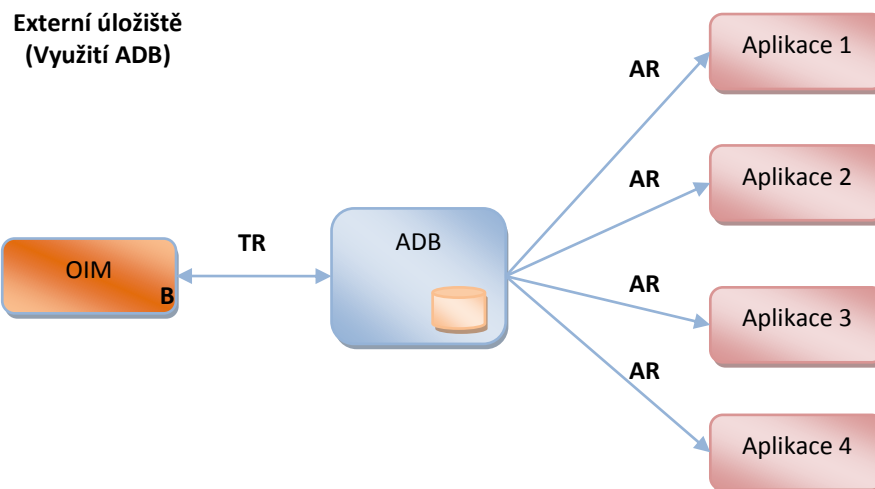
Obrázek 9 - Pyramida rolí

Důvodem použití více úrovní rolí je zajištění jak snadné správy přiřazení rolí uživateli, tj. práce s malým množstvím rolí, tak i v možnosti definovat velké množství oprávnění (aplikačních rolí) na úrovni aplikace.

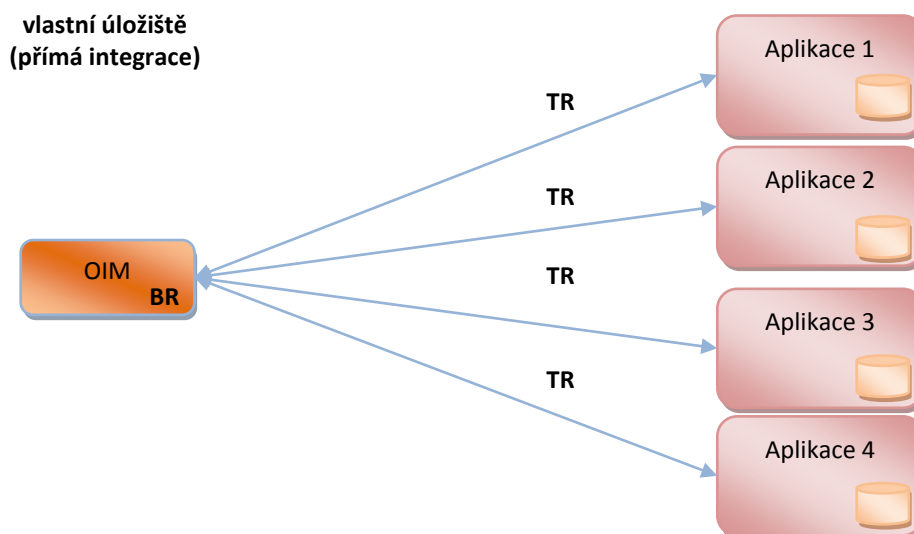
Jednotlivé úrovně jsou umístěny v různých systémech a to na základě typu použité integrace:

- Mapování Business rolí na Typové role jsou vždy umístěny přímo v OIM
- Mapování Typových rolí na role aplikační se liší dle použité integrace
  - **Nepřímá integrace** – typové role jsou na aplikační mapovány v externím úložišti dat, v ADB (viz Obrázek 10 – Role v nepřímé integraci)
  - **Přímá integrace** – typové role jsou na aplikační mapovány ve vlastním úložišti aplikace (viz Obrázek 11 - Role v přímé integraci)





Obrázek 10 – Role v nepřímé integraci



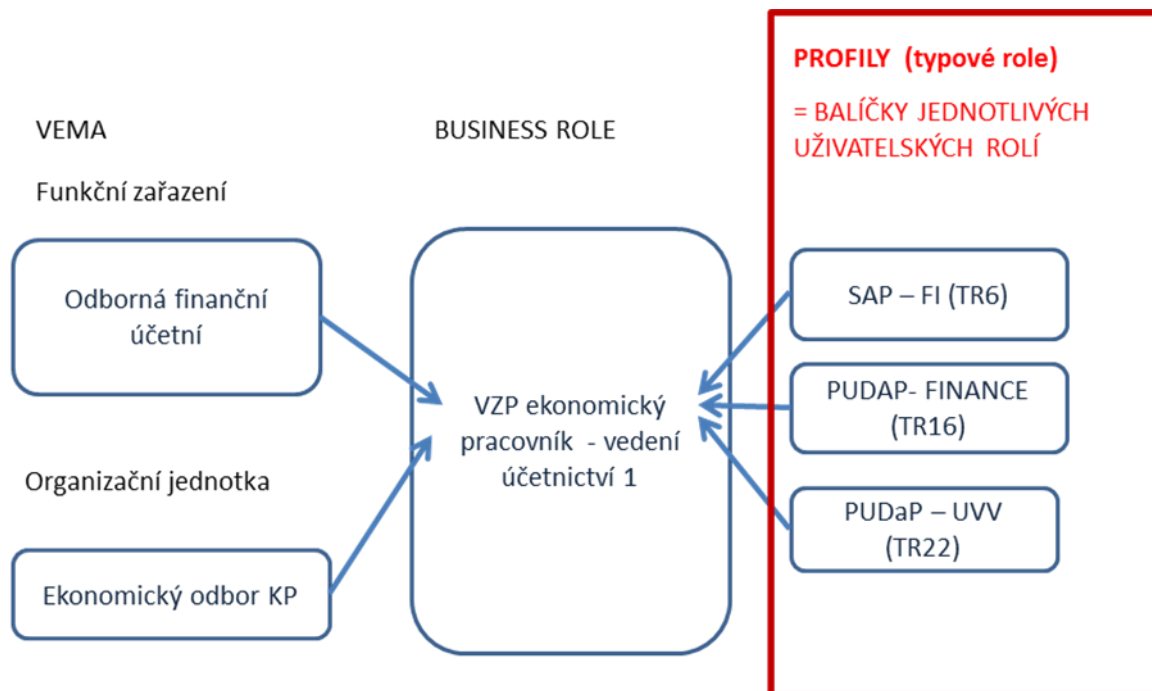
Obrázek 11 - Role v přímé integraci

## 2.4.1 Metodika definování rolí

Jednotlivé úrovně rolí mají rozdílný význam v interpretaci dané role.

- Aplikační role – představují identifikace rolí, které jsou jednoznačně interpretovatelné aplikační logikou aplikace, tj. řídí možnosti oprávnění v aplikaci

- Typové role – představují procesní kroky v agendě, která je aplikací podporovaná. Příkladem může být – zanesení objednávky, schválení faktury, rozhodnutí o žádosti, agenda EU dokladů atd. TR se skládá z AR, tj. TR náleží jedné aplikaci.
- Business role – představuje roli v podnikových procesech, tj. jedná se o tzv. kategorii zaměstnance – například účetní, krajský účetní kontrolor, ekonomický ředitel, přepážková pracovnice atd.

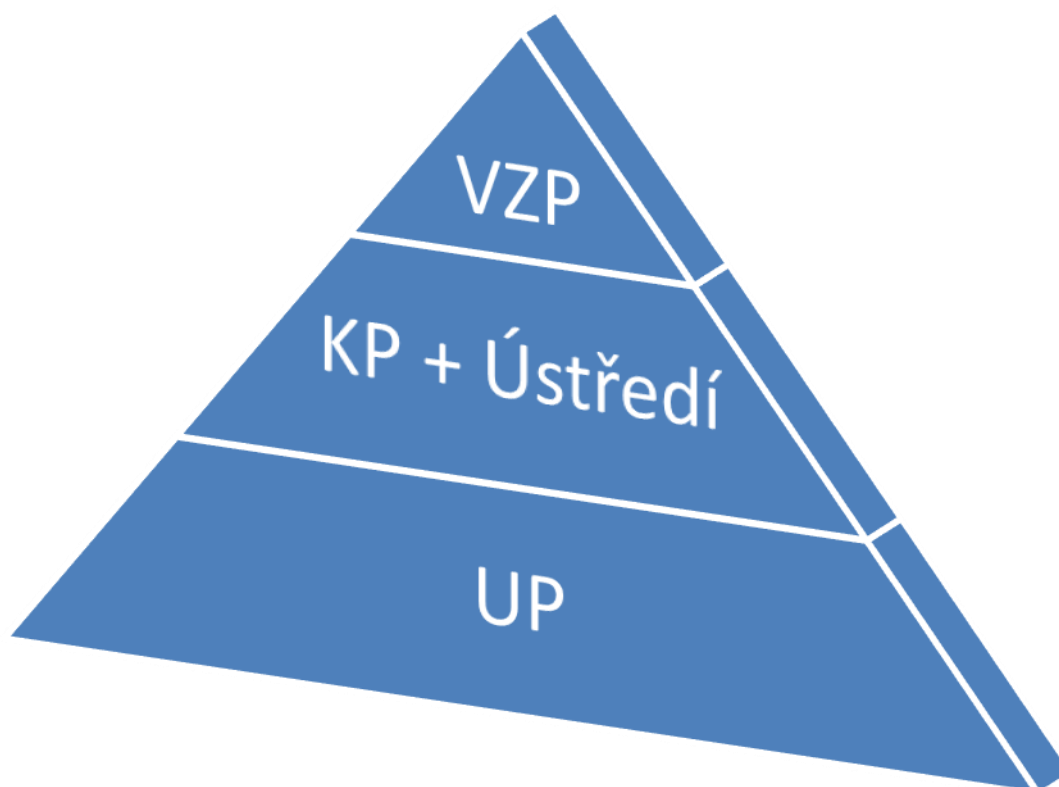


Obrázek 12Příklad Business role a vazby na typové role

## 2.4.2 Kombinace „Role“ a „Pracovní úsek“

V předchozím textu byl výraz „role“ použit pro funkční vymezení v rámci možností VZP. Toto vymezení ale není úplné, konkrétní role, která se přiděluje uživateli, musí ještě obsahovat vymezení se k pracovnímu úseku VZP, tj. vymezuje se datově. Kombinaci „role“ a „pracovního úseku“ budeme označovat jako instanci role. Tato konvence platí pro všechny úrovně rolí – pro business role, typové role i aplikační role.

Následující schéma zobrazuje hierarchické uspořádání pracovních úseků VZP:



Hierarchie se má úrovně:

- VZP – veškerá data VZP
- KP (včetně ústředí) – krajské celky VZP a ústředí, tj. 14 krajů a ústředí
- UP – územní pracoviště, cca 80 okresních měst ČR, každé územní pracoviště přísluší právě jednomu kraji

Kód pro VZP je 0, kraje mají kódy 1 až 14, ústředí má kód 9800, územní pracoviště mají 4 ciferný kód, kde 3 a 4 pozice je 0, např. 2100.

Příklady instancí rolí jsou:

- FIN\_TR34\_7200
- BR15\_0
- RSZP\_PK\_U66\_15

## 2.5 ESSO LM

Oracle Single Sign-On Logon Manager (eSSO LM) zajišťuje zabezpečené uložení přihlašovacích informací a umožňuje automatické přihlášení do různých druhů aplikací, například:

- Windows aplikace
- Internetové aplikace

- Java aplikace
- Oracle Forms aplikace



Obrazek 13 Princip Oracle eSSO LM

Ke spárování uživatele a profilu v eSSO LM slouží uživatelův doménový účet.

Aby bylo možné přihlášení k aplikaci pomocí jejího přihlašovacího dialogu, je potřeba zajistit identifikovatelnou tohoto dialogu, například jednoznačně identifikovatelným textem v názvu přihlašovacího dialogu.

Pro úspěšnou integraci aplikace do IDM řešení je nutné vytvořit přihlašovací profil aplikace v systému eSSO LM. Přihlašovací profil zajišťuje rozeznatelnost přihlašovací dialog aplikace pro automatické zadání jména a hesla systémem Logon Manager, který je nainstalován na pracovní stanici uživatele. V průběhu procesu integrace může být identifikována potřeba provést úpravu přihlašovacího dialogu tak, aby ho mohl Logon Manager jednoznačně identifikovat přihlašovací dialog.

Systém Oracle eSSO není jediným způsobem zajištění SSO ve VZP. Mezi další způsoby patří například metody / technologie:

- Kerberos,
- NTLM,

kteří se ve VZP využívají, především v prostředí technologií společnosti Microsoft.

## 2.5.1 Spolupráce systémů OIM a eSSO

Systém OIM je řídicím prvkem mezi IDM systémy, řídí tedy i životní cyklus účtů v integrovaných aplikacích, tj. včetně událostí typu založení účtu, změna hesla k účtu atd. Systémem OIM při těchto operacích

paralelně komunikuje se systémem eSSO a předává mu přihlašovací údaje, které jsou právě modifikovány v integrované aplikaci. Uživatel nezná přihlašovací údaje a systém eSSO vyplňuje přihlašovací údaje za uživatele v okamžiku zobrazení přihlašovacího dialogu integrované aplikace.

## 2.6 RAP

Rozcestník aplikací (RAP) je z pohledu uživatele aplikace, která zobrazuje seznam dostupných aplikací a umožňuje jejich spuštění. Za aplikací je skryt celý systém pro evidenci dostupných aplikací k jednotlivým uživatelům.



Obrázek 14 - Schéma zobrazení aplikace RAP

Každý uživatel systému RAP musí mít vytvořený uživatelský účet a mít nastaveny pracovní plochy a aplikace. Spuštěním klientské aplikace RAP dojde k přihlášení uživatele (resp. klienta – tj. klientské aplikace) do systému RAP. Uživatel je ověřován na základě uživatelského jména, pod kterým je přihlášen do domény. Při úspěšném přihlášení je uživateli vygenerováno komunikační číslo, které nadále slouží pro vlastní komunikaci se systémem. Dále je uživateli nastavena klientská aplikace RAP. Jsou zjištěny pracovní plochy uživatele, záložky (karty) a aplikace na nich. Klient také získá hodnotu intervalu pro pravidelné oznamování stavu systému RAP.

V tuto chvíli je klient přihlášen a může spouštět přidělené aplikace. Spouštěné aplikace je opět realizováno webovou službou. Dle typu spuštěné aplikace klient rozhodne o způsobu využití vráceného příkazu z odpovědi služby.

- V případě aplikace typu **EXE** dojde k přímému spuštění aplikace na počítači uživatele.
- Pokud se jedná o aplikaci typu **URL**, dojde ke spuštění Internet Exploreru s přednastaveným url.
- U aplikace typu **HOST**, která je vzdálenou aplikací (tzv. server-side) se nejprve na základě tzv. load-balancingu vybere aplikační server a dojde ke spuštění internetového prohlížeče s otevřením aplikace z

vybraného aplikačního serveru. Tento případ může nastat zejména pro aplikace běžící na technologii Oracle Forms.

### 2.6.1 Integrace aplikace s RAP

Pro integraci aplikace se systémem RAP je třeba:

- Určit typ aplikace
- Připravit název a popis aplikace tak, jak bude vystupovat na kartě pracovní plochy uživatele
- Připravit způsob spouštění aplikace (příkazový řádek, URL, parametry, server ...)
- Případně i připravit ikonu představující aplikaci

## 2.7 GMUSERS – Katalog uživatelů

Dalším tématem spolupráce IDM a podnikových aplikací je distribuce katalogu uživatelů. Katalog uživatelů je spravován personálním systémem VEMA, obsahuje veškeré personální informace.

Katalog je realizován ve formě tabulky GMUSERS a primárním úložištěm je sdílený číselník.

Tabulka GMUSERS obsahuje veškeré zaměstnance VZP a je možné jí mít k dispozici pomocí SDI (silné datové integrace).

Sloupec	Typ	Nepovinný (Nullable)
AD_USERNAME	VARCHAR2(30)	No
JMENO	VARCHAR2(30)	No
PRIJMENI	VARCHAR2(30)	No
TITUL	VARCHAR2(20)	Yes
TEL	VARCHAR2(1000)	Yes
FAX	VARCHAR2(100)	Yes
EMAIL	VARCHAR2(100)	Yes
PRAC_USEK	VARCHAR2(4)	No
FUNKCE	VARCHAR2(300)	No
PLATNOST	CHAR(1)	No

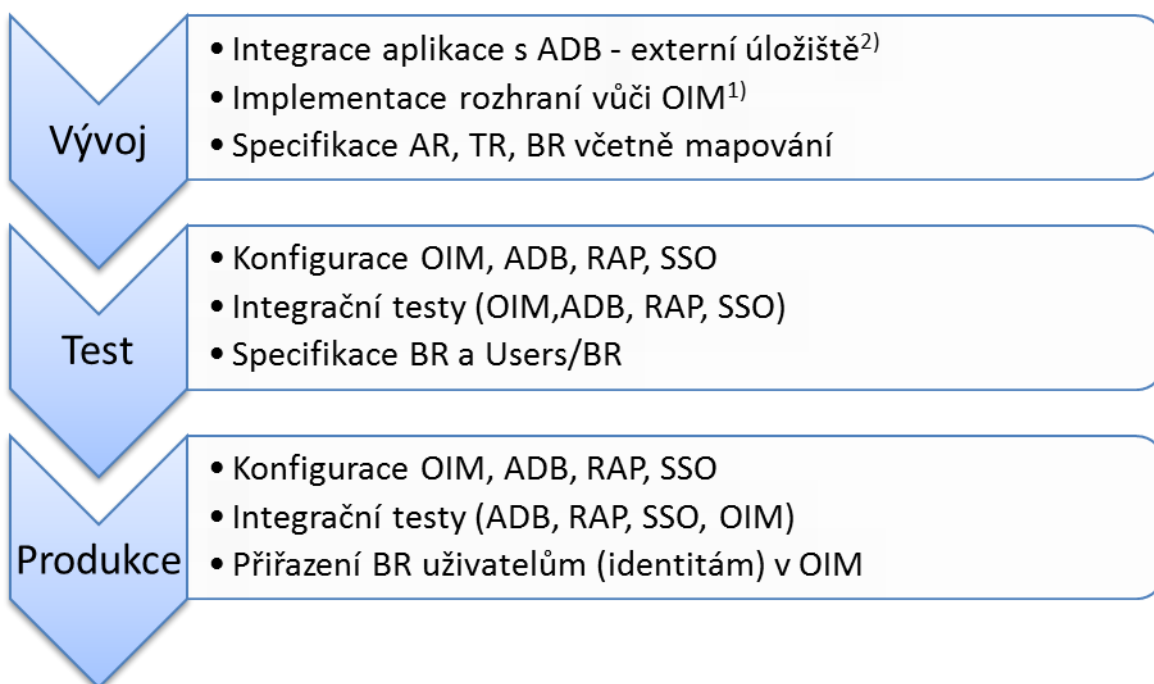
## 3. Fáze integrace aplikace

Integrace aplikace do IDM není otázkou jednoho kroku, ale představuje komplexní proces, který trvá typicky několik týdnů a obsahuje řadu nutných součinností.

Z pohledu dodavatele aplikací proces integrace do IDM dělíme do 3 fází:

- **Vývoj** – vlastní úprava aplikace pro integraci do IDM
- **Test** – mapování business a typových rolí, provádění integračních testů

- **Produkce** – konfigurace a nasazení do produkčního prostředí včetně přidělení business rolí koncovým uživatelům



*Poznámky:*

- 1) Jedná se o variantu integrace „vlastní“ úložiště / přímá integrace s OIM
- 2) Jedná se o variantu integrace „externí“ úložiště / integrace skrze ADB

Samotná proces integrace aplikace se dá dělit do dvou oblastí:

- Technologická oblast – integrační vrstva, tj. jedná se o samotné zajištění komunikace IDM komponent a integrované aplikace.
- Aplikační oblast - business úroveň, tj. jedná se o problematiku řízení identit a rolí v integrovaných aplikacích – definování business rolí, schvalovacích procesů, typových rolí atd.

Ve fázi vývoje se typicky řeší úlohy z technologické (integrační) vrstvy. Ve fázích testů a produkčního provozu se naopak řeší především oblast aplikační.

### 3.1 Kroky a zodpovědnosti během integrace aplikace do IDM řešení

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 <sup>1)</sup>			X		
	Vhodnost LOGIN dialogu aplikace pro SSO			X		
	Integrace s ADB (ADB knihovna) <sup>2)</sup>			X		Případná změna modelu řízení oprávnění
	Podpora dodavatele při integraci s IDM				X	
	Seznam TR, AR (včetně mapování) pro nastavení ADB <sup>2)</sup>			X		
	Seznam TR pro nastavení OIM <sup>1)</sup>			X		
	Specifikace BR a schvalovacích procesů		X		X	
	Rozšíření konfigurace OIM (BR, konektor k aplikaci)				X	
TEST	Konfigurace ADB dle podkladů TR/AR <sup>2)</sup>	X				
	Konfigurace OIM včetně BR <sup>1)</sup>	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 <sup>2)</sup>	X				
	Konfigurace OIM včetně BR <sup>1)</sup>	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



## 4. PL/SQL API – komunikační rozhraní

### 4.1 Procedura Create User

Tato procedura je určena k vytvoření uživatelského účtu.

```
PROCEDURE CreateUser
(
  UserID in varchar2,
  FirstName in varchar2,
  LastName in varchar2,
  Organization in varchar2,
  EmployeeType in varchar2,
  ManagerID in varchar2,
  Email in varchar2,
  Telephone in varchar2,
  UserLocked in varchar2,
  StartDate in DATE,
  EndDate in DATE,
  UserPassword in varchar2,
  Result out varchar2
)
```

*Parametry:*

- *UserID* – jedinečný identifikátor uživatele
- *FirstName* – jméno uživatele
- *LastName* – příjmení uživatele
- *Organization* - organizace
- *EmployeeType* – typ uživatele
- *ManagerID* – jedinečný identifikátor nadřízeného daného uživatele
- *Email* – email uživatele
- *Telephone* – telefon uživatele
- *UserLocked* – určuje, zda je uživatelský účet aktivní (uživatel může přistupovat do Forms aplikace)
- *StartDate* – začátek platnosti účtu
- *EndDate* – konec platnosti účtu
- *UserPassword* – heslo pro uživatelský účet
- *Result* – výsledek procedury

## 4.2 Procedura UpdateUser

Tato procedura je určena k změně parametrů uživatelského účtu.

```
PROCEDURE UpdateUser
(
  UserID in varchar2,
  FirstName in varchar2,
  LastName in varchar2,
  Organization in varchar2,
  EmployeeType in varchar2,
  ManagerID in varchar2,
  Email in varchar2,
  Telephone in varchar2,
  StartDate in DATE,
  EndDate in DATE,
  Result out varchar2
)
```

*Parametry:*

- *UserID* – jedinečný identifikátor uživatele
- *FirstName* – jméno uživatele
- *LastName* – příjmení uživatele
- *Organization* – organizace
- *EmployeeType* – typ uživatele
- *ManagerID* – jedinečný identifikátor nadřízeného daného uživatele
- *Email* – email uživatele
- *Telephone* – telefon uživatele
- *StartDate* – začátek platnosti účtu
- *EndDate* – konec platnosti účtu
- *Result* – výsledek procedury

## 4.3 Procedura ChangePassword

Tato procedura je určena k změně hesla k uživatelskému účtu.

```
PROCEDURE ChangePassword
(
  UserID in varchar2,
  UserPassword in varchar,
```

```
Result out varchar2  
)
```

*Parametry:*

*UserID* – jedinečný identifikátor uživatele

*UserPassword* – nové heslo pro uživatelský účet

*Result* – výsledek procedury

## 4.4 Procedura LockUser

Tato procedura je určena k uzamčení uživatelského účtu. Uživatelský účet se stává neaktivním.

```
PROCEDURE LockUser  
  
(  
  
UserID in varchar2,  
Result out varchar2  
)
```

*Parametry:*

- *UserID* – jedinečný identifikátor uživatele
- *Result* – výsledek procedury

## 4.5 Procedura UnlockUser

Tato procedura je určena k odemčení uživatelského účtu. Uživatelský účet se stává aktivním.

```
PROCEDURE UnlockUser  
  
(  
  
UserID in varchar2,  
Result out varchar2  
)
```

*Parametry:*

- *UserID* – jedinečný identifikátor uživatele
- *Result* – výsledek procedury

## 4.6 Procedura DeleteUser

Tato procedura je určena k vymazání uživatelského účtu ze správy uživatelů.

```
PROCEDURE DeleteUser  
  
(  
  
UserID in varchar2,  
Result out varchar2  
)
```

*Parametry:*

- *UserID* – jedinečný identifikátor uživatele

- *Result – výsledek procedury*

## 4.7 Procedura AddRole

Tato procedura je určena k přidání role pro daného uživatele.

```
PROCEDURE AddRole
(
  UserID in varchar2,
  Workplace in varchar2,
  Role in varchar2,
  Result out varchar2
)
```

*Parametry:*

- *UserID – jedinečný identifikátor uživatele*
- *Workplace – pracoviště uživatele*
- *Role – role uživatele*
- *Result – výsledek procedury*

## 4.8 Procedura RemoveRole

Tato procedura je určena k odebrání role pro daného uživatele

```
PROCEDURE RemoveRole
(
  UserID in varchar2,
  Workplace in varchar2,
  Role in varchar2,
  Result out varchar2
)
```

*Parametry:*

- *UserID – jedinečný identifikátor uživatele*
- *Workplace – pracoviště uživatele*
- *Role – role uživatele*
- *Result – výsledek procedury*

## 4.9 Návrátové kódy

*USER\_NOT\_EXIST - Uživatelský účet neexistuje (UpdateUser, ChangePassword, LockUser, UnlockUser, DeleteUser)*

*USER\_EXIST - Uživatelský účet již existuje (procedura CreateUser)*

*USER\_IS\_LOCKED - Uživatelský účet je již zamčen (procedura LockUser)*

*USER\_IS\_UNLOCKED - Uživatelský účet je již odemčen (procedura UnlockUser)*

*USER\_PHONE\_NULL - Není vyplněn telefonní kontakt (procedury CreateUser)*

*USER\_PASSW\_BAD - Neplatné uživatelské heslo, nelze nastavit nové heslo (procedury CreateUser, ChangePassword )*

*USER\_LAST\_NAME\_NULL - Chybí příjmení uživatele (procedury CreateUser)*

*USER\_FIRST\_NAME\_NULL - Chybí jméno uživatele (procedury CreateUser)*

*/\* návratové kódy související s přiřazením rolí \*/*

*ROLE\_NOT\_EXIST - Dané přiřazení role neexistuje (procedura RemoveRole)*

*ROLE\_EXIST - Dané přiřazení role již existuje (procedura AddRole)*

*ROLE\_USER\_NOT\_EXIST - Uživatelský účet pro přiřazení role neexistuje (procedura AddRole)*

*ROLE\_WORKPLACE\_NOT\_EXIST - Pracoviště pro přiřazení role neexistuje (procedura AddRole)*

*ROLE\_RIGHTS\_NOT\_EXIST - Skupina práv (role) pro přiřazení neexistuje (procedura AddRole)*

*/\* návratový kód pro ostatní případy \*/*

*OIM\_UNKNOWN\_ERROR - Ostatní chyby (všechny procedury při neznámé chybě)*

## 5. Reference

Následující tabulka obsahuje seznam dokumentů, které má VZP k dispozici, včetně krátkého popisu obsahu dokumentu.

Název dokumentu	Popis
ADB_API.doc	Popis knihovny ADB
ADB_uzivatelska_prirucka.doc	Uživatelská příručka aplikace ADB
GMRAP_UzivatelaskaPriruckaAdmin.doc	Uživatelská příručka administrátora RAP
GMRAP_UzivatelaskaPrirucka.doc	Uživatelská příručka uživatele RAP
OIM_PL_SQL_API.docx	Popis rozhraní aplikace pro komunikaci s OIM 1)

*Poznámky:*

- 1) *Popis rozhraní aplikace pro komunikaci s OIM je uveden v kapitole 4. tohoto dokumentu*

# **Integrace aplikace s CSČ**

Příloha standardů a podmínek dodávek  
informačního systému VZP ČR



## UPOZORNĚNÍ:

Tento dokument je zpracován Všeobecnou zdravotní pojišťovnou České republiky (dále též jen „VZP ČR“ nebo „VZP“). Všeobecná zdravotní pojišťovna České republiky jej uveřejňuje v rámci zadávací dokumentace jí zadávaných veřejných zakázek. Tento dokument umožňuje utvořit si představu o standardech informační architektury ICT VZP ČR. Účelem jeho uveřejnění je poskytnout informace nezbytné pro integraci dodávané komponenty se stávajícím informačním systémem v souladu se Standardy ICT- VZP- NIS.

Uveřejněním tohoto dokumentu není dotčena právní odpovědnost spojená s jeho zneužitím.

V tomto dokumentu bylo použito názvů subjektů a názvů produktů, které mohou být chráněny příslušnými právními předpisy.

**Otevřením tohoto dokumentu berete výše uvedené skutečnosti na vědomí.**



## Obsah

1. Úvod .....	7
2. Struktura zprávy .....	7
3. Popis jednotlivých služeb .....	7
3.1 Služba „Poskytnutí seznamu verzí číselníku“ .....	7
3.1.1 Parametry služby.....	8
3.2 Služba „Poskytnutí verzí číselníku“ .....	9
3.2.1 Parametry služby.....	9
3.3 Služba „Nová verze číselníku“ .....	11
3.3.1 Parametry služby.....	11
3.4 Služba „Převzetí protokolu o zpracování číselníku“ .....	13
3.4.1 Parametry služby.....	13
3.5 Služba „Změna stavu balíčku“ .....	14
3.5.1 Parametry služby.....	14
3.6 WSDL popis služeb.....	15
4. Postup zařazení nových číselníků do CSC .....	15

---

## Historie dokumentu

Verze	Datum	Autor	Popis
1.06	17.10.2017	ÚICT VZP ČR	



## 1. Úvod

Dokument obsahuje sadu standardů pro vybudování integračních vazeb nově dodávaných komponent informačního systému se stávajícími komponentami prostřednictvím integrační platformy v souladu se Standardy ICT VZP ČR. Vytvořené standardy jsou základem pro další rozšiřování systému zaváděním nových komponent a to jak „standardních“, tak i vytvářených dle specifických požadavků VZP ČR. Tento dokument je součástí výše uvedených Standardů ICT.

V případě specifikace rozšíření informačního systému zaváděním nových komponent ve smlouvě s dodavatelem, má specifikace uváděná v této smlouvě přednost před Standardy.

Obecně lze říci o službách CSC, že používají pro svoji asynchronní komunikaci technologii Oracle Advanced Queuing. V této technologii probíhá komunikace prostřednictvím front zpráv. V CSC jsou založeny 2 základní fronty SC\_IN\_Q pro sběr vstupních požadavků a SC\_EXTERNI\_Q do níž se ukládají výsledky a dále jsou propagovány do IPF.

## 2. Struktura zprávy

Pro rozesílání i přijímání dat bude použit standardní formát zprávy **vzpipfzprava**, definovaný IPF viz příloha Integrační vazby IPF. CSC generuje zprávu dle následujícího pravidla:

CORRID => request.CORRID nebo request.MSGID v závislosti na vyplnění request.CORRID ,

PUVODCE => request.PUVODCE,

ODESILATEL => 'CSC',

ODESILATELDOPLNEK => '9900',

PRIJEMCE => request.ODESILATEL,

PRIJEMCEDOPLNEK => request.ODESILATELDOPLNEK,

NAZEVSLUZBY => request.NAZEVSLUZBY,

NAZEVZPRAVY => v závislosti na službě,

VERZEZPRAVY => '1.0',

REFERENCE => request.REFERENCE,

PARAMETRD1 => systimestamp,

DATA => xml data – závisí na službě, struktura xml odpovídá jednotlivým schématům.

## 3. Popis jednotlivých služeb

### 3.1 Služba „Poskytnutí seznamu verzí číselníku“

Cílem této služby je poskytnout externím aplikacím seznam všech verzí zvoleného číselníku. Tato služba bude probíhat ve dvou fázích

- IPF nebo externí aplikace uloží požadavek na seznam číselníku do vstupní zprávy CSC SC\_IN\_Q. Tento požadavek bude obsahovat označení číselníku a období
- CSC vygeneruje zprávu, která obsahuje seznam verzí číselníku, informace o stavu zpracování požadavku a propaguje se do IPF fronty GMCSC\_Q. Jednotlivé verze budou obsahovat metadata a anotace.
- V případě, že daný číselník neexistuje, je vrácen chybový kód ve stavu `VyřízeníPozadavku`.

### 3.1.1 Parametry služby

Název služby: Poskytnutí seznamu verzí číselníku

Označení služby: poskytniSeznamCiselniku

Typ služby: Asynchronní

Požadavek:

oznaceniCiselniku	string	1
- označení číselníku musí existovat v CSČ. Např. CISELPOB		
obdobiod	date	1
- datum ve formátu RRRR-MM-DD např. 2000-12-01		
obdobido	date	1

Odpověď

Ciselnik	complex	0-n
oznaceniCiselniku	string	1
- označení číselníku musí existovat v CSČ. Např. CISELPOB		
verzeStruktury	string	1
verzeObsahu	string	1
platnostOd	date	1
expirace	date	1
popisStruktury	string	1
popisObsahu	string	1
interní	enum	1
„A - ano“		
„N - ne“		
externí	enum	1
A - ano“		
„N - ne“		
anotaceStruktury	base64	1
- v této položce je uložen binární soubor		
anotaceObsahu	base64	1
- v této položce je uložen binární soubor		
formatCiselniku	enum	1
default „CSV“		

kodovaStranka	enum	1
default „EE8PC852“		
srovnacniProtokol	base64	1
- protokol je zazipovaný a zakódovaný base64		
sloupec	complex	1-n
poradi	number	1
nazevSloupce	string	1
datovyTyp	string	1
Externi	enum	1
„A – sloupec bude součástí externí a interní formy číselníku“		
„N – sloupec bude součástí pouze interní formy číselníku“		
„E - sloupec bude součástí pouze externí formy číselníku“		
popisSloupce	string	1
stavVyrizeniPozadavku viz. výše 1		

## 3.2 Služba „Poskytnutí verzí číselníku“

Cílem této služby je poskytnout externím aplikacím vybrané číselníky včetně metadat, anotací a dat. Tato služba bude probíhat ve dvou fázích

- IPF nebo externí aplikace uloží požadavek na číselníky do vstupní zprávy CSČ SC\_IN\_Q. Tento požadavek bude obsahovat označení číselníku, seznam verzí číselníku a formu číselníku (interní nebo externí)
- CSČ vygeneruje zprávu, která obsahuje verze číselníků, informace o stavu zpracování požadavku a propaguje se do IPF fronty GMCSC\_Q. Jednotlivé verze budou obsahovat metadata a anotace a data.
- V případě, že daný číselník neexistuje, je vrácen chybový kód ve StavVyrizeniPozadavku.

### 3.2.1 Parametry služby

Název služby: Poskytnutí verzí číselníku

Označení služby: poskytniVerzeCiselniku

Typ služby: Asynchronní

Požadavek:

oznaceniCiselniku	string	1
interni	enum	1
„A“ – požaduje interní formát číselníku		
„N“ – požaduje externí formát		
verzeObsahu	string	1-n

Odpověď

ciselnik complex 0-n

oznaceniCiselniku	string	1
verzeStruktury	string	1
verzeObsahu	string	1
platnostOd	date	1
expirace	date	1
popisStruktury	string	1
popisObsahu	string	1
interní	enum	1
„A“ - ano		
„N“ - ne		
externi	enum	1
„A“ - ano		
„N“ - ne		
anotaceStruktury	base64	1
anotaceObsahu	base64	1
formatCiselniku	enum	1
„CSV“		
„XML“		
default „csv“		
kodovaStranka	enum	1
„EE8PC852“ – dos PC852		
„EE8ISO8859P2“ - iso		
„EE8MSWIN1250“ – ansi 1250		
default „EE8PC852“		
data	base64	1
- Obsah číselníku je zazipovaný a zakódovaný base64		
srovnacíProtokol	base64	1
sloupec complex 1-n		
poradi	number	1
nazevSloupce	string	1
datovyTyp	string	1

externi	enum	1
„A – sloupec bude součástí externí a interní formy číselníku“		
„N – sloupec bude součástí pouze interní formy číselníku“		
„E - sloupec bude součástí pouze externí formy číselníku“		
popisSloupce	string	1
stavVyrizeniPozadavku	enum	1

### 3.3 Služba „Nová verze číselníku“

Cílem této služby CSČ je převzít novou verzi obsahu číselníku, která vznikla v jiném aplikačním modulu VZP. Importovaný číselník se nastaví do stavu „Typováno“.

V případě, že je administrátorem číselníků v CSČ nastaveno automatické schvalování a distribuce, nastaví se číselník do stavu schváleno a provede se vygenerování všech paketů, ve kterých je tento číselník uveden samostatně. U číselníků s tímto režimem nebude povoleno v CSČ editovat jednotlivé záznamy.

Převzetí číselníku bude probíhat následovně:

- IPF uloží požadavek na převzetí číselníku do vstupní fronty CSČ SC\_IN\_Q. Tento požadavek bude obsahovat metadata číselníku a obsah číselníku.
- CSČ překontroluje metadata číselníku(musí souhlasit struktura) a data číselníku dekóduje a uloží do CSČ. Do poznámky verze obsahu zapíše informaci, že byl číselník pořizen z AQ.
- V případě, že je povoleno automatické schvalování číselníku a distribuce, nastaví stav na „schváleno“ a provede distribuci paketu
- CSČ vygeneruje odpověď, která obsahuje informace o stavu zpracování požadavku a propaguje se do IPF fronty GMCSC\_Q. O případných chybách, které vzniknou při následné kontrole či distribuci číselníku, bude notifikován garant číselníku.

#### 3.3.1 Parametry služby

Název služby: Nová verze číselníku

Označení služby: **NovaVerzeCiselniku**

Označení zprávy: **prevezmiVerziCiselniku**

Typ služby: Asynchronní

Požadavek:

ciselnik complex 1-n

oznaceniCiselniku varchar(40) 1

- Označení číselníku musí existovat v CSČ.

popisObsahu varchar(40) 1

verzeStruktury varchar(20) 1



- Pro oddělení desetinných míst je použita tečka. Verze struktury musí existovat v CSČ.

platnostOd date 1

platnostDo date 1

formatCiselniku enum 1

„csv“

„xml“

default „csv“

- V současné době je podporován pouze **csv** formát.

kodovaStranka enum 1

„EE8PC852“

„EE8ISO8859P2“

„EE8MSWIN1250“

default „EE8PC852“

- V současné době je podporována pouze **EE8PC852**

data blob 1

- Data (csv) jsou zazipována a zakódována base64. CSV data jsou v kódové stránce EE8PC852, jako oddělovač je použita čárka, jednotlivé řádky jsou odděleny CRLF, pořadí sloupců csv musí odpovídat pořadí sloupců ve struktuře CSČ, textové sloupce jsou v uvozovkách, datum je ve formátu DDMMRRRR;

anotaceObsahu blob 0-1

- Zip soubor, který je zakódovaný base64

anotaceSoubor varchar(50) 0-1

- Označení souboru, který je v položce anotaceObsahu. Např. anotace.zip

#### Odpověď

ciselnik	complex	1-n
oznaceniCiselniku	varchar(40)	1
verzeObsahu	varchar(20)	1
stavVyrizeniPozadavku	complex	1
kod	enum	1
	„0“	
	„1“	
	„-1“	
	„-2“	

popis varchar(32000) 1

### 3.4 Služba „Převzetí protokolu o zpracování číselníku“

Cílem této služby je uložit protokol o zpracování číselníků na „místě aktualizace“ do databáze CSČ. Místem aktualizace se rozumí jakákoliv aplikace na pobočce nebo v centru VZP. V CSČ existuje číselník těchto míst. Tato služba probíhá následovně:

- IPF uloží požadavek do vstupní zprávy CSČ SC\_IN\_Q. Tento požadavek bude obsahovat protokol, místo aktualizace, datum aktualizace, identifikaci paketu, se kterým číselník dorazil na místo aktualizace
- CSČ uloží protokol a vygeneruje odpověď, která se propaguje se do IPF fronty GMCSC\_Q.
- V případě, že dojde při zpracování požadavku k chybě, je vrácen chybový kód ve StavVyřízeníPozadavku a Popis chyby.

#### 3.4.1 Parametry služby

Název služby: Převzetí zprávy o zpracování číselníku

Označení služby: **ProtokolZpracCiselniku**

Označení zprávy: **prevezmiProtokol**

Typ služby: Asynchronní

Požadavek:

nazevProtokolu varchar(255) 1

typProtokolu enum 1

„S“ - protokol o stavu číselníků po aktualizaci

„O“ – Jakýkoliv jiný protokol

protokol base64 1

- V případě typu protokolu = „S“ se jedná o zazipovaný a zakódovaný (base64) xml protokol o zpracování. Schéma tohoto protokolu je uvedeno v přílohách (**ciselnik.xsd – stavAktualizace**).

- V případě typu protokolu = „O“ se jedná o zazipovaný a zakódovaný plane text.

datumVzniku date 1

mistoVzniku varchar(20) 1

- hodnota musí být z číselníku míst aktualizací. Např. číslo pobočky.

identifikace varchar(50) 1

- V případě typu protokolu = „S“ se zde uvádí identifikace paketu, kterým se číselníky aktualizovaly jinak není povinný.

Odpověď

StavVyřízeníPozadavku complex 1

Kod enum 1

„0“

„1“

„-1“

„-2“

Popis

varchar(32000)

1

### 3.5 Služba „Změna stavu paketu“

Cílem této služby je změnit stav paketu. Tato služba bude probíhat následovně:

- IPF uloží požadavek do vstupní zprávy CSC SC\_IN\_Q. Tento požadavek bude obsahovat označení paketu a nový stav
- CSC provede změnu stavu paketu a případě vzniku produkčního paketu provede distribuci

V případě, že dojde při zpracování požadavku k chybě, je vrácen chybový kód ve StavVyrizeniPozadavku a Popis chyby.

#### 3.5.1 Parametry služby

Název služby: Změna stavu paketu

Označení služby: **ZmenaStavuPaketu**

Označení zprávy: **zmenStavPaketu**

Typ služby: Asynchronní

Požadavek:

oznaceniPaketu varchar(20) 1

- Označení paketu musí být ze seznamu typu paketu v CSC

novyStav enum 1

„T“ – testovací paket. Tento stav vznikne automaticky při vygenerování testovacího paketu.

„TZ“ – zamčený testovací paket.

„P“ – produkční paket.

Odpověď

stavVyrizeniPozadavku complex 1

kod enum 1

„0“

„1“

„-1“

„-2“

popis varchar(32000) 1

Pro změnu stavu paketu platí jistá omezující pravidla. Například nemůžete zamykat paket, který je již uzamčený. V následující tabulce je přehled všech povolených kombinací

Nový stav	Původní stav
Testovací – odemknutý	Testovací - zamknutý
Testovací – zamknutý	Testovací - odemknutý
Produkční	Testovací (nezávisí na zamknutí)

### 3.6 WSDL popis služeb

Odpovídající WSDL popisy výše popsaných služeb jsou uvedeny v aplikaci Evidence služeb, do které má dodavatel přístup od podpisu smlouvy na dodávku komponent IS VZP ČR.

## 4. Postup zařazení nových číselníků do CSC

Nový číselník je zařazen na základě žádosti uživatele v aplikaci Centrální správa číselníků. Žádost poté probíhá workflow ve VZP ČR s následujícími kroky:

- 1) Typování žádosti
- 2) Schvalování žádosti
- 3) Vyřízení žádosti
- 4) Prohlížení žádosti

Postup pro vytvoření číselníku je v souladu s Uživatelskou příručkou Centrální správy číselníků následující :

- 1) Administrátor musí založit číselník
  - a. Nastavit
    - i. garanta struktury
    - ii. operátora/y struktury
    - iii. garanta obsahu
    - iv. operátora/y obsahu
    - v. notifikace
  - b. přiřadí číselník do distribučních paketů, nebo vytvoří zcela nový paket pro distribuci
    - i. nastaví způsob distribuce paketu
      1. AQ
      2. Pomocí souborů (File systém)
- 2) operátor struktury
  - a. založí novou strukturu číselníku a dá ke schválení garantovi struktury
- 3) garant struktury
  - a. musí strukturu schválit, odmítnout
- 4) operátor obsahu
  - a. naplní obsah číselníku a předá ke schválení na garanta obsahu
- 5) garant obsahu
  - a. schválí/odmítne obsah k distribuci
- 6) administrátor
  - a. provede distribuci – odeslání paketu s novým obsahem číselníku