

Product brief

ePasslet Suite by cryptovision GmbH

On SECORA™ ID X Java Card™ platform

The ePasslet Suite by cryptovision GmbH on SECORA™ ID X is a flexible and efficient Java Card™ solution. It is a very user-friendly Java Card™ framework that supports a complete set of applications for implementing electronic ID cards, travel documents, driver's licenses and other similar electronic documents. It complies with various international standards. It relies on field-proven, hardware-based security technology from Infineon, which offers optimized transaction performance especially for electronic government documents.

The ePasslet Suite by cryptovision GmbH runs on the SECORA™ ID X Java Card™ platform based on Infineon's SLC52 security chip featuring Integrity Guard security technology.

SECORA™ ID X is a dynamic Java Card™ 3.0.5 platform, which offers optimized APIs for electronic document use cases.

The SECORA™ ID X platform supports dual-interface, contactless and contact-based communication interfaces. It is compliant with both ISO/IEC 7816 and ISO/IEC 14443 Type A/B. The dual and contactless interfaces support the latest ISO/IEC 14443 VHBR (Very High Bit Rate) standard, which can achieve a data transmission rate of up to 6.8 megabits per second. In addition, this platform enables post-issuance.

The ePasslet Suite on SECORA™ ID X provides applets for various eID document applications, including electronic passports, eIDAS-compliant ID and signature cards, international electronic driver's licenses, electronic health cards (eHIC), custom national eID cards and more. With this ePasslet Suite, several applications with common resources can be realized on the same card. The document's functional scope can be easily extended from the ePasslet Suite core, even by loading additional code onto cards that have already been issued.

Applet key features

Three editions to choose from

- > Edition 1
 - ICAO eMRTD with BAC and PACE
 - ISO 7816 file system
 - ISO driving license with BAP, BAC and PACE
- > Edition 2 with the additional features
 - ICAO eMRTD with EAC v1 (including BAC and PACE)
 - ISO driving license with EAC v1 or EAP (including BAP/BAC/PACE)
 - ePKI/secure signature creation device
 - Vehicle registration
 - Health insurance card
- > Edition 3 with the additional features
 - German eID card with EAC v2, restricted identification and auxiliary functions
 - EU residence permit
 - European citizen card (identification, authentication, signature)
 - eIDAS token functionality
 - Custom eID application

Applet certification

- > ePasslet Suite by cryptovision GmbH on SECORA™ ID X targets CC EAL 5+
 - BSI-CC-PP-0055
 - BSI-CC-PP-0056
 - BSI-CC-PP-0059
 - BSI-CC-PP-0075

ePasslet Suite by cryptovision GmbH

On SECORA™ ID X Java Card™ platform

This ePasslet Suite enables the complete implementation of an electronic Machine Readable Travel Document (eMRTD) according to International Civil Aviation Organization (ICAO) specifications. It supports the security protocols Basic Access Control (BAC), Password Authenticated Connection Establishment (PACE) and Extended Access Control (EAC).

In addition, the ePasslet Suite on SECORA™ ID X can be freely customized through various configuration options. So it can evolve to support new use cases and applications while retaining Common Criteria (CC) certification. It thus enables multiplication cards and documents.

The ePasslet Suite on SECORA™ ID X is available in three editions, offering cost-efficient configurations for standard as well as high-end and customized ID document solutions.

Plattform key features

Platform compliance

- › Java Card 3.0.5, Classic
- › Global Platform® 2.3.1
 - GP ID Configuration v1.0
 - GP Mapping Guidelines v1.0
 - SCP02, SCP03

Cryptography

- › RSA up to 4096 bits
- › Elliptic curves up to 521 bits
- › TDES
- › AES up to 256 bits
- › SHA1, SHA2 up to 512 bits
- › Accelerated by crypto coprocessors

Plattform key features

Communication interfaces

- › Dual interface
- › ISO/IEC 7816-3, T=0, T=1
- › ISO/IEC 14443 Type A/B up to 848 kbps (extended length APDU up to 32 kByte)
- › ISO/IEC 14443 VHBR up to 6.8 Mbps

Supported international standards

- › ICAO Doc 9303 7th edition
- › BSI TR-03110 -1, -3, -4 V2.21
- › ISO/IEC 18013 -2, -3, -4, latest versions
- › ISO/IEC 7816-15, PKCS #15

Certification

- › SLC52G: CC EAL 6+, EMVCo
- › SECORA™ ID platform: CC EAL 6+, EMVCo

cv cryptovision GmbH

cryptovision is an expert for highly efficient secure encryption techniques. Based in Gelsenkirchen, Germany, the company offers innovative cryptography and electronic identity solutions.

Published by
Infineon Technologies AG
81726 Munich, Germany

© 2020 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.