

Product brief – Edition 2

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 Infineon's SLE 78 with Integrity Guard, industry's most advanced security controller, with Oracle's latest Java Card Edition 2 implementation offers the ultimate open platform for eGovernment and enterprise applications. This Java Card platform 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 Java Card platform are:

- › **Security with Integrity Guard:** this exclusive, award-winning technology is the world leading reference for digital security. The Integrity Guard technology relies on a dual CPU concept with encrypted data path, continuously monitoring each other's operation. It expands the lifecycle for long-lasting eID documents.
- › **Certification:** this Java Card open platform is certified **CC EAL5+ (high)**, whereas the Infineon's hardware SLE 78 is certified CC EAL6+ (high).
- › **Performance:** the Oracle Java Card virtual machine is reaching outstanding speeds for best applet performance. The applet developers can now develop for one of the most powerful Java Card virtual machines for smart cards.
- › **Communication:** the contactless interface complies with the latest ISO 14443 standards offering VHBR (**Very High Bit Rates**). The data transmission rate can reach 6.8 Mbps.
- › **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.
- › **Reliability:** the innovative "**coil on module**" package technology from Infineon uses a RF link, rather than the common mechanical-electrical connection, between the card antenna and the chip module, so improving ruggedness of the final assembly.

Oracle's Java Card™ operating system on Infineon's SLE 78 (Edition 2)

Product	User memory [kB]	Features	SP Number
SLJ 52GDA080CC	80	Dual Interface T-M8.4 Open Java Card Platform with GP-ID config without VHBR	SP002466368
SLJ 52GCA080CC	80	Contact based MFC6.8 open Platform with GP-ID config without VHBR	SP002466362
SLJ 52GLA080CC	80	Contactless MCS8 open Platform with GP-ID config without VHBR	SP002466372
SLJ 52GLA080CC	80	Contactless Coil on Module 10.6 open Platform with GP-ID config without VHBR	SP002167944
SLJ 52GLA080VC	80	Contactless MCS8 open platform with GP-ID config with VHBR	SP002466352

Key features

Platform compliance

- › Java Card 3.0.1, classic
- › GlobalPlatform 2.2.1, ID config 1.0

Communication interfaces

- › Dual interface
- › ISO/IEC 7816 up to 312 kbps
- › ISO/IEC 14443 type A/B up to 848 kbps
- › ISO/IEC 14443 VHBR up to 6.8 Mbps

Certification

- › Infineon SLE 78 – CC EAL 6+
- › Oracle Java Card OS – CC EAL 5+

Cryptographic and arithmetic functions

- › RSA up to 2048 bits
- › Elliptic curves up to 512/521 bit
- › TDES, AES up to 256 bit
- › SHA2 up to 512 bit
- › Extended length APDU up to 32 kB

Typical applications

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

Packaging

- › Contact based
- › Contactless
- › Dual interface
- › Coil on module

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 secured eGovernment and enterprise services. Via post issuance, the application can be updated or loaded post-issuance without replacing the entire eID document.

The ID applets by MaskTech cover the following applications:

National eID and 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 has ± 180 degrees (unlimited) fingerprint rotation tolerance.

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 and the access to personal data with the security protocols: Basic Access Protection (BAP), Extended Access Protection (EAP), BAC, EAC, and PACE (Password Authenticated Connection Establishment).

eSign

This applet supports secured electronic signature creation and secure authentication at online services. It supports state-of-the-art cryptography and authentication protocols allowing 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 Elliptic Curve Cryptography (ECC) 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.



VHBR



Integrity Guard



SOLID FLASH™



Published by
Infineon Technologies AG
81726 Munich, Germany

© 2018 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.