Certification Authority Solutions for eID Documents

Electronic documents contain sensitive data. Access to these data and their integrity is secured by digital certificates. These certificates are issued and managed by Certificate Authority (CA) which is a core part of the Public Key Infrastructure (PKI) for digital certificates.

Certificate authority software package provides a technical solution of

- Country Signing Certification Authority (CSCA) to issue Document Signer (DS) certificates
- Country Verifying and Document Verifier Certificate Authorities (CVCA and DVCA) to issue Card Verifiable certificates (CVC)

Country Signing Certification Authority (CSCA)

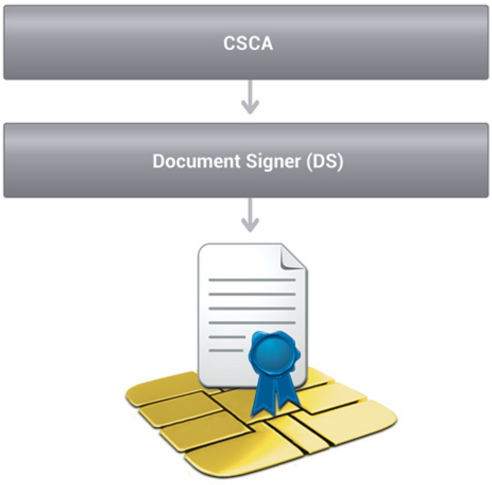
Document Signer (DS) certificates are used to protect the integrity of the data stored in electronic documents, e.g. in eID, eVRC, eRP, ePassport.

Key Features

- DS certificates in format X.509
- Support of all common asymmetric cryptographic algorithms – RSA, DSA and ECDSA
- Support for Hardware Security Modules (HSM)
- Certificate Management Protocol (CMP)
- Simple Certificate Enrollment Protocol (SCEP)
- Certificate Revocation Lists (CRLs) Online Certificate Status Protocol (OCSP)

Main Benefits

- Complete technical solution of Country Signing Certification Authority issuing Document Signer certificates to document issuing authorities



CSCA

Document Signer (DS)

Signed Data in electronic ID Document

Country Verifying and Document Verifier Certificate Authority

Card Verifiable Certificates (CVC) enable terminals of an inspection control infrastructure (police, border control) or terminals of service providers accessing data securely stored in an electronic document's chip – e.g. in ePassport, eID or eRP.

The chip of an electronic document implements an access control mechanism (ref. to the technical guideline BSI TR-03110) allowing access only to terminals having a CV certificate with appropriate permissions specified in it.

The PKI required for issuing and validating terminal certificates is a three tier PKI (often referred to as EAC-PKI) consisting of the following entities:

- Country Verifying CAs (CVCAs)
- Document Verifiers (DVs)
- Terminals

The provided technical solution consists of:

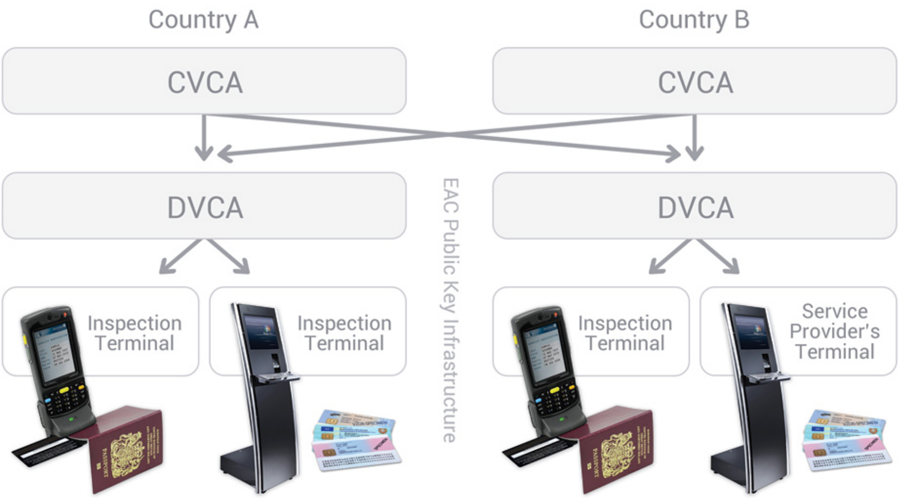
- Country Verifying Certificate Authority (CVCA) for issuing CV certificates to DVCA's
- Document Verifier Certificate Authority (DVCA) for issuing CV certificates to terminals

Key Features

- EAC PKI for ePassports, eIDs and eRPs
- Card verifiable certificates in accordance with BSI TR 03110
- Support of all common asymmetric cryptographic algorithms – RSA, DSA and ECDSA
- Support for HSM
- Integration with SPOC - Single Point of Contact between countries

Main Benefits

- Complete technical solution of EAC-PKI infrastructure providing services for issuing CV certificates for terminals in order to enable them accessing sensitive data stored in an electronic document's chip
- Issuing CV certificates allowing access to electronic documents issued by foreign countries (SPOC)


Country A
Country B
CVCA
CVCA
DVCA
DVCA
EAC Public Key Infrastructure
Inspection Terminal
Inspection Terminal
Inspection Terminal
Service Provider's Terminal