mojeID a NIA

Nelehká cesta mojeID ke statusu kvalifikovaného systému

Jaromír Talíř • jaromir.talir@nic.cz • 14. 11. 2019

CZ.NIC | SPRÁVCE DOMÉNY CZ

Zákon o elektronické identifikaci - 250/2017

- Kvalifikovaný poskytovatel - https://info.eidentita.cz/sep/
  - Provozovatel online služeb umožňující elektronickou identifikaci u kterého ověření totožnosti nařizuje zákon
- Kvalifikovaný správce
  - Státní orgán, nebo osoba, které byla udělena akreditace pro správu kvalifikovaného systému
- **Kvalifikovaný systém -** https://info.eidentita.cz/idp/
  - Systém elektronické identifikace, splňující podmínky dané zákonem
- **Národni bod (NIA)**
  - Informační systém veřejné správy umožňující napojení kvalifikovaného systému

Požadavky zákona na kvalifikovaný systém

- Prokázání bezúhonnosti
- Pojištění odpovědnosti
- Zpracování plánu ukončení činnosti
- Způsobilost z hlediska veřejného pořádku, bezpečnosti a dodržování práv třetích osob
- **Potvrzení, že systém umí komunikovat s národním bodem**
- **Potvrzení, že vydaný prostředek splňuje technické specifikace, normy a postupy stanovené příslušným předpisem Evropské unie**

Komunikace s národním bodem

- Volání API národního bodu
  - Zajištění registrace vydaného prostředku elektronické identifikace a ztotožnění uživatele s údaji v ZR (registr obyvatel). Výsledkem je jednoznačný identifikátor, který se uloží u uživatele. API umožňuje zpětnou synchronizaci údajů uživatele při změně v ZR.
- Napojení přes SAML protokol v roli „Identity Provider“
  - Použije se při každém přihlášení přes NIA. Jako jediný atribut se předává výše uvedený jednoznačný identifikátor.

Povinnost vést evidenci vydaných prostředků

- jméno, popřípadě jména, a příjmení držitele
- adresa místa trvalého pobytu držitele, popřípadě adresa místa bydliště mimo území České republiky, pokud držitel nemá trvalý pobyt na území České republiky
- datum narození držitele
- identifikátor prostředku pro elektronickou identifikaci
- identifikátor držitele v rámci kvalifikovaného systému
- údaj o způsobu ověření totožnosti žadatele o vydání prostředku pro elektronickou identifikaci, a byla-li totožnost ověřena průkazem totožnosti, rovněž číslo a druh průkazu totožnosti
- datum a čas vydání prostředku pro elektronickou identifikaci a datum a čas jeho zneplatnění
- doba platnosti prostředku pro elektronickou identifikaci
- datum a čas přijetí žádosti o zneplatnění prostředku pro elektronickou identifikaci nebo oznámení držitele o zneužití nebo hrozícím nebezpečí zneužití prostředku pro elektronickou identifikaci.

API národního bodu

- **TR_ZTOTOZNENI** – Na základě vstupních údajů vyhledá záznam v ROB a vrátí jednoznačný identifikátor (pseudonym)
- **TR_EVIDENCE_VIP_ZAPIS** – Zaznamená vydaný identifikační prostředek svázaný s konkrétním pseudonym
- **TR_EVIDENCE_VIP_ZMENA** – Zaznamená zrušení nebo jinou změnu u vydaného prostředku
- **TR_EVIDENCE_VIP_UPOZORNENI** – Zaznamená upozornění týkající se vydaného prostředku a notifikuje ostatní IDP
- **TR_ZNEPLATNENE_PSEUDONYMY** – Zpětná notifikace o zneplatnění jednoznačného identifikátoru
- **TR_NOTIFIKACE_IDP** – Zpětná notifikace obecně o změnách údajů

Volání API národního bodu

- Implementace WS-Federation v rámci Windows Communication Foundation – komponenta .NET frameworku
- Hierarchická autentizace – volání tří SOAP zpráv
  - První volání autentizované přes klientský TLS certifikát získá autentizační token – **FP-STS**
  - Druhé volání autentizované prvním tokenem získá druhý token – **IP-STS**
  - Třetí volání autentizované druhým tokenem obsahuje volání služby

Problémy komunikace s WCF

- Odmítnutí validního podepsaného XML pokud podepisovaná část obsahuje konce řádků.
- Odmítnutí XML, které neobsahuje očekávané pořadí elementů uvnitř **<Security>**
- Neúplná implementace standardu wss-x509-token-profile
- Předefinování standardních datových typů jako **<RequestSecurityToken>**

Naše implementace klientské části

- Programovací jazyk Python
- Knihovna pro SOAP komunikaci Zeep - http://www.python-zeep.org/
- Implementace workaroundů pro problémy komunikace s WCF
- https://github.com/CZ-NIC/python-cz-nia

Napojení přes SAML protokol

- SAML protokol umí mojeID cca od 2015
- Metadata NIA v roli „Service Provider“ - https://tnia.eidentita.cz/FPSTS/FederationMetadata/2007-06/FederationMetadataRP.xml?id=11
- Vymění se pouze jeden atribut - http://eidas.europa.eu/attributes/naturalperson/PersonIdentifier
- NIA zatím nepodporuje jako algoritmus podpisu RSA-SHA512 (ani ECDSA)
- Nezkoušeli jsme zatím šifrování

Podmínky nařízení eIDAS

- Prováděcí nařízení CIR 2015/1502 k eIDAS - https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:JOL_2015_235_R_0002
- Návod pro intepretaci úrovní záruky - https://ec.europa.eu/cefdigital/wiki/download/attachments/40044784/Guidance%20on%20Levels%20of%20Assurance.docx
- DKP-IDP 3.0 - https://www.mvcr.cz/clanek/ministerstvo-vnitra-zverejnuje-dokument-konkretizujici-minimalni-pozadavky-na-kvalifikovane-eid-systemy-a-eid-prostredky.aspx
- Úrovně záruky
  - Nízká (Low)
    - Jednofaktorová autentizace + základní ověření totožnosti
  - Značná (Substantial)
    - Dvoufaktorová autentizace + důkladnější ověření totožnosti
  - Vysoká (High)
    - Dvoufaktorová autentizace odolná proti útočníkovi s vysokým potenciálem + fyzické ověření totožnosti

Ověření totožnosti na CzechPointech

- Poskytování údajů z registru obyvatel jiné osobě podle § 58a zákona č. 111/2009 Sb., o základních registrech
  - V roce 2018 přibyla možnost přidat **zprávu pro příjemce**
- https://szrcr.cz/cs/sluzby/obcan-a-podnikatel/prihlaseni-k-odberu-dat
- Zdarma na ~ 7 000 CzechPointech
- Vygenerujeme unikátní identifikátor, který žadatel předá obsluze CzechPointu a prokáže se dokladem totožnosti. Systém základních registrů nám pak zašle identifikátor zpět jako zprávu pro příjemce spolu s údaji o ověřené osobě datovou schránkou
- Získáme přesnou totožnost z Registru obyvatel
- Ověření totožnosti má stejnou sílu jako při zřízení datové schránky

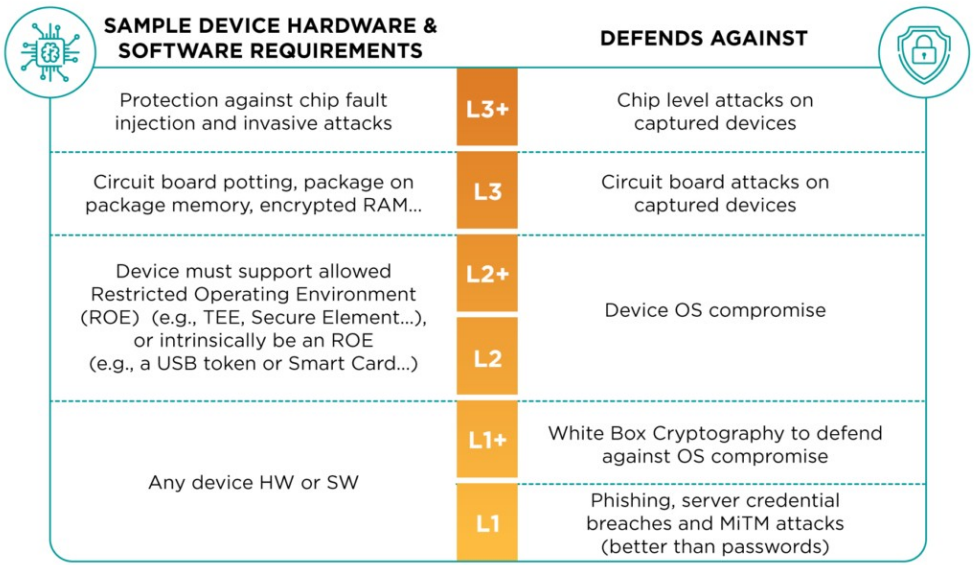
Ověření totožnosti na CzechPointech

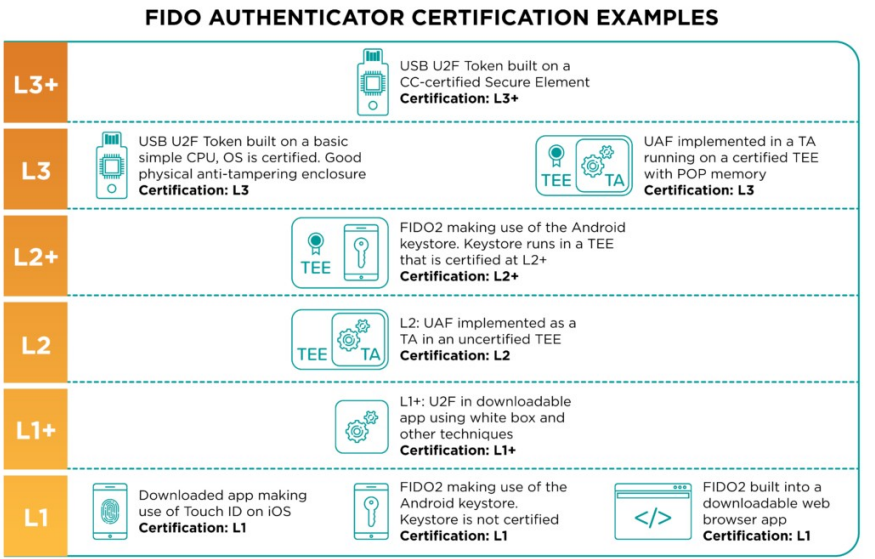
- Úzké hrdlo je obsluha CzechPointů
  - Vyplňuje se formulář obsahující cca 5 polí
  - Chyby zejména v identifikátoru žádosti
  - Ideálním řešením by bylo skenování QR kódu které předvyplní formulář
- Kombinace systému ISDS a ZR neumožňuje jednoduché vytvoření testovacích identit
- Od března 314 validací

Dvoufaktorová autentizace přes FIDO2

- Nejmodernější trend autentizace ve webovém prostředí
- Využívá asymetrické kryptografie
- Podpora prakticky ve všech prohlížečích
- Aktuálně nízká dostupnost na hlavních e-shopech
- Podpora v mojeID spuštěna v říjnu v pilotním provozu
- Děkujeme za otestování a zpětnou vazbu

FIDO certifikace pro zařízení





Propojení autentizace a ověření totožnosti

- Svázání nastavení autentizačního prostředku s návštěvou CzechPointu
- Nutnost zajistit, že prostředek má v držení ztotožněná osoba
- Validace v minulosti nestačí

Ukázka prototypu

- Založení mojeID a propojení s NIA
  - https://mojeid.regtest.nic.cz/registration/
- Dokončení validace přes CzechPoint zatím manuálně
- Přihlášení přes eIDAS ke švédské službě
  - https://qa.test.swedenconnect.se/

Závěr

- Implementace volání API národního bodu aktuálně selhává na diakritice – čekáme na pomoc NAKITu
- Teoreticky by tento koncept mohl splňovat vysokou úroveň záruky
  - Problém je nekompatibilita s aktuální verzí DKP-IDP. Vyjednáváme o možném doplnění ověření totožnosti na CzechPointu
  - Otázka je úroveň FIDO certifikace – stačí L2?
- Minimálně plánujeme akreditaci na úroveň střední
  - Zde by mohl být dostačený systém postavený na našem mojeID autentikátoru, OTP, případně FIDO2 bez nutné certifikace

Děkuji za pozornost

Jaromír Talíř • jaromir.talir@nic.cz

CZ.NIC | SPRÁVCE DOMÉNY CZ