MZE-55485/2022-12121



mzedms024432567

**Požadavek na změnu (RfC)[[1]](#endnote-1) – Z34958**

**a – věcné zadání**

# Základní informace

|  |  |
| --- | --- |
| **ID PK MZe**[[2]](#endnote-2)**:** | 04 |

|  |  |
| --- | --- |
| **Název změny**[[3]](#endnote-3)**:** | **Úprava aplikace CRVE v rámci projektu Migrace LDAPu** |
| **Datum předložení požadavku:** | 5.9.2022 | **Požadované datum nasazení:** | 30.9.2022 |

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

|  |  |  |  |
| --- | --- | --- | --- |
| **Oblas**t**:** | Aplikace [x]   | **Zkratka**[[6]](#endnote-6)**:**  | CRVE |
| **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: | Václav Krejčí | 12121 | 221 812 149 | vaclav.krejci@mze.cz  |
| Metodický garant: | Ivo Jančík | **12122** | 221 812 060 | Ivo.jancik@mze.cz |
| Garant IS: | Vladimír Velas | **12121** | 221 814 502 | vladimir.velas@mze.cz |
| Koordinátor změny: | Václav Krejčí | 12121 | 221 812 149 | vaclav.krejci@mze.cz  |
| Poskytovatel/Dodavatel: | xxx | **T-SOFT** | ----------------- | xxx |

|  |  |  |  |
| --- | --- | --- | --- |
| **Smlouva č.**[[8]](#endnote-8)**:** | S2019-0030, DMS: 273-2019-11150 | **KL:** | HR-001 |

# Stručný popis a odůvodnění požadavku

## Popis požadavku

Vzhledem k dlouhodobým problémům s výpadky nebo omezením LDAPu vlivem DB prostředí
a tím ovlivňování provozní dostupnosti aplikací MZe bylo rozhodnuto o změně řešení LDAP a jeho modernizaci. Tento projekt má za cíl odstranit závislosti centrálního LDAPu MZe na centrálním DB prostředí MZe, případně výrazné omezení těchto vlivů. V aktuálním řešení, pokud dojde k přetížení centrálního DB clusteru Oracle RAC Registry, dojde ke zpomalení a výpadkům na LDAPu MZe, který má uložen data na tomto clusteru, což má negativní dopad na výkon a dostupnost aplikace CRVE.

Současně dojde ke zvýšení výkonu a celkové dostupnosti celého LDAPu MZe prostřednictvím moderního distribuovaného řešení (nezávislé single servery s replikací na aplikační úrovni). Uvedená změna řešení LDAP bude mít dopad i do aplikace CRVE provozované a spravované v rámci smlouvy CRVE 2019+. V rámci ověření jejich funkčnosti se budou muset provést testy,
zda nové řešení neovlivní funkcionalitu a stabilitu této aplikace. V případě objevení chyb nebo nestabilit se budou provádět analytické práce, jejímž cílem bude nalezení problémů a návrhů řešení, programové úpravy a jejich implementace do systémů, včetně testů.

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

Přechod na plně šifrované ověřování mezi aplikacemi a LDAP systémem s šifrováním TLS 1.2
a vyšším.

## Rizika nerealizace

1. Nelze provést zrušení starého prostředí Oracle11, kde je umístěna databáze
pro stávající LDAP (databáze NLDAP).
2. Licenční ukončení provozu stávajícího prostředí k 31.12.2022.
3. Problémy s výkonností a nedostupností aplikace CRVE.

# Podrobný popis požadavku

Změna celého systému LDAP a přechod na LDAP v3 spolu s distribuovaným systémem vyžaduje zásahy do konfigurací, a především aplikačních kódů u všech aplikací.

Úpravy je nutné realizovat na všech prostředích s postupným testováním ve vztahu k novému LDAP prostředí. Dopad změny přechodem na jiné verze a celý nový koncept LDAPu vyžaduje rozsáhlejší změny uvnitř aplikací včetně otestování funkcionalit souvisejících se správou uživatelů (zakládání, přihlašování, mazání, editací vč. změny hesel atd.).

Během oslovení dodavatelů byla potvrzena základní struktura a postupy pro přechod na novou verzi pro všechny aplikace následovně:

* zásahy do zdrojových kódů všech aplikací,
* postupné nasazení nových verzí dle scénáře DEV/AKCEPT > TEST > PROD,
* změna konfiguračních souborů,
* aktualizace komponent a frameworků pro práci s LDAPv3,
* sjednocení komunikace dle RfC pouze na šifrované spojení LDAPS tcp 636 SSL/TLS,
* v některých případech pro ověření funkčnosti vytvoření/aktualizace testovacích scénářů.

Úpravy aplikací – viz níže v rozsahu, které zjistila analýza.

|  |  |  |  |
| --- | --- | --- | --- |
| **Název**  | **Aplikace** | **Prostředí** | **Popis aplikace** |
| **CRVE** | Registry | PRODTEST | Centrální evidence vodních toků |
| Očekávaný rozsah prací:* úprava kódu
* rekonfigurace aplikací
* postupné nasazení na všech prostředích a otestování
* otestování funkčnosti
 |

# 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

Realizace tohoto RFC váže na realizaci Infrastrukturního RFC s názvem: RFC\_INFRA\_II\_2022\_NO010\_vybudovani\_a\_migrace\_PROD\_TEST\_LDAP\_OUD\_cast\_2\_(Z33899), ve kterém jsou zachyceny veškeré změny v oblasti provozu a Infrastruktury.

## Na bezpečnost

Zvýšení bezpečnosti z důvodu přechodu na nové LDAP servery podporující šifrovací protokol TLS 1.2 a vyšší.

## Na součinnost s dalšími systémy

Ze strany MZe je nutné zajistit součinnost všech dodavatelů aplikací a systémů, které jsou integrovány na LDAP Mze.

## Požadavky na součinnost AgriBus

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

Zajištění migrace Portálu služeb na nový LDAP MZe

## Požadavek na podporu provozu naimplementované změny

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

V rozsahu stávající smlouvy.

## Požadavek na úpravu dohledového nástroje

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

Žádný.

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

|  |  |  |  |
| --- | --- | --- | --- |
| **ID** | **Dokument** | **Formát výstupu** (ano/ne) | **Garant[[10]](#endnote-10)** |
| el. úložiště | papír | CD |
|  | Analýza navrhnutého řešení | NE | 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 | ANO | 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, budou předloženy podepsané protokoly o uživatelském testování a splněna případná další kritéria uvedená v tomto bodu.

# Základní milníky

|  |  |
| --- | --- |
| **Milník** | **Termín** |
| Zahájení plnění | Datum uveřejnění v registru smluv |
| Ukončení plnění | 30.09.2022 |

# Přílohy

Žádné.

# Podpisová doložka

|  |  |  |
| --- | --- | --- |
| **Za resort MZe:** | **Jméno:** | **Podpis:** |
| Metodický garant[[14]](#endnote-14) | Ivo Jančík |  |
| Koordinátor změny: | Václav Krejčí |  |

**B – nabídkA řešení k požadavku Z34958**

|  |  |
| --- | --- |
| **ID PK MZe**[[15]](#endnote-15)**:** | 04 |

# Návrh konceptu technického řešení

Úprava bude realizována dle požadavků v kapitole 2 a 3 části A – Věcné zadání.

# Uživatelské a licenční zajištění pro Objednatele

Nejsou.

# 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.)

Nejsou.

# 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) | Bez dopadu. |
|  | Dohledatelnost provedených změn v datech 3.1.7. | Bez dopadu. |
|  | Centrální logování událostí v systému 3.1.7.[[18]](#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.[[19]](#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

Nejsou.

# Na součinnost AgriBus

Nejsou.

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

Nejsou.

# 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** |
| Realizace úpravy CRVE | 30.9.2022 |

# 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** |
|  |  |  |  |  |
|  | Realizace úpravy CRVE | 4 | 32.000 | 38.720 |
| **Celkem:** | **4** | **32.000** | **38.720** |

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

# 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 Z34958**

|  |  |
| --- | --- |
| **ID PK MZe**[[24]](#endnote-21)**:** | 04 |

# 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 | Datum uveřejnění objednávky v registru smluv |
| Dokončení plnění | 30.9.2022 |

# 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:** |
|  |  |  |  |  |
|  | Realizace úpravy CRVE | 4 | 32.000 | 38.720 |
| **Celkem:** | **4** | **32.000** | **38.720** |

(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 | Václav Krejčí |  |
| Garant IS | Vladimír Velas |  |
| Koordinátor změny | Václav Krejčí |  |
| 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)