

Product brief

eMRTD applet from Infineon applet collection

On SECORA™ ID S Java Card™ platform

The eMRTD (electronic Machine Readable Travel Document) applet is a flexible and versatile Java Card™ applet for electronic ID cards and travel documents. It relies on field-proven, hardware-based security technology from Infineon offering optimized transaction performance especially for electronic government documents.

The eMRTD applet runs on the SECORA™ ID S Java Card™ platform, which is based on Infineon's SLC52 security chip featuring Integrity Guard security technology.

It offers the optimum open environment for electronic ID cards 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 and 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 licenses 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.

In addition, the eMRTD applet is highly configurable and can easily support different local or domestic requirements without software modifications. This makes it suited to other use cases such as electronic health cards, while still complying with Common criteria (CC) certification.

Applet key features

eMRTD applet crypto protocols

- › BAC
- › PACE: generic mapping up to 512 bits
- › AA: RSA up to 2048 bits, ECC up to 521 bits
- › EACv1-CA: ECDH 512/521 bits
- › EACv1-TA: ECDSA 512/521 bits

Applet certifications

- › eMRTD applet: CC EAL 5+
 - BSI-CC-PP-0055
 - BSI-CC-PP-0056
 - BSI-CC-PP-0068 included

eMRTD applet use cases

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

eMRTD applet from Infineon applet collection

On SECORA™ ID S Java Card™ platform

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 (4096 bits on request)
- › 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 V 2.21
- › ISO/IEC 18013 -2, -3, -4, latest versions

Certifications

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

Published by
Infineon Technologies AG
81726 Munich, Germany

© 2020 Infineon Technologies AG.
All Rights Reserved.

Please note!

This Document is for information purposes only and any information given herein shall in no event be regarded as a warranty, guarantee or description of any functionality, conditions and/or quality of our products or any suitability for a particular purpose. With regard to the technical specifications of our products, we kindly ask you to refer to the relevant product data sheets provided by us. Our customers and their technical departments are required to evaluate the suitability of our products for the intended application.

We reserve the right to change this document and/or the information given herein at any time.

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.