StarSign Crypto-USB Token S powered by Sm@rtCafé Expert 7.0 Secure Element

FIPS 140-2 Cryptographic Module Non-Proprietary Security Policy

Author	Giesecke+Devrient Mobile Security GmbH
Status	Final
Edition	15 March 2018, 1.2

Giesecke+Devrient Mobile Security GmbH
Prinzregentenstraße 159
D-81667 Munich

4.3 Services

All services implemented by the module are listed in the tables below.

Service	Description
Context	Selects an applet or manage logical channels.
Module Info (Unauthenticated)	Reads unprivileged data objects, e.g., module configuration or status information.
Module Reset	Power cycles or resets the module. Includes Power-On Self-Test.

Table 10 – Unauthenticated Services

Service	Description	CO	User
Lifecycle	Modifies the card or applet life cycle status.	X	
Manage Content	Loads and installs application packages and associated keys and data.	X	
Module Info (Authenticated)	Reads module configuration or status information (privileged data objects).	X	
Secure Channel	Establishes and uses a secure communications channel.	X	X
PIN Authentication	Demonstrates PIN authentication with OwnerPIN.		X
Manage Applet Content	Creates uninitialized key objects for use by the demo applet's cryptographic services. Deletes on-card key objects, arrays, signature objects.		X
Keys	Generates keys and initializes symmetric and asymmetric key objects for the cryptographic services.		X
Digital Signature	Demonstrates DSA, RSA, and ECDSA digital signature generation and verification.		X
Key Agreement Primitive	Demonstrates Approved ECC CDH primitive (SP 800-56A Section 5.7.1.2).		X
Message Authentication	Demonstrates Triple-DES encryption, decryption and MAC.		X
Message Digest	Demonstrates secure message digest (hash) generation (SHA-224, SHA-256, SHA-384, and SHA-512).		X

Table 11 – Authenticated Services

CSPs												
Service	OS-RNG-STATE	SD-KENC	SD-KMAC	SD-KDEK	SD-SENC	SD-SMAC	SD-SRMAC	DAP-SYM	DEM-AUTH	DEM-KAP-PRI	DEM-MAC	DEM-SGV-PRIV
Context	--	--	--	--	Z	Z	Z	--	--	--	--	--
Module Info (Unauthenticated)	--	--	--	--	--	--	--	--	--	--	--	--
Module Reset	GEW	--	--	--	Z	Z	Z	--	--	--	--	--
Lifecycle[1]	Z	Z	Z	Z	E	E	E	Z	Z	Z	Z	Z
Manage Content[2]	--	W	W	W	E	E	E	EW	Z	Z	Z	Z
Module Info (Authenticated)	--	--	--	--	E	E	E	--	--	--	--	--
Secure Channel	EW	E	E	--	GE	GE	GE	--	--	--	--	--
PIN Authentication	--	--	--	--	E	E	--	--	E	--	--	--
Manage Applet Content	--	--	--	--	E	E	--	--	--	C	C	C
Keys	EW	--	--	--	E	E	--	--	--	GZ	GZ	GZ
Digital Signature	EW	--	--	--	E	E	--	--	--	--	--	GE
Key Agreement Primitive	EW	--	--	--	E	E	--	--	--	GE	--	--
Message Authentication	--	--	--	--	E	E	--	--	--	--	E	--
Message Digest	--	--	--	--	E	E	--	--	--	--	--	--

Table 12 – Access to CSPs by Service

- G = Generate: The module generates the CSP.
- C = Create: The module uninitializes key objects for signature and cipher algorithms.
- R = Read: The module reads the CSP (read access to the CSP by an outside entity).
- E = Execute: The module executes using the CSP.
- W = Write: The module writes the CSP. The write access is typically performed after a CSP is imported into the module or when the module overwrites an existing CSP.
- Z = Zeroize: The module zeroizes the CSP. For the Context service, SD session keys are destroyed on applet deselect (channel closure)
- -- = Not accessed by the service.

[1] Zeroize in this row corresponds to card termination.

[2] Zeroize in this row corresponds to the Demonstration Applet deletion.

5 Self-test

5.1 Power-On Self-tests

On power-on or reset, the module performs self-tests as described in Table 13 below. All KATs must be completed successfully prior to any other use of cryptography by the module. If one of the KATs fails, the system emits an error code (0x6666) and enters the SELF-TEST ERROR state.

Test Target	Description
Firmware Integrity	16 bit Reed-Solomon EDC performed over all code in the cryptographic boundary.
DRBG	Performs a fixed input KAT.
Triple-DES	Performs separate encrypt and decrypt KATs using 3-Key Triple-DES in ECB mode.
AES	Performs a decrypt KAT using an AES-128 key in ECB mode.
SP 800-108 KDF	Performs a KAT of SP 800-108 KDF. This self-test is inclusive of AES CMAC and AES encrypt function self-test.
RSA	Performs separate RSA signature and verify KATs using an RSA 2048-bit key.
RSA CRT	Performs RSA CRT signature KATs using an RSA 2048-bit key.
ECDSA	Performs pairwise consistency test using the P-521 curve.
SHA-1	Performs a fixed input KAT.
SHA-256	Performs a fixed input KAT.
SHA-256 (2)	Performs a fixed input KAT for the 2nd SHA-256 implementation.
SHA-512	Performs a fixed input KAT.
DSA	Performs a pairwise consistency test using a DSA 2048-bit key.
ECC CDH	Primitive “Z” Computation KAT for [SP 800-56A] Section 5.7.1.2 ECC CDH Primitive using the P-521 curve.

Table 13 – Power-On Self-Test

5.2 Conditional Self-tests

On every call to the DRBG, the module performs the AS09.42 continuous RNG test to assure that the output is different than the previous value. If the continuous RNG test fails, the module enters the SELF-TEST ERROR state. The NDRNG hardware includes a continuous comparison test, such that each word formed is compared to the previous value; a duplicate value is discarded, and the NDRNG status indicates not ready.

When an RSA, DSA or ECDSA key pair is generated the module performs a pairwise consistency test. If the pairwise consistency test fails, the module enters the SELF-TEST ERROR state.

When new firmware is loaded into the module using the *Manage Content* service, the module verifies the integrity of the new firmware (applet) using MAC verification with the SD-SMAC key. Optionally, the module may also verify a signature of the new firmware (applet) using the DAP-SV-PUB public key or the DAP-SYM key; the signature block in this scenario is generated by an external entity using the private key corresponding to DAP-SV-PUB or the symmetric DAP-SYM. Failure to verify the new firmware results in the BAD APDU error state; the module returns an error specific to the situation (MAC failure or DAP failure).

6 Physical Security Policy

The module is a single-chip implementation available in SMD packaging that meets commercial-grade specifications for power, temperature, reliability, and shock/vibrations. The module was tested at ambient temperature only.

The module is intended to be mounted in additional packaging as described in Section 2. Physical inspection of the die for tamper evidence is typically not practical after packaging.

7 Electromagnetic Interference and Compatibility (EMI/EMC)

The module conforms to the EMI/EMC requirements specified by part 47 Code of Federal Regulations, Part 15, Subpart B, Unintentional Radiators, Digital Devices, Class B.

8 Mitigation of Other Attacks Policy

The module implements defenses against:

- Physical fault induction, such as laser, light, clock glitch or similar attacks
- Side-channel attacks (SPA/DPA and timing analysis)
- Differential fault analysis (DFA)

9 Security Rules and Guidance

The module implementation also enforces the following security rules:

- No additional interface or service is implemented by the module which would provide access to CSPs.
- Data output is inhibited during key generation, self-tests, zeroization, and error states.
- There are no restrictions on which keys or CSPs are zeroized by the zeroization service.
- The module does not support manual key entry, output plaintext CSPs, or output intermediate key values.
- Status information does not contain CSPs or sensitive data that if misused could lead to a compromise of the module.