Certifikačné autority pre elektronické doklady

Elektronické identifikačné doklady obsahujú citlivé údaje. Prístup k týmto údajom a ich integrita sú zabezpečené digitálnymi certifikátmi. Tie sú vydávané a manažované certifikačnou autoritou (CA), ktorá je jadrom PKI infraštruktúry.

Softvérový balík pre certifikačné autority poskytuje technické riešenia:

- Národná certifikačná autorita pre podpisovanie (CSCA) na vydávanie certifikátov pre podpisovanie dokumentov (Document Signer - DS)
- Národná certifikačná autorita pre overovanie (CVCA) a Certifikačná autorita pre overovanie dokumentov (DVCA) na vydávanie Card Verifiable certifikátov (CVC)

Národná certifikačná autorita pre podpisovanie (CSCA)

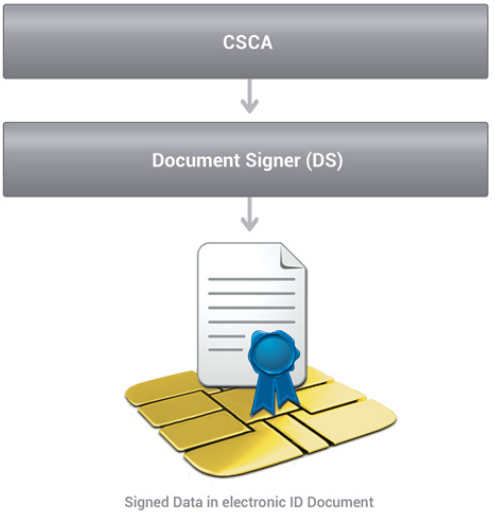
DS certifikáty sú používané na ochranu integrity dát uložených na elektronických dokladoch, akými sú napr. eID, eDoPP, elektronický pas, eVRC.

Kľúčové vlastnosti

- DS certifikáty vo formáte X.509
- Podpora všetkých používaných asymetrických šifrovacích algoritmov – RSA, DSA a ECDSA
- Podpora pre HSM
- Certificate Management Protocol (CMP)
- Simple Certificate Enrollment Protocol (SCEP)
- Certificate Revocation Lists (CRLs)
- Online Certificate Status Protocol (OCSP)

Hlavné výhody

- Úplné technické riešenie CSCA pre vydávanie DS certifikátov



Signed Data in electronic ID Document

Plaut Slovensko, s.r.o.

Karloveská 34, 841 04 Bratislava
Slovenská Republika

Tel.: + 421 2 3215 1411
Fax: + 421 2 3215 1412

E-mail: info@plaut.sk
Web: www.plaut.sk

Národná certifikačná autorita pre overovanie (CVCA) a Certifikačná autorita pre overovanie dokumentov (DVCA)

CV certifikáty umožňujú terminálom inšpekčnej infraštruktúry (polícia, hraničná kontrola) alebo terminálom poskytovateľov služieb pristupovať k dátam bezpečne uloženým na čipe elektronického dokladu – napríklad eID, eDoPP alebo elektronický pas.

Čip elektronického dokladu implementuje mechanizmus kontroly prístupu (podľa technickej smernice BSI TR-03110), povoľujúci prístup len terminálom, ktoré sa preukážu terminálovým CV certifikátom s príslušnými oprávneniami pre prístup k údajom uloženým na doklade.

Infraštruktúra PKI potrebná pre vydávanie a overovanie certifikátov terminálu je trojvrstvová PKI (nazývaná tiež EAC-PKI) pozostávajúca z nasledujúcich entít:

- Národné certifikačné autority pre overovanie (CVCAs)
- Certifikačné autority pre overovanie dokumentov (Document Verifiers)
- Terminály

Poskytované technické riešenie obsahuje:

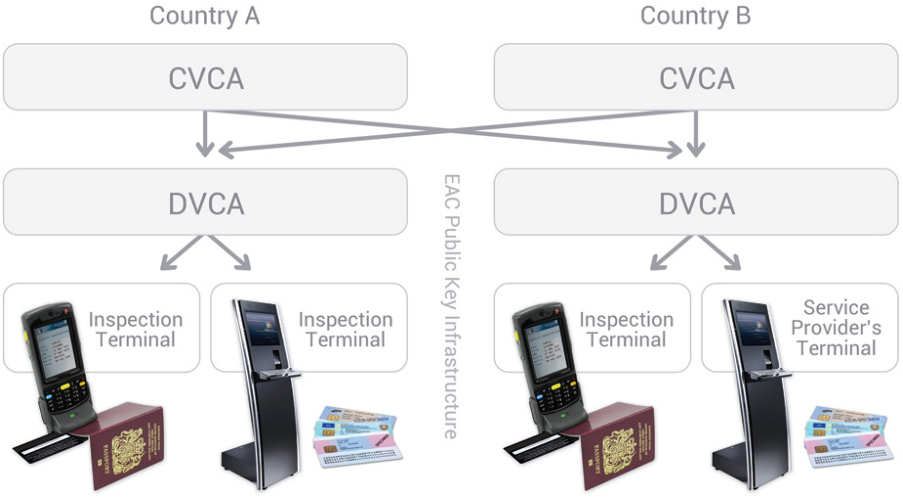
- Národná certifikačná autorita pre overovanie (Country Verifying Certificate Authority - CVCA) na vydávanie certifikátov pre DVCA (DV certifikátov)
- Certifikačná autorita pre overovanie dokumentov (Document Verifier Certificate Authority -DVCA) na vydávanie certifikátov terminálom (terminálových certifikátov)

Kľúčové vlastnosti

- EAC PKI pre elektronické pasy, eID a eDoPP
- CV certifikáty vo formáte podľa BSI TR 03110
- Podpora pre všetky používané asymetrické šifrovacie algoritmy – RSA, DSA, ECDSA
- Podpora pre HSM
- Integrácia so SPOC – Single Point of Contact medzi krajinami

Hlavné výhody

- Úplné technické riešenie EAC-PKI infraštruktúry poskytujúce služby na vydávanie CV certifikátov terminálom pre prístup k citlivým dátam uloženým na čipe elektronického dokladu
- Vydávanie CV certifikátov umožňujúcich prístup k elektronickým dokladom vydaných v zahraničí (SPOC)



Plaut Slovensko, s.r.o.
Karloveská 34, 841 04 Bratislava
Slovenská Republika
Tel.: + 421 2 3215 1411
Fax: + 421 2 3215 1412
E-mail: info@plaut.sk
Web: www.plaut.sk