**Požadavek na změnu (RfC)[[1]](#endnote-1) – Z33256**

**a – věcné zadání**

# Základní informace

|  |  |
| --- | --- |
| **ID PK MZe**[[2]](#endnote-2)**:** | 007 |

|  |  |
| --- | --- |
| **Název změny**[[3]](#endnote-3)**:** | **Šifrování** |
| **Datum předložení požadavku:** | 1.10.2021 | **Požadované datum nasazení:** | 31.7.2022 |

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

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

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Role** | **Jméno**  | **Organizace /útvar** | **Telefon** | **E-mail** |
|  |  |  |  |  |
| Žadatel: | Vladimír Velas | 11150 | 221814588 | vladimir.velas@mze.cz |
| Metodický garant / věcný garant: | Lucie KubáčováOleg Blaško | 1114511150 | 221813032221812777 | lucie.kubacova@mze.czoleg.blasko@mze.cz  |
| PM: | Nikol Janušová | 11151 | 221812777 | nikol.janusova@mze.cz |
| Technický garant: | xxx | MZE | xxx | xxx |
| Poskytovatel / dodavatel: | xxx | T-SOFT a.s. | xxx | xxx |

|  |  |  |  |
| --- | --- | --- | --- |
| **Smlouva č.**[[8]](#endnote-8)**:** | S2021-0013, DMS: 224-2021-11150 | **KL:** | HR-001 |

# Stručný popis a odůvodnění požadavku

## Popis požadavku

## Je požadována úprava spočívající v zavedení šifrování v souladu s požadavky 2.6 a 7.1.22 NSESSS a s požadavky Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů) (dále jen „nařízení GDPR“). Dle požadavku 10.1.5 NSESSS je dále požadováno dodání příslušné technické dokumentace. Šifrování je postup použití komplexní transformace digitální komponenty tak, aby jej aplikace nemohla znázornit ve srozumitelné podobě bez použití odpovídajícího dešifrovacího algoritmu.

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

Cílem úpravy je dosáhnout souladu s požadavky NSESSS a nařízením GDPR se zohledněním minimálních požadavků na kryptografické algoritmy viz metodický dokument NUKIBu -

https://www.nukib.cz/download/uredni\_deska/Kryptograficke\_prostredky\_doporuceni\_v1.0.pdf

## Rizika nerealizace

Nedodržení požadavků stanovených NSESSS a nařízením GDPR.

## Podrobný popis požadavku

Součástí implementace požadavku musí být dodavatelem vypracovaná analýza navrhnutého řešení, ve které budou níže popsané požadavky dodavatelem rozpracovány a MZe akceptovány. Součástí analýzy musí být i návrh životního cyklu šifrovacího certifikátu (sledování platnosti, způsob výměny apod.)

• eSSL v době příjmu dokumentu přijme a uloží informace o šifrování.

• eSSL umožňuje konfigurovat funkci dešifrování, jestliže je nějaký dokument určen pro přenos, export, import nebo příjem. Tuto vlastnost konfiguruje správcovská role.

• eSSL vždy odstraní šifrování při exportu entity do digitálního archivu.

• eSSL umožňuje, aby komponenty byly v aplikaci DMS šifrovány nebo zabezpečeny jinými prostředky k zamezení čtení nebo manipulace s nimi jinou osobou než oprávněným uživatelem a mimo eSSL.

• eSSL umožňuje konfigurovat workflow šifrovaného dokumentu správci dokumentu.

• eSSL v souladu s čl. 32 GDPR zajistí zabezpečení osobních údajů ukládaných v eSSL pomocí jejich šifrování.

• Jako součást dodávky je požadována technická dokumentace – systémová příručka k použitým metodám šifrování a dešifrování.

# 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.).

## Na provoz a infrastrukturu

## Na bezpečnost

## Na součinnost s dalšími systémy

## Požadavky na součinnost AgriBus

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

## Požadavek na podporu provozu naimplementované změny

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

## Požadavek na úpravu dohledového nástroje

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

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

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

### 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“.

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, budou předloženy podepsané protokoly o uživatelském testování a splněna případná další kritéria uvedená v tomto bodu.

# Základní milníky

|  |  |
| --- | --- |
| **Milník** | **Termín** |
|  |  |
| Nasazení na produkci | 31.7.2022 |

# Přílohy

1.

2.

# Podpisová doložka

|  |  |  |
| --- | --- | --- |
| **Za resort MZe:** | **Jméno:** | **Podpis:** |
| Metodický garant[[14]](#endnote-14) | Lucie KubáčováVz. Oleg Blaško |  |
| Koordinátor změny: | Nikol Janušová |  |

**B – nabídkA řešení k požadavku Z33256**

|  |  |
| --- | --- |
| **ID PK MZe**[[15]](#endnote-15)**:** | 007 |

# Návrh konceptu technického řešení

Dodavatel připraví úpravu DMS podle požadovaného zadání zadavatele v části A. Řešení bude reflektovat požadavky na šifrování popsaných v kapitolách 2.6 a 7.1.22 NSESSS a požadavky nařízení GDPR.

Podle požadavku v kapitole 10.1.5 NSESSS bude zadavateli poskytnuta dokumentace. Uživatelská část dokumentace bude součástí hlavního menu DMS v přehledu Dokumentace, technický popis bude předán zadavateli. Typový spis pro ukládání dokumentace požadovaný v kapitole 10 NSESSS, která specifikuje požadavky na dokumentaci, MZe využije, až když takový typový spis bude v rámci eSSL DMS zaveden.

Úprava bude dále zohledňovat požadavky na kryptografické algoritmy doporučené v metodickém dokumentu NUKIB dostupném na odkaze uvedeném v části A kapitole 2.2 tohoto dokumentu.

ESSL DMS bude přijímat povoleným způsobem zašifrované e-mailové dokumenty a umožní oprávněným uživatelům dokument vlastní i přijatý zašifrovat a pracovat s jeho obsahem.

xxx

# Uživatelské a licenční zajištění pro Objednatele

# Dopady do systémů MZe

## 3.1 Na provoz a infrastrukturu

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

#  3.2 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) |  |
|  | Dohledatelnost provedených změn v datech 3.1.7. |  |
|  | Centrální logování událostí v systému 3.1.7.[[18]](#footnote-2) |  |
|  | 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.[[19]](#footnote-3) |  |
|  | Ochrana systému 3.4.7. |  |
|  | Testování systému 3.4.9. |  |
|  | Externí komunikace 3.4.11. |  |

#  3.3 Na součinnost s dalšími systémy

#  3.4 Na součinnost AgriBus

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

#  3.6 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** |
|  |  |
|  |  |

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

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

|  |  |
| --- | --- |
| **Popis etapy** | **Termín** |
| Nasazení na testovací prostředí | 1.7.2022 |
| Nasazení na produkční prostředí / Akceptace | 31.07.2022 |

# 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** |
|  |  |  |  |  |
|  | Analýza a zadání řešení | 18 | 208 800 | 252 648 |
|  | Implementace vč.otestování, Nasazení, Dokumentace | 58 | 672 800 | 814 088 |
|  | Volné Ad-hoc MD pro dodatečné úpravy \* | 5 | 58 000 | 70 180 |
| **Celkem:** | **81** | **939 600** | **1 136 916** |  |

(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** |
| T-SOFT a.s. | xxx |  |

**C – Schválení realizace požadavku Z33256**

|  |  |
| --- | --- |
| **ID PK MZe**[[24]](#endnote-21)**:** | 07 |

# Specifikace plnění

Požadované plnění je specifikováno v části A i 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** |
| T-soft | Součástí implementace požadavku musí být dodavatelem vypracovaná analýza navrhnutého řešení |  |
|  |  |  |

(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** |
| Nasazení na testovací prostředí | 1.7.2022 |
| Nasazení na produkční prostředí / Akceptace | 31.07.2022 |

# 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:** |
|  |  |  |  |  |
|  | Analýza a zadání řešení | 18 | 208 800 |  |
|  | Implementace vč.otestování, Nasazení, Dokumentace | 58 | 672 800 |  |
|  | Volné Ad-hoc MD pro dodatečné úpravy \* | 5 | 58 000 |  |
| **Celkem:** | **81** | **939 600** | **1 136 916** |

(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 | Oldřich Štěpánek |  |
| 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 | Vladimír Velas |  |
| Věcný garant | Oleg Blaško |  |
| Koordinátor změny | Nikol Janušová |  |
| Oprávněná osoba dle smlouvy | 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)