SPRÁVA ZÁKLADNÍCH REGISTRŮ

# POŽADAVEK NA ČERPÁNÍ MD / ZMĚNOVÝ POŽADAVEK Č. 2/2019

| | |
|---|---|
| **Poskytovatel služby** | CZ.NIC |
| **Správce IS** | SZR |
| **Objednatel** | SZR |
| **Smlouva** | SZRAX002BC3T |
| **Číslo RFC SZR** | **655** |
| **Název RFC SZR** | **Příprava eIDAS uzlu na notifikaci eOP** |
| **Číslo tiketu (Service Desk)** | 43483 / 43699 |
| **Katalogový list** | **MG06 (na objednávku)** |
| **Typ odstávky** | A |

## 1. Identifikace vzniku požadavku

V současnosti provozujeme eIDAS uzel v roli Connector, která zajišťuje možnost občanům EU využívat své eID prostředky při přihlášení k českým online službám. S notifikací českých eOP je nutné zprovoznit druhou verzi eIDAS uzlu, tentokrát v roli ProxyService, která zpřístupní držitelům českých eOP služby v zahraničí. V testovacím provozu běží ProxyService využívající CEF eIDAS Node 1.4.5 napojená na NIA v roli SeP. Komunikace této verze eIDAS uzlu v roli SeP s NIA vykazuje několik problémů:

1. CEF eIDAS uzel předpokládá, že národní komponenta zodpovědná za autentizaci vystaví identifikátor PersonIdentifier bez prefixu „Zdrojová země/Cílová země". eIDAS uzel se pak následně stará o přidání správného prefixu. NIA naopak vytváří identifikátor se statickým prefixem CZ/CZ. Výsledný prefix předávaný např. do Švédska tak má podobu „CZ/SE/CZ/CZ". Aktuální verze CEF eIDAS uzlu nepřidává prefix pokud již PersonIdenfier správný prefixu obsahuje. Aby NIA mohla vytvořit správný identifikátor, je nutné jí předat informaci o zemi původu požadavku. Další možností je modifikovat PersonIdentifier obdržený od NIA.
2. CEF eIDAS uzel předpokládá, že šifrování Assertion v SAML odpovědí od NIA je dle SAML2 standardu, který se odkazuje na specifikaci XMLEnc. NIA pro identifikaci certifikátu, kterým šifrovala odpověď nicméně používá specifický element ze specifikace WSSE, kterému ale CEF eIDAS uzel nerozumí a neumí tedy takovou odpověď dešifrovat. Je nutné upravit zpracování odpovědí od NIA a správně identifikovat certifikát pro dešifrování.
3. CEF eIDAS uzel předpokládá, že odmítnutí autentizace je v SAML2 protokolu detekováno jiným stavem než je Success, např. AuthnFailed. NIA naopak, pokud uživatel odmítne autentizaci, vrátí SAML status Success a do seznamu atributů vloží nestandardní atribut Status, ve kterém je hodnota AuthnFailed. Takové nestandardní odpovědi nicméne aktuální verze CEF eIDAS uzlu nerozumí. Je tedy nutné zpracovat odpověd od NIA, aby se do zahraniční předala správná informace o stavu transakce.

Nutné změny v eIDAS uzlu můžeme zapracovat, nicméně bude to vyžadovat přechod na novou architekturu, která je použitá v CEF eIDAS Node verzích 2.x. Tato nová architektura umožňuje implementovat národní část v libovolném programovacím jazyce a není nutné provádět změny v Java kódu.

Aktuální verze eIDAS uzlu v nové architektuře, tedy CEF eIDAS Node 2.3 nepředává do národní části informaci o zemi původu požadavku a tuto informaci tak není možné předat do NIA. Bude tedy nutné zároveň modifikovat generický kód této verze a zajistit předání této informace.

## 2. Zadání požadované změny

Přidat do CEF eIDAS Node 2.3 komponentu, která bude na jedné straně komunikovat s CEF eIDAS Node 2.3 a na druhé straně s NIA a bude překládát požadavky mezi těmito komponentami v obou směrech, tedy jak pro roli Connector tak pro roli ProxyService. Zaimplementovat do tohoto kódu specifika vynucená nekompatibilitou NIA a eIDAS protokolu. Implementovat patch do CEF eIDAS uzlu 2.3 tak, aby předával do národní části informaci o zemi původu požadavku.

## 3. Popis zajištění realizace změny

Naprogramovat kód, otestovat a nasadit na testovací i produkční prostředí.

## 4. Odhad pracnosti

Pracnost

| Činnost | Pracnost MD |
|---|---|
| Analýza | [redacted] |
| Úprava | |
| Testy | |
| Nasazení na všechna prostředí | |
| Projektové vedení a administrativa | |
| **Celkem** | |

[redacted] 120 000 Kč bez DPH, tedy 145 200 Kč s DPH 21%.

## 5. Návrh harmonogramu změnového požadavku

Implementace proběhne v srpnu 2019. Nasazení na produkci pak po dohodě se zadavatelem. Předpokládá se v průběhu září 2019.

## 6. Návrh testovacího scénáře

Ověřit, že vygenerovaný PersonIdentifier obsahuje správný prefix. Ověření funkčnosti odmítnutí autentizace. Ověření funkčnosti autentizace při zapnutém šifrování odpovědí od NIA.

## 7. Výstupy změnového požadavku

Kód pro integraci NIA a CEF eIDAS node 2.3. Patch do CEF eIDAS Node 2.3. Funkční verze nasazená v produkčním prostředí.

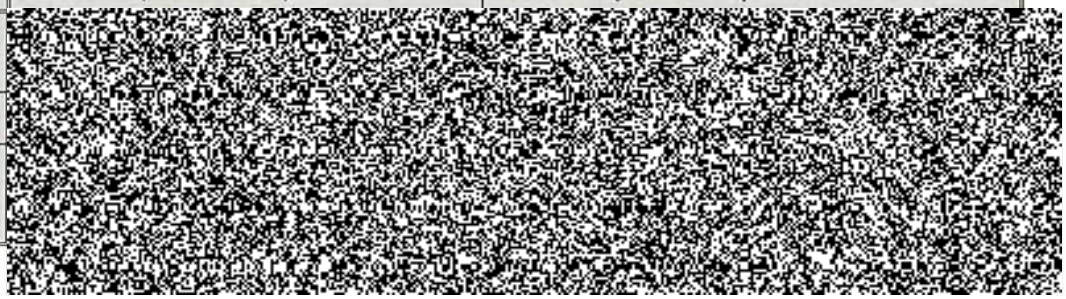
## 8. Akceptační kritéria, způsob ověření na produkci

## 9. Požadavky na součinnosti

Finální řešení problému 1 (prefix u PersonIdentifier) bude vyžadovat součinnost s vývojovým týmem NIA případně architektem SZR.

## 10. Dopady do provozu / dopady do provozní dokumentace

Žádné. Tato komponenta aktuálně neběží v produkčním provozu.

| | Schválil (dodavatel) | Schválil (zákazník) |
|---|---|---|
| Jméno |  | |
| Datum | | |
| Podpis | | |