Prováděcí smlouva č.j. PPR-25027-9/ČJ-2018-990656, č.dod.: CWT053/7

k Rámcové smlouvě o poskytování technické podpory a rozvoje aplikačního software NS-VIS
č. PPR-18586-30/2015-990656 resp. CWT053

Smluvní strany:

Česká republika – Ministerstvo vnitra

Sídlo:	Nad Štolou 936/3, PSČ 170 34, Praha
IČ:	00007064
DIČ:	CZ00007064
Zastoupená:	plk. Mgr. Pavlem Osvaldem, ředitelem Ředitelství pro podporu výkonu služby Policejního prezidia České republiky
Bankovní spojení:	Česká národní banka, Praha 1 č.ú. [redacted]
Korespondenční adresa:	Policejní prezidium ČR, Správa logistického zabezpečení, P.O.BOX 6, 150 05 Praha

(dále jen „Objednatel")

a

IBM Česká republika, spol. s r.o.
Registrovaná u Městského soudu v Praze, oddíl C, číslo vložky 692

Sídlo:	V Parku 2294/4, 148 00 Praha 4
IČO:	14890992
DIČ:	CZ14890992
Zastoupená:	Martinem Kotrusem, jednatelem společnosti
Bankovní spojení:	ČSOB Praha 1, Na příkopě 14, Praha 1 Číslo účtu: [redacted]
Korespondenční adresa:	V Parku 2294/4, 148 00 Praha 4

(dále jen „Dodavatel")

(společně dále také jen „Smluvní strany", nebo jednotlivě „Smluvní strana")

uzavřely tuto Prováděcí smlouvu (dále jen „Prováděcí smlouva") k Rámcové smlouvě o poskytování technické podpory a rozvoje aplikačního software NS-VIS vedené pod č.j.: PPR-18586-30/2015-990656 resp. CWT053, ze dne 10.6.2016 (dále jen „Rámcová smlouva") v souladu s ustanoveními zákona č. 89/2012 Sb., občanský zákoník, (dále jen „občanský zákoník") a zákona č. 137/2006 Sb., o veřejných zakázkách (dále jen „ZVZ", nebo „zákon o veřejných zakázkách") k veřejné zakázce s názvem „Zvýšení efektivity bezpečnostní prověrky a zabezpečení NS-VIS " č.j. PPR-25027-4/ČJ-2018-990656.

1. PŘEDMĚT SMLOUVY

1.1. Předmětem této Prováděcí smlouvy je závazek Dodavatele poskytnout Objednateli následující plnění:

A) Rozšíření systému VIS o funkcionalitu automatické bezpečnostní prověrky o otisky prstů.

B) Technická Implementace zjištěných požadavků vyplývajících z Bezpečnostní dokumentace VIS na základě provedené analýzy

v souladu se specifikací uvedenou v Příloze č. 1 této Prováděcí smlouvy (dále též jen „Předmět plnění").

1.2. Předmětem této Prováděcí smlouvy není:

- změna, úpravy nebo rozšíření funkcionality systému VIS (systém NS-VIS a systém VISMAIL, dále jen „VIS"), které nejsou uvedeny v této Prováděcí smlouvě, garance funkčnosti systému NS-VIS s jinými periferiemi než těmi, které byly dodány IBM v rámci dodávky systému VIS;
- zajištění potřebné komunikační infrastruktury, zajištění nezbytné konektivity na externí systémy včetně dostatečné propustnosti linek, realizace nezbytných změn externích systémů a zajištění zálohování a archivace dat.

1.3. Předmětem této Prováděcí smlouvy dále není zajištění testovacích prostředí, zdrojových dat externích systémů a dalších nezbytných náležitostí (zejména organizačních, legislativních, smluvních a provozních a dále administrátorské a operátorské podpory, atd.) nutných pro realizaci předmětu této Prováděcí smlouvy ani realizace jakýchkoli dalších dodávek, služeb a činností nezbytných pro zajištění provozu VIS, které nejsou definovány v této Prováděcí smlouvě.

1.4. Objednatel se zavazuje řádně dodané Plnění převzít a zaplatit za něj dohodnutou cenu, a to způsobem definovaným v této Prováděcí smlouvě a v Rámcové smlouvě.

2. CENA

2.1. Smluvní strany se dohodly, že fixní část ceny za Plnění poskytnuté dle této Prováděcí smlouvy je **8 650 000,00 Kč** bez DPH **10 466 500,00 Kč** s DPH. Smluvní strany se dohodly, že tato fixní cena může být zvýšena až o 10 % v případě, že vznikne potřeba víceprací a Objednatel tyto vícepráce tj. navýšení celkové ceny za poskytnuté Plnění předem písemně schválí.

2.2. Specifikace fixní části ceny včetně platebních milníků je uvedena v Příloze č. 2 této Prováděcí smlouvy.

3. TERMÍN PLNĚNÍ

3.1. Dodavatel je povinen dodat Předmět plnění do 8 měsíců od účinnosti této Prováděcí smlouvy.

3.2. Realizace Předmětu plnění (Projektu) bude probíhat po jednotlivých částech, resp. etapách. Předpokládané rámcové termíny plnění a základní milníky jsou uvedeny v Příloze č. 3 této Prováděcí smlouvy.

4. KOORDINACE

4.1. Pro realizaci Předmětu plnění a nutnou koordinaci bude vytvořena řídící struktura Projektu a pracovní tým(y). Řídící struktura Projektu a požadované složení pracovního týmu včetně klíčových rolí na straně Objednatele a Dodavatele jsou stanoveny v Příloze č. 4 této Smlouvy.

4.2. Obě Smluvní strany písemně jmenují své koordinátory, tj. kontaktní odpovědné osoby (vedoucí Projektu), případně jejich zástupce nejpozději do jednoho pracovního dne od podpisu Prováděcí smlouvy.

4.3. Smluvní strany se výslovně dohodly, že akceptační protokol, který je přílohou daňového dokladu (faktury) musí být kromě osob uvedených v Příloze č. 4 Rámcové smlouvy podepsán za Objednatele také Vedoucím Projektu, kterým je [redacted] případně [redacted]

4.4. Realizace Předmětu plnění, resp. řízení Projektu, bude probíhat na základě podmínek uvedených v této Prováděcí smlouvě a v Rámcové smlouvě.

5. PODMÍNKY A PŘEDPOKLADY REALIZACE

5.1. Základní podmínky a předpoklady jsou specifikovány v Rámcové smlouvě.

5.2. V průběhu realizace Projektu je nutno na straně Objednatele dále zajistit, resp. splnit, následující podmínky a předpoklady, které jsou nezbytné pro řádné splnění Předmětu plnění a jeho jednotlivých etap - dílčích předmětů plnění:

- zajištění veškerých SW licencí a SW support systému VIS,
- zajištění testovacích prostředí všech externích systémů (ČR i EU) v požadovaných termínech dle harmonogramu,
- zajištění rozhraní externích systémů v souladu s odsouhlasenými popisy rozhraní v požadovaných termínech (při nutnosti úpravy rozhraní Dodavatel připraví na základě informací od objednatele aktuální definici rozhraní pro externí systémy. Objednatel následně zajistí požadované úpravy v externích systémech podle dodané specifikace včetně přípravy dat a spolupráce při testování),
- zajištění funkčních otestovaných externích systémů (ČR i EU) splňujících odsouhlasené popisy rozhraní se systémem VIS (NS-VIS a VIS MAIL) v požadovaných termínech, dle harmonogramu a možnosti testování s externími systémy (ČR i EU: CS-VIS, SIS II, MZV-EVC2) v potřebných termínech dle harmonogramu,
- zajištění technické infrastruktury včetně požadované konektivity,
- zajištění testovacích dat externích systémů, klíčenek, specimenů dokladů, testovacích vízových štítků a dalších rekvizit nezbytných pro provedení aktualizace a testů v požadovaném rozsahu a požadovaných termínech,
- organizační zajištění, zejména zajištění/alokace projektového týmu a klíčových rolí na straně Objednatele.

5.3. Dále je nutno na straně Objednatele zajistit, aby v rámci realizace předmětu plnění nedocházelo k prodlevám z důvodu překážek, zpoždění na straně Objednatele (nesplnění podmínek nebo součinnosti), které by znamenaly vícenáklady nebo škody na straně Dodavatele.

6. PŘEVZETÍ VÝSLEDKŮ PLNĚNÍ

6.1. Předmětné plnění podle této Prováděcí smlouvy bude Objednatelem převzato protokolárním způsobem.

6.2. Bude-li plnění Dodavatele spočívat ve vypracování dokumentu v listinné nebo elektronické podobě, bude jeho akceptace provedena následovně:

- Dodavatel předá v dohodnutém termínu první verzi dokumentu.

- Objednatel vznese své výhrady nebo připomínky k první verzi dokumentu obecně do tří (3), nejpozději do pěti (5) pracovních dnů od jejího doručení; nevznese-li Objednatel ve stanovené lhůtě k první verzi dokumentu žádné výhrady ani připomínky, považují Smluvní strany uplynutím této lhůty dokument ve znění jeho první verze za řádně akceptovaný a pro Smluvní strany závazný.
- Vznese-li Objednatel ve stanovené lhůtě své výhrady nebo připomínky k první verzi dokumentu, zavazuje se Dodavatel obecně do tří (3), nejpozději do pěti (5) pracovních dnů od jejich doručení provést veškeré potřebné úpravy dokumentu dle výhrad a připomínek Objednatele a takto upravený dokument předat jako jeho druhou verzi Objednateli k akceptaci.
- Objednatel se zavazuje vznést své výhrady nebo připomínky k druhé verzi dokumentu obecně do tří (3), nejpozději do pěti (5) pracovních dnů od jejího doručení. Nevznese-li Objednatel ve stanovené lhůtě k druhé verzi dokumentu žádné výhrady ani připomínky, považují Smluvní strany uplynutím této lhůty dokument ve znění jeho druhé verze za řádně akceptovaný a pro Smluvní strany závazný. K výhradám nebo připomínkám, které Objednatel opomněl vznést již k první verzi dokumentu, se pro účely akceptace nebude přihlížet, Dodavatel však bude povinen takovéto výhrady nebo připomínky Objednatele vypořádat do deseti (10) pracovních dnů od akceptace dokumentu.
- Vznese-li Objednatel ve stanovené lhůtě své výhrady nebo připomínky k druhé verzi dokumentu, zavazují se Smluvní strany zahájit společné jednání za účelem odstranění veškerých vzájemných rozporů a za účelem akceptace dokumentu, a to nejpozději do tří (3) pracovních dnů od výzvy kterékoliv Smluvní strany. Nepodaří-li se Smluvním stranám dojít ke shodě o akceptaci dokumentu ani ve lhůtě dvaceti (20) pracovních dnů od zahájení společného jednání dle předchozí věty, je kterákoli ze Smluvních stran oprávněna od této Smlouvy odstoupit s tím, že při vyrovnání bude postupováno v souladu s ustanoveními Rámcové smlouvy.

6.3. Objednatel potvrdí přejímku jednotlivých dílčích částí předmětu plnění – etap podpisem Předávacího nebo Akceptačního protokolu.

6.4. Předmět plnění bude považován za řádně splněný, jestliže Dodavatel úspěšně vykoná přejímací zkoušku – akceptaci provedením oboustranně schválených akceptačních testů a předáním aktualizace příslušné/relevantní dokumentace systému VIS Objednateli.

6.5. Přejímací zkouška – akceptace bude probíhat následujícím způsobem:

a) Před ukončením předmětného plnění musí Objednatel provést za účasti Zhotovitele oboustranně schválené akceptační testy na základě odsouhlasených testovacích scénářů.

b) Předmět akceptace je akceptován, pokud nebude Objednatelem uplatněna žádná závada typu A a takový počet závad typu B nebo kombinací závad typu B, které ve svém důsledku způsobí závadu typu A a takovéto závady Objednatel neprokázal v Akceptačním protokolu.

c) Jestliže předmětné plnění splní akceptační kritéria akceptačních testů dle bodu 7.5 b), podepíší k němu Smluvní strany Akceptační protokol. Podpisem Akceptačního protokolu oběma Smluvními stranami se má se za to, že předmětné plnění bylo řádně Zhotovitelem poskytnuto a Objednatelem převzato. Tím není dotčena povinnost Dodavatele odstranit závady typu B a C, které jsou uvedeny v Akceptačním protokolu v termínech zde uvedených.

d) Jestliže předmětné plnění nesplňuje stanovená akceptační kritéria, zaznamenají tuto skutečnost Smluvní strany do Akceptačního protokolu tak, že zde budou uvedeny, popsány a prokázány veškeré zjištěné závady a nedostatky. Zhotovitel se zavazuje napravit tyto nedostatky ve lhůtě, která bude Smluvními stranami dohodnuta, a příslušné akceptační testy budou provedeny znovu. Tento proces testování a následných oprav se bude opakovat, dokud Zhotovitel nesplní veškerá akceptační kritéria.

e) Závadou se pro účely této Smlouvy rozumí rozpor mezi vlastností nebo funkčností plnění proti plné funkčnosti systému VIS tak, jak bude specifikován v odsouhlasené analytické dokumentaci a skutečnou vlastností či funkčností plnění.

f) Jestliže uplynulo pět (5) pracovních dnů od předložení Akceptačního protokolu Zhotovitelem Objednateli a Objednatel nepodal žádné písemné námitky s uvedením položek, specifikací závad bránících akceptaci a takovéto závady Zhotoviteli neprokázal v Akceptačním protokolu, v takovém případě bude za datum splnění považován den následující po marném uplynutí lhůty uvedené v tomto odstavci; pokud Objednatel užije některé části plnění k produktivním účelům, ať již před nebo po obdržení Akceptačního protokolu k podpisu, bude za datum splnění považován den prvního užití díla nebo jeho části v produkčním provozu.

g) Objednatel má právo schválit akceptaci s výhradou. Smluvní strany potvrdí akceptaci s výhradou sepsáním Akceptačního protokolu, ve kterém budou uvedeny připomínky Objednatele a návrh závazného termínu dodání příslušné opravy ze strany Zhotovitele. Účinky akceptace s výhradou nastávají podpisem tohoto Akceptačního protokolu oběma Smluvními stranami.

h) Specifikace závad

„**Závadou typu A**" se rozumí stav, kdy systém neposkytuje některou z kritických funkcionalit systému (jsou takto specifikovány v akceptované analytické dokumentaci).

„**Závadou typu B**" se rozumí stav, kdy je systém schopen omezeného provozu nebo neposkytuje některou z nekritických funkcionalit (jsou takto specifikovány v akceptované analytické dokumentaci)

„**Závadou typu C**" se rozumí závada, která nemá zásadní vliv na provoz nebo funkcionality systém

6.6. Úspěšným ukončením projektu rozumí smluvní strany akceptaci všech ve smlouvě uvedených plnění a uvedení systému upraveného dle této smlouvy do rutinního provozu a jeho týdenní zvýšený monitoring. Ukončením zvýšeného monitoringu dojde ke splnění všech závazků ze strany Dodavatele dle této Prováděcí smlouvy a Odběratel převezme odpovědnosti za užívání převzaté části předmětu Smlouvy a za výsledky z něho získané stejně jako za jeho kombinaci s jakýmikoliv jinými zařízeními, programy nebo službami.

7. SOUČINNOST OBJEDNATELE

7.1. Základní podmínky součinnosti Objednatele jsou uvedeny v Rámcové smlouvě.
Další součinnost Objednatele při realizaci plnění této Prováděcí smlouvy je uvedena v Příloze č. 5.

7.2. V případě zdržení plnění z důvodů prodlení s poskytnutím součinnosti ze strany Objednatele nebude toto považováno za prodlení Dodavatele s plněním podle této Smlouvy. Zároveň je Dodavatel oprávněn v takovémto případě prodlení ze strany Objednatele požadovat úhradu prokazatelně vynaložených nákladů vzniklých v souvislosti s takovým prodlením.

8. ZMĚNY

8.1. V případě, že Objednatel požaduje změnu v plnění, předá Dodavateli zadání - specifikaci těchto změn a Dodavatel popíše jejich účinek na přejímku - akceptaci, kritéria, data, cenu, harmonogramy a další podmínky/předpoklady jejich realizace. Změny, které nemají dopad na termíny a cenu pak budou realizovány na základě odsouhlaseného zápisu vedoucích Projektu obou Smluvních stran.

8.2. Všechny ostatní změny budou realizovány formou písemného dodatku k této Smlouvě odsouhlaseného oběma Smluvními stranami. Dokud nebude dodatek uzavřen a podepsán oběma Smluvními stranami, bude Dodavatel postupovat ve shodě s naposled autorizovanými podmínkami Smlouvy.

9. OSTATNÍ UJEDNÁNÍ

9.1. Veškerá ujednání této Prováděcí smlouvy navazují na Rámcovou smlouvu a podmínkami uvedenými v Rámcové smlouvě se řídí, tj. práva a povinnosti či skutečnosti neupravené v této Prováděcí smlouvě se řídí ustanoveními Rámcové smlouvy. V případě, že ujednání obsažené v této Prováděcí smlouvě se bude odchylovat od ustanovení obsaženého v Rámcové smlouvě, má ujednání obsažené v této Prováděcí smlouvě přednost před ustanovením obsaženým v Rámcové smlouvě, ovšem pouze ohledně plnění sjednaného v této Prováděcí smlouvě.

Tato Dohoda nabývá účinnosti dnem uveřejnění v registru smluv dle zákona č. 340/2015 Sb., o zvláštních podmínkách účinnosti některých smluv, uveřejňování těchto smluv a o registru smluv (zákon o registru smluv).

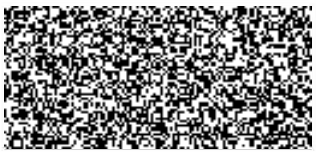
9.2. Tato Prováděcí smlouva je vyhotovena ve 4 (čtyřech) stejnopisech s platností originálu, z nichž každá Smluvní strana obdrží 2 (dva) stejnopisy.

9.3. Nedílnou součástí této Smlouvy jsou následující přílohy:

Příloha č. 1 – „Specifikace předmětu plnění"
Příloha č. 2 – „Rozpočet ceny"
Příloha č. 3 – „Harmonogram plnění"
Příloha č. 4 – „Řídící struktura projektu"
Příloha č. 5 – „Součinnost Objednatele"

03. 10. 2018
V Praze dne .....

Objednatel:

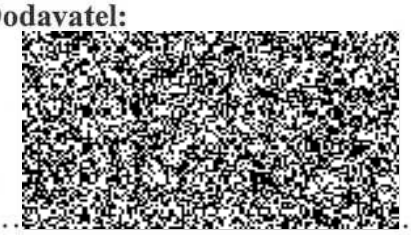


.....

Ministerstvo vnitra – Česká republika
Zástupce: plk. Mgr. Pavel Osvald
Funkce: ředitel ŘPVS PP ČR

08 -10- 2018
V Praze dne .....

Dodavatel:



.....

IBM Česká republika spol. s r.o.
Zástupce: Martin Kotrus
Funkce: jednatel společnosti

Příloha č. 1 – Specifikace předmětu plnění
Počet listů: 25

A) ROZŠÍŘENÍ SYSTÉMU VIS O FUNKCIONALITU AUTOMATICKÉ BEZPEČNOSTNÍ PROVĚRKY O OTISKY PRSTŮ.

Rozšíření funkcionality provádění bezpečnostní prověrky bude znamenat rozšíření seznamu služeb v CA, ve kterých se provádí automatická bezpečnostní o novou službu - lustrace v žádostech vyhledaných dle otisků žadatele v CS-VIS. Bude se ověřovat, zda se alfanumerická data žadatele v žádosti pořízené na MZV shodují s alfanumerickými daty žádostí vyhledaných dle otisků žadatele v CS-VIS. Provede se porovnání jednotlivých položek (např. Příjmení, Jméno, Pohlaví, Číslo CD, Národnost CD, Datum narození).

Současný stav:
V systému NS-VIS je prováděna automatická BP dle alfanumerických dat žadatele a otisky prstů v ní nejsou zohledněny.
Pro žádosti pořízené na MZV provádí hledání v CS-VIS dle otisků prstů pouze MZV, což je již historicky jejich povinnost. Data pořizované žádosti a výsledek vyhledávání žádostí dle otisků prstů porovnává pracovník ZÚ v KA EVC2 vizuálním porovnáním údajů (bez strojové kontroly).

Ve VIS bude realizována následující změna:
Rozšířit automatickou BP, o možnost lustrace žádostí pořízených na MZV, dle otisků prstů v rámci automatické BP.

Změna má dopad do :
- změna na straně MZV: data předávaná z MZV na ESB konektor (pro operaci *SearchByFingerprint*)
- ESB nsvis cs-vis
- CA
- KA Vyčkat

Změna v CA
Změna se bude týkat žádostí typu (applicationType): ***ZU*** **a** ***RepringZU.***

Data pro provedení lustrace budou získávána z výsledků operace *SearchByFingerprint* na ESB *nsviscsvis* (tj. Dojde k strojovému porovnání dat pořizovaných žádosti a výsledků vyhledání žádostí dle otisků prstů, které provedlo MZV vůči CS-VIS).

V NS-VIS CA bude nově rozšířen seznam služeb, ve kterých se provádí ABP o novou službu - ***lustrace v žádostech vyhledaných dle otisků žadatele v CS-VIS.***
Tato služba bude ověřovat, zda alfanumerická data žadatele v žádosti pořízené na MZV se shodují s alfanumerickými daty žádostí vyhledaných dle otisků žadatele v CS-VIS. Budou se porovnávat tyto položky: *Příjmení, Jméno, Pohlaví, Datum narození.* Pro porovnání budou použita pravidla z lustračního algoritmu.

Vyhodnocení výsledků porovnání:
- Pokud nebudou existovat žádné žádosti, pro daného žadatele, v CS-VIS, výsledek služby bude *pass*.
- Pokud budou vyhledány žádosti v CS-VIS, systém ověří, zda je shoda v datech vybraných položek *Příjmení, Jméno, Pohlaví, Datum narození.*
  - Pokud ano, výsledek služby bude *pass*.
  - Pokud ne, výsledek služby bude *fail* a systém žádost předá k ručnímu zpracování na pracovišti Vyčkat.

- Pokud na ESB nsvis csvis nebudou existovat výsledky vyhledání, dle otisků prstů, pro danou žádost, které provedlo MZV (tj. výsledek operace *SearchByFingerprint),* žádost bude nastavena do stavu *error* a dojde k zopakování BP (dle pravidel pro stav *error*).

Operace CA (změna cca 17ti existujících operací a přidání nové operace):
applicationExamination
examinationZu
prepareExamServicesAuto
prepareExamServicesRepeated
executeExamServices
executeExamServicesAppHistory
finalizeExamInvocation
createWaitingExamInvocation
examinationRepringZu
executeExamServicesAppHistory
finalizeExamInvocation
createWaitingExamInvocation
getExamination
updateExamInvocation
updateExamination
repeatExamination
getExaminationOverview

Bude rozšířen Výčtový typ ExamServiceType - Typ služby pro vykonání lustrace
Úprava operace *getApplicationsWaitingZu*, která umožní zobrazení žádostí v KA Vyčkat pro novou lustrační službu.

Změna v ESB nsvis csvis
Při řešení je možné využít výsledky hledání dle otisků prstů v CS-VIS *SearchByFingerprint*, které provedlo MZV (nutná úprav i na straně MZV), které jsou uloženy na ESB nsvis cs-vis.

Je nutné doplnit 3 nové operace:
1.) Bude doplněna nová operace pro vyhledání údajů o žadateli ***searchPersonHitCS***, kterou bude volat CA.

Operace pro danou žádost (určenou číslem žádosti) vyhledá seznam žádostí, který existuje v response operace *searchByFingerPrint*.
Operace bude vracet do CA informace, zda došlo k záchtu hitu nebo ne. Míra shody bude určena dle lustračního algoritmu.

- Pokud nastane shoda, bude se do CA vracet informace, že **není zachycen hit** (data žadatele se shodují není důvod k ručnímu prověřování ve Vyčkat).
- Pokud nastane neshoda, bude se do CA vracet informace, že **je zachycen hit** (data žadatele se neshodují je důvod k ručnímu prověřování ve Vyčkat – nutno prověřit, zda nedošlo ke změně identity žadatele).

Request:
- *Číslo žádosti (applicationNumber)*
- *Příjmení (Surname) – z prověřované žádosti*
- *Jméno (FirstNames) – z prověřované žádosti*
- *Pohlaví (Sex) - z prověřované žádosti*
- *Datum narození (DateOfBirth) - z prověřované žádosti*

Response:
- *Hit (ano/ne)*
- *Id*
- seznam záznamů (0 až n) z response *searchByFingerPrint*, pro každý záznam položky:

- *Číslo žádosti (applicationNumber)*
- *Příjmení (Surname)*
- *Jméno (FirstNames)*
- *Pohlaví (Sex)*
- *Datum narození (DateOfBirth)*

2.) Bude doplněna nová operace ***getHitListCS*** pro vyhledání seznamu žádostí, použitých pro vyhodnocení prověrky. Operaci bude volat KA.

Request:

- *Id*

Response:

- seznam záznamů (0 až n) z response *searchByFingerPrint*
  - *Číslo žádosti (applicationNumber)*
  - *Příjmení (Surname)*
  - *Jméno (FirstNames)*
  - *Pohlaví (Sex)*
  - *Datum narození (DateOfBirth)*

3.) Bude doplněna nová operace pro zobrazení detailu ***getDetailPersonCS.*** Operaci bude volat KA.

Request:

- *Id*

Response:

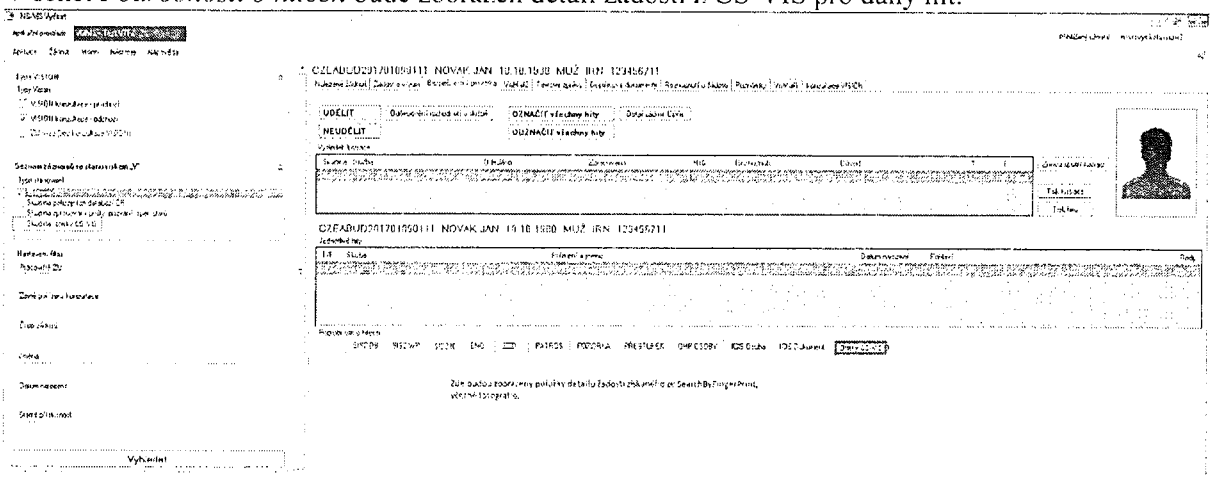
- *Příjmení (Surname)*
- *Jméno (FirstNames)*
- *Pohlaví (Sex)*
- *Datum narození (DateOfBirth)*
- *FormerSurnames*
- *PlaceOfBirth*
- *SurnameAtBirth*
- *Owner*
- *RepresentedUser*
- *Decisions*
- *Attachments*
- *groupSynopses*

Změna v KA Vyčkat

V KA Vyčkat bude doplněn do *Seznamu záznamů se stanoviskem „V"* nový *Typ stanoviska*: ***Skupina otisky CS-VIS***, který umožní prohlížet výsledek této nové lustrační služby a umožní ruční rozhodnutí BP.

V sekci *Jednotlivé hity* bude zobrazen seznam žádostí vrácených této nové lustrační služby.

V sekci *Podrobnosti o hitech* bude zobrazen detail žádosti z CS-VIS pro daný hit.



Nová lustrační služba bude doplněna na detailu žádosti, na záložce *Bezpečnostní prověrka* pro *Žádosti k rozhodnutí* a pro *Žádosti s rozpory* a na záložce Rozhodnutí o žádosti ve všech výskytech (tj. včetně Dotazů na žádosti).

Zároveň musí být realizována změna na straně MZV systému EVC2:

Bude rozšířeno volání operace *sendRequestToCSVIS* MZV na ESB nsvis cs-vis pro operaci *SearchByFingerprint* o vazbu na číslo žádosti, pro kterou byla operace volána a v níž jsou umístěny odpovídající otisky prstů žadatele.

B) TECHNICKÁ IMPLEMENTACE ZJIŠTĚNÝCH POŽADAVKŮ VYPLÝVAJÍCÍCH Z BEZPEČNOSTNÍ DOKUMENTACE VIS NA ZÁKLADĚ PROVEDENÉ ANALÝZY

Realizace se týká pouze těch částí (tj. odstranění nedostatků) zde uvedených, které může provést dodavatel systému VIS – IBM).
Odstranění ostatních nedostatků musí zajistit provozovatel systému VIS – PČR.

Příslušný paragraf vyhlášky č. 316 / 2014 k ZKB	**Popis nápravy, odstranění nedostatku**	**Návrh řešení (odkaz na detailní popis)**	**Oblast**
§18 Identita odst 3 a) b) c) + odst 4 a) b) pro Přístup administrátorů k Host serverům NSVIS (M9-14, M17-19)	Rekonfigurace ověření identity administrátorů v systému RHEL7 odpovídající požadavkům ZKB.	Změny, které bude IBM realizovat jsou uvedeny pod tabulkou - kapitola 10. Centrální správa administračních účtů	Infrastruktura
§18 Identita odst 3 a) b) c) + odst 4 a) b) pro Přístup administrátorů k virtuálním webovým serverům NSVIS (N9-14, N17-19)	Rekonfigurace ověření identity administrátorů v systému RHEL6 odpovídající požadavkům ZKB.	Změny, které bude IBM realizovat jsou uvedeny pod tabulkou - kapitola 10. Centrální správa administračních účtů	Infrastruktura
§18 Identita odst 3 a) b) c) + odst 4 a) b) pro Přístup administrátorů k virtuálním aplikačním, integračním a dm serverům NSVIS (O9-14, O17-19)	Rekonfigurace ověření identity administrátorů v systému RHEL6 odpovídající požadavkům ZKB.	Změny, které bude IBM realizovat jsou uvedeny pod tabulkou - kapitola 10. Centrální správa administračních účtů	Infrastruktura
§18 Identita, Přístup administrátorů: WebSphere Administrační konzole DM-P1,S1 n(P9-14, P17-19)	Identity management není součástí VIS, z konfigurace WebSphere (Federated Repository) odebrat používání file based registry. Rekonfigurace ověření identity administrátorů ve WebSphere Administrační konzoli odpovídající požadavkům ZKB.	Z konfigurace WebSphere (Federated Repository) odebrat používání file based registry. Integrace WebSphere s Centrální správou administračních účtů (s MS Active Directory jako systémem pro centrální správu uživatelských účtů v rámci PČR). Změny, které bude IBM realizovat jsou uvedeny pod tabulkou - kapitola 10. Centrální správa administračních účtů	Infrastruktura

§18 Identita odst 3 a) b) c) + odst 4 a) b) pro Přístup administrátorů k virtuálním monitoring serverům VIS (R9-14, R17-19)	Rekonfigurace ověření identity administrátorů v systému RHEL6 odpovídající požadavkům ZKB.	Integrace monitoring serverů s Centrální správou administračních účtů (s MS Active Directory jako systémem pro centrální správu uživatelských účtů v rámci PČR). Změny, které bude IBM realizovat jsou uvedeny pod tabulkou - kapitola 10. Centrální správa administračních účtů	Infrastruktura
§18 Identita odst 3 a) b) c) + odst 4 a) b) pro Přístup administrátorů ke ELASTIC serverům NSVIS (S9-14, S17-19)	Rekonfigurace ověření identity administrátorů v systému RHEL7 odpovídající požadavkům ZKB.	Změny, které bude IBM realizovat jsou uvedeny pod tabulkou - kapitola 10. Centrální správa administračních účtů	Infrastruktura
§18 Identita odst 3 a) b) c) + odst 4 a) b) pro Přístup administrátorů k SMTP serverům VISMAIL (T9-14, T17-19)	Rekonfigurace ověření identity administrátorů v systému RHEL7 odpovídající požadavkům ZKB.	Změny, které bude IBM realizovat jsou uvedeny pod tabulkou - kapitola 10. Centrální správa administračních účtů	Infrastruktura
§18 Identita odst 3 a) b) + odst 4 a) b) pro Přístup administrátorů a systémových účtů k SMTP serverům VISMAIL (U9-13, U17-19)	Rekonfigurace Users and Groups Management Lotus Domino Directory odpovídající požadavkům ZKB.	Změny, které bude IBM realizovat jsou uvedeny pod tabulkou - kapitola 11. Rekonfigurace PASSWORD QUALITY SCALE a EXPIRATION PERIOD na Domino serverech VISMAIL	Konfigurace Domino
§18 Identita odst 3 a) b) c) + odst 4 a) b) pro Přístup administrátorů k aplikačním serverům VISMAIL (V9-14, V17-19)	Rekonfigurace ověření identity administrátorů v systému RHEL7 odpovídající požadavkům ZKB.	Změny, které bude IBM realizovat jsou uvedeny pod tabulkou - kapitola 10. Centrální správa administračních účtů	Infrastruktura
§18 Identita odst 3 a) b) c) + odst 4 a) b) pro Přístup administrátorů a systémových účtů k aplikačním serverům VISMAIL (W9-13, W17-19)	Rekonfigurace ověření identity administrátorů ve WebSphere Administrační konzoli odpovídající požadavkům ZKB.	Integrace WebSphere s Centrální správou administračních účtů (s MS Active Directory jako systémem pro centrální správu uživatelských účtů v rámci PČR). Změny, které bude IBM realizovat jsou uvedeny pod tabulkou - kapitola 10. Centrální správa administračních účtů	Konfigurace WebSphere
§18 Identita odst 3 a) b) c) + odst 4 a) b) pro Přístup administrátorů k Oracle serverům VIS (Y9-14, Y17-19)	Rekonfigurace ověření identity administrátorů v systému RHEL7 odpovídající požadavkům ZKB.	Změny, které bude IBM realizovat jsou uvedeny pod tabulkou - kapitola 10. Centrální správa administračních účtů	Infrastruktura
§18 Identita odst 3 a) b) c) + odst 4 a) b) pro Přístup administrátorů k databázim VIS (Z9-14, Z17, Z19)	Rekonfigurace Oracle Database Security odpovídající požadavkům ZKB	Změny, které bude IBM realizovat jsou uvedeny pod tabulkou - kapitola 12. Rekonfigurace Oracle Database Security	Konfigurace Oracle
§18 Identita odst 3 a) b) + odst 4 a) pro Přístup systémových účtů k databázim VIS (AA9-13, AA17)	Rekonfigurace Oracle Database Security odpovídající požadavkům ZKB	Návrh změn, které je IBM připravená realizovat na požádaní provozovatelem systému VIS, je uveden v dokumentu: Návrh změn v security VIS - kapitola 12. Rekonfigurace Oracle Database Security	Konfigurace Oracle

§18 Identita odst 4 c) pro Přístup administrátorů k Flex Chassis (AB19)	Technologie samotného Flex Chassis neumožňuje prosadit minimální délku hesla delší, než 8 znaků (max. délka heslo 31 znaků). Nutná integrace s LDAP řešením odpovídajícím požadavkům ZKB.	Integrace Flex Chassis Management s Centrální správou administračních účtů (s MS Active Directory jako systémem pro centrální správu uživatelských účtů v rámci PČR). Změny, které bude IBM realizovat jsou uvedeny pod tabulkou - kapitola 10. Centrální správa administračních účtů	Infrastruktura
§18 Identita odst 3 b) c) + odst 4 a) b) pro Přístup administrátorů k Virtualizační vmWare platformě NSVIS (AC10-14, AC17, AC19)	Technologie virtualizačního vmWare prostředí neumožňuje prosadit některé požadavky ZKB a některé umí jen částečně. Nutná integrace s LDAP řešením odpovídajícím požadavkům ZKB.	Integrace Virtualizační vmWare platformy s Centrální správou administračních účtů (s MS Active Directory jako systémem pro centrální správu uživatelských účtů v rámci PČR). Změny, které bude IBM realizovat jsou uvedeny pod tabulkou - kapitola 10. Centrální správa administračních účtů	Infrastruktura
§19 Řízení přístupu, Aplikační přístup uživatelů: Klientské aplikace VIS/VISMail (K7)	Úprava přihlášení uživatele s expirovaným heslem.	Změny, které bude IBM realizovat jsou uvedeny pod tabulkou - kapitola 3. OPRAVA IMPLEMENTACE AUTENTIZACE S HESLEM PO EXPIRACI	Vývoj
§19 Řízení přístupu, Aplikační přístup uživatelů: Klientské aplikace VIS/VISMail (K7)	Oprava validace typu Authority uživatele při volání do CSVIS.	Změny, které bude IBM realizovat jsou uvedeny pod tabulkou - kapitola 4. OPRAVA VALIDACE TYPU AUTORITY PŘI VOLÁNÍ DO CSVIS	Vývoj
§19 Řízení přístupu, Aplikační přístup uživatelů: Klientské aplikace VIS/VISMail (K7)	Vyčištění a sjednocení kódu nsvis_csvis, aby používal pouze tabulky T_OCP_INFO pro plnění atributů uživatele (AuthorityName, AuthorityPlace) při volání do CSVIS	Změny, které bude IBM realizovat jsou uvedeny pod tabulkou - kapitola 5. ZMĚNA V PLNĚNÍ AUTHORITY NAME A PLACE	Vývoj
§21 Zaznamenávání činností, Aplikační přístup uživatelů: Klientské aplikace VIS/VISMail (K7)	Rozšíření tabulky audit o sloupec C_SUBJECT_ID NVARCHAR 30, kde bude zaznamenán JEE subject autentizovaného uživatele	Změny, které bude IBM realizovat jsou uvedeny pod tabulkou - kapitola 2. DOPLNĚNÍ LOGOVÁNÍ VOLAJÍCÍHO DO AUDITU	Vývoj
§21 Zaznamenávání činností, Přístup systémových účtů: Virtuální integrační srv ESB-P1,S1 Virtuální aplikační srv WAS-P1,S1 Virtuální Deployment Mgr DM-P1,S1 (K13)	Záznam neautorizovaných pokusů o přístup na chráněné zdroje do auditního logu T_AUDIT a tabulky T_LOGIN_ATTEMPT	Změny, které bude IBM realizovat jsou uvedeny pod tabulkou - kapitola 1. NÁVRH ZMĚN V AUDITOVÁNÍ NEOPRÁVNĚNÉHO PŘÍSTUPU	Vývoj

§21 Zaznamenávání činností odst 1 a) b) + odst 2 d) g) + odst 3 pro přístup administrátorů na Host servery NSVIS (M7-8, M13, M16, M18)	Nutné nakonfigurovat Linux Audit System a ochranu zaznamenaných informací. Nutné doplnit logování neprovedení činností, logování přístupu k záznamům o činnostech a nastavení uchovávání logů po dobu 3 měsíců.	Změny, které bude IBM realizovat jsou uvedeny pod tabulkou - 13. KONFIGURACE CENTRALIZOVANÉHO AUDITU ČINNOSTÍ ADMINISTRÁTORŮ VIS	Infrastruktura
§21 Zaznamenávání činností odst 1 a) b) + odst 2 d) g) + odst 3 pro přístup administrátorů na virtuální web servery NSVIS (N7-8, N13, N16, N18)	Nutné nakonfigurovat Linux Audit System a ochranu zaznamenaných informací. Nutné doplnit logování neprovedení činností, logování přístupu k záznamům o činnostech a nastavení uchovávání logů po dobu 3 měsíců.	Změny, které bude IBM realizovat jsou uvedeny pod tabulkou - 13. KONFIGURACE CENTRALIZOVANÉHO AUDITU ČINNOSTÍ ADMINISTRÁTORŮ VIS	Infrastruktura
§21 Zaznamenávání činností odst 1 a) b) + odst 2 d) g) + odst 3 pro přístup administrátorů na virtuální WebSphere servery NSVIS (O7-8, O13, O16, O18)	Nutné nakonfigurovat Linux Audit System a ochranu zaznamenaných informací. Nutné doplnit logování neprovedení činností, logování přístupu k záznamům o činnostech a nastavení uchovávání logů po dobu 3 měsíců.	Změny, které bude IBM realizovat jsou uvedeny pod tabulkou - 13. KONFIGURACE CENTRALIZOVANÉHO AUDITU ČINNOSTÍ ADMINISTRÁTORŮ VIS	Infrastruktura
§21 Zaznamenávání činností, Přístup administrátorů: WebSphere Administrační konzole DM-P1,S1 (P7-8)	Nastavit auditní systém WebSphere Application Server v souladu s požadavky ZKB.	Změny, které bude IBM realizovat jsou uvedeny pod tabulkou - kapitola 9. NASTAVENÍ AUDITNÍHO SYSTÉMU	Konfigurace WebSphere
§21 Zaznamenávání činností, Přístup administrátorů: WebSphere Administrační konzole DM-P1,S1 (P13, P16, P18)	Doplnění auditního systému WebSphere o neprovedení činností administrátorů v prostředí WebSphere. Nutné doplnit logování přístupu k záznamům o činnostech a nastavení uchovávání logů po dobu 3 měsíců.	Změny, které bude IBM realizovat jsou uvedeny pod tabulkou - 13. KONFIGURACE CENTRALIZOVANÉHO AUDITU ČINNOSTÍ ADMINISTRÁTORŮ VIS	Konfigurace WebSphere Infrastruktura
§21 Zaznamenávání činností, Přístup systémových účtů: Virtuální integrační srv ESB-P1,S1 Virtuální aplikační srv WAS-P1,S1 Virtuální Deployment Mgr DM-P1,S1 (Q8)	Změna ve zdrojovém kód VIS: pro ukládaná binární data zajistit ukládání hash do auditního logu (SHA256) pro zajištění validace integrity ukládání binárnich dat systémem VIS.	Změny, které bude IBM realizovat jsou uvedeny pod tabulkou - kapitola 6. ZAJISTIT UKLÁDÁNÍ HASH DO AUDITNÍHO LOGU (SHA512) – U BINÁRNÍCH DAT	Vývoj
§21 Zaznamenávání činností odst 1 a) b) + odst 2 d) g) + odst 3 pro přístup administrátorů na virtuální monitoring servery VIS (R7-8, R13, R16, R18)	Nutné nakonfigurovat Linux Audit System a ochranu zaznamenaných informací. Nutné doplnit logování neprovedení činností, logování přístupu k záznamům o činnostech	Změny, které bude IBM realizovat jsou uvedeny pod tabulkou - 13. KONFIGURACE CENTRALIZOVANÉHO AUDITU ČINNOSTÍ ADMINISTRÁTORŮ VIS	Infrastruktura

	a nastavení uchovávání logů po dobu 3 měsíců.		
§21 Zaznamenávání činností odst 1 a) b) + odst 2 d) g) + odst 3 pro přístup administrátorů na Virtualizační vmWare platformu NSVIS (S7-8, S13, S16, S18)	Nutné nakonfigurovat Audit System a ochranu zaznamenaných informací. Nutné doplnit logování neprovedení činností, logování přístupu k záznamům o činnostech a nastavení uchovávání logů po dobu 3 měsíců.	Změny, které bude IBM realizovat jsou uvedeny pod tabulkou - 13. KONFIGURACE CENTRALIZOVANÉHO AUDITU ČINNOSTÍ ADMINISTRÁTORŮ VIS	Infrastruktura
§21 Zaznamenávání činností odst 1 a) b) + odst 2 d) g) + odst 3 pro přístup administrátorů na SMTP servery VISMAIL (T7-8, T13, T16, T18)	Nutné nakonfigurovat Linux Audit System a ochranu zaznamenaných informací. Nutné doplnit logování neprovedení činností, logování přístupu k záznamům o činnostech a nastavení uchovávání logů po dobu 3 měsíců.	Změny, které bude IBM realizovat jsou uvedeny pod tabulkou - 13. KONFIGURACE CENTRALIZOVANÉHO AUDITU ČINNOSTÍ ADMINISTRÁTORŮ VIS	Infrastruktura
§21 Zaznamenávání činností odst 1 a) b) + odst 2 d) g) + odst 3 pro aplikační servery VISMAIL (V7-8, V13, V16, V18)	Nutné nakonfigurovat Linux Audit System a ochranu zaznamenaných informací. Nutné doplnit logování neprovedení činností, logování přístupu k záznamům o činnostech a nastavení uchovávání logů po dobu 3 měsíců.	Změny, které bude IBM realizovat jsou uvedeny pod tabulkou - 13. KONFIGURACE CENTRALIZOVANÉHO AUDITU ČINNOSTÍ ADMINISTRÁTORŮ VIS	Infrastruktura
§21 Zaznamenávání činností odst 1 a) b) + odst 2 d) g) + odst 3 pro přístup administrátorů na ORACLE servery VIS (Y7-8, Y13, Y16, Y18)	Nutné nakonfigurovat Linux Audit System a ochranu zaznamenaných informací. Nutné doplnit logování neprovedení činností, logování přístupu k záznamům o činnostech a nastavení uchovávání logů po dobu 3 měsíců.	Změny, které bude IBM realizovat jsou uvedeny pod tabulkou - 13. KONFIGURACE CENTRALIZOVANÉHO AUDITU ČINNOSTÍ ADMINISTRÁTORŮ VIS	Infrastruktura
§22 Detekce odst 1 událostí na Host serverech NSVIS (M6)	Klasifikace Identifikátorů a zajištění předání detekovaných událostí do SIEM.	Změny, které bude IBM realizovat jsou uvedeny pod tabulkou - 13. KONFIGURACE CENTRALIZOVANÉHO AUDITU ČINNOSTÍ ADMINISTRÁTORŮ VIS	Infrastruktura
§22 Detekce odst 1 událostí na virtuálních web serverech NSVIS (N6)	Klasifikace Identifikátorů a zajištění předání detekovaných událostí do SIEM.	Změny, které bude IBM realizovat jsou uvedeny pod tabulkou - 13. KONFIGURACE CENTRALIZOVANÉHO AUDITU ČINNOSTÍ ADMINISTRÁTORŮ VIS	Infrastruktura

§22 Detekce odst 1 událostí na virtuálních WebSphere serverech NSVIS (O6)	Klasifikace Identifikátorů a zajištění předání detekovaných událostí do SIEM.	Změny, které bude IBM realizovat jsou uvedeny pod tabulkou - 13. KONFIGURACE CENTRALIZOVANÉHO AUDITU ČINNOSTÍ ADMINISTRÁTORŮ VIS	Infrastruktura
§22 Detekce odst 1 událostí na virtuálních monitoring serverech NSVIS (P6)	Klasifikace Identifikátorů a zajištění předání detekovaných událostí do SIEM.	Změny, které bude IBM realizovat jsou uvedeny pod tabulkou - 13. KONFIGURACE CENTRALIZOVANÉHO AUDITU ČINNOSTÍ ADMINISTRÁTORŮ VIS	Infrastruktura
§22 Detekce odst 1 událostí na Virtualizační vmWare platformě NSVIS (Q6)	Klasifikace Identifikátorů a zajištění předání detekovaných událostí do SIEM.	Změny, které bude IBM realizovat jsou uvedeny pod tabulkou - 13. KONFIGURACE CENTRALIZOVANÉHO AUDITU ČINNOSTÍ ADMINISTRÁTORŮ VIS	Infrastruktura
§22 Detekce odst 1 událostí na SMTP serverech VISMAIL (R6)	Klasifikace Identifikátorů a zajištění předání detekovaných událostí do SIEM.	Změny, které bude IBM realizovat jsou uvedeny pod tabulkou - 13. KONFIGURACE CENTRALIZOVANÉHO AUDITU ČINNOSTÍ ADMINISTRÁTORŮ VIS	Infrastruktura
§22 Detekce odst 1 událostí na aplikačních serverech VISMAIL (S6)	Klasifikace Identifikátorů a zajištění předání detekovaných událostí do SIEM.	Změny, které bude IBM realizovat jsou uvedeny pod tabulkou - 13. KONFIGURACE CENTRALIZOVANÉHO AUDITU ČINNOSTÍ ADMINISTRÁTORŮ VIS	Infrastruktura
§22 Detekce odst 1 událostí na ORACLE serverech NSVIS (U6)	Klasifikace Identifikátorů a zajištění předání detekovaných událostí do SIEM.	Změny, které bude IBM realizovat jsou uvedeny pod tabulkou - 13. KONFIGURACE CENTRALIZOVANÉHO AUDITU ČINNOSTÍ ADMINISTRÁTORŮ VIS	Infrastruktura
§24 Aplikační bezpečnost odst 2 a) Ochrana před neoprávněnými činnostmi v Oracle (O8)	Rekonfigurace Oracle Database Security odpovídající požadavkům ZKB. Oracle bude dokonfigurován k ochraně před popřením provedených činností, kompromitací nebo neautorizovanou změnou.	Změny, které bude IBM realizovat jsou uvedeny pod tabulkou - kapitola 12. Rekonfigurace Oracle Database Security Návrh změn v security VIS - 13. KONFIGURACE CENTRALIZOVANÉHO AUDITU ČINNOSTÍ ADMINISTRÁTORŮ VIS	Infrastruktura
§24 Aplikační bezpečnost odst 2 a) Ochrana před neoprávněnými činnostmi v Monitoringu (P8)	NAGIOS bude dokonfigurován k ochraně před popřením provedených činností, kompromitací nebo neautorizovanou změnou.	Změny, které bude IBM realizovat jsou uvedeny pod tabulkou - 13. KONFIGURACE CENTRALIZOVANÉHO AUDITU ČINNOSTÍ ADMINISTRÁTORŮ VIS	Infrastruktura

§24 Aplikační bezpečnost odst 2 a) Ochrana před neoprávněnými činnostmi v Administračních nástrojích (WebSphere, Domino) (Q8)	Administrační nástroje (WebSphere, Domino) budou dokonfigurovány k ochraně před popřením provedených činností, kompromitací nebo neautorizovanou změnou.	Změny, které bude IBM realizovat jsou uvedeny pod tabulkou - 13. KONFIGURACE CENTRALIZOVANÉHO AUDITU ČINNOSTÍ ADMINISTRÁTORŮ VIS	Infrastruktu
§25 Kryptogr. Prostř. odst 2 b) pro přístup uživatelů a administrátorů Klientskými aplikacemi VIS odst 2 b) Přístup uživatelů CISu k webovým službám EVIC (VIS) odst 2 b) Přístup aplikace EVC2 k webovým službám CSVIS konektoru (VIS) odst 2 b) Přístup uživatelů MZ a KODOX k webovým službám VIS odst 2 b) Vzájemná výměna dat mezi aplikací VIS a ISOP (K29, L29, M29, N29, O29, Q29)	V konfiguracích SSL web serverů nastavit pouze odolné kryptografické algoritmy a kryptografické klíče dle požadavků ZKB.	Změny, které bude IBM realizovat jsou uvedeny pod tabulkou - 14. REKONFIGURACE SSL PRO HTTPS	Konfigurace WebSphere
§25 Kryptogr. Prostř. odst 2 b) Přístup aplikace EVC2 k službám JMS (VIS) (N29)	V konfiguracích Secure JMS ESB serverů nastavit pouze odolné kryptografické algoritmy a kryptografické klíče dle požadavků ZKB.	Změny, které bude IBM realizovat jsou uvedeny pod tabulkou - 15. REKONFIGURACE SSL PRO SECURE JMS	Konfigurace WebSphere
§25 Kryptogr. Prostř., EVC2 JMS (MZV) Přístup aplikace EVC2 k službám JMS (VIS) (N29)	změna ve zdrojovém kód VIS: pro ukládáná binární data zajistit kontrolu jejich integrity	Změny, které bude IBM realizovat jsou uvedeny pod tabulkou - kapitola 7. KONTROLA INTEGRITY BINÁRNÍCH DAT	Vývoj
§25 Kryptogr. Prostř. odst 2 b) pro MZ šifrování dat ukládaných do dočasných úložišť (P29)	V konfiguracích WebSphere vynutit pouze odolné kryptografické algoritmy a kryptografické klíče dle požadavků ZKB.	Změny, které bude IBM realizovat jsou uvedeny pod tabulkou - 16. REKONFIGURACE AES ŠIFROVÁNÍ VE WEBSPHERE A VÝMĚNA KLÍČŮ S MZ	Konfigurace WebSphere
§25 Kryptogr. Prostř. odst 2 b) Přístup aplikace VIS k webovým službám SIS2 (R29)	V konfiguracích WebSphere vynutit pouze odolné kryptografické algoritmy a kryptografické klíče dle požadavků ZKB.	Změny, které bude IBM realizovat jsou uvedeny pod tabulkou - 18. REKONFIGURACE SSL PRO WEBSPHERE	Konfigurace WebSphere
§25 Kryptogr. Prostř., Zpravodajské služby Přístup mailového klienta VIS k poštovní schránce ZS (S25)	Změna konfigurace mail session na použití SSL zabezpečení mailové komunikace	Změny, které bude IBM realizovat jsou uvedeny pod tabulkou - 17. REKONFIGURACE MAIL SESSION PRO SECURE SMTP	Konfigurace WebSphere

§25 Kryptogr. Prostř. odst 2 b) pro ICIS (interpol) (T29)	V konfiguracích WebSphere vynutit pouze odolné kryptografické algoritmy a kryptografické klíče dle požadavků ZKB.	Změny, které bude IBM realizovat jsou uvedeny pod tabulkou - 18. REKONFIGURACE SSL PRO WEBSPHERE	Konfigurace WebSphere
§25 Kryptogr. Prostř. odst 2 b) pro CSVIS (U29)	Nutné zabezpečit komunikaci pomocí HTTPS k přípojnému bodu sTESTA TAP. V konfiguracích WebSphere vynutit pouze odolné kryptografické algoritmy a kryptografické klíče dle požadavků ZKB. Nebo alternativně zajistit komunikaci vyhrazenými VLANy (OIPIT, SIMAC)	Změny, které bude IBM realizovat jsou uvedeny pod tabulkou - 18. REKONFIGURACE SSL PRO WEBSPHERE	Konfigurace WebSphere
§25 Kryptogr. Prostř. odst 2 b) pro službu Active Directory (V29)	V konfiguracích WebSphere vynutit pouze odolné kryptografické algoritmy a kryptografické klíče dle požadavků ZKB.	Změny, které bude IBM realizovat jsou uvedeny pod tabulkou - 19. REKONFIGURACE FEDERATED REPOSITORY VE WEBSPHERE PRO LDAPS VŮČI ACTIVE DIRECTORY SERVERŮM VIS	Konfigurace WebSphere
§25 Kryptogr. Prostř. odst 1 a) b) a odst 2 a) b) pro Nagios Monitoring (W24-26, W28-29)	Zamezit použití sdíleného účtu (donastavit účty uživatelům, integrovat s OpenLDAP řešením). Nutné zabezpečit komunikaci pomocí HTTPS.	Změny, které bude IBM realizovat jsou uvedeny pod tabulkou - 13. KONFIGURACE CENTRALIZOVANÉHO AUDITU ČINNOSTÍ ADMINISTRÁTORŮ VIS Návrh změn v security VIS - 14. REKONFIGURACE SSL PRO HTTPS	Infrastruktura
§25 Kryptogr. Prostř. odst 1 a) b) pro přístup na Host servery NSVIS (Y25-26)	Omezit přihlášení pod účtem root (lze jej použít jako sdílený účet a v tom případě nelze jednoznačně identifikovat koncového uživatele).	Změny, které bude IBM realizovat jsou uvedeny pod tabulkou - 20. REKONFIGURACE SSH V PROSTŘEDÍ RHEL	Infrastruktura
§25 Kryptogr. Prostř. odst 1 a) b) pro přístup na virtuální web servery NSVIS (Z25-26)	Omezit přihlášení pod účtem root (lze jej použít jako sdílený účet a v tom případě nelze jednoznačně identifikovat koncového uživatele).	Změny, které bude IBM realizovat jsou uvedeny pod tabulkou - 20. REKONFIGURACE SSH V PROSTŘEDÍ RHEL	Infrastruktura
§25 Kryptogr. Prostř. odst 1 a) b) pro přístup na virtuální WebSphere servery NSVIS (AA25-26)	Omezit přihlášení pod účtem root (lze jej použít jako sdílený účet a v tom případě nelze jednoznačně identifikovat koncového uživatele).	Změny, které bude IBM realizovat jsou uvedeny pod tabulkou - 20. REKONFIGURACE SSH V PROSTŘEDÍ RHEL	Infrastruktura
§25 Kryptogr. Prostř. odst 2 b) pro WebSphere Administrační konzoli (AB29)	V konfiguracích SSL Deployment Manager serverů nastavit pouze odolné kryptografické algoritmy a kryptografické klíče dle požadavků ZKB.	Změny, které bude IBM realizovat jsou uvedeny pod tabulkou - 14. REKONFIGURACE SSL PRO HTTPS	Konfigurace WebSphere

§25 Kryptogr. Prostř. odst 1 a) b) pro přístup na virtuální Monitoring servery NSVIS (AC25-26)	Omezit přihlášení pod účtem root (lze jej použít jako sdílený účet a v tom případě nelze jednoznačně identifikovat koncového uživatele).	Změny, které bude IBM realizovat jsou uvedeny pod tabulkou - 20. REKONFIGURACE SSH V PROSTŘEDÍ RHEL	Infrastruktu
§25 Kryptogr. Prostř. odst 1 a) b) pro přístup na Virtualizační vmWare platformu NSVIS (AD25-26)	Omezit přihlášení pod účtem root (lze jej použít jako sdílený účet a v tom případě nelze jednoznačně identifikovat koncového uživatele).	Změny, které bude IBM realizovat jsou uvedeny pod tabulkou - 20. REKONFIGURACE SSH V PROSTŘEDÍ ESXi	Infrastruktura
§25 Kryptogr. Prostř. odst 1 a) b) a odst 2 b) pro přístup na SMTP servery VISMAIL (AE25-26, AE29)	Omezit přihlášení pod účtem root (lze jej použít jako sdílený účet a v tom případě nelze jednoznačně identifikovat koncového uživatele). V konfiguracích Domino serveru (SSH) vynutit pouze odolné kryptografické algoritmy a kryptografické klíče dle požadavků ZKB.	Změny, které bude IBM realizovat jsou uvedeny pod tabulkou - 20. REKONFIGURACE SSH V PROSTŘEDÍ RHEL	Infrastruktura
§25 Kryptogr. Prostř. odst 1 a) b) a odst 2 b) pro přístup na správu SMTP serverů VISMAIL (AF29)	V konfiguracích HTTPS pro přístup k Lotus Domino vynutit pouze odolné kryptografické algoritmy a kryptografické klíče dle požadavků ZKB.	Změny, které bude IBM realizovat jsou uvedeny pod tabulkou - 21. REKONFIGURACE HTTPS V PROSTŘEDÍ LOTUS DOMINO	Konfigurace Domino
§25 Kryptogr. Prostř. odst 1 a) b) a odst 2 b) pro přístup na aplikační servery VISMAIL (AG25-26)	Omezit přihlášení pod účtem root (lze jej použít jako sdílený účet a v tom případě nelze jednoznačně identifikovat koncového uživatele).	Změny, které bude IBM realizovat jsou uvedeny pod tabulkou - 20. REKONFIGURACE SSH V PROSTŘEDÍ RHEL	Infrastruktura
§25 Kryptogr. Prostř. odst 2 a) b) pro Aplikační přístup uživatelů a administrátorů k aplikaci VISMAIL (AH28-29)	V konfiguracích SSL Deployment Manager serverů nastavit pouze odolné kryptografické algoritmy a kryptografické klíče dle požadavků ZKB.	Změny, které bude IBM realizovat jsou uvedeny pod tabulkou - 22. REKONFIGURACE HTTPS V PROSTŘEDÍ VISMAIL	Konfigurace WebSphere
§25 Kryptogr. Prostř. odst 1 a) b) pro přístup na Oracle servery NSVIS (AI25-26)	Omezit přihlášení pod účtem root (lze jej použít jako sdílený účet a v tom případě nelze jednoznačně identifikovat koncového uživatele).	Změny, které bude IBM realizovat jsou uvedeny pod tabulkou - 20. REKONFIGURACE SSH V PROSTŘEDÍ RHEL	Infrastruktura
§25 Kryptogr. Prostř. Odst 2 b) pro přístup na Flex Chassis (AJ29)	V konfiguracích Flex Chassis vynutit pouze odolné kryptografické algoritmy a kryptografické klíče dle požadavků ZKB.	Změny, které bude IBM realizovat jsou uvedeny pod tabulkou - 23. REKONFIGURACE HTTPS PRO PŘÍSTUP K AMM FLEXCHASSIS	Infrastruktura
§26 Dostupnost odst 2 c) zálohování důležitých technických aktiv VISu (K26, L26, M26, N26, O26, P26, R26)	Zálohují se pouze konfigurační soubory. Neprovádí se kompletní záloha aplikačních serverů.	Změny, které bude IBM realizovat jsou uvedeny pod tabulkou - 24. PRAVIDELNÉ ZÁLOHOVÁNÍ KOMPLETNÍHO FILE SYSTÉMU SERVERŮ VIS	Infrastruktura

§26 Dostupnost odst 1) 2 a) zajištění dostupnosti informací monitoringu (M22, M24)	Nedostupnost monitoring serverů je řešena náhradním technickým aktivem, které si přebírá IP adresaci původního monitoring serveru.	Změny, které bude IBM realizovat jsou uvedeny pod tabulkou - 25. OVĚŘENÍ NÁHRADNÍHO TECHNICKÉHO AKTIVA MONITORING SERVERU	Infrastruktura
Ostatní zjištění - §12 Akvizice, vývoj a údržba odst. 2 c) (B7)	Doporučujeme proto v rámci technických opatření zavést provádění statické analýzy kódu se zaměřením na včasné odhalení bezpečnostních rizik.	Změny, které bude IBM realizovat jsou uvedeny pod tabulkou - kapitola 8. 8. STATICKÁ ANALÝZA ZDROJOVÉHO KÓDU	Vývoj

1. Návrh změn v auditování neoprávněného přístupu

1.1. Popis problému

V případě pokusu o neautorizovaný přístup k webové službě je v tabulce NSVISAUDIT.T_LOGIN_ATTEMPT zalogováno "pass" = login prošel, ale není zalogováno, že následná autorizace byla zamítnuta.

1.2. Požadovaná změna

Je nutné zalogovat neoprávněný přístup do tabulky NSVISAUDIT.T_LOGIN_ATTEMPT a NSVISAUDIT.T_AUDIT (request a response).

1.3. Návrh změn

V tabulce NSVISAUDIT.T_LOGIN_ATTEMPT bude kromě záznamu o autentizaci i záznam o autorizaci. Autentizace bude probíhat stejně jako v současnosti – to znamená, že do NSVISAUDIT.T_LOGIN_ATTEMPT bude v případě zadání správných přihlašovacích údajů zapsáno „pass“. Autorizace se provádí až na úrovni webové služby (@RolesAllowed), proto není možné na úrovni login modulu určit, jestli má uživatel oprávnění nebo ne.

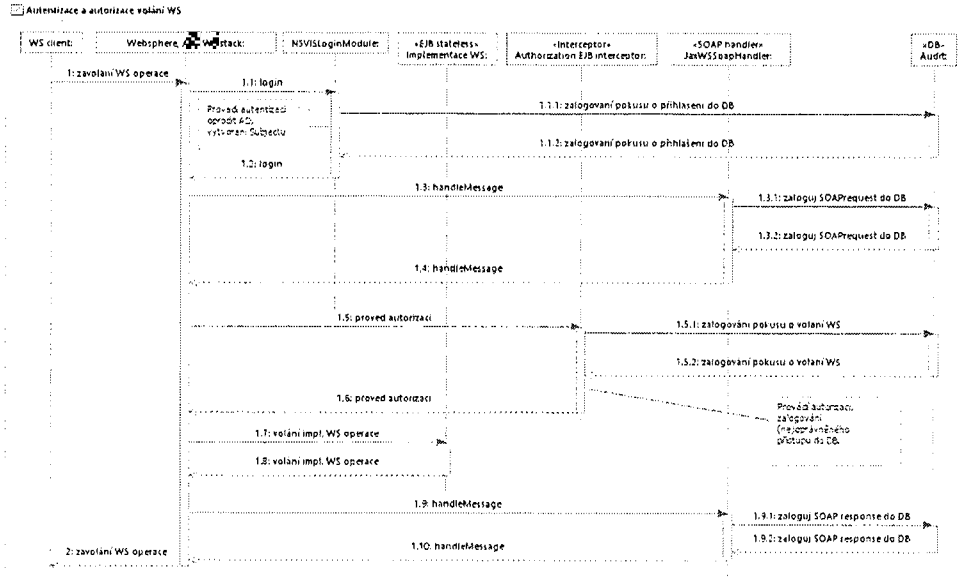
Na všechny WS (všechny webové služby jsou implementovány jako stateless EJB bean) přidáme interceptor, který bude provádět autorizaci, a ten v případě neoprávněného přístupu vytvoří 'fail' záznam v tabulce NSVISAUDIT.T_LOGIN_ATTEMPT. Záznam bude mít v atributu action uloženo 'authorization', abychom odlišili záznamy o loginu a autorizaci.

Aby mohla být na úrovni interceptoru prováděna autorizace, bude nutné provést několik úprav na úrovni implementace WS. Každá operace WS má v anotaci @RollesAllowed definované role, které jsou oprávněné volat danou operaci. "Vyhodnocení" této anotace (javax.annotation.security.RolesAllowed) probíhá ještě před zpracováním SOAP handlerů a EJB interceptorů. Tzn. není kam připojit custom komponentu, která by zalogovala neoprávněný přístup k WS. Z toho důvodu je nutné použít vlastní anotaci @RollesAllowed (cz.ibm.mv.vis.esb.common.annotation.RollesAllowed). Obsah (definované role, které mají přístup) zůstane u nové anotace stejný - změní se pouze import.

Dále bude nutné na úrovni třídy, která je implementací WS, doplnit anotaci @DeclareRoles. Ta bude obsahovat všechny role, které daná WS používá (tj. všechny role definované v anotacích RollesAllowed na jednotlivých operacích).

Vzhledem k tomu, že custom RollesAllowed anotace se vyhodnocuje až v interceptoru, který je aktivován až po SOAP handlerech, dojde k zalogování SOAP request/response do T_AUDIT i v případě neoprávněného přístupu.

Sequenční diagram:



2. Doplnění logování volajícího do Auditu

Do tabulky NSVISAUDIT.T_AUDIT bude doplněn sloupec C_USER_LOGIN, který bude obsahovat login uživatele, který danou operaci volal. Získání a zapsání loginu uživatele do DB bude implementováno v JAXWS SOAP Handleru současně s ostatními atributy jako callerInfo aj.

3. oprava implementace autentizace s heslem po expiraci

V aktuální verzi systém pracuje takto: pokud dojde k chybě autentizace, je vždy do tabulky NSVISAUDIT.T_LOGIN_ATTEMPT uložen „fail" záznam, kde ve sloupci C_REASON je vždy „invalid.credentials".

Oprava implementace autentizace s heslem po expiraci bude provedena tak, že budou parsovány chybové zprávy vrácené z Active Directory při pokusu o přihlášení. Tzn. když se při loginu vrátí z AD chybová zpráva obsahující kód ze sloupce „**AD**", bude text výjimky transformován na text uvedený ve sloupci „**Výjimka vrácená klientovi**". Tento text bude předán v security výjimce klientovi. Klient daný text transformuje na zprávu, která bude zobrazena uživateli.

V nové verzi budou chyby z AD parsovány, takže bude možné detailněji rozlišit důvod neúspěšné autentizace. Viz níže přiložená tabulka.

Tabulka mapování chybových kódů z AD na výjimky NSVIS:

AD	Význam	Výjimka vrácená klientovi	Reason v auditu

525	user not found	USER_NOT_FOUND	user.not.found
52e	invalid credentials	INVALID_CREDENTIALS	invalid.credentials
530	not permitted to logon at this time	LOGIN_NOT_PERMITTED_AT_TIME	login.not.permitted.at.time
531	not permitted to logon at this workstation	LOGIN_NOT_PERMITTED_AT_MACHINE	login.not.permitted.at.machine
532	password expired	PASSWORD_EXPIRED	password.expired
533	account disabled	ACCOUNT_DISABLED	account.disabled
534	The user has not been granted the requested logon type at this machine	LOGIN_NOT_GRANTED	login.not.granted
701	account expired	ACCOUNT_EXPIRED	account.expired
773	user must reset password	PASSWORD_RESET_REQUIRED	password.reset.required
775	user account locked	ACCOUNT_BLOCKED	account.blocked

4. oprava validace typu autority při volání do CSVIS

V současnosti probíhá kontrola oprávnění volání CSVIS na dvou místech. Nejprve klientská aplikace ověřuje, jestli má daný uživatel správnou autoritu (v NSVISCA.T_OCP_INFO) pro volání dané CSVIS operace/varianty. Další část ověření je na straně modulu nsvis_csvis, který podle mapovací tabulky csvis rolí (NSVISMAPPING.T_CSVIS_ROLES_MAP) ověří, jestli má uživatel požadované role pro volání této CSVIS operace/varianty. Z dané tabulky navíc modul získá další atributy, které použije pro volání CSVIS (např. endUserRole, autorityType).

V současné verzi může dojít k tomu, že klient nebude mít požadovanou autoritu, pod kterou je pak volána CSVIS operace.

Proto bude v nsvis_csvis implementována kontrola autority získané z mapovací tabulky oproti autoritám, které má uživatel v NSVISCA.T_OCP_INFO. Pokud nebude mít uživatel autoritu uvedenou v tabulce, bude ukončeno zpracování a uživateli bude vrácena výjimka.

5. Změna v plnění Authority Name a Place

Změna v plnění autorityName a Place:
- stávající funkcionalita umožnuje při nenalezení útvaru (v tabulce NSVISCA.T_OCP) odeslat požadavek do CSVIS s tím, že do autorityPlace se vyplní kód útvaru OSRI a do autorityName kód OCP (tyto kódy adaptér získá z AD)
- nová úprava bude v případě nenalezení útvaru vracet výjimku a neumožní odeslání requestu do CSVIS

6. Zajistit ukládání hash do auditního logu (SHA256) – u binárních dat

Následující úprava bude provedená z důvodu zajištění integrity binárních dat před neoprávněným čtením nebo změnou. Při přijetí zprávy evc2 ukládá modul nsvis_evc2 binární

data do databáze. Nově, v době ukládání provede výpočet hash SHA256 ukládaných binárních dat. Modul nsvis_evc2 předá do CA spolu s identifikátorem také vypočtený hash, který bude takto uložen do tabulky NSVISAUDIT.T_AUDIT.

7. Kontrola integrity binárních dat

Následující úprava bude provedená z důvodu zajištění integrity binárních dat před neoprávněným čtením nebo změnou. Nově, když bude CA přijímat odkaz na binární data z modulu nsvis_evc2, provede výpočet hash SHA256 a kontrolu, zda vypočtený hash odpovídá předávanému hash prostřednictvím webové služby.

8. Statická analýza zdrojového kódu

Nově bude zavedena statická analýza kódu (která se dosud neprovádí) se zaměřením na včasné odhalení bezpečnostních rizik v souladu s požadavky paragrafu 12 vyhlášky č. 316/2014. Statická analýza se bude zaměřovat na zajištění kvality kódu v souladu s projekty The Open Web Application Security Project (OWASP)

- OWASP Application Security Verification Standard (https://www.owasp.org/index.php/Category:OWASP_Application_Security_Verification_Standard_Project)
- OWASP Guide Project (https://www.owasp.org/index.php/Category:OWASP_Guide_Project#tab=Main)

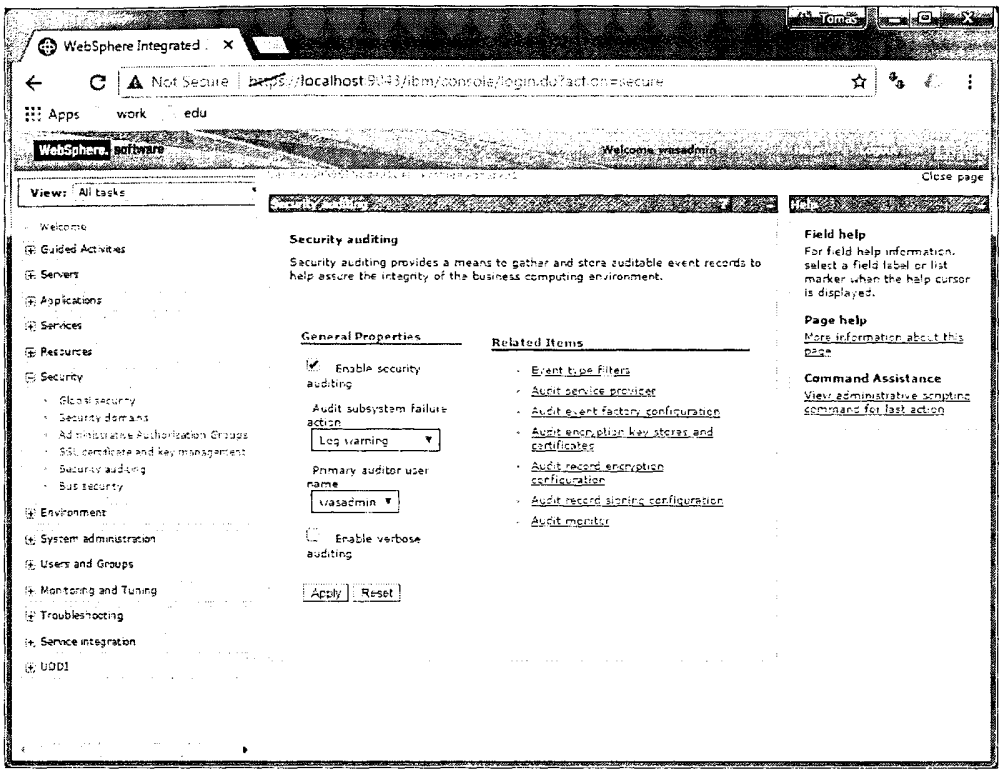
Statická analýza kódu bude prováděna pomocí nástroje Sonar Qube pro statickou analýzu zdrojového kódu Java a C#.

8.1. Nástroj Sonar Qube

SonarQube® je open source platforma určená pro řízení kvality zdrojového kódu na základě průběžně prováděných analýz a měření technické kvality zdrojového kódu od úrovně portfolia projektů do úrovně jednotlivých metod a jejich kódu. Jedna z oblastí kontroly je také bezpečnost.
Licence: SonarQube je volně distribuovaný pod open source licencí GNU Lesser GPL License, Version 3.
Požadavky na HW a SW: OS Linux, operační paměť 8 GB RAM, diskový prostor 30 GB, databázový systém MySQL 5.6.

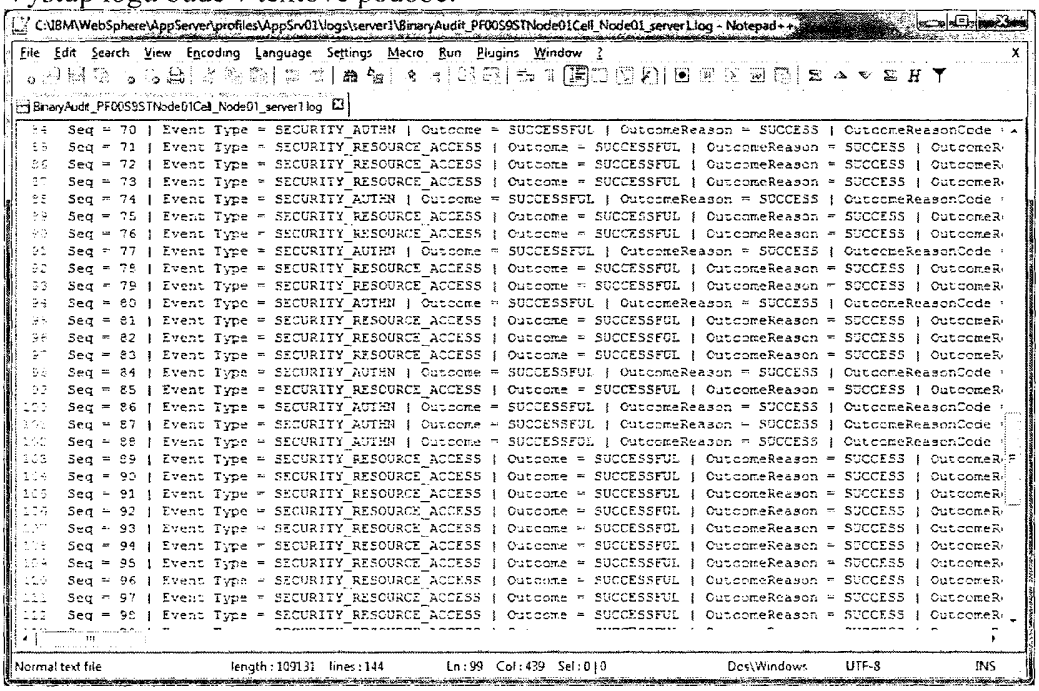
9. Nastavení auditního systému

Auditní systém bude nastaven pro záznam událostí prováděných/iniciovaných administrátory v prostředí WebSphere Application Server. Auditované budou tyto události: přihlášení do administrativní konzole, změny konfigurace prostřednictvím WebSphere Administration Console, změny konfigurace prostřednictvím wsadmin, runtime změny prostřednictvím WebSphere Administration Console, změny runtime prostřednictvím wsadmin.



Výstup auditního systému bude nastavený na filesystém ke každému aplikačnímu serveru. Auditní logy budou sehrávány na filesystém deployment manageru.

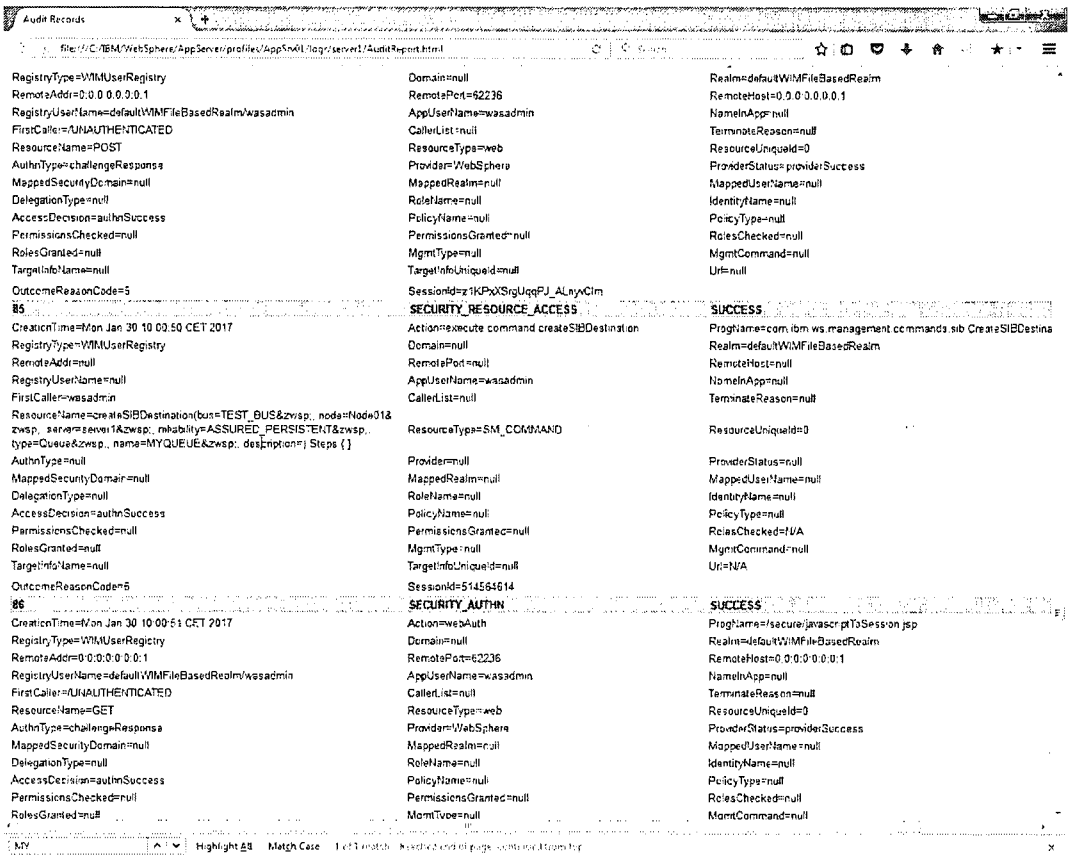
Výstup logů bude v textové podobě:



Pro zajištění ochrany získaných informací před neoprávněným čtením nebo změnou bude možné auditní záznamy kryptovat a podepisovat.
Další zpracování auditních záznamů. Z auditních záznamů lze produkovat html report pomocí příkazu binaryAuditLogReader s použitím utility wsadmin. Pro spuštění tohoto příkazu je

potřeba oprávnění auditor. Utilita poskytuje report i z kryptovaných dat, potřebuje mít přístup ke klíči (cestu ke klíčence a heslo).

```
AdminTask.binaryAuditLogReader('[-fileName
BinaryAudit_PF00S9STNode01Cell_Node01_server1.log -reportMode complete
-keyStorePassword password123 -outputLocation C:\binaryLogs]')
```



9.1. Postup provedení změn v nastavení auditního systému

Příprava auditních filtrů a faktory – společné pro všechna prostředí
Nastavení auditovacího subsystému aplikačních serverů – pro každé prostředí zvlášť
Nastavení kryptování a podepisování – pro každé prostředí zvlášť
Konfigurace sehrávání auditních logů – pro každé prostředí zvlášť
Příprava skriptů pro reporty – společné pro všechna prostředí

10. Centrální správa administračních účtů

Cílem je vytvoření řešení pro bezpečnou a jednotnou autentizaci administrátorů systému VIS, která dnes není napříč řešením harmonizována. Řešení využije stávající MS Active Directory server systému VIS (xdc-v1.pcr.cz, xdc-v2.pcr.cz, xdc-t1.tpcr.cz) a na všech linuxových serverech, virtuálních serverech a HW zařízeních (FlexCHassis) se provede integrace s těmito MS Active Directory servery.

10.1. Instalace a Konfigurace služeb pro Centrální správu administračních účtů

- Příprava implementace
- Integrace s MS Active Directory
  - Aktualizace komunikačních matic (IP adres a portů)
  - Aktualizace FW pravidel
- MS Active Directory
  - Vytvoření příslušných skupin uživatelů
  - Vytvoření příslušných účtů externích administrátorů VIS
- Ověření
  - Ověření autentizace proti MS Active Directory serverům
  - Ověření platnosti pravidel nastavených dle požadavku vyhlášky č. 316/2014 k ZKB

10.2. Integrace serverů VIS vůči službám Centrální správy administračních účtů

- Instalace a konfigurace služeb pro integraci RHEL s MS Active Directory
  - Instalace příslušných balíčků v RHEL (realmd, sssd, adcli, krb5-workstation, openldap-clients, apod.)
  - Nezbytná systémová nastavení dle požadavků ZkB
  - Přičlenění RHEL serverů k AD doménám PČR (pcr.cz, tpcr.cz)
  - Konfigurace SSH démona
- Konfigurace klienta
  - Nezbytná systémová nastavení dle požadavků ZkB
  - Konfigurace SSH klienta
- Ověření
  - Přihlášení ke klientskému stroji (Administrační PC, Administrační konzole)
  - Přihlášení k serveru pomocí SSH s podporou SSO
  - Ověření nastavení sudo oprávnění v RHEL pro autentizované uživatele v MS AD

10.3. Konfigurace komplexnosti hesel pro administrátory VIS

Komplexnost hesel administrátorů VIS, která budou uložená v MS Active Directory serverech, bude na základě požadavků ZkB řízená pomocí Globální doménové politiky domény PČR.CZ.

Požadavky vyhlášky č. 316/2014 k ZKB:

- minimální délka hesla patnáct znaků
- nejméně jedno velké písmeno
- nejméně jedno malé písmeno
- nejméně jedna číslice
- nejméně jeden speciální znak
- maximální doba pro povinnou výměnu hesla nepřesahující sto dnů
- zamezí opětovnému používání dříve používaných hesel a neumožní více změn hesla jednoho uživatele během stanoveného období, které musí být nejméně 24 hodin
- provádí opětovné ověření identity po určené době nečinnosti

Příklad: kadmin: add_policy -minlength 15 -maxlife "90 days" -minlife "1 day" -minclasses 4 -history 10 -lockoutduration "60 mins" -failurecountinterval 0 -maxfailure 5 default

Pro re-autentizaci po době nečinnosti vložit do konfigurace profilů uživatelů v RHEL nasledující řádky:

```
TMOUT=900
readonly TMOUT
export TMOUT
```

11. Rekonfigurace password quality scale a expiration period na DOMINO serverech VISMAIL

Na DOMINO serverech systému VISMAIL bude na přístupových účtech nastaveno:

- pro přístup administrátorů (přístup ke schránce SPOC) bude nastaven Password quality scale na hodnotu 15 a bude vygenerováno a nastaveno nové heslo (organizačně zajištěno, aby délka hesla byla minimálně 15 znaků)
- pro přístup administrátorů (přístup ke schránce SPOC) bude nastaven Password expiration na hodnotu 90 a grace period na hodnotu 30
- Zaškrtnout volbu Check Passwords on Notes IDs
- pro přístup systémových účtů bude nastaven Password quality scale na hodnotu 15 a budou vygenerována a nastavena nová hesla (organizačně zajištěno, aby délka hesel byla minimálně 8 znaků)

12. Rekonfigurace Oracle Database Security

Rekonfigurace Oracle Database Security, Database User Privileges, Roles and Profiles:

Pro přístup administrátorů (uživatele s rolí DBA, RSCPADM, IBMADM) bude nastaveno:

- ora12c_verify_function Password Requirements (po upgrade na Oracle 12) (stávající konfigurace síly hesla podle verify_function_11G Function Password Requirements neodpovídá všem požadavkům vyhlášky, splňuje jen částečně)
- pro přístup administrátorů (uživatele s rolí DBA, RSCPADM, IBMADM) bude nastaveno:
  - PASSWORD_LIFE_TIME 90
  - PASSWORD_GRACE_TIME 30

Pro přístup systémových účtů (tyto účty jsou konfigurovány v MS AD) bude nastaveno:

- ora12c_verify_function Password Requirements (po upgrade na Oracle 12) (stávající konfigurace síly hesla podle verify_function_11G Function Password Requirements neodpovídá všem požadavkům vyhlášky, splňuje jen částečně)
- Heslo bez expirace

13. Konfigurace Centralizovaného Auditu činností administrátorů VIS

Konfigurace RHEL Auditního systému pro zaznamenávání provozních a bezpečnostních činností administrátorů systému VIS. Na úrovni systémových oprávnění bude zajištěná ochrana

zaznamenaných informací. Rovněž bude nastaveno logování neprovedení činností, logování přístupu k záznamům o činnostech a nastavení uchovávání logů po dobu 3 měsíců.

- Konfigurace komponent auditd (auditd.conf)
- Definice pravidel (audit.rules)
  - Control rules
  - File System rules
  - System Call rules
- Konfigurace utilit
  - auditd: daemon to capture events and store them (log file)
  - auditctl: client tool to configure auditd
  - audispd: daemon to multiplex events
  - aureport: reporting tool which reads from log file (auditd.log)
  - ausearch: event viewer (auditd.log)
  - autrace: using audit component in kernel to trace binaries
  - aulast: similar to last, but instaed using audit framework
  - aulastlog: similar to lastlog, also using audit framework instead
  - ausyscall: map syscall ID and name
  - auvirt: displaying audit information regarding virtual machines
  - auditd: daemon to capture events and store them (log file)
  - auditctl: client tool to configure auditd
  - audispd: daemon to multiplex events
  - aureport: reporting tool which reads from log file (auditd.log)
  - ausearch: event viewer (auditd.log)
  - autrace: using audit component in kernel to trace binaries
  - aulast: similar to last, but instaed using audit framework
  - aulastlog: similar to lastlog, also using audit framework instead
  - ausyscall: map syscall ID and name
  - auvirt: displaying audit information regarding virtual machines
- Konfigurace pam_tty_audit (včetně záznamů aktivit uživatele root)
- Konfigurace přenosu dat ze serverů VIS na centrální auditní server
- Centrální auditní server
  - Agregace provozních logů všech administračních nástrojů a konzolí (WebSphere, Domino)
  - Agregace systémových a auditních logů všech serverů VIS
  - Agregace event logů všech HW management modulů (FlexChassis)
  - Bezpečné úložiště záznamů s řízeným přístupem
  - Konfigurace automatické 3 měsíční rotace záznamů
- Klasifikace identifikátorů provozních a bezpečnostních událostí
- Konfigurace předávaní požadovaných provozních a bezpečnostních informací z Centrálního auditního serveru do SIEM

14. Rekonfigurace SSL pro HTTPS

V konfiguracích SSL webových serverů VIS budou nastaveny pouze odolné kryptografické algoritmy a kryptografické klíče dle požadavků ZKB.

14.1. httpd.conf

V konfiguračních souborech HTTPD budou povoleny pouze šifry pro protocol TLS v1.2.

```
...
SSLProtocolDisable SSLv2 SSLv3 TLSv10 TLSv11
SSLCipherSpec ALL NONE
SSLCipherSpec TLSv12 TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
SSLCipherSpec TLSv12 TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
SSLCipherSpec TLSv12 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
SSLCipherSpec TLSv12 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
SSLCipherSpec ALL TLS_RSA_WITH_AES_128_GCM_SHA256
SSLCipherSpec ALL TLS_RSA_WITH_AES_256_GCM_SHA384
SSLCipherSpec ALL TLS_RSA_WITH_AES_128_CBC_SHA256
SSLCipherSpec ALL TLS_RSA_WITH_AES_256_CBC_SHA256
SSLCipherSpec ALL TLS_RSA_WITH_AES_128_CBC_SHA
SSLCipherSpec ALL TLS_RSA_WITH_AES_256_CBC_SHA
SSLCipherSpec ALL SSL_RSA_WITH_3DES_EDE_CBC_SHA
SSLEnable
...
```

15. Rekonfigurace SSL pro Secure JMS

V konfiguracích SSL WebSphere ESB serverů VIS budou nastaveny pouze odolné kryptografické algoritmy a kryptografické klíče dle požadavků ZKB.

15.1. Konfigurace TLS pomocí administrační konzole WebSphere

- Vytvoření vlastní SSL konfigurace pro JMS (TLS_for_JMS)
- Specifikace Quality of protection (QoP) pro TLS for JMS
  - Protocol - TLSv1
  - Provider - IBMJSSE2
  - Cipher Suite Group - Strong
  - Update selected ciphers
- Přiřazení konfigurace TLS_for_JMS messaging server v HC
  - Specifikace Transport Chain pro esbp1MEserver1
  - Specifikace SSL inbound channel (SIB_SSL_JFAP) pro InboundSecureMessaging
  - Změna SSL Configuration z z Centrally managed na TLS_for_JMS
- Přiřazení konfigurace TLS_for_JMS messaging server v ZC
  - Specifikace Transport Chain pro esbs1MEserver1
  - Specifikace SSL inbound channel (SIB_SSL_JFAP) pro InboundSecureMessaging
  - Změna SSL Configuration z z Centrally managed na TLS_for_JMS
- Restart klastru esbMEcluster
- Ověření startu Messaging Enginů a dostupnosti JMS front řešení VIS

16. Rekonfigurace AES šifrování ve WebSphere a výměnA klíčů s MZ

16.1. Generování nového AES klíče

Modul nsvis_mz používá AES klíč, který je uložený v Keystore ve formátu JCEKS. Nový AES klíč o délce 256 bitů vygeneruje administrátor nástrojem keytool, který je součástí Java JDK.

keytool -genseckey -alias **mzExportKey** -keyalg **AES** -keysize **256** -keypass **mySecretKeyPassword** -storepass **myKeystorePassword** –storetype **jceks** -keystore **mzKeystore.jck**

16.2. Nasazení nového AES klíče

Vygenerovaná klíčenka obsahující nový klíč bude administrátorem prostředí WebSphere umístěná do předem definovaných adresářů na obou ESB serverech řešení VIS.

cp **mzKeystore.jck /home/esbbe1/mzKeystore.jck (jak na serveru ESB-P1 tak na serveru ESB-S1)**

16.3. Úprava systémových parametrů modulu nsvis_mz pro použití nového AES klíče

Příslušné systémové parametry budou nastaveny pomocí KA Administrace ve shodě s předešlými kroky.

mz.export.keystore.filePath	/home/esbbe1/mzKeystore.jck	nsvis_mz	Absolutni cesta JCEKS keystore souboru obsahujici sdileny klic pro sifrovani vyexportovanych dat pro MZ.
mz.export.keystore.psswd	myKeystorePassword	nsvis_mz	Heslo k souboru keystore, ktere je ulozene na ceste pod klicem mz.export.keystore.filePath
mz.export.key.psswd	mySecretKeyPassword	nsvis_mz	Heslo klice v keystore, ulozenym pod aliasem mz.export.key.alias
mz.export.key.alias	mzExportKey	nsvis_mz	Alias sifrovaciho klice v keystore ulozisti mz.export.keystore.filePath

16.4. Export AES klíče

Administrátor NSVIS předá nový AES klíč administrátoru systému mobilních zařízení. Pro tento účel administrátor systému NSVIS vyexportuje klíč do tvaru pro předání. Export provede administrátor utilitou keyexporter. Tato utilita je dodávána samostatně v knihovně keyexporter.jar.

java -jar **keyexporter.jar mzKeystore.jck JCEKS myKeystorePassword mySecretKeyPassword mzExportKey exportfile.key**

Soubor **exportfile.key** následně administrátor VIS předá administrátoru systému mobilních zařízení.

17. Rekonfigurace Mail Session pro Secure SMTP

V konfiguracích WebSphere ESB serverů VIS budou nastaveny mail sessions pro ZS v odchozím směru na protokol Secure SMTP dle požadavků ZKB.

18. Rekonfigurace SSL pro WebSphere

V konfiguracích SSL WebSphere ESB serverů VIS budou nastaveny pouze odolné kryptografické algoritmy a kryptografické klíče dle požadavků ZKB. Certifikáty externích rozhraní včetně certifikátů CA budou uloženy do úložiště CellDefaultTrusStore Signer certificates.

Pro odchozí zabezpečenou komunikaci na servery SISII bude na ESB serverech VISu konfigurována Dynamic outbound endpoint SSL configuration. Pro autentizaci vůči siiap.pcr.cz se budou ESB servery VISu prokazovat interními certifikáty obou server podepsaných CA (esb-p1.out.vis, esb-s1.out.vis)

19. Rekonfigurace Federated Repository ve WebSphere pro ldaps vůči Active Directory serverům VIS

V konfiguracích WebSphere bude nastaven vůči Active Directory pouze zabezpečený protokol LDAPS a bude nastaveno použití odolných kryptografických algoritmů a kryptografických klíčů dle požadavků ZKB.

20. Rekonfigurace SSH v prostředí RHEL

V konfiguracích RHEL bude zakázáno vzdálené přihlášení se pod uživatelem root, a pro SSH přístup bude nakonfigurováno použití odolných kryptografických algoritmů a kryptografických klíčů dle požadavků ZKB.

21. Rekonfigurace HTTPS v prostředí LOTUS DOMINO

Pomocí administračního klienta Lotus Domino bude na všech SMTP serverech systému VISMAIL rekonfigurováno SSL pro HTTPS bude nastaveno použití pouze odolných kryptografických algoritmů a kryptografických klíčů dle požadavků ZKB.

22. Rekonfigurace HTTPS v prostředí VISMAIL

Na všech aplikačních serverech systému VISMAIL rekonfigurovat SSL pro HTTPS, nastavit použití odolných kryptografických algoritmů a kryptografických klíčů dle požadavků ZKB. Zároveň nastavit, aby byly certifikáty a klíče pro WebSphere uložené v zaheslované klíčence.

23. Rekonfigurace HTTPS pro přístup k AMM FlexChassis

Rekonfigurovat SSL pro HTTPS, nastavit použití odolných kryptografických algoritmů a kryptografických klíčů dle požadavků ZKB. Omezit přihlášení pod účtem USERID, zamezit použití tohoto sdíleného účtu (donastavit účty uživatelům, integrovat s OpenLDAP řešením).

24. pravidelné Zálohování kompletního File systému serverů VIS

Konfigurace a provádění pravidelných záloh kompletních FS serverů VIS. Zálohování bude probíhat prostředky daného serveru do komprimovaných offline souborů na předem specifikované úložiště (diskové pole provozovatele systému VIS). Zálohy se budou provádět pravidelně (1x měsíčně) a vždy při změně konfigurace, nebo při nasazení jakékoliv nové verze aplikace VIS. Záloha serverů bude obsahovat všechny důležité adresáře OS, adresáře s instalovanými aplikacemi a moduly, instalovanými dodatečnými ovladači, klientskými aplikacemi, nebo agenty. Zálohy FS serverů VIS nebudou obsahovat log soubory.

25. Ověření náhradního technického aktiva monitoring serveru

Vytvoření a ověření plné funkčnosti identické kopie monitoring serveru NAGIOS. Pro vytvoření kopie bude použita RHEL virtualizace. V reálnem čase bude v provozu vždy pouze jeden monitoring server (originál nebo identická kopie). Identická kopie bude využívat stejnou IP adresu jako originální monitoring server a bude možné ji spustit na jiném KVM hostu prostředí, než na kterém běží originální monitoring server.

Příloha č. 2 – Rozpočet ceny a platební podmínky

Počet listů: 4

Celková fixní část ceny činí **8 650 000,00 Kč bez DPH 10 466 500,00 Kč včetně DPH** a zahrnuje pouze činnosti zde uvedené a v rozsahu (počtu MD) zde uvedeném.

Tato fixní cena může být zvýšena až o 10 % v případě, že vznikne potřeba víceprací.

Předem schválené vícepráce až do výše 10% z fixní části ceny budou poskytovány za sazby uvedené v Příloze č.2 Rámcové smlouvy (bod 2. CENA ZA SLUŽBY na bázi čas a materiál) a budou fakturovány měsíčně dle výkazů odvedených víceprací odsouhlasených Objednatelem a podepsaných oprávněnou osobou.

Fixní část ceny za jednotlivé části Plnění dle této Prováděcí smlouvy je:

A) Rozšíření systému VIS o funkcionalitu automatické bezpečnostní prověrky o otisky prstů.

Cena za tuto část Plnění činí **2 700 000,00 Kč** (slovy dva miliony sedm set tisíc korun) **bez DPH 3 267 00,00 Kč** (slovy korun) **včetně DPH** a zahrnuje pouze činnosti uvedené v následující tabulce a v rozsahu (počtu MD) zde uvedeném.

Rozšíření ABP	MD	Role
Detailní analýza	12	analytik
Úprava databáze (úprava lustračního algoritmu, mapování státní příslušnosti, přípravy fonetických tvarů, úprava změnových skriptů	15	db.specialista
Úprava CA (design, vývoj, unit testy)	15	senior developer
Úprava ESB modulů (design, vývoj, unit testy)	16	senior developer
Úprava KA Vyčkat (design, vývoj, unit testy)	21	senior developer
Plán, sledování, kontrola vývoje (design, kontrola kódu), integrace mezi moduly	9	app. architekt
Linkování, zavedení nové role	3	app.architekt (2), senior developer (1)
Dokumentace (úprava relevantní dokumentace - designy, uživ. příručka)	6	analytik(2), app.architekt(2), senior developer(2)
Testy (funkční testy, integrační testy, podpora UAT)	22	test manager (12) , analytik(3), app.architekt(3), senior developer(4)
Deployment, releases	4	app.architekt (2), senior developer (2)
Součinnost specialisty MZV	5	EVC2 specialista
PM	9	project manager
Administrativa, komunikace, eskalace, issues v průběhu projektu (interní schůzky 1x týdně, maily s podporou WAS, provozem OIPIT, zadání programátorům, apod.)	6	IT architekt , db specialista, aplikační architekt , tester, analytik , případně senior programátor,

Úhrada fixní části ceny za tuto část plnění Prováděcí smlouvy bude provedena následujícím způsobem:

	Cena bez DPH v Kč	**DPH v %**	**DPH v Kč**	**Cena včetně DPH**
Etapa I - Analýza (30% z ceny)	810 000,00	21%	170 100,00	980 100,00
Etapa II - Implementace, instalace na testovací prostředí objednatele (35% z ceny)	945 000,00	21%	198 450,00	1 143 450,00
Etapa III - Akceptační testy a nasazení do provozu (35% z ceny)	945 000,00	21%	198 450,00	1 143 450,00
Celková cena	**2 700 000,00**	**21%**	**567 000,00**	**3 267 000,00**

B) Technická Implementace zjištěných požadavků vyplývajících z Bezpečnostní dokumentace VIS na základě provedené analýzy

Cena za tuto část Plnění činí **5 950 000,00 Kč** (slovy pět milionů devět set padesát tisíc korun) **bez DPH, 7 199 500,00 Kč** (slovy sedm milionů sto devadesát devět tisíc korun) **včetně DPH** a zahrnuje pouze oblasti uvedené v následující tabulce a činnosti/změny uvedené v Příloze č.1 a v rozsahu (počtu MD) zde uvedeném.

Oblast bezpečnosti (detail viz ZkB, Příloha č.1 smlouvy)	**MD**	**oblast činnosti**	**role**
Par.18 Identita	35	infra29, konfigurace6	IT architekt (21), Ap.architekt(8), LN specialista (2), db specialista (4)
Par.19 Řízení přístupu	5	vývoj	senior developer
Par.20 Ochrana před malware			
par.21 Zaznamenávání činností	55	vývoj12, WAS17, infra26	IT architekt (21), Ap.architekt(5),WAS specialista (17), senior developer(12)
Par.22 Detekce	8	infra	IT architekt
Par.23			
Par.24 Apl.bezpečnost	8	infra	Ap. Architekt
Par.25 Kryptogr.prost.	41	infra 23, konfigurace18	It architekt (17), Ap.architekt(6), LN specialista (2), WAS specialista (16)
Par.26 Dostupnost	7	infra	IT architekt
Ostatní zjištění - stat.analýza	35	Design, Konfigurace, vývoj	App.architekt (10), db specialista (5), senior developer(20)
Otestování VIS (funkčnosti) na jednotlivých prostředích	14	testy	test manager(8), ap.architekt(3) IT architekt(3)
UAT support	5	testy	test manager(3), Ap.architekt(1), IT architekt(1)
Aktualizace relevantní dokumentace	10	dokumentace	IT architekt (5), Ap.architekt (5)

Administrativa, komunikace, eskalace, issues v průběhu projektu (interní schůzky 1x týdně, maily s podporou WAS, provozem OIPIT, zadání programátorům, apod.)	20		IT architekt, LN specialista, WAS specialista, db specialista, Ap.architekt, senior developer, test manager
Project management	20		PM

Úhrada fixní části ceny za tuto část plnění Prováděcí smlouvy bude provedena následujícím způsobem:

	Cena bez DPH v Kč	**DPH v %**	**DPH v Kč**	**Cena včetně DPH**
Etapa I – Příprava, realizace na vývojovém a testovacím prostředí VUMS (40% z ceny)	2 380 000,00	21%	499 800,00	2 879 800,00
Etapa II - Implementace, realizace na testovacím prostředí objednatele (30% z ceny)	1 785 000,00	21%	374 850,00	2 159 850,00
Etapa III– realizace na produkčním prostředí zákazníka, akceptační testy předání do provozu (30% z ceny)	1 785 000,00	21%	374 850,00	2 159 850,00
Celková cena	**5 950 000,00**	**21%**	**1 249 500,00**	**7 199 500,00**

1. Daň z přidané hodnoty bude účtována v souladu se zákonem č. 235/2004 Sb., o dani z přidané hodnoty, v platném znění. Pokud se DPH na základě nové právní úpravy během smluvního období změní, výše DPH se automaticky změní v souladu s touto právní úpravou. V takovém případě Dodavatel vyúčtuje výše uvedenou cenu bez DPH a připočítá DPH v příslušné zákonem stanovené výši. Tato změna nebude považována za změnu ceny ani za změnu této Prováděcí smlouvy.
2. Kompletnost každého dodaného milníku bude potvrzena podepsáním Předávacího nebo Akceptačního protokolu. Úhrada ceny Plnění vč. DPH bude realizována Objednatelem na základě faktur, které budou vystaveny v souladu s podepsanými Předávacími nebo Akceptačními protokoly.
3. Datem zdanitelného plnění bude datum podpisu příslušného Akceptačního protokolu, Předávacího protokolu, či datum splnění příslušné části plnění. Dodavatel je povinen po vzniku práva fakturovat, vystavit a Objednateli předat do 5 pracovních dnů ode dne podpisu příslušného protokolu fakturu ve dvojím vyhotovení.
4. Splatnost faktur je 30 dnů od data jejich prokazatelného doručení Objednateli na adresu uvedenou ve Smlouvě. V případě doručení faktur po 15. prosinci se splatnost faktur prodlužuje na 60 dnů ode dne jejich prokazatelného doručení.
5. Daňový doklad musí obsahovat číslo Rámcové smlouvy, číslo této Prováděcí smlouvy a náležitosti řádného daňového dokladu podle příslušných právních předpisů, zejména pak zákona č. 235/2004 Sb., o dani z přidané hodnoty, ve znění pozdějších předpisů. V případě, že daňový doklad nebude mít odpovídající náležitosti nebo nebude vystaven v souladu s Rámcovou smlouvou, je Objednatel oprávněn zaslat jej ve lhůtě splatnosti zpět k doplnění Dodavateli, aniž se dostane do prodlení se splatností. Lhůta splatnosti počíná běžet znovu od opětovného doručení náležitě doplněného či opraveného daňového dokladu Objednateli.
6. Adresa Objednatele pro doručení daňového dokladu je:

Policejní prezidium ČR, Ředitelství pro podporu výkonu služby, Strojnická 27, poštovní schránka 62/ŘPVS, PSČ 170 89, Praha 7."

7. Fakturovaná částka se považuje za uhrazenou okamžikem odepsání příslušné finanční částky z bankovního účtu Objednatele uvedeného v této Prováděcí smlouvě ve prospěch bankovního účtu Dodavatele uvedeného v této Prováděcí smlouvě.

8. Společně s fakturami Dodavatel dodá kopie podepsaných předávacích nebo akceptačních protokolů, dle čl. 8.3. Rámcové smlouvy. Společně s poslední fakturou Dodavatel dodá počet skutečně odpracovaných hodin. Bez předložení uvedených dokumentů Objednatel nebude fakturu Dodavatele akceptovat.

9. Objednatel neposkytuje Dodavateli finanční zálohy na předmět plnění.

10. Jestliže Objednatel nesplní své platební závazky v souladu s termínem uvedeným v této Prováděcí smlouvě, a to ani po písemném upozornění Dodavatelem, bude Dodavatel oprávněn pozastavit dodávku plnění až do zaplacení splatné pohledávky nebo si vzít bez jakékoli odpovědnosti za případné škody zpět dodané nezaplacené Produkty, Programy, Materiály i další dodané položky a zároveň využít jiných právních prostředků.

11. V případě pozastavení plnění z důvodů prodlení s platbou ze strany Objednatele nebude toto považováno za prodlení Dodavatele s plněním podle této Prováděcí smlouvy.

Příloha č. 3 – Harmonogram plnění

Počet listů: 1

Předpokládáme, že realizace výše specifikovaných změn systému VIS bude trvat cca 7 měsíců a to bez přerušení, od začátku Projektu do konce implementace.

Rámcové harmonogramy prací jednotlivých částí Plnění jsou odvozeny od termínu podpisu Smlouvy a závisí na splnění předpokladů a součinnosti na straně Objednatele.

A) Rozšíření systému VIS o funkcionalitu automatické bezpečnostní prověrky o otisky prstů.

Termín plnění této části je do 4 měsíců od účinnosti této Smlouvy.

	Část plnění	Trvání	Předpokládané datum ukončení
1.	Etapa I – Analýza	1 měsíc	Do 1 měsíce od účinnosti smlouvy
2.	Etapa II – Implementace - instalace na testovacím prostředí zákazníka	1-2 měsíce	Do 3 měsíců od účinnosti smlouvy
3.	Etapa III – UAT, uvedení do provozu	1 měsíc	Do 4 měsíců od účinnosti smlouvy

B)Technická Implementace zjištěných požadavků vyplývajících z Bezpečnostní dokumentace VIS na základě provedené analýzy

Termín plnění této části je do 8 měsíců od účinnosti této Smlouvy.

	Část plnění	Trvání	Předpokládané datum ukončení
1.	Etapa I - Příprava, realizace na vývojovém a testovacím prostředí Dodavatele	1-4 měsíce	Do 4 měsíců od účinnosti smlouvy
2.	Etapa II - Realizace na testovacím prostředí zákazníka	1-2 měsíce	Do 6 měsíců od účinnosti smlouvy
3.	Etapa III – realizace na produkčním prostředí zákazníka, předání do provozu	1-2 měsíce	Do 8 měsíců od účinnosti smlouvy

Konkrétní harmonogram plnění bude vypracován Dodavatelem v souladu s tímto Rámcovým harmonogramem do jednoho týdne od podpisu Smlouvy.

Práce mohou být realizovány ve výše uvedených termínech za předpokladu, že nedojde ke změně zadání ze strany Objednatele a že budou splněny Podmínky a předpoklady a součinnosti uvedené v této Prováděcí smlouvě a to v požadovaných termínech.

V případě nedodržení výše uvedených termínů nebo neposkytnutí potřebné spolupráce, součinnosti ze strany Objednatele budou tyto termíny přiměřeně prodlouženy nebo posunuty. Termín plnění může být změněn jenom na základě dodatku ke smlouvě.

Harmonogram může být upraven též na základě vzájemné písemné dohody.

Příloha č. 4 – Řídící struktura projektu

Počet listů: 3

	Řídící rada Projektu	
Sponzor Projektu Objednatele		Sponzor Projektu Dodavatele
Manažer Projektu Objednatele		Vedoucí projektu Dodavatele
Vedoucí Projektu Objednatele		
Projektový tým Objednatele		**Projektový tým Dodavatele**

Řídící rada	Rozhoduje o klíčových otázkách Projektu, změně harmonogramu a změně rozpočtu. Členy řídící rady jsou sponzoři Projektu, projektový manažer, vedoucí Projektu obou Smluvních stran a dva zástupci každé Smluvní strany. Řídící rada je konečnou instancí pro změnová řízení. Řídící rada kontroluje řízení Projektu.

Klíčové role projektu na straně Objednatele

Sponzor Projektu	*Vrcholový pracovník* Sponzor projektu je pracovník vrcholového vedení Objednatele/Dodavatele, který má rozhodovací pravomoc a současně je odpovědný za úspěšné ukončení projektu. ▪ Účastní se schůzek Řídící rady projektu ▪ Odpovídá zejména za zajištění finančních zdrojů, zajištění včasného podpisu smluv resp. dodatků. ▪ Zajišťuje podporu projektu v rámci Objednatele/Dodavatele, splnění podmínek a předpokladů jeho realizace a nutné součinnosti v termínech potřebných pro projekt, ▪ Provádí strategická rozhodnutí, která mají vliv na úspěšnost projektu a informuje vedení Objednatele/Dodavatele o průběhu projektu. ▪ Závazně podepisuje požadavky na změnu, které jsou pro projekt zásadní a byly schváleny Řídícím výborem.
Manažer Projektu	*Vrcholový pracovník* ▪ Má konečnou pravomoc pro určení priorit, urovnání otevřených problémů. V případě rozporů eskaluje řešení na vyšší úroveň řízení v rámci resortu MV a PČR. ▪ Přebírá materiály předané druhou smluvní stranou. ▪ Má konečnou pravomoc pro rozhodování o změnách v projektu, které nemají vliv na smluvní vztahy mezi Objednatelem a Dodavatelem. ▪ Prosazuje systém VIS v podmínkách resortu Ministerstva vnitra. ▪ Jmenuje a odvolává členy ŘR za Objednatele. ▪ Projektový manažer Objednatele svolává a řídí zasedání společného orgánu ŘR. ▪ Zajišťuje vrcholové řízení projektu dle schváleného rozpočtu, harmonogramu a rozsahu implementace ▪ Koordinuje činnosti na mimorezortní úrovni.

	▪ Rozhoduje ve sporných případech ve vztahu k centrálním systémům CS-VIS a VISMAIL.
Vedoucí Projektu	***Hlavním úkolem vedoucího Projektu je koordinace práce jednotlivých týmů a přijímání rozhodnutí přesahující kompetence těchto týmů.*** ▪ Koordinuje práci jednotlivých členů projektového týmu a pravidelně informuje manažera Projektu o splněných úkolech či případných problémech. ▪ Přebírá materiály předané druhou Smluvní stranou. ▪ Je zodpovědný za akceptace dílčích předmětů plnění a jejich částí. ▪ Je odpovědný Řídící radě. ▪ Kontroluje průběžně postup všech fází a částí Projektu. ▪ Přijímá návrhy jednotlivých členů týmu a rozhoduje o nich v rámci svých kompetencí, případně je předkládá k rozhodnutí ŘR. ▪ Připravuje materiály pro jednání ŘR. ▪ Schvaluje harmonogramy dílčích fází Projektu ▪ Svolává pravidelně (minimálně 1x týdně), případně dle potřeby, schůzky vedení Projektu.
Provozní gestor	Je koordinátorem práce v technické oblasti, oblasti infrastruktury, rozhraní, user managementu a provozu. Je zodpovědný za spolupráci při zabezpečení provozu jednotlivých prostředí systému VIS, replikací, připravenost testovacích prostředí externích systémů. Je garantem technického řešení a souladu systému IS s provozní a technickou dokumentací předanou v rámci dodávky systému VIS. Řídí práci a součinnost provozního týmu.
Věcný gestor	Je zodpovědný za správnost specifikace zadání, požadavků, soulad procesů a funkcionalit systému VIS s odsouhlasenou analytickou dokumentací, která byla předána s úpravami systému VIS. Řídí práci a součinnost věcného týmu.
Koordinátor testování	Je zodpovědný za přípravu testovacích scénářů, soulad s odsouhlasenou analytickou dokumentací, která byla předána s dodávkou systému NS-VIS, organizaci a zajištění testů Dodavatele a Objednatele a akceptačních testů v definovaných termínech, evidenci výsledků, projednávání chyb a problémů z průběhu testování na straně Objednatele. Řídí práci a součinnost testovacího týmu.

Objednatel zajistí pracovníky pro každou z výše uvedených klíčových rolí Projektu (jmenuje pracovníky, kteří budou Dodavateli k dispozici po celou dobu Projektu). Objednatel si může přizvat zástupce třetích dotčených stran (externích systémů), podílejících se na vízovém procesu.

Klíčové role projektu na straně Dodavatele

Vedoucí Projektu	Je zodpovědný za řízení projektu v rámci schváleného rozpočtu, harmonogramu a rozsahu. Je zodpovědný akceptace dílčích předmětů plnění a jejich částí. Je odpovědný řídící radě.
Vedoucí analytik	Je zodpovědný za řešení dotazů a soulad aktualizace se specifikací procesů a funkcionalit s odsouhlasenou analytickou dokumentací, která bude předána s úpravou systému VIS na straně Dodavatele.
Aplikační architekt, vedoucí vývoje	Je zodpovědný za aplikační architekturu systému VIS, realizaci změn a úprav

IT architekt	Je zodpovědný za IT infrastrukturu serverové části VIS, technickou část rozhraní, user management.
Koordinátor testování	Je zodpovědný za přípravu testovacích scénářů, organizaci a zajištění testů Dodavatele a Objednatele, evidenci výsledků, projednávání chyb a problémů z průběhu testování na straně Dodavatele.
Vedoucí KA	Je zodpovědný za aktualizaci klientských aplikací systému VIS

Akceptační komise

Akceptační komise se skládá z:

- projektového manažera Objednatele,
- vedoucího projektu Objednatele,
- vedoucího projektu Dodavatele,
- provozního gestora Objednatele,
- věcného gestora Objednatele,

případně Sponzorů projektu.

Po dohodě mohou být na jednání akceptační komise přizváni další členové projektového týmu.

Příloha č. 5 – Součinnost Objednatele

Počet listů: 1

Základní součinnost objednatele je specifikována v Rámcové smlouvě.

1. Objednatel dále po celou dobu projektu:

- vytvoří pro realizační tým organizační a věcné podmínky pro naplnění součinnosti objednatele.
- nese odpovědnost za správnost obsahu existujících dat a číselníků a jejich předání Dodavateli v požadovaných termínech.
- ponese odpovědnost a náklady za integraci řešení do stávající infrastruktury MV ČR.
- poskytne potřebné informace, specifikace požadavků nezbytné pro vypracování analýzy, detailní specifikaci úprav systému VIS (NS-VIS a VIS MAIL) a designu aplikací včetně nezbytných konzultací k těmto specifikacím, požadavkům.
- zajistí aktualizaci a správu účtů uživatelů systému VIS (NS-VIS a VIS MAIL) v Active Directory Policie ČR a poskytování jeho služby s požadovanou dobou odezvy on-line autentizační informace.
- zajistí služby certifikační autority PČR (vydávaní a obnova certifikátů dle požadavků ZKB).
- nese odpovědnost za správnost a kompletnost specifikace požadavků na změny/úpravy systému VIS (NS-VIS a VIS MAIL) vhledem k požadavkům, specifikacím, dokumentům EU informačního systému ČR a dalších směrnic a metodických pokynů.

2. Objednatel je dále povinen:

- jmenovat členy Řídící rady, Manažera a Vedoucího projektu a jednotlivé gestory nejpozději do jednoho týdne od podpisu Smlouvy a udělit jim patřičné pravomoci.
- zajistit aktualizaci a správu účtů uživatelů systému NS-VIS a VIS MAIL v Active Directory Policie ČR.
- zajistit přístup zástupcům Dodavatele do prostor Objednatele, kde jsou instalovaná zařízení Dodavatele, v odůvodněných případech i mimo řádnou pracovní dobu Objednatele.

Objednatel se dále zavazuje k následující součinnosti:

a) Správa účtů uživatelů VIS (NS-VIS a VIS MAIL) v Active Directory Policie ČR
b) Uvolňování pracovníků, jmenovaných osob/gestorů a zástupců uživatelů Objednatele podle potřeb Projektu, a to alespoň po dobu od jmenování do předání předmětu plnění do užívání.
c) Objednatel se bude podílet na aktualizaci a připomínkování testovacích scénářů a na testování předané části předmětu plnění.
d) Objednatel souhlasí s posuzováním a zasláním vyjádření k předkládaným dokumentům od Dodavatele do 3 - 5 pracovních dnů podle obsahu a rozsahu pokud nebude dohodnuto jinak.
e) Zabezpečení účasti klíčových rolí na pravidelných projektových schůzkách jednou týdně a setkání s ostatními členy týmu do příštího pracovního dne a odbornými pracovníky a zástupci uživatelů systému VIS (NS-VIS a VIS MAIL) do 2 pracovních dnů po zadání požadavku na setkání, pokud nebude dohodnuto jinak.
f) Zajištění spolupráce s externími Dodavateli existujících informačních systémů, které budou předmětem komunikačního rozhraní.
g) Účasti na předtestování a předběžných testech
h) Provedení UAT - akceptačních testů za podpory Dodavatele
i) Jakékoli případné zaškolení operátorů, koncových uživatelů je plně v zodpovědnosti a bude provedeno Objednatelem.