MTG

WHITE PAPER

German PKI
for Machine Readable Travel Documents (MRTD) based on MTG CARA

MTG AG
Dolivostraße 11
D-64293 Darmstadt
Tel: +49 (0) 6151 8000-0
Fax: +49 (0) 6151 8000-43
E-Mail: contact@mtg.de

SecurITy made in Germany

TeleTrusT Quality Seal
www.teletrust.de/itsmig

Table of content

Table of figures

1 About MTG AG and MTG CARA

MTG AG is an IT security specialist located in Darmstadt, Germany. MTG AG was founded in 1995 and has a main focus and long-term experience in consulting and software development in the area of IT-security. Besides the PKI product family, MTG AGoffers products and solutions in the context of electronic identity cards, e.g., an eID-Server product conforming to the technical guidelines for the electronic identity function of the German identity card.

The MTG AG Certification Authority and Registration Authority solution MTG CARA is a high-end product for the establishment and administration of company or public authority PKI security infrastructures. MTG CARA covers all features for the application and issuance of X.509 and CV certificates as well as their administration and publication. Especially the system is optimally suitable for setting up national PKIs for machine readable travel documents and identity cards.

In 2009 MTG AG was charged by the German Republic represented by the German Federal Office for Information Security (Bundesamt für Sicherheit in der Informationstechnik, BSI) to develop and setup the root instances for the German PKI for machine readable travel documents. Since 2010 the German MRTD PKI root systems based on MTG CARA are at work. They are operated by the BSI and comprise the national CSCA Root as well as three national CVCA Root Systems for different access types to the German ePassport and eIdentity card.

Since 2011 different document verifier certification authorities (DVCA) based on MTG CARA are in work to issue terminal certificates for different access types. They are operated by the BSI and by one of the important German digital certificate service providers.

The MTG security products carry the national seal of quality “IT-Security made in Germany”. For further information about MTG CARA please contact

MTG AG
Dolivostraße 11
64293 Darmstadt
contact@mtg.de

The current whitepaper gives an overview of the technical properties of the German MRTD PKI infrastructure based on MTG CARA. For a better understanding it starts with a short summary of the security mechanisms for machine readable travel documents.

2 Overview of Security Mechanisms for MRTD

Following international and European standards, data stored on machine readable travel documents (MRTD) has to be protected against manipulation and unauthorized access by Passive Authentication and Terminal Authentication (as part of Extended Access Control), respectively.

Passive Authentication is a mechanism standardized in [Doc9303-1-2] and [Doc9303-3-2]. Passive Authentication uses a digital signature to authenticate data stored on the MRTD. This signature is generated by a Document Signer (DS) in the personalization phase of the MRTD. The Document Signer in turn is certified by the Country Signing CA (CSCA) of the issuing country.
If a terminal has to read data from a MRTD, the terminal must perform Passive Authentication to verify that the data is authentic and has not been manipulated. For Passive Authentication the terminal must have access to the corresponding Document Signer certificate and Country Signing CA certificate. While the Document Signer certificate can usually easily be obtained from the MRTD itself, the CSCA certificate must be securely distributed to and stored at the terminal.
To support the secure distribution of CSCA certificates, Master Lists [Master List] have been introduced. Master Lists are signed lists of (nationally) trusted CSCA certificates. Thus, the terminals only have to store the public key required for the verification of such a Master List securely.

Terminal Authentication is a mechanism standardized in [TR-EAC]. Terminal Authentication is based on a challenge-response protocol using digital signatures and card-verifiable (CV) certificates both to be validated by the MRTD. After verification of the terminal certificate the MRTD calculates the rights assigned to the terminal and grants the terminal access to the corresponding data stored on the MRTD. The terminal certificate is issued by the Document Verifier (DV) the terminal is associated with. The Document Verifier in turn is certified by (at least) the national Country Verifying CA (CVCA) but it may also be certified by foreign CVCAs.

For the processing of cross-border certification, each country will operate a **SPOC (single point of contact)** for incoming and outgoing foreign requests and responses. If a DV requests a CV certificate from a foreign CVCA, it does not send its request to the foreign CVCA directly. Instead, it sends its request to its national SPOC. If accepted the national SPOC forwards the request to the SPOC of the intended foreign country. This SPOC then forwards the request to the CVCA of that country. See [SPOC] for details of the messages used for cross-border communication.

3 The German Country Signing Public Key Infrastructure based on MTG CARA

The German CSCA is the Root Certification Authority of the German Country Signing Public Key Infrastructure (CSPKI).
The German CSCA issues so-called Document Signer Certificates (DS) which are used for producing German machine-readable travel documents. During the production process the data stored on the contactless chips is (partially) signed by the document manufacturer using DS Certificates. If a terminal reads data from a MRTD, the terminal must perform Passive Authentication based on the country signing PKI to verify that the data is authentic and has not been manipulated.

In Germany the following MRTDs are issued:

- Passport (ePass),
- Residence permits (eAT), and
- ID cards for German citizens (nPA).

The German CSCA also issues communication (COM) certificates used for SSL/TLS-based data connections. These connections are used to protect communication processes that support the handling of official ID documents, e.g., between national and foreign SPOCs.

3.1 System Architecture

The German CSCA is operated in offline mode for security reasons. DS certificate requests and issued DS certificates are imported/exported via a file interface. The following figure illustrates the logical system architecture.

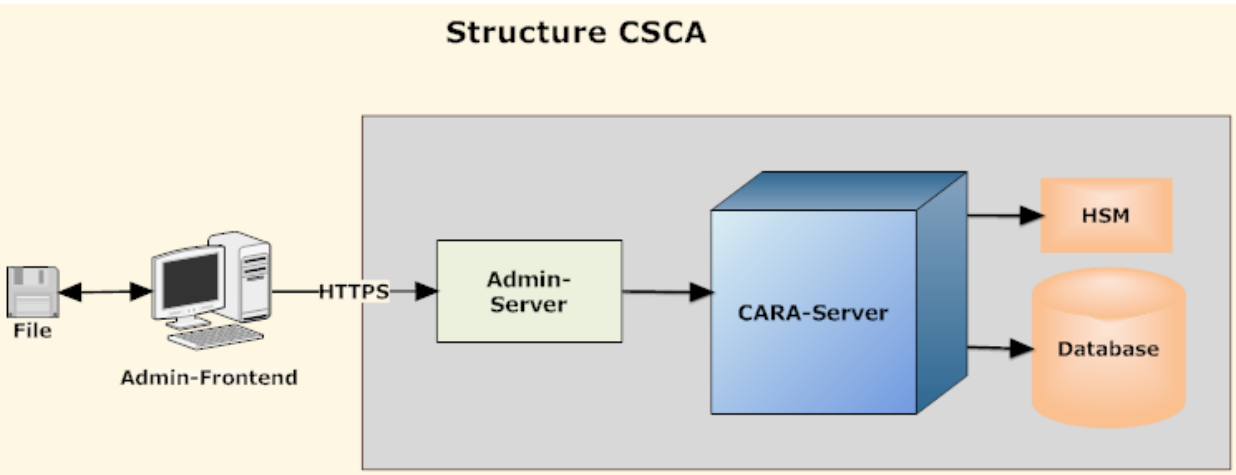

Figure 1: CSCA system architecture

Main component of the system is the MTG CARA server, which realizes all necessary functions of a certification authority, registration authority, and for PKI administration issues. Attached to the server is a hardware security module (HSM) which is certified by BSI for that purpose and a database system.

The so-called Admin-Server is a Java-Servlet application providing all necessary function interfaces for CSCA operation and administration. The admin server is accessed via a web-based administration frontend.

Besides various administration functions, the following operations are provided:

- Generation and administration of self-signed CSCA certificates and CSCA link certificates
- issuance of DS certificates signed by the CSCA based on imported PKCS#10 requests
- issuance of master list signing certificates signed by the CSCA based on imported PKCS#10 requests
- issuance of certificates for secure TLS/SSL communication (e.g., SPOC communication) signed by the CSCA based on imported PKCS#10 requests
- issuance of X.509 revocation lists

3.2 Technical Parameters

The system supports the following features:

- Key algorithms: RSA, ECC
- Hash algorithms: SHA1, SHA-2, RIPEMD
- X.509 certificates and revocation lists conform to RFC 5280
- Customizable templates for certificate and CRL generation
- Support for all X.509-extensions

3.3 Supported Standards

The system conforms to the following national and international standards:

[Doc9303-1-2] ICAO Doc 9303, Machine Readable Travel Documents - Part 1: Machine Readable Passport, Volume 2, Specifications for electronically enabled passports with biometric identification capabilities, 6th Edition, 2006

[Doc9303-3-2] ICAO Doc 9303, Machine Readable Travel Documents - Part 3: Machine Readable Official Travel Documents, Volume 2, Specifications for electronically enabled official travel documents with biometric identification capabilities, 3rd Edition, 2008

[ICAO ML] ICAO, CSCA Countersigning and Master List issuance, Technical Report Version 1.0, June 2009

For a complete list of supported standards see chapter REFERENCES.

4 The German SPOC and Country Verifying Public Key Infrastructure based on MTG CARA

According to the extended access control (EAC) mechanisms defined in [TR-03110] a three step PKI hierarchy is needed to issue terminal certificates to allow terminals access to the data stored in the chip of an MRTD.

The national CVCA ePass root is the anchor of trust for defining access rights to the national MRTDs (passports, residence permits and id cards). The ePass CVCA root issues so-called DV-certificates for Document Verifier (DV). A DV is a certification authority that issues terminal certificates and governs the access rights of a group of terminals with a similar range of access rights. The access rights defined in the terminal certificates comprise at most the access rights defined in the DV certificate, or are a subset of them.

A terminal communicates with the chip of an MRTD and proves its identity and access rights with the terminal authentication mechanism.

The following figure illustrates the EAC PKI hierarchy and certification chain.

Figure 2: EAC PKI hierarchy

A national CVCA issues DV certificates to national as well as foreign DV entities. For a DV entity in country B which governs border control terminals in country B it is necessary to apply for a DV certificate from the CVCA of country A to enable it's terminals to get read access to travel documents from country A. This procedure is illustrated in the next figure.

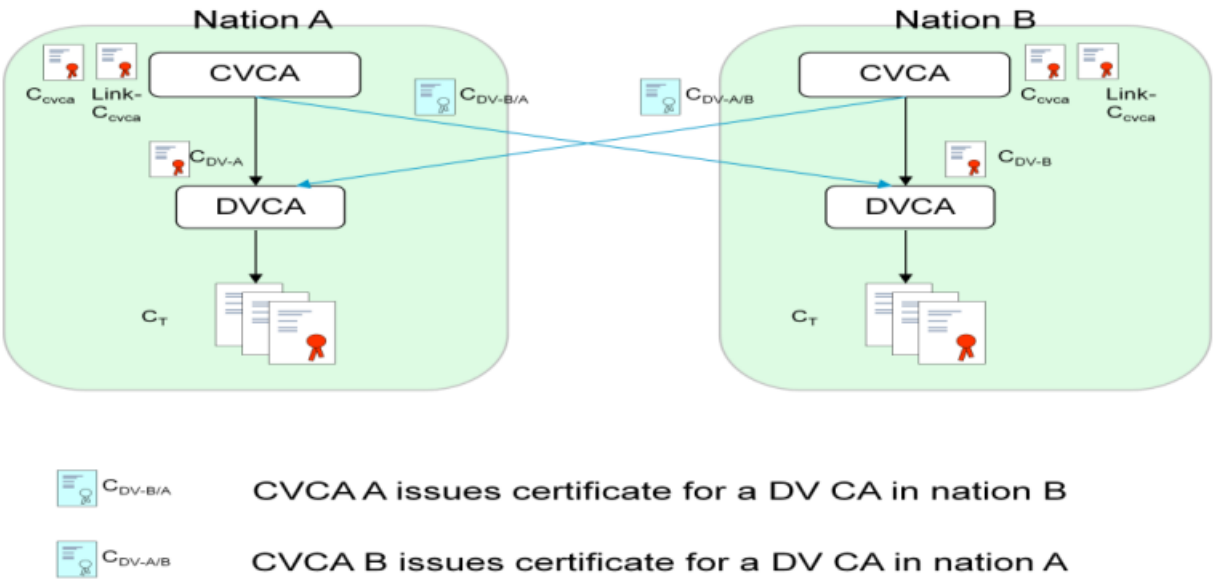

Figure 3: Cross-border certification of DV entities

All electronic cross-border communication between CVCA and DV instances is routed over the national “single points of contact” (SPOC) entities.

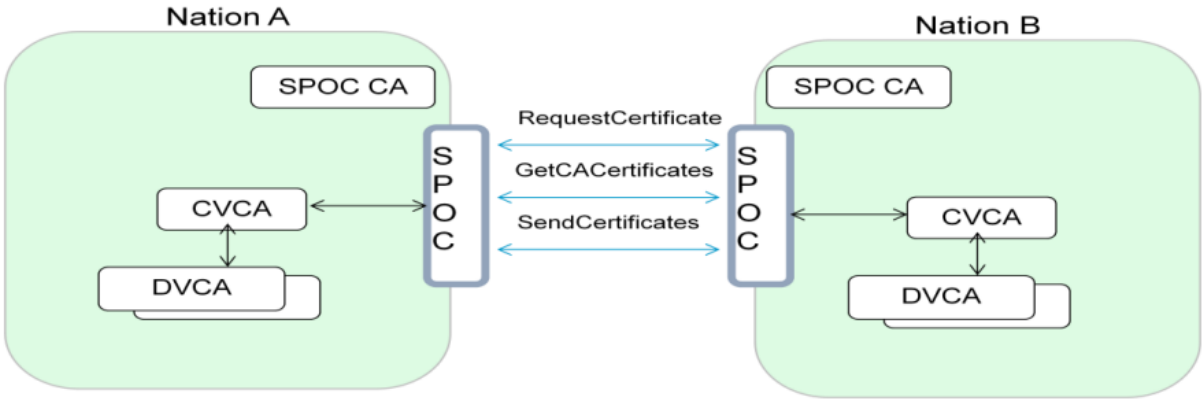

Figure 4: cross-border communication with SPOC

[SPOC] defines the set of messages for the SPOC-SPOC communication as well as profiles for the specific certificate profiles which are used for securing the SPOC communication. In the German solution the SPOC CA is integrated with the CSCA.

4.1 System Architecture of SPOC and CVCA

The German CVCA root for responsibilities of public administration (e.g., border control and police) is called CVCA ePass in the following. It mainly consists of the MTG CARA system and the SPOC component provided by MTG AG. The SPOC component is operated in online mode and DV certificate requests and issued DV certificates are exchanged via the standardized secure interfaces of the national SPOC instance. The following figure illustrates the system architecture.

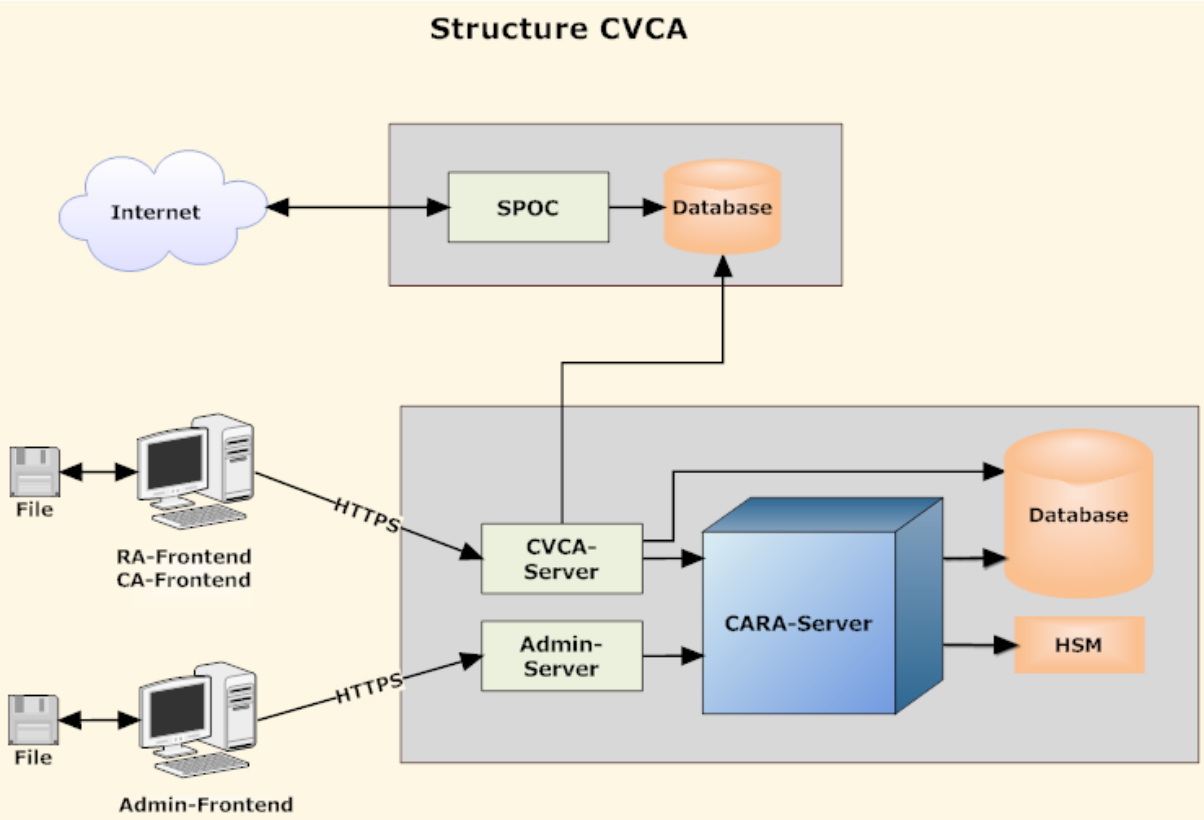

Figure 5: System architecture of the German SPOC and CVCA for ePass applications

One main component of the system is the MTG CARA server, which realizes all necessary functions of a certification authority, registration authority, and for PKI administration issues. Attached to the server is a hardware security module (HSM) which is certified by BSI for that purpose and a database system.

The so-called Admin-Server is a Java-Servlet application providing all necessary functions interfaces for CVCA administration. The admin server is accessed via a web-based administration frontend.

All necessary function interfaces of the CVCA for certificate application, registration and generation are provided by the so-called CVCA-Server. It is a Java-Servlet application. The CVCA server is accessed via the web-based registration authority (RA) and certification authority (CA) frontend. The CVCA Server is only accessible within the intranet of the operation environment by authorized system roles which are authenticated to the CVCA via role-specific X.509 certificates.

The SPOC component is connected with the Internet. It has no online connection to the internal CVCA system. Communication between SPOC and the CVCA system is realized via requests/responses which are stored in a database and which is periodically checked by CVCA and SPOC.

SPOC provides the standardized secure interfaces for communication with national and foreign DV CA, which are:

- Reception and storage of certificate requests for national and foreign DV entities under the national CVCA and sending of corresponding responses
- Reception and forwarding of certificate requests from national DV to foreign CVCAs
- Reception and forwarding of certificate responses from foreign CVCAs to national DV entities
- Functionality of NPKD instance: distribution of master and defect lists.

Besides various administration functions, the CVCA provides the following operations:

- Generation and administration of self-signed CVCA certificates and CVCA link certificates
- Administration of national DV entities
- Administration of foreign CVCA entities
- issuance of DV CA certificates signed by the CVCA
- verification of inner and outer signatures of certificate requests

4.2 Technical Parameters

The system supports the following features:

- Key algorithms: RSA, ECC
- Hash algorithms: SHA1, SHA-2, RIPEMD
- CV format conformant to TR-03110
- Customizable Templates for certificate generation
- TLS-Features used within SPOC:
    1. Key algorithms: RSA, ECC
    2. Cipher suites from CSN 36 9791:
       TLS_RSA_WITH_AES_128_CBC_SHA
       TLS_DHE_RSA_WITH_AES_128_CBC_SHA
       TLS_RSA_WITH_AES_256_CBC_SHA
       TLS_DHE_RSA_WITH_AES_256_CBC_SHA

TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA

3. Supported certificate formats with ECC conformant to RFC 3279:
   client-certificates with ECC-key coded as namedCurve defined in RFC 4492
   server-certificates coded as namedCurve or as ecParameters

4.3 Supported Standards

The system conforms to the following national and international standards:

- TR-03110, Advanced Security Mechanisms for Machine Readable Travel Documents –Extended Access Control (EAC), Password Authenticated Connection Establishment (PACE), and Restricted Identification (RI), Version 2.03, 24. March 2010
- Common Certificate Policy for the Extended Access Control infrastructure for passports and travel documents issued by EU member states, Version 1.0, 22 April 2008
- Information Technology - Country Verifying Certification AuthorityKey Management Protocol for SPOC -ČSN 36 9791, Draft 1.0, July 2009
- TR-03129, PKI for Extended Access Control (EAC) – Protocol for the Management of Certificates, version 1.10

For a complete list of supported standards see chapter REFERENCES.

The German Identity Card carries two further applications (identity/authorization function and digital signature function) besides the ePass application. Both applications are access protected by the EAC mechanisms. Due to that, Germany operates three separate CVCA root instances, one for each application, to separate access rights for the different kinds of applications:

- CVCA ePass for ePass applications on German passport, German identity card and German residence permits (which is described in the present chapter),
- CVCA eID for the identity/authorization function of the German eID and eAT cards,
- CVCA eSign for digital signatures of an optional qualified certificate on the German identity card.

All CVCA entities are based on the MTG CARA product and operated by the BSI.

5 German Document Verifiers based on MTG CARA

As described in the previous chapter the second level in the EAC PKI hierarchy is the Document Verifier (DV). A DV is a certification authority that issues terminal certificates and governs the access rights of a group of terminals with a similar range of access rights. The access rights defined in the terminal certificates comprise at most the access rights defined in the DV certificate, or are a subset of them.

A terminal communicates with the chip of an MRTD and proves its identity and access rights with the terminal authentication mechanism.

Since 2011 different document verifier certification authorities (DVCA) based on MTG CARA are in work to issue terminal certificates for different access types. They are operated by the BSI and by one of the important German digital certificate service providers.

5.1 System Architecture

The following figure illustrates the system architecture of a DV CA based on MTG CARA.

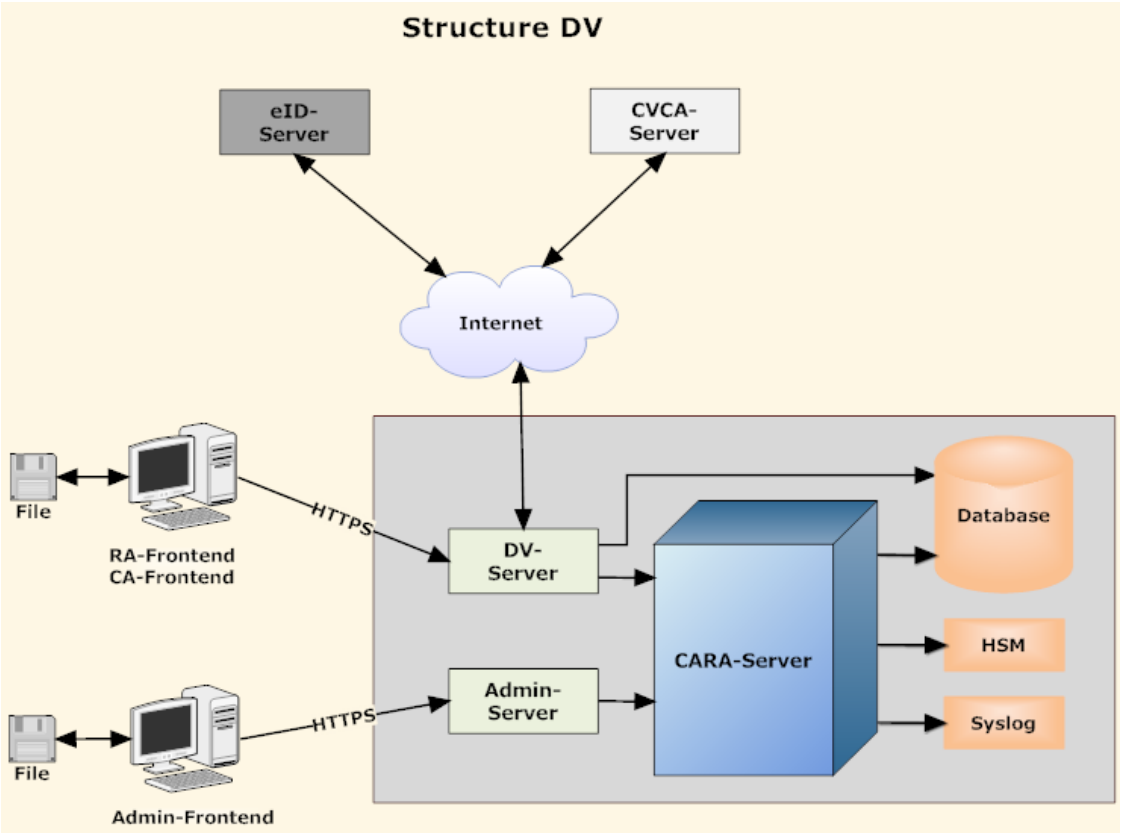

Figure 6: System architecture of a DV for ePass, eID or eSign applications

The main component of the system is the MTG CARA server, which realizes all necessary functions of a certification authority, registration authority, and for PKI administration issues. Attached to the server is a hardware security module (HSM) which is certified by BSI for that purpose, a database system and an external syslog server.

The DV provides the standardized communication interface to the SPOC component of a national CVCA in order to request national or foreign DV CA certificates.

For usage within the context of the German identity card with its eID application the system provides standardized interfaces to so-called eID Servers and the national eID revocation service.

The so-called Admin-Server is a Java-Servlet application providing all necessary functions interfaces for CVCA administration. The admin server is accessed via a web-based administration frontend.

All necessary function interfaces of the DV for certificate application, registration and generation are provided by the so-called DV-Server. It is a Java-Servlet application. The DV server is accessed via the web-based registration authority (RA) and certification authority (CA) frontend. The DV Server is only online accessible by authorized system roles which are authenticated to the DV via role-specific X.509 certificates.

Besides various administration functions, the DV provides the following operations:

- Administration of national and foreign CVCA entities
- Administration of connected eID Servers or Terminal Control Centers
- Sending of certificate requests for a national and foreign DV entity to the national SPOC component
- Reception of certificate responses from national or foreign CVCAs via SPOC
- Reception of certificate requests from eID Servers or Terminal Control Centers
- Issuance of terminal certificates
- Sending of certificate responses to eID Servers or Terminal Control Centers
- Distribution of master and defect lists

5.2 Technical Parameters and Supported Standards

The system supports the same technical features and supports the same standards as the CVCA system described in chapter 4.2 and 4.3.

6 Technical characteristics of MTG CARA

Supported operating systems:

- Linux
- Windows

System prerequisites:

- JAVA 11 Runtime Environment
- Web server, e.g. apache http-server 2.4
- Servlet Engine, e.g., apache tomcat 9.0

Supported Database-Systems:

- Oracle 10
- MariaDB 10.3
- PostgreSQL 11

Supported HSMs:

- Safenet Luna SA
- Utimaco Deutschland HSM
- PKCS#11 HSM (EnTrust – nCipher)

The system license can provide a set of software packages or a complete appliance including hardware. It is high-performing and designed to fulfill high-availability requirements. It provides a connection layer to connect a set of HSMs and operate them in high-availability mode.

The system is extensively customizable. All processes on top of the core PKI functionality can be fully adapted to user's requirements.

The set of supported cryptographic algorithms can as well be extended if necessary and if provided by the HSM.

REFERENCES

[Doc9303-1-2] ICAO Doc 9303, Machine Readable Travel Documents - Part 1: Machine Readable Passport, Volume 2, Specifications for electronically enabled passports with biometric identification capabilities, 6th Edition, 2006

[Doc9303-3-2] ICAO Doc 9303, Machine Readable Travel Documents - Part 3: Machine Readable Official Travel Documents, Volume 2, Specifications for electronically enabled official travel documents with biometric identification capabilities, 3rd Edition, 2008

[EC2252] European Council. EC Regulation 2252/2004. December 2004.

[ICAO] PKI for Machine Readable Travel Documents offering ICC Read-Only Access. Technical Report Version 1.1, 2004.

[ICAO ML] ICAO. CSCA Countersigning and Master List issuance, Technical Report Version 1.0, June 2009

[PKCS7] RSA Laboratories. PKCS#7. Cryptographic Message Syntax Standard. Version 1.5, 1993.

[PKCS9] RSA Laboratories. PKCS#9. Selected Object Classes and Attribute Types. Version 2.0, 2000.

[PKCS10] RSA Laboratories. PKCS#10. Certification Request Syntax Standard. Version 1.7, 2000.

[PPSSCD] Protection Profile. Secure Signature Creation Device. Type 1-3. 2002.

[RFC822] RFC 822. Standard for the format of ARPA internet text messages. available at www.ietf.org/rfc/rfc822.txt. 1982.

[RFC5280] RFC 5280 Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile. available at www.ietf.org/rfc/rfc5280.txt. 2008.

[SHS] NIST. FIPS Publication 180-2. Secure Hash Standard (SHS). 2002.

[SPOC] Česká Technická Norma. Information Technology - Country Verifying Certification AuthorityKey Management Protocol Specification for SPOC -ČSN 36 9791, Draft 1.0, July 2009

[TR EAC] Advanced Security Mechanisms for Machine Readable Travel Documents –Extended Access Control (EAC), Password Authenticated Connection Establishment (PACE), Version 2.01

[TR-03111] Elliptic Curve Cryptography. BSI Technical Guideline TR-03111, Version1.11, 2009.