infineon

Product Brief

Oracle's Java Card operating system on 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 eGoverment and enterprise applications. It enables any stakeholders to easily introduce tailored applications, like ePassport, eSignature or eHealth on a single card.

The 5 key performance 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.
- **Communications**: 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.
- **Security with Integrity Guard**: this exclusive technology is the world leading reference for digital security. It is based on a dual-CPU core with fully encrypted data path. It expands the lifecycle for long-lasting eID documents.
- **Certification**: this Java Card open platform combining the SLE 78 (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. The applet software developers can now develop for one of the most powerful JCVM for smart cards.

Sample evaluation

Product	User memory[1]	Features
SLJ 52GLA080AR	80 kB	Contactless preloaded SAC/BAC/AA/EAC ePassport
SLJ 52GDA080BR	80 kB	Dual interface preloaded EAP eDriver's license
SLJ 52GDA080DR	80 kB	Dual interface preloaded National eID/eSign
SLJ 52GDA128CR	128 kB	Dual interface open platform with Oracle Java Card implementation
SLJ 52GLA128CR	128 kB	Contactless open platform with Oracle Java Card implementation
SLJ 52GCA128CR	128 kB	Contact based open platform with Oracle Java Card implementation

1) Memory sizes are depending on configuration

Key features

Typical applications

- ePassport (ICAO 9303, BAC, EAC, AA, SAC, EAL4+ targeted)
- eDriver's license (ISO/IEC 18013, BAP, EAP)
- eSignature (CEN 15480-2, CEN 14890, PIN, PUK, PKCS#15, EAL4+ targeted)
- eHealth care
- eSocial security
- Biometric fingerprint match-on-card (ISO 19794-2)

Cryptographic & arithmetic functions

- RSA up to 3072 bits
- Elliptic curves up to 512/521 bit
- TDES and AES up to 256 bit
- MD5 and 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: 848 kbps
- ISO/IEC 14443 VHBR < 6.8 Mbps

Platform compliance

- Java Card 3.0.1
- Global platform 2.2.1, ID config 1.0
- NFC ready
- ANSSI-CC-PP-2010/03 open conf.
- CIPURSE™ V2 compliant

Integrity Guard

VHBR SOLID FLASH™

Applications for Oracle's Java Card operating system for SLE 78

The flexibility of our fully certified Java platform, including the state-of-the-art cryptography, enables several kinds of application configurations.

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 whole eID document.

National eID & match-on-card (biometric API)
Binding the match-on-card library (supplied by Neurotechnology), with the National eID application (provided by MaskTech), offers an ISO 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: 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 of personal data with the protocols: Basic Access Protocol (BAP), AA, EAC and SAC/PACE.

eSign: Secure electronic signature creation for online services can be protected by PACE: this protects authentications like PIN, PUK, CAN, for a maximum of data privacy. It can be used for Windows log on or for log on to a web service. 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. More than 150 reference projects across all Government ID applications in 69 countries (73% of the world's population) trust Infineon's solutions.

Oracle

With more than 400,000 customers and with deployments across a wide variety of industries in more than 145 countries, Oracle offers a comprehensive and fully integrated stack of cloud applications, platform services, and engineered systems.

MaskTech GmbH

MaskTech is the leading independent provider of high security operating systems and related embedded applications. The companies solutions are used in more than 65 countries secure travel and ID documents as well as 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.

CIPURSE™ is a trademark of the OSPT Alliance

Java Card and the coffee cup logo are registered trademarks of Oracle and/or its affiliates.

Published by
Infineon Technologies AG
85579 Neubiberg, Germany

Order Number: B181-I0046-V3-7600-EU-EC
Date: 04 / 2016

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.