SSSVD – ZÁKLAD DŮVĚRY

ROK INFORMATIKY 2024

TELČ 12. – 14. června 2024

Správa státních služeb
vytvářejících důvěru

NÁRODNÍ CERTIFIKAČNÍ AUTORITA

Program

1. Představení stavu vytváření úřadu SSSVD
2. Převod služeb SZR – SSSVD – jak to probíhalo
3. Hlavní priority 2024 – provoz, rozvoj a legislativa
4. Projekt 2FA – pozice SSSVD
5. Diskuse, ukončení

1. Vytváření úřadu SSSVD

- 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 k 1.1.2024 bylo řízeno 5ti kmenovými zaměstnanci, k dnešnímu dni má SSSVD 10 kmenových zaměstnanců.
- Sídlo úřadu bude stále oficiálně Praha 3 Na Vápence, ale pracoviště se přesunulo do Zelenče – NDC SPCSS Zeleneč
- SSSVD má definováno zákonem č. 297/2016 S., o službách vytvářejících důvěru v §14 odst. (4):
  Předmětem činnosti Správy je poskytování služeb vytvářejících důvěru pro potřeby České republiky.

1. Vytváření úřadu SSSVD – externí vlivy

- PERSONÁLNÍ ZDROJE – nábor zaměstnanců do státní příspěvkové organizace musí respektovat nejvyšší průměrný plat – lidé se nám „nehrnou“.
- FINANČNÍ ZDROJE – zatím pouze hlavní činnosti, tedy zdrojem je pouze příspěvek zřizovatele. Nyní se schvaluje nová verze STATUTu pro možnost „výdělku“, v budoucnosti počítáme s vedlejšími činnostmi.
- LEGISLATIVA – známe novou legislativu eIDAS2 a NIS2, která přinese hodně požadavků na změny, bude nás tlačit čas na implementaci požadavků. Změny českých zákonů jako je ZOSVD (297/2016 Sb.) a nový ZOKB.

1. K čemu a jaký certifikát použít?

	Fyzická osoba	OSVČ	Firma (komerční subjekt)	Státní instituce, úřad
Komerční osobní certifikát	✓	✓	✗	✗
Kvalifikovaný certifikát pro el. podpis	✓	✓	✗	✗
Komerční technologický certifikát	✗	✗	✓	✓
Kvalifikovaný certifikát pro el. pečeť	✗	✗	✓	✓

NÁRODNÍ CERTIFIKAČNÍ AUTORITA

1. Jaké druhy podpisů mohu vytvořit?

	Jaký prostředek používám	Obstojnost v rámci právního napadení	Soukromě nebo interně ve společnosti	Mezi společnostmi navzájem	Bezpečný, když neznáme protistranu	Komunikace s úřady v České republice	Komunikace s úřady v rámci celé EU
Prostý elektronický podpis	Obrázek s naskenovaným vlastnoručním podpisem, nebo potvrzení obchodních podmínek na webu.	✗	✗	✗	✗	✗	✗
Zaručený elektronický podpis	Použití osobního komerčního certifikátu, ten však nemusí splňovat žádné speciální náležitosti a může tedy být vydán jakoukoliv certifikační autoritou.	✗	✓	✗	✗	✗	✗
Zaručený elektronický podpis založený na kvalifikovaném certifikátu	Použití kvalifikovaného certifikátu pro elektronický podpis, který je vydán kvalifikovaným poskytovatelem služeb vytvářejících důvěru a nemusí být uložen na certifikovaném zařízení.	✓	✓	✓	✓	✓	✗
Kvalifikovaný elektronický podpis	Použití kvalifikovaného certifikátu pro elektronický podpis, který je vydán kvalifikovaným poskytovatelem služeb vytvářejících důvěru a musí být uložen na certifikovaném zařízení (čipová karta).	✓	✓	✓	✓	✓	✓

2. PŘEVOD SLUŽEB NA (STARO)NOVOU NCA

Činnost	ETAPA I
1	Aktualizace směrnice „Ukončení činnosti služeb CA, TSA NCA“ a zpracování „Plánu uko pro
2	Uza zaj
3	Akt slu

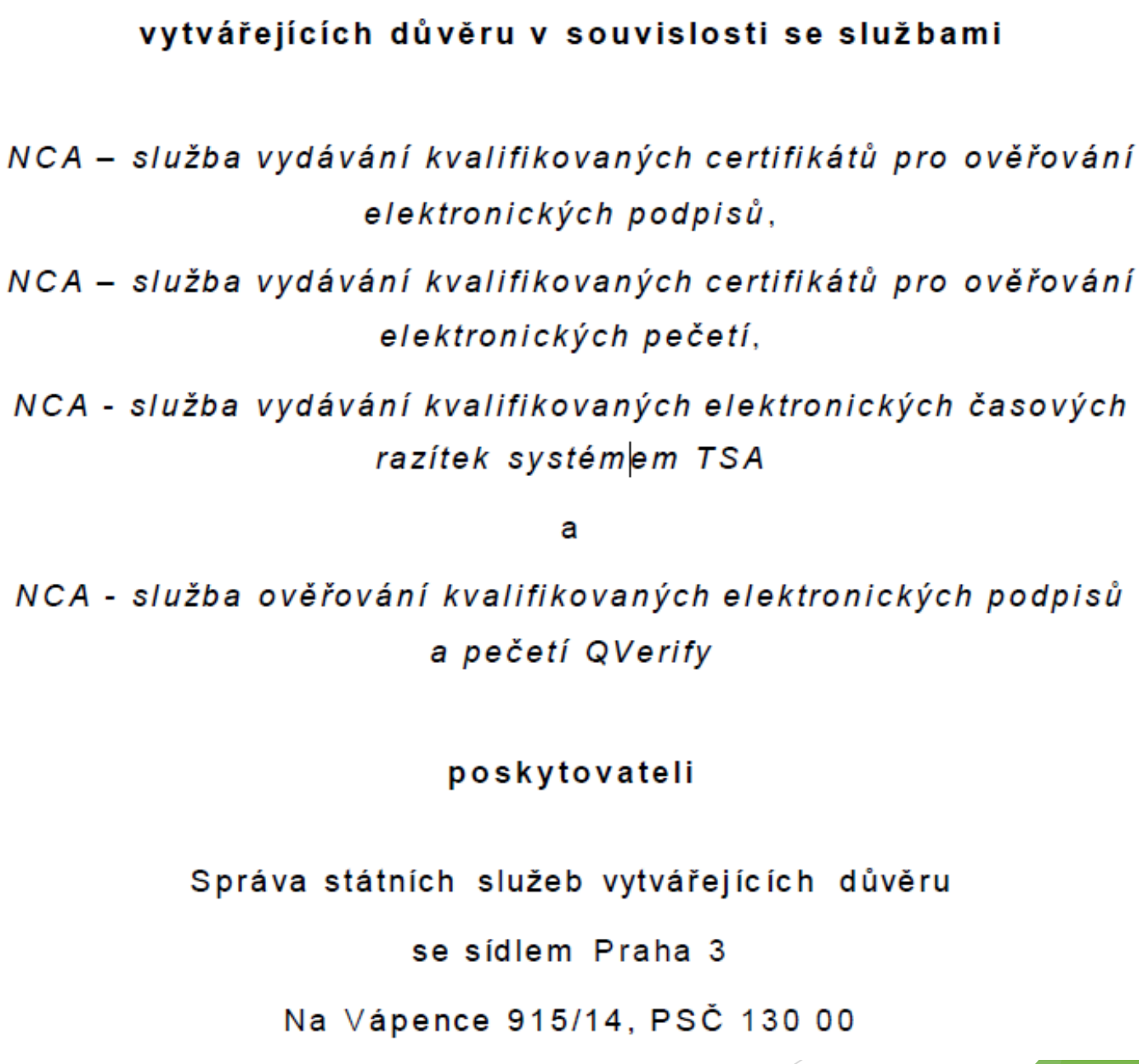
Činnost	ETAPA I
4	Vygenerování párových dat, vydání certifikátů veřejných klíčů kořenových a mezilehlých certifikačních autorit (kryptografie RSA i ECC) v PREPROD prostředí
5	Vygenerování párových dat, vydání certifikátů veřejných klíčů časových autorit TSU v Pl
6	Vyg pro
7	Dist vyb
8	Akt pro
9	Zaj vyb

Činnost	ETAPA III
10	Zpracování Analýzy rizik NCA, protože NCA je VIS dle ZoKB
11	Vygenerování párových dat, vydání certifikátů veřejných klíčů kořenových a mezilehlých certifikačních autorit (kryptografie RSA i ECC) v PROD prostředí
12	Vygenerování párových dat, vydání certifikátu pro službu ověřování podpisu v PROD prostředí
13	Oznámení změny v poskytování kvalifikovaných služeb DIA, audit DIA, správní rozhodnutí a zápis certifikátů a poskytovatele do TL
14	Vygenerování párových dat, vydání certifikátů veřejných klíčů časových autorit TSU v PROD prostředí (17 lokalit, v každé 2 instance + on-line služby (2 instance)), vytvoření profilů, konfigurace profilů, profylaxe, odstranění privátních klíčů předchozích certifikátů
15	Zajištění přístupů do chráněných zón BS, instalace root a mezilehlých certifikátů včetně služby ověřování podpisu na BS a v centru NCA do PROD prostředí (deblokace schváleného certifikátu TSU, blokace a odstranění privátních klíčů předchozích certifikátů)

NÁRODNÍ CERTIFIKAČNÍ AUTORITA

2. Převod s

- Audit společnosti T
- V říjnu 2023 byly certifikátů
  - Služba vydávání
  - Služba vydávání
  - Služba vydávání
  - Služba ověřován
- Začátkem listopadu vytvářejících důvěr
- **Služby byly zapsá**
- **Spuštěn web** naro



uděluje se kvalifikovaný status poskytovatele služeb vytvářejících důvěru v souvislosti se službami

NCA – služba vydávání kvalifikovaných certifikátů pro ověřování elektronických podpisů,

NCA – služba vydávání kvalifikovaných certifikátů pro ověřování elektronických pečetí,

NCA - služba vydávání kvalifikovaných elektronických časových razítek systémem TSA

a

NCA - služba ověřování kvalifikovaných elektronických podpisů a pečetí QVerify

poskytovateli

Správa státních služeb vytvářejících důvěru

se sídlem Praha 3

Na Vápence 915/14, PSČ 130 00

3. Hlavní priority 2024 - stručně

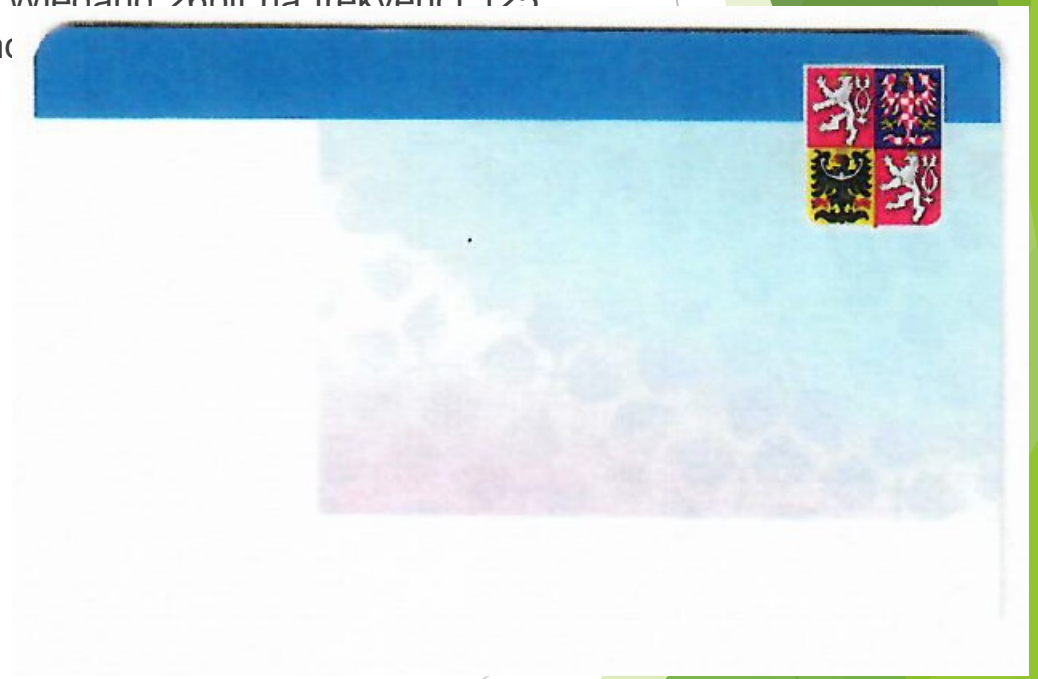
- Přechod na silnější kryptografii na základě Technického standardu (Algopaper) ETSI TS 119 312 u TSA certifikátů na 4K klíče RSA-PSS a u certifikátů koncových uživatelů na ECC 384 dle NIST od ledna 2025.
- NIS2 a nový ZOKB (určený systém) - mnoho změn v oblasti zajišťování kybernetické bezpečnosti
- Implementace EIDAS2 – EUDIW a Atributová CA
- Podílení se na projektu 2FA – bezpečný partner státu

3. Hlavní priority 2024+

- Příprava řešení ověřovacího provozu EUDIW s využitím infrastruktury a procesů NCA
- Podpora certifikátů založených na ECC při vytváření kvalifikovaných elektronických pečetí
- Vydávání prvotních certifikátů na dálku s využitím Portálu národního bodu pro identifikaci a autentizaci
- Vzdálené pečetění/podepisování jako kvalifikované služby
- Výměna 33 ks HSM QSCD nShield Connect 1500+CC za typ HSM Entrust nShield 5c (nové technické normy 419 221-5 - pro HSM a 419 241-2 - pro SAM), výměna HW NCA po 6-7 letech (zvýšené náklady na maintenance)
- Pro podřízené domény jednotlivých úřadů v doméně .gov.cz jsou nyní používány certifikáty pro autentizaci internetových stránek vydávané autoritami ze zemí mimo EU. Pro zajištění důvěryhodnosti v souvislosti s revizí nařízení eIDAS, která klade důraz na nezávislost na autoritách mimo EU, SSSVD vybuduje podřízenou CA vydávající kvalifikované certifikáty pro autentizaci internetových stránek QWAC (RSA i ECC).
- Optimalizace infrastruktury – 2. lokalita
- Zajištění služby LTA (long-term-archival) pro BS, která ošetří dokumenty před archivací tak, aby je bylo možné dlouhodobě ověřovat a správně archivovat
- Rozvojové požadavky BS

4. Projekt 2FA

- Jedná se o projekt dvoufaktorové identifikace pro resort Ministerstva vnitra s využitím hybridních čipových karet HID
  - dva bezkontaktní čipy (vysokofrekvenční čip na frekvenci 13,56 MHz dle ISO/IEC 14443, typ A, bezpečnostní mód iClass Seos a nízkofrekvenční čip ISO 30+ s Wiegand 26bit na frekvenci 125 kHz technologie Indala FlexPass, formát záznamu Indala Wiegand
  - Kontaktní čip Starcos 3.7 eIDAS C1
- Certifikáty a služby NCA
- Projekt je rozdělen do dvou etap
- I. etapa (MVČR) se dokončuje (3000 nových karet)
- II. etapa (PČR a HZS) – 2024 až 2025



4. Projekt 2FA

- Dodávka embeddingu a inicializace kontaktního čipu Starcos 3.7 eIDAS C1 do 6.000 ks čipových karet HID specifikace:
  - Karty budou opatřeny základním vzorovým potiskem pro příslušné role (zaměstnanec ve služebním poměru/v pracovním poměru …)
  - Karty budou obsahovat ochranné prvky ve formě hologramu a další
  - Budou obsahovat vysokofrekvenční čip na frekvenci 13,56 MHz dle ISO/IEC 14443, typ A, bezpečnostní mód iClass Seos
  - Dále nízkofrekvenční čip ISO 30+ s Wiegand 26bit na frekvencí 125kHz technologie Indala FlexPass, formát záznamu Indala Wiegand 26
  - Tloušťka karet bude v souladu s technickými normami ISO/IEC 7810 a ISO/IEC 7816-2 a bude činit 0,76 mm +-0,03 mm (5 vrstev: uprostřed prelaminát s bezkontaktními čipy, po obou stranách PVC a vnější vrstvy z PC).
- I.CA (resp. STC) zajistí vyfrézování a vlepení (embedding) kontaktního PKI čipu Starcos 3.7 eIDAS C1 do těla karty a dále nahrání interní struktury do čipu.

4. Projekt 2FA

- II. etapa (rozšíření pro PČR a HZS):
  - 133 tis. karet s kontaktním čipem
  - 30 tis. karet bez kontaktního čipu
  - 124 tis. čteček čipových karet
  - Implementace CMS 2FA do prostředí PČR a HZS
  - Vydání certifikátů uživatelům
  - Prostřednictvím výjezdů Mobilní registrační autority vydá I.CA určeným zaměstnancům/pracovníkům MVČR certifikáty na dodané čipové karty, tj. včetně generování žádosti. Žadatel musí disponovat a operátorovi předložit 2 doklady totožnosti (OP a druhý doklad = pas, ŘP, služební průkaz MV…) pro QC a jeden pro KC.

Shrnutí legislativy a důležité odkazy

- 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 aneb 3SVD je základem důvěry v elektronickém světě
  - https://sssvd.gov.cz/
  - https://www.narodni-ca.cz/

NÁRODNÍ CERTIFIKAČNÍ AUTORITA

5. Diskuse, ukončení

DĚKUJI ZA VAŠÍ POZORNOST
MICHAL PEŠEK