**Požadavek na změnu (RfC) Z32950**

**a – věcné zadání**

# Základní informace

|  |  |
| --- | --- |
| **ID PK MZe**[[1]](#endnote-1)**:** | 005 |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Název změny**[[2]](#endnote-2)**:** | **Vybudování nového develop prostředí SSO včetně portálu a testy SAML** | | | |
| **Datum předložení požadavku:** | | 25.10.2021 | **Požadované datum nasazení:** | Klikněte sem a zadejte datum. |

|  |  |  |  |
| --- | --- | --- | --- |
| **Kategorie změny**[[3]](#endnote-3)**:** | Normální  Urgentní | **Priorita**[[4]](#endnote-4)**:** | Vysoká  Střední  Nízká |

|  |  |  |  |
| --- | --- | --- | --- |
| **Oblas**t**:** | Aplikace | **Zkratka**[[5]](#endnote-5)**:** |  |
| **Typ požadavku:** | Legislativní  Zlepšení  Bezpečnost |
| Infrastruktura | **Typ požadavku:** | Nová komponenta  Upgrade  Bezpečnost  Zlepšení  Obnova |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Role** | **Jméno** | **Organizace /útvar** | **Telefon** | **E-mail** |
|  |  |  |  |  |
| Žadatel: | Karel Štefl | **MZe** |  | karel.stefl@mze.cz |
| Metodický / věcný garant: | Ivo Jančík | **MZe** |  | Ivo.jancik@mze.cz |
| Change koordinátor: | Petra Honsová | **MZe** | 1019 | petra.honsova@mze.cz |
| Poskytovatel / dodavatel: | xxx | **O2 IT Services s.r.o.** | xxx | xxx |

|  |  |  |  |
| --- | --- | --- | --- |
| **Smlouva č.**[[6]](#endnote-6)**:** | 242-2021-11150 | **KL:** | HR-001 |

# Stručný popis a odůvodnění požadavku

## Popis požadavku

V rámci tohoto požadavku dojde vybudování nového develop prostředí AM SSO včetně vybudování develop portálu s OpenID Connect agentem. Na prostředí bude následně testována funkčnost SAML.

## Odůvodnění požadované změny (legislativní změny, přínosy)

Důvodem je vytvoření testovacího prostředí, které bude využíváno v rámci integrací celého prostředí MZe a jeho aplikací a služeb autentizací s protokolem SAML, který je zásadní technologií v ICT připravované VZ SAU. Prostředí pak bude využito na testy propojení IDP, SP a práci se SAML v rámci klíčových aplikací, SSO a dalšími organizacemi resortu. Příprava na návrh používání SAML v rámci Speciálních registrů a integrací s ÚKZÚZ.

## Rizika nerealizace

Neschopnost MZe a jejích dodavatelů integrace protokolu SAML.

# Podrobný popis požadavku

V rámci realizace budou využity některé komponenty a původní servery ze stávajícího develop prostředí SSO, které bylo využíváno pro SharePoint 2013, který se bude aktuálně mazat.

xxx

# Testování SAML2 – Develop SSO

V rámci realizace bude provedena konfigurace SAML2 na develop SSO, kdy SSO bude konfigurováno jako IdP a jako SeP bude napojen servery n2rhpvy1, který bude na separátním URL. Pro testy bude využit SAML post binding a server po přijetí dat zobrazí odbržená data na webové stránce server.

V rámci SAML2 tokenu bude zasláno UID a DN uživatele.

V rámci testování bude proveden i test zasílání SAML2 tokenu, pokud bude aplikace schována za URL portaldev.mze.cz např specifické URL /SAML/…..

# Dokumentace

V rámci realizace dojde k aktualizaci dokumentace.

* Adresní plán
* Seznam VIP
* CMDB – iTOP
* Dokumentace SSO
* Seznam backup úloh

# Dopady na IS MZe

(V případě předpokládaných či možných dopadů změny na infrastrukturu nebo na bezpečnost je třeba si vyžádat stanovisko relevantních specialistů, tj. provozního, bezpečnostního garanta, příp. architekta.).

Při každé jednotlivé změně bude změna řešena s relevantními specialisty

## Na provoz a infrastrukturu

Při každé jednotlivé změně bude změna řešena s relevantními specialisty

## Na bezpečnost

Při každé jednotlivé změně bude změna řešena s relevantními specialisty

## Na součinnost s dalšími systémy

Při každé jednotlivé změně bude změna řešena s relevantními specialisty

## Požadavky na součinnost AgriBus

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

Při každé jednotlivé změně bude změna řešena s relevantními specialisty

## Požadavek na podporu provozu naimplementované změny

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

Při každé jednotlivé změně bude změna řešena s relevantními specialisty

## Požadavek na úpravu dohledového nástroje

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

Při každé jednotlivé změně bude změna řešena s relevantními specialisty

# Požadavek na dokumentaci[[7]](#endnote-7)

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **ID** | **Dokument** | **Formát výstupu** (ano/ne) | | | **Garant[[8]](#endnote-8)** |
| el. úložiště | papír | CD |
|  | Analýza navrhnutého řešení |  |  |  |  |
|  | Dokumentace dle specifikace Závazná metodika návrhu a dokumentace architektury MZe[[9]](#endnote-9) | ANO |  |  |  |
|  | Testovací scénář, protokol o otestování |  |  |  |  |
|  | Uživatelská příručka |  |  |  | Věcný garant |
|  | Provozně technická dokumentace (systémová a bezpečnostní dokumentace) | ANO |  |  | OKB, OPPT[[10]](#endnote-10) |
|  | Zdrojový kód a měněné konfigurační soubory |  |  |  |  |
|  | Webové služby + konzumentské testy |  |  |  |  |
|  | Dohledové scénáře (úprava stávajících/nové scénáře)[[11]](#endnote-11) |  |  |  |  |

### V připojeném souboru je uveden rozsah vybrané technické dokumentace – otevřete dvojklikem: xxx

Dohledové scénáře jsou požadovány, pokud Dodavatel potvrdí dopad na dohledové scénáře/nástroj.

U dokumentů, které již existují, se má za to, že je požadována jejich aktualizace. Pokud se požaduje zpracování nového dokumentu namísto aktualizace stávajícího, uveďte toto explicitně za názvem daného dokumentu, např. „Uživatelská příručka – nový“.

Povozně-technická dokumentace bude zpracována dle vzorového dokumentu, který je připojen – otevřete dvojklikem: xxx

# Akceptační kritéria

Plnění v rámci požadavku na změnu bude akceptováno, jestliže budou akceptovány dokumenty uvedené v tabulce výše v bodu 5, budou předloženy podepsané protokoly o uživatelském testování a splněna případná další kritéria uvedená v tomto bodu.

|  |  |  |  |
| --- | --- | --- | --- |
| **ID** | **Akceptační kritérium** | **Způsob verifikace** | **Akceptuje** |
|  |  |  |  |

# Základní milníky

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

# Přílohy

1.

2.

# Podpisová doložka

|  |  |  |  |
| --- | --- | --- | --- |
| **Za resort MZe:** | **Jméno:** | **Datum:** | **Podpis:** |
| Metodický/Věcný garant | Ivo Jančík |  | Viz schválení |
| Change koordinátor: | Petra Honsová |  | Viz schválení |

**B – nabídkA řešení k požadavku Z32950**

|  |  |
| --- | --- |
| **ID PK MZe**[[12]](#endnote-12)**:** | 005 |

# Návrh konceptu technického řešení

Viz část A tohoto RfC, body 2 a 3

# Uživatelské a licenční zajištění pro Objednatele

V souladu s podmínkami smlouvy č. 242-2021-11150

# Dopady do systémů MZe

# Na provoz a infrastrukturu

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

# 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[[13]](#endnote-13)** | **Předpokládaný dopad a navrhované opatření/změny** |
|  | Řízení přístupu 3.1.1. – 3.1.6.[[14]](#footnote-1) | Bez dopadu |
|  | Dohledatelnost provedených změn v datech 3.1.7. | Bez dopadu |
|  | Centrální logování událostí v systému 3.1.7.[[15]](#footnote-2) | Bez dopadu |
|  | Šifrování 3.1.8., Certifikační autority a PKI 3.1.9. | Bez dopadu |
|  | Integrita – constraints, cizí klíče apod. 3.2. | Bez dopadu |
|  | Integrita – platnost dat 3.2. | Bez dopadu |
|  | Integrita - kontrola na vstupní data formulářů 3.2. | Bez dopadu |
|  | Ošetření výjimek běhu, chyby a hlášení 3.4.3. | Bez dopadu |
|  | Práce s pamětí 3.4.4. | Bez dopadu |
|  | Řízení - konfigurace změn 3.4.5.[[16]](#footnote-3) | Bez dopadu |
|  | Ochrana systému 3.4.7. | Bez dopadu |
|  | Testování systému 3.4.9. | Bez dopadu |
|  | Externí komunikace 3.4.11. | Bez dopadu |

# Na součinnost s dalšími systémy

# Na součinnost AgriBus

# Na dohledové nástroje/scénáře[[17]](#endnote-14)

# Ostatní dopady

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

# Požadavky na součinnost Objednatele a třetích stran

|  |  |
| --- | --- |
| **MZe / Třetí strana** | **Popis požadavku na součinnost** |
| MZe | Vytvoření prostupů na VTS, zavedení potřebných záznamů do SEC domény a požadavků na nastavení WhiteList proxy |
|  |  |

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

# Harmonogram plnění[[18]](#endnote-15)

|  |  |
| --- | --- |
| **Popis etapy** | **Termín** |
| Zahájení plnění | zveřejnění v registru smluv |
| Dokončení plnění | 12 týdnů od zveřejnění v registru smluv |

# Pracnost a cenová nabídka navrhovaného řešení

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

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Oblast / role**[[19]](#endnote-16) | **Popis** | **Pracnost v MD/MJ** | **v Kč bez DPH** | **v Kč s DPH** |
|  |  |  |  |  |
|  | Viz cenová nabídka v příloze č.01 | 25 | 192 375,00 | 232 773,75 |
| **Celkem:** | | 25 | 192 375,00 | 232 773,75 |

(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**[[20]](#endnote-17) | **Podpis** |
| **O2 IT Services s.r.o.** | xxx |  |

**C – Schválení realizace požadavku Z32950**

|  |  |
| --- | --- |
| **ID PK MZe**[[21]](#endnote-18)**:** | 005 |

# Specifikace plnění

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

Dle části B jsou pro realizaci příslušných bezpečnostních opatření požadovány následující změny[[22]](#footnote-4):

|  |  |  |  |
| --- | --- | --- | --- |
| **Č.** | **Oblast požadavku** | **Realizovat**  **(ano  / ne )** | **Upřesnění požadavku** |
|  | 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. |  |  |

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

# Požadavek na součinnost

|  |  |  |
| --- | --- | --- |
| **Útvar / Dodavatel** | **Popis požadavku na součinnost** | **Odpovědná osoba** |
| MZe | Vytvoření prostupů na VTS, zavedení potřebných záznamů do SEC domény a požadavků na nastavení WhiteList proxy |  |

(V případě, že má změnový požadavek dopad na napojení na SIEM, PIM nebo Management zranitelnosti dle bodu 1, uveďte také požadovanou součinnost Oddělení kybernetické bezpečnosti.)

# Harmonogram realizace[[23]](#endnote-19)

|  |  |
| --- | --- |
| **Popis etapy** | **Termín** |
| Zahájení plnění – zveřejnění v registru smluv |  |
| Dokončení plnění – 12 týdnů od zveřejnění v registru smluv |  |

# Pracnost a cenová nabídka navrhovaného řešení

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

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Oblast / role**[[24]](#endnote-20) | **Popis** | **Pracnost v MD/MJ** | **v Kč bez DPH:** | **v Kč s DPH:** |
|  |  |  |  |  |
|  |  | MD 25 | 192 375,00 | 232 773,75 |
| **Celkem:** | | MD 25 | 192 375,00 | 232 773,75 |

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

# Posouzení

Bezpečnostní garant, provozní garant a architekt potvrzují svým podpisem za oblast, kterou garantují, správnost specifikace plnění dle bodu 1 a její soulad s předpisy a standardy MZe a doporučují změnu k realizaci.

|  |  |  |  |
| --- | --- | --- | --- |
| **Role** | **Jméno** | **Datum** | **Podpis/Mail[[25]](#endnote-21)** |
| Bezpečnostní garant | Karel Štefl | | |
| Provozní garant |  |  |  |
| Architekt |  |  |  |

(Pozn.: 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.)

# Schválení

Svým podpisem potvrzuje požadavek na realizaci změny.

|  |  |  |  |
| --- | --- | --- | --- |
| **Role** | **Jméno** | **Datum** | **Podpis** |
| Change koordinátor | Petra Honsová |  |  |
| Věcný/Metodický garant | Ivo Jančík |  | |
| Žadatel | Ivo Jančík |
| Oprávněná osoba dle smlouvy | Ivo Jančík |

(Pozn.: Oprávněná osoba se uvede v případě, že je uvedena ve smlouvě.)

# Vysvětlivky

1. ID PK MZe – pomocný identifikátor požadavku přidělený v pomocné evidenci projektové kanceláře MZe [↑](#endnote-ref-1)
2. Předmět změny – stručná informace, název požadavku [↑](#endnote-ref-2)
3. 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-3)
4. Priorita – vyjadřuje důležitost zapracování požadavku. Vyplní se v případě volby kategorie „Normální změna“. [↑](#endnote-ref-4)
5. Zkratka – zkratka aplikace (viz „kód služby“ v katalogu služeb) [↑](#endnote-ref-5)
6. Smlouva č. – uvede se, pokud existuje smlouva, v rámci níž se požadavky předkládají, totéž platí pro KL (katalogový list). [↑](#endnote-ref-6)
7. Vyplní Change koordinátor. Uvedený seznam dokumentace je pouze příkladem. [↑](#endnote-ref-7)
8. Garant odpovídá za správnost a úplnost dodané dokumentace a zajišťuje její akceptaci. Např. Provozní dokumentaci posuzuje Oddělení kybernetické bezpečnosti (OKB) a Oddělení provozu a podpory technologíí (OPPT). [↑](#endnote-ref-8)
9. Rozsah požadované dokumentace uveďte do tabulky. [↑](#endnote-ref-9)
10. OKB – Oddělení kybernetické bezpečnosti, OPPT – Oddělení provozu a podpory technologií [↑](#endnote-ref-10)
11. Požadováno, pokud Dodavatel potvrdí dopad na dohledové scénáře/nástroje. [↑](#endnote-ref-11)
12. ID PK MZe – pomocný identifikátor požadavku přidělený v pomocné evidenci projektové kanceláře MZe [↑](#endnote-ref-12)
13. Jednotlivé oblasti – položky v tabulce korespondují s kapitolami Standardu systémové bezpečnosti. [↑](#endnote-ref-13)
14. Uveďte, zda vznikají servisní účty a budou řízené PIMem nebo v něm budou jen evidované. [↑](#footnote-ref-1)
15. Uveďte, zda a jakým způsobem se mění/vytváří napojení na SIEM. [↑](#footnote-ref-2)
16. Uveďte, zda má RfC vliv na napojení na Management zranitelností (Vulnerability scanner). [↑](#footnote-ref-3)
17. Pokud z vyhodnocení dopadů vyplyne potřeba upravit dohledové scénáře nebo zpracování nového scénáře, pak se má za to, že položka seznamu „Požadavek na dokumentaci“ v b. 5 části A RfC „Dohledové scénáře (úprava stávajících/nové scénáře)“ je vyžadována a bude součástí akceptačního řízení, nebude-li v části C RfC v bodu 1 „Specifikace plnění“ stanoveno jinak. [↑](#endnote-ref-14)
18. Uvede se datum zahájení a ukončení realizace, příp. další etapy. [↑](#endnote-ref-15)
19. Role se vyplní pouze v relevantních případech, např. u požadavku na infrastrukturu. [↑](#endnote-ref-16)
20. Oprávněná osoba – smluvně určená osoba oprávněná k předkládání požadavku na předložení nabídky. [↑](#endnote-ref-17)
21. ID PK MZe – pomocný identifikátor požadavku přidělený v pomocné evidenci projektové kanceláře MZe [↑](#endnote-ref-18)
22. Potvrzení realizace příslušných opatření/změn vyznačí posuzovatel za Oddělení kybernetické bezpečnosti. [↑](#footnote-ref-4)
23. Uvede se datum zahájení a ukončení realizace, příp. další etapy. [↑](#endnote-ref-19)
24. Role se vyplní pouze v relevantních případech, např. u požadavku na infrastrukturu. [↑](#endnote-ref-20)
25. Doplní se podpis nebo se uvede odkaz na mailovou zprávu, v které bylo posouzení doručeno. [↑](#endnote-ref-21)