



Product Brief

Oracle's Java Card™ operating system on Infineon's SLE 78

A modern Java Card platform from world leading hardware and software providers, offering the best foundation for any Java Card eco-system.

The combination of the SLE 78 with Integrity Guard, industry's most advanced security controller, with Oracle's latest Java Card implementation offers the ultimate open platform for eGovernment and enterprise applications. It enables designers, manufacturers and other stakeholders to easily introduce tailored applications without compromising on security. It facilitates the implementation of multiple applications such as ePassport, eSignature or eHealth on a single card.

The key features of this platform are:

- › **Adaptability:** the wide catalogue of high-performance ready-to-go applets provides advantages in terms of time to market and reliability to manufacturers, service providers and governments alike.
- › **Security with Integrity Guard:** this exclusive, award-winning technology is the world leading reference for digital security. It is based on a dual-CPU core with fully encrypted data path, each CPU continuously monitoring each other's operation. It expands the lifecycle for long-lasting eID documents.
- › **Certification:** this Java card open platform combining the SLE 78 (hardware CC certified EAL6+ high) and the Oracle Java Card OS is CC EAL5+ (high) and FIPS 140-2 level 3 certified.
- › **Performance:** the Oracle Java Card virtual machine is reaching outstanding speeds for best applet performance. Software developers can now develop on one of the most powerful Java Card virtual machines for smart cards.

Product	User memory [kB]	Features
SLJ 52GLA080AR	80	Contactless preloaded BAC/SAC/AA/EAC ePassport
SLJ 52GLA080BR	80	Contactless preloaded EAP eDriver's license
SLJ 52GLA128CR	128	Contactless 16-bit open platform with Oracle Java Card implementation

Key features

Typical applications

- › ePassport (ICAO 9303, BAC, EAC, AA, SAC)
- › eDriver's license (ISO/IEC 18013, BAP, EAP, SAC, EAC)
- › eSignature (CEN 15480-2, EN 419211, PIN, PUK, PKCS#15)
- › eHealth care
- › eSocial security
- › Biometric fingerprint match-on-card (ISO/IEC 19794-2)

Cryptographic & arithmetic functions

- › RSA up to 3072 bits
- › Elliptic curves up to 512/521 bit
- › TDES, AES up to 256 bit
- › SHA2 up to 512 bit
- › SEED up to 128 bit
- › Extended length APDU up to 32 kB

Communication interfaces

- › ISO/IEC 7816 up to 312 kbps
- › ISO/IEC 14443 A/B up to 848 kbps

Platform compliance

- › Java Card 3.0.1
- › GlobalPlatform 2.2.1, ID config 1.0
- › NFC ready
- › ANSSI-CC-PP-2010/03 open conf.

Applications for Oracle's Java Card™ operating system on Infineon's SLE 78

The flexibility of our fully-certified Java Card platform, including strong state-of-the-art cryptography, enables several kinds of applications.

We also offer a **ready-to-go application portfolio** supporting long-lasting secure eGovernment and enterprise services. Via post issuance, the application can be updated or loaded after issuance without replacing the entire eID document.

National eID & match-on-card (biometric API)

Binding the Match-on-Card (MoC) library (supplied by Neurotechnology) with the National eID application (provided by MaskTech) offers an ISO/IEC 19794-2 compatible MoC solution.

The latest algorithm is fully rotational invariant with an average card holder matching speed less than 150 ms.

The ID applets by MaskTech cover the following applications:

ePassport – ICAO Doc 9303

Support of all data groups defined in the ICAO standard and the following security protocols: Basic Access Control (BAC), Active Authentication (AA), Extended Access Control (EAC), Supplemental Access Control (SAC/PACE).

eDriver's licence – ISO/IEC 18013

This applet complies with the ISO/IEC standard 18013 and the EU directive 2006/126/EC. It secures the storage of and the access to personal data with the security protocols: Basic Access Protocol (BAP), EAP, SAC, and EAC.

eSign

This applet supports secure electronic signature creation and secure authentication at online services. It supports state-of-the-art cryptography and authentication protocols ensuring also a maximum of data privacy. The applet can be used for Windows or web service log on. It supports on-card key generation based on ECDSA and RSA.

Infineon Technologies AG

Infineon is an innovative and long-standing supplier of hardware-based secure ID solutions, leading the chip card controller market for 15 consecutive years. 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 including secure travel and ID documents as well as strong authentication products are used in more than 65 countries 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.



Published by
Infineon Technologies AG
81726 Munich, Germany

© 2017 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.

Order Number: B181-I0046-V4-7600-EU-EC-P
Date: 04 / 2017