ČESKÁ TECHNICKÁ NORMA

ICS 35.100.30 **Prosinec 2009**

ČSN 36 9791

Informační technologie – Protokol pro správu klíčů Národní ověřovací certifikační autority používaný SPOC

Information technology – Country Verifying Certification Authority Key Management Protocol for SPOC

Technologies de I,information – Protocole d,échange de clés CVCA par un point unique de communication

Informationstechnik – Protokoll für SPOC zur Verwaltung von Schlüsseln der Country Verifying Certification Autority

Obsah

Strana

Úvod 3

1 Předmět normy 4

2 Citované normativní dokumenty 4

3 Termíny a definice 4

4 Zkratky 4

5 Přehled 5

6 Jednotné kontaktní rozhraní (SPOC) 6

6.1 Iniciální registrační informace SPOC 6

7 Zprávy 7

7.1 RequestCertificate 7

7.2 SendCertificates 8

7.3 GetCACertificates 9

7.4 GeneralMessage 9

8 Webové služby 10

8.1 Použití SOAP 10

8.2 Bezpečnostní úvahy 10

9 Manuální kanál 11

9.1 Formát média a jmenné konvence 11

9.2 Metadata 11

9.3 Bezpečnostní úvahy 12

10 PKI pro interní bezpečnost SPOC 12

10.1 Profily certifikátu SPOC 12

11 Definice WSDL pro rozhraní webových služeb 14

12 Přiřazení OID 17

Bibliografie 18

Úvod

Strojově čitelné dokumenty (MRTD, e-cestovní doklady) podporují pro ochranu uložených dat pokročilé bezpečnostní mechanismy. Jedním z těchto mechanismů je tzv. Extended access control (EAC). Jestliže jsou data uložená v MRTD chráněna tímto mechanismem, musí být ověřovací terminál autentizován vůči MRTD a musí před přístupem k jeho datům prokázat své právo přístupu k nim. EAC spolu s dalšími pokročilými bezpečnostními mechanismy jsou popsány v [BSI-EAC].

Terminálová autentizace provedená před čtením chráněných dat z MRTD je založena na tzv. ověřovacích certifikátech (CV), které mohou být ověřovány pomocí MRTD. Přístupová práva daná ověřovacímu terminálu jsou zakódována v tomto certifikátu. Po ověření CV certifikátu MRTD udělí terminálu práva přístupu ke svým datům vzhledem k právům zakódovaným v CV certifikátu. Infrastruktura veřejného klíče pro generování a distribuci CV certifikátů je nastíněna v [BSI-EAC]. Tato EAC-PKI bude vytvořena ve všech členských státech EU. Společná certifikační politika pro entity EAC-PKI je prezentována v [EUCP].

Uvnitř svého EAC_PKI provozuje každý stát svou kořenovou certifikační autoritu, tzv. národní ověřovací certifikační autoritu (CVCA). Druhá úroveň tohoto PKI je tvořena certifikačními autoritami nazvanými „kontrolní jednotka“ (Dokument verifier – DV). Každá DV je propojena s CVCA dané země. DV dostává své certifikáty od národní nebo cizí CVCA a generuje certifikáty pro jí podřízené inspekční systémy (IS). Z tohoto pohledu jsou inspekční systémy koncovými držiteli řetězce certifikátů EAC-PKI.

1 Předmět normy

Tento dokument specifikuje protokol správy klíčů v mezistátních operacích mezi komponentami

architektury EAC: Národními ověřovacími certifikačními autoritami (CVCA) a Národními kontrolními jednotkami (DV).

Tento protokol se používá pro výměnu klíčů a certifikátů pro:

- DV může odeslat žádost o certifikát cizí CVCA
- CVCA může odeslat vydaný certifikát žádající DV
- DV a CVCA může žádat o seznam platných certifikátů (řetězec certifikátů) nezbytných pro čtení e-cestovních dokladů vydaných s pomocí cizí CVCA
- Entity EAC-PKI si vyměňují obecné zprávy

Tato specifikace definuje pro výměnu dat následující kanály:

- Manuální výměna dat uložených na přenositelném médiu (CD-R,DVD+/-R, USB úložiště) nebo publikace na internetu
- Rozhraní webové služby

Tato specifikace se nezabývá:

- Interní výměnou dat a komunikací uvnitř státu (domácí DV – domácí CVCA, IS – DV)
- Výměnou dat spojenou s iniciálním registračním procesem vyjma určení formátu dat (formát média, obsah metadat).