ČESKÁ TECHNICKÁ NORMA

ICS 35.100.30

Prosinec

2018

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

ČSN 36 9791

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

Nahrazení předchozích norem

Touto normou se nahrazuje ČSN 36 9791 z prosince 2009.

Obsah

Strana

Předmluva

Změny proti předchozí normě

Text normy byl proti předchozímu vydání doplněn a upraven v souladu s nejnovější používanou technologií.

Patentová práva

Upozorňuje se na možnost, že některé prvky tohoto dokumentu mohou být předmětem patentových práv. ÚNMZ nelze činit odpovědným za identifikaci jakéhokoliv nebo všech patentových práv.

Vypracování normy

Zpracovatel: Ing. Jiří Děcký, Ministerstvo vnitra ČR, IČO 7064

Technická normalizační komise: TNK 42 Výměna dat

Pracovník České agentury pro standardizaci: Ing. Miroslav Škop

Česká agentura pro standardizaci je státní příspěvková organizace zřízená Úřadem pro technickou normalizaci, metrologii a státní zkušebnictví na základě ustanovení § 5 odst. 2 zákona č. 22/1997 Sb., o technických požadavcích na výrobky a o změně a doplnění některých zákonů, ve znění pozdějších předpisů.

Úvod

Elektronické strojově čitelné cestovní doklady (eMRTD) podporují pro ochranu dat, uložených na čipu e-cestovního dokladu, pokročilé bezpečnostní mechanismy. Jedním z těchto mechanismů je tzv. Extended Access Control (EAC) – rozšířené řízení přístupu. Jestliže jsou data uložená v eMRTD chráněna EAC, musí být ověřovací terminál autentizován pomocí eMRTD a musí před získáním přístupu prokázat eMRTD své právo přístupu k těmto chráněným datům. EAC spolu s dalšími pokročilými bezpečnostními mechanismy jsou popsány v [BSI-EAC].

Terminálová autentizace (TA) provedená před čtením chráněných dat z MRTD je založena na tzv. verifikačních certifikátech (CV), které mohou být verifikovány pomocí eMRTD. Přístupová práva daná verifikačnímu terminálu jsou zakódována v tomto certifikátu. Po verifikaci CV certifikátu eMRTD 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 verifikační certifikační autoritu (CVCA). Druhá úroveň tohoto PKI je tvořena certifikačními autoritami nazvanými „kontrolní jednotka“ (Document Verifier – DV). Každá DV je propojena s CVCA dané země. DV dostává své certifikáty od domácí nebo cizích 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 definuje požadavky a doporučení týkající se zřízení SPOC a jeho interakcí s dalšími SPOC tak, aby:

– Entity EAC-PKI si mohly vyměňovat obecné zprávy;

– DV mohla odeslat žádost o certifikát cizí CVCA;

– CVCA mohla odeslat vydaný certifikát žádající DV;

– DV a CVCA mohly žádat o seznam certifikátů (řetězec certifikátů) nezbytných pro čtení e-cestovních dokladů vydaných s pomocí cizí CVCA.

Tato specifikace definuje pro výměnu dat následující kanály:

– Rozhraní webových služeb.

Tato specifikace se nezabývá:

– Interní výměnou dat a komunikací uvnitř státu (domácí DV – domácí CVCA, IS – DV);

– Výměnou dat spojenou s iniciálním registračním procesem. Registrační proces je pokryt [EUCP].