Product brief

eMRTD and ePKI applets from applet collection by Masktech GmbH

On the SECORA™ ID S Java Card™ platform

The eMRTD (electronic Machine Readable Travel Document) and ePKI (electronic Public Key Infrastructure) applets from Applet Collection by Masktech GmbH run on Infineon's SECORA™ ID S platform. These flexible and versatile Java Card™ applets rely on field-proven hardware-based security technology from Infineon, which offers optimized transaction performance especially for electronic government documents. The eMRTD applet is designed for electronic ID cards and travel documents, whereas the ePKI applet supports all functionality required by Secured/Qualified Signature Creation Devices (SSCD/QSCD).

Both the eMRTD and ePKI applets run on the SECORA™ ID S Java Card™ platform based on Infineon's SLC52 security microcontroller supporting Integrity Guard security technology.

They provide the optimum open environment for electronic ID and travel documents for eGovernment and enterprise applications.

The eMRTD applet is fully compliant with the ICAO Doc 9303 standards and the TR-03110 technical guidelines issued by the German BSI, making it a perfect fit for interoperable electronic passport or electronic ID solutions. It provides the basis for biometric passports and electronic residence permits for several countries. Supported authentication protocols include Basic Access Control (BAC), PACE (Password Authenticated Connection Establishment), Active Authentication (AA) and Extended Access Control (EAC).

The eMRTD applet could also be used for electronic driver's license as it is fully compliant with the ISO/IEC 18013 standard series and the EU regulation 383/2012. It supports BAC/BAP (Basic Access Control/Protection), PACE, AA and EAC so personal data can be securely stored and accessed.

Applet key features

Applet crypto protocols

- eMRTD applet
  - BAC
  - PACE: Generic mapping up to 512 bits
  - AA: RSA up to 2048 bits
  - EACv1-CA: ECDH 512
  - EACv1-TA: ECDSA 512
- ePKI applet
  - PACE: Generic mapping up to 512 bits
  - EACv1-CA: ECDH 512/521 bits
  - EACv1-TA: ECDSA 512/521 bits
  - ECDSA 521 bits
  - RSA 2048 bits

Applet certification

- eMRTD applet: targeting CC EAL 5+,
  - BSI-CC-PP-0055
  - BSI-CC-PP-0056
- ePKI applet: targeting CC EAL 5+,
  - BSI-CC-PP-0059

eMRTD applet use cases

- Electronic passport
- Electronic ID
- Electronic driver's license
- Electronic residence permit
- Electronic health card

ePKI applet use cases

- eSignature
- eAuthentication and identification
- eHealthcare
- eSocial security
- eVoting
- Secured file transfer
- Data encrtyption/decryption

MaskTech GmbH
MaskTech is the independent supplier for high-security chip card operating systems for identification cards, travel documents and authentication solutions.

www.infineon.com/secora-id

eMRTD and ePKI applets from applet collection by Masktech GmbH

On the SECORA™ ID S Java Card™ platform

The ePKI applet supports the following basic applications
- Assuring identity: **eAuthentification**
- Ensuring authenticity and integrity of data and protecting against forgery: **eSignature**
- Determining, based on an established identity, the associated privileges: **eAuthorization**
- Securing information transfer for maximum confidentiality: **data encryption/decryption**

In addition, the ePKI applet can be used for digitally signing electronic documents, logging in to Windows systems and authenticating access to online services.

The ePKI applet supports on-card key generation as well as key import based on elliptic curves and RSA. PACE, a well-established security protocol supporting PIN, PUK and CAN secures the communications.

In addition, both the eMRTD and ePKI applets are highly configurable and can easily support different local or domestic requirements without software modifications. This makes them suited to other use cases such as electronic health cards, while still complying with Common Criteria (CC) certification.
The eMRTD and ePKI applets can be ordered individually and together.

Plattform key features

Platform compliance
- Java Card 3.0.5, Classic
- Global Platform® 2.3.1
  - GP ID Configuration 1.0
  - GP Mapping Guidelines V 1.0
  - SCP02, SCP03

Cryptography
- RSA up to 2048 bits
- Elliptic curves up to 521 bits
- TDES
- AES up to 256 bits
- SHA2 up to 512 bits
- Accelerated by crypto coprocessors

Plattform key features

Communication interfaces
- Dual interface
- ISO/IEC 7816-3, T=0, T=1
- ISO/IEC 14443 Type A/B up to 848 kbps (extended length APDU up to 32 kByte)
- ISO/IEC 14443 VHBR up to 6.8 Mbps

Supported international standards
- ICAO Doc 9303 7th edition
- BSI TR-03110 -1, -3, -4 V2.21
- ISO/IEC 18013 -2, -3, -4, latest versions
- ISO/IEC 7816-15, PKCS #15

Certification
- SLC52G: CC EAL 6+, EMVCo
- SECORA™ ID platform: CC EAL 6+, EMVCo

Published by
Infineon Technologies AG
81726 Munich, Germany

Additional information
For further information on technologies, our products, the application of our products, delivery terms and conditions and/or prices, please contact your nearest Infineon Technologies office (www.infineon.com).

Warnings
Due to technical requirements, our products may contain dangerous substances. For information on the types in question, please contact your nearest Infineon Technologies office.

Except as otherwise explicitly approved by us in a written document signed by authorized representatives of Infineon Technologies, our products may not be used in any life-endangering applications, including but not limited to medical, nuclear, military, life-critical or any other applications where a failure of the product or any consequences of the use thereof can result in personal injury.

Document number: B181-I1041-V1-7600-EU-EC
Date: 09/2020