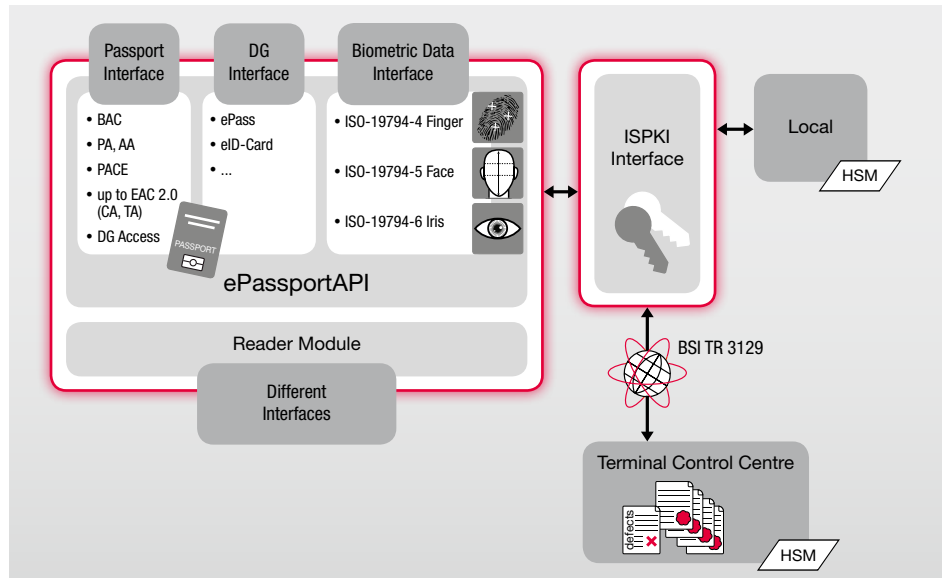


# A Standard Interface for Electronic Machine Readable Travel Documents



## Benefits:

- » Accredited evaluation laboratory
- » Comprehensive know-how in the fields of electronic passport and biometrics
- » Vendor-independence

In the new generation of electronic machine readable travel documents (eMRTDs) a RFID chip is implemented that contains biographic as well as biometric information. Data integrity, authenticity and confidentiality have to be ensured to avoid misuse of this personal data. The realisation of suitable security mechanisms requires different cryptographic algorithms in combination with several types of key and certificate storages. eMRTDs are accessed using RFID capable reading devices. **With the ePassportAPI secunet offers a solution that reduces the complexity and diversity of the reading process.**

secunet's ePassportAPI is a vendor-independent and easy-to-use standard interface for reading eMRTDs. The application interface comprises the following parts:

### Passport Interface

The passport interface provides functions to perform all security mechanisms and to retrieve the electronically stored data on the chip. The ePassportAPI supports both, security mechanisms defined by the ICAO and the EU. Last-mentioned regulations refer to the Extended Access Control mechanisms (EAC), which specify the access to sensitive biometric data.

To get direct access to all Data Groups stored on the chip, the following security mechanisms have to be performed at first. The data are provided

in a raw binary form, which makes further handling much easier: Data can either be forwarded to another related system or processed further using the ePassportAPI Data Group Interface.

The passport interface supports the following mechanisms:

### ■ Passive Authentication (PA)

- » Certificate Chain validation (CSCA, DS)
- » Certificate Revocation List check
- » Defect List check
- » RSA with SHA-1, SHA-224 and SHA-256, SHA-384, SHA-512
- » RSA PSS, RSA PKCS#1
- » ECDSA with SHA-1, SHA-224 and SHA-256, SHA-384, SHA-512

■ **Active Authentication (AA)**

- » RSA
- » ECDSA

■ **Basic Access Control (BAC)**

- » Two line MRZ
- » Three line MRZ for ID-cards

■ **Extended Access Control (EAC) Version 1.11**

- » Chip Authentication (DH and ECDH)
- » Terminal Authentication (RSA and ECDSA)
- » Handling of CVCA-Link-Certificate for eMRTD-Trust-Point update

■ **Extended Access Control (EAC) Version 2.0x**

- » Password Authenticated Connection Establishment (PACE v2, ICAO SAC)
- » Terminal Authentication v2 (RSA and ECDSA)
- » Chip Authentication v2 (DH and ECDH)
- » Restricted Identification, Age Verification, Document Validity Check

**Data Group Interface**

The data elements on the chip are coded according to the ICAO LDS specification. The Data Group Interface allows detailed access to the individual elements stored inside each data group. Specific access functions are available for the following data groups:

- Data Group 1 (Machine Readable Zone)
- Data Group 2 (Facial Image)
- Data Group 3 (Fingerprint Image)
- Data Group 4 (Iris Image)
- Data Group 5 (Displayed Portrait)
- Data Group 7 (Displayed Signature)
- Data Group 11 (Additional Personal Details)
- Data Group 12 (Additional Document Details)
- Data Group 14 (Security Infos for EAC)
- Data Group 15 (Active Authentication Info)

For the biometric features the Data Group Interface delivers the following elements according to the CBEFF standard published by ISO:

- Biometric Information Template (BIT)
- Biometric Header Template (BHT)
- Biometric Data Block (BDB)

The Biometric Header Template contains additional information while the Biometric Data Block is used for the coding of the actual biometric feature. Further processing of the biometric data is possible using the Biometric Data Interface.

**Biometric Data Interface**

The Biometric Data Interface supports biometric data blocks encoded according to the following standards:

- ISO 19794-4 (Fingerprint image)
- ISO 19794-5 (Facial image)
- ISO 19794-6 (Iris image)

It provides access to the current biometric image as well as further information related to the biometric features, such as for example colour of hair or eye and facial feature points.

**eID Data Group Interface**

The ePassportAPI completely supports the eID data groups as defined for the German national ID card (nPA).

**Reader Module**

The ePassportAPI accesses the chip inside the ePassport by using RFID reading devices. Currently there is a wide range of readers available on the market; specific organisational requirements determine the type of reader. They differ in structural shape and functional capabilities. The ePassportAPI therefore defines a standard interface, which supports both, all PC/SC compliant readers and many proprietary readers.

Security mechanisms often require the management of cryptographic keys. Those keys can either be stored locally or remotely, this is why the application of HSMs or Public Key Servers is of special interest.

**ISPKI Interface**

The mechanisms for eMRTDs require secure handling of the cryptographic material. Appropriate solutions highly depend on environmental factors such as legal and/or organisational restrictions. The ePassportAPI defines a standard ISPKI interface to support different solutions. Often the main cryptographic functionality for Passive Authentication and Terminal Authentication (EAC) is concentrated in a centralised system the so called Terminal Control Centre (TCC). The standard ePassportAPI comes with a comprehensive implementation of the Web Service Interface defined by the BSI TR 03129, for an easy connection to a TCC. For stand-alone operation, an offline implementation of the ISPKI interface is available. Customer specific implementations of the ISPKI interface are possible.

**Supported Development Environments**

The entire ePassportAPI C++ implementation is modularly designed and therefore suitable for many different 32 bit and 64 bit platforms. It just needs the necessary reader device drivers. The standard versions of the ePassportAPI are available for Microsoft Visual Studio 2008. Java and .NET interfaces are available on request.

More information:  
[www.secunet.com/en/eID](http://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: [biometrics@secunet.com](mailto:biometrics@secunet.com)  
[www.secunet.com](http://www.secunet.com)