# Požadavek na změnu (RfC)[[1]](#endnote-2)

**a – věcné zadání**

# Základní informace

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **ID SD MZe**[[2]](#endnote-3)**:** | Z22651 | **ID ShP MZe**[[3]](#endnote-4)**:** | **2016\_0031\_191** | **ID PK MZe**[[4]](#endnote-5)**:** | **365** |

|  |  |
| --- | --- |
| **Název změny**[[5]](#endnote-6)**:** | **Analýza nasazení ochrany proti CSRF v LPIS** |
| **Datum předložení požadavku:** | 15.1.2018 | **Požadované datum nasazení:** | 31.3.2018 |

|  |  |  |  |
| --- | --- | --- | --- |
| **Kategorie změny**[[6]](#endnote-7)**:** | Normální [x]  Urgentní [ ]  | **Priorita**[[7]](#endnote-8)**:** | Vysoká [ ]  Střední [x]  Nízká [ ]  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Oblas**t**:** | Aplikace [x]   | **Kód**[[8]](#endnote-9)**:**  | LPIS | Verze:  |  |
| **Typ požadavku:**  | Legislativní [ ]  Zlepšení [ ]  Reklamace [ ]  Bezpečnost [x]  |
| Infrastruktura [x]  | **Typ požadavku:** | Nová komponenta [ ]  Upgrade [ ]  Bezpečnost [x]  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Role** | **Jméno**  | **Organizace /útvar** | **Telefon** | **E-mail** |
|  |  |  |  |  |
| Žadatel o změnu: | … | … | … | … |
| Metodický / věcný garant: | … | … | … | … |
| Change koordinátor: | … | … | … | … |
| Poskytovatel / dodavatel: | … | … | … | … |

|  |  |  |  |
| --- | --- | --- | --- |
| **Smlouva č.**[[9]](#endnote-10)**:** | 353-2015-13310 /1,2 (S2016-0118) | **KL:** | KL HR-001 |

# Stručný popis požadavku

Předmětem požadavku je primárně analyzovat možné způsoby ochrany aplikace LPIS proti zneužití Cross-site Request Forgery (dále také CSRF nebo XSRF). Tento typ útoku pracuje na bázi nezamýšleného požadavku realizovaného prostřednictvím a bez vědomí regulérního uživatele, vedeného z nelegitimního zdroje. Tímto způsobem je možné vložit, upravit, smazat nebo načíst neoprávněně data a tedy narušit atributy bezpečnosti jako je důvěrnost, dostupnost a integrita informací. Tento typ útoku spadá do položek bezpečnostního dokumentu OWASP 10, který je zaměřený na celosvětovou ochranu webových aplikací. Ochrana proti tomuto typu útoku vyžaduje detailní analýzu struktury, funkčních oblastí a technologií aplikace.

LPIS je z tohoto hlediska velice komplexní a heterogenní prostředí sestávající se z mnoha komponent, modulů a různých použitých technologií. Ty jsou navíc vyvíjeny v různých prostředích a jsou spravované různými subjekty a mají za sebou určitý historický technologický vývoj. Z předchozích zkušeností (viz PZ 193) se ukazuje, že problematika ochrany proti CSRF vyžaduje též hlubší a komplexnější přístup. Na tomto základě doporučuje OKB provést analýzu možnosti nasazení této ochrany, která by vymezila rozsah a typ opatření. Výstupem by mělo být přesné zadání pro implementaci ochrany proti CSRF.

## Popis požadavku

Je požadováno vytvořit dokument, který popisuje průběh a závěr analýzy, která odpoví na otázky zadavatele v oblasti implementace ochrany proti CSRF v širším pojetí aplikace LPIS. Analýza musí též obsahovat varianty možných řešení s popisem kladů a záporů s doporučením vhodné volby. Níže uvádíme seznam okruhů a otázek které je třeba v analýze zodpovědět:

1. Jaké způsoby realizace ochrany jsou technicky možné a vhodné pro aplikaci LPIS?
2. Je možné definovat části nebo moduly v LPISu, jejichž funkce směřují k možnosti vložit, upravit, smazat nebo načíst citlivá data a jsou potencionálně náchylné na CSRF? Typicky např. formuláře, administrativní funkce apod. Je možné pro každou takovou transakci v této části LPISU generovat CSRF token, který se posílá v transakci?
3. Je možné nasadit ochranu proti CSRF celoplošně[[10]](#footnote-2) v LPISu?
4. Jaké mohou být provozní dopady při využití tohoto LPIS celoplošného nasazení?
5. Je možné pro každou transakci v LPISu se generovat samostatný CSRF token, který bude součástí transakce? (zasílá se přímo v transakci?)
6. Je možné navrhnout a otestovat řešení ochrany proti CSRF jen v části aplikace a dále pak použít takový způsob pro nasazení u ostatních modulů?
7. Je možné realizovat pouze dílčí opatření, tedy pouze v jednotlivých vybraných částech LPISu?
8. Je možné exaktně definovat oblasti nasazení? Je možné definovat ověřitelný seznam míst, oblastí nebo modulů s nasazením ochrany? Bude možné ověřit účinnost nasazení, a jaký je doporučený postup?
9. Původní moduly na technologii ExsJS3/JBoss5 nemají ochranu proti CSRF, je možné ji zde zavést?
10. Mají nově zaváděné moduly ExsJS4/JBoss7 zavedenu ochranu proti CSRF ?
11. Jak bude vypadat proces nakládání s CSRF tokeny a jak bude modul/aplikace reagovat na jejich změnu, podvržení nebo neexistenci?
12. Mohou být CSRF tokeny obtížně predikovatelné (nepredikovatelné) a unikátní?
13. Může systém přerušit transakci a vizualizovat chybové stavy v případě narušení ochrany proti CSRF?
14. Bude se jednat spíše o jednorázové tokeny nebo tokeny s omezenou dobou platnosti? Jaká doba platnosti bude pro CSRF tokeny doporučena?
15. Bude možné vytvořit vhodné testovací scénáře pro ověření funkčnosti a akceptaci ochrany?
16. Jak bude implementováno opatření proti CSRF v budoucích modulech nebo zohledněno v budoucích úpravách LPISU?
17. Je možné pro výstupy analýzy použít doporučení v dokumentu OTGv4 (Testing for Cross Site Request Forgery,CSRF OTG-SESS-005)? Které doporučení budou aplikovány?

## Odůvodnění požadované změny (legislativní změny, přínosy)

Zadavatel plánuje použít tyto informace pro reálná opatření v aplikaci LPIS pro povýšení bezpečnosti a snížení rizika hrozby zneužití CSRF.

## Rizika nerealizace

Bez analýzy možností nasazení ochrany proti CSRF hrozí neúčinná nebo nevyhovující implementace ochrany, tak jak se ukázalo při realizaci PZ 193. Hrozí též ekonomická ztráta v podobě neúčelně vynaložených finančních prostředků. Pro ochranu této investice je nutné se detailně zaobírat touto problematikou.

# Podrobný popis požadavku

## Popis současného stavu

V současné době je dle znalostí zadavatele účinná a správně implementovaná ochrana proti CSRF pouze v modulu „Veřejný export dat LPIS“ na adrese http://eagri.cz/public/app/eagriapp/lpisdata/. V ostatních částech aplikace LPIS není tato problematika řešena nebo není známo, že by byla dostatečně ošetřena v jiných částech LPIS . Je tedy nutné v prvé řadě vyjasnit, zda znalosti zadavatele odpovídají skutečnému stavu. Požadovaná analýza vede k této skutečnosti. Pro určení rozsahu implementace přikládáme schéma, které v části červeně orámované plochy zahrnuje moduly a jejich typy, které společně tvoří LPIS chápaný jako VIS dle ZoKB viz poznámka pod čarou č.1.



 Tyto části LPISU musí být analyzovány a musí být podrobně zodpovězeny otázky zadavatele uvedené v kapitole 2.1. Analýza se musí zabývat minimálně rozsahem, způsobem, technickými detaily, možností otestování a ověřitelností, možným budoucím vývojem aplikace a dopady implementace ochrany v budoucnosti, a to pro každý jednotlivý modul nebo část LPISu dle struktury naznačené v dokumentu LPIS\_IS1v0.pdf. Pokud došlo v mezičase od vzniku tohoto dokumentu ke změnám ve struktuře LPISu, musí být tyto změny v dokumentu LPIS\_IS1v0.pdf nebo jeho ekvivalentní editovatelné verzi, vyznačeny nebo doplněny tak, aby schéma odpovídalo aktuální situaci struktury v LPISu. V úvahu se pro potřeby finální analýzy se musí brát v potaz předpokládatelný známý stav pro období, kdy bude analýza dokončena nebo kdy dojde k implementaci ochrany. Tím je myšleno, že moduly nebo části LPIS, které budou zrušeny v době realizace, není nutné analyzovat. Ty moduly nebo části LPIS o kterých má dodavatel znalost v době analýzy, že budou realizovány nebo i úpravy zásadního charakteru ve stávajících nebo nově vzniklých částech či modulech budou brány v potaz s ohledem na analýzu ochrany proti CSRF a musí být do ní tedy zahrnuty.

## Popis cílového stavu

Dodaná analýza bude obsahovat všechny požadované výstupy, tak aby se zadavatel mohl zodpovědně rozhodnout pro odpovídající formu realizace s ohledem na hospodárnost vynaložených prostředků. V tomto ohledu musí zodpovědět na otázky uvedené v kapitole 2.1.

## Dopady na IS MZe

### Technické aspekty implementace

### Dopady na agendu[[11]](#endnote-11) – ano [ ]  / ne [x]

### Dopady na aplikace – ano [ ]  / ne [x]

### Dopady na data – ano [ ]  / ne [x]

### Dopady na síťovou infrastrukturu – ano [ ]  / ne [x]

### Dopady na serverovou infrastrukturu[[12]](#endnote-12) – ano [ ]  / ne [x]

### Dopady na bezpečnost – ano [x]  / ne [ ]


### (Pozn.: V případě, že má změna dopady na síťovou infrastrukturu, doplňte tabulku (otevřete dvojklikem):

### Pokud má požadavek dopady do dalších požadavků MZe, uveďte je též v bodu 3.3.)

### Seznam měněných komponent nebo funkcionalit (vycházející z ArchiMate modelu architektury)[[13]](#endnote-13)

### Obecný návrh nové architektury v Sparx EA  projektu[[14]](#endnote-14)

### (Pozn.: Uveďte v případě implementace nových systémů, modulů, nebo funkcionalit a komunikace.)

### Dotčené konfigurační položky[[15]](#endnote-15)

|  |  |  |
| --- | --- | --- |
| **ID** | **Název položky** | **Předpokládaný dopad** |
|   |  |  |
|   |   |   |

## Rizika implementace změny

Žádná.

## Požadavek na podporu provozu naimplementované změny

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

# Požadavek na dokumentaci[[16]](#endnote-16)

|  |  |  |  |
| --- | --- | --- | --- |
| **ID** | **Název položky** | **Zpracovat**(ANO/NE) | **Formát výstupu** (elektronické úložiště / CD / listinná forma) |
|  | Analýza navrhnutého řešení | ANO | El. dokument |
|  | Dokumentace dle specifikace Závazná metodika návrhu a dokumentace architektury MZe[[17]](#endnote-17) | NE |  |
|  | Testovací scénář, protokol o otestování | NE |  |
|  | Uživatelská příručka | NE |  |
|  | Systémová příručka | NE |  |
|  | Bezpečnostní dokumentace | NE |  |

# Akceptační kritéria

Plnění v rámci požadavku na změnu bude akceptováno, jestliže budou akceptovány dokumenty uvedené v tabulce výše v bodu 4 a budou předloženy protokoly o uživatelském testování podepsané garantem, který je uveden ve sloupci Akceptuje.

|  |  |  |  |
| --- | --- | --- | --- |
| **ID** | **Akceptační kritérium** | **Způsob verifikace** | **Akceptuje** |
|  | Požadovaný obsah dokumentu. | Kontrola dokumentu | … |

**B – nabídkA řešení**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **ID SD MZe**[[18]](#endnote-18): | Z22651 | **ID ShP MZe**[[19]](#endnote-19): | **2016\_0031\_191** | **ID PK MZe**[[20]](#endnote-20): | **365** |

id pro komunikaci s dod.: PZ\_prais\_2018\_no199\_lpis\_anal\_ochr\_CSRF

# Návrh konceptu technického řešení

Viz část A tohoto PZ, body 2 a 3

# Uživatelské a licenční zajištění pro Objednatele

V souladu s podmínkami smlouvy 353-2015-13310 /1,2

# Dopady do systémů MZe

Vzniklý materiál je analýza problému, tzn. nebude mít dopad na fungování systémů.

### (Pozn.: V popisu dopadů zohledněte strukturu informací uvedenou v části A - Věcné zadání v bodech 3.3, 3.4 a 3.5. Pokud má požadavek dopady do dalších požadavků MZe, uveďte je též v tomto bodu.)

# Požadavky na součinnost Objednatele a třetích stran

Součinnost není požadována.

|  |  |
| --- | --- |
| **MZe / Třetí strana** | **Popis požadavku na součinnost** |
| MZe | Konzultace při tvorbě analýzy |
|  |  |

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

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

|  |  |
| --- | --- |
| **Popis etapy** | **Termín** |
| Předání plnění | 31.3.2018\*/ |

*\*/ Uvedený harmonogram je platný pouze v případě, že Dodavatel obdrží objednávku do 23.01.2018*

# Pracnost a cenová nabídka navrhovaného řešení

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

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Oblast / role**[[22]](#endnote-22) | **Popis** | **Pracnost v MD/MJ** | **v Kč bez DPH:** | **v Kč s DPH:** |
|  |  |  |  |  |
|  | Viz cenová nabídka v příloze č.01 | 11,13 |  93 683,63 | 113 357,19 |
| **Celkem:** | 11,13 |  93 683,63 | 113 357,19 |

(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 / Poskytovatele:** | **Jméno** **oprávněné osoby**[[23]](#endnote-23): | **Datum:** | **Podpis:** |
| … | … |  |  |

**C – Schválení realizace požadavku**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **ID SD MZe**[[24]](#endnote-24): | Z22651 | **ID ShP MZe**[[25]](#endnote-25): | **2016\_0031\_191** | **ID PK MZe**[[26]](#endnote-26): | **365** |

# Specifikace plnění

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

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

# Požadavek na součinnost

|  |  |  |
| --- | --- | --- |
| **Útvar / Dodavatel** | **Popis požadavku na součinnost** | **Odpovědná osoba** |
|  |  |  |
|  |  |  |

# Harmonogram realizace[[27]](#endnote-27)

|  |  |
| --- | --- |
| **Popis etapy** | **Termín** |
| **Předání plnění** | **31.3.2018\*/** |

# Pracnost a cenová nabídka navrhovaného řešení

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

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Oblast / role**[[28]](#endnote-28) | **Popis** | **Pracnost v MD/MJ** | **v Kč bez DPH:** | **v Kč s DPH:** |
|  |  |  |  |  |
|  | Viz cenová nabídka v příloze č.01 | 11,13 | 93 683,63 | 113 357,19 |
| **Celkem:** | **11,13** | **93 683,63** | **113 357,19** |

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

# Případné další obchodní podmínky[[29]](#endnote-29)

# Schválení[[30]](#endnote-30)

|  |  |
| --- | --- |
| **Žadatel:** | Schvaluji [ ]  / Neschvaluji [ ]  |
| … |  |
| Jméno a příjmení |  | Datum |  | Podpis |

|  |  |
| --- | --- |
| **Metodický/Věcný garant:** | Schvaluji [ ]  / Neschvaluji [ ]  |
| … |  |
| Jméno a příjmení |  | Datum |  | Podpis |

|  |  |
| --- | --- |
| **Change koordinátor:** | Schvaluji [ ]  / Neschvaluji [ ]  |
| … |  |
| Jméno a příjmení |  | Datum |  | Podpis |

|  |  |
| --- | --- |
| **Oprávněná osoba dle smlouvy:** | Schvaluji [ ]  / Neschvaluji [ ]  |
| … |  |
| Jméno a příjmení |  | Datum |  | Podpis |

# 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-2)
2. ID SD MZe – identifikátor požadavku přidělený v ServiceDesku MZe [↑](#endnote-ref-3)
3. ID ShP MZe – identifikátor projektu k požadavku přidělený v projektovém portálu MZe [↑](#endnote-ref-4)
4. ID PK MZe – identifikátor požadavku přidělený v pomocné evidenci projektové kanceláře MZe [↑](#endnote-ref-5)
5. Předmět změny – stručná informace, název požadavku [↑](#endnote-ref-6)
6. 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-7)
7. Priorita – vyjadřuje důležitost zapracování požadavku z pohledu časového. Vyplní se v případě volby kategorie „Normální změna“. [↑](#endnote-ref-8)
8. Kód – zkratka aplikace (viz „kód služby“ v katalogu služeb [↑](#endnote-ref-9)
9. Smlouva č. – uvede se, pokud existuje smlouva, v rámci níž se požadavky předkládají, totéž platí pro KL (katalogový list). [↑](#endnote-ref-10)
10. Rozsah aplikace LPIS je v tomto případě definován vztahem k ZoKB (Zákon č. 181/2014 Sb.) tedy tak jak je chápán jako VIS (významný informační systém) dle tohoto zákona. Jeho vymezení bylo stanoveno interně a je uvedeno v přiloženém dokumentu LPIS\_IS\_1v0.pdf [↑](#footnote-ref-2)
11. Agenda – jedná se o postupy a činnosti, které provádí uživatel. [↑](#endnote-ref-11)
12. Systémy – myšleno servery, operační systémy, standardní software a jimi tvořené clustery, geografické clustery atd. [↑](#endnote-ref-12)
13. Nepovinná položka při zpracování RfC [↑](#endnote-ref-13)
14. Nepovinná položka při zpracování RfC [↑](#endnote-ref-14)
15. Vyplňte ve spolupráci s provozním garantem. [↑](#endnote-ref-15)
16. Vyplní Change koordinátor s Provozním garantem. [↑](#endnote-ref-16)
17. Rozsah požadované dokumentace uveďte pod tabulkou. [↑](#endnote-ref-17)
18. ID SD MZe – identifikátor požadavku přidělený v ServiceDesku MZe, zkopíruje se z věcného zadání. [↑](#endnote-ref-18)
19. ID ShP MZe – identifikátor projektu k požadavku přidělený v projektovém portálu MZe, zkopíruje se z věcného zadání. [↑](#endnote-ref-19)
20. ID PK MZe – identifikátor požadavku přidělený v pomocné evidenci projektové kanceláře MZe, zkopíruje se z věcného zadání. [↑](#endnote-ref-20)
21. Uvede se datum zahájení a ukončení realizace, příp. další etapy. [↑](#endnote-ref-21)
22. Role se vyplní pouze v relevantních případech, např. u požadavku na infrastrukturu. [↑](#endnote-ref-22)
23. Oprávněná osoba – smluvně určená osoba oprávněná k předkládání požadavku na předložení nabídky. [↑](#endnote-ref-23)
24. ID SD MZe – identifikátor požadavku přidělený v ServiceDesku MZe, zkopíruje se z věcného zadání. [↑](#endnote-ref-24)
25. ID ShP MZe – identifikátor projektu k požadavku přidělený v projektovém portálu MZe, zkopíruje se z věcného zadání. [↑](#endnote-ref-25)
26. ID PK MZe – identifikátor požadavku přidělený v pomocné evidenci projektové kanceláře MZe, zkopíruje se z věcného zadání. [↑](#endnote-ref-26)
27. Uvede se datum zahájení a ukončení realizace, příp. další etapy. [↑](#endnote-ref-27)
28. Role se vyplní pouze v relevantních případech, např. u požadavku na infrastrukturu. [↑](#endnote-ref-28)
29. Změna smluvních podmínek - vyplní se v případě, že dohodnuté podmínky realizace požadavku se liší od smluvních. [↑](#endnote-ref-29)
30. Jméno a příjmení vyplní Change koordinátor, zbývající údaje podepisující. Ve volbě schvaluji/neschvaluji se zaškrtne hodící se volba. [↑](#endnote-ref-30)