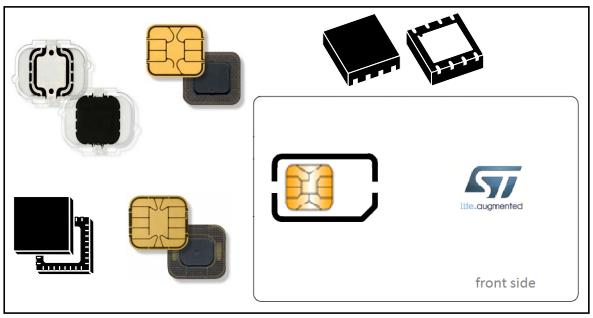
J-SIGN

80 Kbyte dual-interface Java Card™ for digital signatures

Data brief



Features

Hardware features

- Secure ST23 MCU with enhanced 8/16-bit CPU core
- 80 Kbytes of user EEPROM
- Asynchronous receiver transmitter supporting ISO 7816-3 T=0 and T=1 protocols with extended length
- ISO/IEC 14443 Type B contactless interface with RF UART up to 848 Kbps
- Supply voltage ranges: 3 V and 5 V
- 500 000 read/write cycles in EEPROM
- ESD protection greater than 6 kV (HBM)

Platform features

- Java Card™ v.3.0.4 - Classic Edition
- GlobalPlatform® v.2.1.1
- Object deletion (garbage collection) with memory reclamation
- Additional secure API for:
  - Secure storage (integrity-protected arrays)
  - Generation of random primes

Security features

- Active shield
- Memory protection unit (MPU)
- Unique serial number on each die
- Enhanced NESCRYPT cryptoprocessor for public key cryptography (RSA, ECC, ECDSA)
- Hardware security enhanced DES accelerator
- AIS-31 class P2 compliant true random number generator (TRNG)
- Hashing algorithm: SHA1, SHA-224, SHA-256, SHA-384 and SHA-512
- Ciphering/Deciphering algorithm: DES/3DES ECB and 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
- Differential power analysis (DPA) and differential fault analysis (DFA) countermeasures against side-channel attacks

Packages

- D68, D70, CB4 and CB6 micromodules in reels
- Smartcard ISO 7810 ID-1
- DFN8 & VFQFPN32 (ECOPACK®-compliant)

Certifications

- Common Criteria EAL6+ certification for hardware: Security IC Platform Protection Profile (BSI-PP-0035), July 15, 2007
- Common Criteria EAL5+ for Software platform: JC Protection Profile - Closed Configuration (ANSSI PP 2010-07), Version 3.0, December 2012)
- Common Criteria EAL4+ certification for application: Protection Profile CWA 14169 - Annex C -Secure Signature Creation Device Type 3, version: 1.05, March 2002 (BSI-PP-0006-2002 EAL 4+)

Contents

1 Description

J-SIGN is a Smartcard application implementing a type-3 secure-signature-creation device (SSCD) according to protection profile CWA 14169 and CIE/CNS application (Italian identity and service citizen card).

The hardware architecture is based on the enhanced ST23 MPU with 16-Mbyte linear addressing mode.

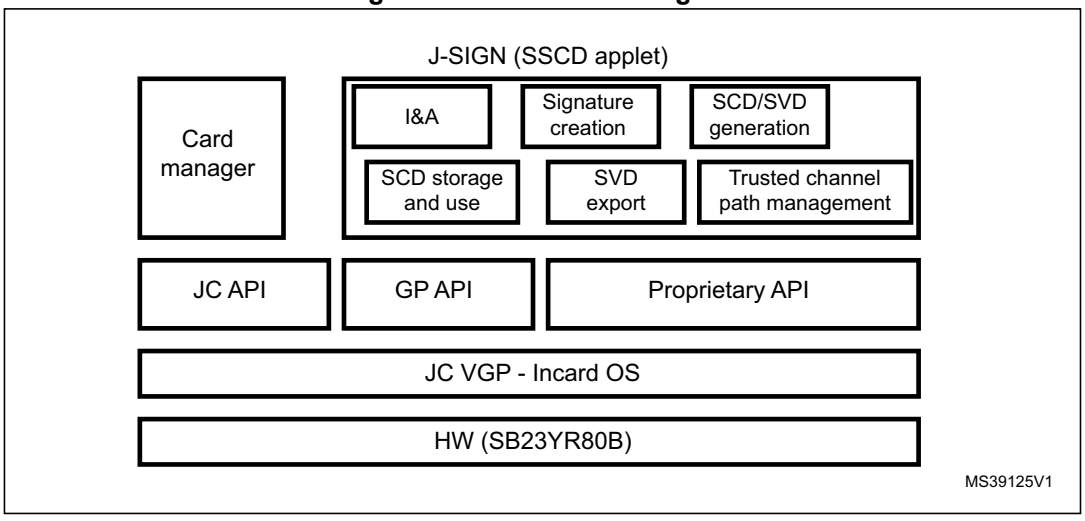
J-SIGN is compliant with Java Card v. 3.0.4 Classic Edition and GlobalPlatform Card Specification v.2.1.1 industry standards The product has been designed to be versatile: it guarantees high performances to secure applications while granting the highest security level in terms of CC security certification on the hardware (EAL6+) and the operating system (EAL5+).

The Java Card isolation mechanism provided by the J-SIGN has been certified to support the coexistence of highly-secure applications on the same card. The J-SIGN can be configured to provide a preloaded public-key infrastructure (PKI) application. Besides, the J-SIGN application manager allows customer applications to be integrated in EEPROM during pre-issuance.

Java Card 3.0.4 allows the definition of access conditions both on shared data and to control the card lifecycle (*install*, *configure*, *activate* and *delete*).

The J-SIGN multifunctional Smartcard product is intended to provide all required capabilities to devices involved in creating qualified electronic signatures.

Figure 1. J-SIGN block diagram



1. SCD stands for Signature creation data; SVD stands for Signature validation data; JC stands for Java Card; GP stands for GlobalPlatform; and VGP stands for VISA® GlobalPlatform.

The main J-SIGN functionalities cover 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.

The J-SIGN is available in the following packages:

- D70, D68, CB4 and CB6 micromodule formats in reels
- Smartcard ISO 7810 ID-1
- ECOPACK®-compliant DFN8 and VFQFPN32

2 Revision history

Table 1. Document revision history

Date	Revision	Changes
23-Jun-2015	1	Initial release.