Dílčí smlouva č. 20

k Rámcové smlouvě o poskytování služeb podpory provozu a rozvoje systémů EKIS MV a ISoSS

(dále jen „**Dílčí smlouva**“)

Česká republika – Ministerstvo vnitra

se sídlem:	Nad Štolou 936/3, 170 34 Praha 7
kontaktní adresa:	Nám. Hrdinů 1634/3, 140 00 Praha 4
IČO:	00007064
DIČ:	CZ00007064
zastoupena:	Ing. Ivo Rosypalem, ředitelem odboru provozu a rozvoje EKIS, na základě NMV č. 45/2011, o řízení, organizaci a výkonu ekonomické činnosti
bankovní spojení:	Česká národní banka, č. ú.: 3605881/0710
číslo smlouvy:	MV-148200- /2018

(dále jen „**Objednatel**“)

a

Národní agentura pro komunikační a informační technologie, s. p.,

se sídlem:	Kodaňská 1441/46, Vršovice, 101 00 Praha 10
IČO:	04767543
DIČ:	CZ04767543
ID datové schránky	hkrkpwn
zastoupen:	Vladimírem Dzurillou, ředitelem
zapsán v obchodním rejstříku	vedeném Městským soudem v Praze pod sp.zn A 77322
bankovní spojení:	ČSOB, a. s., č. ú.: 117404973/0300
číslo smlouvy:	2019/062 NAKIT

(dále jen „**Poskytovatel**“)

(dále jednotlivě jako „**Smluvní strana**“ nebo společně jako „**Smluvní strany**“)

uzavírají v souladu s ustanovením § 1746 odst. 2 zákona č. 89/2012 Sb., občanského zákoníku, tuto Dílčí smlouvu k Rámcové smlouvě o poskytování služeb podpory provozu a rozvoje systémů EKIS MV a ISoSS ze dne 31. 3. 2017 [č.j. Objednatele MV-151932-10/EKIS-2016; č.j. Poskytovatele 2017/036 NAKIT (dále jen „**Smlouva**“).

Preambule

Tato Dílčí smlouva je uzavřena za účelem naplnění rozvojového projektu „Zvýšení bezpečnosti informačních systémů EKIS MV a ISoSS – Etapa II“.

1 Předmět Dílčí smlouvy

1.1 Předmětem Dílčí smlouvy je:

a) dodávka hardware a souvisejícího SW a dodávka SW (dále jen „**HW a SW**“) v rozsahu dle Přílohy č. 1 část 1a) a 1e),
b) implementace, tj. provedení implementačních prací v podobě instalace a konfigurace, tak aby mohlo být dosaženo výstupů dle Přílohy č. 1 část 1a) - e) (dále jen „**implementace“)**
(vše dále též jako „**Plnění**“)
c) konzultační činnosti v rozsahu maximálně 100 MD v roli SAP Konzultant III (dále též jako „**konzultační služby**“).

1.2 Plnění bude poskytováno po samostatných milnících, kdy klíčové milníky Plnění ze strany Poskytovatele jsou definovány následovně:

I.	Instalace a konfigurace HW/SW v DC
II.	Implementace řešení SAP ETD (instalace a konfigurace)
III.	GRC Roll-out na útvarech PČR a pilot pro HZS (3 ÚO)
IV.	Implementace řešení pro EKIS WEB a OE
V.	Implementace opatření proti výpadku a ztrátě dat, vč. instalace a konfigurace HW/SW
VI.	Dodávka konzultačních služeb I.
VII.	Implementace řešení SAP ETD (testování a předvedení)
VIII.	GRC Roll-out na zbylých útvarech resortu MV
IX.	Dodávka konzultačních služeb II.

1.3 Dodávka HW a SW bude v souladu s požadavkem Objednatele poskytnuta s podporou v rozsahu 24 měsíců.

1.4 Poskytovatel se podpisem této Dílčí smlouvy zavazuje poskytnout Objednateli předmět Dílčí smlouvy specifikovaný v odst. 1.1 tohoto článku Dílčí smlouvy za podmínek uvedených v této Dílčí smlouvě a Smlouvě.

1.5 Předmětem Dílčí smlouvy je dále závazek Objednatele zaplatit Poskytovateli za poskytnutí předmětu Dílčí smlouvy dle odst. 1.1 tohoto článku Dílčí smlouvy Dílčí cenu dle čl. 2 Dílčí smlouvy.

2 Dílčí cena a platební podmínky

2.1 Dílčí cena za Předmět Dílčí smlouvy dle čl. 1 odst. 1.1 Dílčí smlouvy činí maximálně 20 073 187,47 Kč bez DPH, výše DPH činí 4 215 369,37 Kč, cena včetně DPH činí 24 288 556,84 Kč s DPH a skládá se z:

2.1.1. Ceny za Plnění ve výši maximálně 18 433 187,72 bez DPH složené z ceny za:

milník	Předmět milníku (stručný popis)	Částka v Kč bez DPH
I.	Instalace a konfigurace HW/SW v DC	Maximálně 4 791 527,47
II.	Implementace řešení SAP ETD (instalace a konfigurace)	2 186 100,00
III.	GRC Roll-out na útvarech PČR a pilot pro HZS (3 ÚO)	1 860 400,00
IV.	Implementace řešení pro EKIS WEB a OE	1 144 710,00
V.	Implementace opatření proti výpadku a ztrátě dat, vč. instalace a konfigurace HW/SW	7 417 250,25
VII.	Implementace řešení SAP ETD (testování a předvedení)	344 400,00
VIII.	GRC Roll-out na zbylých útvarech resortu MV	688 800,00

2.1.2. Ceny za konzultační služby dle čl. 1.1. c), tj. milníky VI. a IX., které budou poskytnuty v maximálním rozsahu 100 MD v roli Konzultant SAP III, kdy cena 16 400 Kč bez DPH za MD vychází z cen role uvedené v Příloze č. 8 Smlouvy. Maximální cena za konzultační služby činí částku 1 640 000,00 Kč bez DPH. Tyto konzultační služby budou čerpány dle požadavků Objednatele průběžně od podpisu této Dílčí smlouvy. Tyto konzultační služby budou hrazeny dle skutečného čerpání.

2.2 Konečná částka Dílčí ceny za plnění dle milníku č. I bude upravena dodatkem k této Dílčí smlouvě na základě cen za HW a SW ze smluv uzavřených Poskytovatelem s dodavateli po provedení zadávacích řízení při zohlednění souvisejících nákladů Poskytovatele.

2.3 Plnění dle čl. 1 odst. 1.1 Dílčí smlouvy bude předloženo k akceptaci postupně, a jeho akceptace proběhne formou podpisu jednotlivých dílčích akceptačních protokolů (dále jen „Dílčí akceptační protokol“), který tvoří Přílohu č. 2 této Dílčí smlouvy.

2.4 Dílčí cena bude hrazena na základě daňových dokladů (faktur) vystavených Poskytovatelem, a to po splnění dílčích milníků I. – IX. dle čl. 3 odst. 3.1. této Dílčí smlouvy, a to na základě Dílčího akceptačního protokolu. Část plnění se považuje za poskytnutou dnem jeho akceptace formou Dílčího akceptačního protokolu. Den podpisu Dílčího akceptačního protokolu je datem uskutečnění zdanitelného plnění. Součástí Dílčího akceptačního protokolu je i položkový rozpočet.

2.5 Poskytnutí konzultačních služeb dle čl. 1 odst. 1.1 c) bude předloženo k akceptaci maximálně ve dvou částkách, první k datu 31.12.2019 (dle milníku VI.) a druhá k datu 31.03.2020 (dle milníku IX.), a považuje se za dodané dnem jeho akceptace formou podpisu akceptačního protokolu konzultačních služeb, který tvoří Přílohu č. 3 této Dílčí smlouvy (dále jen „Akceptační protokol konzultačních služeb“). Cena za konzultační služby bude hrazena na základě daňového dokladu (faktury) vystaveného Poskytovatelem po jeho písemné akceptaci. Den podpisu tohoto Akceptačního protokolu konzultačních služeb je datem uskutečnění zdanitelného plnění – konzultačních služeb.

2.6 Ostatní platební podmínky jsou stanoveny ve Smlouvě.

3 Doba, místo a podmínky plnění

3.1 Poskytovatel se zavazuje dodat Plnění nejpozději v termínu do 31.03.2020 za předpokladu poskytnutí nezbytné součinnosti ze strany Objednatele, tak jak je definováno touto Dílčí smlouvou v čl. 4. Konzultační služby mohou být poskytovány nejpozději do 31.03.2020 s tím, že první část konzulačních služeb (milník VI. dle čl. 3 odst. 3.1) bude poskytnuta do 15.12.2019.

3.2 Poskytovatel se zavazuje dodat Plnění dle jednotlivých milníků takto:

I.	Instalace a konfigurace HW/SW v DC	Do 31.10.2019
II.	Implementace řešení SAP ETD (instalace a konfigurace)	Do 15.12.2019
III.	GRC Roll-out na útvarech PČR a pilot pro HZS (3 ÚO)	Do 15.12.2019

IV.	Implementace řešení pro EKIS WEB a OE	Do 15.12.2019
V.	Implementace opatření proti výpadku a ztrátě dat, vč. instalace a konfigurace HW/SW	Do 15.12.2019
VII.	Implementace řešení SAP ETD (testování a předvedení)	Do 31.01.2020
VIII.	GRC Roll-out na zbylých útvarech resortu MV	Do 31.03.2020

3.3 Objednatel a Poskytovatel se shodují, že realizace plnění dle milníků II. – V. je navázána na řádné a včasné splnění milníku I. Poskytovatel je tedy povinen poskytnout plnění dle milníků II. – V. v termínech dle čl. 3 odst. 3. 2 Dílčí smlouvy pouze za předpokladu, že bude řádně a v termínu dle čl. 3 odst. 3.2 Dílčí smlouvy poskytnuto plnění dle milníku č. I. V případě, že realizace dílčího milníku I. nebude provedena v termínu dle čl. 3 odst. 3.2 Dílčí smlouvy bude návazné plnění poskytnuto v termínu dle čl. 3 odst. 3.1 Dílčí smlouvy.

3.4 Místem plnění jsou adresy Objednatele uvedené v čl 4 odst. 4.2 Smlouvy.

4 Závazky smluvních stran a součinnost

4.1 Poskytovatel odpovídá za časové a obsahové plnění této Dílčí smlouvy, pokud Objednatel včas splní své závazky specifikované v odst. 4.2 tohoto článku Dílčí smlouvy.

4.2 Pro úspěšný průběh realizace Plnění a poskytování konzultačních služeb dle této Dílčí smlouvy se Objednatel zavazuje k poskytnutí součinnosti podle požadavků Poskytovatele dle Přílohy č. 1.

4.3 Každá smluvní strana jmenuje svého zástupce, který ji bude zastupovat v realizačních záležitostech souvisejících s plněním této Dílčí smlouvy.

zástupce za Objednatele: Ing. Petr Pechar

zástupce za Poskytovatele: Ing. Libor Mrázek

4.4 Ostatní závazky smluvních stran a podmínky součinnosti jsou stanoveny ve Smlouvě.

5 Sankce

5.1 V případě prodlení Poskytovatele s poskytnutím Plnění ve sjednaných termínech pro jednotlivé milníky dle čl. 3 odst. 3.2 této Dílčí smlouvy z důvodů ležících na straně Poskytovatele, má Objednatel vůči Poskytovateli právo na smluvní pokutu ve výši 0,05

% z ceny za daný milník (či maximální ceny v případě milníku I.) dle čl. 2 odst. 2.1.1 Dílčí smlouvy, a to za každý, byť jen započatý den prodlení maximálně však do výše ceny za daný milník dle Dílčí smlouvy bez DPH.

5.2 V případě, že k nesplnění termínu dle čl. 3 odst. 3.1 této Dílčí smlouvy došlo z důvodu, že cena HW a SW od dodavatelů přesáhla maximální částku uvedenou v čl. 2.1 písm. a) Dílčí smlouvy a bylo nutné opakovat zadávací řízení, se do doby rozhodné pro výpočet smluvní pokuty nezapočítávají dny, kdy probíhalo nové zadávací řízení, maximálně však 60 dní.

5.3 Vznikem povinnosti platit smluvní pokutu ani jejím skutečným zaplacením nezaniká povinnost Smluvních stran splnit povinnost, jejíž plnění bylo zajištěno smluvní pokutou.

5.4 Smluvní pokuty jsou splatné do 30 kalendářních dnů po obdržení vyúčtování smluvní pokuty na základě samostatné faktury.

6 Ostatní ujednání

6.1 Veškerá ujednání této Dílčí smlouvy navazují na Smlouvu a Smlouvou se řídí, tj. práva, povinnosti či skutečnosti neupravené v této Dílčí smlouvě se řídí ustanoveními Smlouvy. V případě, že ujednání obsažené v této Dílčí smlouvě se bude odchylovat od ustanovení obsaženého ve Smlouvě, má ujednání obsažené v této Dílčí smlouvě přednost před ustanovením obsaženým ve Smlouvě, ovšem pouze ohledně plnění sjednaného v této Dílčí smlouvě.

6.2 Dílčí smlouva nabývá platnosti dnem podpisu obou Smluvních stran a účinnosti po splnění zákonné podmínky vyplývající z § 6 odst. 1 zákona č. 340/2015 Sb., o registru smluv, ve znění pozdějších předpisů.

6.3 Objednatel se zavazuje, že povinnost zveřejnění Smlouvy v registru smluv uvedenou v odst. 2 tohoto článku Dílčí smlouvy splní neprodleně po podpisu této Dílčí smlouvy oběma Smluvními stranami.

6.4 Dílčí smlouva je uzavírána elektronicky.

6.5 Smluvní strany prohlašují, že Dílčí smlouva ve spojení se Smlouvou vyjadřuje jejich úplné a výlučné vzájemné ujednání týkající se daného předmětu Dílčí smlouvy. Smluvní strany po přečtení Dílčí smlouvy prohlašují, že byla uzavřena po vzájemném projednání, určitě a srozumitelně, na základě jejich pravé, vážně míněné a svobodné vůle. Na důkaz uvedených skutečností připojují podpisy svých oprávněných osob či zástupců.

6.6 Provoz Plnění (implementovaného řešení) bude řešen dodatkem k příslušným Dílčí smlouvám upravující provoz EKIS MV a ISoSS.

6.7 Nedílnou součást Dílčí smlouvy tvoří následující přílohy:
Příloha č. 1 – Technická specifikace
Příloha č. 2 – Dílčí akceptační protokol
Příloha č. 3 – Akceptační protokol konzultačních služeb

V Praze dne ……..

_____

Ing. Ivo Rosypal
ředitel odboru provozu a rozvoje EKIS
Česká republika – Ministerstvo vnitra

V Praze dne 20. 9. 2019

v z. Ing. Antonín Chlum
Ing. Vladimír Dzurilla
ředitel
Národní agentura pro komunikační informační technologie, s. p.

Příloha č. 1 – Technická specifikace

Příloha 1 se dělí na části dle jednotlivých Milníků

- Část 1a) pro Milník I., II. a VII.
- Část 1b) pro Milník IV.
- Část 1e) pro Milník V.
- Část 1d) pro Milník III. a VIII.

Část 1a – Technická specifikace a návrh řešení pro SAP

Rozsah řešení implementovaný NAKIT

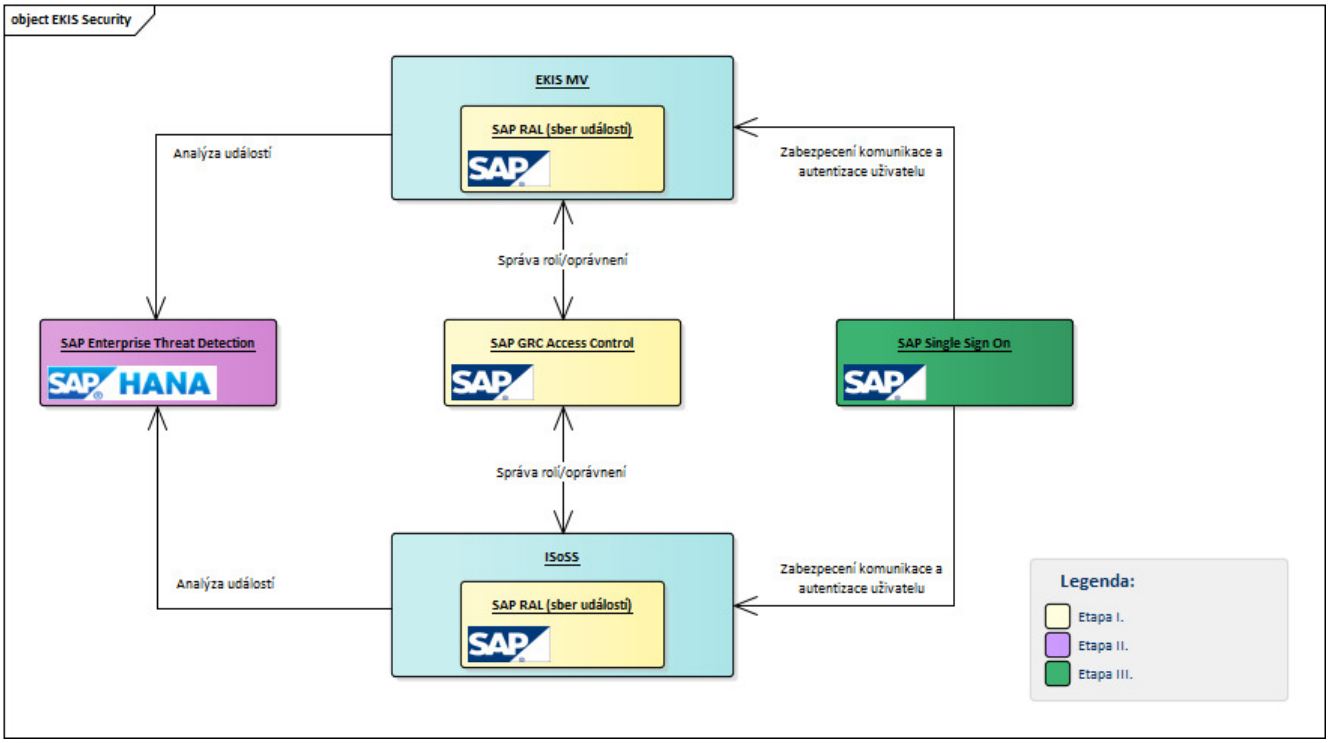
Informační systémy EKIS MV a ISoSS budou doplněny o společný subsystém, který se bude skládat z modulu SAP ETD a funkcionality logovacích nástrojů systému SAP navazujících věcně a technologicky na řešení připravované v první etapě. Řešení je navrženo tak, aby bylo možné v rámci konfigurace jednotlivých modulů oddělit kontext systémů EKIS MV a ISoSS, i když se předpokládá jednotná správa bezpečnostních modulů. Přestože bude řešení fyzicky sdílet prvky stávající infrastruktury, logicky bude v maximální možné míře odděleno tak, aby byla možná nezávislá administrace i používání bezpečnostního subsystému.

Pro zajištění vzájemné kompatibility a hladké integrace se stávajícími moduly obou IS je pro pokrytí požadovaných oblastí navržena implementace následujícího produktu SAP:

SAP Enterprise Threat Detection (ETD)

Nástroj pro konsolidaci logů z mnoha systémů a jejich vyhodnocování v reálném čase s následnou možností automatických i manuálních akcí - upozornění administrátora, předání incidentu externímu dohledovému systému atd. Systém zohledňuje informace publikované v rámci „SAP security notes“.

- Konsoliduje a normalizuje logy z různých komponent SAP i non-SAP
- Detekuje v reálném čase automaticky podezřelé aktivity.
- Databáze událostí je k dispozici pro následné analýzy.
- Události jsou vyhodnocovány na základě „vzorů“ (patterns), které jsou součástí dodávky.
- „Vzory“ (patterns) pro vyhodnocování se automaticky aktualizují ze SAP interních zdrojů a veřejných databází zranitelností.
- Možnost zadávat vlastní záznamy do databáze „vzorů“ (patterns).
- Používá informace o SAP landscape k zvýšení efektivity hledání podezřelých činností.
- API na non-SAP komponenty.
- K odhalování podezřelých aktivit se používají statistické metody a korelace událostí.
- Bohaté informace o SAP prostředí umožní optimální hlídání bezpečnosti v rámci SAP systémů.
- Vhodný pro využití reaktivního přístupu k bezpečnostním metodám.
- Napomáhá maximálně rychlé reakci na kybernetický útok.



Obrázek 1 - Návrh aplikační architektury

Logování událostí

Konsolidace bezpečnostních a aplikačních logů ze SAP systémů

Bude revidováno a sjednoceno nastavení logovacích nástrojů SAP, vč. dříve implementovaného SAP RAL, s cílem poskytnout ucelený zdroj událostí pro další analýzu v SAP ETD.

Implementace SAP ETD

Bude implementován nástroj SAP ETD, který bude načítat a normalizovat logované události a umožní jejich centrální analýzu, vč. automatického vytváření incidentů na základě zaznamenaných událostí. Zároveň bude ze SAP ETD probíhat export všech událostí pro účely archivace a předávání vybraných incidentů do dohledového systému (DCeGOV). V rámci implementace vznikne krátkodobé (cca 1. měs.) a střednědobé (cca 6 měs.) úložiště pro konsolidované logy událostí.

Doplnění funkcí logování událostí v oblasti zákaznického vývoje a non-SAP aplikací

Zákazníkem určené zákaznické a non-SAP aplikace budou upraveny / nastaveny tak, aby zaznamenávaly klíčové události ve formátu vhodném pro SAP ETD, kde budou zahrnuty do centrálního vyhodnocení.

Tyto logy budou využity i pro účely kompenzačních kontrol. Pro rizikové operace nebo kombinace operací, které bude nezbytné zachovat v oprávněních uživatelů, lze pomocí logu kontrolovat, zda došlo k podezřelým akcím.

Požadavky na součinnost MV

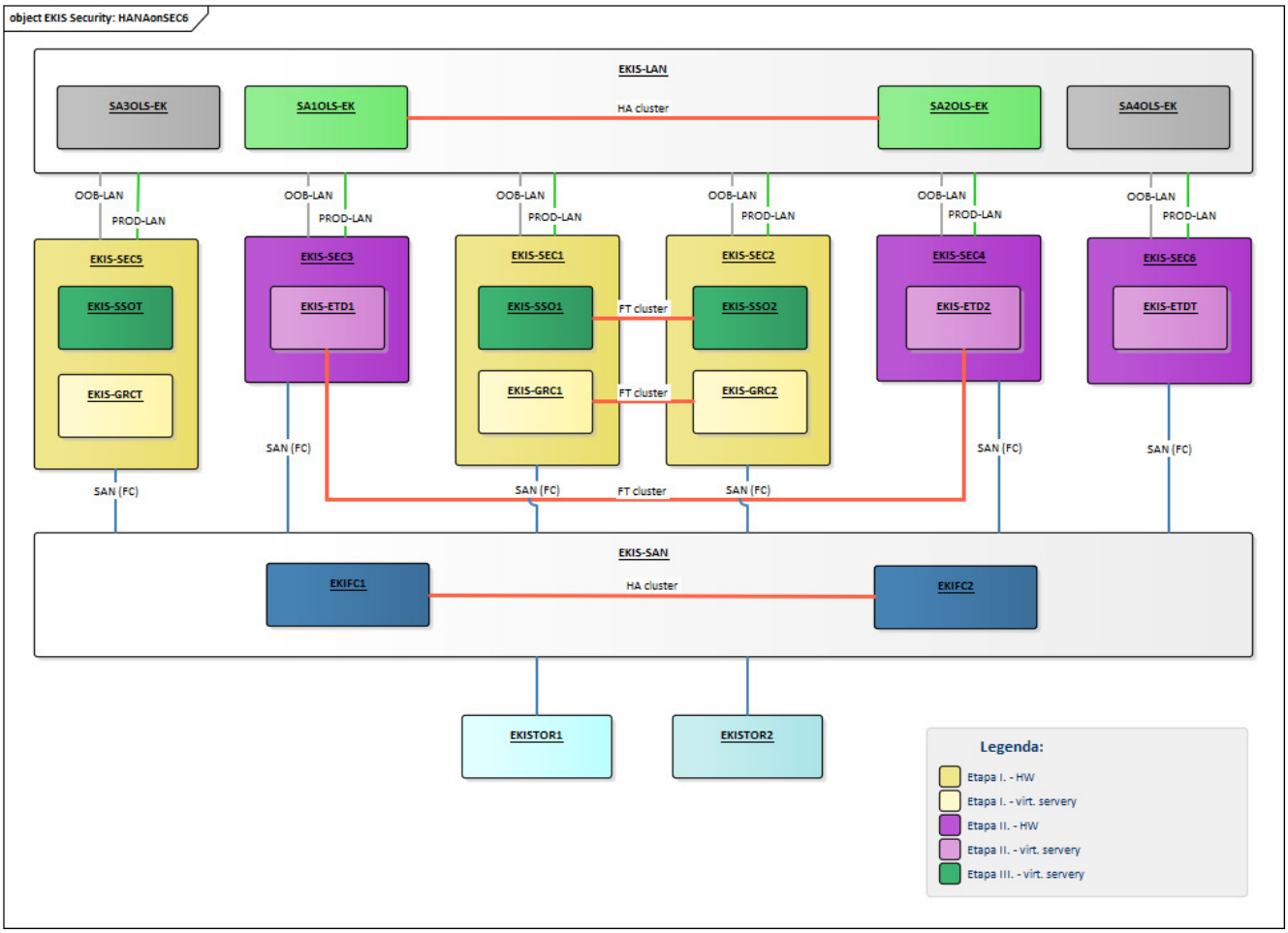
MV zajistí identifikaci klíčových událostí, které mají být zaznamenány v logu.

Oblast „Autentizace a Oprávnění“ a Šifrování databáze a komunikace uživatelů

Aktuální stav implementace nástrojů v resortu MV v rámci projektu budování resortního IdM (zejména SSO a dvoufaktorová autentizace) zastřešovanými OKB zatím neposkytuje možnost jejich užití. Proto je tato oblast odložena na další etapu, kde bude tato možnost opět prověřena.

HW architektura

Vzhledem k tomu, že SAP ETD používá platformu SAP HANA, budou do stávající infrastruktury doplněny odpovídající servery. Řešení pro datová úložiště (storage) bylo již implementováno v předchozí etapě a bude dále využito.



Obrázek 2 - Návrh HW architektury

Položkový rozpis HW a SW

Implementace modulu SAP ETD	Popis	počet ks
HW		
Rack server (PRIMERGY RX4770 M3, 4U)	2x Xeon E7-8880v4 22C/44T 2.20GHz 55MB, 512GB DDR4	2
Rack server (PRIMERGY RX4770 M3, 4U)	2x Xeon E7-8880v4 22C/44T 2.20GHz 55MB, 256GB DDR4	1
SW		
LicRHEV - Red Hat Enterprise Virtualization (2-sockets), Standard	RV0236407F4	3
LicRHELP - Red Hat Enterprise Linux for SAP Applications, Premium	RH00150F4	4
LicRHELS - Red Hat Enterprise Linux for SAP Applications, Standard	RH00151F4	2
LicRHHA - Red Hat High Availability	RH00025F4	4

HW a SW je pořizován s 2 letou podporou/zárukou.

Část 1b – Technická specifikace a návrh řešení pro EKIS WEB a OE

Oblast Logování

Požadavky MV: návrh řešení problematiky logování činností uživatelů systémů EKIS MV a ISoSS na platformě SAP i non-SAP. Řešení musí obsahovat návrh sběru, ukládání a archivace logů. Dále řešení musí zahrnovat nástroj na vyhodnocování těchto logů.

Součástí řešení také musí být možnost vyhrávání vybraných logů pro DCeGOV.

Rozsah logování bude rozdělen na dvě části, privilegované účty a ostatní účty. U privilegovaných účtů bude logovaná veškerá činnost a u ostatních účtů bude logována vybraná činnost.

Návrh řešení EKIS WEB

Předpokladem je existence společného systému pro sběr a logů ze všech subsystémů EKIS MV. Do tohoto systému budeme stanoveným rozhraním periodicky odesílat logy z několika zdrojů, které nyní ukládají logy na serveru IBM Domino:

1) Systémový log (systémová databáze log.nsf) - zde je velké množství logů vesměs nepotřebných pro daný účel. Zajistíme výběr relevantních logů jednoduchým způsobem dle vyhledání nakonfiguravaných klíčových slov, odesílat tak půjde např. jen logy o přihlášení a odhlášení IBM Notes uživatelů, resp. administrátorů.

2) Webový log (textové soubory Access, Agent, Referer alternativně systémová databáze domlog.nsf) - zde se protokolují všechny HTTP požadavky uživatelů, ale bez dat. Pokud se při detailní analýze ukáže, že je potřeba logovat jakékoliv přístupy ke specifickým prvkům aplikací, půjde to zajistit výběrem z těchto logů.

3) Administrační požadavky (systémová databáze admin4.nsf) - ve strukturovaných dokumentech se zde ukládají požadavky na specifické akce (asi 200 typů) a záznamy o jejich vyřízení. Buď by se odesílaly všechny, nebo jen vybrané typy, např. Change HTTP Password in Domino Directory.

4) Log změn ACL (v každé .nsf databázi) - v jednoduché struktuře (čas, akce). Změn není mnoho, takže je lze odesílat všechny.

5) Protokol webových aktivit (aplikační databáze wlog.nsf) - aplikační protokol EKIS WEB protokoluje otevření dílčích aplikací uživateli. Zde předpokládáme odesílání všech logů a v plné struktuře (Začátek, Konec, Trvání, IP, Uživatel (OEČ a jméno), Jednotka a nadřazené jednotky (kódy a názvy), Aplikace).

Pro každý zdroj bude potřeba naprogramovat modul pro načtení (s rozpoznáním naposledy odeslaného), výběr relevantních a transformaci do struktury společného systému. Dále modul pro odesílání logů do společného systému.

V této etapě nepředpokládáme doplnění logování událostí, které se doposud nelogují. Pokud by bylo požadováno další zpodrobnění logů, bylo by nutno na IBM Domino server nainstalovat auditní SW. To má významný dopad na jeho zatížení, takže by byla nutná výměna HW.

Návrh řešení OE

Předpokladem je existence společného systému pro sběr logů ze všech subsystémů EKIS MV. Do tohoto systému budeme stanoveným rozhraním periodicky odesílat logy o událostech, jejichž logování bylo smluveno.

Pro každý zdroj logovaných událostí bude potřeba naprogramovat výběr relevantních informací a transformaci do struktury společného systému. Dále bude potřeba naprogramovat modul pro odesílání logů do společného systému.

V aplikační agendě nastavování přístupových práv bude doplněno logování veškerých změn přístupových práv tak, aby bylo dohledatelné, jaké přístupy, kdo a kdy přiděloval.

Oblast Autentizace a oprávnění

Požadavky MV: Požadavkem je návrh řešení problematiky autentizace a oprávnění uživatelů systémů EKIS MV a ISoSS na platformě SAP i non-SAP.

V rámci navrhovaného řešení pro oblast autentizace je požadováno sjednocení přihlášení uživatelů do systémů (SSO) a zavedení dvoufaktorové autentizace vybraných uživatelů (zřízení vlastní certifikační autority).

V rámci navrhovaného řešení pro oblast oprávnění je požadováno pravidelné automatické i manuální přezkoumávání a vyhodnocování KKO. Dále je požadováno, aby navrhované řešení zabránilo přidělení KKO a bylo co nejvíce automatizováno a plně integrováno do stávajícího landscape SAP.

Návrh řešení EKIS WEB

Zatím není požadováno zavedení vícefaktorové autentizace.

Sada uživatelů EKIS WEB a jejich přiřazení k rolím a jednotkám se kompletně zadává v prostředí SAP, odkud se synchronizuje do prostředí IBM Domino. Případné požadavky KKO je tedy nutno řešit už při přidělování rolí WEB uživatelům v SAP.

Návrh řešení OE

Pro přihlášení do aplikace OE bude zavedeno SSO dle možností integrace do systému oprávnění a uživatelů v OE.

Vzhledem ke komplexnímu nastavování přístupových práv, které aplikace OE vyžaduje, předpokládáme, že autorizace uživatelů nadále zůstává na úrovni aplikace OE.

Šifrování databáze a komunikace uživatelů

Požadavky MV: návrh řešení pro šifrování komunikace na informace přenášené v síti. Zvláště pak na identifikační a autentizační informace a informace které by mohly být využity pro získání přístupu ke koncovému systému.

Dále je požadováno zpracování samostatného návrhu, kde jsou data zašifrována ještě před samotným přenosem.

Je požadováno prověřit možnost nasazení produktu SAP Single Sign-On k zajištění některých ze zmíněných bodů.

Návrh řešení EKIS WEB

Aktuálně je zapnuto šifrování na TCPIP portech (pro komunikaci mezi Domino servery a s Notes uživateli protokolem Notes RPC).

Pro přístup web uživatelů se vynucuje HTTPS (tedy šifrování). Konfiguraci upravíme tak, aby se uživatelé se staršími prohlížeči, tedy s podporou jen slabšího šifrování, k serveru vůbec nepřipojili.

Návrh řešení OE

V současné době není šifrován přenos dat mezi klientským prohlížečem a centrálním serverem. Bude provedeno zapnutí zabezpečeného protokolu SSL a jeho vynucení pro veškerou komunikaci mezi koncovým uživatelem a serverem.

V případě zajištění licence SQL Serveru Enterprise je možné na jeho straně zapnutí šifrování celé databáze tak, že nebude nutné provést žádné změny v programovém kódu aplikace. Bude pouze provedena příslušná rekonfiguraci na straně SQL Serveru.

Část 1d – Roll-out oprávnění

Oprávnění - roll-out nového konceptu oprávnění a eliminace rizik v oprávněních na útvarech v resortu MV

Nový autorizační koncept a role připravené v rámci první etapy budou rolloutovány na útvary resrotu MV. Útvarům bude po nasazení nových rolí poskytnuta zvýšená podpora. Budou navržena řešení rizk v oprávněních skupin uživatelů vycházejících ze systemizovaných pozic pracovníků PČR, HZS a centrálních útvarů.

Seznam oblastí:

- EP Role pro HZS - systemizace rolí HZS, rollout na útvary, výjezdy, předvedení
- EP Role na centrální a specializované útvary - dtto
- Zvýšená podpora útvarů během první fáze produktivního provozu, zapracování návrhů a požadavků z produktivního provozu
- HR Role - revize HR rolí, očištění od nepoužívaných transakcí, dílčí úpravy
- Rozvoj GRC - uživatelsky definovaný reporting pro vyhodnocování rizik pro účely správců rizik, úpravy modelu rizik v GRC
- Řešení rizik odpovídající systemizovaným skupinám uživatelům (odstranění těchto rizik nelze požadovat po útvarech), součástí bude cílový koncept pro úpravy systému.
- Analýza rizik Operativní evidence a EKISWeb, vzhledem k povaze aplikací se předpokládá pouze popis a zhodnocení.

Část 1e – Opatření proti výpadku a ztrátě dat EKIS MV

Jedná se o implementaci opatření pro zvýšení odolnosti a zabezpečení systému EKIS MV proti výpadku a ztrátě dat. Popis jednotlivých opatření:

Změna konfigurace VPN

Jedná se o změnu poskytovatele VPN přístupu do prostředí EKIS MV, z vlastního FW ASA, pro který je databáze uživatelů držena v AD umístěném v serveru Afaria, na službu CMS.

Popis činností:

- Export uživatelů z AD
- Konfigurace VPN (sítě do kterých má být VPN směřována)
- Zadání MV požadavku na službu VPN (vzdáleného přístupu) skrze CMS2 s podklady získaných z přípravy

Úprava konfigurace sítě

Jedná se o úpravu nastavení FW prostupů na úrovni L3 mezi VLAN DMZ a zálohovací VLAN pro korektní funkci OneTouch Recovery.

Popis činností:

- Příprava požadavků na prostupy (Odkud – Kam – porty)
- Zadání požadavku na provoz síťové části EKIS MV

Zvýšení odolnosti Media Agent Serverů (MAS)

Jedná se o dokoupení interních řadičů, disků a upgrade CPU Media Agent Serverů. V rámci tohoto kroku se instalují interní disky do serverů, provede se upgrade CPU a provede instalace MAS serverů na lokální uložiště.

Popis činností:

- Příprava postupu upgrade serverů
- Nákup potřebného HW
- Instalace nového HW do serverů MAS
- Instalace MAS serverů na lokální uložiště
- Konfigurace serverů a otestování funkčnosti

Zvýšení odolnosti centrálního serveru zálohovacího systému

Jedná se o nákup 2ks RACK serveru a migraci řídícího serveru z prostředí virtualizace s umístěním VM na produkčním diskovém poli do vlastní HW/storage.

Popis činností:

- Příprava postupu instalace a migrace centrálního zálohovacího serveru a jeho HA.
- Nákup potřebného HW.

- Instalace nového HW do prostředí EKIS MV.
- Instalace centrálního zálohovacího serveru a konfigurace HA.
- Migrace DB z virtualizace do nových serverů.
- Testování funkčnosti a HA.

Zvýšení výkonu zálohovacího systému

Jedná se o navýšení IOPS výkonu zálohovacího diskového pole. V rámci kroku dojde k nákupu třetí diskové police, nákupu HDD a zálohovacích pásek.

Popis činností:

- Příprava postupu instalace nového HW a rekonfigurace diskového pole
- Nákup potřebného HW
- Instalace nové police a HDD
- Rekonfigurace zálohovacího diskového pole
- Rekonfigurace zálohovacího systému na nové prostory
- Testování funkčnosti

Zvýšení rebuild priority

Jedná o změnu konfigurace v primárním diskovém poli v nastavení rebuild priority RAID skupin z nízké za střední.

Popis činností:

- Provedení konfigurační změny

Rozdělení na více Tier Poolů

Jedná se o úpravu rozložení Tier Poolů v diskovém poli z 1 poolu/druh disků na 2 pooly/druh disků. Z tohoto důvodu dojde k výměně a doplnění části disků v primárním diskovém poli a dále rekonfiguraci pole. Tento bod je přímo závislý na novém diskovém poli, které bude využito pro dočasné přemístění dat.

Popis činností:

- Příprava konfigurace
- Nákup potřebného HW
- Plná záloha celého prostředí EKIS MV
- Migrace dat na nové diskové pole
- Instalace nových HDD
- Rekonfigurace diskového pole
- Migrace dat z nového diskového pole

Storage Cluster“ – druhé diskové pole + rozšíření záruky pro stávající

Jedná se o nákup druhého diskového pole v minimálně stejné konfiguraci jako je stávající, doplnění stávajícího diskového pole o porty pro propojení s nových polem a licence na clusterovou funkcionalitu. Dále pak dokoupení záruk na stávající diskové pole na plánovou dobu životnosti.

Disková pole budou propojena pomoci 8xFC 16G přímými linkami. Pole budou nakonfigurována v režimu active-active s možností úpravy na active-pasive (bude určeno na základě provozních a výkonnostních testů).

Popis činností:

- Příprava volného místa v raccích MV v DC
- Nákup potřebného HW
- Instalace do Racků MV, zahoření
- Konfigurace DA do finálního stavu
- Konfigurace SAN
- Migrace dat z původního pole
- Konfigurace clusteru
- Syntetické testy zátěže clusteru
- Testy dostupnosti clusteru

Položkový rozpis HW a SW

Implementace opatření proti výpadku a ztrátě dat	Popis	počet ks
doplnění RAID řadičů do MA	BX2560 PCH connection kit	2
	BX2560 PCIe x4	2
	PRAID CM400i	2
	PRAID EM400i BP	2
disky do MA	SSD SATA 6G 480GB Mixed-Use 2.5' H-P EP	4
CPU do MA	CPU XEON E5-2609 V3 1,9GHZ 85W	2
	Cooler kit for 2nd CPU	2
paměti do MA	8GB (1X8GB) 1RX4 DDR4-2133 R ECC	2
Rack server	12 core, 64GB, 2x480gb ssd + 2x2TB SAS, konfigurace R1, 4x1GB, OS Windows Server 2012r2 nebo novější	2
Rozšíření a doplnění backup pole	DX1/200 S3 Drive Encl 2.5" w 2x IO Mod.	1
	DX1/200S3 HD SAS 1.8TB 10k 2.5 AF x1	24
	DX1/200S3 HD SAS 1.8TB 10k 2.5 AF x1	5
	DX1/200S3 Value SSD 1.92TB DWPD1 3.5 x1	11
	TP 2y OS,9x5,NBD Rec	1
Rozšíření počtu zálohovacích pásek	LTO6, 20-pack	5
Doplnění primárního pole	DX5/600 S3 HD 2.5" 1.0TB 7.2krpm x1	9
	DX5/600 S3 HD 2.5" 1.2TB 10krpm x1	27

Storage cluster	Sekundární diskové pole	1
	Clusterová funkcionalita pro stávající diskové pole	1

HW a SW je pořizován dle s 2 letou podporou/zárukou.

Příloha č. 2 – Dílčí akceptační protokol

DÍLČÍ AKCEPTAČNÍ PROTOKOL Č. …

Poskytovatel	*Národní agentura pro komunikační a informační technologie, s.p.*
Objednatel	*Česká republika – Ministerstvo vnitra*
Smlouva	*Dílčí smlouva č. 20 k Rámcové smlouvě o poskytování služeb podpory provozu a rozvoje systémů EKIS MV a ISoSS*
Datum uzavření Dílčí smlouvy	*DD. MM. 2019*
Datum	*DD. MM. YYYY*

Předmět akceptace

Číslo	Popis	Akceptováno	Akceptováno s výhradou	Neakceptováno
01				

Výhrady

Číslo	Popis

Poskytovatel a Objednatel svým podpisem stvrzují předání a Akceptaci předmětu plnění dle výše specifikované Dílčí smlouvy.

V Praze dne

	Jméno	Podpis
Předal za Poskytovatele		
Akceptoval za Objednatele		

Součástí tohoto Dílčího akceptačního protokolu je položkový rozpočet Plnění dle uvedeného vzoru

HW/SW	Parametry	počet ks	Cena za ks bez DPH	Cena implementačních prací bez DPH	Cena celkem bez DPH	DPH	Cena celkem s DPH

Příloha č. 3 – Akceptační protokol konzultačních služeb

AKCEPTAČNÍ PROTOKOL KONZULTAČNÍCH SLUŽEB Č. …

Poskytovatel	*Národní agentura pro komunikační a informační technologie, s.p.*
Objednatel	*Česká republika – Ministerstvo vnitra*
Smlouva	*Dílčí smlouva č. 20 k Rámcové smlouvě o poskytování služeb podpory provozu a rozvoje systémů EKIS MV a ISoSS*
Datum uzavření Dílčí smlouvy	*DD. MM. 2019*
Datum	*DD. MM. YYYY*

Předmět akceptace

Číslo	Popis	Akceptováno	Akceptováno s výhradou	Neakceptováno
01				

Součástí akceptace je akceptace rozsahu konzultačních služeb a to následovně:

Role	Počet MD	Akceptováno	Akceptováno s výhradou	Neakceptováno
Konzultant SAP III				

Výhrady

Číslo	Popis

Poskytovatel a Objednatel svým podpisem stvrzují poskytnutí konzultačních služeb a to včetně rozsahu.

V Praze dne

	Jméno	Podpis
Předal za Poskytovatele		
Akceptoval za Objednatele		