Product brief

PKI applet on Oracle's Java Card™ on Infineon's SLE 78

Infineon releases the latest version of its PKI applet on a modern Java Card platform from world leading hardware and software providers.

The PKI applet is part of a solution consisting of the SLE 78, the industry's most advanced security controller using Integrity Guard, and Oracle's latest Java Card implementation Edition 2. This platform is under certification CC EAL5+ (high). It offers the ultimate open environment for eGovernment and enterprise applications.

This PKI applet can support the following basic use cases

- Online assurance of an identity: **eAuthentification**
- Enabling authenticity and integrity of data: **eSignature**
- The process of determining - given an established identity – what privileges someone is entitled to: **eAuthorization**
- Secured information transfer, enabling confidentiality: Data En-/Decryption

Moreover, the applet can be used for the digitally signing of electronic documents, logging in to Windows systems, or for authentication for online services.

The PKI applet supports all functionality required to act as a secured and qualified signature creation device (SSCD, QSCD). The applet supports on-card key generation, as well as key import, based on elliptic curves and RSA. Secured communication is enabled by relying on PACE- a well-established security protocol, supporting PIN, PUK, and CAN.

The PKI applet is designed to be highly configurable to match local requirements, without the need for software modifications. Thus, the PKI applet can support many use cases and still keeping its Common Criteria certification. The applet is targeted to be certified as CC EAL4+ (high).

Sample evaluation

Memory sizes depend on configuration: 80 KB are available with GP-eSign. Other user memories are possible with other configurations (i.e. up to 130 KB with GP Basic)

Product	User memory [kB]	Features	SP Number
SLJ 52GDA080DC	80	Dual interface (T-M8.4) with preloaded PKI applet	SP001698238
SLJ 52GLA080DC	80	Contactless (MCS8i) with preloaded PKI applet	SP001698276
SLJ 52GCA080DC	80	Contact based (MFC6.8) with preloaded PKI applet	SP002035202
SLJ 52GDA080DC	80	Dual Interface with Coil On Module (CML1) with preloaded PKI applet	SP002035210

Key features

Typical use cases

- eSignature
- eAuthentication
- eHealthcare
- eSocial security
- Secured file transfer
- eVoting
- eTax

Cryptographic functions

- ECC up to 512 bits
- RSA up to 2048 bits
- SHA1, SHA-256, SHA-384 and SHA-512
- 3DES and AES up to 128 bits

Communication interfaces

- ISO/IEC 7816 up to 312 kbit/s
- ISO/IEC 14443 A/B up to 848 kbit/s
- ISO/IEC 14443 VHBR up to 6.8 Mbit/s

Supported international standards

- ISO/IEC 7816, PKCS #15
- Design based on BSI TR-03117
- BSI TR-03110

Java Card platform features

- Java Card 3.0.1
- Global Platform 2.2
- Common Criteria EAL 5+ certification

Other applets for Oracle's Java Card™ Operating System on Infineon's SLE 78

The flexibility of our fully certified Java Card platform, including state-of-the-art cryptography, enables the installation of various applets and different configurations for each. In addition to the PKI applet, Infineon has qualified the **eMRTD applet** provided by MaskTech GmbH to cover additional use cases.

eMRTD applet
The main use case of this applet is the **ePassport** functionality. It supports the ICAO Doc 9303 standard series in its latest edition. The contactless interface complies with the latest ISO/IEC 14443 standards, offering VHBR (Very High Bit Rates). The data transmission rate can reach up to 6.8 Megabit per second.
This Java Card applet is designed to be highly configurable, to enable further use cases. Thus, this applet can also be used for **eDriver's Licences**, as it complies with the ISO/IEC18013 standard series for international driving licenses.

Match-on-card (biometric API) library
The Match-on-Card (MoC) library supplied by Neurotechnology offers an ISO/IEC 19794-2 compatible, MoC solution, enabling fast biometric authentication in addition to traditional PIN authentication.

A second version of **the PKI applet** (provided by MaskTech GmbH) can be combined with this Match-On-Card (MoC) library, allowing for convenient fingerprint authentication, instead of using a PIN. Combined with the **eMRTD applet**, this **PKI applet** can provide a fully-fledged national eID solution.

Infineon offers a **ready-to-go applet** portfolio, supporting long-lasting, secure eGovernment and enterprise solutions. We partner with approved Java Card developers, who have developed qualified applets for our platform, to deliver customer-specific use cases and functionality. These partners also develop customized software on demand.

Infineon Technologies AG
Infineon is an innovative and long-standing supplier of hardware-based secure ID solutions and the leading manufacturer of chip card controllers. More than 150 reference projects across all Government ID applications, covering 75 percent of the world's population, trust Infineon's solutions.

MaskTech GmbH
MaskTech is the leading independent provider of high security operating systems and related embedded applications. The company's solutions are used in more than 65 countries' secure travel and ID documents as well as providing strong authentication solutions worldwide.

Neurotechnology
Neurotechnology provides recognition algorithms and SDKs for different biometric modalities and licenses more than 2,500 system integrators and hardware providers in more than 100 countries.

Integrity Guard
SOLID FLASH™
VHBR

Biometric and Artificial Intellignece Technologies

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.

Order Number: B181-I0604-V1-7600-EU-EC
Date: 05 / 2018