**Požadavek na změnu (RfC)[[1]](#endnote-1) – Z28202**

**a – věcné zadání**

# Základní informace

|  |  |
| --- | --- |
| **ID PK MZe**[[2]](#endnote-2)**:** | 544 |

|  |  |
| --- | --- |
| **Název změny**[[3]](#endnote-3)**:** | **Integrace SSO EAGRI na identitní prostor systému Datových schránek** |
| **Datum předložení požadavku:** | 20.1.2020 | **Požadované datum nasazení:** | 30.4.2020 |

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

|  |  |  |  |
| --- | --- | --- | --- |
| **Oblas**t**:** | Aplikace [x]   | **Zkratka**[[6]](#endnote-6)**:**  | Portál eAGRI, SZR (editace kontaktů, LDAP farmář, SURF). |
| **Typ požadavku:**  | Legislativní [ ]  Zlepšení [x]  Bezpečnost [ ]  |
| Infrastruktura [ ]  | **Typ požadavku:** | Nová komponenta [x]  Upgrade [ ]  Bezpečnost [ ]  Zlepšení [x]  Obnova [ ]  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Role** | **Jméno**  | **Organizace /útvar** | **Telefon** | **E-mail** |
|  |  |  |  |  |
| Žadatel: | Oleg Blaško | **CPR** | 221814588 | oleg.blasko@mze.cz |
| Metodický / věcný garant: | Václav Koubek | **ICT** | 221812392 | vaclav.koubek@mze.cz |
| Change koordinátor: | Václav Krejčí | **ICT** | 221812149 | vaclav.krejci@mze.cz |
| Poskytovatel / dodavatel: | xxx | **O2ITS** | xxx | xxx |

|  |  |  |  |
| --- | --- | --- | --- |
| **Smlouva č.**[[7]](#endnote-7)**:** | S2019-0043; DMS 391-2019-11150 | **KL:** | KL HR-001 |

# Stručný popis a odůvodnění požadavku

## Popis požadavku

Předmětem požadavku je realizace pilotního PoC napojení identitního prostoru eAGRI/Mze(tj. výhradně farmářských účtů 99xxx) na identitní prostor systému Datových schránek (ISDS) – dále i ISDS\_BRIDGE. Jinými slovy, aby se na portále eAGRI mohl uživatel přihlásit svými autentizačními údaji ze systému ISDS (datovou schránkou). Systém ISDS je z hlediska autentizace důvěryhodný a vedle NIA (e-Občanky) pro resort Mze klíčový. Oproti systému NIA
je z pohledu použití v rámci resortu MZe efektivnější, protože klienty agendových systémů MZe jsou především právnické osoby. Toto PZ nebrání pozdější realizaci napojení autentizace MZe na NIA.

Z hlediska identitního prostoru eAGRI je třeba zdůraznit, že stávající řešení má nezměnitelné principy fungování:

* Pro každou kombinaci fyzické osoby jakožto uživatele a fyzické/právnické osoby jakožto subjektu, za který daný uživatel přistupuje, existuje právě jeden fyzický login. Jedna fyzická osoba tak může mít více loginů, pokud přistupuje za více právnických osob.
* Protože je takto dána vazba 1:1 mezi uživatelem a subjektem, za nějž se přihlašuje, mohou být i role do jednotlivých systémů přidělovány na úrovni loginu uživatele.
* Vazba uživatel x subjekt, za který je přihlášen, se přenáší do registrů za portálem
a i registry s tím takto pracují.

Oproti tomu identita z prostoru ISDS je vázána k fyzické osobě jako takové nebo se může jednat o osobu zastupující určitý subjekt (k jehož datové schránce se přihlašuje). Oproti tomu případná identita z prostoru NIA se jednoznačně váže k fyzické osobě, která vystupuje sama za sebe. K prokázání příslušnosti k právnické osobě je pak zapotřebí v případě NIA dotazů do Základních registrů, a to není předmětem stávajícího řešení. **S ohledem na tuto situaci se může účet z prostoru ISDS mapovat na jeden až N účtů doposud evidovaných v LDAP MZe,
tj. identitním prostoru eAGRI**. Je zjevné, že je třeba zajistit mapování a následnou volbu uživatele, v rámci níž si uživatel zvolí za jakou kombinaci uživatel x subjekt hodlá v příslušné session pracovat. **Tento krok znamená zásadní posun v práci s identitami v prostoru eAGRI
a současně zachovává zpětnou kompatibilitu s dosavadním řešením.** Uživatel nebude spravovat X hesel pro svých X účtů a může se přihlašovat pomocí autentizačních údajů datových schránek. **Tento krok přispěje ke zvýšení bezpečnosti portálu eAGRI.**

Současně je možné rozšířit funkcionalitu na portálu eAGRI tak, že pokud přistoupí autentizovaný uživatel z prostoru ISDS (později i NIA), který v prostoru eAGRI doposud není evidován, je možné mu bezprostředně vytvořit účet, který bude vázán buď na totožný subjekt anebo na subjekt, za který byl přihlášen v prostoru ISDS. Pro pozdější situaci přihlášení z NIA by pak byl vytvářen pouze účet fyzické osoby sama za sebe.

Z výše uvedeného plyne několik dílčích úloh, které je nezbytné vyřešit:

1. **Implementovat autentizační bránu vůči ISDS s příjmem údajů o autentizovaném uživateli.**
2. **Zajistit vhodnou formu logování komunikace s ISDS v souladu s pravidly bezpečnostní politiky MZe**
3. **Zajistit chování pro mezní (chybové) stavy při použití autentizační brány vůči ISDS – např. nevyhovující typ DS, nedostatek oprávnění pro DS nebo problém s autentizací/volání služby ISDS.**
4. **Implementovat mechanismus spárování externí identity s existujícími účty v LDAP MZe.**
	1. **volání systému ISZR/ROB,**
	2. **zpracování dat v SZR.**
5. **Zajistit poskytování informací o způsobu přihlášení pro agendový systém.**
6. **Na základě přihlášení z ISDS zajistit vytvoření nového účtu na straně identitního prostoru eAGRI.**
	1. **zakládání účtů do LDAPu MZe**
	2. **administrace účtů prostřednictvím aplikace SURF a Editace kontaktů včetně zohlednění změn v aplikaci LDAP farmáře.**
7. **Vytvoření modulu v rámci portálu eAGRI, která bude spravovat vazby mezi externí identitou a stávajícími účty 99xx a současně umožní uživateli si vybrat „podúčet“, pod kterým bude operovat v rámci příslušné session na portále eAGRI.**
8. **Vytvořit autentizační mechanismus pro externí autentizaci vůči SSO portálu eAGRI.**

Pro účely řešení budou vytvořeny v rámci portálu eAGRI/farmy portálových aplikací dva dílčí moduly:

* Body 1 až 5 bude zajišťovat nový modul ISDS\_BRIDGE**.**
* Body 6 až 8 bude zajišťovat nový modul SPRAVA\_IDENTIT\_FARMARU.

Dále je nutné pro pochopení řešení vysvětlit používané pojmy:

|  |  |
| --- | --- |
| Účet99 | Entita v LDAPu MZe ve větvi cn=farmar,cn=users,o=mze,c=cz.Tyto účty jsou zřizovány na základě vyplněné a doručené žádosti na MZe nebo SZIF. Účet je vždy párován na SZR – na SZRID dané osoby, jakožto přistupujícího uživatele. V SZR je poté vazba na ISZR (základní registry). Vazba u loginu je realizována přes SZRID na fyzickou osobu a subjekt, za který má účet v PF pracovat. **Prakticky tedy vždy obsahuje 2 SZRID**. Pokud fyzická osoba pracuje pod sebou (FO nebo FOP) tak je SZRID totožné.Existují určité historické případy, kdy v rámci hromadného importu dat do LDAPu, nebylo uvedeno SZRID osoby. Optimální by bylo, aby MZe tyto účty s uživateli napravilo, ale není to nezbytný předpoklad realizace PZDeaktivaci provádí MZe nebo SZIF (lze i na ÚKZÚZ). Deaktivaci si může provést i správce organizace (subjektu), pokud je subjekt v režimu manuální správy.Kontaktní údaje účtů 99 jsou sdíleny prostřednictvím SZR a každý 99 účet tak má stejné kontaktní údaje – email, telefon nebo mobilní číslo. Změna u jednoho účtu je tak zohledněna v LDAPu i u ostatních účtů 99 stejného subjektu. |
| Účet98 | Entita v LDAPu MZe ve větvi cn=farmar98,cn=users,o=mze,c=cz.Tyto účty zakládá ve vlastní režii subjekt, který si zvolil manuální správu uživatelských účtů. Není nutná fyzická návštěva SZIFu, MZe nebo ÚKZÚZ. Účet je vždy párován na SZRID subjektu **a nemá vyplněno SZRID konkrétní osoby.** Účty se automaticky po 18 měsících nepoužívání deaktivují. Tyto účty mají omezená práva, např. účet nemůže operovat na Portále SZIF. |
| Správce organizace | Jedná se vždy o účet začínající 99. Správce organizace může být automatický nebo manuálně nastavený (někdy se nazývá ADMIN organizace)Automatický správce organizace může být pouze u podnikající fyzické osoby, která má účet „sama na sebe“.Pokud je 99 účet zřízen podnikající fyzické osobě stává se tato automaticky správcem za organizaci. Za podnikající fyzickou osobu tak může být pouze 1 automatický správce organizace.Další správce organizace za podnikající fyzickou osobu nebo za právnickou osobu nastavuje regionální oddělení SZIFu nebo MZe. Zřízení správce organizace je na základě vyplněné a doručené žádosti.Tento správce organizace následně může: zakládat/měnit/rušit účty 98, omezovat přístupy pro 99 účty, nastavovat způsob přidělování rolí za organizaci. |

## Rizika nerealizace

Setrvání ve stávajícím režimu vnitřního ekosystému přístupových entit MZe. Tento ekosystém má vlastní pravidla pro zřizování přístupových účtů, ale jeho potenciál oproti informačnímu systému datových schránek je mnohem nižší. V systému datových schránek je uložen systém přihlašovacích údajů pro všechny jednatele právnických osob a určité procento i podnikatelů
a fyzických osob. Systém ISDS je i z pohledu správní řádu vedle NIA jediným, který lze považovat za vhodný pro podání dle správního řádu.

Zavedením přihlašování prostřednictvím datových schránek je možné plošně zavést plné elektronické podání, protože stávající zápisová forma v některých integrovaných systémech vyžaduje potvrzení prostřednictvím datové schránky nebo klasickou poštou. Zpřístupnění přihlašování přes datové schránky tak narovná určité rozpory ve využívání účtů 99 při používání portál eAGRI.

# Podrobný popis požadavku

Neveřejná část požadavku.

# 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.).

Neveřejná část požadavku.

# Požadavek na dokumentaci[[8]](#endnote-8)

|  |  |  |  |
| --- | --- | --- | --- |
| **ID** | **Dokument** | **Formát výstupu** (ano/ne) | **Garant[[9]](#endnote-9)** |
| el. úložiště | papír | CD |
|  | Analýza navrhnutého řešení | NE | NE | NE |  |
|  | Dokumentace dle specifikace Závazná metodika návrhu a dokumentace architektury MZe[[10]](#endnote-10) | ANO | NE | NE |  |
|  | Testovací scénář, protokol o otestování | ANO | NE | NE |  |
|  | Uživatelská příručka  | ANO | NE | NE | Věcný garant |
|  | Provozně technická dokumentace (systémová a bezpečnostní dokumentace) | ANO | NE | NE | OKB, OPPT[[11]](#endnote-11) |
|  | Zdrojový kód a měněné konfigurační soubory | ANO | NE | NE |  |
|  | Webové služby + konzumentské testy | ANO | ANO | NE |  |
|  | Dohledové scénáře (úprava stávajících/nové scénáře)[[12]](#endnote-12) | ANO | NE | NE |  |

# 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, zejména pak úspěšné penetrační testy.

# Základní milníky

|  |  |
| --- | --- |
| **Milník** | **Termín** |
| Nasazení na testovací prostředí | 15.4.2020 |
| Provedení penetračních testů | 10.5.2020 |
| Nasazení na provozní prostředí | 31.5.2020 |

# Přílohy

|  |  |
| --- | --- |
| **Číslo** | **Název přílohy** |
| 01 | Podrobná specifikace ws LDA\_PFL01A , LDA\_GFL01A a EAA\_GILD01A |

# Podpisová doložka

|  |  |  |  |
| --- | --- | --- | --- |
| **Za resort MZe:** | **Jméno:** | **Datum:** | **Podpis:** |
| Metodický/Věcný garant | Václav Koubek |  |  |
| Change koordinátor: | Václav Krejčí |  |  |

**B – nabídkA řešení k požadavku Z28202**

|  |  |
| --- | --- |
| **ID PK MZe**[[13]](#endnote-13)**:** | 544 |

# Návrh konceptu technického řešení

Viz část A tohoto PZ, body 2 a 3.

V kapitole projektové řízení jsou zakomponovány práce nesouvisející s programovými úpravami. Např. se jedná o konzultace s MZe, vytváření dokumentů pro MVČR, kontrola nastavení DS, spolupráce s tvorbou certifikátu apod. Také v této kapitole jsou práce související s konzultace vůči infra smlouvě.

Z kapitoly *dodatečné požadavky z testování* předpokládáme čerpání konzultací nebo změn, které vzniknou v rámci připomínek zástupců MZe nebo z infra smlouvy a MZe je nedefinovalo nebo definovalo nedostatečně v rámci zadání PZ.

# Uživatelské a licenční zajištění pro Objednatele

V souladu s podmínkami smlouvy č. 391-2019-11150

# 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[[14]](#endnote-14)** | **Předpokládaný dopad a navrhované opatření/změny** |
|  | Řízení přístupu 3.1.1. – 3.1.6.[[15]](#footnote-1) |  |
|  | Dohledatelnost provedených změn v datech 3.1.7. | Předpokládá se, že založení účtů do LDAPu novou službou bude logováno na ESB, kdy archivace služby bude 120 měsíců. Ve volání služby bude i info o loginu z DS. |
|  | Centrální logování událostí v systému 3.1.7.[[16]](#footnote-2) | Zavedení nového logování při zpracování dat z ISDS. Bude v DB eAGRIAPP. |
|  | Šifrování 3.1.8., Certifikační autority a PKI 3.1.9. | Použití certifikátů pro volání WS ISDS. Volání bude mimo ESB. |
|  | Integrita – constraints, cizí klíče apod. 3.2. | Bez dopadu |
|  | Integrita – platnost dat 3.2. | Bez dopadu |
|  | Integrita - kontrola na vstupní data formulářů 3.2. | Obvyklá v rámci html formulářů a kontrola na úrovni WSDL služeb. |
|  | Ošetření výjimek běhu, chyby a hlášení 3.4.3. | Stávající řešení v eAGRIAPP a SZR |
|  | Práce s pamětí 3.4.4. | Stávající řešení v eAGRIAPP a SZR |
|  | Řízení - konfigurace změn 3.4.5.[[17]](#footnote-3) | Bez dopadu |
|  | Ochrana systému 3.4.7. | Bez dopadu |
|  | Testování systému 3.4.9. | Bez dopadu |
|  | Externí komunikace 3.4.11. | **Nově Vůči ISDS** |

# Na součinnost s dalšími systémy

# Na součinnost AgriBus

Nová WS pro zápis farmářských účtů – autorizace pro eAGRIAPP.

# Na dohledové nástroje/scénáře[[18]](#endnote-15)

Ne

# 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 | Součinnost při testování a akceptaci PZ |
| MZe | Vystavení RSA klíče pro volání SSO a příslušná konfigurace SSO |
| MZe | Certifikát pro volání ISDS |
| MZe | Autorizace ke službám na AGRIBUS |

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

# Harmonogram plnění[[19]](#endnote-16)

|  |  |
| --- | --- |
| **Popis etapy** | **Termín \*/** |
| Zahájení | Datum objednávky |
| Nasazení za test | 31.08.2020 |
| Dokumentace - akceptace | 11.09.2020 |

\*/ Upozornění: Uvedený harmonogram je platný v případě, že Dodavatel obdrží objednávku v rozmezí 20.03.-31.03.2020. 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**[[20]](#endnote-17) | **Popis** | **Pracnost v MD/MJ** | **v Kč bez DPH** | **v Kč s DPH** |
|  |  |  |  |  |
|  | Viz cenová nabídka v příloze č. 02 | 97,88 |  871 087,50  | 1 054 015,88 |
| **Celkem:** | 97,88 |  871 087,50  | 1 054 015,88 |

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

# Přílohy

|  |  |  |
| --- | --- | --- |
| **ID** | **Název přílohy** | **Formát** (CD, listinná forma) |
| 02 | Cenová nabídka | Listinná forma |
| 03 | Detailní rozpad | Listinná forma |

# Podpisová doložka

|  |  |  |  |
| --- | --- | --- | --- |
| **Název Dodavatele / Poskytovatele** | **Jméno** **oprávněné osoby**[[21]](#endnote-18) | **Datum** | **Podpis** |
| O2 IT Services s.r.o. | xxx |  |  |

**C – Schválení realizace požadavku Z28202**

|  |  |
| --- | --- |
| **ID PK MZe**[[22]](#endnote-19)**:** | 544 |

# 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[[23]](#footnote-4):

|  |  |  |  |
| --- | --- | --- | --- |
| **Č.** | **Oblast požadavku** | **Realizovat****(ano** [x]  **/ ne** [ ] **)** | **Upřesnění požadavku** |
|  | Řízení přístupu 3.1.1. – 3.1.6. |[ ]  viz RfC část B bod 3.2. |
|  | Dohledatelnost provedených změn v datech 3.1.7. |[ ]  viz RfC část B bod 3.2. |
|  | Centrální logování událostí v systému 3.1.7. |[ ]  viz RfC část B bod 3.2. |
|  | Šifrování 3.1.8., Certifikační autority a PKI 3.1.9. |[ ]  viz RfC část B bod 3.2. |
|  |  Integrita – constraints, cizí klíče apod. 3.2. |[ ]  viz RfC část B bod 3.2. |
|  | Integrita – platnost dat 3.2. |[ ]  viz RfC část B bod 3.2. |
|  | Integrita - kontrola na vstupní data formulářů 3.2. |[ ]  viz RfC část B bod 3.2. |
|  | Ošetření výjimek běhu, chyby a hlášení 3.4.3. |[ ]  viz RfC část B bod 3.2. |
|  | Práce s pamětí 3.4.4. |[ ]  viz RfC část B bod 3.2. |
|  | Řízení - konfigurace změn 3.4.5. |[ ]  viz RfC část B bod 3.2. |
|  | Ochrana systému 3.4.7. |[ ]  viz RfC část B bod 3.2. |
|  | Testování systému 3.4.9. |[ ]  viz RfC část B bod 3.2. |
|  | Externí komunikace 3.4.11. |[ ]  viz RfC část B bod 3.2. |

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

# Požadavek na součinnost

|  |  |  |
| --- | --- | --- |
| **Útvar / Dodavatel** | **Popis požadavku na součinnost** | **Odpovědná osoba** |
| MZe | Součinnost při testování a akceptaci PZ | bude stanoveno |
| MZe | Vystavení RSA klíče pro volání SSO a příslušná konfigurace SSO | bude stanoveno |
| MZe | Certifikát pro volání ISDS | bude stanoveno |
| MZe | Autorizace ke službám na AGRIBUS | bude stanoveno |

(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[[24]](#endnote-20)

|  |  |
| --- | --- |
| **Popis etapy** | **Termín** |
| Zahájení | Datum objednávky |
| Nasazení za test | 31.08.2020 |
| Dokumentace - akceptace | 11.09.2020 |

# Pracnost a cenová nabídka navrhovaného řešení

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

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Oblast / role**[[25]](#endnote-21) | **Popis** | **Pracnost v MD/MJ** | **v Kč bez DPH:** | **v Kč s DPH:** |
|  |  |  |  |  |
|  | Viz cenová nabídka v příloze č. 02 | 97,88 |  871 087,50  | 1 054 015,88 |
| **Celkem:** | 97,88 |  871 087,50  | 1 054 015,88 |

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

# Posouzení

**Stanovisko/vyjádření OKB**

Zmiňované rozšíření z pohledu současného stavu vítáme, jedná se o funkcionalitu, která zcela jistě **zvýší úroveň bezpečnosti** a také **zlepší uživatelský komfort**.

Máme několik připomínek, které je vhodné brát v potaz.

* Funkcionalita rozšíření se významně protíná s novou funkcionalitou plánovaných projektů: SAU (federace identit), obsahující zejména „Registr identit a zmocnění“. Pokud budou projekty implementovány v jejich aktuálně plánovaném rozsahu, budou veškeré nasazené funkce v rámci tohoto PZ nahrazeny. Využití nově vyvinutých komponent v rámci této změny, nebo alespoň jejich částí, ve zmíněných plánovaných projektech je velmi nepravděpodobné. Důvodem je to, že změna je přímo integrovaná ve stávajícím prostředím (ForgeRock AM, LDAP, SSO eAgri) a využívá stávající principy (proprietární mezi-portálová integrace SSO, autentizace pomocí DN v hlavičce). Cílem nových projektů je však právě oproštění se od již zastaralých a nekoncepčních přímých integrací na stávající prostředí a implementace moderních univerzálních a bezpečných standardů pro autentizaci a federaci, jako je např. SAML2 a WS Federation, univerzální uložiště identit a přístupů v DB namísto v současném LDAP apod. **Současné prostředí a stávající principy fungování autentizace a federace byly identifikovány jako nevhodné a jsou také součástí několika stále otevřených bezpečnostních incidentů**, které ICT a OKB MZe musí vyřešit. Na základě vyjádření L. Hajnala, který zodpovídá za projekt SAU není realizace stávajícího PZ v rozporu s cíli projektu SAU. Realizace předmětného PZ je proof of concept nakládání s připojováním externích poskytovatelů identit.
* Komplexnost nových projektů bohužel znamená delší dobu na jejich přípravu a nasazení, proto může mít smysl navrhovanou změnu v PZ 544 implementovat, avšak s uvědoměním, že se jedná pouze o dočasné řešení a dojde k její plné náhradě. .
* Změna zasahuje do zásadní funkcionality autentizace, proto je nezbytné věnovat velkou pozornost nejen funkčním, ale také bezpečnostním/penetračním testům, a to před uvedením do produkce pro veřejnost!
* Dále prosím ICT o prověření „vhodnosti“ použití DS k autentizaci. Tento požadavek nepramení z toho, že by řešení či DS bylo špatné, ale z jednání na MV cca před rokem, kdy MV (OHA) vyslovilo myšlenku změny či zrušení této části funkčnosti DS (použití DS k autentizaci). Bylo by dobré alespoň ověřit, abychom nešli cestou, kterou již MV nepodporuje Dle telefonického vyjádření P. Kuchaře, ředitele OHA MV ČR s L. Hajnalem bude autentizační prvek ISDS využíván ještě nejméně v průběhu let 2021 a 2022; po uvedeném období bude nahrazován autentizačními rutinami NIA. Předmětné období plně pokrývá potřeby předkládaného PZ.

|  |  |  |  |
| --- | --- | --- | --- |
| **Role** | **Jméno** | **Datum** | **Podpis/Mail[[26]](#endnote-22)** |
| Bezpečnostní garant | Karel Štefl |  |  |
| Provozní garant | Pavel Štětina |  |  |
| 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

|  |  |  |  |
| --- | --- | --- | --- |
| **Role** | **Jméno** | **Datum** | **Podpis** |
| Oprávněná osoba dle smlouvy | Vladimír Velas |  |  |
| Žadatel | Oleg Blaško |  |  |
| Věcný/Metodický garant | Václav Koubek |  |  |
| Change koordinátor | Václav Krejčí |  |  |

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

**Příloha č. 01: specifikace LDA\_PFL01A**

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Typ** | **Výskyt** | **Popis** |
| **Request** |
|  | LOGIN | String | 1 – 1 | Login. Musí začínat na 99 nebo 98. |
|  | SZRID | Number | 1 – 1 | SZRID fyzické osoby, které login náleží. |
|  | SZRIDSUBJEKTU | Number | 1 - 1 | SZRID subjektu, za který login v ekosystému MZe působí. |
|  | MAIL | String | 1 - 1 | Emailová adresa. Více adres odděleny středníkem. |
|  | MOBIL | String | 1 - 1 | Mobilní telefon – z důvodů odesílání např. hesla. |
|  | ZALOZIT\_HESLO | Boolean | 1 – 1 | Informace zda má být založeno do LDAPu i heslo a zda má být odesláno přes SMS – pokud false tak se heslo nezakládá a neposílá. |

Ostatní údaje si služba dotáhne ze SZR:

Jméno, příjmení, město, ulice, rodné číslo, IČO, Identifikátory, číslo domu a uloží do LDAPu.

Manager se u účtu 99 neeviduje.

Odpověď je prázdná, pokud uložení projde.

**Specifikace LDA\_GFL01A**

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Typ** | **Výskyt** | **Popis** |
| **Request** |
|  | LOGIN | String | 0 – 1 | Login. Musí začínat na 99 nebo 98. |
|  | SZRID | Number | 0 – 1 | SZRID fyzické osoby, které login náleží. |
|  | SZRIDSUBJEKTU | Number | 0 - 1 | SZRID subjektu, za který login v ekosystému MZe působí. |
|  | **Typ** | **Výskyt** | **Popis** |
| **Response** |
|  | LOGIN\_LIST | Pole | 0 – N | Pole loginů |
|  |  | LOGIN | String | 1 – 1 | Login |
|  |  | SZRID | Number | 1 - 1 | SZRID fyzické osoby, které login náleží. |
|  |  | SZRIDSUBJEKTU | Number | 1 – 1 | SZRID subjektu. |
|  |  | ORLCISENABLED | Bool | 1 – 1 | False – účt není aktivní |
|  |  | BLOK\_DUVOD | String | 0 - 1 | Důvod zablokování – uložen v DB LDAPfarmare. |

**Specifikace EAA\_GILD01A**

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Typ** | **Výskyt** | **Popis** |
| **Request** |
|  | ISDS\_TOKEN\_COOKIES | String | 1 – 1 | Cookies ISDS\_TOKEN |
|  | OPENAM\_COOKIES | String | 1 – 1 | OPENAM cookies |
|  |  |  |  |  |
|  | **Typ** | **Výskyt** | **Popis** |
| **Response** |
|  | TIMESTAMP\_ISDS\_LOGIN |  | 1 – 1 | Timestamp přihlášení do ISDS |
|  | **dbID** |  |  | ID schránky (7 znaků). |
|  | **dbDescription** |  |  | Složený název schránky (PO a OVM –název firmy, FO –jméno, další jména a příjmení, PFO –jméno, další jména a příjmení + pomlčka + název subjektu) |
|  | **ic** |  |  | IČ subjektu (OVM, PO, PFO) |
|  | **firmName** |  |  | název subjektu (OVM, PO, PFO) |
|  | **biDate** |  |  | datum narození (FO, PFO) ve formátu YYYY-MM-DD |
|  | **fullUserName** |  |  | Kompletní složené jméno uživatele nebo nestrukturované jméno |
|  | **userType** |  |  | Typ uživatele podle číselníku. Pouze stav hodnoty S znamená Oprávněná osoba. |
|  | **userPrivils** |  |  | Informace o následujících právech uživatele (každé právo je reprezentováno jedním bitem): 0x1 Číst zprávy (kromě zpráv do vlastních rukou) 0x2 Číst zprávy –všechny 0x4 Posílat zprávy 0x8 Zobrazovat seznamy a dodejky 0x10 Vyhledávat schránky 0x20 Primární uživatel nebo administrátor 0x80 Mazat zprávy v trezoru |
|  | **SubjektSZRID** |  |  |  |
|  | **OsobaSZRID** |  |  |  |
|  | **LOGIN\_V\_PF** |  |  | Login použitý v PF |

Business chyby:

* token byl zneplatněn,
* token nebyl nalezen,

# 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. Smlouva č. – uvede se, pokud existuje smlouva, v rámci níž se požadavky předkládají, totéž platí pro KL (katalogový list). [↑](#endnote-ref-7)
8. Vyplní Change koordinátor. Uvedený seznam dokumentace je pouze příkladem. [↑](#endnote-ref-8)
9. 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-9)
10. Rozsah požadované dokumentace uveďte do tabulky. [↑](#endnote-ref-10)
11. OKB – Oddělení kybernetické bezpečnosti, OPPT – Oddělení provozu a podpory technologií [↑](#endnote-ref-11)
12. Požadováno, pokud Dodavatel potvrdí dopad na dohledové scénáře/nástroje. [↑](#endnote-ref-12)
13. ID PK MZe – pomocný identifikátor požadavku přidělený v pomocné evidenci projektové kanceláře MZe [↑](#endnote-ref-13)
14. Jednotlivé oblasti – položky v tabulce korespondují s kapitolami Standardu systémové bezpečnosti. [↑](#endnote-ref-14)
15. Uveďte, zda vznikají servisní účty a budou řízené PIMem nebo v něm budou jen evidované. [↑](#footnote-ref-1)
16. Uveďte, zda a jakým způsobem se mění/vytváří napojení na SIEM. [↑](#footnote-ref-2)
17. Uveďte, zda má RfC vliv na napojení na Management zranitelností (Vulnerability scanner). [↑](#footnote-ref-3)
18. 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-15)
19. Uvede se datum zahájení a ukončení realizace, příp. další etapy. [↑](#endnote-ref-16)
20. Role se vyplní pouze v relevantních případech, např. u požadavku na infrastrukturu. [↑](#endnote-ref-17)
21. Oprávněná osoba – smluvně určená osoba oprávněná k předkládání požadavku na předložení nabídky. [↑](#endnote-ref-18)
22. ID PK MZe – pomocný identifikátor požadavku přidělený v pomocné evidenci projektové kanceláře MZe [↑](#endnote-ref-19)
23. Potvrzení realizace příslušných opatření/změn vyznačí posuzovatel za Oddělení kybernetické bezpečnosti. [↑](#footnote-ref-4)
24. Uvede se datum zahájení a ukončení realizace, příp. další etapy. [↑](#endnote-ref-20)
25. Role se vyplní pouze v relevantních případech, např. u požadavku na infrastrukturu. [↑](#endnote-ref-21)
26. Doplní se podpis nebo se uvede odkaz na mailovou zprávu, v které bylo posouzení doručeno. [↑](#endnote-ref-22)