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. There is no doubt about it: only verifiably authorised instances are to have access to such sensitive biometric data. 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 set-up for safeguarding eIDs, however they represent different security aspects. secunet has hands-on experience in operating eID PKIs in the field in a highly reliable and professional manner. Thus, software products have been deduced from previous eID projects which are “ready-to-implement” for your projects, too.

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

The introduction of 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.
ICAO PKI
An electronic signature prevents eID data from being tampered. The authenticity and integrity of an eID can be checked later on by the verification of this electronic signature. To establish full trust in the verification result, the complete corresponding X.509 certificate chain, including certificate revocation lists (CRLs), needs to be available and checked. 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 has to be provided.

Every country issuing electronic machine-readable travel documents has to establish a national CSCA to issue valid certificates to and updated revocation information about the Document Signer. In times of continuously increasing numbers of flight passengers, checking the genuineness of foreign electronic ID documents is of utmost importance at borders. CSCA certificates, DS certificates and the corresponding CRLs of the eID country of origin have to be available for the respective Inspection System. The exchange of all this data can be processed via the ICAO PKD – a global and up-to-date directory which manages all of this information of the participating countries. Each country taking part in the ICAO PKD can choose to map the ICAO PKD to a national layer so that a national directory is established.

EAC PKI
Extended Access Control with its security mechanisms respectively ensures that only authorised persons and instances have access to the electronic data. After establishing secure communication and the verification of the eID chips’ authenticity by carrying out Chip Authentication, an Inspection System can request access to sensitive data. There are two things which have to be available to the Inspection System: an asymmetric key pair and a card verifiable certificate chain. During Terminal Authentication, the Inspection System sends the certificate chain to the eID. If the document can make reference to its trust anchor, a challenge-response protocol can be established in order to check the authenticity and access rights of the Inspection System.

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. The product range comprises components for application in the ICAO PKI field, e.g. CSCA and DS services; and components which fulfil the requirements of the EAC PKI, e.g. CVCA and DVCA services. Together with the ePassportAPI, secunet covers the important requirements regarding the various PKIs.

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