EVIDEN

IDnomic ePass PKI

Protect ePassports and traveler biometric data

Electronic and biometric passports are critical sovereign travel documents and require a very high level of protection to guarantee both document authenticity and controlled access to sensitive personal data of the holder. IDnomic ePass PKI is a PKI suite covering all aspects of ePassport security and complies to stringent international standards including interoperability schemes.

The electronic passport has clearly demonstrated to be by far the most successful international eID endeavor at present, with more than 150 out of 193 member countries issuing more than 500 million electronic travel documents (cf. ICAO MRTD Report Q2/2013).

This evolution is based on extensive efforts in standardization and security, allowing to use an ePassport all over the world.

Given ICAO and IATA projections of travel increase, automated verification of ePassports and inspection of traveler biometric data will become crucial.

Within this context, two major challenges arise for the production and inspection of electronic and biometric travel documents:

· Guarantee document's authenticity
· Control access to biometric data

To cover those subjects, ICAO and the EU have issued frameworks of standards which require implementation of Public key Infrastructure (PKI) solutions:

· ICAO Doc9303
· EU TR 03110

IDnomic ePass PKI is a software suite which covers all aspects of ePassport security, from secure production of sovereign electronic travel documents to implementation of trusted digital identities for inspection terminals (IS).

An important place is also given to the interoperability modules, which are fully compliant to stringent international standards.

IDnomic ePass PKI suite enables our customers to deploy their ePassport production and inspection projects with confidence and to rely on strictly compliant and future proof PKI products.

Covering all ePassport PKI use cases

Production
Basic Access Control (BAC)
Supplemental Access Control (SAC)
Passive Authentication (PA)

Inspection
Extended Access Control (AEC)
Terminal Authentication (TA)

Interoperability
ICAO PKD
EU SPOC

EVIDEN

IDnomic ePass PKI – complete, performance oriented and strictly compliant

IDnomic ePass PKI provides all necessary software modules to implement ICAO 9303 and EU TR 03110 part 1 specified and standardized PKI systems including international interoperability. These PKI systems can be deployed separately or combined, thus profiting from shared hardware and software resources and common project management tasks.

Passive Authentication PKI (BAC/SAC)

Terminal Authentication PKI (EAC)
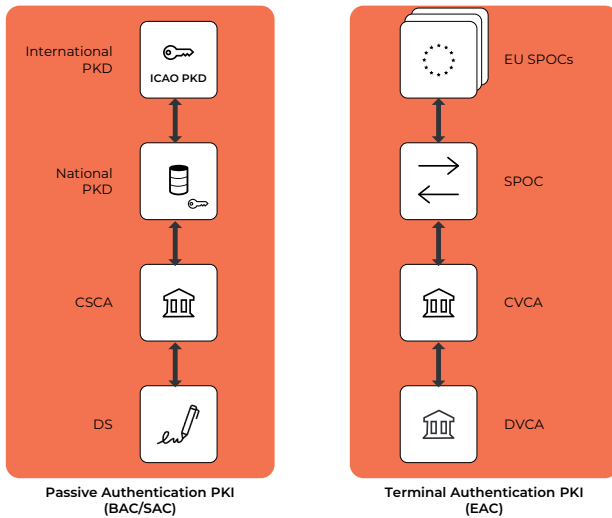
IDnomic ePass PKI suite forBAC/SAC:

- CSCA: Offline Root CA issuing DS certificates
- Document Signer: Signature server, interfacing the production chain
- National PKD (N-PKD): Module interfacing the ICAO Public Key Directory

IDnomic ePass PKI suite for EAC:

- CVCA: Offline Root CA issuing DVCA certificates
- DVCA: Online CA issuing inspection system certificates (IS)
- Single Point of Contact (SPOC): Module interfacing with other SPOC to exchange terminal certificates

Benefits for our customers

- Strictly compliant with international standards from ICAO and EU.
- Highly secure - Common Criteria EAL4+ software modules using CC and FIPS certified HSM
- Flexible solutions – from single server to n-tiers architecture with Disaster Recovery site
- Proven and reliable – deployed project worldwide with all major system integrators
- Multi-tenant design – allowing several separate PKI instances within one deployment

Standards and technical specifications

Conformité et environnements pris en charge

- » X.509v3 and ISO 7816 CVC
- » PKCS#7,8,10,11,12
- » RSA 1024-4096, ECDSA 256-512
- » SOAP/WSDL/XML DSig/XML Enc
- » ICAO Doc9303

- » EU TR 03110 part 1 (travel documents)
- » BSI TR 03139 EU Common Policy for Extended Access Control
- » ETSI TS 101-456
- » Java platform / Linux RHEL / Oracle DB

Find out more about us: www.cryptovision.com

Connect with us

in   🐦   📷   ▶

eviden.com