**Požadavek na změnu (RfC)[[1]](#endnote-1) – Z25542**

**a – věcné zadání**

# Základní informace

|  |  |  |  |
| --- | --- | --- | --- |
| **ID ShP MZe**[[2]](#endnote-2)**:** | **2017\_0061\_20** | **ID PK MZe**[[3]](#endnote-3)**:** |  |

|  |  |
| --- | --- |
| **Název změny**[[4]](#endnote-4)**:** | **Upgrade SSO DEV, TEST a PRODUKCE** |
| **Datum předložení požadavku:** |   | **Požadované datum nasazení:** |   |

|  |  |  |  |
| --- | --- | --- | --- |
| **Kategorie změny**[[5]](#endnote-5)**:** | Normální [x]  Urgentní [x]  | **Priorita**[[6]](#endnote-6)**:** | Vysoká [x]  Střední [x]  Nízká [x]  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Oblas**t**:** | Aplikace [x]   | **Zkratka**[[7]](#endnote-7)**:**  |  | Verze:  | 6 |
| **Typ požadavku:**  | Legislativní [x]  Zlepšení [x]  Reklamace [x]  Bezpečnost [x]  |
| Infrastruktura [x]  | **Typ požadavku:** | Nová komponenta [x]  Upgrade [x]  Bezpečnost [x]  Zlepšení [x]  Obnova [x]  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Role** | **Jméno**  | **Organizace /útvar** | **Telefon** | **E-mail** |
|  |  |  |  |  |
| Žadatel: | xxx | xxx | xxx | xxx |
| Metodický / věcný garant: | xxx | xxx | xxx | xxx |
| Change koordinátor: | xxx | xxx | xxx | xxx |
| Poskytovatel / dodavatel: | xxx | xxx | xxx | xxx |

|  |  |  |  |
| --- | --- | --- | --- |
| **Smlouva č.**[[8]](#endnote-8)**:** | 470-2017-13330 | **KL:** | KL HR-001 |

# Stručný popis požadavku

## Popis požadavku

Upgrade stávajícího po stránce SW a HW nepodporovaného řešení centrálního SSO MZe na aktuální verze OS RedHat a ForgeRock Access Management (aktuálně provozovaný ForgeRock OpenAM byl nahrazen novým produktem) formou migrace na nové prostředí vybudované na nově pořízené servery HP ProLiant BL460 gen 9. Souběžně bude vybudováno nové develop prostředí ForgeRock Access Management, stávající develop prostředí OpenAM s integrací SharePoint 2013 MZe bude zachován.

## Odůvodnění požadované změny (legislativní změny, přínosy)

Stávající provozovaná verze OpenAM a OS Red-Hat 5 jsou již morálně zastaralé a ze strany výrobce nepodporované. Celá SSO infrastruktura je provozována na zastaralých serverech HP BL460Gen6 pořízených na konci roku 2009, které jsou již druhým rokem bez podpory ze strany výrobce a MZe udržuje jejich provoz do doby obnovy serverů pouze s využitím dílů ze shodného HW připraveného k vyřazení. Stávající verze OpenAM jsou od předešlého poskytovatele provozu INFRA nejednotné – na každém prostředí je instalována jiná verze OpenAM. Všechny na MZe aktuálně provozované verze jsou zastaralé, obsahují známe zranitelnosti a neobsahují ze strany MZe požadované funkcionality.

## Rizika nerealizace

V bodě 2.2 uvedený stav sebou nese vysoké provozní riziko možnosti výpadku služeb centrálního SSO MZe, s dopadem do všech aplikací a registrů MZe, které využívají SSO. Výpadkem, nebo kompromitací SSO bude ohroženo vykonávání agend úřadu, které může mít dopad do vyplácení dotací v rozsahu několika miliard Kč.

# Podrobný popis požadavku

## Popis současného stavu

OpenAM je provozován na nepodporované verzi OS RedHat5 a OpenAM verze 11.x a na morálně zastaralém a výrobcem nepodporovaném HW z roku 2009.

## Popis cílového stavu

* **Vybudování nového develop SSO prostředí Mze**
	+ Dojde k vybudování nového develop prostředí SSO na kterém dojde k otestování všech změn funkcionalit provedených v prostředí MZe, souběžně dojde k zátěžovému testování, aby se odladili parametry pro testovací a produkční prostředí
* **Upgrade testovacího SSO Mze**
	+ Bude provedena instalace a konfigurace nového ForgeRock Access Management prostředí pro test a následně dojde k odstavení původního prostředí a readresaci nového prostředí se souběžným přesměrováním agentů (rewrite proxy) a upgrade jejich verze. Detailní popis je uveden níže.
* **Upgrade produkčního SSO Mze**
	+ Bude provedena instalace a konfigurace nového ForgeRock Access Management prostředí pro test a následně dojde k odstavení původního prostředí a readresaci nového prostředí se souběžným přesměrováním agentů (rewrite proxy) a upgrade jejich verze. Detailní popis je uveden níže.
* **Postup vytvoření nového DEVELOP prostředí pro ForgeRock Access Management**

Vytvoření nového develop SSO serveru bude realizováno dle následujícího postupu:

* Příprava nového develop SSO serveru n2rhpvu9 na RedHat verze 7.4
	+ Konfigurace serveru
		- 2 x vCPU
		- 8 GB RAM
		- Disk dle standardu
		- VLAN - 172.17.166.0/24
		- IP adresa serveru: 172.17.166.39
	+ Instalace serveru z KickStart MZe
	+ Základní nastavení serveru přes Ansible
	+ Server bude odpovídat požadovaným změnám dle template OKB
	+ Instalace a konfigurace nejaktuálnější verze JAVA a TOMCAT dle doporučení výrobce SW
	+ Instalace a konfigurace ForgeRock Access Management verze 6.5
	+ Instalace a konfigurace reverzní proxy v DMZ1 (náhrada DAUI) - nginx
	+ Úprava vzhledu dle standardů MZe, testování a úprava autentizačních modulů
	+ Příprava WARu, který bude obsahovat všechny potřebné úpravy
	+ Testy výkonnosti a stability produktu ForgeRock Access Management
	+ Zavedení serveru do patchovací skupiny OS – Linux-G
	+ Zavedení serveru do patchovací skupiny APP –SSO
	+ Nastavení zálohování serveru
* **Postup upgrade testovacího SSO**

Upgrade testovacího SSO bude realizován dle následujícího postupu:

* Příprava nových SSO a SSO RP serverů
	+ Pozice nového SSO serveru n2rhpsu5 – bc11rack6sal1 – bay 14
		- Dočasná IP adresa serveru: 172.17.7.21
	+ Pozice nového SSO serveru n2rhpsu6 – bc12rack7sal2 – bay 14
		- Dočasná IP adresa serveru: 172.17.7.22
	+ Nový VM SSO RP server - n2rhpsu7 – 2 x vCPU, 4 GB RAM, 40 GB HDD
		- Dočasná IP adresa serveru: 172.16.216.137
	+ Nový VM SSO RP server - n2rhpsu8 – 2 x vCPU, 4 GB RAM, 40 GB HDD
		- Dočasná IP adresa serveru: 172.16.216.138
	+ Instalace serverů z KickStart MZe
	+ Základní nastavení serveru přes Ansible
	+ Server bude odpovídat požadovaným změnám dle template OKB
	+ Instalace a konfigurace nejaktuálnější verze JAVA a TOMCAT dle doporučení výrobce SW
	+ Instalace a konfigurace produktu ForgeRock Access Management verze 6.5
	+ Instalace a konfigurace reverzní proxy v DMZ1 (náhrada DAUI) – nginx
	+ Úprava vzhledu dle standardů MZe, testování a úprava autentizačních modulů
	+ Příprava WARu, který bude obsahovat všechny potřebné úpravy
	+ Testy výkonnosti a stability produktu ForgeRock Access Management
	+ Zavedení serveru do patchovací skupiny OS – HW-A, Linux-G
* Zavedení serveru do patchovací skupiny APP –SSOOdstávka (kompletní výpadek testu)
	+ Odstavení starých SSO a DAUI serverů
	+ Readresace nových serverů na původní IP adresy
	+ Kontrola celého prostředí
	+ Znovu zavedení všech SSO agentů
	+ Upgrade SSO agentů na poslední verzi
	+ Testy celého prostředí včetně funkcí externí autentizace
* Post implementační kroky
	+ Následně bude provedena instalace OMU agentů
	+ Instalace DataProtector agenta a obnovení zálohování aplikačních serverů
	+ Přejmenování nodů v F5 na nové názvy serverů, je nutné provést smazání celého node a znovu zavedením pod novým jménem
* **Postup upgrade produkčního SSO**

Upgrade produkčního SSO bude realizován dle následujícího postupu:

* Příprava nových SSO a SSO RP serverů
	+ Pozice nového SSO serveru n2rhpsu1 – bc11rack6sal1 – bay 12
		- Dočasná IP adresa serveru: 172.17.7.19
	+ Pozice nového SSO serveru n2rhpsu2 – bc12rack7sal2 – bay 12
		- Dočasná IP adresa serveru: 172.17.7.20
	+ Nový VM SSO RP server - n2rhpsu3 – 2 x vCPU, 4 GB RAM, 40 GB HDD
		- Dočasná IP adresa serveru: 172.16.216.179
	+ Nový VM SSO RP server - n2rhpsu4 – 2 x vCPU, 4 GB RAM, 40 GB HDD
		- Dočasná IP adresa serveru: 172.16.216.180
	+ Instalace serverů z KickStart MZe
	+ Základní nastavení serveru přes Ansible
	+ Server bude odpovídat požadovaným změnám dle template OKB
	+ Instalace a konfigurace nejaktuálnější verze JAVA a TOMCAT dle doporučení výrobce SW
	+ Instalace a konfigurace produktu ForgeRock Access Management verze 6.5
	+ Instalace a konfigurace reverzní proxy v DMZ1 (náhrada DAUI) – nginx
	+ Úprava vzhledu dle standardů MZe, testování a úprava autentizačních modulů
	+ Příprava WARu, který bude obsahovat všechny potřebné úpravy
	+ Testy výkonnosti a stability produktu ForgeRock Access Management
	+ Zavedení serveru do patchovací skupiny OS – HW-A, Linux-G
	+ Zavedení serveru do patchovací skupiny APP –skupina SSO
* Odstávka (kompletní výpadek produkce)
	+ Odstavení starých SSO a DAUI serverů
	+ Readresace nových serverů na původní IP adresy
	+ Kontrola celého prostředí
	+ Znovu zavedení všech SSO agentů
	+ Upgrade SSO agentů na poslední verzi
	+ Testy celého prostředí včetně funkcí externí autentizace
* Post implementační kroky
	+ Následně bude provedena instalace OMU agentů
	+ Instalace DataProtector agenta a obnovení zálohování aplikačních serverů
	+ Přejmenování nodů v F5 na nové názvy serverů, je nutné provést smazání celého node a znovu zavedením pod novým jménem

**Společné dočasné prostředí pro produkční a testovací prostředí SSO**

Pro potřeby přípravy a testování nového testovacího a produkčního prostředí SSO bude potřeba připravit dvě nové dočasné VIP s identickou konfigurací, jako mají produkční VIP pro SSO. Tyto VIP budou dočasné pouze po dobu instalace a testování nových prostředí TEST a PROD. Souběžně bude nutné vytvořit dočasné prostupy mezi DMZ1 a DMZ2 dle níže uvedené specifikace a souběžně bude nutné vypublikovat SSO RP servery z DMZ1 pod dočasnou IP do internetu.

Dle následujících VIP budou vytvořeny dočasné VIP pro testování PROD a TEST prostředí na dočasných IP.

Kontext DMZ2-P – vytvoření dočasné VIP dle konfigurace této VIP:



Kontext DMZ1-P – vytvoření dočasné VIP dle konfigurace této VIP:



Vytvoření prostupů /publikace (v rámci realizace budou doplněny potřebné IP VIP):

Internet -> dočasná iLOGIN VIP TCP 443

n2rhpsu3, 4, 7, 8 -> dočasná SSO VIP TCP 443

**Sběr a zobrazování logů**

V současné době jsou pro sběr a zobrazování logů používány na míru vyvinuté aplikace LogReader a LogViewer, se kterými se již v novém prostředí nepočítá. Logy se již nebudou ukládat do Oracle DB.

Aby bylo možné efektivně sbírat a zobrazovat logy bude na všech serverech nainstalován nástroj Filebeat, který bude textové logy přeposílat do Graylogu. Nástroj Graylog bude sloužit k zobrazování a analýze logů.

Nástroj Graylog poskytuje autentizaci a autorizaci pro práci s logy a umožňuje vytváření reportů (dostupné až ve verzi 3.0)

Autentizace: <http://docs.graylog.org/en/2.4/pages/users_and_roles/external_auth.html>

Autorizace: <http://docs.graylog.org/en/2.4/pages/users_and_roles/permission_system.html>

Reporty: <https://www.graylog.org/products/graylog-3-preview>

Přeposílání logů do SIEM bude možné pomocí Filebeat output pluginů (<https://www.elastic.co/guide/en/beats/filebeat/current/configuring-output.html>) nebo přímo prostřednictvím Graylogu (<https://marketplace.graylog.org/addons?tag=output>).

* 3 x Server pro ElasticSearch na RedHat verze 7.4
	+ Konfigurace per server
		- 2 x vCPU
		- 8 GB RAM
		- Disk 200GB
		- VLAN - 172.17.80.0/24
		- IP adresa serverů: 172.17.80.31, 32, 33
		- Názvy serverů: n2rhpvz2, 3, 4
	+ Instalace serveru z KickStart MZe
	+ Základní nastavení serveru přes Ansible
	+ Server bude odpovídat požadovaným změnám dle template OKB
	+ Instalace a konfigurace OS RedHat 7.4
	+ Zavedení serveru do patchovací skupiny OS - bude doplněno při realizaci
	+ Zavedení serveru do patchovací skupiny APP - bude doplněno při realizaci
	+ Nastavení zálohování serveru
* 1 x Server pro Graylog na RedHat verze 7.4
	+ Konfigurace serveru
		- 2 x vCPU
		- 8 GB RAM
		- Disk 50GB
		- VLAN - 172.17.80.0/24
		- IP adresa serverů: 172.17.80.30
		- Názvy serverů: n2rhpvz1
	+ Instalace serveru z KickStart MZe
	+ Základní nastavení serveru přes Ansible
	+ Server bude odpovídat požadovaným změnám dle template OKB
	+ Instalace a konfigurace OS RedHat 7.4
	+ Zavedení serveru do patchovací skupiny OS - bude doplněno při realizaci
	+ Zavedení serveru do patchovací skupiny APP - bude doplněno při realizaci
	+ Nastavení zálohování serveru

**Úklidové práce**

Po cca 14 dnech od ukončení migračních prací budou provedeny následující činnosti:

* Zastavení všech starých OpenAM a OpenAM DAUI serverů test a produkce
* Demontáž serverů a smazání dat na HDD
* Smazání serverů z OneView
* Smazání pozůstatků po dočasném prostředí
* Úprava a vyčištění starých zálohovacích jobů
* Odstranění serverů z monitoringu

Dokumentace

* Servisní účty
* Mapa komunikací
* Spouštění a zastavování
* Konfigurace produktu ForgeRock Access Management a změny v konfiguraci, její umístění
* Konfigurace a umístění konfigurace Agentů
* Seznam a umístění certifikátů
* Aktualizace CMDB
* Aktualizace plánu patchování
* Předání změněných WAR souborů včetně popisu
* Předání zdrojových souborů u custom pluginů včetně popisu
* Zálohování
* Provozní příručka obsahující popis nejběžnějších postupů na výměnu certifikátů, hesla k SSO a podobně.

# Dopady na IS MZe

## Dopady

(V případě předpokládaných či možných dopadů změny na agendu, aplikaci, data, infrastrukturu nebo na bezpečnost je třeba si vyžádat stanovisko relevantních specialistů, tedy věcného/metodického, provozního, bezpečnostního garanta, příp. architekta.)

Požadovaná změna má dopad do architektury celé aplikace, která bude po nasazení v souladu s trendy nasazování aplikací a zároveň dojde k povýšení celé infrastruktury na podporované verze OS a aplikačních komponent celého řešení.

## Požadavky na součinnost AgriBus

(Pokud existují požadavky na součinnost Agribus, uveďte specifikaci služby ve formě strukturovaného požadavku (request) a odpovědi (response) s vyznačenou změnou.)

Není požadována.

## Dotčené konfigurační položky[[9]](#endnote-9)

|  |  |  |
| --- | --- | --- |
| **ID** | **Název položky** | **Předpokládaný dopad** |
| 1 | n2rhps93 | Výměna HW |
| 2 | n2rhps94 | Výměna HW |
| 3 | n2rhpsa4 | Nahrazení za virtuální server |
| 4 | n2rhpsa5 | Nahrazení za virtuální server |
| 5 | n2rhpsa6 | Nahrazení za virtuální server |
| 6 | n2rhpsa7 | Nahrazení za virtuální server |
| 7 | N2RHPV91 | Nahrazení za nový virtuální server |
| 8 | N2RHPV92 | Nahrazení za nový virtuální server |
| 9 | n2rhpvy0 | Nahrazení za nový virtuální server |

## Rizika implementace změny

V rámci toho RfC připadají v úvahu dvě rizika:

* Plánovaná odstávka se díky komplikacím při upgrade protáhne mimo navržený čas
* Nebude umožněno odstavit testovací nebo produkční OpenAM z důvodu předtisků

## Požadavek na podporu provozu naimplementované změny

(Uveďte, zda zařadit změnu do stávající provozní smlouvy, konkrétní požadavky na požadované služby, SLA.)

V rámci nasazení změny na produkční a testovací prostředí je požadována součinnost infra a zvýšený dohled i druhý den po nasazení prostředí.

## Požadavek na úpravu dohledového nástroje

(Uveďte, zda a jakým způsobem je požadována úprava dohledových nástrojů.)

V rámci provedené změny bude potřeba upravit scénáře OS a aplikačních serverů.

# Požadavek na dokumentaci[[10]](#endnote-10)

|  |  |  |
| --- | --- | --- |
| **ID** | **Dokument** | **Formát výstupu** (ano/ne) |
| el. úložiště | papír | CD |
|  | Analýza navrhnutého řešení | NE |  |  |
|  | Dokumentace dle specifikace Závazná metodika návrhu a dokumentace architektury MZe[[11]](#endnote-11) | NE |  |  |
|  | Testovací scénář, protokol o otestování | ANO |  |  |
|  | Uživatelská příručka | NE |  |  |
|  | Systémová příručka | ANO |  |  |
|  | Bezpečnostní dokumentace | NE |  |  |
|  | Profylaktické činnosti | ANO |  |  |

# Akceptační kritéria

Plnění v rámci požadavku na změnu bude akceptováno, jestliže budou akceptovány dokumenty uvedené v tabulce výše v bodu 5 a provedeny činnosti dle bodu 3.

|  |  |  |  |
| --- | --- | --- | --- |
| **ID** | **Akceptační kritérium** | **Způsob verifikace** | **Akceptuje** |
|  | Upgrade DEV, Test a Prod prostředí | Testovací scénáře | xxx |
|  | Dokumentace | Aktualizovaná dokumentace  | xxx |
|  |  |  |  |

# Základní milníky

|  |  |
| --- | --- |
| **Milník** | **Termín** |
|  |  |
|  |  |

# Přílohy

1.

2.

# Podpisová doložka

|  |  |  |  |
| --- | --- | --- | --- |
| **Za resort MZe:** | **Jméno:** | **Datum:** | **Podpis:** |
| Metodický/Věcný garant | xxx |  |  |
| Change koordinátor: | xxx |  |  |

**B – nabídkA řešení k požadavku Z25542**

|  |  |  |  |
| --- | --- | --- | --- |
| **ID ShP MZe**: |  | **ID PK MZe**: |  |

ID pro komunikaci s dodavatelem: rfc\_infra\_2019\_NO018\_OpenSSO\_upgrade

# Návrh konceptu technického řešení

Viz část A body 2 a 3.

# Uživatelské a licenční zajištění pro Objednatele

V souladu s podmínkami smlouvy: 470-2017-13330

# Dopady do systémů MZe

(Pozn.: V popisu dopadů zohledněte strukturu informací uvedenou v části A - Věcné zadání v bodu 4.U dopadů dle bodu 4.1 uveďte, zda může mít změna dopad do agendy, aplikace, na data, na síťovou strukturu, na serverovou infrastrukturu, na bezpečnost.)

# Dopady do agendy, aplikace, na data, na serverovou infrastrukturu

# Dopady na bezpečnost

Návrh řešení musí být v souladu se všemi požadavky v aktuální verzi Směrnice systémové bezpečnosti MZe. Upřesnění požadavků směrnice ve vztahu k tomuto RfC:

|  |  |  |
| --- | --- | --- |
| **Č.** | **Oblast požadavku[[12]](#endnote-12)** | **Předpokládaný dopad a navrhované opatření/změny** |
|  | Řízení přístupu 3.1.1. – 3.1.6. |  |
|  | Dohledatelnost provedených změn v datech 3.1.7. |  |
|  | Centrální logování událostí v systému 3.1.7. |  |
|  | Šifrování 3.1.8., Certifikační autority a PKI 3.1.9. |  |
|  | Integrita – constraints, cizí klíče apod. 3.2. |  |
|  | Integrita – platnost dat 3.2. |  |
|  | Integrita - kontrola na vstupní data formulářů 3.2. |  |
|  | Ošetření výjimek běhu, chyby a hlášení 3.4.3. |  |
|  | Práce s pamětí 3.4.4. |  |
|  | Řízení - konfigurace změn 3.4.5. |  |
|  | Ochrana systému 3.4.7. |  |
|  | Testování systému 3.4.9. |  |
|  | Externí komunikace 3.4.11. |  |

# Dopady na síťovou infrastrukturu

 (Pozn.: V případě, že má změna dopady na síťovou infrastrukturu, doplňte tabulku v připojeném souboru - otevřete dvojklikem.)

# Ostatní dopady

(Pozn.: Pokud má požadavek dopady do dalších požadavků MZe, uveďte je v tomto bodu.)

# Požadavky na součinnost Objednatele a třetích stran

|  |  |
| --- | --- |
| **MZe / Třetí strana** | **Popis požadavku na součinnost** |
| MZe  | Testování SSO po provedení upgrade TEST a PROD prostředí |
| MZe | Součinnost při testování |
| MZe | Umožnění odstávek pro migraci prostředí – TEST a PROD |
| MZe | Součinnost při publikaci nového develop prostředí přes CMS2, vytvoření nových prostupů DMZ1-DMZ2 |

(Pozn.: K popisu požadavku uveďte etapu, kdy bude součinnost vyžadována.)

# Harmonogram plnění[[13]](#endnote-13)

|  |  |
| --- | --- |
| **Popis etapy** | **Termín** |
| Realizace RFC (T=datum objednávky) | T1= T + 8 měsíců |
| Akceptace | T2 = T1 + 1 týden |

# Pracnost a cenová nabídka navrhovaného řešení

včetně vymezení počtu člověkodnů nebo jejich částí, které na provedení poptávaného plnění budou spotřebovány

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Oblast / role**[[14]](#endnote-14) | **Popis** | **Pracnost v MD/MJ** | **v Kč bez DPH** | **v Kč s DPH** |
|  |  |  |  |  |
|  | Cenová nabídka v příloze č. 01 | 79,50 | 521 679,00 | 631 231,59 |
| **Celkem:** | 79,50 | 521 679,00 | 631 231,59 |

(Pozn.: MD – člověkoden, MJ – měrná jednotka, např. počet kusů)

# Přílohy

|  |  |  |
| --- | --- | --- |
| **ID** | **Název přílohy** | **Formát** **(CD, listinná forma)** |
| 01 | Cenová nabídka | Listinná forma |
|  |  |  |

# Podpisová doložka

|  |  |  |  |
| --- | --- | --- | --- |
| **Název Dodavatele / Poskytovatele** | **Jméno** **oprávněné osoby**[[15]](#endnote-15) | **Datum** | **Podpis** |
| O2 Czech Republic a.s. | xxx |  |  |

**C – Schválení realizace požadavku Z25542**

|  |  |  |  |
| --- | --- | --- | --- |
| **ID ShP MZe**: |  | **ID PK MZe**: |  |

# Specifikace plnění

Požadované plnění je specifikováno v části A a B tohoto RfC.

Dle části B bod **Chyba! Nenalezen zdroj odkazů.** jsou pro realizaci příslušných bezpečnostních opatření požadovány následující změny[[16]](#footnote-1):

|  |  |  |  |
| --- | --- | --- | --- |
| **Č.** | **Oblast požadavku** | **Realizovat****(ano** [x]  **/ ne** [x] **)** | **Upřesnění požadavku** |
|  | Řízení přístupu 3.1.1. – 3.1.6. | [x]  |  |
|  | Dohledatelnost provedených změn v datech 3.1.7. | [x]  |  |
|  | Centrální logování událostí v systému 3.1.7. | [x]  |  |
|  | Šifrování 3.1.8., Certifikační autority a PKI 3.1.9. | [x]  |  |
|  |  Integrita – constraints, cizí klíče apod. 3.2. | [x]  |  |
|  | Integrita – platnost dat 3.2. | [x]  |  |
|  | Integrita - kontrola na vstupní data formulářů 3.2. | [x]  |  |
|  | Ošetření výjimek běhu, chyby a hlášení 3.4.3. | [x]  |  |
|  | Práce s pamětí 3.4.4. | [x]  |  |
|  | Řízení - konfigurace změn 3.4.5. | [x]  |  |
|  | Ochrana systému 3.4.7. | [x]  |  |
|  | Testování systému 3.4.9. | [x]  |  |
|  | Externí komunikace 3.4.11. |  |  |

# Uživatelské a licenční zajištění pro Objednatele (je-li relevantní):

# Požadavek na součinnost

|  |  |  |
| --- | --- | --- |
| **Útvar / Dodavatel** | **Popis požadavku na součinnost** | **Odpovědná osoba** |
| MZe | Testování SSO po provedení upgrade TEST a PROD prostředí |  |
| MZe | Součinnost při testování |  |
| MZe | Umožnění odstávek pro migraci prostředí – TEST a PROD |  |
| MZe | Součinnost při publikaci nového develop prostředí přes CMS2, vytvoření nových prostupů DMZ1-DMZ2 |  |

# Harmonogram realizace[[17]](#endnote-16)

|  |  |
| --- | --- |
| **Popis etapy** | **Termín** |
| Realizace RFC (T=datum objednávky) | T1= T + 8 měsíců |
| Akceptace | T2 = T1 + 1 týden |

# Pracnost a cenová nabídka navrhovaného řešení

včetně vymezení počtu člověkodnů nebo jejich částí, které na provedení poptávaného plnění budou spotřebovány

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Oblast / role**[[18]](#endnote-17) | **Popis** | **Pracnost v MD/MJ** | **v Kč bez DPH:** | **v Kč s DPH:** |
|  |  |  |  |  |
|  |  | 79,50 | 521 679,00 | 631 231,59 |
| **Celkem:** | 79,50 | 521 679,00 | 631 231,59 |

(Pozn.: MD – člověkoden, MJ – měrná jednotka, např. počet kusů)

# Případné další obchodní podmínky[[19]](#endnote-18)

# Posouzení[[20]](#endnote-19)

|  |  |  |  |
| --- | --- | --- | --- |
| **Role** | **Jméno** | **Datum** | **Podpis/Mail[[21]](#endnote-20)** |
| Bezpečnostní garant | xxx |  |  |
| Provozní garant |  |  |  |
| Architekt |  |  |  |

# Schválení

|  |  |  |  |
| --- | --- | --- | --- |
| **Role** | **Jméno** | **Datum** | **Podpis** |
| Žadatel | xxx |  |  |
| Věcný/metodický garant | xxx |  |  |
| Change koordinátor | xxx |  |  |
| Oprávněná osoba dle smlouvy | xxx |  |  |

# Vysvětlivky

1. Formulář RfC je tvořen třemi částmi, A - Věcné zadání, B – Nabídka řešení, C - Potvrzení realizace požadavku. První část (Věcné zadání) je předložena poskytovateli/dodavateli jako pobídka k předložení nabídky řešení. Druhou část, tj. část B použije dodavatel řešení k vypracování nabídky, kterou předloží MZe. Třetí část (Potvrzení realizace požadavku) se po vyplnění přiloží k první a druhé části a předloží se ke schválení osobám uvedeným v části C RfC. Poskytovateli/dodavateli se poté vyplněný formulář RfC předkládá v příloze objednávky na realizaci změnového požadavku. Pouze tato podepsaná objednávka je pokynem pro dodavatele/poskytovatele k realizaci změny. [↑](#endnote-ref-1)
2. ID ShP MZe – pomocný identifikátor projektu k požadavku přidělený v projektovém portálu MZe [↑](#endnote-ref-2)
3. ID PK MZe – pomocný identifikátor požadavku přidělený v pomocné evidenci projektové kanceláře MZe [↑](#endnote-ref-3)
4. Předmět změny – stručná informace, název požadavku [↑](#endnote-ref-4)
5. Kategorie změny – kategorie urgentní se využije v naléhavých případech, kdy je třeba vyřešit nedostupnost zásadní funkcionality systému vzhledem ke zpracování agendy, pro jejíž podporu systém slouží. [↑](#endnote-ref-5)
6. Priorita – vyjadřuje důležitost zapracování požadavku z pohledu časového. Vyplní se v případě volby kategorie „Normální změna“. [↑](#endnote-ref-6)
7. Zkratka – zkratka aplikace (viz „kód služby“ v katalogu služeb) [↑](#endnote-ref-7)
8. Smlouva č. – uvede se, pokud existuje smlouva, v rámci níž se požadavky předkládají, totéž platí pro KL (katalogový list). [↑](#endnote-ref-8)
9. Vyplňte ve spolupráci s provozním garantem. [↑](#endnote-ref-9)
10. Vyplní Change koordinátor s Provozním garantem. Uvedený seznam dokumentace je pouze příkladem. [↑](#endnote-ref-10)
11. Rozsah požadované dokumentace uveďte pod tabulkou. [↑](#endnote-ref-11)
12. Jednotlivé oblasti – položky v tabulce korespondují s kapitolami Standardu systémové bezpečnosti. [↑](#endnote-ref-12)
13. Uvede se datum zahájení a ukončení realizace, příp. další etapy. [↑](#endnote-ref-13)
14. Role se vyplní pouze v relevantních případech, např. u požadavku na infrastrukturu. [↑](#endnote-ref-14)
15. Oprávněná osoba – smluvně určená osoba oprávněná k předkládání požadavku na předložení nabídky. [↑](#endnote-ref-15)
16. Potvrzení realizace příslušných opatření/změn vyznačí posuzovatel za Oddělení kybernetické bezpečnosti. [↑](#footnote-ref-1)
17. Uvede se datum zahájení a ukončení realizace, příp. další etapy. [↑](#endnote-ref-16)
18. Role se vyplní pouze v relevantních případech, např. u požadavku na infrastrukturu. [↑](#endnote-ref-17)
19. Změna smluvních podmínek - vyplní se v případě, že dohodnuté podmínky realizace požadavku se liší od smluvních. [↑](#endnote-ref-18)
20. RfC se zpravidla předkládá k posouzení Bezpečnostnímu garantovi, Provoznímu garantovi, Architektovi, a to podle předpokládaných dopadů změnového požadavku na bezpečnost, provoz, příp. architekturu. Change koordinátor rozhodne, od koho vyžádat posouzení dle konkrétního případu změnového požadavku. [↑](#endnote-ref-19)
21. Doplní se podpis nebo se uvede odkaz na mailovou zprávu, v které bylo posouzení doručeno. [↑](#endnote-ref-20)