Sm@rtCafé Expert 7.0

FIPS 140-2 Cryptographic Module Non-Proprietary Security Policy

Version: 1.4
Date: 15 September 2020

Author	Giesecke+Devrient Mobile Security GmbH
Status	Final
Edition	20..05.2020

Giesecke+Devrient Mobile Security GmbH
Prinzregentenstraße 159
D-81677 Munich

Table of Contents

List of Tables

List of Figures

References

Acronym	Full Specification Name
[FIPS140-2]	NIST, *Security Requirements for Cryptographic Modules*, May 25, 2001
[GlobalPlatform]	*GlobalPlatform Consortium: GlobalPlatform Card Specification 2.2.1,* January 2011, http://www.globalplatform.org *GlobalPlatform Consortium: GlobalPlatform Card Specification 2.2* Amendment A, Confidential Card Content Management, Version 1.0, October 2007
[ISO 7816]	ISO/IEC 7816-1: 1998 *Identification cards -- Integrated circuit(s) cards with contacts -- Part 1: Physical characteristics* ISO/IEC 7816-2:2007 *Identification cards -- Integrated circuit cards -- Part 2: Cards with contacts -- Dimensions and location of the contacts* ISO/IEC 7816-3:2006 *Identification cards -- Integrated circuit cards -- Part 3: Cards with contacts -- Electrical interface and transmission protocols* ISO/IEC 7816-4:2005 *Identification cards -- Integrated circuit cards -- Part 4: Organization, security and commands for interchange*
[ISO 14443]	ISO/IEC 14443-1:2008 *Identification cards -- Contactless integrated circuit cards -- Proximity cards -- Part 1: Physical characteristics* ISO/IEC 14443-2:2010 *Identification cards -- Contactless integrated circuit cards -- Proximity cards -- Part 2: Radio frequency power and signal interface* ISO/IEC 14443-3:2011 *Identification cards -- Contactless integrated circuit cards -- Proximity cards -- Part 3: Initialization and anticollision* ISO/IEC 14443-4:2008 *Identification cards -- Contactless integrated circuit cards -- Proximity cards -- Part 4: Transmission protocol*
[JavaCard]	*Java Card 3 Platform Runtime Environment (JCRE) Specification, Classic Edition. Version 3.0.4* *Java Card 3 Platform Virtual Machine (JCVM) Specification, Classic Edition. Version 3.0.4* *Java Card 3 Platform Application Programming Interface, Classic Edition. Version 3.0.4* Published by Oracle, September 2011
[SP800-131A]	*Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths*, January 2011
[ANS X9.31]	American Bankers Association, *Digital Signatures Using Reversible Public Key Cryptography for the Financial Services Industry (rDSA)*, ANSI X9.31-1998 - Appendix A.2.4.
[SP 800-67]	NIST Special Publication 800-67, *Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher*, version 1.2, July 2011
[FIPS113]	NIST, *Computer Data Authentication*, FIPS Publication 113, 30 May 1985.
[FIPS197]	NIST, *Advanced Encryption Standard (AES)*, FIPS Publication 197, November 26, 2001.
[PKCS#1]	*PKCS #1 v2.1: RSA Cryptography Standard*, RSA Laboratories, June 14, 2002
[FIPS 186-4]	NIST, *Digital Signature Standard (DSS)*, FIPS Publication 186-4, July, 2013
[SP 800-56A]	NIST Special Publication 800-56A, *Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography*, March 2007
[SP 800-56B]	NIST Special Publication 800-56B, *Recommendation for Pair-Wise Key-Establishment Schemes Using Integer Factorization Cryptography*, September 2014
[FIPS 180-4]	NIST, *Secure Hash Standard*, FIPS Publication 180-4, March 2012
[SP800-108]	NIST, *Recommendation for Key Derivation Using Pseudorandom Functions (Revised),* October 2009
[SP800-38F]	NIST, *Recommendation for Block Cipher Modes of Operation: Methods for Key Wrapping,* December 2012
[IG]	NIST, *Implementation Guidance for FIPS PUB 140-2 and the Cryptographic Module Validation Program,* last updated 25 July 2013.

Acronym	Full Specification Name
[RS]	Irving S. Reed, Gustave Solomon: *Polynomial codes over certain finite fields*. In: Journal of the Society for Industrial and Applied Mathematics, SIAM J. 8, 1960, ISSN 0036-1399, p. 300–304.

Table 1 – References

Acronyms and definitions

Acronym	Definition
APDU	Application Protocol Data Unit, see [ISO 7816]
API	Application Programming Interface
ATR	Answer To Reset
CSP	Critical Security Parameter, see [FIPS 140-2]
DAP	Data Authentication Pattern, see [GlobalPlatform]
DPA	Differential Power Analysis
GP	GlobalPlatform
IC	Integrated Circuit
ISD	Issuer Security Domain, see [GlobalPlatform]
KAT	Known Answer Test
NVM	Non-volatile memory
PCT	Pairwise Consistency Test
SCP	Secure Channel Protocol, see [GlobalPlatform]
SPA	Simple Power Analysis

Table 2 – Acronyms and Definitions

1 Introduction

This document defines the Security Policy for the Giesecke+Devrient Sm@rtCafé Expert 7.0 cryptographic module, hereafter denoted *the module*. The module, validated to FIPS 140-2 overall Level 3, is a single chip module implementing the GlobalPlatform operational environment, with Card Manager and a Demonstration Applet.

The Demonstration Applet is available only to demonstrate the complete cryptographic capabilities of the module for FIPS 140-2 validation, and is not intended for general use. The term *platform* herein is used to describe the chip and operational environment, not inclusive of the Demonstration Applet.

The module is a limited operational environment under the FIPS 140-2 definitions. The module includes a firmware load function to support necessary updates. New firmware versions within the scope of this validation must be validated through the FIPS 140-2 CMVP. Any other firmware loaded into this module is out of the scope of this validation and requires a separate FIPS 140-2 validation.

The FIPS 140-2 security levels for the module are as follows:

Security Requirement	Security Level
Cryptographic Module Specification	3

Security Requirement	Security Level
Cryptographic Module Ports and Interfaces	3
Roles, Services, and Authentication	3
Finite State Model	3
Physical Security	3
Operational Environment	N/A
Cryptographic Key Management	3
EMI/EMC	3
Self-Tests	3
Design Assurance	3
Mitigation of Other Attacks	3

Table 3 – Security Level of Security Requirements

1.1 Versions, Configurations and Modes of operation

Hardware: SLE78CLFX4000P(M) M7892
Firmware: Sm@rtCafé Expert 7.0, Demonstration Applet V1.0
Packaging options (configurations):

Contact only:	P-M4.8-8-1, S-MFC6.8
Dual-interface:	P-M8.4-8-3, S-COM8.6
Contactless only:	P-MCS8-2-1, P-MCC8-2-6

The chip and firmware are identical in all configurations. The chip design is a superset of all possible interface options; unused options are disabled during production.

The card is always in the Approved mode; the explicit indicator of Approved mode is given in the ATR: the value 0x46 ('F') in Historical Byte 9 indicates the Approved mode.

```
interface bytes              historical bytes
3B F9 96 00 00 80 31 FE 45   46 69 70 73 20 41 70 70 46 6E
                             F  i  p  s     A  p  p  F
```

2 Hardware and Physical Cryptographic Boundary

The module is designed to be embedded into plastic card bodies, with a contact plate and contactless antenna connections. The physical forms of the module are depicted in Figures 1 through 3. The cryptographic boundary is the surface and edges of the packages as shown in the Figures.

The contactless ports of the module require connection to an antenna. The module relies on [ISO7816] and [ISO14443] card readers as input/output devices.

Figure 1 – Contact only: P-M4.8-8-1 front and back (left); S-MFC6.8 front and back (right)

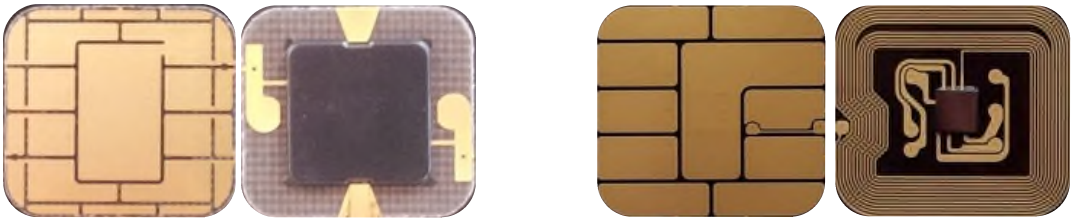

Figure 2 – Dual interface: P-M8.4-8-3 front and back (left); S-COM6.8 front and back (right)

Figure 3 – Contactless-only: P-MCS8-2-1 front and back (left); P-MCC8-2-6 front and back (right)

Port	Description	Logical Interface Type
V_{CC}, GND	ISO 7816: Supply voltage	Power – Contact configurations only
RST	ISO 7816: Reset	Control in - Contact configurations only
CLK	ISO 7816: Clock	Control in - Contact configurations only
I/O	ISO 7816: Input/Output	Control in, Data in, Data out, Status out – Contact configurations only
LA, LB	ISO 14443: Antenna	Power, Control in, Data in, Data out, Status out - Contact configurations only
NC	Not connected	Not connected

Table 4 – Ports and Interfaces

Control/data input and status/data output share a common physical port, with the logical separation into interfaces determined by the ISO 7816 and ISO 14443 protocols.

2.1 Firmware and Logical Cryptographic Boundary

Figure 4 depicts the module operational environment.

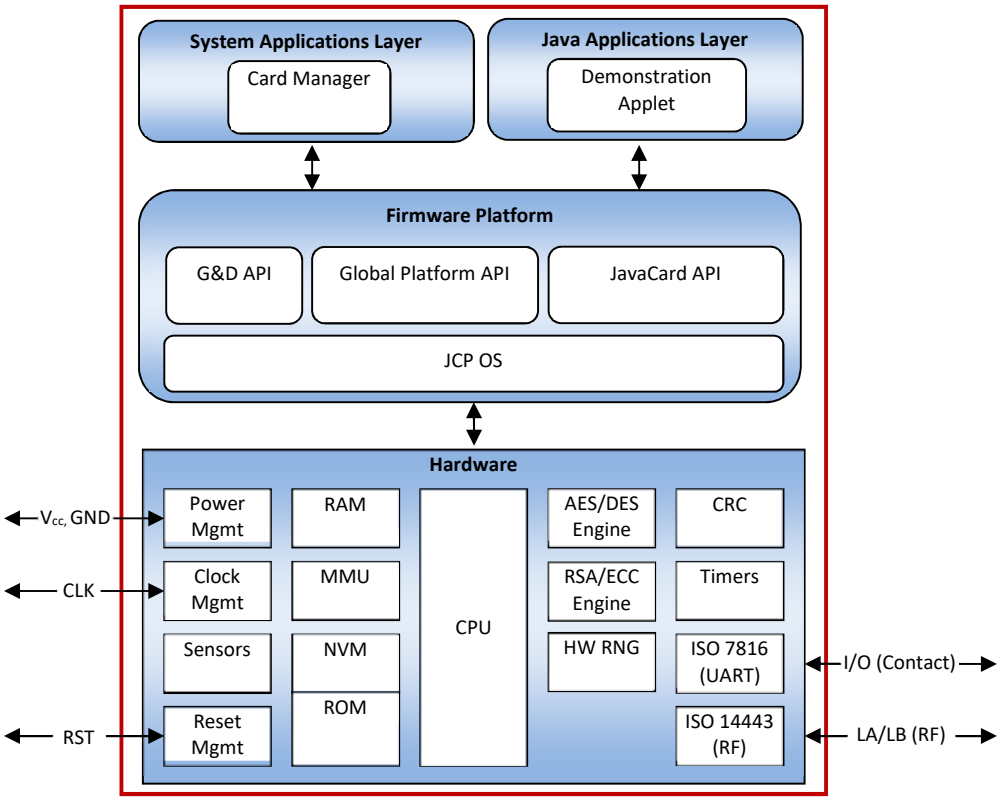

Figure 4 - Module Block Diagram

The JavaCard, GlobalPlatform and G&D APIs are internal interfaces available only to applets and security domains (i.e., Card Manager). Only applet services are available at the card edge (the interfaces that cross the cryptographic boundary). Section 3 describes applet functionality in greater detail.

The NVM is separated into segments with different access rules, enforced by the hardware MMU. The MMU is initialized with the correct settings by startup code, and verified by the operating system each time the system starts. The MMU settings cannot be changed at run time. All code is executed from ROM and NVM.

3 Cryptographic Functionality

The module implements the Approved and Non-Approved but Allowed cryptographic functions listed in Tables 5 and 6 below.

Algorithm	Description	Cert #
AES CMAC	[SP800-38B] AES-256 CMAC. The module supports AES-128, AES-192 and AES-256 keys.	2720
AES	[FIPS 197] Advanced Encryption Standard algorithm. The module supports AES-128, AES-192- and AES-256 keys, and ECB and CBC modes.	2721
CVL	[SP 800-56A] The Section 5.7.1.2 ECC CDH Primitive only (as used by the PIV specification). The module supports the NIST defined P-224 P-256, P-384 and P-521 curves.	177
CVL	[FIPS 186-4] RSASP1 Signature Primitive. The module supports 2048-bit RSA keys.	1192
CVL	[SP 800-56B] RSASDP Primitive. The module supports 2048-bit RSA keys.	1193
DRBG	[SP 800-90A] AES-256 CTR_DRBG. Does not support prediction resistance.	455
DSA	[FIPS 186-4] DSA key generation, signature generation and verification. The module supports 2048 bit keys.	837
ECDSA	[FIPS 186-4] Elliptic Curve Digital Signature Algorithm. The module supports the NIST defined P-224, P-256, P-384, P-521 curves for key pair generation, signature and signature verification.	476
KBKDF	[SP 800-108] CMAC-based KDF with AES-128, AES-192, AES-256.	18
KTS	AES Key Wrapping compliant with SP800-38F §3.1 ¶3 (Combination method using Cert. #2721 AES and Cert. #2720 AES CMAC). Key establishment methodology provides between 128 to 256 bits of encryption strength.	2720, 2721
RSA	[FIPS 186-4] RSA key generation, signature generation and verification. The module supports 2048-bit RSA keys.	1506
RSA CRT	[FIPS 186-4] RSA key generation and signature generation. The module supports 2048-bit RSA keys.	1507
SHA-2	SHA-256	2288
SHA-2	[FIPS 180-4] Secure Hash Standard compliant one-way (hash) algorithms; SHA-224, SHA-256, SHA-384, SHA-512	2289
SHA-1	SHA-1	2290

Table 5 –Approved Cryptographic Functions

Algorithm	Description
NDRNG	Hardware NDRNG used to seed the FIPS approved DRBG.

Table 6 – Non-Approved but Allowed Cryptographic Functions

Algorithm	Description
Triple-DES (no security claimed)**	[SP 800-67] Triple Data Encryption Algorithm. The module supports 3-Key keys only, and CBC and ECB modes.
Triple-DES MAC (no security claimed)**	[FIPS113] Triple-DES MAC, vendor affirmed based on Cert. #1637.

Table 7 – Non-Approved Cryptographic Functions

**Note: The Triple-DES algorithm, used by the Demonstration Applet's Message Authentication Service, is solely used for testing purposes and therefore is not subject to IG A.13.

3.1 Critical Security Parameters and Public Keys

All CSPs and public keys used by the module are described in this section. In the tables below, the OS prefix denotes operating system, the SD prefix denotes the GlobalPlatform Security Domain, the DAP prefix denotes the GlobalPlatform Data Authentication Protocol, and the DEM prefix denotes a Demonstration Applet CSP.

CSP	Description / Usage
OS-RNG-STATE	384 bit value; the current RNG state.
SD-KENC	AES-128, AES-192, AES-256 Master key used to generate SD-SENC.
SD-KMAC	AES-128, AES-192, AES-256 Master key used to generate SD-SMAC.
SD-KDEK	AES-128, AES-192, AES-256 Sensitive data decryption key used to decrypt CSPs.
SD-SENC	AES-128, AES-192, AES-256 Session encryption key used to encrypt / decrypt secure channel data.
SD-SMAC	AES-128, AES-192, AES-256 Session MAC key used to verify inbound secure channel data integrity.
SD-SRMAC	AES-128, AES-192, AES-256 Session MAC key used to verify response secure channel data integrity.
CTR-DRBG Key	AES-256 Key, part of the seed data for the CTR DRBG
CTR-DRBG V	Counter value, part of the seed data for the CTR DRBG
DAP-SYM	AES-128, AES-192, AES-256 authentication key used by the *Manage Content* service.
DEM-AUTH	An 8 byte PIN value allowing all 256 values for each byte, used by the *PIN Authentication* service. The module always checks all 8 bytes of the PIN.
DEM-KAP-PRI	EC P-256 private key used to demonstrate the ECC CDH shared secret generation. The *Key Agreement Primitive* service allows any of the valid EC curves to be used.
DEM-MAC	AES MAC key used by the Message Authentication service.
DEM-SGV-PRIV	DSA 2048 bit, ECDSA P-256 or RSA 2048 bit private key used by the *Digital Signature* service.

Table 8 –Critical Security Parameters

Key	Description / Usage
DAP-PUB	RSA 2048 new firmware signature verification key.
DEM-KAP-PUB	EC P-256 ECDSA public key used by the *Key Agreement Primitive* service.
DEM-SGV-PUB	DSA 2048 bit, EC P-256 ECDSA or RSA 2048 bit public key used by the *Digital Signature* service.

Table 9 – Public Keys

4 Roles, Authentication and Services

The module:

- Does not support a maintenance role.
- Clears previous authentications on power cycle.
- Supports Global Platform SCP logical channels, allowing concurrent operators in a limited fashion.

Authentication of each operator and their access to roles and services is as described below, independent of logical channel usage. Only one operator at a time is permitted on a channel. Applet de-selection (including Card Manager), card reset or power down terminates the current authentication; re-authentication is required after any of these events for access to authenticated

services. Authentication data is encrypted during entry (by SD-KDEK), and is only accessible by authenticated services.

Table 9 lists all operator roles supported by the module.

Role ID	Role Description
CO	Cryptographic Officer – role that manages module content and configuration, including issuance and management of module data via the ISD. Authenticated as described in *Secure Channel Protocol Authentication* in Section 4.1 below.
User	User – role for use in Demonstration applet. Authenticated as described in *Demonstration Applet Authentication* in Section 4.2 below.

Table 10 - Roles Supported by the Module

4.1 Secure Channel Protocol Authentication Method

The Secure Channel Protocol authentication method is provided by the *Secure Channel* service. The SD-KENC and SD-KMAC keys are used to derive the SD-SENC and SD-SMAC keys, respectively. The key derivation uses KDF in counter mode as specified in NIST SP 800-108 [NIST 800-108]. The PRF used in the KDF is CMAC as specified in [NIST 800-38B], used with full 16 byte output length.

The initial step of the Secure Channel Service initiates the session key derivation on the card and conveys also the host challenge. The card returns the card challenge and the card cryptogram, calculated as a CMAC with the session keys. This is checked by the host.

To perform finally the mutual authentication the final step of the Secure Channel Service conveys the host cryptogram to the card, which is a CMAC based on the card challenge and calculated with the session keys on host side. After the successfully check of the exchanged cryptograms by card and host, the two participants are mutually authenticated (the external entity is authenticated to the module in the CO role).

WN:

The probability that a random attempt will succeed using this authentication method is:

- 1/2^128 = 2.9E-39 (for any of AES-128/192/256 SD-KENC/SD-SENC, assuming a 128-bit block)

The module enforces a maximum of fifteen (15) consecutive failed SCP authentication attempts. The probability that a random attempt will succeed over a one minute interval is:

- 15/2^128 = 4.4E-38 (for any of AES-128/192/256 SD-KENC/SD-SENC, assuming a 128-bit block)

4.2 Demonstration Applet Authentication Method

The Demonstration Applet Authentication method is provided by the *Secure Channel* service combined with the *Authenticate* service. The module accepts an 8 byte PIN value and compares all 8 bytes to a stored reference, with no restriction on character space (each character can be any value from 0-255). The probability that a random attempt will succeed using this authentication method is:

- 1/256^8 = 5.4E-20

The module enforces a maximum of three (3) consecutive failed authentication attempts. The probability that a random attempt will succeed over a one minute interval is:

- 3/256^8 = 1.6E-19.

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 11 - 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 AES encryption, decryption and MAC.		X
Message Digest	Demonstrates secure message digest (hash) generation (SHA-224, SHA-256, SHA-384, and SHA-512).		X

Table 12 –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

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

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
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 13 –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.

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.

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

Test Target	Description
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 14 – 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/MAC of the new firmware (applet) using a DAP-key and its associated algorithm, in case of asymmetric cryptography using the DAP-PUB public key or in case of symmetric cryptography the DAP-SYM key; the signature/MAC block in this scenario is generated by an external entity using the private key corresponding to DAP-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 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; physical inspection of the die 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 attacks
- Side-channel attacks (SPA/DPA and timing analysis)
- Differential fault analysis (DFA)

8.1 Physical Attacks

This kind of attack is directed against the IC and is often independent of the embedded software (i.e., it could be applied to any embedded software and is independent of software countermeasures).

This module applies counter-measures against physical attacks, implemented on the chip hardware. Examples for mitigation of physical attacks are e.g. sensors to avoid exposure of e.g. light, high/low clock frequency, glitches or high/low voltage. These measures are part of the hardware. In addition the chip hardware applies also counter-measures against overcoming sensors and filters, e.g. deactivating or avoiding the different types of sensors that an IC may use to monitor the environmental conditions and to protect itself from conditions that would threaten normal operation.

8.2 Side-channel attacks (SPA/DPA and timing analysis)

In this type of attack an attacker uses power analysis to extract the secret key from power consumption traces taken during the execution of the crypto algorithm itself. The same can be achieved by using other information leaking with the analysis of time consumption in the calculation of crypto operations.

Counter-measures are implemented in software and hardware. The module uses the counter-measures of the crypto coprocessor which uses e.g. randomized and hiding methods of the key material and calculated (intermediate) results applied in the crypto operation, uses a noise generator for CPU and crypto unit, defines constant timing function for coprocessors and applies data and register masking.

Additionally software counter-measures against timing attacks and SPA/DPA attacks are e.g. transient data arrays in RAM (clear on reset, clear on applet selection), mechanisms for sensitive data areas (creation, access and clearing), data manipulation hiding, constant time code execution, randomized algorithm execution, randomized data initialization, erasure and comparison.

8.3 Differential fault analysis (DFA)

DFA can break cryptographic key systems, allowing retrieval of AES, RSA and ECC keys for example, by running the device under unusual physical circumstances. The attacker needs to inject an error at the right time and location to obtain exploitable erroneous cryptographic outputs.

The module uses and implements several counter-measures against DFA. The chip hardware controls and checks the physical circumstances by the chip hardware (sensors, filters, light detection) and detects data errors on the bus system in the hardware (bus controls, etc.). Additional measures are e.g. logical countermeasures like integrity checking, masking of data, active metal shield (complex implementation), frequency detection, voltage detection, temperature detection, constant timing for coprocessors, illegal address and instruction detector.

The error detection in software are e.g. multiple (crypto) operations, secure data storage, secure data comparison, checksums and checksum management, flow control, timing control etc.

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.
- Symmetric keys and seeds (for asymmetric key generation) are unmodified outputs from the DRBG.