PEPS, NIA a mojeID

Budoucnost elektronické identity

Jaromír Talíř • jaromir.talir@nic.cz • 03.12.2016

mojeID

Obsah

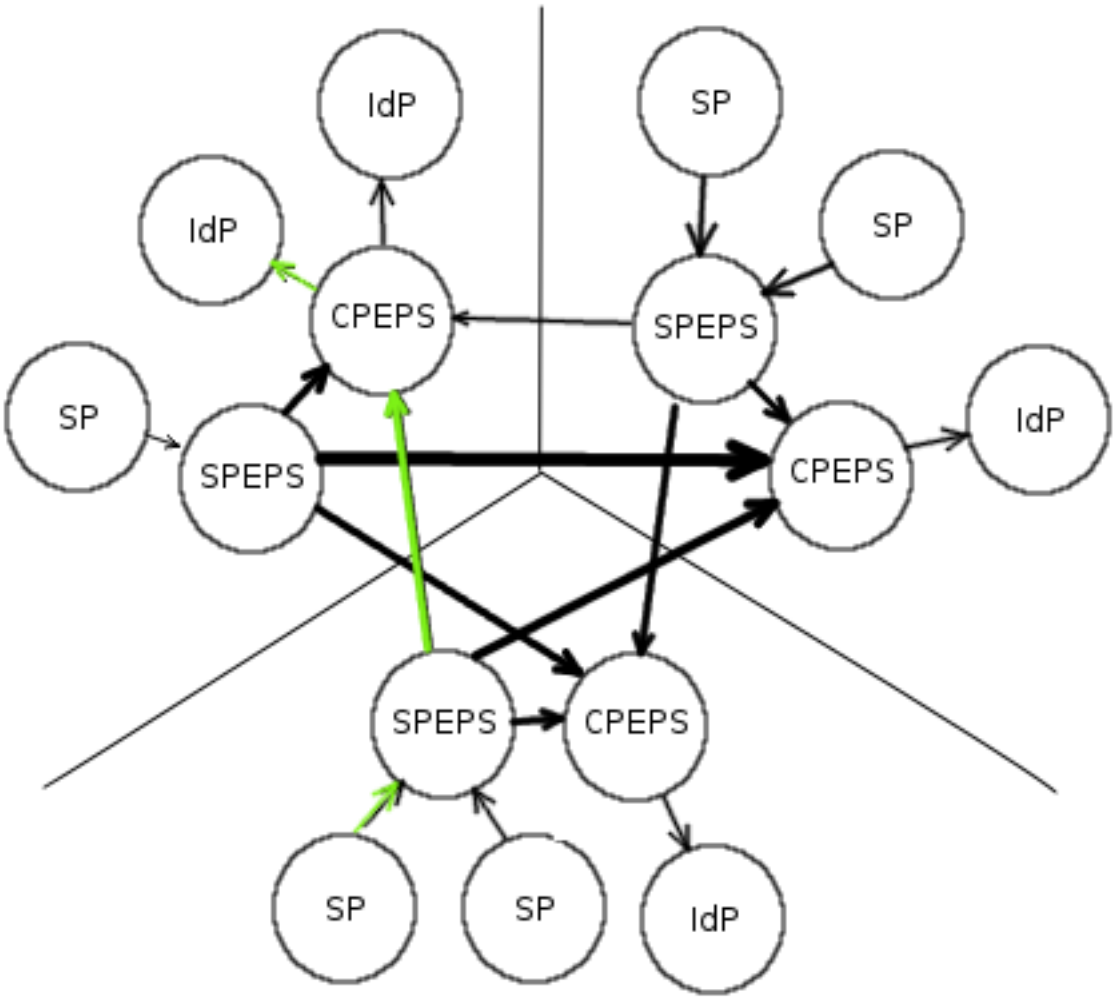
- Přeshraniční autentizace
  - Projekt STORK, nařízení eIDAS a CZ.PEPS
- Elektronická identita v ČR
  - NIA a nový zákon o elektronické identitě
- Služba mojeID
  - Zapojení do konceptu elektronické identity v ČR a novinky z letošního roku

Přeshraniční autentizace - STORK

- Pilotní projekty STORK1(2009-2011) a STORK2(2012-2015)
- Architektura propojených národních bodů PEPS (Pan-European Proxy Service) na bázi SAML 2.0 federace
- Propojení realizováno vzájemnou manuální výměnou certifikátů a konfigurací

mojeID

Přeshraniční autentizace - STORK



Přeshraniční autentizace - STORK

- Referenční implementace v jazyce Java
- Definice sady atributů
  - eIdentifier ve formátu XX/YY/ZZZZZZ
  - QAA1-QAA4 – Quality Authentication Assurence
- Specifické vlastnosti
  - Digitální podepisování dokumentů
  - Anonymita – dotazníky
  - Právnické osoby – zodpovědné fyzické osoby

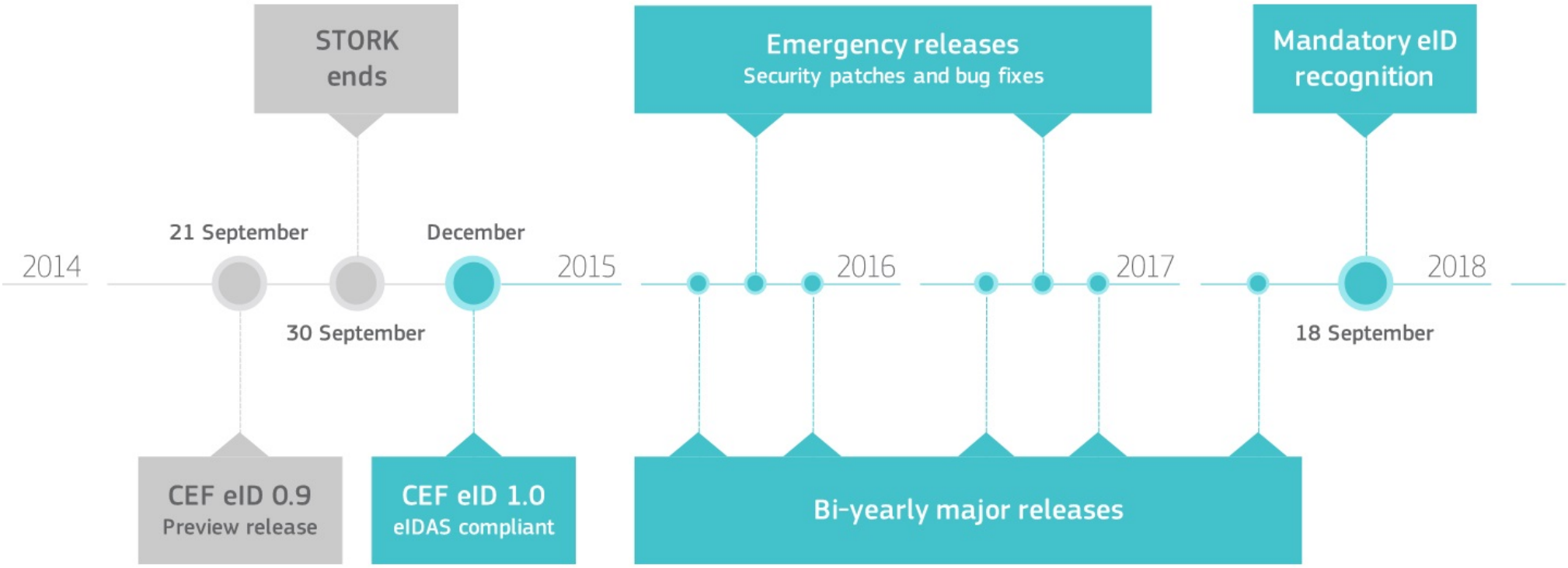
mojeID

Přeshraniční autentizace - eIDAS

- Nařízení EU řeší eID + (digitální podpisy, časová razítka, TLS certifikáty, e-delivery)
  - Přijato v červenci 2014, povinné ohlášení eID systémů do září 2018
- Vývoj řídí Directorate-General for Informatics (DIGIT)
  - Vychází ze zkušenosti STORKu, přebírá architekturu a částečně i kód
  - Hlavní změna je implementace nařízení EU
  - Kompatibilitu se STORK mají zajistit konektory

mojeID

Přeshraniční autentizace - eIDAS



Přeshraniční autentizace - eIDAS

- Změna terminologie – PEPS = eIDAS Node
  - S-PEPS = eIDAS Connector
  - C-PEPS = eIDAS Proxy Service
  - QAA = LOA (Level Of Assurance)
- Mnohem jednodušší než STORK
  - Jen základní atributy
  - Propojení zajistí repozitář SAML 2.0 metadat

mojeID

Přeshraniční autentizace - eIDAS

- CZ.PEPS
  - Grant EU na provoz národního uzlu (eIDAS node) v CZ.NIC do roku 2019
  - Napojení na NIA se diskutuje v rámci pracovní skupiny MVČR
- Zákoutí nařízení eIDAS odhaluje kurz CZ.NIC Akademie - https://akademie.nic.cz/akademie/course/112/detail/

mojeID

Elektronická identita v ČR

- Novela zákona o občanských průkazech
  - Nové občanské průkazy s čipem v roce 2018
  - Splňující normy eIDAS
  - Bezplatné vystavení
  - Možnost výměny pro stávající držitele průkazů s čipem
- Projednáváno v legislativních komisích vlády

mojeID

Elektronická identita v ČR

- Zákon o elektronické identifikaci – ZoEI
  - Kvalifikovaný systém – akreditovaný systém elektronické identifikace (IdP)
  - Kvalifikovaný správce – provozovatel kvalifikovaného systému
  - Kvalifikovaná online služba – služba využívající autentizaci kvalifikovaným systémem (SP)
- ZoEI by se měl již brzy posunout do vnějšího připomínkového řízení

mojeID

Elektronická identita v ČR

- NIA – Národní bod identifikace a autentizace
- Zajišťuje propojení zaregistrovaných IdP a SP
  - Uživatel si bude moci zvolit IdP pro autentizaci
    - Plánované IdP – eOP, datové schránky, další...
  - Po autentizaci budou předána data ze základních registrů
  - Uživatel může uložit souhlas s předáváním údajů
  - SP neví nic o IdP a naopak
  - Podpora protokolů WS-Federation a SAML 2.0

mojeID

Elektronická identita v ČR

- Napojení na EU gateway (CZ.PEPS?)
  - NIA IdP => S-PEPS => Zahraniční eID systémy
  - NIA SP <= C-PEPS <= Zahraniční služby
- Portál eidentita.cz
  - Správa souhlasů uživatelů s předáváním údajů
  - Možnost ukládat dodatečné údaje
  - Správa poskytovatelů služeb
- Zahájení ověřovacího provozu plánováno již na začátek roku 2017

mojeID

mojeID

- Často je mojeID uváděno jako příklad potenciálního komerčního IdP
  - Zákon s touto variantou počítá
- Zapojení mojeID by vyžadovalo ztotožnění uživatele s identitou v základních registrech
- Služba mojeID by zjevně byla využita pouze jako autentizační prostředek, nikoliv jako zdroj atributů

mojeID

mojeID

- Aktuálně provozujeme STORK PEPS napojený ma mojeID
  - Propojení na další země zapojené do projektu STORK
  - Využíváno pro přihlašování do informačních systémů EK
  - Máme již i systémy zapojené i jako místní poskytovatele služeb

mojeID - novinky

- Ověřování ostatních emailových adres
  - Dříve se ověřoval pouze „hlavní e-mail“
  - Nyní totéž platí pro „e-mail pro oznámení“ a „další e-mail“
- Předávání alternativních e-mailů
  - Možnost předat poskytovateli služeb libovolný ze svých nastavených e-mailů
  - Obdobně jako již dříve implementováno pro dodací adresu

mojeID - novinky

- Implementace požadavků pro zapojení do eduID federace
  - Předávání eduID specifických identifikačních atributů
  - Úspěšně otestováno v prostředí testovací federace
  - Spuštěno akceptování všech poskytovatelů služeb zapojených do federace
  - Probíhají úpravy WAYF

mojeID

mojeID - novinky

- Úpravy v autentizačních protokolech
  - Certifikace OpenID Connect u OpenID Foundation
  - Sladění předávání stavu ověření účtu ve všech protokolech
  - Lepší dokumentace pro poskytovatele služeb
- Nový systém pro podporu validačních pracovišť
- Validace mojeID zasláním zprávy přes datovou schránku

mojeID - novinky

- mojeID datovka
  - Webová služba implementující rozhraní datových schránek podle § 14a zákona č. 300/2008
  - Získali jsme certifikaci teprve jako druhý poskytovatel vedle ČSOB
  - Přihlašování do služby přes účet mojeID
  - Možnost uložení zpráv na serveru
  - Plánované spuštění začátkem roku 2017

Děkuji za pozornost

Jaromír Talíř • jaromir.talir@nic.cz • www.mojeid.cz

CZ.PEPS
CZECH REPUBLIC PAN-EUROPEAN PROXY SERVICES

Spolufinancováno Evropskou unií
Nástroj pro propojení Evropy

mojeID