mtG-CARA:
The PKI for Identity Documents

mtG-CARA is a high-end product for the establishment and administration of company or public authority PKI security infrastructures. Developed by media transfer AG it covers all features for the application and issuance of X.509 and CV certificates for machine-readable travel documents and identity cards, as well as their administration and publication.

mtG-CARA is in use at the German Federal Office for Information Security (BSI) as Root CA for German PKI. It is also operating at a leading European Trust Center.

Bundesamt für Sicherheit in der Informationstechnik

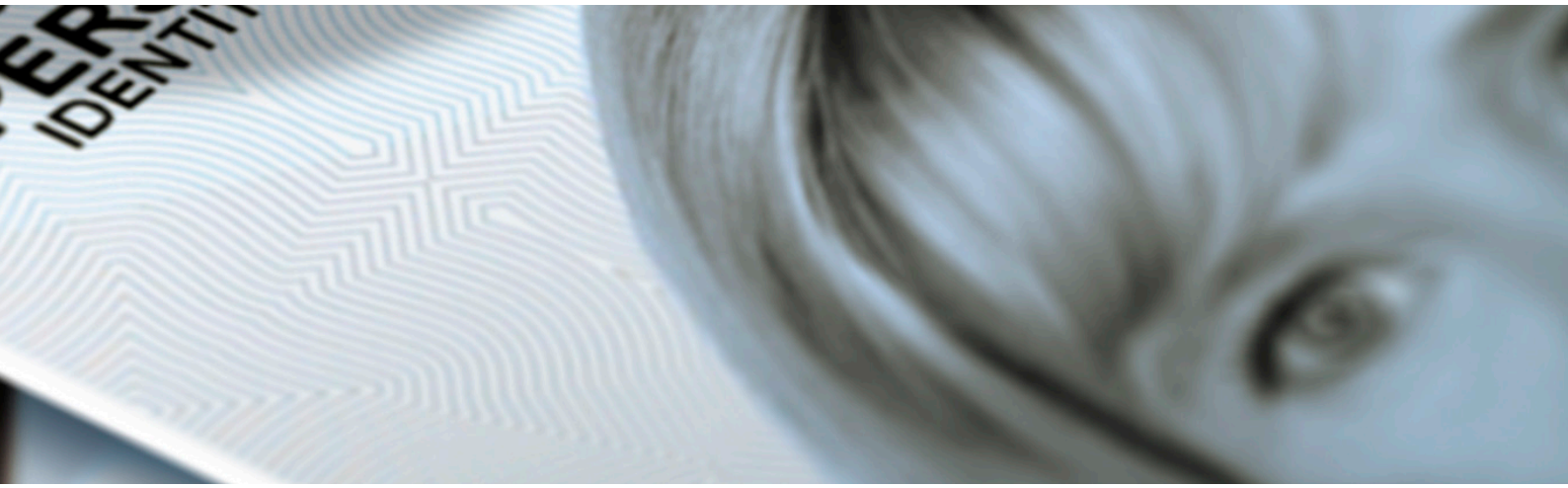
The right choice for ICAO and EAC PKIs

mtG-CARA is especially optimized for ...

- setting up national Public Key Infrastructures (PKIs)
- Country Signing Certification Authority (CSCA)
- Country Verifying Certification Authority (CVCA)
- Document Verifying Certification Authority (DVCA)
- cross-border certification based on SPOC (Single Point of Contact) applications

Benefits:

- mtG-CARA supports all relevant protocols and interfaces to support Extended Access Control (EAC) and ICAO PKIs for electronic documents
- Flexible configuration in terms of processes, algorithms and cryptographic modules
- Can be used as integrated PKI or as individual components



mtG-CARA key components

CVCA (Country Verifying Certification Authority)
mtG-CARA offers a CVCA as the national anchor of trust for defining access rights to the national MRTDs (passports, residence permits and ID cards). The CVCA root issues DVCA-certificates for Document Verifiers (DV).

DVCA (Document Verifier Certificate Authorities)
A DVCA 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. mtG-CARA offers all functionalities to manage DVCA certificates, providing an interface to the corresponding SPOC. The DVCA issues certificates for inspections systems (IS) and authentication terminals (AT) requiring access to data stored in the MRTD chip.

SPOC (Single Point of Contact)
For the processing of cross-border certification, each country will operate a SPOC for incoming and outgoing foreign DV certificate requests and responses. mtG-CARA supports certificate exchange on national and international level based on CSN 369791:2009. You can also use mtG-CARA to issue client and server certificates for secure communications via SSL/TLS, e.g. between SPOC and DVCA.

CSCA PKI (Country Signing Certification Authority)
mtG-CARA offers all functionality necessary to run a CSCA. The CSCA issues so-called Document Signer Certificates (DS) which are used for producing machine-readable travel documents.

Flexible PKI Suite
You can use mtG-CARA as a highly integrated platform to run all certification authorities (CSCA, CVCA, DVCA) —including SPOC— which are necessary to set up a complete PKI infrastructure for identity documents. It is also possible to run mtG-CARA as a single CA. The SPOC can be integrated into existing PKIs not based on mtG-CARA. The necessary adaptations are provided on demand.

mtG-CARA Features

Highly portable due to the underlying Java-based technologies and standard protocols. The supported operating systems are:

> SUN Solaris
> LINUX
> Windows

Permits different signer modules such as Soft-PSE and HSM.

The following cryptographic modules are currently supported:

> Utimaco Deutschland HSM
> Safenet LUNA SA
> Other signer modules can be offered upon request

Founded in 1995 media transfer AG (mtG) is a hightech software company with very unique and leading expertise in the field of IT security, innovative business internet solutions and in the energy industry.

mtG is an evaluation facility for IT security accredited and licensed by BSI and the Republic of Germany.

SecurITy made in Germany

Selection of supported Standards:

CSN 36 9791	Country Verifying Certification Authority, Key Management Protocol Specification for SPOC
TR-03110	Advanced Security Mechanisms for Machine Readable Travel Documents, Technical Guideline, BSI
TR-03111	Elliptic Curve Cryptography, Technical Guideline, BSI
TR-03129	PKIs for Machine Readable Travel Documents-Protocols for the Management of Certificates and CRLs, Technical Guideline, BSI
TR-03139	Common Certificate Policy for the Extended Access Control Infrastructure for Passports and Travel Documents issued by EU Member States, Technical Guideline, BSI
TR-CSCA-ML	CSCA countersigning and Master List issuance, Technical Report, ICAO
TR-LDS-PKI	LDS and PKI Maintenance, Technical Report, ICAO
ICAO Doc 9303	Machine Readable Travel Documents, ICAO

mtG media transfer AG

For further information please contact:

Jürgen Ruf
media transfer AG
Dolivostraße 11
D-64293 Darmstadt
Germany

Tel +49 6151 8193-0
jruf@mtg.de