MZE-49212/2022-12121



mzedms024101892

**Požadavek na změnu (RfC)[[1]](#endnote-1) – Z34549**

**a – věcné zadání**

# Základní informace

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

|  |  |
| --- | --- |
| **Název změny**[[3]](#endnote-3)**:** | **Logování posledního použití webových služeb do LDAP MZe** |
| **Datum předložení požadavku:** | 24.6.2022 | **Požadované datum nasazení:** | 31.10.2022 |

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

|  |  |  |  |
| --- | --- | --- | --- |
| **Oblas**t**:** | Aplikace [x]   | **Zkratka**[[6]](#endnote-6)**:**  | EPO |
| **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 | **11151** | 221 812 149 | vaclav.krejci@mze.cz |
| Metodický garant: | Ivo Jančík | **11152** | 221 812 060 | ivo.jancik@mze.cz |
| Věcný garant: | Vladimír Velas | **11151** | 221 814 502 | vladimir.velas@mze.cz |
| Koordinátor změny: | Václav Krejčí | **11151** | 221 812 149 | vaclav.krejci@mze.cz |
| Poskytovatel/Dodavatel: | xxx | **O2ITS** | xxx | xxx |

|  |  |  |  |
| --- | --- | --- | --- |
| **Smlouva č.**[[8]](#endnote-8)**:** | S2021-0007, DMS: 130-2021-11150 | **KL:** | HR - 001 |

# Stručný popis a odůvodnění požadavku

## Popis požadavku

Cílem požadavku je realizace mechanismu, který umožní v LDAPu MZe uchovávat informaci
o posledním použití autorizované webové služby. EPO server zajistí každodenní zápis timestamp údaje do atributu epowsLastLoginTime. Zápis bude pro všechny účty, které EPO server obsluhuje – tedy jak farmářské tak účty, které se využívají pro systém MS2014+.

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

Důvodem realizace úpravy je zajištění kompletního přehledu využití farmářských účtů,
kdy v současné době MZe loguje pouze přihlášení formou SSO a formou externí autentizace. Logování přihlášení volání autentizované webové služby MZe neloguje.

Tento nedostatek poté neumožňuje MZe mít přehled o neaktivních/spících farmářských účtech.
U ostatních účtů je poté možnost upravovat orclactiveenddate nikoliv podle posledního přihlášení přes SSO, ale i použitím webových služeb.

## Rizika nerealizace

V případě nerealizace úpravy nebude možné definovat se 100% jistotou účty, které jsou neaktivní/spící a MZe tak bude v nejistotě při správě těchto účtů.

# Podrobný popis požadavku

V kontextu nedávných požadavků SZIFu na zablokování některých účtů 99 a případné revize v automatickém blokování účtů 99 bude upraven systém EPO tak, že bude do LDAPu MZe zapisovat informaci o posledním použití účtu při volání EPO služeb.

V současné době obsahuje LDAP MZe informaci o:

* posledním přihlášení přes standardní přihlašovací stránku a použití LDAP bind příkazu,
* posledním přihlášením formou externí autentizace (tedy přihlášení z PF SZIF, přihlášení přes DS a přihlášení přes NIA).

Tyto údaje, které má MZe k dispozici, ale nepodchytí případ, kdy se účet používá pouze pro volání webových služeb na EPO. Pro přístup k webovým službám se používá WS klíč nebo kvalifikovaný certifikát a nepoužívá se přihlášením heslem ani formou externí autentizace. MZe tedy nemá relevantní údaj pro posouzení používání účtů.

V LDAP MZe je připraven nový atribut,

xxx

který bude možné modifikovat servisním účtem EPO.

EPO server bude provádět 1x denně aktualizaci tohoto atributu. Nebude tak probíhat zápis
při každém volání EPO serveru, ale pouze první volání za den bude otisknuto u atributu.

Cílem je omezit zátěž vůči LDAP serveru, který je primárně určen pro rychlé vyhledávání a pomalé zápisy.

Z pohledu účelu je přesnost na úrovni 24 hodin dostatečná.

EPO server primárně obslouží samotné volání a jako poslední událost v rámci volání bude realizován zápis do atributu 'epowsLastLoginTime'.

* Tento zápis proběhne pouze v případě úspěšné autentizace účtu (ws klíč nebo použití certifikátu).
* EPO server primárně obslouží samotné volání a jako poslední událost v rámci volání bude realizován zápis do atributu 'epowsLastLoginTime'..

## Dopady do aplikace SUR a LDAP farmáře

V rámci PZ se provede úprava aplikace LDAP farmáře tak, že v detailu účtu budou vidět informace o posledním přihlášení a to jak SSO, Externí autentizace tak WS.

xxx

Na detailu tak budou nové 3 údaje.

Obdobným způsobem bude upravena i aplikace SUR – tato úprava bude mimo smlouvu PRAIS.

# 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

Nový atribut v novém i starém LDAP serveru – již zařízeno.

## Na bezpečnost

Žádný – pouze zvýšení přesnosti v použití účtů.

## Na součinnost s dalšími systémy

Úprava aplikace SUR – mimo smlouvu PRAIS.

Úprava aplikace LDAP farmáře – v rámci PZ.

Úprava aplikace SURF a editace kontaktů – v budoucnu.

## Požadavky na součinnost AgriBus

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

ne

## 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.)

Ne.

# 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 | ANO | 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: 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** |
| Zahájení plnění | Uveřejnění v registru smluv |
| Ukončení plnění | 31.10.2022 |

# 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 Z34549**

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

# 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. 130-2021-11150

# Dopady do systémů MZe

# Na provoz a infrastrukturu

Nový atribut v novém i starém LDAP serveru – již zařízeno.

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

# 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

Úprava aplikace SUR – mimo smlouvu PRAIS.

Úprava aplikace LDAP farmáře – v rámci PZ.

Úprava aplikace SURF a editace kontaktů – v budoucnu.

# Na součinnost AgriBus

# Bez dopadu

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

Bez dopadu

# Ostatní dopady

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

Bez dopadu

# Požadavky na součinnost Objednatele a třetích stran

|  |  |
| --- | --- |
| **MZe / Třetí strana** | **Popis požadavku na součinnost** |
| MZe | Součinnost při realizaci a akceptaci PZ |

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

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

|  |  |
| --- | --- |
| **Popis etapy** | **Termín \*/** |
| Zahájení plnění | Uveřejnění v registru smluv |
| Ukončení plnění | 31.10.2022 |

\*/ Upozornění: Uvedený harmonogram je platný v případě, že Dodavatel obdrží objednávku do 01.08.2022. 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** |
|  |  |  |  |  |
|  | Viz cenová nabídka v příloze č. 01 | 11,75 | 104 575,00 | 126 535,75 |
| **Celkem:** | 11,75 | 104 575,00 | 126 535,75 |

(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** | **Jméno** **oprávněné osoby**[[23]](#endnote-20) | **Podpis** |
| O2 IT Services s.r.o. | xxx |  |

**C – Schválení realizace požadavku Z34549**

|  |  |
| --- | --- |
| **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** |
|  | Úprava aplikace SUR – mimo smlouvu PRAIS. | Koordinátor změny |
|  | Úprava aplikace LDAP farmáře – v rámci PZ. | Koordinátor změny |
|  | Úprava aplikace SURF a editace kontaktů – v budoucnu. | Koordinátor změny |

(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 | Uveřejnění v registru smluv |
| Dokončení plnění | 31.10.2022 |

# 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:** |
|  |  |  |  |  |
|  | Viz cenová nabídka v příloze č. 01 | 11,75 | 104 575,00 | 126 535,75 |
| **Celkem:** | 11,75 | 104 575,00 | 126 535,75 |

(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** | **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 |  |
| Věcný garant | 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)