SSSVD

SPRÁVA STÁTNÍCH SLUŽEB VYTVÁŘEJÍCÍCH DŮVĚRU

DŮVĚRYHODNÉ SLUŽBY PRO EUDIW

ROK INFORMATIKY

CHEB KC SVOBODA 5. ČERVNA 2025

SSSVD

SPRÁVA STÁTNÍCH SLUŽEB VYTVÁŘEJÍCÍCH DŮVĚRU

Program

- Představení stavu vytváření úřadu SSSVD
- Hlavní priority 2025 – provoz, rozvoj a legislativa
- ZOKB versus DŮVĚRYHODNÉ SLUŽBY
- Významné projekty 2025

SSSVD

SPRÁVA STÁTNÍCH SLUŽEB VYTVÁŘEJÍCÍCH DŮVĚRU

Představení úřadu

- Správa státních služeb vytvářejících důvěru, s. p. o. vznikla 1 dubna 2023
- Zřizovatelskou funkci vůči příspěvkové organizaci vykonává Digitální a informační agentura
- Ředitelem SSSVD jmenován Ing. M. Pešek k 1. září 2023
- Převzetí činností poskytovatele Národní certifikační autority, k dnešnímu dni má SSSVD **12** kmenových zaměstnanců zajišťujících jak odborné, tak i administrativní činnosti
- Sídlo úřadu je stále oficiálně Praha 3, Na Vápence, ale pracoviště je v Zelenči u Prahy v NDC SPCSS Zeleneč
- SSSVD má definováno zákonem č. 297/2016 S., o službách vytvářejících důvěru v §14odst.(4):
  Předmětem činnosti Správy je poskytování služeb vytvářejících důvěru pro potřeby České republiky. Hlavní a vedlejší činnosti definuje STATUT

SSSVD

SPRÁVA STÁTNÍCH SLUŽEB VYTVÁŘEJÍCÍCH DŮVĚRU

Představení základních poskytovaných služeb

- Hlavní službou je Národní certifikační autorita – NCA
  - Služby vytvářející důvěru podle nařízení EU č. 910/2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu (eIDAS)
  - V ČR tuto oblast definuje zákone č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce
- Další související služby
  - Podpora klientů NCA – budování registračních autorit (vydávání el. podpisů), školení, metodická pomoc
  - Účast na projektech jako je CMS2FA neboli nové služební karty resortu MV
- Připravované služby
  - V rámci evropské digitální služby se jedná o služby pro stát/DIA i pro občany
  - Školení a edukace v rámci jiné činnosti definované Statutem

SSSVD

SPRÁVA STÁTNÍCH SLUŽEB VYTVÁŘEJÍCÍCH DŮVĚRU

Představení základních poskytovaných služeb NCA

- Patříme mezi největší poskytovatele služeb vytvářejících důvěru v ČR – **POSKYTOVATELÉ**
- **Vydávání kvalifikovaných certifikátů pro elektronické podpisy**
- **Vydávání kvalifikovaných certifikátů pro elektronické pečetě**
- **Vydávání kvalifikovaných elektronických časových razítek**
- **Kvalifikovaná služba ověřování platnosti kvalifikovaných elektronických podpisů a pečetí**
- Školení a metodická podpora uživatelů

SSSVD

SPRÁVA STÁTNÍCH SLUŽEB VYTVÁŘEJÍCÍCH DŮVĚRU

Klienti SSSVD využívající NCA

- Klienti SSSVD v oblasti NCA jsou **výhradně** vybrané organizační složky státu jako jsou Bezpečnostní sbory a složky zajišťující bezpečnost státu, nebo se na této činnosti podílejí.
- MV ČR, PČR, HZS, OAMP, policejní školy, hasičské školy, další podřízené organizace resortu MV, MO ČR, VZ, BIS, UZSI, NBU, NUKIB, GIBS, GŘC, DIA, národní, zemské a oblastní archivy
- Služby jsou těmto speciálním složkám poskytovány bezúplatně

SSSVD

SPRÁVA STÁTNÍCH SLUŽEB VYTVÁŘEJÍCÍCH DŮVĚRU

Používání RSA klíčů

- Byla vydána nová verze specifikací: ETSI TS 119 312 V1.5.1 (2024-12): https://www.etsi.org/deliver/etsi_ts/119300_119399/119312/01.05.01_60/ts_119312v010501p.pdf

- Doporučená data ukončení používání RSA klíčů dle jejich délky:

8.4 Recommended end dates for key sizes

The parameters defined in Table 6 and Table 7, derived from [14], page 23 and page 25, respectively, should be used.

The key size (security parameter) for RSA is the bit length of the modulus *n*.

Table 6: Recommended end dates for RSA key sizes

Key size ($\log_2(n)$ in bits)	End date	Recommendation
≥ 1 900 and < 3 000	2028-12-31	L[2028]
≥ 3 000	n/a	R

SSSVD

SPRÁVA STÁTNÍCH SLUŽEB VYTVÁŘEJÍCÍCH DŮVĚRU

Používání RSA klíčů

- Zároveň tabulka č. 10 uvedená v předchozí verzi Algo paperu (https://www.etsi.org/deliver/etsi_ts/119300_119399/119312/01.04.03_60/ts_119312v010403p.pdf) obsahující informaci, že po roce 2025 nebude doporučována délka klíče RSA menší než 3000 bitů, byla odstraněna z nové verze Algo paperu.

- Doporučení:
  - V případě vydání Twins certifikátů s platností na 3 roky do konce roku 2025 přejít na vydávání certifikátů RSA 4096b nebo eliptické křivky ECDSA384
  - V případě vydání certifikátů s platností 1 rok přejít nejpozději do konce roku 2027 na vydávání certifikátů RSA 4096b nebo eliptické křivky ECDSA384

SSSVD

SPRÁVA STÁTNÍCH SLUŽEB VYTVÁŘEJÍCÍCH DŮVĚRU

Nové verze aplikací NCA

- **Aplikace**
  - NCARA 2.7.1.0 a NCARATwins 1.5.0.5
  - NewCertNCA 2.7.0.5 a NewCertNCATwins 1.5.0.9
- **Provedené úpravy a nové funkčnosti:**
  - **Přechod TSA certifikátů a certifikátů koncových uživatelů na silnější kryptografii**

    Nově je možné vydávat osobní certifikáty s délkou klíče 4096 bitů RSA-PSS

    Při obnově TSA certifikátů (s platností 6 let) v2025 dojde k přechodu na 4096 bitů RSA-PSS.
  - **On-line evidence šablon a smluv**

    Odstranění šablon protokolů z distribuce aplikací NCARA (TWINS) a umístění na server NCA, odkud je NCARA získá on-line pomocí nově vzniklé služby
  - **Vydání balíčku kvalifikovaného certifikátu pro el. pečeť a komerčního technologického certifikátu**

    Spojení vydání kvalifikovaného certifikátu pro elektronickou pečeť a komerčního technologického certifikátu na jednu žádost on-line bez osobní návštěvy registrační autority na základě podpisu žádosti kvalifikovaným certifikátem NCA žadatele o balíček

SSSVD

SPRÁVA STÁTNÍCH SLUŽEB VYTVÁŘEJÍCÍCH DŮVĚRU

- **Nový profil TWINS certifikátu a rozšíření profilu komerčního certifikátu pro přihlašování do OS Windows**

Rozšíření možného naplnění položek kvalifikovaného a komerčního certifikátu v rámci produktu TWINS o trojnásobný výskyt položky OU a úpravy formátu žádosti o tyto certifikáty tak, aby bylo možné načítat žádosti a vydávat certifikáty s těmito položkami.
Pro možnost přihlašování komerčním certifikátem do operačního systému Windows (dvoufaktorová autentizace) bude profil komerčního certifikátu rozšířen o potřebné položky

- **Úpravy NCARA, CA a Úložiště dokumentů**

Doplnění funkčnosti o možnost výběru operátora, zda uložit dokumenty do úložiště SSSVD nebo lokálního úložiště daného uživatele NCA - bezpečnostní či zpravodajské složky na předem definované adrese v souborovém systému. Jde o doplnění volby operátora, zda po podpisu smluvních dokumentů (před odesláním do Úložiště SSSVD či uložení do souborového úložiště uživatele NCA) je uloží v PDF formátu na jím definované místo jako zálohu (v nastavení NCARA

- **Vyhledání certifikátu nově i dle ID držitele certifikátu**

- **Revize – úpravy aplikací pro slabozraké**

Naplnění zákonných požadavků - web aplikace (zneplatnění, certlist, crllist), desktop (generátor žádosti a obnovy NewCertNCA(Twins) a NCARA

SSSVD

SPRÁVA STÁTNÍCH SLUŽEB VYTVÁŘEJÍCÍCH DŮVĚRU

Připravované služby 2025/2026

- **Služba vzdáleného podepisování - řešení, které umožní přijetí požadavku na vydání certifikátu, vydání a předání certifikátu přes rozhraní (včetně obnovy certifikátu)**
- Cílem služby je plnohodnotná služba vzdáleného podpisu podle eIDAS2 s cílem auditu jako kvalifikované služby vlastními prostředky
- Bude vytvořena nová verze aplikace NCARA pro příjem žádosti o QC(kvalifikovaný el. podpis)
- Žádost odeslána na flash disk/server NCA/předána na rozhraní NCARA -> Žadatel se dostaví na RA, kde bude ověřen -> Načtení žádosti do NCARA -> Vydání QC certifikátu na NCA a uveřejnění na definovaném rozhraní NCA, odkud si jej systém BS stáhne -> Žadatel podepíše papírový protokol a smlouvu na RA

SSSVD

SPRÁVA STÁTNÍCH SLUŽEB VYTVÁŘEJÍCÍCH DŮVĚRU

Projekty na kterých se SSSVD podílí, nebo do nich přispívá 2025+

- Služby vytvářející důvěru pro ověřovací provoz EUDIW realizovaný DIA s využitím znalostí procesů NCA
- Realizace služeb vytvářejících důvěru pro DIA při vytváření a provozu státní části EUDIW
- Projekt dvoufaktorové identifikace pro resort Ministerstva vnitra (MV, PČR a HZS)

SSSVD

SPRÁVA STÁTNÍCH SLUŽEB VYTVÁŘEJÍCÍCH DŮVĚRU

Legislativa v ČR

USNESENÍ
VLÁDY ČESKÉ REPUBLIKY

ze dne 26. března 2025 č. 218

k preferované variantě realizace Evropské peněženky digitální identity

Vláda

I. **schvaluje** pro realizaci klientské části Evropské peněženky digitální identity variantu Koncese (dále jen „preferovaná varianta“), podle části III materiálu čj. 208/25;

II. **ukládá** řediteli Digitální a informační agentury

1. zajistit preferovanou variantu realizace Evropské peněženky digitální identity podle bodu I tohoto usnesení v termínu do 31. prosince 2026,

2. zajistit ve spolupráci se Správou státních služeb vytvářejících důvěru služby vytvářející důvěru nezbytné pro provoz státní části Evropské peněženky digitální identity.

Provede:
ředitel Digitální a informační agentury

SSSVD

SPRÁVA STÁTNÍCH SLUŽEB VYTVÁŘEJÍCÍCH DŮVĚRU

EUDIW - SSSVD jako vhodný partner státu a občana

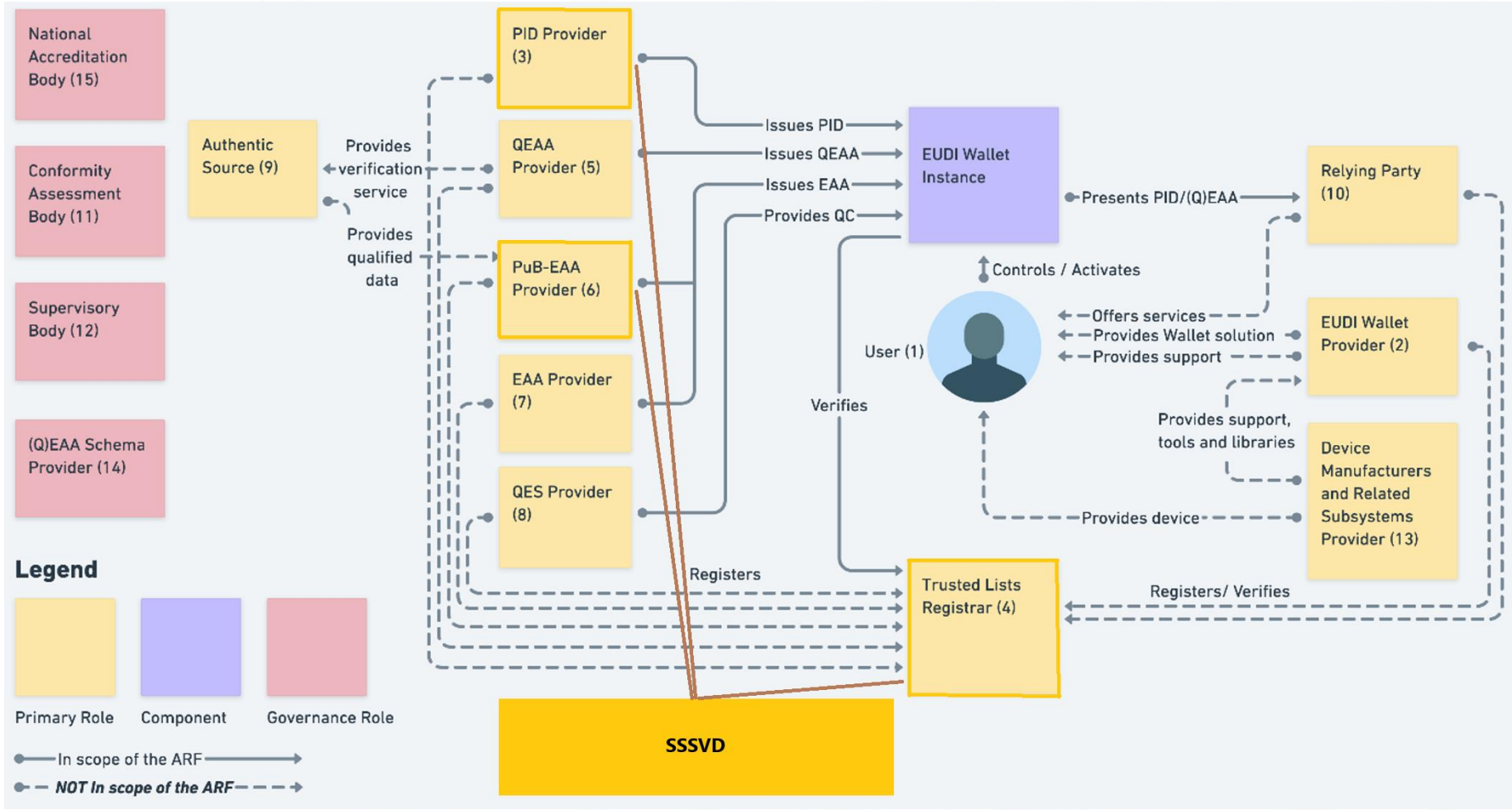
EU Digital Identity

Wallet

SSSVD

SPRÁVA STÁTNÍCH SLUŽEB VYTVÁŘEJÍCÍCH DŮVĚRU

EUDIW v podmínkách ČR



SSSVD

SPRÁVA STÁTNÍCH SLUŽEB VYTVÁŘEJÍCÍCH DŮVĚRU

EUDIW – odpovědnosti DIA a SSSVD

- **Agentura** bude odpovídat za činnost PID Provider (služba poskytování Personal Identification Data).
- **Správa** zajistí službu vzdáleného opatřování (kvalifikovanou) pečetí pro data vytvořená PID Providerem a zajistí správu klíčů.
- **Agentura** bude odpovídat za činnost PuB_EAA Provider (služba kvalifikovaných potvrzení atributů a potvrzení ze státních zdrojů).
- **Správa** zajistí službu vzdáleného opatřování (kvalifikovanou) pečetí pro data vytvořená PUB_EAA Providerem a zajistí správu klíčů.
- **Agentura** bude odpovídat za činnost Trusted List Register.
- **Správa** zajistí služby pečetí pro data vytvořená Trusted List Register, což zahrnuje zejména následující činnosti:
  - vydávání přístupových certifikátů spoléhajících se stran,
  - vydávání registračních certifikátů spoléhajících se stran,
  - zajišťování celého životního cyklu certifikátů uvedených v písm. a) a b) v souladu s příslušnými prováděcími akty.
- **Správa** bude odpovídat za činnost QES Provider

SSSVD

SPRÁVA STÁTNÍCH SLUŽEB VYTVÁŘEJÍCÍCH DŮVĚRU

EUDIW – plánovaný harmonogram SSSVD

- Harmonogram budování státní části EUDIW v rámci odpovědností SSSVD:
  - Q1 2025 – Popis certifikačních procesů v rámci ekosystému státní části EUDIW
  - Q2 2025 – Studie proveditelnosti a návrh implementace služeb poskytovaných SSSVD v prostředí státní části EUDIW
  - Soutěž na vytvoření testovacího a integračního prostředí pro ověření
  - Q3 2025 – Vytvoření testovacího a integračního prostředí pro ověření rozhraní realizovaného technického řešení státní části EUDIW
  - Soutěž na implementaci a provoz certifikačních služeb pro ekosystém
  - Q4 2025 - 2026 – Implementace a provoz certifikačních služeb pro ekosystém EUDIW v České republice - vybudování ekosystému certifikačních služeb.
  - Konec roku 2026 - spuštění EUDIW společně s DIA.

SSSVD

SPRÁVA STÁTNÍCH SLUŽEB VYTVÁŘEJÍCÍCH DŮVĚRU

Projekt 2FA a podpora resortu MV ze strany SSSVD

- Cílem projektu 2FA zvýšení KB rozšířením dvoufaktorové autentizace uživatelů k informačním systémům prostřednictvím kontaktní části čipové karty/služebního průkazu zaměstnance včetně vytvoření kvalifikovaného elektronického podpisu a použití bezkontaktní části čipové karty pro přístupové systémy.

- Projekt 2FA je realizován v resortu Ministerstva vnitra (MV, PČR a HZS) s využitím hybridních čipových karet HID pro všechny uživatele.

- **Projekt využívá certifikáty a služby Národní CA (NCA)**

- Projekt je rozdělen do dvou fází
  - I. fáze (MVČR) se dokončuje

    (6 tis. nových karet vybavených certifikáty NCA)
  - II. fáze (PČR a HZS) – 2024 až 2025

    (148 tis. nových karet vybavených certifikáty NCA

- Po ukončení projektu bude podporu certifikátů NCA u cca. 200 operátorů RA2FA a 154tis. uživatelů zajišťovat SSSVD

SSSVD

SPRÁVA STÁTNÍCH SLUŽEB VYTVÁŘEJÍCÍCH DŮVĚRU

Shrnutí důležitých kroků a legislativy

- **Uzavření Memoranda s DIA o spolupráci mezi Digitální a informační agenturou a Správou státních služeb vytvářejících důvěru při zajišťování funkcionalit ekosystému evropské peněženky digitální identity.**
  - Strany uzavřely toto memorandum za účelem spolupráce na zajištění komponent ekosystému EUDIW dle eIDAS a dle všech relevantních prováděcích předpisů, včetně národních implementačních právních předpisů, a to i těch, které vstoupí v platnost a nabydou účinnosti až po podpisu tohoto Memoranda.
- Revize nařízení eIDAS
  - https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=CELEX%3A52021PC0281
- Návrh nového ZOKB
  - https://odok.cz/portal/veklep/material/ALBSCSSFKU7S/
- SSSVD je základem důvěry v elektronickém světě
  - https://sssvd.gov.cz/
  - https://www.narodni-ca.cz/

SSSVD

SPRÁVA STÁTNÍCH SLUŽEB VYTVÁŘEJÍCÍCH DŮVĚRU

Zkratky

- CA – Certifikační autorita
- CRL – seznam zneplatněných certifikátů (certificate revocation list)
- ECC – novější metoda šifrování pomocí eliptických křivek
- EIDAS - Evropský standard pro elektronickou komunikaci (electronic Identification, Authentication and Trust Services)
- EUDIW - Evropská peněženka digitální identity (EU Digital information wallet)
- EWALLET – elektronická peněženka
- LTA – služba pro dlouhodobé uchování el. Dokumentů (Long Term Archiving)
- QWAC – Kvalifikovaný certifikát pro webové stránky (qualified website authentication certificate)
- RA2FA – Registrační autorita pro projekt dvou faktorová autentizace
- RSA – metoda šifrování
- TSA IZOL - služba razítek a vzdáleného pečetění dokumentů v prostředí izolovaných sítí klientů

DĚKUJI ZA VAŠI POZORNOST