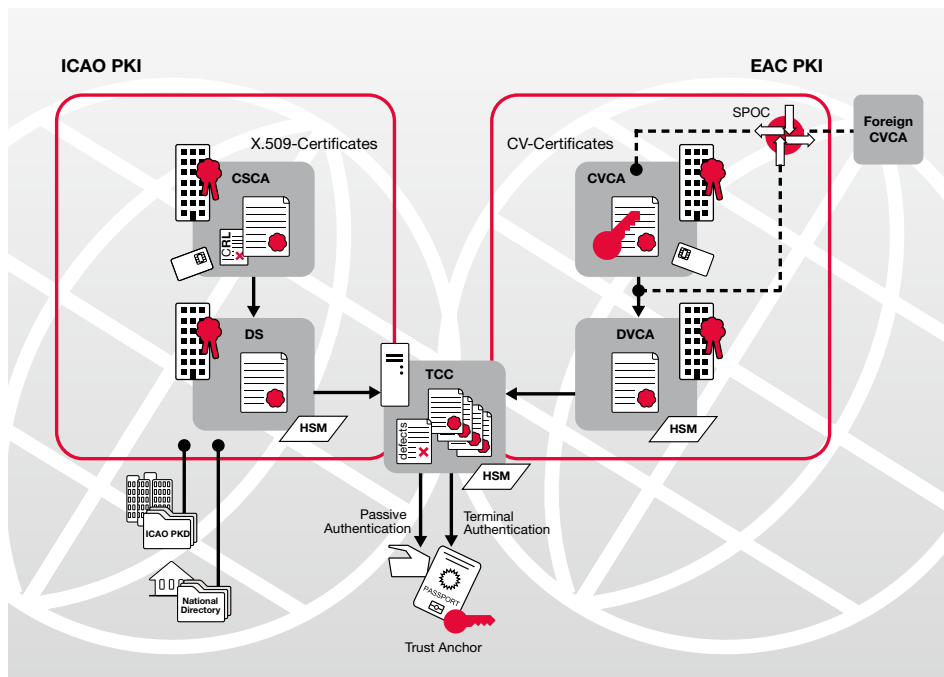


Comprehensive Infrastructure for Identity Documents



Benefits:

- » One solution meets all important eID PKI requirements
- » Flexible in terms of signature components and certificate handling
- » Supports all relevant standards and protocols

Introducing electronic identity documents means in most cases the implementation of biometric data in the document. Just like traditional optical data, this electronic data has to be secured against manipulation and unauthorised access. Usually, this protection is achieved by means of public key infrastructure (PKI) mechanisms. For electronic identity documents, generally two PKIs are needed. **With the eID PKI Suite, secunet worked out a specific PKI solution meeting all the requirements for issuance, infrastructure and control. The design particularly focuses on the international exchange of certificates and other relevant information.**

In the past, requirements for authenticity and data integrity referred to the optical features of ID documents. With the implementation of biometric features, the requirements are now extended to the electronic layer of the document. The International Civil Aviation Organization (ICAO) has therefore published specifications describing security mechanisms to ensure the authenticity and integrity of the electronic data (Document 9303) – by this means, ICAO established a PKI which is referred to as the ICAO PKI.

Only verifiably authorised instances are to have access to the sensitive biometric data in eIDs. Thus, the requirements regarding access control and confidentiality for communication have been specified within the so-called EAC PKI. The EAC PKI describes security mechanisms which allow

an eMRTD to verify an access request all by itself despite its computational restrictions. To get access to eMRTDs from other countries, you have to be equipped with the corresponding rights. To obtain those rights, the countries in the European Union have agreed to accept the Czech Standard CSN 369791:2009 as the common protocol for communication.

Of course, the realisation of such infrastructures is a complex undertaking: different PKIs and the related certificates are used all in one setup for safeguarding eIDs, however they represent different security aspects. secunet has hands-on experience in operating in the field of eIDs in a highly reliable and professional way. Thus, software products have been deduced from previous eID projects – such as the eID PKI Suite – which are “ready-to-implement” for your projects, too.

EAC PKI

Extended Access Control provides security mechanisms to ensure that only authorised instances and readers get access to specific eID data. Therefore, a secure communication has to be established (BAC|PACE) and access to sensitive data is granted to an Inspection System (IS) if a certificate with sufficient entitlements is available for the mechanism of Terminal Authentication. A technical infrastructure is required to provide a valid certificate chain for the entitlementments.

Due to their very short validity, handling of Certificate Revocation Lists (CRLs) is not necessary. The three-layered infrastructure consists of a national trust anchor (CVCA) that is connected via a centralised interface called "SPOC" to the issuer (DVCA) of CV-certificates for the Inspection System. An IS can be realised by following either an integrated or distributed approach. In the latter case, a Terminal Control Centre (TCC) offers a central unit that connects distributed readers.

ICAO PKI

Authenticity and integrity of an eID can be checked by the verification of the electronic signature of the eID data. ICAO has introduced the mechanism which is used for this validation check: Passive Authentication. A complete PKI with the Country Signing Certificate Authority (CSCA) as the national trust anchor and the Document Signer as document manufacturer has to be provided. The exchange of the certificate data can be processed via the ICAO-PKD, a global and up-to-date directory, and a national directory.

Good arguments for secunet's eID PKI Suite

secunet has developed software products in previous eID projects which are "ready-to-implement" for your projects, too. Together with the ePassportAPI, secunet covers the important requirements regarding the various PKIs. The product range comprises components for application in the ICAO PKI field such as CSCA and DS services and components which fulfil the requirements of the EAC PKI, like CVCA and DVCA services. Here is a short overview for you:



secunet offers a Country Verifying Certification Authority that generates the first two necessary Card Verifiable-certificates of a valid certificate chain for Terminal Authentication based on valid certificate requests: root and DVCA certificates. Secure storage of asymmetric key pairs, certificates and the provision of electronic signatures are available – this key feature of the CVCA is realised by the integration of HSMs or smartcards.



As a centralised interface the Single Point of Contact allows certificate exchange on international and national level; according to CSN 369791:2009 respectively to the technical guideline BSI-TR-03129. secunet's solution covers both communication parts based on secure communication via TLS. Thus, the TLS CA powered by secunet issues client and server certificates for the web services by supporting RSA and elliptic curve keys. As a special feature secunet provides a SPOC test system.



secunet's Document Verifying Certification Authority offers all functionalities to generate and provide DVCA certificate requests to the corresponding CVCA, even with interface for the according SPOC. IS certificate requests can be received, checked and, if correct, be issued by the DVCA. For certificate and key storage, functionality to sign the certificate requests and the issuance of IS certificates a secure storage is essential. DVCA from secunet therefore supports the integration of HSMs.



The Terminal Control Centre is a centralised approach of an IS that allows connection of various distributed readers. The TCC solution from secunet supports different application scenarios for BAC and EAC protected documents (Basic and Extended Identity Check). A secure centralised certificate storage and/or secure centralised key storage are part of the solution allowing the TCC to take over the authentication procedure for permitted readers. For Passive Authentication, the TCC imports CSCA certificates from the Master List and known defects from the Defect List.



The Country Signing Certification Authority is the trust anchor for protected eIDs: It generates root certificates, receives and checks DS certificate requests, and issues DS certificates and CRLs in order to enable genuineness checks. The CSCA software permits integration of a HSM or smartcard to provide signature generation for Passive Authentication.



The Document Signer software allows easy management of DS certificates. Based on the valid DS key pair the security object (SOD) including the hash values of all data groups of an underlying eID can be signed. Integration of a HSM or smartcard is available.

More information:
www.secunet.com/en/eID

secunet

secunet Security Networks AG
 Kronprinzenstraße 30
 45128 Essen, Germany

Phone: +49-201-5454-0
 Fax: +49-201-5454-1000
 E-mail: info@secunet.com
www.secunet.com