MZE-70376/2022-12122



mzedms025125708

**Požadavek na změnu (RfC)[[1]](#endnote-1) – Z35466**

**a – věcné zadání**

# Základní informace

|  |  |
| --- | --- |
| **ID PK MZe**[[2]](#endnote-2)**:** | 14 |

|  |  |
| --- | --- |
| **Název změny**[[3]](#endnote-3)**:** | **Sjednocení ASM politik XML FW** |
| **Datum předložení požadavku:** | 28.11.2022 | **Požadované datum nasazení:** | 30.4.2023 |

|  |  |  |  |
| --- | --- | --- | --- |
| **Kategorie změny**[[4]](#endnote-4)**:** | Normální [x]  Urgentní [ ]  | **Priorita**[[5]](#endnote-5)**:** | Vysoká [ ]  Střední [ ]  Nízká [x]  |

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

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Role** | **Jméno**  | **Organizace /útvar** | **Telefon** | **E-mail** |
|  |  |  |  |  |
| Žadatel: | Karel Štefl | MZe/ 10023 | 221812659 | karel.stefl@mze.cz |
| Metodický garant: | Roman Smetana  | MZe/10023  | 221812491  | roman.smetana@mze.cz |
| Věcný garant: | Vladimír Velas | MZe/ 12121 | 221814502 | vladimir.velas@mze.cz |
| Koordinátor změny: | David Neužil | MZe/12122  | 221812012  | david.neuzil@mze.cz |
| Poskytovatel/Dodavatel: | Xxx | **GEM System****a.s.** | xxx | xxx |

|  |  |  |  |
| --- | --- | --- | --- |
| **Smlouva č.**[[8]](#endnote-8)**:** | *S2020-0081,DMS 1539-2020-11150* | **KL:** | HR-001 |

# Stručný popis a odůvodnění požadavku

## 2.1 Popis požadavku

Cílem tohoto požadavku je sjednocení bezpečnostních kontrol XML komunikace Agribus v rámci F5 BIG-IP. Filtrování XML komunikace nyní probíhá jak ve virtuálním kontextu XMLFW, tak historicky v jemu předřazených virtuálních kontextech TEST a PROD. Výsledkem realizace tohoto požadavku bude stav, kdy XML komunikace Agribus bude z hlediska bezpečnosti vyhodnocována pouze v instanci k tomu určené (tedy XMLFW).

## Odůvodnění požadované změny (změny právních předpisů, přínosy)

Toto opatření má za cíl zefektivnit správu bezpečnostních pravidel Agribus XML komunikace a zejména urychlit investigaci a řešení incidentů, kdy Agribus komunikace neproběhne z důvodu kolize s bezpečnostním pravidlem. Takové případy již následně budou vyšetřovány pouze na jedné instanci F5 BIG-IP.

## Rizika nerealizace

Pokud nebude změna realizována, bude zachován současný stav správy bezpečnostních pravidel na dvou (resp. třech instancích) dvěma různými subjekty. Z toho vyplývají následující rizika:

* Delší doba řešení provozních incidentů
* Vzájemná nekonzistence bezpečnostních pravidel

# Podrobný popis požadavku

Řešení požadavku proběhne v následujících krocích:

1. Detailní analýza pravidel na instancích TEST a PROD
2. Návrh sjednocení pravidel z instancí TEST a PROD s pravidly XML FW
3. Připomínkování analýzy a návrhu
4. Schválení analýzy a návrhu
5. Úprava testovacích scénářů
6. Realizace změn na XML FW pro testovací prostředí
7. Odstranění ASM pravidel pro Agribus z instance TEST
8. Otestování bezpečnostních pravidel
9. Testovací provoz a zvýšená podpora
10. Nasazení změny na XML FW pro produkční prostředí
11. Odstranění ASM pravidel pro Agribus z instance PROD
12. Zvýšená podpora po nasazení do produkčního provozu
13. Aktualizace související dokumentace

# 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.).

## 4.1 Na provoz a infrastrukturu

Negativní dopad na provoz není v případě bezchybné realizace očekáván. V rámci realizace nedojde k zpřísnění bezpečnostních pravidel, které by vedlo k výpadkům dosud fungující komunikace. Riziko chyb v nastavení s negativními důsledky do provozu bude minimalizováno jednak provedením detailní analýzy a také důsledným vyhodnocením testovacího provozu. Zbytkové riziko je ošetřeno zvýšenou podporou po nasazení do produkčního provozu, tak aby případné dopady byly řešeny neprodleně.

Po dokončení změny bude dopad na provoz pozitivní v tom smyslu, že kolize s bezpečnostními pravidly bude řešena rychleji. Předpokládáme dále z principu mírný pozitivní dopad do výkonnosti platformy (ASM pravidla budou vyhodnocována pouze jednou a nikoli duplicitně).

## Na bezpečnost

Cílem je provést tuto změnu bez dopadu na úroveň bezpečnosti. V rámci analýzy, testovacího provozu i zvýšené podpory produktivního provozu může dojít k dílčím optimalizacím pravidel XML FW, které mohou mít za následek zvýšení bezpečnosti či v odůvodněných případech např. udělení výjimky z některého pravidla.

## Na součinnost s dalšími systémy

Předpokládá se úzká součinnost správců a dodavatelů podpory všech F5 BIG-IP instancí (TEST, PROD, XMLFW). Dále může v průběhu řešení požadavku vzniknout požadavek na součinnost správců síťové infrastruktury (firewallů) a dotčených aplikací/služeb komunikujících přes platformu Agribus v rámci testovacího provozu a řešení zjištěných problémů.

## Požadavky na součinnost AgriBus

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

Součinnost Agribus bude zajištěna dodavatelem v rámci tohoto změnového požadavku.

## Požadavek na podporu provozu naimplementované změny

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

Bez dopadu.

## Požadavek na úpravu dohledového nástroje

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

Bez dopadu.

# Požadavek na dokumentaci[[9]](#endnote-9)

|  |  |  |  |
| --- | --- | --- | --- |
| **ID** | **Dokument** | **Formát výstupu** (ano/ne) | **Garant[[10]](#endnote-10)** |
| el. úložiště | papír | CD |
|  | Analýza navrhnutého řešení | ANO | NE | NE |  |
|  | Dokumentace dle specifikace Závazná metodika návrhu a dokumentace architektury MZe[[11]](#endnote-11) | NE | NE | NE |  |
|  | Testovací scénář, protokol o otestování | ANO | NE | NE |  |
|  | Uživatelská příručka | NE | NE | NE | Věcný garant |
|  | Provozně technická dokumentace (systémová a bezpečnostní dokumentace) | ANO | NE | NE | OKB, OPPT[[12]](#endnote-12) |
|  | Zdrojový kód a měněné konfigurační soubory | NE | NE | NE |  |
|  | Webové služby + konzumentské testy | NE | NE | NE |  |
|  | Dohledové scénáře (úprava stávajících/nové scénáře)[[13]](#endnote-13) | NE | NE | NE |  |

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

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“.

Provozně-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.

# Základní milníky

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

# Přílohy

1.

2.

# Podpisová doložka

|  |  |  |
| --- | --- | --- |
| **Za resort MZe:** | **Jméno:** | **Podpis:** |
| Metodický garant[[14]](#endnote-14) | Roman Smetana |  |
| Koordinátor změny: | David Neužil |  |

**B – nabídkA řešení k požadavku Z35466**

|  |  |
| --- | --- |
| **ID PK MZe**[[15]](#endnote-15)**:** | 14 |

# Návrh konceptu technického řešení

# Technické řešení bude dodavatelem realizováno v F5 BIG-IP kontextu XML FW. Detailní analýza a návrh bude vypracována na základě exportu ASM politik z F5 BIG-IP kontextů dodaných jejich správcem. Nastavení XML FW proběhne na základě Detailní analýzy a návrhu schválené zadavatelem.

# Technické řešení bude v souladu se zadáním popsaným v části A tohoto požadavku.

# Uživatelské a licenční zajištění pro Objednatele

Tento změnový požadavek nemá dopad na licenční zajištění dotčených systémů.

# 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.)

Viz část A

# 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[[16]](#endnote-16)** | **Předpokládaný dopad a navrhované opatření/změny** |
|  | Řízení přístupu 3.1.1. – 3.1.6.[[17]](#footnote-1) | Zajištění VPN přístupů pro dodavatele |
|  | Dohledatelnost provedených změn v datech 3.1.7. | **Ne** |
|  | Centrální logování událostí v systému 3.1.7.[[18]](#footnote-2) | **Ne** |
|  | Šifrování 3.1.8., Certifikační autority a PKI 3.1.9. | **Ne** |
|  | Integrita – constraints, cizí klíče apod. 3.2. | **Ne** |
|  | Integrita – platnost dat 3.2. | **Ne** |
|  | Integrita - kontrola na vstupní data formulářů 3.2. | **Ne** |
|  | Ošetření výjimek běhu, chyby a hlášení 3.4.3. | **Ne** |
|  | Práce s pamětí 3.4.4. | **Ne** |
|  | Řízení - konfigurace změn 3.4.5.[[19]](#footnote-3) | **Ne** |
|  | Ochrana systému 3.4.7. | **Ne** |
|  | Testování systému 3.4.9. | Testovací provoz vč. zvýšené podpory |
|  | Externí komunikace 3.4.11. | **Ne** |

# Na součinnost s dalšími systémy

Viz část A

# Na součinnost AgriBus

Viz část A

# Na dohledové nástroje/scénáře[[20]](#endnote-17)

Viz část A

# Ostatní dopady

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

Nejsou

# Požadavky na součinnost Objednatele a třetích stran

|  |  |
| --- | --- |
| **MZe / Třetí strana** | **Popis požadavku na součinnost** |
| MZe | Schválení analýzy a návrhuSchválení RTPAkceptace změnového požadavku |
| O2 | Připomínkování analýza a návrhuÚprava nastavení instancí TEST a PRODSoučinnost při řešení incidentů v testovacím provozuSoučinnost při řešení incidentů po nasazení do produkce |
| Ostatní zúčastněné strany (konzumenti, správci firewallů, poskytovatelé služeb apod.) | Součinnost při řešení incidentů v testovacím provozuSoučinnost při řešení incidentů po nasazení do produkce |

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

# Harmonogram plnění[[21]](#endnote-18)

Konkrétní termíny budou odvozeny od data zahájení prací (vystavení objednávky/zveřejnění v registru smluv)

|  |  |
| --- | --- |
| **Popis etapy** | **Termín** |
| Zahájení prací | 02.01.2023 |
| Detailní analýza a návrh | 27.01.2023 |
| Nasazení do testovacího prostředí | 10.02.2023  |
| Vyhodnocení testovacího provozu | 24.03.2023 |
| Nasazení do produkčního prostředí | 07.04.2023 |
| Ukončení zvýšené podpory | 21.04.2023 |
| Uzavření změnového požadavku (aktualizace dokumentace a akceptace) | 28.04.2023 |

Uvedený harmonogram je platný v případě, že Dodavatel obdrží objednávku do 31.12.2022. V případě pozdějšího data objednání si Dodavatel vyhrazuje právo na úpravu harmonogramu v závislosti na aktuálním vytížení kapacit daného realizačního týmu Dodavatele či stanovení priorit ze strany Objednatele.

# Pracnost a cenová nabídka navrhovaného řešení

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

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Oblast / role**[[22]](#endnote-19) | **Popis** | **Pracnost v MD/MJ** | **v Kč bez DPH** | **v Kč s DPH** |
|  |  |  |  |  |
| Projektový manažer | Vedení projektu | 8 |  50 400,00 Kč  |  60 984,00 Kč  |
| Analytik | Analýza, dokumentace | 8 |  50 400,00 Kč  |  60 984,00 Kč  |
| Specialista F5 | Implementace | 14 |  88 200,00 Kč  |  106 722,00 Kč  |
| Architekt | Architektura řešení | 5 |  31 500,00 Kč  |  38 115,00 Kč  |
| QA | Testování, kontrola kvality | 5 |  31 500,00 Kč  |  38 115,00 Kč  |
| **Celkem:** | 40 |  252 000,00 Kč  |  304 920,00 Kč  |

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

Případné další informace.

# Přílohy

|  |  |  |
| --- | --- | --- |
| **ID** | **Název přílohy** | **Formát** **(CD, listinná forma)** |
|  |  |  |
|  |  |  |

# Podpisová doložka

|  |  |  |
| --- | --- | --- |
| **Název Dodavatele** | **Jméno** **oprávněné osoby**[[23]](#endnote-20) | **Podpis** |
| GEM System a.s. | xxx |  |

**C – Schválení realizace požadavku Z35466**

|  |  |
| --- | --- |
| **ID PK MZe**[[24]](#endnote-21)**:** | 14 |

# Specifikace plnění

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

Dle části B bod 3.2 jsou pro realizaci příslušných bezpečnostních opatření požadovány následující změny[[25]](#footnote-4):

|  |  |  |  |
| --- | --- | --- | --- |
| **Č.** | **Oblast požadavku** | **Realizovat****(ano** [x]  **/ 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** |
|  |  |  |
|  |  |  |

(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[[26]](#endnote-22)

|  |  |
| --- | --- |
| **Popis etapy** | **Termín** |
| Zahájení plnění | Zveřejněním v registru smluv |
|  |  |
| Dokončení plnění | 28.4.2023 |

# Pracnost a cenová nabídka navrhovaného řešení

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

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Oblast / role**[[27]](#endnote-23) | **Popis** | **Pracnost v MD/MJ** | **v Kč bez DPH:** | **v Kč s DPH:** |
|  |  |  |  |  |
|  |  | 40 |  252 000,00 Kč  |  304 920,00 Kč  |
| **Celkem:** | 40 |  252 000,00 Kč  |  304 920,00 Kč  |

(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** | **Podpis/Mail[[28]](#endnote-24)** |
| Bezpečnostní garant | Roman Smetana |  |
| Provozní garant | Ivo Jančík |  |
| 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. Koordinátor změny rozhodne, od koho vyžádat posouzení dle konkrétního případu změnového požadavku.)

# Schválení

Svým podpisem potvrzuje požadavek na realizaci změny:

|  |  |  |
| --- | --- | --- |
| **Role** | **Jméno** | **Podpis** |
| Žadatel | Karel Štefl |  |
| Metodický garant | Roman Smetana |  |
| Koordinátor změny | David Neužil |  |
| Oprávněná osoba dle smlouvy/Věcný garant | Vladimír Velas |  |

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

# 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 PK MZe – pomocný identifikátor požadavku přidělený v pomocné evidenci projektové kanceláře MZe [↑](#endnote-ref-2)
3. Předmět změny – stručná informace, název požadavku [↑](#endnote-ref-3)
4. 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-4)
5. Priorita – vyjadřuje důležitost zapracování požadavku. Vyplní se v případě volby kategorie „Normální změna“. [↑](#endnote-ref-5)
6. Zkratka – zkratka aplikace (viz „kód služby“ v katalogu služeb) [↑](#endnote-ref-6)
7. Typem požadavku „legislativní“ je myšlen požadavek, který vyplývá ze změny právního předpisu, příp. z nového právního předpisu. [↑](#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. Vyplní Koordinátor změny. Uvedený seznam dokumentace je pouze příkladem. [↑](#endnote-ref-9)
10. 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-10)
11. Rozsah požadované dokumentace uveďte do tabulky. [↑](#endnote-ref-11)
12. OKB – Oddělení kybernetické bezpečnosti, OPPT – Oddělení provozu a podpory technologií [↑](#endnote-ref-12)
13. Požadováno, pokud Dodavatel potvrdí dopad na dohledové scénáře/nástroje. [↑](#endnote-ref-13)
14. Pokud není určen metodický garant, podepíše věcné zadání věcný garant. [↑](#endnote-ref-14)
15. ID PK MZe – pomocný identifikátor požadavku přidělený v pomocné evidenci projektové kanceláře MZe [↑](#endnote-ref-15)
16. Jednotlivé oblasti – položky v tabulce korespondují s kapitolami Standardu systémové bezpečnosti. [↑](#endnote-ref-16)
17. Uveďte, zda vznikají servisní účty a budou řízené PIMem nebo v něm budou jen evidované. [↑](#footnote-ref-1)
18. Uveďte, zda a jakým způsobem se mění/vytváří napojení na SIEM. [↑](#footnote-ref-2)
19. Uveďte, zda má RfC vliv na napojení na Management zranitelností (Vulnerability scanner). [↑](#footnote-ref-3)
20. 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-17)
21. Uvede se datum zahájení a ukončení realizace, příp. další etapy. [↑](#endnote-ref-18)
22. Role se vyplní pouze v relevantních případech, např. u požadavku na infrastrukturu. [↑](#endnote-ref-19)
23. Oprávněná osoba – smluvně určená osoba oprávněná k předkládání požadavku na předložení nabídky. [↑](#endnote-ref-20)
24. ID PK MZe – pomocný identifikátor požadavku přidělený v pomocné evidenci projektové kanceláře MZe [↑](#endnote-ref-21)
25. Potvrzení realizace příslušných opatření/změn vyznačí posuzovatel za Oddělení kybernetické bezpečnosti. [↑](#footnote-ref-4)
26. Uvede se datum zahájení a ukončení realizace, příp. další etapy. [↑](#endnote-ref-22)
27. Role se vyplní pouze v relevantních případech, např. u požadavku na infrastrukturu. [↑](#endnote-ref-23)
28. Doplní se podpis nebo se uvede odkaz na mailovou zprávu, v které bylo posouzení doručeno. [↑](#endnote-ref-24)