

Product brief

jTOP ID on SLE 78

Java Card™ platform for government ID projects

jTOP ID is a versatile Java Card 3.0 and GlobalPlatform 2.2.1 compliant platform based on the SLE 78 controller family from Infineon with the award winning Integrity Guard digital hardware security. Together with the Trusted Logic operating system this platform delivers the highest security level, compliance to international standards and flexibility ready for smooth integration into a wide range of governmental infrastructure.

Application fields

jTOP ID supports all major governmental applications such as national eID, electronic driver's license, eHealth, electronic social security and ePassport. The LDS and eSignature applets are compliant to the ICAO 9303, ISO/IEC 18013 and EN 14890 standards respectively and support RSA as well as elliptic curve based cryptography. Custom applets can be developed with the on-card debugger and rolled out using the IDE. This software can use the Java Card extensions for government ID of the platform (fast personalization, readout and PACE/SAC protocols). Full compliance to the GlobalPlatform ID configuration makes this platform the perfect fit for either standard compliant or country specific projects needing the highest interoperability, performance and security requirements. An EAC dataset of 43 KB can be read out at border control in less than 3.5 s.

Certified, long-lasting security

The jTOP ID platform is based on Infineon SLE 78 security controllers with Integrity Guard – the new standard for long lasting secure eGovernment. These CC EAL 5+ certified controllers feature an unrivalled full encryption of the data path. Even within the CPU, data is only processed in encrypted form. Digital error detection over the complete data path is completed by two CPUs that continuously monitor each other's operation.

The platform provides a defensive virtual machine and is certified CC EAL 5+ following the latest Java Card protection profile. On top of this platform, the applets are certified EAL4+ following the ePassports and eSignature protection profiles. Also, using state of the art cryptography, GovID extensions and post issuance functions are certified with the platform and may be used in tailored applets.

Cryptography

- › RSA up to 2048
- › Elliptic curves up to 512/521 bits
- › TDES and AES up to 256
- › MD5 and SHA2 up to 512

Key features

Communication

- › ISO/IEC 7816 contact based
- › ISO/IEC 14443 type A
- › ISO/IEC 14443 type B
- › Extended length 32 KB

Platform compliance

- › BSI TR-03110, 03105-2/3.1/3.2
- › ISO 18013 part 1–4
- › Java Card 3.0.4
- › GlobalPlatform 2.2.1
- › GlobalPlatform ID configuration 1.0
- › Multiple SD, delegated management and mandated DAP
- › PP JCS open configuration ANSSI-CC-PP-2010/03

LDS applet

- › BAC/AA/EAC/SAC
- › BAP/EAP configurations 1 to 4
- › BSI PP 0055, 0056 and ANSSI PP 2010-06

eSignature applet

- › ISO 7816-4/8/9 and EN 14890
- › PIN/PUK and optional MoC authentication
- › Windows minidriver V6.02
- › BSI PP 0059

jTOP ID on SLE 78

Java Card™ platform for government ID projects

Broad portfolio for government solutions

jTOP ID is part of a family of products, that use the jTOP operating system on Infineon chip card controllers and will be supported in the future in new technologies. Available in different configurations and hardware, the family provides tailored solutions for government projects ranging from basic configurations to complex feature combinations. Different memory configurations from 36 KB up to 160 KB are at hands to store the required amount of personal data.

On request, project specific adaptations are possible to cover specific requirements – ready for personalization to decrease handling and personalization costs.

Easy deployment & smooth integration

jTOP ID is supported by tools for applet development, debug and platform configuration. Integration into production processes is easily possible through third party middleware that supports jTOP. On top of the dual interface capability both standardized contactless communication types (ISO/IEC 14443 type A and type B) are available, as well as a NRG¹⁾ 1 k/4 k emulation, allowing integration with readers from many vendors and usable in a variety of other applications such as access control or transport. Due to its full Java Card/GlobalPlatform compliance, third party applets can be loaded with confidence on to the platform (e.g. match-on-card). The jTOP ID platform is available in all Infineon standard packages for government ID projects (dual interface, contactless and contact based) that have proven reliability in governmental projects around the world.

Product configurations

Product	E ² PROM [KB] ²⁾	Interfaces ²⁾	Applet
SLJ 52GCAxxxBL	up to 150	Contact-based T = 0 and T = 1	LDS: BAP/AA/EAP
SLJ 52GCAxxxCL	up to 150	Contact-based T = 0 and T = 1	Open platform
SLJ 52GCAxxxDL	up to 150	Contact-based T = 0 and T = 1	ePass, eDriver license and eSignature
SLJ 52GLAxxxAL	up to 150	Contactless type A or type B (default)	LDS: BAC/SAC/AA/EAC
SLJ 52GDAxxxBL	up to 150	Contactless type A or type B (default) and (contact-based T = 0 and T = 1)	LDS: BAP/AA/EAP
SLJ 52GDLxxxCL	up to 150	Contactless type A or type B (default), NRG ¹⁾ 1 k/4 k and contact-based T = 0 and T = 1	Open platform
SLJ 52GDLxxxDL	up to 150	Contactless type A or type B (default), NRG ¹⁾ 1 k/4 k and contact-based T = 0 and T = 1	ePass, eDriver license and eSignature
SLJ 52GLA080DL	up to 80	Contactless type A or type B (default)	ePass, eDriver licence and eSignature

1) ISO/IEC 14443-3 type A with CRYPTO1

2) E²PROM available in 36 KB, 80 KB, 128 KB & 150 KB

Infineon and Trusted Logic

jTOP ID combines the strengths of three of the main players in the government ID market worldwide: Infineon, Trusted Logic and cryptovision. Infineon is an innovative and long-standing supplier of hardware-based secure ID solutions, leading the chip card controller market for more than 15 consecutive years. In Europe, the leading region for new governmental applications, over 75 percent of the national eID projects rely on chips from Infineon. In addition, many high economic growth countries such as Brazil, Turkey, India, Indonesia & China trust in

Infineon secure controllers for their new eID documents. In the field of healthcare, 60 percent of the smart health cards worldwide use Infineon chips. Trusted Logic SA is a Java Card pioneer, providing open and secure software for smart cards, terminals & consumer devices. Its subsidiary Trusted Labs has written the Java Card protection profile, which is used across the industry for Java Card multi-application platform certifications. Cryptovision is a leading supplier of innovative cryptography & public key infrastructure (eSign) products.

Published by
Infineon Technologies AG
81726 Munich, Germany

© 2019 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.