Standardy IS VZP – NIS

Verze dokumentu

Verze	Datum	Autor	Popis
3.10	25.6.2021	VZP ČR	

Obsah

1 Úvod

1.1 STANDARDY IS VZP - NIS

- **Představují -** soubor pravidel určených pro vytváření, rozvoj a využívaní 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 ČR jsou povinni** po akceptaci standardu ho respektovat ve znění, v jakém ho přijali.
- **Všichni dodavatelé komponent IS do VZP ČR jsou oprávněni** navrhnout změnu tohoto standardu. Návrh na změnu musí podat formou vypracovaného nového znění**.**
- **Od standardu se lze odchýlit pouze na základě výjimky.**
  Stanovisko k výjimce zpracovává oddělení architektury VZP ČR, 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 ČR o výjimku.
- **Jejich účelem je** nazování a následné provozování IT řešení/komponent v prostředí VZP ČR s požadovanými technickými i právními garancemi, s požadovanými provozními parametry, s požadovanou odbornou aplikační a provozní podporou provozu IT při celkové 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 neznamenala (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 Standardy a požadavky na licenční model dodávaného díla

Pokud je dodavatelem dodáváno plnění, které je chráněno právem duševního vlastnictví, zejména pak plnění, které je autorským dílem nebo se za autorské dílo považuje (srov. § 2 zákona č. 121/2000 Sb., o právu autorském, právech souvisejících s právem autorským a o změně dalších zákonů (autorský zákon), ve znění pozdějších předpisů) (dále jen „**autorské dílo**“), pak jsou ve věci užití takového autorského díla uplatňovány tyto zásady:

2.1.1.1 Dodavatel při realizaci příslušného plnění neporuší práva třetích osob, která těmto osobám mohou plynout z práv duševního vlastnictví, zejména z autorských práv a práv průmyslového vlastnictví.

2.1.1.2 **Software vytvořený dodavatelem tzv. „na míru“:**

Pokud je předmětem plnění dodavatele **dodání nového autorského díla vytvořeného tzv. „na míru“ nebo se jedná o uvolňování dosud neuvolněného autorského díla vytvořeného „na míru“, či úpravu již dříve uvolněného autorského díla vytvořeného „na míru“, pak:**

a) Primárně je k takovému autorskému dílu v souladu s ust. § 58 odst. 1 autorského zákona vždy příslušnou smlouvou dodavatelem postoupen VZP ČR výkon autorských majetkových práv (dále jen „postoupení“). VZP ČR může postoupit právo výkonu majetkových autorských práv na třetí osoby bez jakéhokoli omezení. (VZP ČR tak vstoupí při splnění zákonných

podmínek do veškerých autorských majetkových práv dodavatele k dodávanému autorskému dílu).

b) Pro případ, že bude v budoucnu zjištěno, že dodavatel právo výkonu majetkových práv k příslušným uvolňovaným autorským dílům VZP ČR platně nepostoupil nebo v případech, kdy se VZP ČR a dodavatel výslovně v příslušné smlouvě dohodnou na nevyužití postoupení , vždy je pak k příslušným autorským dílům dodavatelem příslušnou smlouvou poskytována podle § 2358 a násl. občanského zákoníku licence, kdy VZP ČR je příslušné autorské dílo oprávněna užít nejméně takto:

- k jakémukoliv účelu a v rozsahu podle svého uvážení a svých potřeb,
- v původní nebo zpracované či jinak změněné podobě, samostatně nebo v souboru nebo ve spojení s jinými jakýmikoliv díly nebo prvky,
- v neomezeném množstevním a v neomezeném územním rozsahu,
- ke všem způsobům užití (tj. zejména autorské dílo rozmnožovat a dále distribuovat, jakkoliv a kdykoliv je měnit, překládat, zpracovávat, upravovat, spojovat s jiným jakýmkoliv dílem či prvkem, atp.), a to i za pomoci třetích osob a bez jakéhokoliv omezení,
- pokud je autorským dílem software, pak tato licence se vztahuje na příslušný software ve zdrojovém i strojovém kódu, na příslušné související koncepční a přípravné materiály, analytický projekt a jeho postupné úpravy, jakož i na případné další verze příslušného software (upgrade/update), získané či realizované na základě příslušné smlouvy (např. pak i na základě záruky/Technické podpory) nebo na základě jiných smluv a na veškerou související a průběžně dodavatelem upravovanou další související dokumentaci,
- příslušným softwarem, na nějž se tato licence vztahuje, se rozumí vždy počítačový program a související příslušná dokumentace a dále jak příslušná úprava příslušného software, tak upravený příslušný předmětný software jako celek (který je též vždy považován za verzi/upgrade/update) to vše vždy v aktuální podobě a bez ohledu na jeho historické úpravy,
- VZP ČR je oprávněna získat od dodavatele vždy příslušné zdrojové kódy s příslušnou dokumentací, a to vždy v aktuální podobě,
- licence je poskytována jako výhradní,
- licence je poskytována na dobu trvání majetkových práv autora a nelze ji ze strany dodavatele vypovědět, ustanovení § 2370 občanského zákoníku se pro účely licenčního ujednání nepoužije,
- VZP ČR je oprávněna udělit bez omezení třetí osobě podlicenci k užití autorského díla (podlicence), jakož i svoje oprávnění k užití autorského díla třetí osobě bez omezení postoupit (postoupení licence).

2.1.1.3 **Proprietární (tzv. balíkový nebo COTS) software** může být součástí plnění dodavatele pouze s předchozím písemným souhlasem VZP ČR a za dále uvedených podmínek. Dodavatel je povinen ve svých řešeních navrhnout využití především takového proprietárního softwaru, u něhož lze poskytnout licenci rovněž podle bodu 2.1.1.2 tohoto odst. 2.1.1.

Pokud u tohoto software nelze poskytnout oprávnění dle bodu 2.1.1.2 tohoto odst. 2.1.1, bude VZP ČR příslušnou smlouvou poskytnuta licence **zpravidla** takto:

- licence k tomuto autorskému dílu je poskytována jako nevýhradní, v neomezeném územním rozsahu, ke způsobu užití dle potřeb VZP ČR a v rozsahu (věcném i množstevním) podle potřeb VZP ČR; současně je poskytováno VZP ČR též oprávnění užít i nové verze příslušného proprietárního software (upgrade, update, další změny, atd.), které VZP ČR získá podle příslušné smlouvy nebo v rámci příslušné podpory či záruky, apod. , jakož i oprávnění užít příslušnou související dokumentaci, pokud je VZP ČR předána,
- licence k tomuto autorskému dílu je poskytována na dobu trvání majetkových práv autora, přičemž se nepoužije ustanovení § 2370 občanského zákoníku,
- VZP ČR je oprávněna udělit třetí osobě podlicenci k užití proprietárního software (podlicence) nebo i svoje oprávnění k užití proprietárního software třetí osobě postoupit (postoupení licence),
- dodavatel je současně povinen zajistit, aby příslušná oprávnění, která VZP ČR získá, byla v souladu s licenčními podmínkami příslušného „výrobce“.

2.1.1.4 **Open source software** může být součástí plnění vždy pouze s předchozím písemným souhlasem VZP ČR. Před vydáním písemného souhlasu musí být VZP ČR dodavatelem informována, pod jakou veřejnou licencí je příslušný open source poskytován (šířen). Pro užití open source software je dále podmínkou:

- dodavatel je povinen udělit, popř. toto udělení zajistit, VZP ČR oprávnění k veškerému open source software poskytnutému VZP ČR na základě příslušné smlouvy v rozsahu takových veřejných licencí, které se na příslušný open source software vztahují,
- dodavatel k využitému open source software vždy VZP ČR poskytne nebo zprostředkuje poskytnutí úplných komentovaných a nezašifrovaných zdrojových kódů software včetně související dokumentace,
- zahrnutím open source software do plnění podle příslušné smlouvy nesmí dojít k omezení práv VZP ČR k tomuto software, zároveň nesmí zahrnutí open source software do plnění zapříčinit situaci, kdy by plnění podle příslušné smlouvy nebo jeho část muselo být poskytnuto třetí osobě v jakékoli podobě nebo by musel být uveřejněn zdrojový nebo binární kód plnění nebo by musel být uveřejněn zdrojový nebo binární kód spolupracujících komponent, ať už VZP ČR, dodavatelem nebo jinou osobou.

2.1.1.5 V případě, že dodavatel využije při plnění dle příslušné smlouvy **proprietární software anebo open source software,** je za účelem vyloučení vzniku proprietárního uzamčení VZP ČR (tzv. vendor lock-in) povinen, není-li sjednáno jinak, použít výlučně takový software, u kterého je v době využití dále splněna alespoň jedna z následujících podmínek:

- jedná se o software, jenž je na trhu běžně dostupný a který může být upravován udržován, provozován a rozvíjen na území České republiky alespoň třemi (3) na sobě nezávislými a vzájemně nepropojenými subjekty; nebo
- jedná se o software, u kterého je s ohledem na jeho (i) marginální význam, (ii) nekomplikovanou propojitelnost či (iii) oddělitelnost a nahraditelnost v IT prostředí bez nutnosti vynakládání větších prostředků (ne více než 50.000 Kč / rok) zajištěno, že další rozvoj jinou osobou než tvůrcem/distributorem takového software je možné provádět bez toho, aby tím byla dotčena práva nositelů práv k takovému softwaru, neboť nebude nutné zasahovat do zdrojových kódů takovéhoto softwaru anebo proto, že případné nahrazení takovéhoto softwaru nebude představovat výraznější komplikaci a náklad na straněVZP ČR; nebo
- jedná se o software, jehož API („Application Programming Interface“) pokrývá všechny moduly a funkcionality software, je dobře dokumentované, umožňuje zapouzdření software a jeho adaptaci v rámci měnících se podmínek IT prostředí VZP ČR a software bez nutnosti zásahu do zdrojových kódů software, a u kterého dodavatel poskytne VZP ČR právo užít toto rozhraní pro programování aplikací ve stejném rozsahu, jako software;

a u kterého lze zároveň důvodně předpokládat, že tento stav zůstane zachován.

2.1.1.6 **Databáze jako autorské dílo**:

- Databáze, která vznikne, bude vytvořena nebo bude upravena a specifikována v rámci plnění dodavatele dle příslušné smlouvy a bude autorským dílem **vytvořeným „na míru“,** bude postupováno podle způsobu plnění dle bodu 2.1.1.2 této kapitoly.
- Databáze, která bude poskytnuta a specifikována v rámci plnění dodavatele dle příslušné smlouvy, bude autorským dílem, ale **nevytvořeným „na míru“,** bude postupováno dle bodu 2.1.1.3 této kapitoly.

2.1.1.7 **Zvláštní práva pořizovatele databáze**:

- Pokud bude součástí plnění dodavatele podle příslušné smlouvy vytvoření databáze, k níž **dodavatel jako pořizovatel bude vykonávat zvláštní práva k databázi** (§ 88a a násl. autorského zákona), je příslušnou smlouvou dodavatelem k takové databázi na VZP ČR **převáděno** toto zvláštní právo pořizovatele databáze (k tomu viz § 90 odst. 6 autorského zákona). Převodem zvláštního práva pořizovatele databáze pak náleží VZP ČR veškerá oprávnění vyplývající z ustanovení § 88a a násl. autorského zákona.
- Pokud bude součástí plnění dodavatele podle příslušné smlouvy vytvoření/dodání databáze, k níž **VZP ČR ani dodavatel nevykonávají zvláštní právo pořizovatele databáze**, je příslušnou smlouvou dodavatelem k takové databázi **uděleno** dodavatelem VZP ČR **oprávnění** k výkonu tohoto práva – tj. licence/podlicence, a to v rozsahu dle § 90 odst. 1 autorského zákona (dále jen „Licence k databázi“). Licence k databázi je vždy udělena pro vytěžování a zužitkování celého obsahu příslušné databáze, a to na dobu trvání zvláštního práva pořizovatele databáze (§ 90 a § 93 autorského zákona).

2.1.1.8 **Záznamy**:

- K záznamu, který vznikne, bude vytvořen nebo bude upraven v rámci v rámci plnění dodavatele dle příslušné smlouvy nebo v souvislosti s tímto plněním a **dodavatel bude jako pořizovatel záznamu vykonávat právo výrobce**, je příslušnou smlouvou dodavatelem na VZP ČR toto právo výrobce záznamu k příslušnému záznamu převedeno (§ 76 odst. 5 autorského zákona).
- K záznamu, který vznikne, bude vytvořen nebo bude upraven v rámci v rámci plnění dodavatele dle příslušné smlouvy nebo v souvislosti s tímto plněním a **dodavatel nebude jako pořizovatel záznamu vykonávat právo výrobce**, k takového záznamu, je příslušnou smlouvou dodavatelem uděleno VZP ČR oprávnění k výkonu práva výrobce příslušného záznamu, tj. licence (dále jen **„Licence k záznamu“).** Licence k záznamu je udělena v rozsahu práv záznam užít, uvedených v § 76 odst. 2 a § 80 odst. 2 autorského zákona, a to na dobu trvání práv výrobce příslušného záznamu (§ 77 a § 81 autorského zákona).

2.1.1.9 Společná ustanovení k licenčnímu modelu

Podrobně jsou oprávnění k užití dodávaného plnění, které je chráněno právem duševního vlastnictví, upravena v příslušné smlouvě.

2.1.2 Analytická dokumentace

V rámci budování informačních systémů a implementace změn je dodávaná i analytická dokumentace se skládá z:

- Modelů – vytvořených podle standardu UML importovatelných do Sparx EA a použitých v dokumentech
- Strukturovaných dokumentů v textové formě s vloženými modely, respektive generované z modelu

Níže uvedený seznam modelů je volitelný, vhodnou kombinaci zvolí oddělení architektury VZP ČR dle charakteru dodávky. Specifikace rozsahu výstupů bude proveden VZP ČR jako výběr povinně požadovaných dokumentů od dodavatele řešení v rámci specifikace požadavků zadávací dokumentace. Dodavatel zpracuje analytickou dokumentaci v nástroji, který umožní předání těchto modelů do správy VZP ČR formou XMI souborů importovatelných do nástroje Enterprise Architect, alternativně pro předání modelů využije platformu přímo Enterprise Architect. Pro zpracování analytické dokumentace použije standard UML, minimálně ve verzi 2.4 a jazyk BPMN 2.0.2. Požadavek na dodání analytické dokumentace je závazný pro dodávky:

- Dodávka aplikace formou vývoje SW
- Customizace funkcionality aplikace založené na standardním produktu formou vývoje software

Analytická dokumentace se vyžaduje i pro ty části aplikace, které jsou založené na standardním produktu (produkt dodávaný více než 20 zákazníkům dodavatelem nebo výrobcem produktu), který je zdokumentován v produktové dokumentaci předané VZP ČR, pokud oddělení architektury požadavek na dodání analytické dokumentace nestanoví jinak.

V takovém případě bude analytická dokumentace obsahovat analýzu na míru vyhotovených úprav produktového řešení a jeho implementaci. Rozsah modelu je pak závislý na charakteru úprav.

Použité zkratky

BPMN	Business Process Model and Notation; grafická notace a pravidla pro modelování podnikových procesů
CASE	Computer Aided Software/System Engineering; použití výpočetní techniky při návrhu a vývoji počítačových programů
UML	Unified Modeling Language; grafický jazyk pro vizualizaci, specifikaci, navrhování a dokumentaci programových systémů

2.1.2.1 *Vypracování systémové analýzy*

Dodavatel se zavazuje předat jako součást zdrojových kódů **detailní systémovou analýzu pro dodávanou aplikaci (dále Analýza)** v požadovaném rozsahu (dále Analýza) a po dobu jím realizovaného provozu a rozvoje systému také tuto Analýzu udržovat v aktuálním stavu vzhledem ke stavu aplikace.

Analýza bude probíhat ve spolupráci s pracovníky VZP ČR. Hlavním cílem Analýzy je ve formě vhodných modelů a přiměřeného detailu popsat vlastnosti a fungování zamýšlené aplikace, jako jsou zejména:

- Uživatelské funkce poskytované aplikacemi systému
- Automatizované a integrační funkce a algoritmy systému
- Strukturu, forma a způsob ukládání datových informací v systému
- Strukturu, formu a způsob datových rozhraní a komunikací na okolní systémy a rozhraní systému jako takového
- Grafické uživatelské rozhraní

Primární úlohou Systémové analýzy je poskytnout informační nástroj, který umožní oběma stranám (jak dodavateli, tak VZP ČR) vždy vzájemně porozumět vytvořené detailní specifikaci systému ještě před její implementací a tím v maximální míře eliminovat chybové či nezamýšlené chování systému plynoucí ze vzájemného nepochopení.

Předaná Systémová analýza VZP ČR jakožto součást dodávky taktéž musí umožnit v budoucnu svým dostatečným informačním rozsahem bezproblémový přechod dalšího pokračujícího provozu a rozvoje systému na případného jiného dodavatele.

Analýza musí být zpracována v takovém rozsahu a šíři, aby zachytila i celkovou:

- Aplikační architekturu
- Integrační architekturu
- Datovou architekturu
- Technologickou architekturu
- Technické předpoklady, omezení

2.1.2.2 *Forma vypracování a vedení Systémové analýzy*

Dodavatel vypracuje a povede Analýzu pro systém ve formátu dle požadavku 2.1.2.2 Forma vypracování a vedení Systémové analýzy. V dohodnutých případech bude repository EA sdíleno mezi dodavatelem a VZP ČR.

Analýza bude dodavatelem vypracována za použití modelovacího jazyka UML a případně dalších doplňujících běžných modelovacích technik/notací/jazyků (Wireframe, Archimate, viz dále).

2.1.2.3 *Rozsah vypracování a vedení Systémové analýzy*

Dodavatel vypracuje a povede Analýzu v přiměřeném rozsahu a informační hloubce pro její pochopení jak stranou VZP ČR, tak stranou dodavatele jako implementátora systému. Analýza bude minimálně obsahovat následující modely (mohou být omezeny s odhledem na zadávací dokumentaci a požadavky na dodávku):

- Strukturovaný seznam požadavků *… s využitím Modelu požadavků*
  - popis potřeby/záměru
  - provázání s analytickými prvky, kterými je požadavek řešen
- Popis návrhu řešení
- Detailní funkční popis *… s využitím Modelu případů užití*
  - popis dynamického chování systému jakými jsou např. uživatelské funkce, systémové výpočetní algoritmy, automatizované systémové funkce a procesy či systémové komunikace s externími systémy
- Popis dat v systému *… s využitím Modelu tříd*
  - popis struktury, formy a způsobu perzistence dat v systému
  - popis případných stavů a stavových přechodů pro životní cykly datových záznamů
- Popis datových rozhraní *… s využitím Modelu tříd*
  - popis struktury, formy a způsobu datových rozhraní vystavených aplikací
  - popis struktury, formy a způsobu datových rozhraní okolních systémů, s nimiž aplikace komunikuje
- Návrh obrazovek …. *s využitím Wireframe nebo obdobné techniky*
  - prototypy hlavních obrazovek
- Funkční architektura systému *… s využitím Komponentního modelu či modelů Archimate*
  - popis funkčních bloků/komponent/aplikací systému
  - schéma a popis jejich logického uspořádání a způsobu a formy vzájemné komunikace
- Funkční architektura integrace systému / Okolí systému *… s využitím Komponentního modelu či modelů Archimate*
  - popis okolních systémů a účelu komunikace s nimi
  - schéma a popis způsobu a formy funkční a datové komunikace

Další typy modelovacích pohledů UML (Model aktivit, Komponentní model, Sekvenční model, …) či dalších jazyků/notací (Archimate, BPMN, …) mohou být použity, je-li to ku prospěchu sdělnosti příslušného analytického tématu.

2.1.2.4 *Předání výstupů Systémové analýzy*

Dodavatel se zavazuje poskytnout a předat VZP ČR všechny informace a podklady, které tvoří dodavatelem vypracovanou Analýzu l akceptaci.

Dodavatel bude předávat export před každou akceptací dodávky nebo změny nebo na vyžádání nebude-li pracovat v repository VZP ČR nebo sdílené repository. Dále může být na základě žádosti dodavatele přístup pro čtení stávajících modelů nebo i pro tvorbu modelů dodavatele.

Dodavatel musí VZP ČR předat vždy aktuální stav Analýzy v takové technické zdrojové formě, která VZP ČR umožní tuto Analýzu s pomocí EA dále rozvíjet – tj. nejen číst, ale i doplňovat, měnit, a to v podobě datové exportu z EA nástroje, který bude plně a funkčně importovatelný do EA VZP ČR. Fyzické předání bude provedeno dodavatelem do GIT VZP ČR, kterou je Azure Pipelines.

V případě, že je dodavateli povolen přístup do repository VZP ČR, je předání formálně potvrzeno předávacím protokolem pro zdrojové kódy.

V průběhu projektové fáze Implementace systému je třeba v důsledku nových zjištění či upřesnění provést změny do již schválených částí Analýzy. Tyto musí být opět předány VZP ČR.
Dodavatel bude poskytovat nově vypracované nebo upravené části Analýzy ke schválení dodavateli v postupných přírůstcích obdobně jako zdrojový kód aplikace.

2.1.3 Dokumentace pro rozhodnutí OHA MV ČR

Je-li v případě veřejné soutěže v závislosti na charakteru informačního systému nutné stanovisko Odboru hlavního architekta MV ČR v souladu se zákonem č. 365/2000 Sb., o informačních systémech veřejné správy, usnesením vlády č. 86 ze dne 27. 1. 2020, je součástí dokumentace řešení i formulář žádosti o stanovisko a jeho přílohy.
Náplň formuláře je dána metodikou OHA.
Formulář A – nákup nových nebo významně pozměněných informačních systémů
Formulář B – smlouva o provozu, podpoře, údržbě IS nebo potenciálním legislativním rozvoji existujícího řešení
Formulář C – při pořízení typizovaného komoditního ICT produktu
Formulář D – pro spotřební materiál nebo náhradní díly

2.1.4 Standardy uživatelského rozhraní

Aplikace dodané do prostředí VZP ČR budou plnit následující standardy uživatelského prostředí:

Definice požadavku
Uživatelské prostředí bude optimalizováno pro minimální standardy vybavení uživatele, který tvoří: - Operační systém MS Windows 10 - Minimální konfigurace PC: procesor Intel / AMD, 2 jádra, 8 GB RAM, 512 GB SSD pevný disk, připojení do sítě 50 MB/sec. - Rozlišení monitoru: Full HD (1920 x 1080) - Tiskový výstup - Uživatel je ověřován vůči MS AD, protokolem NTLM ve webových aplikacích - Na stanicích je dostupné aplikační vybavení: prohlížeče Chrome a Edge, PDF Acrobat, MS Office

Pro definici uživatelských vizuálních prvků v prostředí internetového prohlížeče bude použit značkovací jazyk ve standardu HTML5. Žádný z prvků uživatelského rozhraní nebude obsahovat přímou definici vzhledu, definice vzhledu bude ve zdrojovém i výsledném kódu oddělena od definice obsahu a struktury jednotlivých vizuálních prvků. Vzhled prvků bude definován s využitím kaskádových stylů CSS.
Pro skriptování bude využit jazyk JavaScript, s možností využití rozšiřujících knihoven nebo nástaveb.
Grafické uživatelské rozhraní aplikace se bude přizpůsobovat různým rozlišením na úrovni standardům VZP ČR pro pracovní stanice
Každý typ ovládacího nebo formulářového prvku v aplikaci bude mít samostatnou, avšak jednotnou definici vzhledu.

Vzhled jednotlivých aplikačních formulářů bude konzistentní, tedy umožní uživatelům aplikovat naučené návyky a postupy pracovních úkonů na všech formulářích obdobného typu stejně.
Uživatelské prostředí bude konfigurovatelné. Uživatel si bude moci nastavit velikost zobrazovaného písma a základní barvy v aplikaci bez dopadu na funkcionalitu aplikace. Pro nastavení parametrů vzhledu bude mít aplikace aplikační formulář, který nastavení uloží do databáze.
Každá uživatelská operace, která bude měnit obsah databáze, před jejím provedením, bude vyžadovat potvrzení uživatelem s využitím výzvy pro potvrzení akce nebo modálního okna, kde bude akce potvrzena.
Uživatelské rozhraní bude odpovídat platným požadavkům a doporučením v souladu s normou ČSN EN ISO 9241, a to zejména:

- Požadavky na formuláře,
- Prezentaci informací,
- Interakce,
- Volbu prvků formulářů.

Každá obrazovka bude obsahovat kontextovou nápovědu k obsahu a funkcím obrazovky.
Každá obrazovka bude obsahovat číselný identifikátor obrazovky a informace o verzi aplikace.
Uživatel nebude moci opustit zobrazený formulář bez výzvy k uložení rozpracované akce nebo k opuštění formuláře bez uložení změn.
Jazykem systému pro práci uživatele je český jazyk, pro rozhraní administrátora se připouští jazyk anglický, pokud požadavky nestanoví jinak. Formulářová část systému musí mít kontrolu dat již při vyplňování formulářů a pomoc při vyplňování s kontextovou nápovědou (automatické výpočty). Základní validace vstupních dat z formulářů budou probíhat bez odeslání dat na server přímo v prohlížeči.
Uživatelské rozhraní nebude vyžadovat instalaci specifických komponent a rozšíření do prohlížeče uživatele ve standardu pracovní stanice.
Všechny uživatelské formuláře budou dostupné ze strukturovaných nabídek v menu, pokud nejsou součástí uceleného procesu.
Aplikační formuláře s detailním záznamem nebo souhrnem záznamů musí umožňovat poskytovat možnost tisku zobrazených dat a jejich uložení na stanici uživatele do formátu PDF, DOCX nebo obdobného.
Hlavní aplikační formulář se bude skládat z povinných sekcí

- Záhlaví okna – nachází se v horní části aplikace a obsahuje následující údaje menu aplikace těsně pod záhlavím okna. Menu bude typu pull-down a jeho obsah bude sestaven na základě aplikačních rolí uživatele.
- Ikonová lišta – obsahuje ikony pro rychlé volání funkcí pomocí myši.
- Panel nástrojů a informací – prostor pro zobrazení identifikačních informací a umístění aplikačních nástrojů.
- Pracovní oblast – prostor pro aplikační formuláře.
- Lišta zpráv a hlášení – je umístěna pod formulářem a obsahuje zprávy od aplikace pro přihlášeného uživatele.
- Lišta stavových údajů – obsahuje další údaje, například počet vybraných záznamů, po-řadí aktivního záznamů atd.

Data do formulářů, zejména typu GRID budou asynchronně načítány v případě potřeby, nebude docházet k odesílání celého formuláře na server k aktualizaci dat ve formuláři.
Dodavatel ve svých aplikačních formulářích použije druhy formulářů z následujícího obecného členění, kdy VZP ČR pro vybrané typy formulářů definuje společná pravidla pro jejich chování. Jedná se o následující typy aplikačních formulářů:

- Výpis informací bez interakce,
- Editační formulář s tlačítky pro jednotlivé operace
- Master detail formulář pro výběr entity a její přímou editaci na formuláři,
- Formulář typu “GRID“ se seznamem jednotlivých entit umožňující jejich postupné procházení,
- Vyhledávací formulář,
- Report,
- Dialogový formulář
- Modální okno
- Formulář se záložkami
- Výpis informací bez interakce (např. statický report)

Editační formulář s tlačítky pro jednotlivé operace

- Tlačítka všech obdobných formulářů budou vždy ve stejném pořadí na spodní straně formuláře na stejném místě a v případě, že se formulář nevejde na jednu stránku, budou tlačítka i na horní straně formuláře,
- Po uložení dat formuláře bude uživateli zobrazena vždy obrazovka nebo formulář, z které se na editační formulář dostal se záznamem, který ve formuláři editoval,
- Před uložením změny bude uživatel vyzván k potvrzení akce,
- Povinná pole budou odlišena, doporučení je barevné odlišení

Master detail formulář

- Formulář bude sloužit pro editaci entit jednoho typu spojených s hlavní entitou v poměru 1:N,
- V záhlaví budou vždy v read only podobě uvedena data hlavní entity,
- Ve spodní části bude obsažen formulář typu „GRID“, který bude splňovat požadavky na tento typ formuláře a obsahovat seznam svázaných entit,
- Po uzavření formuláře bude uživateli zobrazena vždy obrazovka nebo formulář, se seznamem typu hlavní entity, z které se na master-detail formulář uživatel dostal se záznamem, který byl ve formuláři zobrazen,
- Na master-detail formuláři může být měněn stav hlavní entity, je možné i editovat její vybrané atributy. Pro editaci entity by však měl být zpravidla použit editační formulář.
- Formulář umožní zobrazit historii změn u editované entity.

Formulář typu “GRID“:

- Slouží pro zobrazení hodnot entity jednoho druhu ve sloupcovém přehledu,
- Formulář typu GRID bude v horní části obsahovat vyhledávací formulář, který umožní filtrování zobrazeného seznamu,
- Vyhledávací formulář bude obsahovat pouze některé atributy entity, vhodně zvolené, avšak uživatel bude mít možnost do vyhledávání použít všechny atributy entity,
- Procházení seznamu entit bude možné s pomocí tlačítek, které budou posunovat seznam o jednu stránku nebo na stránku zadanou uživatelem, případně na začátek nebo na konec seznamu,
- Seznam sloupců bude uživatelsky konfigurovatelný, uživatel bude moci sloupce přidat nebo odebrat.
- Třídění – seznam bude možné třídit podle hodnot jednotlivých sloupců vzestupně nebo sestupně ev. filtrovat podle hodnot v konkrétním sloupci,
- Stránkování – uživatel bude moci vybrat rozsah zobrazeného seznamu z přednastavených hodnot, např. 20/50/100

Všechny nastavení formuláře, které provede uživatel na konkrétním formuláři, se budou ukládat pro konkrétního uživatele a aplikují se při každém zobrazení formuláře, vyjma nastavení třídění a filtrování. Filtry bude možné na formuláři uložit do seznamu filtrů.

Vyhledávací formulář – slouží pro vyhledávání entit, většinou nad formulářem typu GRID:

- Formulář umožní vyhledávání podle základních atributů entity nebo navázaných číselníků,
- Uživatel bude moci rozšířit formulář o nezobrazené atributy entity, které do formuláře bude moci přidat a vyhledávat podle nich,
- Nastavený filtr vyhledávání bude moci uživatel uložit do seznamu vyhledávání na každém takovém formuláři,
- Systém umožní vyhledávání (formou masky se zástupnými znaky) a třídění dat.

Dialogový formulář

- Slouží pro reakci na výzvu nějakého jiného formuláře,
- Umožní vždy potvrdit nebo zrušit nabízenou akci,
- Do potvrzení akce uživatelem nebo zavření dialogu se chová jako modální okno a není možné se vrátit do původního formuláře.
- Stisknutím klávesy ESC a/nebo příslušným tlačítkem bude možné formulář zavřít bez provedení akce, kterou obsahuje dialogový formulář.

Modální okno – slouží pro zobrazení formuláře, které způsobí, že uživatel nemůže bez zavření modálního okna pracovat v jiné části aplikace.

Formulář se záložkami

- Pro každou záložku bude existovat název a klávesová zkratka pro její zobrazení,
- Pokud bude na záložce editační formulář, nebude možné opustit záložku formuláře s neuloženými změnami bez výzvy uživateli k potvrzení opuštění bez uložení změn nebo k jejich uložení.

Pořadí tlačítek jednotlivých akcí a jejich pojmenování bude na formulářích vždy sjednoceno v rámci aplikace k dosažení vhodné ergonomie práce aplikací..

Formuláře budou mít podporu pro elektronickými certifikáty.

Aplikace bude plně využitelná i pro osoby se zdravotním postižením (WCAG verze 2.0 dle doporučení konsorcia W3C, Vyhláška č. 64/2008 o přístupnosti).

2.1.5 Požadavky na předávaný zdrojový kód, strukturu a architekturu aplikace

Pokud zadávací dokumentace obsahuje požadavek na předání zdrojového kódu a binární podoby aplikace pro instalaci, provede se dodávku v souladu se zde uvedeným požadavky. Tento požadavek je svázán zejména s dodávkou aplikací programovaných na míru dle požadavků VZP ČR nebo aplikací, které budou překládány pro potřeby VZP ČR z upraveného zdrojového kódu do binárního.

Slovník

Azure Repos	Úložiště zdrojových kódů, GIT
Azure Pipelines	CI/CD nástroj pro sestavení instalačních balíčků, testování, distribuci a nasazování aplikací
Azure Artifact	Prostředí pro správu a sdílení balíčků

Za zdrojový kód standardy VZP ČR považují všechny výstupy dodavatele nezbytné pro sestavení spustitelného tvaru aplikace i výstupy při vývoji aplikace vytvořené, či nezbytné pro pochopení funkcionality aplikace. A to zejména:

- Zdrojový programátorský kód,
- Analytické modely vytvořené v rámci dodávky – předávány do úložiště Enterprise architect
- Konfigurační soubory,

- Konfigurační soubory nezbytné pro sestavení binárního tvaru aplikace,
- Knihovny zdrojového kódu použité pro sestavení binárního tvaru aplikace,
- Programátorská dokumentace ve tvaru zdrojových komentářů i generované dokumentace,
- Konfigurace pro vývojové prostředí (IDE) programátora, která nastavuje parametry prostředí IDE
- Unit testy
- SQL skripty,
- Skripty plnící databázi, např. číselníky,
- Grafika použitá pro aplikaci,
- Ostatní soubory a dokumenty.

Dodavatel nesmí do Azure Repos VZP ČR uložit potencionálně škodlivý kód.
Všechny externí knihovny a balíčky a binární obsah vyjma zdrojového kódu aplikace dodavatel uloží do Azure Artifactory s tím, že předá a naimplementuje konfiguraci pro automatickou aktualizaci balíčků z externích zdrojů.

Dodavatel je povinen předat zdrojový kód do prostředí Azure Repos VZP ČR vždy v aktuální verzi releasu, který bude předmětem nasazení, předání nebo akceptace.

Výsledný instalační balíček aplikace, který bude nasazen do jakéhokoliv prostředí VZP ČR jako oprava chyby, nasazení nového releasu, předání aplikace nebo k akceptaci ze strany VZP ČR bude vytvořen pouze z obsahu v Azure Repos a Azure Artifact s využitím procesů nakonfigurovaných dodavatelem v Azure Pipelines.

Zdrojový kód naplní následující požadavky:

Definice požadavku
VZP ČR neomezuje programovací jazyky, nicméně u použitých technologií zejména s ohledem na ochranu investic vyžaduje dlouhodobou garanci provozu aplikace a dostatek běžně dostupných lidských zdrojů pro budoucí aplikační rozvoj. Programovací jazyk dodávané aplikace musí být kompatibilní s požadavky standardů VZP ČR na aplikační servery, databáze a operační systémy. Požadavek se nevztahuje na produkty, které nebudou předmětem vývoje nebo SW úprav vývojem ze strany dodavatele a půjde zároveň o produkty třetích stran. Pojmenování objektů, metod a vlastností ve zdrojovém kódu bude zvoleno tak, aby bylo zřejmé, čeho se daný prvek týká, co obsahuje nebo co dělá. Přičemž VZP ČR připouští pro programový kód pojmenování elementů v anglickém jazyce s následujícím pravidly: *Třídy* – k pojmenování bude použito podstatné jméno ve formátu Pascal case. *Rozhraní* – k pojmenování bude použito podstatné jméno nebo přídavné jméno vyjadřující chování (např. IDisposable) ve formátu Pascal case s předponu I. Atributy – bude použito Pascal case. *Statické položky* pro pojmenování bude použit Pascal case s podstatným jménem. *Parametry* – bude použito pojmenování v Camel case. *Metody* – bude použito Camel case, pro název metody bude využito sloveso (např. compute, start atd.)

Pascal case je způsob zápisu, je použito velké písmeno v prvním a každém dalším slově názvu, např. BeginInvoke, FileName atd.

Camel case používá malého písmena v prvním a velkého písmena v každém dalším slově názvu, např. customerOrders, tempFileName atd.

Repository zdrojové kódu a nástroje a CI/CD

Definice požadavku

Dodavatel dodá zdrojový kód do určené databáze zdrojových kódů v prostředí Azure Repos/ Artifacts ke správě verzí zdrojového kódu a vytvoření a nasazování instalačních balíčků (CI/CD) na aplikační servery a změnových skriptů do databáze automatizovaným způsobem s pomocí Azure Pipelines.

Dodavatel odpovídá za to, že jim předané skripty a konfigurace pro vytvoření binárního tvaru aplikace, spuštění automatických testů a distribuce výsledných balíčků a do prostředí Azure Pipelines, přeloží aplikaci do takové podoby, že bude nasaditelná/spustitelná v kvalitě, která je vyžadována pro akceptaci dodávky.t

V Azure Repos bude uložen a verzován veškerý zdrojový kód aplikace vyjma analytických modelů, dodavatel sem bude umísťovat zdrojový kód i v rámci vývoje změnových požadavků.

Nasazení aplikací bude realizováno vždy pouze z Azure Pipelines prostřednictvím zde vytvořených konfigurací. V případě požadavku VZP ČR bude dodavatel instalační balíčky nasazovat manuálně.

Nástroj pro automatický build CI/CD bude ze zdrojových kódů vytvářet instalační balíčky a tyto nahrávat na jednotlivé servery. Konfiguraci provede dodavatel
Pro nasazení jsou požadovány minimálně čtyři typová prostředí (dev, test, předprodukce , produkce)

Dodavatel definuje v Azure Pipelines automatické kontroly (buildy) ověřující základní funkčnost (tj. lze buildovat i po změně).

Dodavatel definuje samotný build celé aplikace (ideálně celku, a nikoliv dílčí části)

Výstupem buildu je samotná aplikace v binární nasaditelné podobě (produkt/artifakt)

Dodavatel spolupracuje s VZP ČR na automatizaci nasazení produktů/artifaktů do příslušných prostředí VZP ČR

- Automatizace využívá nástroje Azure DevOps Pipelines (Releases)
- Vstupem pro automatické nasazení je vždy produkt/artifakt získaný z Azure Pipelines,
- Stejný balíček (artifakt) je vždy nasazen postupně nejprve na test a na základě rozhodnutí VZP ČR na produkci

2.1.6 Požadavky na vývojové a implementační postupy (Open Development Framework)

Pro implementaci zákaznických aplikací pro VZP ČR je povinně aplikován Open Development Framework (ODF) – tj platforma nástrojů a postupů pro vývoj a správu software umožňující úzkou spolupráci IT vývoje a businessu na bázi rychlých, kontinuálních, agilních a dokumentovaných postupů vývoje SW.
Účelem vyžití takové platformy je mimo zvýšení efektivity eliminaci tzv. vendor lock-in a to formou standardizace pracovních postupů, dokumentace, udržení znalostí.

V rámci ODF jsou využívány Aplikační Frameworky – softwareové platformy vývojářských nástrojů, postupů, knihoven pro samotný vývoj software a to zejména ve vazbě na programovací jazyky a samotnou aplikaci a její běhové prostředí. Slouží zejména k programování a běhu aplikace. Jde o technickou podmnožinu ODF pro programování.
Framework je modulární systém, který se z licenčního pohledu řídí podmínkami vyplývajícími ze základního obsahu softwarových prvků frameworku (komponent), přičemž mohou mít specifické licenční podmínky za zachování podmínek kompatibility s požadavky na předávaný zdrojový kód aplikací.

Příkladem je OracleForms, Oracle Reports, AngularJS, React, Spring

2.1.6.1 *Definice požadavku ODF na Aplikační frameworky*

Vývoj zákaznických aplikací je prováděn pomocí LowCodePlatform aplikačních frameworků ve vizuálních IDE prostředích.

Aplikace připravené pomocí frameworku musí splňovat podmínky hostingu dle tohoto standardu.

Aplikace – komponenty samotného frameworku musí splňovat podmínky dle tohoto standardu.

Framework musí být kompatibilní s požadavky na předávaný zdrojový kód aplikací, zejména uvedenými v 2.1.4 Standardy uživatelského rozhraní a 2.1.5 Požadavky na předávaný zdrojový kód, strukturu a architekturu aplikace.

Framework nesmí vytvářet závislost VZP ČR na dodavateli aplikačního software. Použití technologie frameworku nesmí vázat na konkrétního dodavatele.

Framework musí umožňovat VZP ČR realizovat změny a úpravy aplikací, procesů vlastními silami nebo třetími stranami.

Vývojové, dokumentační, testovací nástroje a postupy frameworku umožňují vývojářům analytikům a zástupcům business útvarů rychlý vývoj autonomních aplikací na bázi tzv. „low-code“ bez hlubokých znalostí kódování a programování, a to ve vizuálním vývojovém prostředí. „Low code“ musí být omezen na naprosté minimum.

Framework může být sestaven z komerčně dostupných technologických prostředí, open source prostředí, knihoven nebo jiných prvků.

Framework může být dodavatelem frameworku doplněn o další součásti pomocí připravených skriptů nebo dalšího zákaznického software. V takovém případě se stává

z hlediska VZP ČR výrobcem těchto komponent a je nejméně po dobu jeho využívání povinen zajistit podporu výrobce.

Dodavatel frameworku je povinen zajistit či postoupit VZP ČR všechna práva nutná k dalšímu využívání jím vytvořených součástí a konfigurací postačující pro další rozvoj a využívání frameworku VZP ČR ať samostatně nebo s pomocí libovolného jiného dodavatele.

Licenční ujednání žádné z komponent frameworku nesmí vytvořit pro VZP ČR ani případné další dodavatele žádnou zvláštní povinnost, zejména ne povinnost zveřejňovat zákaznický kód vytvořený s pomocí takto licencovaných nástrojů a software.

Pro každou komponentu aplikačního frameworku musí existovat v ČR nejméně 3 dodavatelé schopní zajistit údržbu a rozvoj frameworku.

Pro Framework musí v ČR nejméně 5 významných dodavatelů [1] schopných provádět rozvoj a údržbu alikací s pomocí tohoto frameworku a poskytovat takové služby dalším zákazníkům.

2.1.7 Třídy Aplikací

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

2.1.7.1 *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).

2.1.7.2 *Třída B*

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

2.2 Požadavky na škálovatelnost, odezvu a rychlost aplikací

Požadavky na škálovatelnost, odezvu a rychlost aplikace

Definice požadavku
V aplikaci, která bude výsledkem dodávky bude použita architektury systému, kde je požadavkem VZP ČR oddělení business logiky od prezentace a dat, garance škálovatelnosti a auditovatelnosti systému a možnost dalšího rozvoje a rozšíření o další funkčností a systémy nezávisle na dodavateli. Architektura celého systému bude navržena tak, aby bylo možné kontinuálně dodržovat provozní parametry systému požadované na rychlost, odezvu, kapacitu a provoz systému bez ohledu na počet transakcí, které v systému budou probíhat. Všechny moduly aplikace budou na sobě nezávislé a bude možné škálovat jejich výkon díky použitým technologiím a architektuře bez nutnosti zásahu do aplikace jen na úrovni HW a SW infrastruktury např. posílením výkonu, přidáním serveru, přidáním load balanceru apod.

[1] Za významného dodavatele považuje VZP ČR dodavatele, který dodává služby vývoje, rozvoje a podpory sotware založených na předmětmém frameworku za více než 10 mil. kč za poslední tři roky v prostředí EU.

Komunikace mezi jednotlivými vrstvami bude probíhat prostřednictvím standardních komunikačních protokol.
Aplikace a dodaný aplikační software nebude závislý na dodané hardwarové platformě a bude možné ji v budoucnu migrovat na jinou HW platformu jiného výrobce.
VZP ČR předpokládá zhotovení takové aplikace s využitím programovacího jazyka, která po přeložení do spustitelné podoby nebude závislá na běhu v konkrétním aplikačním serveru konkrétního výrobce a za přiměřeného úsilí na případné změny nebude závislá ani na konkrétní databázové platformě.
Rychlost úplného zobrazení požadovaných dat z databáze v aplikaci na obrazovce uživatele od požadavku do jejich zobrazení bude v rámci běžného provozu maximálně 5 sec.
VZP ČR zároveň požaduje, aby se vybraná data, např. číselníky a položky ze zobrazovaných seznamů načítala asynchronně tak, aby celková odezva pro uživatele nebyla načítáním takových dat ovlivněna.
Rychlost odezvy aplikace při zápisu dat do databáze v aplikaci od odeslání aplikačního formuláře na server do zobrazení potvrzení o provedené operaci v databázi na obrazovce uživatele bude v rámci běžného provozu maximálně 6 sec.
Rychlost odezvy výpočetní operace při výpočtu hodnoty dávky od požadavku na výpočet do zobrazení na obrazovce uživatele bude max. 6 sekund.
Požadavkem VZP ČR je, aby jednotlivé operace, které provádí uživatelé nad různými klienty, na sebe vzájemně nečekali, avšak zároveň, aby při operacích nad jedním klientem při změně jeho dat nebo výpočtu dávky nebylo možné výsledky operací uživatelů a systému vybraných business operací možné si vzájemně přepisovat.
VZP ČR požaduje pro aplikace kategorie A, aby jednotlivé komponenty pro aplikační servery, která jsou součástí aplikace, umožňovaly vybudovat clusterové řešení v režimu active-pasive i active-active.
Řešení musí být navrženo jako robustní a spolehlivé, bez „Single point of failure“, tedy tak, aby výpadek jediné komponenty nezpůsobil výpadek celého systému nebo ztrátu dat.
Budou-li využity některé open source komponenty při vývoji bude dodavatel zodpovědný za přenesení výsledků zpět do open source komunity ve vhodných oblastech a dále zajistí respektování komunitních pravidel při výrobě částí komponent, které mají být předány zpět komunitě.
VZP ČR požaduje, aby dodavatel ať už při volbě způsobu vývoje aplikace nebo výběrem technologií postupoval způsobem, který umožní snadnou modifikovatelnost a rozšiřitelnost aplikace, kdy změna jedné funkce nebude vyžadovat rozsáhlé a průřezové změny aplikace nebo její architektury. Rozšiřitelnost systému musí být zajištěna ve smyslu:

- rozšíření množství funkcionalit, procesů či agend,
- množství uživatelů,
- možnost postupného zapojování modulů

Rozšiřování systému musí být možné zadat dalšímu dodavateli, nezávisle na původním dodavateli systému.
Použité technologie musí mít garanci průběžného vývoje a oprav po dobu deseti let od zahájení produkčního provozu a podpory od výrobce nebo dodavatele.

Dodavatel nastavuje automatické akce nad dodanými zdrojovými kódy v Azure DevOps Pipelines.

Součinnost VZP ČR v rámci procesu správy zdrojového kódu a procesů build a release

poskytuje prostředí Azure DevOps

aktivně se podílí na konfiguraci nasazovacích agentů (serverů vykonávajících automatizaci nasazení)

aktivně se podílí na konfiguraci síťových prostředí a prostupů potřebných pro nasazení z Azure DevOps

aktivně se podílí na definici automatizace samotného procesu nasazení (skriptování)

Součinnost dodavatele v rámci procesu správy zdrojového kódu a procesů build a release

Předává zdrojové kódy do Azure Repos

Navrhuje aplikace tak, aby splňovala podmínky pro použití principů Devops, Azure Repos a Pipelines a naplnění podmínek standardu (oddělení konfigurace od zdrojových kódů, opakovatelnost…)

Definuje automatizaci kontrol (lze buildovat, tzv. Continuous Integration)

Definuje automatizace vytváření produktu/artifaktů (tj. build)

Vznáší požadavky na nasazovací a buildovací agenty

Spolupracuje při definici kroků nezbytných pro nasazení do testovacího prostředí

Naplnění zde uvedených požadavků jsou nezbytnou součástí akceptace dodávky do prostředí VZP ČR.

2.3 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[2], tam kde je to možné.
- Veškeré vazby systému na ostatní systémy jsou formou volné vazby (loosely coupled), doporučeným mechanizmem aplikační komunikace je využití messagingu, případně synchronních REST služeb.
- Pro přenos souborů (MFT) a datových objektů větších, než 2 MB 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[3]).
- Spojení mezi stávajícími systémy VZP ČR provádět přes integrační platformu (ESB).
- V maximální možné míře je nutno využívat stávajících již implementovaných aplikačních služeb nabízených v infrastruktuře VZP ČR.

[2] (https://en.wikipedia.org/wiki/Idempotence)

[3] http://restcookbook.com/Basics/hateoas/

- 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 nepřípustné;
- Proces zpracování dávek (batch, ETL, MFT) musí obsahovat dílčí kontrolní body a kontrolní mechanizmy.
- Detailní specifikace integračního a komunikačního standardu prostřednictvím IPF je popsána v metodikách implementace, dokumentace a homologace integračních služeb v příloze 5, 6, 7.

2.3.1 Integrace se stávajícím IS

Ke dni vzniku tohoto standardu VZP ČR provozuje i 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.

2.4 Vývojové standardy Vlastník kapitoly: OAVRZ

2.4.1 Schválené nástroje pro vybrané fáze vývoje sw aplikací

Oblast	Interně vyvíjené aplikace	Externí dodávky aplikačního charakteru
Funkční analýza a design	Enterprise Architekt, MS Word, Balsamiq Mockups	Dle volby dodavatele splňující předpoklady kapitoly 2.1.3
Technický design-aplikační logika	Visual Studio 2015/2017	Dle volby dodavatele
Technický design-datový design	Visual Studio 2017 Database Tools (MSSQL / Oracle)	Dle volby dodavatele splňující předpoklady kapitoly 2.1.3
Technický design-integrační procesy	OpenAPI / AutoRest (Enterprise Architect, MS Word)	Dle volby dodavatele splňující předpoklady kapitoly 2.1.3
Správa verzí	Azure Pipelines	Azure Pipelines
Vývoj aplikací	Visual Studio 2015/2017, Visual Studio Code, SQL Server Management Studio, XCode / Android Studio, SOAP UI, Postman	Dle volby dodavatele splňující požadavky kapitoly 2.1.6
Migrace a deployment aplikací	Azure DevOps	Azure DevOps

2.4.2 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

- Vyvíjená aplikace bude verzována pomocí tzv. sémantického verzování[3]

2.5 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 datech
- Pokud to charakter testu neumožňuje tak se provádí testování na pseudonymizovaných datech (vyžaduje to například vyhodnocení testu, nebo jeho neproveditelnost na anonymizovaných datech)
- Součástí řešení jsou nástroje pro anonymizaci/pseudonymizaci testovacích dat.
- Musí být zajištěna jednotná anonymizace/pseudonymizace dat integrovaných aplikací v rámci testovacího prostředí
-

2.5.1 Typy požadovaných testů pro předání do provozu IT

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

Nefunkční testy

[3] https://semver.org/lang/cs/

[4] Společně s testery VZP ČR znamená poskytnutí přiměřené součinnosti VZP ČR k provedení a přípravě testu tam kde je to věcně nezbytné.

Název testu	Provádí	Vstupy	Výstupy
zátěžový test[4] 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 o ověření provedení obnovy ze zálohy. (Zpráva o výsledku testu)

Bezpečnostní testy

Název testu	Provádí	Vstupy	Výstupy
bezpečnostní test	testeři OIKB ČR	Identifikace komponent k testování (dodavatel a VZP ČR)	Výsledky testu provedeného dle standardní metodiky (například OWASP, OSSTMM dle typu aplikace). Dále bude předložen plán k eliminaci nalezených hrozeb.

[4] Pro zátěžové testy prefreuje VZP ČR nástroj jMeter (https://jmeter.apache.org/)

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 provedeného dle standardní metodiky pro webové aplikace, tj. například OWASP, a to včetně plánu eliminace nalezených hrozeb.
Bezpečný vývoj aplikace	dodavatel	Vyvíjená aplikace	Vývoj aplikace bude probíhat dle obecně uznávaných metodik „bezpečný vývoj aplikace“, včetně například využívání enterprise verze GIThub pro testování vyvíjeného kódu.

Akceptační uživatelské testy

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

Testy integračních služeb a adaptérů aplikací vystavených na IPF

- Součástí dodávky pro všechny služby vystavené na IPF jsou SoapUI testy,
- které bude možné použít v aplikaci Test Services a to včetně vzorů pro vyhodnocení odpovědi.
- SoapUI testy budou svojí strukturou, členěním odpovídat vzorům uvedeným v dokumentu Struktura SoapUI testů pro MIPF
- Budou použity Centrální i environmentální properties, které se budou automaticky načítat při startu aplikace a pomocí groovy skriptů, endpointy budou dynamicky skládané dle těchto properties.
- Nad odpovědmi budou prováděny validace (assertions) minimálně na úrovni SOAP Response, Schema Compliance, Not SOAP Fault, Response SLA a Property Content.

Validace, které jsou specifické pro jednotlivá prostředí je možné provádět na úrovni Test Services pomocí regulárních výrazů. Pro testy SOAP asynchronnich služeb budou na úrovni projektu rozšířeny o deklaraci SOAPBinding-u pro callback a generovanou definici mockService definovanou pro tento SOAPBinding.

- Asynchonní AQ scénáře budou realizované formou groovy test kroků dle popisu funkčnosti ve výše uvedeném dokumentu Struktura SoapUI testů pro MIPF .

2.6 Požadavky na testovací dokumentaci

Povinnou součástí dodávky v závislosti na jejím charakteru je následující dokumentace a data.

Testovací dokumentace	Dokumentuje průběh testování pro danou komponentu. Rozsah povinné dokumentace se stanoví dle metodiky testování VZP ČR 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
		Postup na obnovu dat v testovacím prostředí Postup pro vytváření řezů dat a anonymizaci/pseudonymizaci dat Akceptační protokol

2.7 Dokumentační standard

Vlastník kapitoly: OAVRZ

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 ČR.
- Kromě odůvodněných a schválených a smysluplných výjimek (např. zdrojový kód) je dokumentace vedena v nástroji Sparx Enterprise Architect.

Požadavky na dokumentaci v oblasti systémové analýzy a architektury jsou umístěny v kapitole 2.1.3.
Požadavky na dokumentaci v oblasti bezpečnosti jsou umístěny v kapitole 4.11.
Požadavky na provozní dokumentaci jsou umístěny v kapitole 6.5
Požadavky na test dokumentaci jsou umístěny v kapitole 2.6

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. Takový provoz je možný pouze na základě scválené výjimky.

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 neproprietálních 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, access, active-standby
- Datový interface, 2x10GE, trunk, active LACP

3.2.2 On Premise SAN infastruktura

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 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.

3.2.3 Podmínky pro on – premise infrastrukturu podle Třídy Aplikací

3.2.3.1 *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.

3.2.3.2 *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 Sítě

Vlastník kapitoly: OTP OSS

3.3.1 VLAN

VLANy jsou implementované v přístupové vrstvě. Uživatelé z různých oddělení, rozděleni 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 pomoci ACL – Access Control List (přístupových listů).

3.3.2 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.

3.3.2.1 *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 ČR 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.

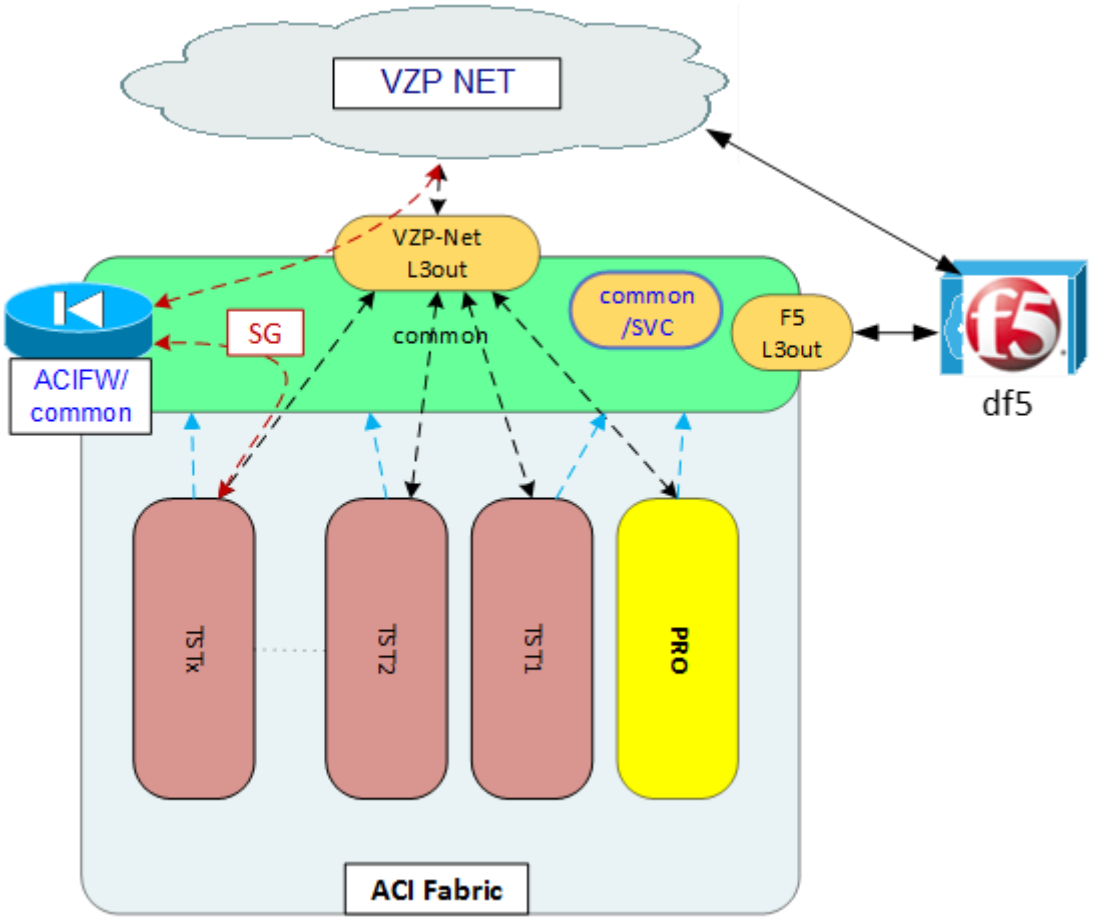
Produkční a testovací prostředí NDC je rozděleno do aplikačních celků. Každý aplikační celek je tvořen samostatným aplikačním profilem. Aplikační celek se typicky skládá z jednotlivých EPG (End Point Group) reprezentujících vrstvu aplikace:

- 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 využit servisní graf obsahující firewall.
- North-South provoz – komunikace ze sítě VZP ČR (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 ČR (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

3.3.3 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 ČR
- vnitřní perimetr – bezpečnostní oddělení veřejně vystavených služeb VZP ČR od vnitřní (uživatelské) sítě VZP ČR

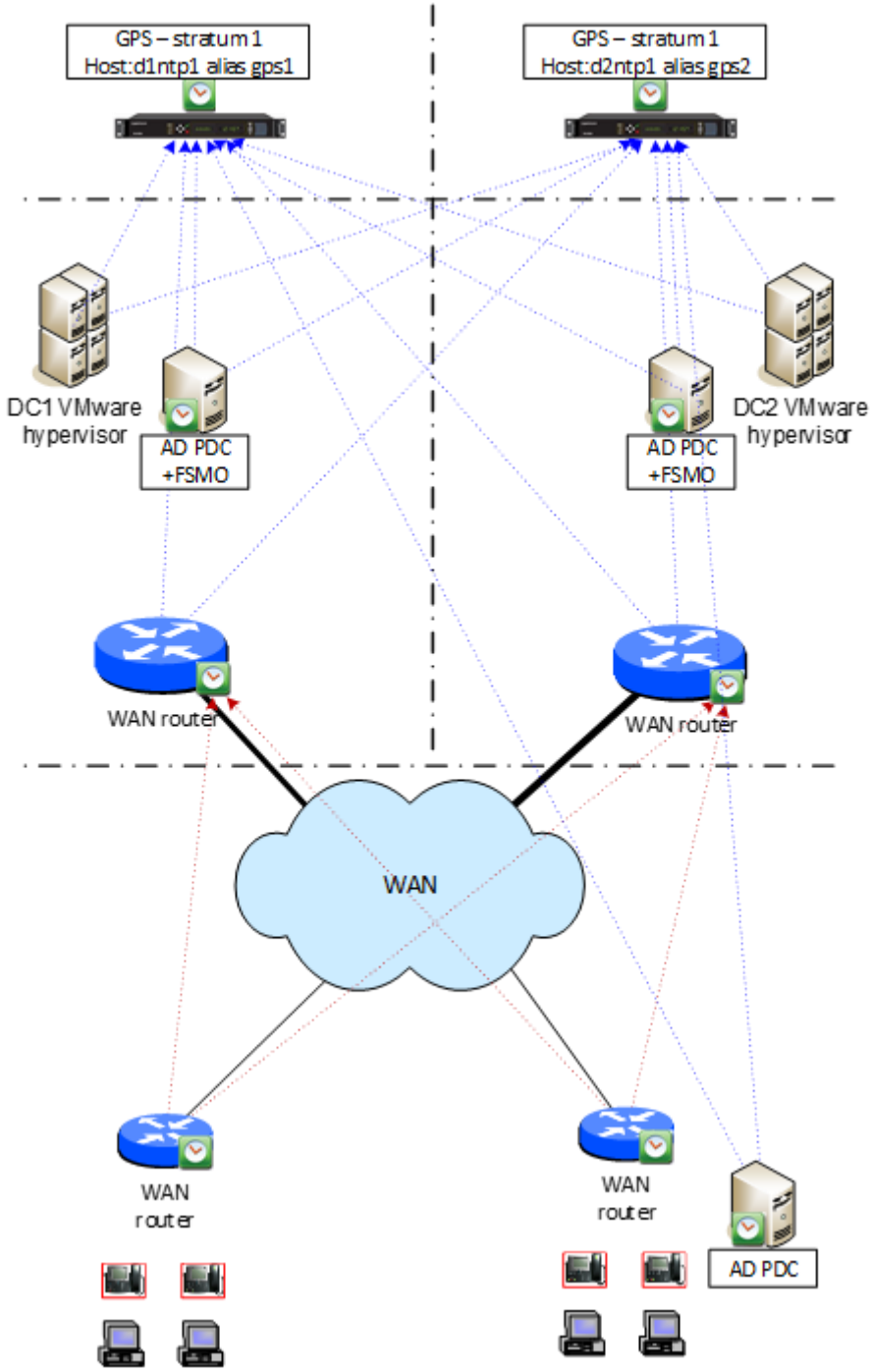
Součástí řešení je i VPN přístup do VZP ČR. Standardem pro připojení klientů do sítě VZP ČR pomocí VPN je autentizace pomocí dvou faktorů (uživatelským účtem spravovaným v AD VZP ČR a osobním certifikátem vydaným CA VZP ČR) a navázání šifrovaného SSL tunelu do VZP ČR. VPN slouží pro vzdálený přístup zaměstnanců a externích kontraktorů do sítě VZP ČR z Internetu.

3.3.4 Síťové služby

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

3.3.4.1 *Časová synchronizace (NTP)*

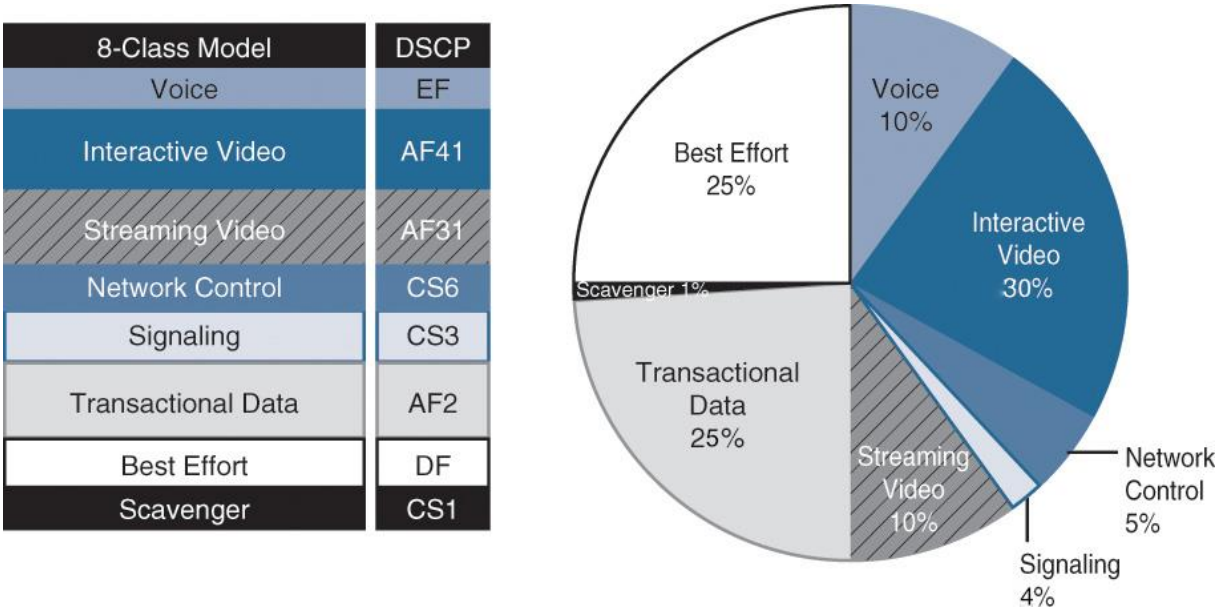
Primárním zdrojem času jsou dva servery GPS - NTP, umístěné v datových centrech: DC1 Orlická 4 a DC2 v ČD Telematika. Pokud to jednotlivé platformy/servery podporují je třeba použít pro ověření zdroje NTP autentizační klíč.



3.3.4.2 *QoS (QUALITY OD SERVICE)*

QoS zajišťuje rovnoměrné vyvažování zátěže sítě s ohledem na druh přenášených dat, spravedlivě rozděluje šířku pásma mezi jednotlivé aplikace dle nastavených priorit a zabraňuje tím snížení kvality síťových služeb pro prioritní aplikace ve stavu přetížení sítě.

Ve VZP ČR je použit 8-ti třídní QoS model reprezentující Cisco interpretaci RFC 4594[5].



VZP ČR řadí jednotlivé komunikační toky do tříd buď automaticky na základě analýzy datových toků pomocí Cisco technologie NBAR (Network Based Application Recognication)[6] nebo manuálně na základě provozních požadavků.

3.3.4.3 *DNS, DHCP, IPAM (DDI)*

Služby DDI zajišťují v síti fungování IPAM (IP Address Management) DNS a DHCP a zároveň správu a konfiguraci těchto služeb.

3.3.4.3.1 DNS

Domain Name Systém (DNS) zajišťuje v síti překlad jmenných názvů na IP adresy a obráceně (reverzní DNS). V IS VZP ČR máme doménu vzp.cz a několik subdomén podle typu zařízení či umístění – srv.vzp.cz, tz.vzp.cz., kz.vzp.cz, dc.vzp.cz, atp. K ochraně DNS je použito DNS rozšíření – DNSSEC.

3.3.4.3.2 DHCP

Dynamic Host Configuration Protocol (DHCP) zajišťuje v síti dynamickou konfiguraci klienta pomocí protokolu DHCP tak, aby byl schopen fungovat v daném segmentu sítě. Přiděluje klientovi IP adresu, masku podsítě, výchozí bránu, DNS servery a případně další volitelná nastavení.

3.3.4.3.3 IPAM

IP adres management (IPAM) software slouží k přehlednému zobrazení dostupných adresních rozsahů, jejich obsazenosti a stavu jednotlivých zařízení v nich.

3.3.4.4 *Loadbalancing*

Ve VZP ČR jsou k loadbalancingu – rozkladu zátěže – použity modulární loadbalancery Viprion firmy F5. Loadbalancery mimojiné zakončují spojení od klienta a následně navazují jiné spojení k aplikačnímu serveru.

[5] RFC 4594 - Configuration Guidelines for DiffServ Service Classes (ietf.org)
[6] Network Based Application Recognition - Wikipedia

3.4 OS

Vlastník kapitoly: OTP OSSM/OSSU

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 Enterpise Linux, Oracle Linux, CentOS (verze 7 a vyšší)
- MS Windows Server 2019

3.4.2 OS pro aplikace třídy B

- Red Hat Enterprise Linux, Oracle Linux, CentOS (verze 7 a vyšší)
- MS Windows Server 2019

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 ČR mohou být nasazeny technologie, VMWare vSphere 6.75 Enterprise Plus a vyšší, Oracle Linux Virtualization Manager 4.3 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 Linux Virtualization Manager 4.3 nebo vyšší.

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 ČR. 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 ČR:

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 ČR:

- 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)

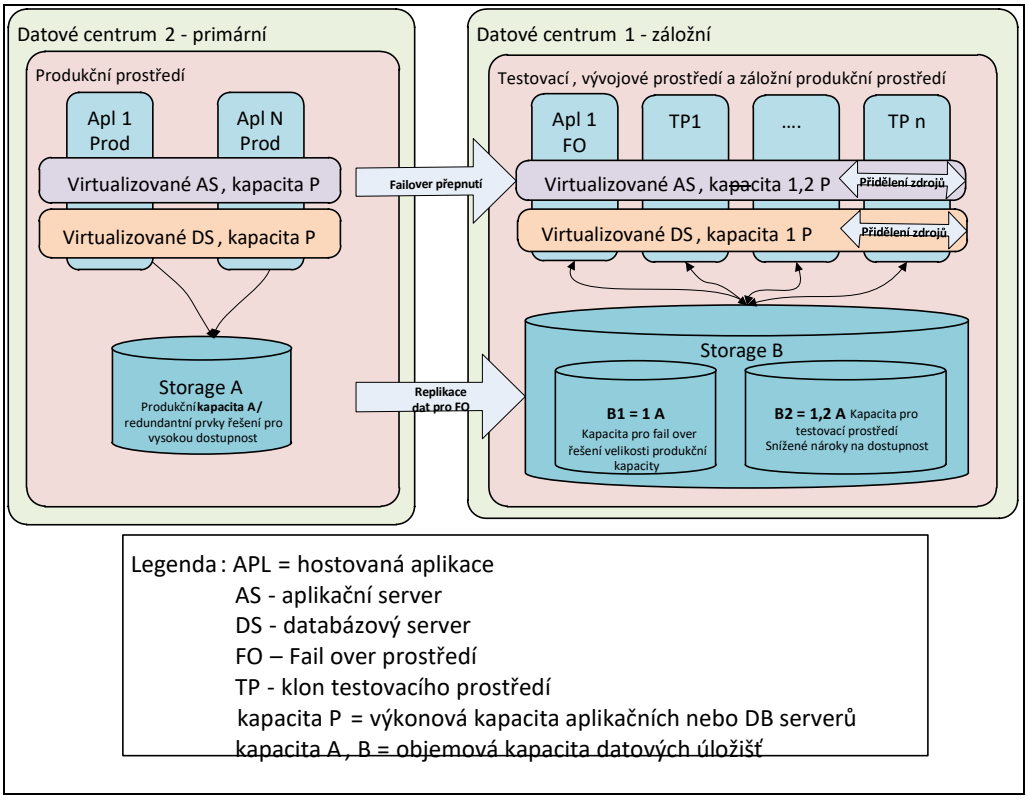
Aplikační server	OS Windows nebo Linux aplik. serveru Oracle Weblogic Suite
Databázový server Oracle	OS Linux, Oracle dB EE + RAC + partitioning
Databázový server MS SQL	OS MS Windows, MS SQL Server v edici Enterprise

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

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 velkosti 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 2019, 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: • Názvu tablespace • fyzických atributů segmentu (pctused, pctfree, storage params,...) 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, triggery apod.) začínají dvouznakovým prefixem příslušné aplikační komponenty (nebo historicky 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. Logování je detailně rozepsáno v dalších kapitolách, nicméně každý systém bude logovat minimálně tyto aktivity:
    - přihlašování a odhlašování ke všem účtům, a to včetně neúspěšných pokusů,
    - činností provedených administrátory,
    - úspěšné i neúspěšné manipulace s účty, oprávněními a právy,
    - neprovedení činností v důsledku nedostatku přístupových práv a oprávnění,
    - činností uživatelů, které mohou mít vliv na bezpečnost informačního a komunikačního systému,
    - zahájení a ukončení činností technických aktiv,
    - kritických i chybových hlášení technických aktiv a přístupů k záznamům o událostech, pokusy o manipulaci se záznamy o událostech a změny nastavení nástrojů pro zaznamenávání událostí

4.1.3 Minimální bezpečnostní standard

Dodávaný systém nebo aplikace musí být vždu v souladu s minimálním bezpečnostním standardem vydávaným NÚKIB a pravidelně uveřejňovaným na webových stránkách úřadu.

4.1.4 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 Minimum běžících a instalovaných služeb

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

4.3 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).

4.4 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.

4.5 Kryptografie

Kryptografickými metodami a algoritmy budou chráněna data specifikovaná jako citlivá v rámci tohoto standardu, dále všechna data spadající pod zde uvedené legislativní normy (tj. GDPR, ZoKB atd.) a v neposlední řadě všechna data či vybrané části informačních systémů, pokud budou identifikována jako citlivá v rámci analýzy rizik. Konkrétní použitý algoritmus či metoda kryptování vždy podléhá schválení VZP ČR.

4.5.1 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/.

4.5.2 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.

4.5.3 Požadavky na CA / PKI

- VZP ČR provozuje centrální CA, každý dodávaný systém musí být schopen kooperace s touto CA a splňovat mimo jiné dále uvedené požadavky:

- 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 vlastníkovi 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.

4.6 Komunikace s veřejnou sítí

4.6.1 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.

4.6.2 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 centrální proxy server (proxy server zajišťuje terminaci šifrovaného kanálu a inspekci provozu).

4.6.3 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).

4.7 Řízení přístupu

4.7.1 Autentizace a autorizace při přístupu k systémům, nebo aplikacím 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 Systém) 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 „CN“ v rámci „DN“ certifikátu. Na základě předaného „CN“ 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.

4.7.2 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 (včetně administrátorů) přistupuje do vnitřní sítě VZP ČR z veřejné sítě Internet vždy pouze prostřednictvím VPN VZP ČR.
- **Autentizace**:
    - uživatelským účtem spravovaným v AD VZP ČR a osobním certifikátem vydaným CA VZP ČR.
- **Autorizace**:
    - 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:wsse="http://docs.oasis-
open.org/wss/2004/01/oasis-200401-wss-wssecuritysecext-
1.0.xsd"                   xmlns:wsu="http://docs.oasis-
open.org/wss/2004/01/oasis-200401-wss-wssecurityutility-
1.0.xsd"> <wsse:Security>

 <wsse:UsernameToken wsu:Id="UsernameToken-484-624e-
938a-a986-a5e8717dcb3c">

 <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/12332222777/content http 1.1

host: esb.ecm.vzp.cz iv-user: melich99
```

4.7.3 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.

4.7.4 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.

4.7.5 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.

4.7.6 Zobrazení varovného hlášení

V případě systému, nebo aplikace, kdy uživateli jsou pracovníci VZP ČR 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. Aktivity v tomto systému jsou monitorovány.*".

4.8 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.

4.8.1 Klasifikační schéma informačních aktiv

Pro účely klasifikace informací VZP ČR je stanoveno následující klasifikační schéma informací, přičemž konečná rozhodovací pravomoc ohledně klasifikace je na straně VZP ČR a dodavatel musí následně implementovat a dodržet:

- **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 nenese žádná osobní data.

4.8.2 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.

4.8.3 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.

4.8.4 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.

4.8.5 Antimalware ochrana

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

4.8.6 Plán obnovy (Disaster Recovery)

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

4.9 Bezpečnostní testy

4.9.1 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 ČR v součinnosti s dodavatelem.

4.9.2 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.

4.10 Požadavky na bezpečnostní dokumentaci

U dodávek řešení se vyžaduje níže uvedená bezpečnostní dokumentace:

Bezpečnostní dokumentace[7]	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 komunikaci mimo síť VZP ČR. Výčet služeb poskytovaných do veřejné a vnitřní sítě.	Síťová bezpečnost
	Popis mechanismu autentizace a autorizace uživatelů. Napojení na centrální autority 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 Site 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

[7] Pokud informace požadované bezpečnostní dokumentací uvedl zpracovatel v rámci jiné dokumentační oblasti, pak je v bezpečnostní dokumentaci řešeno odkazem.

	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
	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. 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.	Kryptografická opatření
	Výčet zaznamenávaných bezpečnostních událostí, včetně popisu formátu, místa uložení a retence. Soulad s interní směrnicí VZP, případně s Vyhláškou ZoKB (Zákona o Kybernetické bezpečnosti). Formát logu (RFC standard, případně jiná), množství produkovaných logů za jednotku času.	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

4.11 Bezpečnostní monitoring

Každý dodávaný informační systém či aplikace bude schopna poskytovat data nástrojům bezpečnostního monitoringu používaného v rámci VZP ČR. Kromě poskytování provozních záznamů bude generovat logy definované tímto standardem.

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
Výkonností 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) Encoding logu je UTF-8, v ostatních případech je nutné schválení výjimky encodingu VZP ČR.
c) Všechny generované logy budou mimo výše uvedeného splňovat obecně platný standard definovaný v RFC 5424.

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 použití 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 vztahuji 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) Formát časového razítka je v souladu s ISO 8601 (vč. užití offsetu vůči UTC).
c) Ostatní formáty časového razítka musí být schváleny 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:

a) všechny logy jsou online uchovány minimálně po dobu 30 dní;
b) logy, které obsahují informace v souladu s požadavky ZoKB, resp. Vyhlášky 82/2018 o významných informačních systémech jsou k dispozici minimálně po dobu 12 měsíců;
c) logy všech systémů, které nespadají pod platný ZoKB a související vyhlášky, jsou k dispozici minimálně po dobu 12 měsíců;
d) 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:

a) výčet auditovaných událostí;
b) vzorky událostí;
c) při použití JSON formátu názvy použitých klíčů vč. jejich popisu;
d) způsob uložení (místo uložení na souborovém systému);
e) zajištění retence a rotace;
f) 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 přenáší 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 uzamčením 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 *definice* 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 přenáší 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 přenáší 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 ČR (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 které 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 transakce 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).

a) Logování zajistí komponenta, která je původcem transakce.
b) Vždy je zajištěna jednoznačná identifikace iniciátora transakce, a to i při zřetězení transakce.
c) Ze zaznamenané transakce musí být zjevné, zda je událost vyvolána interakcí uživatele s UI, nebo zda se jedná o automatizovaný proces.
d) 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[8]

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.

[8] 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.

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 (messagingu)
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.)
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[9]	VARCHAR2	Technologický identifikátor partnera, kterého se volání
		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",
```


[9] ID_PARTNER slouží k logování pro GDPR, 101/2000 Sb. a ZoKB jako zdroj informaci o žádajícím subjektu

"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

5.5.1 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 5.1.3.1 Časové razítko

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 ČR.

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

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

Microsoft System Center 2012 R2 Operations Manager (SCOM) a vyšší – agent na úrovni OS, integrace vybraných událostí do HP OM

Nagios – bez agentní, s integrací vybraných zpráv do HP OM

6.1.2.2 *HP Business Service Management (HP BSM) – integrace do HP OM o 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 – bez agentní, 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 implementovánu 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 ČR. 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 řídící 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 řídící 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 ČR 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 ČR do standardních ITIL procesů.

6.5.1 Definování 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 ČR 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.

6.6 Požadavky na provozní dokumentaci

Provozní dokumentace bude tvořena:

- Dokumentací skutečného provedení (dále DDS), která bude obsahovat popis provedení a konfigurace všech prostředí. V případě použití automatizačních nástrojů pro deployment prostředí aplikace, může být DDS nahrazeno příslušnými rolemi a CI/CD skripty.

- Administrátorskou příručkou, která bude obsahovat postupy pro instalaci a správu prostředí a aplikace.
- Uživatelská příručka
- Řešení typických chyb a problémů

Dokument Detail design specification (DDS)

DDS dokument a jeho obsah bude vždy přizpůsoben obsahu dodávky a rozsahu implementovaných služeb. Konzumuje-li dodávka služby, které dodávkou a provozem zajišťuje VZP ČR, nebude předmětem DDS konfigurace těchto služeb. DDS dokument je podkladem pro prvotní naplnění struktury konfigurační databáze.

Základní karta DDS pro službu (dodávku) zahrnuje následující atributy:

Public Domain Name
Internal Domain Name
IP subnet for all locations
Default GW
DNS Resolvers
NTP Servers
DNS Resolvers
VPN Gateway
RIPE
ASN: AS206344

U každé služby musí být zřejmé, jakou konfiguraci využívá přesto, že v rámci infrastruktury VZP ČR jsou tyto služby jednotně sdíleny a nastaveny.

Jmenné konvence:

Fyzická zařízení

Typ položky	**[type]-[location][dc]-[###]**	
typ zařízení	rt	router
	sw	switch
	lb	loadbalancer
	fw	firewall
	sr	server
	st	storage
	sm	service module (ILO, Idrac, IPMI, ...)
	ch	chassis (FX chassis)
	io	Chassis IO module management

umístění	Prg1	Lokalita Orlická
	Prg2	Lokalita XX
[###]	pořadí	001 - 999
Příklady:	sr-prg1-005	Fyz. server 005 v PRG DC Orlická
	sw-prg2-001	Switch 1 v PRG DC2
	sm-prg1-001	Service Module serveru 001 v PRG DC1

Provozované servery

Formát:	**[env]-[role]-[###]**	
[env]	mng	Management
	prd	Production
	tst	Test
	dev	Dev
	bop	Back Office Production
	bck	Backup
	drm	DR Management
	drp	DR Production
	drb	DR Back Office Production
Role serveru	[a-z], max lenght: 12 chars	Příklady: appwebapi, capsule, engine, db, media, backend, SAP, ...
[###]	pořadí	001 - 999 (zerofilled)
Příklady:	prd-appwebapi-003	produkční server, App WebAPI, č. 003
	tst-capsule-001	Capsule server v test prostředí

Prostředí:

Zkratka prostředí	Popis prostředí
E_MNG	Management
E_PRD	Production
E_TST	Test
E_DEV	Dev
E_BCK	Backup
E_NET	Network
E_DRM	DR Management
E_DRP	DR Production
E_DRB	DR Back Office Production

Popis komponent a jejich nastavení v DDD dokumentu se provádí tabulkami v MS Excel s následujícími záložkami dle seznamu a řádky položek:

1) Popis nastavení loadbalanceru:

Položka popisu	Význam položky
FQDN	
Internal / External	Typ balancingu
LB port	Adresa portu LB
LAN port	
LB Virtual Servers	
Incoming IP	Příchozí adresa LB
LAN IP	
Outgoing IP	Odchozí adresa LB
Target IPs	Cílové adresy LB
Sticky Sessions	Typ ballancingu
LB mode	adresa LB (AA, AP)

2) Parametry fyz. zařízení za jednotlivá prostředí:

Položka popisu	Význam položky
Hostname	Jméno hosta dle konvence
TYPE	Typ fyz. zařízení dle konvence
Environment	Typ prostředí
DC	Hosting dle konvence
FX	Rozměr zařízení (1,2,4…)
SLOT	Umístění zařízení v racku
Rack	Označení umístění
VLAN	Identifikace VLAN
IP's	Seznam přidělených adres
Hypervizor/OS	Základní provozovaný engine

3) Serverové clustery a jejich parametry za jednotlivá prostředí

Položka popisu	Význam položky

ID		Identifikace clusteru serverů s jedním hypervizorem
DC		Primární DC umístění
Environment		Označení prostředí dle konvence
Label		Typ prostředí
Servers	Dostupná kapacita	Počet serverů fyz
Cores		Počet core
RAM [GB]		Hodnota RAM
VMs	Požadovaná kapacita	Počet VM
Cores		Počet vCore
RAM [GB]		Hodnota RAM VM
Cores		obsazenost
RAM		obsazenost

Obsazenost se později v rámci provozního deníku a CMDB stanovuje výpočtem vzorcem.

4) Úložiště:

Položka popisu	Význam položky
ID	Identifikace úložiště
Label	
DC	Primární DC umístění
Replica DC	Prostředí kam se storage replikuje
LUN ID	
Alokace v GB	
Použito v GB	
Obsazenost v procentech	0%

5) Firewall nastavení:

Položka popisu		Význam položky
Zdroj	**VLAN (Group)**	
	Net/IP	

	port/protokol	
Cíl	**VLAN (Group)**	
	Net/IP	
	port/protokol	
Politika		Allow/Deny

6) Virtuální (provozované) servery:

Položka popisu	Význam položky
Hostname	Jméno serveru dle konvence
Popis účelu	
Cluster	Serverový clustery - ID
SysVol Storage	Úložiště – ID system
DataVol Storage	Úložiště – ID data
Host Group	
VLAN	
Subnet	
IP	
vCPU	
Mem[GB]	
SysVol[GB]	
DataVol[GB] **Instalované aplikace**	

7) Network Groups:

Položka popisu	Význam položky
Group Name	**Jméno skupiny**
VLAN(s)	**Jméno VLan**
IP(s)/Network(s)	**Sítě – seznam**

8) Backup plan:

Položka popisu	**Význam položky**
Application/Service	**Označení aplikace, služby**
Server hostname	Označení hostname virtuálního (provozovaného) servery
Path – zálohované objekty	Zálohované adresáře (cesty, soubory)
Pre-script	Umístění skriptu pro pre procesing zálohy
Post-script	Umístění skriptu pro post procesing zálohy
Pool – typ zálohovaných dar	Standard soubory/db/archive/nas/other

Schedule	Naplánováno (př.: vždy v 02:00), týdně, měsíčně, denně, hodiny, jinak Př: týden = každou sobotu full + denní increment Př. měsíčně = 1. sobotu v měsíci full + měsíční rozdíl + denní increment
Velikost očekávané plné kapacita zálohy [GB]	
Velikost očekávané denní kapacita zálohy [GB]	
Ideální nebo naplánovaný čas zálohy	
Odhad doby trvání	
Zálohovací zařízení	
Zálohovací úložiště Zálohovací technologie	

9) IDM

Položka popisu	Význam položky
Administrátorský účet	**username**
Server hostname nebo aplikace	
Seznam oprávnění	

10) Monitoring

Obsahuje seznam měřených rozhraní, sond a umístění agentů a metrik a jejich parametrů, která monitoring vyhodnocuje.

Položka popisu	Význam položky
Měřený bod nebo agent	**Metriky a jejich mezní parametry**

11) Další konfigurace:

Položka popisu	Význam položky
Aplikační komponenta	**Označení aplikace, služby**

Využívaná databáze	Server, schéma, uživatel, kapacita
Využívaný aplikační server	Server, technologie, cesta k nainstalované aplikaci

Administrátorská příručka

Příručka obsahuje odkaz na DDS dokument, který popisuje konfiguraci prostředí aplikace (dodávky) a k jednotlivým položkám (typům položek) DDS obsahuje následující strukturu informací. Pro jednotlivé komponenty označené dle DDS tabulky:

1) Odkaz na dokumentaci výrobce komponenty
2) Popis kroků a činností, které je třeba vykonat v případě, že monitorované hodnoty dosahují definovaných limitů
3) Instalační postup
4) Postup pro obnovu dat a provozu (DR)
5) Nainstalované licence
6) Seznam použitých certifikátů
7) Seznam kroků pravidelné údržby a profylaxe

Strukturu administrátorské příručky k položce DDS lze krátit v případě, že už VZP ČR má komponentu v provozu o:

- Odkaz na dokumentaci výrobce komponenty
- Instalační postup
- Seznam kroků pravidelné údržby a profylaxe

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: Metodika implementace integračních služeb
Příloha 6: Metodika dokumentace integračních služeb
Příloha 7: Metodika homologace integračních služeb

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)