Product brief

ISO FS applet from Infineon applet collection

On SECORA™ ID S Java Card™ platform

The ISO FS (File System) applet is one of the most essential part of Infineon applet collection, enabling designers to customize ID documents in accordance with individual needs. Data is stored and protected by the same secure authentication mechanisms applied to electronic passports and eIDs. This applet relies on field-proven, hardware-based security technology from Infineon offering optimized transaction performance especially for electronic government documents.

The ISO FS 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 ISO FS applet provides a robust basis for designing customized ID documents. It allows customer data to be securely stored, protected by well-trusted security protocols typically used for eMRTD (electronic Machine Readable Transport Document) applications. This personal or security-sensitive information can be stored in any format, including simple text and binary data such as facial images and fingerprints. This applet supports the following security protocols: Basic Access Control (BAC), PACE (Password Authenticated Connection Establishment), Active Authentication (AA) and Extended Access Control (EAC) – all of which comply with ICAO Doc 9303 specifications. It also supports full customization of ID documents spanning national eIDs, voter ID cards, health insurance cards and vehicle registration cards.

The ISO FS applet is designed according to the ISO/IEC 7816-4/8/9 standards.
Infineon offers customers full flexibility to design the ID document of their choice. With the dedicated File System Explorer software tool, customers can visually define their individual file structure, personalize their files, and test and verify the final document in operation.

Complementing this customization tool, Infineon offers a set of default document profiles, where dedicated file structures and security protocols are pre-defined to support common use cases. Hence, customers can take a default profile as a starting point and rapidly personalize it for an almost "off-the-shelf" solution aligned with individual needs.

The document profiles supported by the ISO FS applet are listed overleaf. All document profiles can of course be extended or adapted to meet individual requirements.

Applet key features

ISO FS 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

ISO FS applet use cases

- Store voter information on voter ID cards
- Store permissions for accessing governmental services
- Store loyalty information for loyalty programs
- Store vehicle data for eVehicle registration
- Store medical records, health insurance data for eHealth use cases
- Customer-defined applications

ISO FS applet from Infineon applet collection

On SECORA™ ID S Java Card™ platform

Health insurance card profile: This default profile is especially designed around the needs of ID cards in the health sector. It offers storage capacity for basic personal information, a facial image, a social security number and health information – all of which is protected by strong security protocols. This profile is aligned with the European Health Insurance Card (EHIC).

Voter card profile: A voter card typically includes personal information to uniquely identify the voter, establish eligibility to vote and prevent the holder from voting multiple times. All this information needs to be strongly protected by cryptographic mechanisms, e.g. by a secret PIN known only to the holder. The ISO FS voter card profile supports all of these requirements.

Vehicle registration profile: These type of cards usually confirm that a certain vehicle has been duly registered with a trusted authority. Typical datasets stored on such cards include car type, registration number and registration date. The profile may also specify different access granted to the card holder or other authorized persons. This profile is based on European Union directives.

Plattform key features

Platform compliance

- Java Card™ 3.0.5, Classic
- Global Platform® 2.3.1,
  - GP ID Configuration 1.0
  - GP Mapping Guidelines V1.0
  - SCP02, SCP03

Cryptography

- RSA up to 2048 bits (4098 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

- ISO/IEC 7816-4
- ISO/IEC 7816-8
- ISO/IEC 7816-9

Certification

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

Published by
Infineon Technologies AG
81726 Munich, Germany

Document number: B181-I1044-V1-7600-EU-IC
Date: 08/2020