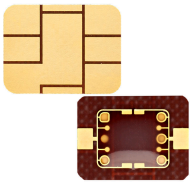
J-SIGN4

Data brief

Java® Card for digital signatures



D7G-D17 micromodule

ISO 7810 ID-1 smartcards with 2FF or 3FF SIM form factor

Product status link
J-SIGN4

Features

Hardware features

- Arm® SecurCore® SC000™ 32-bit RISC core
- Contact assignment compatible with ISO/IEC 7816-3 standards
- Asynchronous receiver transmitter (IART) for high-speed serial data support (ISO/IEC 7816- 3 and EMV® compliant)
- RF universal asynchronous receiver transmitter (RFUART) in contactless mode compliant with ISO/IEC 14443 Type A at up to 848 Kbps
- ISO/IEC 7816 T=0 and T=1 fully supported
- Electrostatic discharge (ESD) protection greater (HBM) on contact and contactless input/outputs
- 2.7 V to 5.5 V supply voltages
- AIS-31 class PTG.2 compliant true random number generator (TRNG)
- Enhanced cryptographic algorithms
  - DES/3DES (data encryption standard), AES (advanced encryption standard), RSA and ECC (elliptic curve cryptography)
  - SHA-1, SHA-256, SHA-384, SHA-512, MD5, CRC16 and CRC32
- NESCRYPT (next step cryptoprocessor) coprocessor for public key cryptography
- Differential power analysis (DPA) and differential fault analysis (DFA) countermeasures against side-channel attacks

Security features

- Active shield
- Memory protection unit (MPU)
- Unique serial number on each die
- Enhanced NESCRYPT cryptoprocessor for public key cryptography: RSA, ECC, elliptic curve digital signature algorithm (ECDSA)
- Hardware security enhanced DES accelerator
- Random number generation compliant with PTG.2 Class and DRG.3 Class as defined in AIS-31
- Hashing algorithm: SHA1, SHA-224, SHA-256, SHA-384 and SHA-512
- Ciphering/Deciphering algorithm: DES/3DES Electronic codebook (ECB) and Cipher-block chaining (CBC) up to 192 bits, AES (up to 256 bits), RSA (up to 2048 bits)
- RSA (up to 2048 bits) and EC (up to 521 bits) key pair generation
- Digital signatures: ECDSA (EC over GF(p) up to 521 bits), RSA-PSS, RSA PKCS#1
- Key agreement schemes: Diffie-Hellmann, ECDH
- Checksum algorithm: ISO 3309 CRC-16, CRC-32
- DPA and DFA countermeasures against side-channel attacks

1 Description

The J-SIGN4 is a smartcard implementing a secure signature-creation device (SSCD) with key generation as described in the CNS application (Italian citizen service card) and according to protection profiles EN 419211-2, EN 419211-4 and EN 419211-5.

It is based on a 32-bit Arm® SecurCore® SC000™ RISC core.

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

The Arm word and logo are trademarks of Arm Limited (or its subsidiaries or its affiliates) in the US and/or elsewhere. All rights reserved.

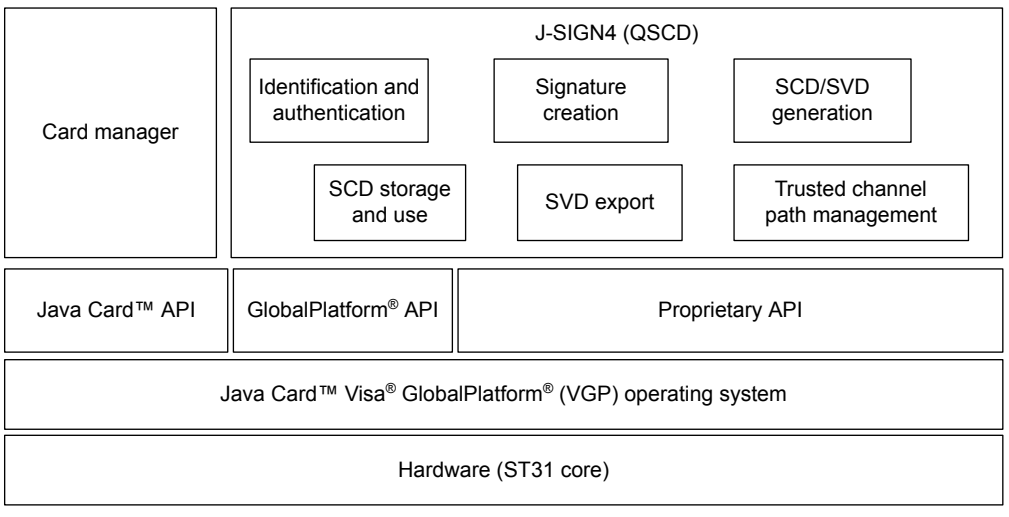
The J-SIGN4 is designed to be versatile: it guarantees high performance to secure applications, and grants the highest security level in terms of CC security certification on the hardware (EAL5+) and on the operating system (EAL4+).

It is intended to provide all required capabilities to devices involved in creating qualified electronic signatures.

The main J-SIGN4 functionality covers the following areas:

- Cryptographic-key generation and secure management
- Secure-signature generation with secure management of data to be signed
- Identification and authentication (I&A) of trusted users and applications
- Data storage and protection from modification or disclosures
- Secure exchange of sensitive data between the MCU and a trusted application
- Secure exchange of sensitive data between the MCU and a trusted human-interface device

Figure 1. Block diagram



Note: QSCD stands for qualified signature creation device, SCD is for signature creation data, SVD is for signature validation data and API is for application programming interface.

1.1 Certifications

Hardware

Common Criteria (EAL5+) certification (ANSSI CC 2019/12), based on Security IC Platform Protection Profile with Augmentation Packages (BSI PP-0084-2014).

Software

Common Criteria EAL4+ certification for the application. Protection Profile for QSCD in accordance with the eIDAS rules as outlined in "*REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014 ANNEX II*" and in "*COMMISSION IMPLEMENTING DECISION (EU) 2016/650 of 25 April 2016*":

- EN 419211-2 - Protection profiles for secure signature creation device - Part 2: Device with key generation - 2013.
- EN 419211-4 - Protection profiles for secure signature creation device - Part 4: Extension for device with key generation and trusted channel to certificate generation application - 2013.
- EN 419211-5.- Protection profiles for secure signature creation device - Part 5: Extension for device with key generation and trusted channel to signature creation application - 2013.

1.2 Package features

The J-SIGN4 is available in the following package options:

- D7G dual interface and D17 6 contact micromodules reels
- ISO 7810 ID-1 smartcards with plug-in 2FF and plug-in 3FF SIM form factors

1.3 Middleware

The J-SIGN4 can be used in a bundle with the STMicroelectronics SafeDive middleware to implement applications compliant with PKCS#11.

Revision history

Table 1. **Document revision history**

Date	Revision	Changes
14-Sep-2026	1	Initial release.

IMPORTANT NOTICE – READ CAREFULLY

STMicroelectronics NV and its subsidiaries (“ST”) reserve the right to make changes, corrections, enhancements, modifications, and improvements to ST products and/or to this document at any time without notice.

In the event of any conflict between the provisions of this document and the provisions of any contractual arrangement in force between the purchasers and ST, the provisions of such contractual arrangement shall prevail.

The purchasers should obtain the latest relevant information on ST products before placing orders. ST products are sold pursuant to ST’s terms and conditions of sale in place at the time of order acknowledgment.

The purchasers are solely responsible for the choice, selection, and use of ST products and ST assumes no liability for application assistance or the design of the purchasers’ products.

No license, express or implied, to any intellectual property right is granted by ST herein.

Resale of ST products with provisions different from the information set forth herein shall void any warranty granted by ST for such product.

If the purchasers identify an ST product that meets their functional and performance requirements but that is not designated for the purchasers' market segment, the purchasers shall contact ST for more information.

ST and the ST logo are trademarks of ST. For additional information about ST trademarks, refer to www.st.com/trademarks. All other product or service names are the property of their respective owners.

Information in this document supersedes and replaces information previously supplied in any prior versions of this document.