secunet
eID PKI Suite

Public Key Infrastructures

For Modern Identity Documents

With the eID PKI Suite, secunet offers its standard PKI, tailored to meet all the requirements for issuance, infrastructure and control. The design particularly focuses on the international exchange of certificates and other relevant information.

Introducing electronic identity documents in most cases means 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.

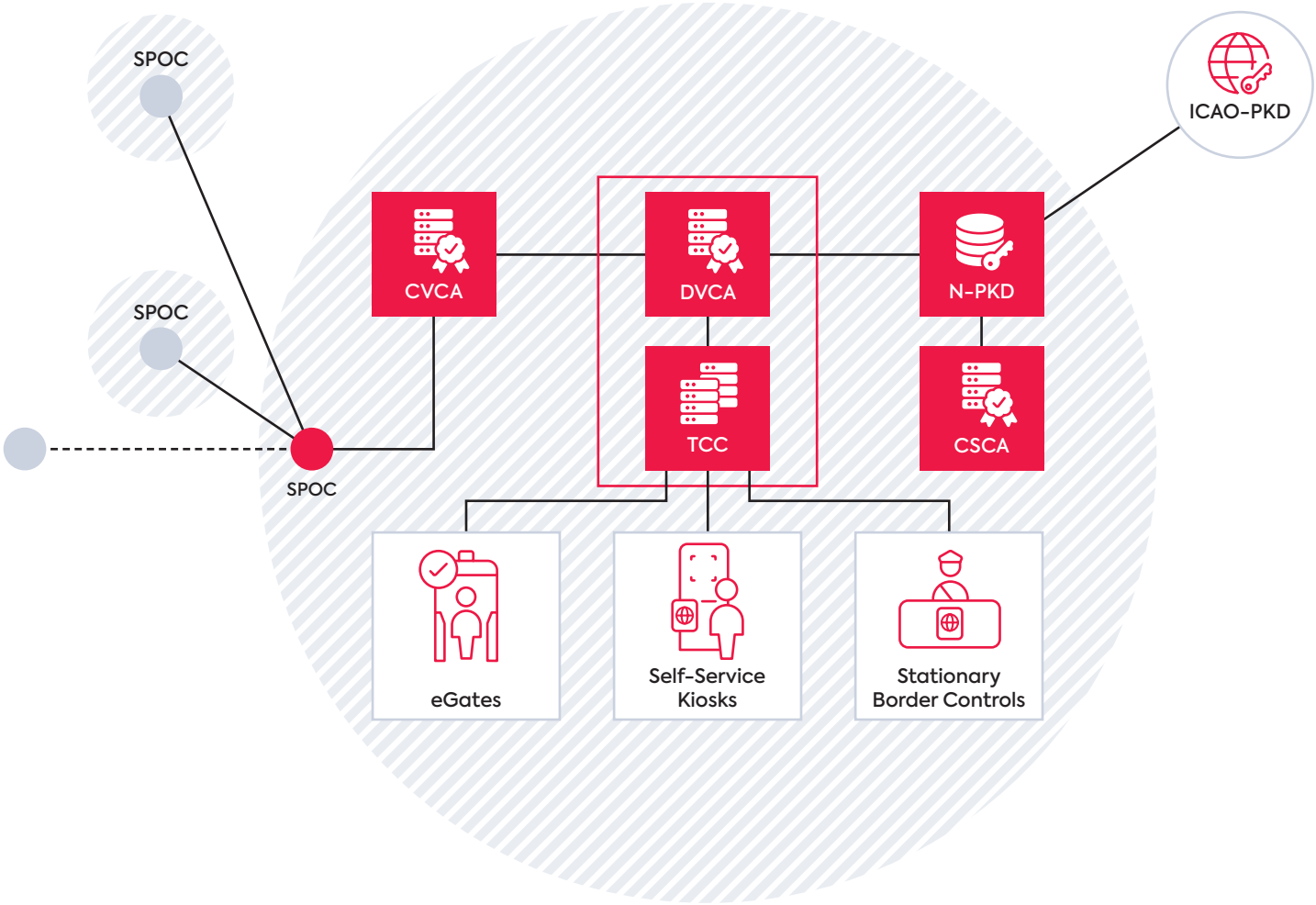
In the past, requirements for authenticity and data integrity referred to the optical features of ID documents. With the implementation of biometric features, the requirements are now extended to the electronic layer of the document. The International Civil Aviation Organization (ICAO) has published specifi cations 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.

Because only verifiably authorised instances are to have access to the sensitive biometric data in eIDs, 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, one has 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 369791:2018 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 is truly known for a reliably and professionally handling highly complex eID projects. 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 (EAC) 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|SAC|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 entitlements. 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.

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.

Benefits

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

Good reasons 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 software modules 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. You can choose between individual software modules for easy integration into your existing setup, and the complete turn-key solution – just as you need it.

CSCA

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

N-PKD

As the national layer of the ICAO PKD the N-PKD stores all trusted domestic and foreign CSCA certificates, DS certificates and corresponding CRLs.
In this context the N-PKD supports the ICAO PKD interface, requests CRLs from the distribution points and manually imports certificates and Master Lists. The N-PKD supports the operator reliably by analysing the various qualities of the imported data and storing them separately according to their trustworthiness. Additionally the N-PKD is able to create and store Master and Defect Lists to be used for Passive Authentication in the border control process.

SPOC

As a centralised interface the Single Point of Contact allows certificate exchange on national and international level; according to CSN 369791:2018 respectively to the technical guideline BSI-TR-03129. secunet's SPOC covers both communication parts based on secure communication via TLS. Thus, secunet's TLS CA issues client and server certificates for the web services by supporting RSA and elliptic curve keys. As a special service secunet provides a SPOC test system.

CVCA

secunet offers a Country Verifying Certification Authority that generates the first two necessary Card Verifiable certificates of a valid certificate chain for Terminal Authentication: root and DVCA certificates. A key benefit is the secure storage of asymmetric key pairs, certificates and electronic signatures which is realised by integrating HSMs or smartcards.

DVCA

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 corresponding SPOC. IS certificate requests can be received, checked and, if approved, 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 – so secunet's DVCA of course supports the integration of HSMs.

TCC

The Terminal Control Centre is a centralised approach of an IS – the idea is to take over EAC and Passive Authentication for the numerous readers distributed in the field. secunet's TCC supports different application scenarios for BAC-, EAC- and SAC-protected documents (Basic and Extended Identity Check). A secure centralised certificate and/or key storage enable 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.

C²K

The Certified CA Kernel (C^2K) meets the highest security demands and can be flexibly combined with all CAs of secunet eID PKI Suite. It fulfils all the requirements of version 1.5 of the Certificate Issuing and Management Components (CIMC) Protection Profile. The C^2Kernel is third party evaluated according to Common Criteria with Evaluation Assurance Level (EAL) 4+ and certified by the German Federal Office for Information Security referenced by certificate number BSI-DSZ-CC-0960-2015 (the detailed certification report is available on the BSI's homepage at www.bsi.bund.de; Topics/Certification/Certified Products).

secunet Security Networks AG
Kurfürstenstraße 58 · 45138 Essen · Germany
T +49 201 5454-0 · F +49 201 5454-1000
info@secunet.com · secunet.com

More information:
secunet.com/en/eidpki