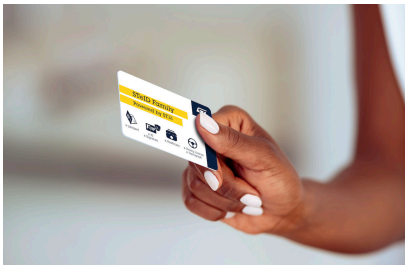
Secure Java Card™ solutions for e-Identity and e-Government



Product status link
STeID-Java

Features

Operating system

- Open Java Card™ operating system
- Java Card™ 3.0.5
- Global platform 2.3.1
- Cryptographic support (DES, AES, RSA, EC)
- Biometric Java Card™ API
- Post-issuance
- Match-on-card support
- Certified CC EAL 6+ (ongoing)

Java Card applets

- eMRTD applet supporting
- Basic Access Control (BAC)
- Extended Access Control (EAC)
- Password Authenticated Connection Establishment (PACE)
- ePKI applet with Key generation and Key import
- All applets to be CC certified

Key hardware features

- Dual Core 32-bit ARM® SecurCore® SC000™
- RSA, EC, AES, and DES coprocessors
- AIS-31 class PTG.2 compliant true random number generator (TRNG)
- ISO 7816 and ISO 14443 with best-in-class RF performance
- Data retention >25 years
- Endurance (erase/write cycling) >500 K cycles
- Certified CC EAL 6+

Application features

- Electronic ID and national eID
- Electronic passports
- Electronic residence permit
- Electronic health and social security cards
- Electronic driving license
- Electronic vehicle registration card
- Electronic voting card
- Electronic company, governmental administration cards
- Electronic card used in Public Key Infrastructure such as digital signature
  - Secure Signature Creation Device (SSCD)
  - Qualified Signature Creation Device (QSCD) according to eIDAS

1 Description

The STeID Java is a complete solution targeting the Identity and eGovernment markets, and possibly other projects requiring a high-end Java Card OS platform on a smartcard IC. It is developed on the secure microcontroller ST31N600 and includes:

- STeID JC Open OS, which is based on an open Java multi-application platform,
- and a set of Java applets dedicated to the ID market.

The STeID Java is enabled with Java Card technology allowing multiple applications to run on a single card and provides features for secure interoperability of applications. It also provides a secure framework for the execution of the Java Card programs and data access management (via firewall).

2 General information

2.1 Trademarks and references

The STeID JC OS is compliant with Java Card platform, Classic edition 3.0.5.

Note: Java Card is a registered trademark of Oracle corporation.

The ST31 secure microcontrollers are based on Arm® SecurCore®.

Note: Arm and SecurCore are registered trademarks of Arm Limited (or its subsidiaries) in the US and/or elsewhere.

2.2 Compliance with standards

- ISO/IEC 7816
- ICAO Doc 9303, BSI TR-03110
- ISO/IEC 18013-3 and ISO/IEC TR 19446 (eDL)
- ISO/IEC 19794

3 Application features

The STeID JC Open OS provides all the features needed to host important applications for electronic identity (eID) and eGovernment use cases:

- Java Card 3.0.5 card application framework
- Global Platform® 2.3.1 security and card -management architecture
- DES, 3DES, AES, RSA cryptographic algorithms
- EC, ECDSA, ECDH with all supported curves and key sizes
- Secure Channel Protocol
- Post-issuance
- Match-on-card for secure offline biometric authentication.

The eMRTD applet compliant with the International Civil Aviation Organization ICAO 9303 standard supports implementation of eIDs requiring:

- Basic access control
- Extended access control
- Password authenticated connection establishment (PACEv2)

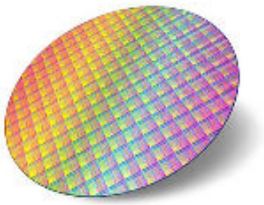
It supports access protection schemes as used for eDLs according to ISO/IEC 18013.

The ePKI applet makes the STeID Java a Secure Signature Creation Device (SSCD) and an eIDAS Qualified Signature Creation Device (QSCD). The ePKI applet allows the generation and the importation of Signature Creation Data (SCD), and offers qualified digital signatures over contact and contactless interfaces.

The STeID Java incorporates support for NFC specifications thereby providing a secure framework for digital identity applications on NFC-enabled mobile devices.

4 Delivery forms

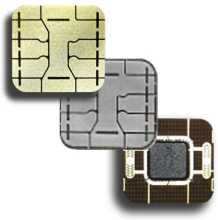
The product is available for delivery in several formats as detailed below:



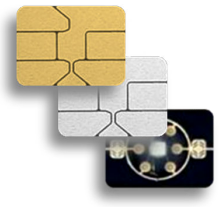
Wafer

Contactless Micromodule

Wafer-level chip-scale packages



8-pin



6-pin

Contact and Dual Interface Micromodule (8-pin and 6-pin)

Appendix A

A.1 Glossary

This section lists all the terms that are used in this document.

Table 1. Glossary

Term	Description
AES	Advanced encryption standard
BAC	Basic access control
DES	Data encryption standard
DH	Diffie-Hellman
EAC	Extended access control
ECDH	Elliptic curve Diffie–Hellman
ECDSA	Elliptic curve digital signature algorithm
eID	Electronic ID
ICAO	International Civil Aviation Organization
OS	Operating system
PACE	Password authenticated connection establishment
RSA	Ron Rivest, Adi Shamir and Leonard Adleman Public-key cryptosystem
QSCD	Qualified signature creation device
SSCD	Secure signature creation device
TRNG	True random number generator

Revision history

Table 2. **Document revision history**

Date	Revision	Changes
11-June-2024	1	Initial release.

Contents

List of tables