POŽADAVEK NA ČERPÁNÍ MD / ZMĚNOVÝ POŽADAVEK Č. 82

Poskytovatel služby	Národní agentura pro komunikační a informační technologie, s.p.
Správce IS	Digitální a informační agentura, Na Vápence 915/14, 130 00 Praha 3
Objednatel	Digitální a informační agentura, Na Vápence 915/14, 130 00 Praha 3
Smlouva	Dílčí smlouva č. 1 na podporu provozu Informačního systému Národní bod pro identifikaci a autentizaci
Číslo RFC DIA	**1558**
Název RFC DIA	**Logování LoA SeP**
Kategorie RFC	**Urgent Change**
Číslo tiketu (Service Desk)	**199611/686666**
Katalogový list	**KL NIA 13 - Objednávka**
Typ odstávky	Kat. 0 (Zero)

1. Identifikace vzniku požadavku

Service Desk 199611/686666 Nacenění RFC 1558 – Logování LoA SeP.

2. Zadání požadované změny

Zadání požadavku na LoA v současné době není povinné. V případě chybného zadání, či nezadání žádné hodnoty, NIA automaticky doplní požadovanou úroveň záruky, která je definována v nastavení NIA.

Úkolem je monitorování, zda SeP při autentizačním procesu vloží do volání požadavek na LoA. Požadavkem je i rozlišení, že SeP vloží požadavek na LoA ve špatném formátu či nevloží vůbec a NIA požadovanou úroveň automaticky doplní.

3. Popis zajištění realizace změny

3.1 Popis současného stav

Level of Assurance (LoA) je specifické rozšíření protokolu SAML2P, které je požadováno specifikací eIDAS a slouží pro:

1. Zobrazení seznamu identitních prostředků (IdP) na straně NIA
2. Vytvoření autentizačního požadavku, který se předává eIDAS bráně.

NIA pro své interní operace související s výběrem IdP převádí hodnoty LoA na číselnou hodnotu dle následující tabulky.

LoA parametr	NIA hodnota
Bez uvedeného LoA	0
http://eidas.europa.eu/LoA/low	1
http://eidas.europa.eu/LoA/substantial	2
http://eidas.europa.eu/LoA/high	3

LoA pro komunikaci s NIA ze strany SePů není povinný element a v případě jeho nepřítomnosti, anebo pokud element LoA obsahuje jinou hodnotu než ve výše uvedené tabulce, pak je přiřazená hodnota 0. Toto přiřazení pak následně ovlivňuje chování při výběru IdP.

Při komunikaci s eIDAS bránou NIA respektuje vstupní hodnotu od SePa a beze změny ji předává dále. Pokud SeP o LoA nepožádá, pak NIA při výběru eIDAS brány automaticky doplní hodnotu http://eidas.europa.eu/LoA/substantial.

3.2 Navrhované úpravy NIA Federačního hubu (GG FPSTS)

Navrhované úpravy budou respektovat možnosti protokolů, které GG FPSTS podporuje pro přihlašování (WS-Federation, SAML2P, OpenID Connect). Vzhledem k tomu, že každý protokol má jiné možnosti a způsoby pro zadávání požadavků o LoA, jsou možnosti kontroly a logování pro každý protokol rozdílné.

Federační hub (GG FPST) bude upraven následujícím způsobem.

3.2.1 Globální konfigurační parametry

Budou vytvořeny nové konfigurační parametry, které umožní konfiguraci chování a řízení úrovně logování v Application Insights.

1. Parametr ***FP_Saml2AuthnContextValues.*** Tento parametr bude obsahovat seznam povolených hodnot požadavku SAML AuthnRequest pro atribut *<saml2:AuthnContextClassRef>.* Pokud bude přijat požadavek, který bude obsahovat v elementu *<saml2:AuthnContextClassRef>* jinou hodnotu než v uvedeném seznamu a zároveň bude mít parametr *FP_TraceWrongSaml2AuthnContext* hodnotu True, bude do AI zapsán trace s identifikátorem SePa a špatnou hodnotou. Zároveň bude nastavena hodnota LoA 0 pro interní operace NIA. Tato kontrola bude prováděna pouze pro protokoly WS-Federation a SAMP2. Protokol OpenID Connect tyto hodnoty o žádost pro LoA nepoužívá.
2. Parametr ***FP_TraceWrongSaml2AuthnContext.*** True/False pro zapínání a vypínání logovaní špatných hodnot v žádosti o LoA.
3. Parametr ***FP_TraceMissingLoAinRequest.*** True/False pro zapínání a vypínání logovaní pro případ, že SeP v žádosti o přihlášení LoA vůbec neuvádí. Tento parametr bude použit pro protokoly WS-Federation, SAML2P a OpenID Connect. Vzhledem k tomu, že LoA není povinné a existuje veliké množství scénářů, kdy SePové o LoA nežádají může zapnutí této úrovně logování způsobit veliké množství dat v AI a vytvoření šumových informací. Tato volba by měla být aktivní pouze v testovacím prostředí.

3.2.2 Nová konfigurace IdP

Konfigurace položky *Trusted Identity Provider* bude rozšířena o nový parametr „Minimal required LoA“ tak, aby každý IdP mohl definovat minimální požadovanou hodnotu LoA. Výchozí hodnota tohoto parametru bude 0. To znamená, že výchozí chování NIA a výběr seznamu IdP bude probíhat bez změny. Následně bude moci být IdP eIDAS (anebo i další) nastaven tak, že bude vyžadovat minimální hodnotu LoA = http://eidas.europa.eu/LoA/low (1). Tím se zajistí, že požadavky od SePů bez požadovaného LoA anebo chybně vyplněného LoA budou na NIA zpracovány, ale

v seznamu IdP nebude uveden IdP eIDAS (anebo i další). Tím bude zajištěno, že NIA nebude na eIDAS bránu zasílat nevalidní požadavky.

Úprava konfigurace IdP bude znamenat úpravu datového modelu pro ukládání parametrů IdP, úpravu GG MMC Admin a úpravu API kontraktu, který vrací atributy IdP pro strojové zpracování.

3.3 Logování v Application Insights

V Application insights vznikne nový workbook, který umožní zobrazit SePy, které posílají chybný požadavek na LoA nebo tento požadavek neposílají vůbec.

4. Odhad pracnosti

Tabulka 1. Pracnost a nacenění dle KL NIA 13

Činnosti	Role	Popis	MD
Projektové* řízení	Projektový manažer senior	• Administrativní spuštění projektu • Vedení interních schůzek • Schůzky se zákazníkem, organizace a kontrola jednotlivých činností v harmonogramu, report aktuálního stavu, řízení a kontrola finančních zdrojů a nákladů, komunikace s dodavatelem • Ukončení projektu, akceptace	2
	Projektový administrátor	• Administrace projektu, příprava PnČ, nacenění, zápisy, účast na jednáních, akceptace, fakturace, objednávka dodavatele	2,5
Analýza + úprava uživatelské dokumentace	Analytik senior	• Schůzky • Úprava vybraných detailních scénářů UC • Zapracování změn do Příručky pro kvalifikované poskytovatele	1
Testování*	Tester senior	• Příprava TC • Testování, oprava chyb • Příprava na akceptaci + akceptace	4
Bezpečnost*	Bezpečnostní tester	• Příprava • Testy integrity logování • Testy konzistence a bezpečnosti webové části • Základní penetrační testy autentizačního procesu • Základní automatizovaný zranitelnostní sken	6
Vývoj	Vývojář senior	• Příprava PnČ, vyjasňování se zákazníkem, interní schůzky • Konzultace Neurodot, Analýza, Testování, Bezpečnost • Součinnost při testování • Implementace změn na TEST • Implementace změn na PROD • Součinnost při UAT • Schůzky • Příprava workbooku v Application Insights • Součinnost při penetračních testech a řešení nálezů	5
Celkem			**20,5**

**detailní rozsah prací včetně odhadu pracnosti je uveden v příloze č.1 tohoto dokumentu*

Tabulka 2. Celkem dle rolí

Role	Cena MD bez DPH	Počet MD	Cena bez DPH	DPH	Cena s DPH
Projektový manažer senior		2			
Projektový administrátor		2,5			
Analytik senior		1			
Tester senior		4			
Bezpečnostní tester (Bezpečnostní architekt)		6			
Vývojář senior		5			
Celkem		**20,5**	**188 011,69**	**39 482,45**	**227 494,14**

Tabulka 3. Pracnost dle klientské služby KL NIA 13 (nacenění dodavatele poskytovatele)

Dodavatel	Cena MD bez DPH	Počet MD	Cena v Kč bez DPH	DPH	Cena v Kč s DPH
Projektový manažer		1			
Architekt		3			
Vývojář		4			
Tester		1			
Technická podpora – úpravy systému		2,5			
Celkem		**11,5**	**230 600,00**	**48 426,00**	**279 026,00**

Tabulka 4. Celková částka RFC 1558 NAKIT a dodavatel Neurodot

Pracnost celého RFC 1558	Cena v Kč bez DPH	DPH	Cena v Kč s DPH
Neurodot	230 600,00	48 426,00	279 026,00
NAKIT	188 011,69	39 482,45	227 494,14
Celkem	**418 611,69**	**87 908,45**	**506 520,14**

Poznámka: Článek 4.1.2 Dílčí smlouvy č.1 „Cena Služeb na objednávku“, Katalogový list NIA13 „Další služby“ – tento KL v rámci tohoto PnČ neslouží k pracím, které vedou k navýšení stávajících funkcionalit, a tedy k technickému zhodnocení IS NIA dle vyhlášky č. 410/2009 Sb., k provedení zákona č. 563/1991 Sb., o účetnictví, ve znění pozdějších předpisů pro vybrané jednotky. V rámci tohoto PnČ nebudou prováděny žádné rozvojové činnosti.

5. Návrh harmonogramu změnového požadavku

Logování LoA SeP bude realizováno do **18.05.2025**. Termín realizace může být prodloužen v případě neposkytnutí nezbytné součinnosti dle bodu 9. tohoto PnČ, nebo z dalších důvodů na straně objednatele do **31.12.2025.**

Harmonogram je pouze orientační a bude se upravovat podle skutečně odvedených prací.

	Činnost	Poznámka
T_0	Předání realizačního ticketu RFC na NAKIT	
$T_1 = T_0 + 1$ týden	Analýza	
$T_2 = T_1 + 2$ týdny	Vývoj + nasazení na TEST	Vývoj ND a NAKIT
$T_3 = T_2 + 1$ týden	Testing na TEST prostředí	
$T_4 = T_3 + 1$ týden	Příprava na UAT + UAT	
$T_5 = T_4 + 1$ týden	Nasazení na PROD	
$T_6 = T_5 + 1$ týden	Akceptace	

6. Návrh testovacího scénáře

Ověření správného logování v případě, kdy SeP v rámci autentizačního procesu vloží do volání požadavek na LoA.

Ověření správného logování v případě, kdy SeP vloží požadavek chybně či ho nevloží vůbec.

7. Výstupy změnového požadavku

Realizované úpravy a rozšíření dle bodu 3.2 a 3.3 tohoto dokumentu. Aktualizovaná příručka pro kvalifikované poskytovatele.

8. Akceptační kritéria, způsob ověření na produkci

Do reportingu/Provozního monitoringu NIA bude doplněn přehled SeP jaké LoA při autentizaci požadují, požadavek na LoA nezadávají nebo zadávají požadavek chybně.

9. Požadavky na součinnosti

Žádné.

10. Dopady do provozu / dopady do provozní dokumentace / dopady na finanční prostředky na podporu provozu daného IS

Služby definované v čl. 3. „Popis zajištění realizace změny“ tohoto PnČ nebudou generovat další dodatečné finanční prostředky na podporu provozu daného IS.

11. Dopady na bezpečnost IS / dopady do bezpečnostní dokumentace

Pravděpodobnost potřeby změn bezpečnostní dokumentace (politika a analýzy rizik) je nízká, ale nelze ji vyloučit.

	Schválil (dodavatel)	Schválil (zákazník)
Jméno		
Datum		
Podpis		

Příloha č.1

Rozsah prací projektové kanceláře (a hrubý odhad pracnosti)

Projektový manažer

- **Komunikace s týmem a rozdělení vypracování jednotlivých částí PnČ - 1,5 hod**
    - Nasdílení zadání RFC týmu, přiřazení dílčích částí PnČ jednotlivým pracovníkům. Dodatečná komunikace a zajištění informovanosti týmu.
- **Interní schůzky ke scope, nacenění a harmonogram PnČ – 2 hod**
    - Po vypracování analýzy, je svolána interní schůzka celého týmu, na které se představí přesná podoba scope a způsob provedení změny. Interní tým následně dopracuje zbývající body v PNČ včetně odhadu pracnosti. PM na základě těchto informací začne navrhovat harmonogram.
- **Komunikace s dodavatelem a schůzka ke scope a nabídce – 2 hod**
    - Předání zadání na dodavatele, upřesnění rozdělení prací a harmonogramu, komunikace dodání nabídky
- **Schůzka interního týmu s PM k vyplněným informacím a kontrola správnosti – 1 hod**
    - Na schůzce jsou doplněné dílčí části PNČ projednány a revidovány. Navržená pracnost je interně posouzena a jsou objasněny důvody jejího ocenění. Rovněž je projednán a odsouhlasen návrh harmonogramu.
- **Finalizace PnČ - 0,5 hod +**
    - Dokončení PnČ, finální kontrola a předání na zákazníka.
- **Realizace RFC, kontrola týmu (Příprava na UAT, schůzka k UAT), reporting zákazníkovi + komunikace a kontrola dodavatele - 6 hod**
    - Sledování průběhu realizace RFC, kontrola dodaných výstupů a kontrola předávky mezi týmy. Sledování termínů dle harmonogramu. Příprava na pravidelné schůzky se zákazníkem (páteční synchro s PM DIA, HTP PM). Kontrola a urgence dodavatele. Příprava před UAT, schůzka UAT a kontrola dokumentace k UAT. Pravidelné schůzky s dodavatelem k realizaci plnění.
- **Komunikace s interním týmem k nasazení – 1 hod**
    - Přípravná schůzka s týmem před nasazením + informování zákazníka
- **Akceptace – 1 hod**
    - Kontrola akceptačního protokolu, předání na zákazníka
    - Kontrola akceptačního protokolu na dodavatele a předání
- **Fakturace se zákazníkem – 1 hod**
    - Kontrola a schválení požadavku na vystavení faktury
    - Kontrola a schválení dodavatelské faktury

- **Celková odhadovaná pracnost: 16 hod = 2 MD**

Projektový administrátor

- **Přijetí požadavku - 0,5 hod**
    - Přijetí požadavku v Service Desk, nahrání schváleného PnČ do SD
- **Základní zpracování dokumentu PnČ – 1 hod**
    - Přenesení základních informací ze zadání do PnČ a příprava dokumentu pro vyplnění ostatními členy týmu
- **Založení Sharepoint k uložení dokumentace a správa dokumentace – 4 hod**
    - Vytvoření adresářů na Sharepointu projektu pro nové RFC, správa a archivace veškeré dokumentace související s RFC (nabídka od dodavatele, objednávka na dodavatele, zápisy z jednání, akceptační protokol, reporty, dokumentace k výstupům)
- **Založení AVYK a SAP pro vykazování MD - 0,5 hod**
    - Zajištění vytvoření vykazovací položky pro členy týmu.
- **Kontrola vykazování každý měsíc – 1 hod**
    - Kontrola výkazů za předchozí měsíc, příprava reportu pro projektového manažera
- **Komunikace – 4 hod**
    - Zpracování požadavků od projektového manažera, Komunikace se zákazníkem, dodavatelem a interním týmem.
- **Kontrola PnČ, vytvoření objednávky na dodavatele – 2,5 hod**
    - Finální kontrola PnČ před odesláním na zákazníka (dopočítání rozpočtu). Zajištění interního schválení a podpisu PnČ. Zprocesování založení a vystavení objednávky na dodavatele.
- **Účast na schůzkách a zápisy interních a externích schůzek – 4 hod**
    - Příprava zápisů ze schůzek, zapracování revizí a předání k podpisu. Ukládání na SHP Nakit a DIA.
- **Příprava akceptačních protokolů pro zákazníka a vystavení požadavku na vytvoření faktury - 2,5 hod**
    - Příprava akceptačních protokolů a požadavku na vytvoření faktury a zajištění podpisů
- **Celková odhadovaná pracnost: 20 hod = 2,5 MD**

Rozsah prací testerů (a hrubý odhad pracnosti)

- **Schůzky a nacenění (0,5 MD):** Účast na schůzkách a odhad pracnosti.
- **Příprava testovacích scénářů (0,5 MD):** Studium analýzy nových požadavků, příprava testovacích scénářů pokrývající nové funkcionality (případně zapracování změn do stávajících regresních scénářů.)
- **Testování na TEST prostředí (2 MD):** Ověření správné funkčnosti logování a správnosti logovaných údajů (např. ověření správného logování v případě, kdy SeP v rámci autentizačního procesu vloží do volání požadavek na LoA. Ověření správného logování v případě, kdy SeP vloží požadavek chybně či ho nevloží vůbec. Součástí je i zaevidování chyb a jejich retestování.
- **Příprava na akceptaci + akceptace (0,5 MD):** Závěrečné ověření stavu, příprava testovacích dat pro UAT. Příprava protokolů. Součástí je samotná akceptace se zákazníkem.
- **Nasazení PRODUKCE (0,5 MD):** Součinnost při nasazení do Produkce, ověření funkcionality hned po nasazení, provedení Smoke testů.
- **Celková odhadovaná pracnost: 4 MD.**

Rozsah prací bezpečnosti (a hrubý odhad pracnosti)

Na základě zhodnocení prováděných změn a souvisejících zásahů manažer kyberbezpečnosti (Martin Helebrant) změnu charakterizuje tak, že není natolik bezvýznamná (minoritní), aby nebylo nutné provést bezpečnostní otestováni. Změna má potenciál ovlivnit bezpečnost autentizace a federace identity. Existuje také riziko vzniku zranitelností v důsledku úprav kódu nebo nedostatečné implementace.

Plánované změny v systému mají potenciál mít bezpečnostní dopad na proces autentizace a výběru Identity Providerů (IdP). Klíčovým aspektem úprav je správná identifikace a zpracování Level of Assurance (LoA), který ovlivňuje přihlašování uživatelů a jejich přístup k jednotlivým IdP. Vzhledem k těmto změnám je nutné provést testování zaměřené na integritu logování, konzistenci přihlašovacího procesu a bezpečnost autentizačního mechanismu. Testování bude převážně explorativní, zaměřené na identifikaci případných chyb nebo bezpečnostních rizik. Důležitou součástí bude také validace, zda úpravy v kódu nevedly k nežádoucím vedlejším efektům, zejména v části výběru IdP, procesu přihlašování a autentizačního požadavku od SeP.

- **Příprava (0,75 MD):** Analýza fungování současného systému a dopadu změn. Zmapování způsobu logování požadavků SeP na LoA a aplikace nových konfiguračních parametrů. Příprava testovacích směrů a scénářů pokrývající relevantní situace.
- **Testy integrity logování (0,75 MD):** Ověření správnosti a úplnosti logovaných údajů (např. zda SeP zasílá požadavek na LoA v odpovídající podobě), jak se systém chová při chybějících nebo neplatných hodnotách. Sledování možných nesrovnalosti a prověření, zda logovací mechanismus umožňuje spolehlivé sledování požadavků.

- **Testy konzistence a bezpečnosti přihlašovacího procesu (0,75 MD):** Ověření, zda výběr IdP odpovídá očekávanému chování podle pravidel pro LoA a zda uživatelé nejsou nesprávně přesměrováni v důsledku chybných nebo chybějících hodnot LoA. Ověření procesu výběru IdP, průchodu autentizací a validace přenášených údajů.
- **Penetrační testy autentizačního mechanismu (1,25 MD):** Základní bezpečnostní testy zaměřené na možnosti manipulace s LoA, pokusy o obejití autentizace nebo podvržení hodnot v rámci přihlašovacího procesu. Ověření odolnosti systému proti neoprávněným úpravám požadavků a prověření možných dopadů změn na bezpečnost.
- **Automatizovaný zranitelnostní sken a ověření výstupů (1,5 MD):** Identifikace potenciálních slabin v autentizačním mechanismu a přidružených rozhraních. Ověření, zda změny v kódu nevedly k zavedení nových zranitelností, které by mohly být zneužitelné například prostřednictvím manipulace s autentizačními tokeny nebo nevalidních požadavků.
- **Vyhotovení závěrečné zprávy (1 MD):** Vyhotovení závěrečné zprávy, která bude obsahovat shrnutí zjištění, identifikované problémy a doporučení k dalším krokům.
- **Celková odhadovaná pracnost: 6 MD.**