Giesecke+Devrient ePayments GmbH

Sm@rtCafe Expert 8.1

FIPS 140-3 Non-Proprietary Security Policy

Document Version: 1.3
Date: 09/16/2025

Table of Contents

List of Tables

List of Figures

1 – General

1.1 Overview

This document is the non-proprietary FIPS 140-3 Security Policy for the Sm@rtCafé Expert 8.1. It contains the security rules under which the module must operate and describes how this module meets

the requirements as specified in FIPS PUB 140-3 (Federal Information Processing Standards Publication 140-3) for an overall Security Level 3 module.

1.2 Security Levels

The FIPS 140-3 security levels for the Module are as follows from Table 1:

Section	Title	Security Level
1	General	3
2	Cryptographic module specification	3
3	Cryptographic module interfaces	3
4	Roles, services, and authentication	3
5	Software/Firmware security	3
6	Operational environment	N/A
7	Physical security	3
8	Non-invasive security	N/A
9	Sensitive security parameter management	3
10	Self-tests	3
11	Life-cycle assurance	3
12	Mitigation of other attacks	3
	Overall Level	3

Table 1: Security Levels

2 – Cryptographic Module Specification

2.1 Description

Purpose and Use:
The Module is intended for use by US Federal agencies or other markets that require FIPS 140-3 validated applications for authorized condition access, like secure ID applications (PIV Card), the Module is intended to be used in a wide range of different end-user environments.

Module Type: Hardware

Module Embodiment: SingleChip

Module Characteristics:

Cryptographic Boundary:

The physical form of the Module is depicted in Figure 1. The cryptographic boundary is designed to be embedded into plastic card bodies, with a contact plate and contactless antenna connections. 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.

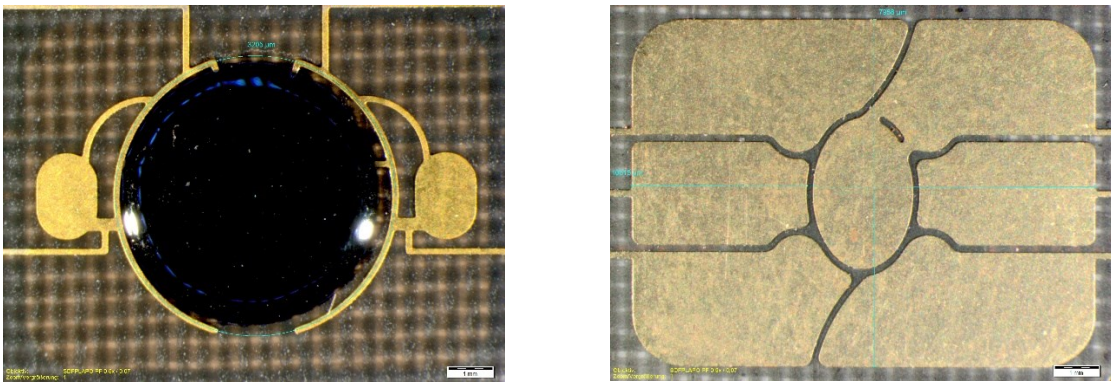

Figure 1 – G+D's PD6 (PHS2.2) module: black encapsulation (left); lead frame (right)

Figure 2 depicts the module block diagram.

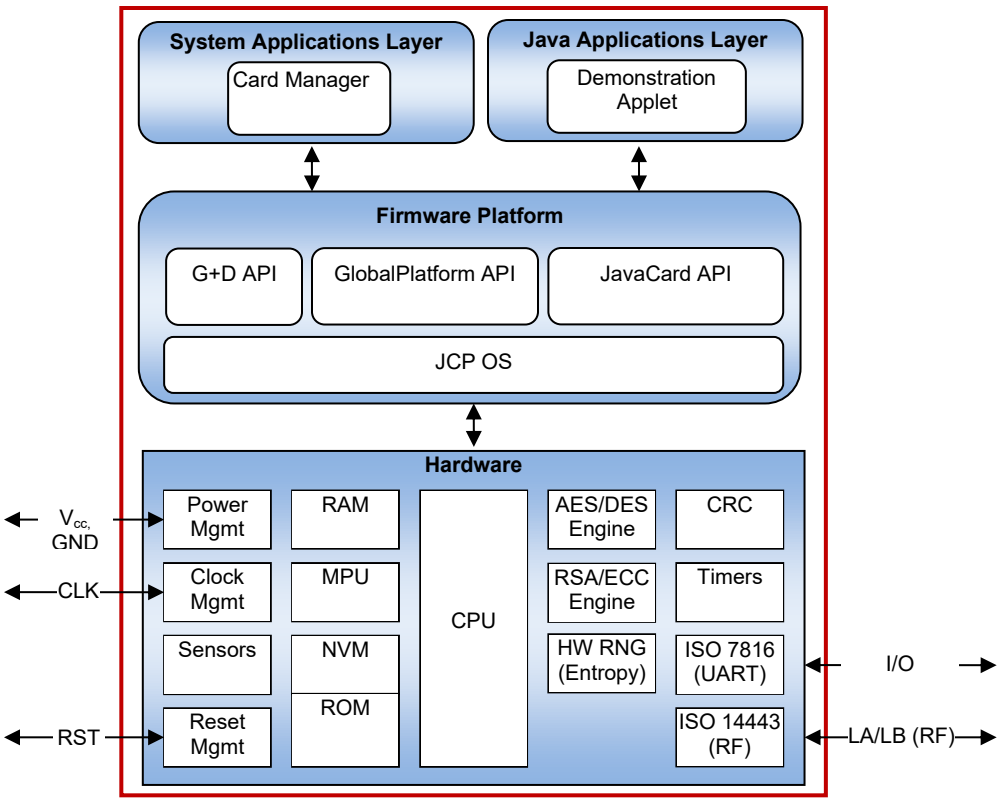

Figure 2 - Module Block Diagram

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).

2.2 Tested and Vendor Affirmed Module Version and Identification

The HW version and the OS version can be retrieved by a GET DATA command:

GET DATA: 00 CA 52 C0 will return the response data field containing the HW-Version: 02 00 42.[1]

GET DATA: 00 CA DF E3 will return the response data field containing the OS-Version in tag 85: B3 E8 CE 6A.[2]

The Version of the loaded applet can be retrieved by a GET STATUS command with the AID of the applet:

GET STATUS: 80 F2 20 00 0D 4F 0L <AID> 00 will return response data containing the AID followed by 2 version bytes. The demonstration applet AID is 31 42 33 34 35 AA FF CA FE FF AA, and the version is 0x0100.

[1] This response value of Get Data is mapped to the Hardware Version in Table 2.

[2] This response value of Get Data is mapped to the Firmware Version in Table 2.

Tested Module Identification – Hardware:

Giesecke+Devrient Sm@rtCafé Expert 8.1 cryptographic module is tested on the following operational environment.

Model and/or Part Number	Hardware Version	Firmware Version	Processors	Features
ST31N600	ST31N60054BBF5	Sm@rtCafe Expert 8.1, Demonstration Applet 1.0	STMicroelectronics ST31	Dual Interface smart card

Table 2: Tested Module Identification – Hardware

2.3 Excluded Components

There are no components that are excluded from the cryptographic boundary.

2.4 Modes of Operation

Modes List and Description:

Mode Name	Description	Type	Status Indicator
Approved Mode	The module is set to approved mode at manufacturing and is always in the Approved mode	Approved	The explicit indicator of Approved mode is given in the ATR: the value 0x46 ('F') in Historical Byte 10 indicates the Approved mode (See table below)

Table 3: Modes List and Description

The ATR has the following structure:

interface bytes	historical bytes
3B DF 97 80 31 FE 45	00 53 43 45 20 38 2E 31 2D ("SCE 8.1–") 46 ("F" FIPS approved mode) 31 4D 31 ("1M1" Variant) 03 (Life cyclee state) XX XX (9000 or error code if self test error occurs) XX (CRC)

Table 4 – ATR Structure

2.5 Algorithms

Approved Algorithms:

The Module implements the FIPS Approved cryptographic algorithms listed in the table below.

Algorithm	CAVP Cert	Properties	Reference
AES-CBC	A5371	-	SP 800-38A
AES-CFB128	A5371	-	SP 800-38A
AES-CMAC	A5372	-	SP 800-38B
AES-CTR	A5371	-	SP 800-38A
AES-ECB	A5371	-	SP 800-38A
AES-KW	A5384	-	SP 800-38F
AES-KWP	A5384	-	SP 800-38F
Counter DRBG	A5383	-	SP 800-90A Rev. 1
ECDSA KeyGen (FIPS186-5)	A5375	-	FIPS 186-5
ECDSA KeyVer (FIPS186-5)	A5375	-	FIPS 186-5
ECDSA SigGen (FIPS186-5)	A5375	-	FIPS 186-5
ECDSA SigVer (FIPS186-4)	A5375	-	FIPS 186-4
ECDSA SigVer (FIPS186-5)	A5375	-	FIPS 186-5
HMAC-SHA2-224	A5376	-	FIPS 198-1
HMAC-SHA2-256	A5376	-	FIPS 198-1
HMAC-SHA2-384	A5376	-	FIPS 198-1
HMAC-SHA2-512	A5376	-	FIPS 198-1
KAS-ECC Sp800-56Ar3	A5378	-	SP 800-56A Rev. 3
KAS-ECC-SSC Sp800-56Ar3	A5379	-	SP 800-56A Rev. 3
KDF SP800-108	A5377	-	SP 800-108 Rev. 1
RSA Decryption Primitive Sp800-56Br2 (CVL)	A5374	-	SP 800-56B Rev. 2
RSA KeyGen (FIPS186-5)	A5373	-	FIPS 186-5
RSA SigGen (FIPS186-5)	A5374	-	FIPS 186-5
RSA Signature Primitive (CVL)	A5374	-	FIPS 186-4
RSA SigVer (FIPS186-4)	A5374	-	FIPS 186-4
RSA SigVer (FIPS186-5)	A5374	-	FIPS 186-5
SHA-1	A5380	-	FIPS 180-4
SHA2-224	A5380	-	FIPS 180-4
SHA2-224	A5381	-	FIPS 180-4
SHA2-256	A5380	-	FIPS 180-4
SHA2-256	A5381	-	FIPS 180-4
SHA2-384	A5380	-	FIPS 180-4
SHA2-384	A5381	-	FIPS 180-4
SHA2-512	A5380	-	FIPS 180-4
SHA2-512	A5381	-	FIPS 180-4

Algorithm	CAVP Cert	Properties	Reference
SHA3-224	A5382	-	FIPS 202
SHA3-256	A5382	-	FIPS 202
SHA3-384	A5382	-	FIPS 202
SHA3-512	A5382	-	FIPS 202

Table 5: Approved Algorithms

Vendor-Affirmed Algorithms:

The Module implements the FIPS Vendor Affirmed cryptographic algorithms listed.

Name	Properties	Implementation	Reference
CKG	Key Type:Asymmetric	N/A	SP800-133rev2 Sections 4 example 1 and IG D.H

Table 6: Vendor-Affirmed Algorithms

Non-Approved, Allowed Algorithms:

The Module implements the FIPS Non-Approved, but Allowed cryptographic algorithms listed.

Name	Properties	Implementation	Reference
KAS-ECC-SSC	brainpoolP224r1: brainpoolP256r1: brainpoolP384r1: brainpoolP512r1: brainpoolP256t1: brainpoolP384t1: brainpoolP512t1:	kasssc	IG C.A, D.F Scenario #3

Table 7: Non-Approved, Allowed Algorithms

Non-Approved, Allowed Algorithms with No Security Claimed:

The Module does not implement the FIPS Non-Approved, Allowed cryptographic Algorithms with No Security Claimed.

N/A for this module.

Non-Approved, Not Allowed Algorithms:

The Module does not implement the FIPS Non-Approved, Not Allowed cryptographic algorithms listed.

N/A for this module.

2.6 Security Function Implementations

The following table shows the Security Function Implementations that the module implements:

Name	Type	Description	Properties	Algorithms
ecckeygen	AsymKeyPair-KeyGen	Asymmetric Key-Pair Generation		ECDSA KeyGen (FIPS186-5): (A5375) Counter DRBG: (A5383) CKG: () Key Type: Asymmetric
rsakeygen	AsymKeyPair-KeyGen	Asymmetric Key-Pair Generation		RSA KeyGen (FIPS186-5): (A5373) Counter DRBG: (A5383) CKG: () Key Type: Asymmetric
eckeyval	AsymKeyPair-KeyVer	Public key validation		ECDSA KeyGen (FIPS186-5): (A5375) ECDSA KeyVer (FIPS186-5): (A5375)
aesenc	BC-UnAuth	Block Cipher		AES-CBC: (A5371) AES-ECB: (A5371) AES-CTR: (A5371) AES-CFB128: (A5371)
aesdec	BC-UnAuth	Block Cipher		AES-CBC: (A5371) AES-ECB: (A5371) AES-CTR: (A5371) AES-CFB128: (A5371)
ecsiggen	DigSig-SigGen	Digital Signature Generation		ECDSA SigGen (FIPS186-5): (A5375) Counter DRBG: (A5383) SHA2-224: (A5380) SHA2-256: (A5380)

Name	Type	Description	Properties	Algorithms
				SHA2-384: (A5380) SHA2-512: (A5380)
ecsiggencomp	DigSig-SigGen	Digital Signature Generation Component		ECDSA SigGen (FIPS186-5): (A5375) Counter DRBG: (A5383) SHA2-224: (A5380) SHA2-256: (A5380) SHA2-384: (A5380) SHA2-512: (A5380)
rsasiggen	DigSig-SigGen	Digital Signature Generation		RSA SigGen (FIPS186-5): (A5374) Counter DRBG: (A5383) SHA2-224: (A5380) SHA2-256: (A5380) SHA2-384: (A5380) SHA2-512: (A5380) SHA3-224: (A5382) SHA3-256: (A5382) SHA3-384: (A5382) SHA3-512: (A5382)
rsasp1	DigSig-SigGen	Digital Signature Generation Component		RSA Signature Primitive: (A5374) Counter DRBG: (A5383)
ecsigver	DigSig-SigVer	Digital Signature Verification		ECDSA SigVer (FIPS186-4): (A5375) Counter DRBG: (A5383) SHA-1: (A5380) SHA2-224: (A5380) SHA2-256: (A5380) SHA2-384: (A5380) SHA2-512: (A5380)

Name	Type	Description	Properties	Algorithms
				ECDSA SigVer (FIPS186-5): (A5375)
rsasigver	DigSig-SigVer	Digital Signature Verification		RSA SigVer (FIPS186-4): (A5374) Counter DRBG: (A5383) SHA2-224: (A5380) SHA2-256: (A5380) SHA2-384: (A5380) SHA2-512: (A5380) RSA SigVer (FIPS186-5): (A5374)
rsadp	UNK	RSA Decryption Component		RSA Decryption Primitive Sp800-56Br2: (A5374)
drbg	DRBG	Random Number Generation		Counter DRBG: (A5383) AES-ECB: (A5371)
trng	ENT-ESV	Entropy Source		
kasecc	KAS-Full	Key Agreement	Caveat:Key establishment method provides between 128 and 192 bits of encryption strength	KAS-ECC Sp800-56Ar3: (A5378) SHA2-256: (A5381) SHA2-384: (A5381) AES-CMAC: (A5372)
kasssc	KAS-SSC	Key Agreement Shared Secret		KAS-ECC-SSC Sp800-56Ar3: (A5379)
kbkdf	KBKDF	Key-Based Key Derivation		KDF SP800-108: (A5377) AES-CMAC: (A5372)
aeskw	BC-Auth	Key Unwrapping for internal use importing keys at manufacturing		AES-KW: (A5384) AES-KWP: (A5384)
aescmac	MAC	Message Authentication Generation		AES-CMAC: (A5372)

Name	Type	Description	Properties	Algorithms
hmac	MAC	Message Authentication Generation		HMAC-SHA2-224: (A5376) HMAC-SHA2-256: (A5376) HMAC-SHA2-384: (A5376) HMAC-SHA2-512: (A5376)
shs#1	SHA	Secure Hash Standard		SHA2-224: (A5380) SHA2-256: (A5380) SHA2-384: (A5380) SHA2-512: (A5380)
shs#2	SHA	Secure Hash Standard		SHA2-224: (A5381) SHA2-256: (A5381) SHA2-384: (A5381) SHA2-512: (A5381)
sha-3	SHA	Secure Hash Standard		SHA3-224: (A5382) SHA3-256: (A5382) SHA3-384: (A5382) SHA3-512: (A5382)
scp03	KTS-Wrap	Key Transport - Wrapping	Caveat:Key establishment methodology provides between 128 and 256 bits of encryption strength	AES-CMAC: (A5372) AES-CBC: (A5371)

Table 8: Security Function Implementations

2.7 Algorithm Specific Information

KAS [56Ar3] - Per [IG] D.F Scenario 2 path (2), compliant key agreement scheme where testing is performed end-to-end for the shared secret computation and a KDF compliant with SP 800-56C2 with key confirmation.

KAS-SSC [56Ar3] - Per [IG] D.F Scenario 2 path (2), compliant with the derivation of a shared secret Z in one or more of the key agreement schemes in Section 6 of SP 800-56Arev3.

2.8 RBG and Entropy

Cert Number	Vendor Name
E112	STMicroelectronics

Table 9: Entropy Certificates

The Module uses the following entropy sources:

Name	Type	Operational Environment	Sample Size	Entropy per Sample	Conditioning Component
ESV Entropy Source	Physical	ST31N600 revB and revC	1 bit	0.75	N/A

Table 10: Entropy Sources

The entropy source provides a min-entropy of H >= 0.75. The output of the entropy source is used for the instantiation of the NIST SP800-90A compliant DRBG (#A5383). 568 bits of entropy is collected which provides 384 bits of entropy for the DRBG and 184 bits of entropy for the nonce. The 384 bits of entropy accounts for 288 bits of entropy which exceeds the 256-bits required. 184 bits of entropy for the nonce accounts for 138 bits of entropy.

2.9 Key Generation

For Key Generation methods, see Section 2.5 Algorithms and Section 2.6 Security Function Implementations above.

2.10 Key Establishment

For Key Establishment methods, see Section 2.5 Algorithms and Section 2.6 Security Function Implementations above.

3 Cryptographic Module Interfaces

3.1 Ports and Interfaces

The Module's ports and associated FIPS defined logical interface categories are listed below.

Physical Port	Logical Interface(s)	Data That Passes
VCC, GND	Power	ISO 7816: Supply voltage - Contact configurations only
RST	Control Input	ISO 7816: Reset - Contact configurations only
CLK	Control Input	Control in - Contact configurations only
I/O	Data Input Data Output Control Input Status Output	ISO 7816: Clock - Contact configurations only
LA, LB	Data Input Data Output Control Input Status Output Power	ISO 7816: Input/Output - Contact configurations only

Table 11: Ports and Interfaces

Note: The module does not support Control Output.

Control/data input and status/data output are separated by the command-response nature of the Module. The Module is either transmitting or receiving, but never both at once. ISO/IEC 7816-4 APDUs are used for communication over the contact-based (ISO7816) and contactless (ISO14443) interfaces.

The APDU interface is used by an external Card Acceptance Device (CAD), i.e. an off card application and card reader/writer, to send commands to the Module. The APDU interface is mapped to the physical I/O port and LA/LB port. It comprises the logical interface for Data in, Control in, Data out and Status out. Data in corresponds to the data field of APDU commands received by the Module. Control in corresponds to APDU command header. Data and status output are mapped to APDU responses sent by the Module. Data out is mapped to the data field of APDU responses. The Status out is mapped to the status code, SW1 SW2 (ISO/IEC 7816 status word).

The Hardware interface for contact-based, contactless, and dual-interface operations is composed of the parameters to supply the Module for start-up and for operation.

The Control input for contact-based (ISO 7816-3) operation is mapped to RST (reset signal) and CLK (clock signal).

The Control input (clock and reset) and the power supply for contactless (ISO 14443) operation is mapped to the coil connections LA and LB.

Dual-interface controllers may be powered either by contact-based or by contactless power supply.

4 Roles, Services, and Authentication

4.1 Authentication Methods

Method Name	Description	Security Mechanism	Strength Each Attempt	Strength per Minute
AM1	Identity Based Authentication: The CO role manages module content and configuration,	Secure Channel Protocol Authentication Method See Section 4.1.1	The probability that a random attempt will succeed using this authentication method is:	The module enforces a maximum of fifteen (15) consecutive failed SCP authentication attempts. The probability that a random attempt

Method Name	Description	Security Mechanism	Strength Each Attempt	Strength per Minute
	including issuance and management of module data via the ISD..	Secure Channel Protocol Authentication Method	1/2^128 = 2.9E-39 (for any of AES-128/192/256 SD-KENC/SD-SENC, assuming a 128-bit block)	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
AM2	Identity Based Authentication: The User role is for use in Demonstration applet.	Demonstration Applet Authentication Method See section 4.1.2 Demonstration Applet Authentication Method:	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 (4) consecutive failed authentication attempts. The probability that a random attempt will succeed over a one minute interval is: 4/256^8.

Table 12: Authentication Methods

After activation or reset of the Module no operator is authenticated. Actions on behalf of an operator require the operator's prior successful authentication. The Module's authentication methods prevent unauthorized disclosure and modification of SSPs.

The Module supports identity-based operator authentication by means of SCP03, defined in [GP Amd D].

The Module prevents reuse of authentication data related to the Secure Channel Protocol.

After completion of the authentication protocol, the Module accepts commands with correct message authentication code only. These commands must have been sent via the Secure Channel using the key previously agreed with the terminal during the authentication. Protection of user data transmitted from the Module to the terminal is achieved by means of secure messaging with encryption and message authentication codes. After authentication, user data in transit is protected from unauthorized disclosure, modification, deletion, insertion and replay attacks. In the usage phase, authentication data entry, modification and substitution is performed within a Secure Channel only.

The Module does not output the Secure Channel static keys or the Secure Channel session keys.

The PIN used by the Demonstration Applet's PIN authentication service can only be transmitted to the Module after successful initiation of a Secure Channel. The PIN is never output by the Module.

Feedback provided during an authentication attempt is indicated in the status words (SW1 SW2) returned in the response message to the INITIALIZE UPDATE and EXTERNAL AUTHENTICATE commands. Successful execution of the command is indicated by the status bytes ’90’ ‘00’. In case of an error, the status code either corresponds to one of the General Error conditions or to a specific error condition defined in [GPCS]. Status information does not contain CSPs or sensitive data that if misused could lead to a compromise of the module. The status returned does not weaken the strength of the mechanism.

Secure Channel Protocol Authentication Method

The Secure Channel Protocol authentication method (I2 in the SSP Input-Output Methods table) 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 [108]. The PRF used in the KDF is CMAC as specified in NIST 800-38B [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).

Demonstration Applet Authentication Method

The Demonstration Applet Authentication method is provided by the Secure Channel Protocol Authentication Method (I1 in the SSP Input-Output Methods table) combined with the PIN 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 Module does not visibly display the PIN.

4.2 Roles

The Module supports two distinct operator roles, User and Cryptographic Officer (CO). The Module enforces the separation of roles using authentication. Re-authentication is enforced when changing roles.

The table below lists all operator roles supported by the Module. In addition, the Module supports services which does not require to be authenticated, see also services table below.

The Module does not support a maintenance role and bypass capability. The Module supports concurrent operators in a limited fashion. The module allows for multiple logical channels. Only one operator at a time is permitted on a logical channel, which explains the limitation posed upon concurrent operators. The separation of roles operating on different logical channel is ensured by having different secure channels with different session keys.

Name	Type	Operator Type	Authentication Methods
Cryptographic Officer	Identity	CO	AM1
User	Identity	User	AM2

Table 13: Roles

4.3 Approved Services

All approved services implemented by the Module are listed in the table below:

The SSPs modes of access shown in the table below are defined as:

- G = Generate: The Module generates or derives the SSP.
- R = Read: The SSP is read from the Module (e.g., the SSP is output).
- W = Write: The SSP is updated, imported, or written to the Module (SSP is input).
- E = Execute: The Module uses the SSP in performing a cryptographic operation.
- Z = Zeroize: The Module zeroizes the SSP

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Lifecycle	Modifies the card or applet life cycle status.	Approved mode is given in the ATR: the value 0x46 ('F')	GET STATUS/ SET STATUS	Lifecycle state, status word	scp03	Cryptographic Officer - SD-SENC: E,Z - SD-SMAC: E,Z - SD-SRMAC: E,Z - DRBG-EI: Z - DRBG-SM: Z - DRBG-Nonce: Z - OS-DRBG-STATE: Z - SD-KENC: Z - SD-KMAC: Z - SD-KDEK: Z - SD-DAP-AES: Z - SD-DAP-ECC: Z - SD-DAP-RSA: Z - SD-CIPH-LD-AES: Z - SD-DM-TOKEN-AES: Z - SD-DM-TOKEN-ECC: Z - SD-DM-TOKEN-RSA: Z - SD-DM-RCPT-AES: Z - SD-DM-RCPT-ECC: Z

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						- SD-DM-RCPT-RSA: Z - PIN_KEY: Z - DEM-PIN: Z - DEM CMAC: Z - DEM HMAC: Z - DEM-DH-PRIV: Z - DEM-DH-PUB: Z - DEM-KAS-PRIV: Z - DEM-KAS-PUB: Z - DEM-SGV-RSA-PRIV: Z - DEM-SGV-RSA-PUB: Z - DEM-SGV-ECC-PRIV: Z - DEM-SGV-ECC-PUB: Z - DEM_SHARED_SEC_SSC: Z - DEM SHARED_SEC_ECC: Z
Manage Content	Loads and installs application packages and associated keys and data.	Approved mode is given in the ATR: the value 0x46 ('F')	Content management commands LOAD, INSTALL, DELETE, STORE DATA, PUT KEY	Status word	aesenc aesdec ecsiggen ecsigver aeskw scp03	Cryptographic Officer - SD-SENC: E - SD-SMAC: E - SD-SRMAC: E - SD-KDEK: E - SD-DAP-RSA: E - SD-DAP-AES: E - SD-CIPH-LD-AES: E - SD-DM-TOKEN-AES: E - SD-DM-TOKEN-ECC: E - SD-DM-TOKEN-RSA: E - SD-DM-RCPT-AES: E - SD-DM-RCPT-ECC: E - SD-DM-RCPT-RSA: E - SD-DAP-ECC: E

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Module Info (Authenticated)	Reads module configuration or status information (privileged data objects).	Approved mode is given in the ATR: the value 0x46 ('F')	GET DATA, GET STATUS command	Configuration data, status word	scp03	Cryptographic Officer - SD-SENC: E - SD-SMAC: E - SD-SRMAC: E User - SD-SENC: E - SD-SMAC: E - SD-SRMAC: E
Module Info (Unauthenticated)	Reads module configuration or status information.	Approved mode is given in the ATR: the value 0x46 ('F')	GET DATA	Configuration data, Status word	None	Unauthenticated
Secure Channel	Establishes and uses a secure communications channel.	Approved mode is given in the ATR: the value 0x46 ('F')	INTIALIZE UPDATE/EXTERNAL AUTH command	card challenge, card cryptogram, status word	kbkdf	Cryptographic Officer - SD-KENC: E - SD-KMAC: E - SD-SENC: G - SD-SMAC: G - SD-SRMAC: G User - SD-SENC: G - SD-KENC: E - SD-KMAC: E - SD-SMAC: G - SD-SRMAC: G
PIN Authentication	Demonstrates PIN authentication with OwnerPIN.	Approved mode is given in the ATR: the value	Command to Demo Applet to call API OwnerPIN.checkwith PIN	Status word	aesenc aesdec	User - PIN_KEY: E - DEM-PIN: R

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
		0x46 ('F')				
Key Generation	Generates keys and initializes symmetric and asymmetric key objects for the cryptographic services.	Approved mode is given in the ATR: the value 0x46 ('F'	Command to Demo Applet to call API for key generation. API input: Domain parameters	status word	ecckeygen rsakeygen eckeyval	User - DEM-DH-PRIV: G - DEM-DH-PUB: G - DEM-KAS-PRIV: G - DEM-KAS-PUB: G - DEM-SGV-RSA-PRIV: G - DEM-SGV-RSA-PUB: G - DEM-SGV-ECC-PRIV: G - DEM-SGV-ECC-PUB: G
Digital Signature	Demonstrates RSA and ECDSA digital signature generation and verification, ECDSA digital signature component and the RSA Signature Primitive.	Approved mode is given in the ATR: the value 0x46 ('F'	Command to Demo Applet to call API: API input: Signature Generation: ECDSA, RSA private key and message Signature Verification: ECDSA public key and signature	Signature, status word.	ecsiggen ecsiggencomp rsasiggen rsasp1 ecsigver rsasigver rsadp	User - DEM-SGV-RSA-PRIV: E - DEM-SGV-RSA-PUB: E - DEM-SGV-ECC-PRIV: E - DEM-SGV-ECC-PUB: E
Key Agreement Primitive	Generates a common secret from a DH key exchange	Approved mode is given in the ATR: the value 0x46 ('F'	Command to Demo Applet to call API: API input: Card Privat key, Host Public key	common secret	kasssc	User - DEM-DH-PRIV: E - DEM-DH-PUB: E - DEM_SHARED_SEC_SSC: G,E
RSA Decryption Primitive	Demonstrates the RSA Decryption Primitive	Approved mode is given in the	Command to Demo Applet to call API: API input: RSA	Cryptogram, status word	rsadp	User - DEM-SGV-ECC-PRIV: E - DEM-SGV-RSA-PUB: E

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
		ATR: the value 0x46 ('F'	private key, plain input data			
Opacity	KAS-Full with parameters according to SP.800-73-4	Approved mode is given in the ATR: the value 0x46 ('F'	Command to Demo Applet to call API: API input: Card Privat key, Host Public key	AuthCrytogram	kasecc	User - DEM-KAS-PRIV: E - DEM-KAS-PUB: E - DEM SHARED_SEC_ECC: G,E
Message Authentication	Authenticate messages	Approved mode is given in the ATR: the value 0x46 ('F'	Command to Demo Applet to call API: API input: Message	MAC	aescmac hmac	User - DEM CMAC: E - DEM HMAC: E
Message Digest	Generates hashes	Approved mode is given in the ATR: the value 0x46 ('F'	Command to Demo Applet to call API: API input: Message	Hash value	shs#1 shs#2 sha-3	User
Error Log	Logging of error states	Approved mode is given in the ATR: the value 0x46 ('F'	Error state triggered	Error status in ATR	None	Cryptographic Officer User Unauthenticated
Module Reset	Resets the module. Includes	Approved mode is given	RST or Power OFF+ Power ON	ATR	drbg trng	Cryptographic Officer - DRBG-EI: E,Z - OS-DRBG-STATE: G

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
	Power-On Self-Test.	in the ATR: the value 0x46 ('F'				- SD-SENC: Z - SD-SMAC: Z - SD-SRMAC: Z - DEM_SHARED_SEC_SSC: Z - DEM SHARED_SEC_ECC: Z - DEM-KAS-PUB: Z - DEM-DH-PUB: Z - DEM-DH-PRIV: Z User - DRBG-EI: E - OS-DRBG-STATE: G - SD-SENC: Z - SD-SMAC: Z - SD-SRMAC: Z - DEM_SHARED_SEC_SSC: Z - DEM SHARED_SEC_ECC: Z Unauthenticated

Table 14: Approved Services

4.4 Non-Approved Services

NOTE: There are no non-approved services available.

N/A for this module.

4.5 External Software/Firmware Loaded

NOTE: There is no External Software/Firmware Loaded.

5 Software/Firmware Security

5.1 Integrity Techniques

The Module's firmware is composed of the embedded operating system and Java card packages including the demonstration applet.

An error detection code is applied to all software and firmware components within the hardware module's defined cryptographic boundary.

5.2 Initiate on Demand

The operator can initiate the integrity test on demand by Module reset.

6 Operational Environment

6.1 Operational Environment Type and Requirements

Type of Operational Environment: Non-Modifiable

The Module has a non-modifiable operational environment under the FIPS 140-3 definitions.

7 Physical Security

The Module is a single-chip implementation that meets commercial-grade specifications for power, temperature, reliability, and shock/vibrations. The Module uses standard passivation techniques.

7.1 Mechanisms and Actions Required

The Module's chip packaging uses tamper evident material that is opaque within the visible spectrum. The material is designed so that attempts at removal or penetration will have a high probability of causing serious damage.

Mechanism	Inspection Frequency	Inspection Guidance
Tamper-Evident Material	Before first use by end user.	Operator should look for damage

Table 15: Mechanisms and Actions Required

7.5 EFP/EFT Information

Temp/Voltage Type	Temperature or Voltage	EFP or EFT	Result
LowTemperature	-60°C	EFP	Shutdown
HighTemperature	128°C	EFP	Shutdown
LowVoltage	2.2V	EFP	Shutdown
HighVoltage	6.2V	EFP	Shutdown

Table 16: EFP/EFT Information

7.6 Hardness Testing Temperature Ranges

Temperature Type	Temperature
LowTemperature	-25°C
HighTemperature	85°C

Table 17: Hardness Testing Temperatures

8 Non-Invasive Security

Non-invasive mechanisms employed by the Module are under Section 12 Mitigation of other attacks.

9 Sensitive Security Parameters Management

9.1 Storage Areas

Storage Area Name	Description	Persistence Type
S1	Only stored in volatile memory RAM	Dynamic
S2	Stored in NVM in plaintext, associated by memory location pointer	Static
S3	Stored in NVM, obfuscated by dynamically generated mask	Static

Table 18: Storage Areas

9.2 SSP Input-Output Methods

Name	From	To	Format Type	Distribution Type	Entry Type	SFI or Algorithm
Input encapsulated in Secure Channel (I1)	Application Software (outside)	S3	Encrypted	Manual	Electronic	scp03
Input encapsulated in Secure Channel (I2)	Application Software (outside)	S3	Encrypted	Automated	Electronic	scp03

Table 19: SSP Input-Output Methods

9.3 SSP Zeroization Methods

Zeroization Method	Description	Rationale	Operator Initiation
Z1	Replace with zeros	All data in storage area S1 are zeroized if module is reset. Not time critical, related SSPs are not accessible by unauthorized operators.	Any role: reset Module
Z2	Replace with zeros	Used to zeroize all sensitive data at end of life of module. See also chapter End of Life.	CO role: set life cycle state to TERMINATED

Table 20: SSP Zeroization Methods

The zeroization of SSPs is implemented as an internal process without connection to data output.

Zeroization is implicit

Z1: Concerning the “Temporary Storage Duration”, an SSP which is stored in category S1 is stored until the next reset of the module. There is no specific time duration for this.

Z2: Issuing the APDU SET STATUS (TERMINATE) command will destroy all sensitive data on the module and leave the module inoperable.

9.4 SSPs

All usage of these SSPs by the Module are described in the services detailed in Section 4.3 Approved Services.

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
DRBG-EI	Entropy input	384 - N/A	Entropy - CSP	trng		drbg
DRBG-SM	Seed material	568 - N/A	Entropy - CSP	trng		drbg
DRBG-Nonce	Nonce	184 - N/A	Entropy - CSP	trng		drbg
OS-DRBG-STATE	Internal state: V (128 bits) and Key (AES 256)	384 - N/A	Entropy - CSP	trng		drbg
SD-KENC	Master key decryption Key	128,192,1256 - 128,192,256	Symmetric authentication key - CSP	Input at manufacturing		kbkdf
SD-KMAC	Master MAC Key	128,192,256 - 128,192,256	Secret - CSP	Input at manufacturing		kbkdf
SD-KDEK	Master key decryption Key	128,192,256 - 128,192,256	Secret - CSP	Input at manufacturing		aesenc aesdec
SD-SENC	Session Key	128,192,256 - 128,192,256	Secret - CSP	kbkdf		aesenc aesdec

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
SD-SMAC	Session Key	128,192,256 - 128,192,256	Secret - CSP	kbkdf		aescmac
SD-SRMAC	Session Key	128,192,256 - 128,192,256	Secret - CSP	kbkdf		aescmac
SD-DAP-AES	AES DAP verification key	128,192, 256 - 128,192, 256	Secret - CSP	Input at manufacturing		aescmac
SD-DAP-ECC	ECC DAP verification key	P Curves (192, 224, 256,384 521) - 96-256	Public - PSP	Input at manufacturing		ecsigver
SD-DAP-RSA	RSA DAP verification key	1024- 4096 - 80-200	Public - PSP	Input at manufacturing		rsasigver
SD-CIPH-LD-AES	Loadfile decryption key	128, 192, 256 - 128, 192, 256	Secret - CSP	Input at manufacturing		AES-CBC (A5371)
SD-DM-TOKEN-AES	AES token verification key	128, 192, 256 - 128, 192, 256	Public - PSP	Input at manufacturing		aescmac
SD-DM-TOKEN-ECC	ECC token verification key	P Curves (192, 224, 256,384 521) - 96-256	Public - PSP	Input at manufacturing		ecsigver
SD-DM-TOKEN-RSA	RSA token verification key	1024- 4096 - 80-200	Public - PSP	Input at manufacturing		rsasigver
SD-DM-RCPT-AES	AES receipt generation key	128, 192, 256 - 128, 192, 256	Secret - CSP	Other		aescmac
SD-DM-RCPT-ECC	ECC receipt generation key	P Curves (224, 256,384 521) - 112-256	Private - CSP	Input at manufacturing		ecckeygen
SD-DM-RCPT-RSA	RSA receipt generation key	2048-4096 - 112-200	Private - CSP	Other		rsakeygen
PIN_KEY	Key for PIN obfuscation	256 - 256	Secret - CSP	Input at manufacturing		aesenc aesdec
DEM-PIN	Demo Applet User PIN	256 - 256	PIN - CSP	Other		aesdec
DEM CMAC	Key for CMAC calculation	128, 192, 256 - 128, 192, 256	Secret - CSP	N/A		aescmac

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
DEM HMAC	Key for HMAC calculation	Min: 8 Max: 2040 - -	Secret - CSP	N/A		hmac
DEM-DH-PRIV	Demo Applet ECC CDH private key	P Curves (224, 256,384 521 - 112-256	Private - CSP	ecckeygen		ecckeygen
DEM-DH-PUB	Demo Applet ECC CDH public key	P Curves (224, 256,384 521) - 112-256	Public - PSP	N/A		ecckeygen
DEM-KAS-PRIV	Demo Applet KAS ECC (Opacity) private key	P Curves (256,384) - 128, 192	Private - CSP	ecckeygen		kasssc
DEM-KAS-PUB	Demo Applet KAS ECC public key	P Curves (256,384) - 128, 192	Public - PSP	N/A		kasssc
DEM-SGV-RSA-PRIV	Demo Applet RSA signature private key	2048-4096 - 112-200	Private - CSP	rsakeygen		rsasiggen
DEM-SGV-RSA-PUB	Demo Applet RSA signature public key	1024-4096 - 80-200	Public - PSP	rsakeygen		rsasigver
DEM-SGV-ECC-PRIV	Demo Applet ECC signature private key	P Curves (224, 256,384 521) - 112-256	Private - CSP	ecckeygen		ecsiggen
DEM-SGV-ECC-PUB	Demo Applet ECC signature public key	P Curves (192, 224, 256,384 521) - 96-256	Public - PSP	ecckeygen		ecsigver
DEM_SHARED_SEC_SSC	Shared secret	224, 256, 384, 521 - 112-256	Private - CSP	N/A	kasssc	kasssc
DEM SHARED_SEC_ECC	Shared secret	128, 256 - 128, 256	Private - CSP	N/A	kasecc	kasecc

Table 21: SSP Table 1

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
DRBG-EI		S1:Plaintext	until the next reset of the module	Z1	DRBG-SM:Derived From
DRBG-SM		S1:Plaintext	until the next reset of the module	Z1	DRBG-EI:Used by
DRBG-Nonce		S1:Plaintext	N/A until the next reset of the module	Z1	DRBG-SM:Used by
OS-DRBG-STATE		S1:Plaintext	until the next reset of the module	Z1	DRBG-EI:Derived From
SD-KENC		S3:Obfuscated	N/A	Z2	SD-SENC:Derived From
SD-KMAC		S3:Obfuscated	N/A	Z2	SD-SMAC:Derived From SD-SRMAC:Derived From
SD-KDEK		S3:Obfuscated	N/A	Z2	DEM-PIN:Decrypts DEM CMAC:Decrypts DEM HMAC:Decrypts DEM-DH-PUB:Decrypts DEM-KAS-PUB:Decrypts
SD-SENC		S1:Plaintext	until the next reset of the module	Z1	SD-KENC:Derived From
SD-SMAC		S1:Plaintext	until the next reset of the module	Z1	SD-KMAC:Derived From

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
SD-SRMAC		S1:Plaintext	until the next reset of the module	Z1	SD-KMAC:Derived From
SD-DAP-AES		S3:Obfuscated	N/A	Z2	
SD-DAP-ECC		S3:Obfuscated	N/A	Z2	
SD-DAP-RSA		S3:Obfuscated	N/A	Z2	
SD-CIPH-LD-AES		S3:Obfuscated	N/A	Z2	
SD-DM-TOKEN-AES		S3:Obfuscated	N/A	Z2	
SD-DM-TOKEN-ECC		S3:Obfuscated	N/A	Z2	
SD-DM-TOKEN-RSA		S3:Obfuscated	N/A	Z2	
SD-DM-RCPT-AES		S3:Obfuscated	N/A	Z2	
SD-DM-RCPT-ECC		S3:Obfuscated	N/A	Z2	
SD-DM-RCPT-RSA		S3:Obfuscated	N/A	Z2	
PIN_KEY		S3:Obfuscated	N/A	Z2	DEM-PIN:Derived From
DEM-PIN	Input encapsulated in Secure Channel (I1)	S3:Obfuscated	N/A	Z2	PIN_KEY:Derived From
DEM CMAC	Input encapsulated in Secure Channel (I2)	S3:Obfuscated		Z2	
DEM HMAC	Input encapsulated in Secure Channel (I2)	S3:Obfuscated		Z2	
DEM-DH-PRIV		S3:Obfuscated S1:Plaintext		Z1 Z2	DEM_SHARED_SEC_SSC:Calculates secret with DEM-DH-PUB DEM SHARED_SEC_ECC:Calculates secret with DEM-DH-PUB
DEM-DH-PUB	Input encapsulated	S1:Plaintext	until the next reset	Z1	DEM_SHARED_SEC_SSC:Calculates secret with DEM-DH-PRIV

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
	in Secure Channel (I2)		of the module		DEM SHARED_SEC_ECC:Calculates secret with DEM-DH-PRIV
DEM-KAS-PRIV		S3:Obfuscated	N/A	Z2	DEM-KAS-PUB:Calculates secret with
DEM-KAS-PUB	Input encapsulated in Secure Channel (I2)	S1:Plaintext	until the next reset of the module	Z1	DEM-KAS-PRIV:Calculates secret with
DEM-SGV-RSA-PRIV		S3:Obfuscated		Z2	DEM-SGV-RSA-PUB:Paired With
DEM-SGV-RSA-PUB		S2:Plaintext		Z2	DEM-SGV-RSA-PRIV:Paired With
DEM-SGV-ECC-PRIV		S3:Obfuscated		Z2	DEM-SGV-ECC-PUB:Paired With
DEM-SGV-ECC-PUB		S2:Plaintext		Z2	DEM-SGV-ECC-PUB:Paired With
DEM_SHARED_SEC_SSC		S1:Plaintext	until the next reset of the module	Z1	DEM-DH-PRIV:Derived From DEM-DH-PUB:Derived From
DEM SHARED_SEC_ECC		S1:Plaintext	until the next reset of the module	Z1	DEM-KAS-PRIV:Derived From DEM-KAS-PUB:Derived From

Table 22: SSP Table 2

9.5 Transitions

The following list specifies applicable transition periods or timeframes where an algorithm or key length transitions from Approved to non-Approved:

• SHA-1: The module includes an implementation of SHA-1 for hashing and digital signature verification. This implementation will be non-Approved for all uses starting January 1, 2030.

10 Self-Tests

The Module performs self-tests to ensure the proper operation of the Module. Per FIPS 140-3 these are categorized as either pre-operational self-tests or conditional self-tests.

The Module will not accept any commands when a self-test is running, because another command can only be processed if the actual command which triggers the self-test is finished. The command which has triggered the self-test may still be in the I/O buffer and will be processed if the self-tests are finished. Therefore, no operator action is involved in executing the self-tests.

If a self-test succeeds, the last two bytes of the historical bytes of the ATR is set to '9000'. If a self-test fails, the Module logs the latest self-test error in the last two bytes of the historical bytes of the ATR, see ATR structure in section 2.4 Modes of Operation. The CO/User can consult the error log by observing these bytes which are unique for every self-tests.

10.1 Pre-Operational Self-Tests

Periodic Method: All pre-operational self-tests are performed by the Module at the first command after every reset. As the Module is frequently reset the tests are performed periodically (IG 10.3.E, Resolution 3.a.).

The Module performs the following pre-operational self-tests.

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details
Firmware integrity	Reed Solomon-32	KAT	SW/FW Integrity	Pass - Approved mode Fail - Error Code	A 16 bit Reed-Solomon EDC performed over all code in the cryptographic boundary is compared to a pre-stored value.
TRNG	RCT and APT	SP 800-90B health-test	Critical Function	Pass - Approved mode Fail - Error Code	An RCT and APT as specified in [90B] section 4.4 are executed before generation of the DRBG entropy input

Table 23: Pre-Operational Self-Tests

10.2 Conditional Self-Tests

As the column space is limited here some explanations for some columns:

Periodic Method: The conditional self-tests are performed before the first use of an algorithm after every reset. This results in a periodic execution as the module is reset frequently. (IG 10.3.E, Resolution 3.a.).

Period: Until next reset.

Indicator: The self-test pass indicator is a '9000' in the ATR, the fail indicator is an error code in the ATR.

Condition: There are two conditions when a conditional self-test is executed:

COND1: Before the first use of an algorithm after reset.

COND2: After each key generation.

The below tests with test method KAT consist of a set of known input vectors (input data, keys) which are operated on by the cryptographic algorithm to generate a result. The result is compared to the known expected output result. If the calculated output does not equal the known answer, the self-test error state is set.

The Module performs the following conditional self-tests:

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
AES-ECB (A5371)	AES-128	KAT	CAST	Pass - Approved mode Fail - Error Code	AES-128 ECB decryption of 16 byte data	COND1
AES CMAC Generation	AES-128	KAT	CAST	Pass - Approved mode Fail - Error Code	AES CMAC 128. KAT for CMAC generation. As CMAC uses AES encryption this self-tests includes an AES ENC self-test	COND1
AES-CMAC Verification	AES-128	KAT	CAST	Pass - Approved mode Fail - Error Code	AES CMAC 128. KAT for CMAC verification.	COND1
Counter DRBG (A5383)	AES-256 CTR_DRBG.	KAT	CAST	Pass - Approved mode Fail - Error Code	One KAT for instantiation and generation performed before the first random data generation.	COND1
KAS-ECC Sp800-56Ar3 (A5378)	P-256	KAT	CAST	Pass - Approved mode Fail - Error Code	ECCDH Shared Secret computation.	COND1
One-Step KDF (A5378)	SHA-256	KAT	CAST	Pass - Approved mode Fail - Error Code	"One-Step KDF" part of KAS ECC. The other parts ECC CDH and the final AES CMAC (key confirmation) are tested already by the self-tests KAS-SCC and AES-CMAC above.	COND1
KDF SP800-108 (A5377)	AES-128 CMAC	KAT	CAST	Pass - Approved mode Fail - Error Code	SP 800-108 KDF. This self-test is inclusive of AES CMAC and AES encrypt self-test.	COND1
ECDSA KeyGen (FIPS186-5) (A5375)	P-224, P-256, P-384, P-521	PCT	PCT	Pass - Approved mode Fail - Error Code	With the generated key pair an ECDSA signature is generated and the result is given as input to the verify method, and it is checked that the call is successful.	COND2

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
ECDSA SigGen (FIPS186-5) (A5375)	P-256	KAT	CAST	Pass - Approved mode Fail - Error Code	Test mode activated, so that a fix random is used to get a constant oupout from ECDSA sign	COND1
ECDSA SigVer (FIPS186-5) (A5375)	P-256	KAT	CAST	Pass - Approved mode Fail - Error Code	KAT for signature verification	COND1
HMAC-SHA2-256 (A5376)	HMAC-256 with SHA-256	KAT	CAST	Pass - Approved mode Fail - Error Code	HMAC with key length 256 and SHA-256 hash	COND1
RSA Decryption Primitive Sp800-56Br2 (A5374)	2048	KAT	CAST	Pass - Approved mode Fail - Error Code	RSA CRT sign and verify with known key and known 256 bytes input data	COND1
RSA KeyGen (FIPS186-5) (A5373)	2048, 3072	PCT	PCT	Pass - Approved mode Fail - Error Code	With the generated RSA Standard key pair known input data are decrypted and encrypted and the result is compared to the input data.	COND2
RSA SigGen (FIPS186-5) (A5374)	2048	KAT	CAST	Pass - Approved mode Fail - Error Code	RSA-2048 KAT for signature generation.	COND1
RSA SigVer (FIPS186-5) (A5374)	2048	KAT	CAST	Pass - Approved mode Fail - Error Code	-RSA-2048 KAT for signature verification.	COND1
RSA KeyGen CRT	2048, 3072, 4096	-	PCT	Pass - Approved mode Fail - Error Code	With the generated RSA CRT key pair known input data are decrypted and encrypted and the result is compared to the input data.	COND2
SHA-1 (A5380)	SHA-1	KAT	CAST	Pass - Approved	Hashing of 67 bytes input data	COND1

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
				mode Fail - Error Code		
SHA2-256 (A5381)	SHA2-256	KAT	CAST	Pass - Approved mode Fail - Error Code	Hashing of 67 bytes input data	COND1
SHA3-256 (A5382)	SHA3-256	KAT	CAST	Pass - Approved mode Fail - Error Code	Hashing of 67 bytes input data	COND1
SHA2-512 (A5381)	SHA2-512	KAT	CAST	Pass - Approved mode Fail - Error Code	Hashing of 67 bytes input data	COND1
SHA2-256 (A5380)	SHA2-256	KAT	CAST	Pass - Approved mode Fail - Error Code	Hashing of 67 bytes input data	COND1
SHA2-512 (A5380)	SHA2-512	KAT	CAST	Pass - Approved mode Fail - Error Code	Hashing of 67 bytes input data	COND1

Table 24: Conditional Self-Tests

10.3 Periodic Self-Test Information

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
Firmware integrity	KAT	SW/FW Integrity	Every Reset	All Pre-operational self-tests are performed by the Module at the first command after every reset. As the module is frequently reset the tests are periodically performed (IG 10.3.E, Resolution 3.a.).
TRNG	SP 800-90B health-test	Critical Function	Every Reset cycle	All Pre-operational self-tests are performed by the Module at the first command after every reset. As the module is frequently reset the tests are periodically performed (IG 10.3.E, Resolution 3.a.)

Table 25: Pre-Operational Periodic Information

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
AES-ECB (A5371)	KAT	CAST	no specific duration	The conditional self-tests are performed before the first use of an algorithm after every reset. This results in a periodically execution as the

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
				module is frequently reset. (IG 10.3.E, Resolution 3.a.).
AES CMAC Generation	KAT	CAST	no specific duration	The conditional self-tests are performed before the first use of an algorithm after every reset. This results in a periodically execution as the module is frequently reset. (IG 10.3.E, Resolution 3.a.).
AES-CMAC Verification	KAT	CAST	no specific duration	The conditional self-tests are performed before the first use of an algorithm after every reset. This results in a periodically execution as the module is frequently reset. (IG 10.3.E, Resolution 3.a.).
Counter DRBG (A5383)	KAT	CAST	no specific duration	The conditional self-tests are performed before the first use of an algorithm after every reset. This results in a periodically execution as the module is frequently reset. (IG 10.3.E, Resolution 3.a.).

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
KAS-ECC Sp800-56Ar3 (A5378)	KAT	CAST	no specific duration	The conditional self-tests are performed before the first use of an algorithm after every reset. This results in a periodically execution as the module is frequently reset. (IG 10.3.E, Resolution 3.a.).
One-Step KDF (A5378)	KAT	CAST	no specific duration	The conditional self-tests are performed before the first use of an algorithm after every reset. This results in a periodically execution as the module is frequently reset. (IG 10.3.E, Resolution 3.a.).
KDF SP800-108 (A5377)	KAT	CAST	no specific duration	The conditional self-tests are performed before the first use of an algorithm after every reset. This results in a periodically execution as the module is frequently reset. (IG 10.3.E, Resolution 3.a.).
ECDSA KeyGen (FIPS186-5) (A5375)	PCT	PCT	no specific duration	Before key generation request
ECDSA SigGen (FIPS186-5) (A5375)	KAT	CAST	no specific duration	The conditional self-tests are performed

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
				before the first use of an algorithm after every reset. This results in a periodically execution as the module is frequently reset. (IG 10.3.E, Resolution 3.a.).
ECDSA SigVer (FIPS186-5) (A5375)	KAT	CAST	no specific duration	The conditional self-tests are performed before the first use of an algorithm after every reset. This results in a periodically execution as the module is frequently reset. (IG 10.3.E, Resolution 3.a.).
HMAC-SHA2-256 (A5376)	KAT	CAST	no specific duration	The conditional self-tests are performed before the first use of an algorithm after every reset. This results in a periodically execution as the module is frequently reset. (IG 10.3.E, Resolution 3.a.).
RSA Decryption Primitive Sp800-56Br2 (A5374)	KAT	CAST	no specific duration	The conditional self-tests are performed before the first use of an algorithm after every reset. This results in a periodically execution as the

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
				module is frequently reset. (IG 10.3.E, Resolution 3.a.).
RSA KeyGen (FIPS186-5) (A5373)	PCT	PCT	no specific duration	Before key generation request
RSA SigGen (FIPS186-5) (A5374)	KAT	CAST	no specific duration	The conditional self-tests are performed before the first use of an algorithm after every reset. This results in a periodically execution as the module is frequently reset. (IG 10.3.E, Resolution 3.a.).
RSA SigVer (FIPS186-5) (A5374)	KAT	CAST	no specific duration	The conditional self-tests are performed before the first use of an algorithm after every reset. This results in a periodically execution as the module is frequently reset. (IG 10.3.E, Resolution 3.a.).
RSA KeyGen CRT	-	PCT	no specific duration	Before key generation request
SHA-1 (A5380)	KAT	CAST	no specific duration	The conditional self-tests are performed before the first use of an algorithm after every reset. This results in a periodically execution as the

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
				module is frequently reset. (IG 10.3.E, Resolution 3.a.).
SHA2-256 (A5381)	KAT	CAST	no specific duration	The conditional self-tests are performed before the first use of an algorithm after every reset. This results in a periodically execution as the module is frequently reset. (IG 10.3.E, Resolution 3.a.).
SHA3-256 (A5382)	KAT	CAST	no specific duration	The conditional self-tests are performed before the first use of an algorithm after every reset. This results in a periodically execution as the module is frequently reset. (IG 10.3.E, Resolution 3.a.).
SHA2-512 (A5381)	KAT	CAST	no specific duration	The conditional self-tests are performed before the first use of an algorithm after every reset. This results in a periodically execution as the module is frequently reset. (IG 10.3.E, Resolution 3.a.).
SHA2-256 (A5380)	KAT	CAST	no specific duration	The conditional self-tests are

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
				performed before the first use of an algorithm after every reset. This results in a periodically execution as the module is frequently reset. (IG 10.3.E, Resolution 3.a.).
SHA2-512 (A5380)	KAT	CAST	no specific duration	The conditional self-tests are performed before the first use of an algorithm after every reset. This results in a periodically execution as the module is frequently reset. (IG 10.3.E, Resolution 3.a.).

Table 26: Conditional Periodic Information

10.4 Error States

If any self-test fails or a fault attack is detected, the first indication is that the card mutes, i.e. all data output via the data output interface are inhibited and no further communication is possible. The module does not perform any command execution or cryptographic operations in this state. The module has to be reset and the ATR shows the error status (see Section 2.4). After that the module enters one of the following error states listed in below table.

Name	Description	Conditions	Recovery Method	Indicator
ES1	Persistent error state (SELF-TEST ERROR)	Entered when the module fails a Firmware integrity test Self-test (KAT/PCT) 2 times SP800-90B Health Test in a row Any fault detection occurs	None, the module is not operative anymore.	Error code in the ATR. Any further command sent to the module is blocked and will return the status word 0x6666.

Name	Description	Conditions	Recovery Method	Indicator
ES2	Intermediate error state (INTERMEDIATE TEST ERROR)	Entered when the module fails a SP800-90B Health Test	After reset the module is ready for use again. If the health test succeeds the next time, the error code in the ATR is cleared. If the heath test fails 2 times in a row the persistent error state ES1 is entered,	Error code in the ATR.

Table 27: Error States

10.5 Operator Initiation of Self-Tests

The Module allows the operator to initiate power-up self-tests by power cycling or resetting the Module.

11 Life-Cycle Assurance

11.1 Installation, Initialization, and Startup Procedures

No specific procedures have to be applied for secure installation, initialization, startup, and operation of the Module.

Installation and Initialization:
There are no specific rules to be performed in order to securely install, initialize, and start up the cryptographic module in the FIPS 140-3 Approved mode of operation.

Delivery:
The Module is delivered in approved mode and it starts-up in approved mode.
Authorized operators of the Module are the Crypto Officer and the User. Authentication mechanisms for those operators are described in section 4.1 Authentication Methods Authentication Methods.

All security mechanisms of the Module are active after production such that the Module protects itself against attacks and unauthorized access to security functions. Therefore, no additional security measures have to be applied for the delivery to the Crypto Officer or User.

The module must be delivered securely, with tracking and protection against theft, by contracted logistic partners to the authorized operator. The recipient must check and confirm correct reception.

11.2 Administrator Guidance

The Crypto Officer (Administrator) guidance is covered by the submission document Sm@rtCafé Expert 8.1 Reference Manual [REF_MAN] that will be sent to the Administrator.

11.3 Non-Administrator Guidance

The User (non-administrator) guidance is covered by the submission document Sm@rtCafé Expert 8.1 Reference Manual [REF_MAN] that will be sent to the User.

11.4 Design and Rules

There are no specific overall security design and the rules of operation for the Module.

Rules of Operation

1. The Module provides two distinct operator roles: User and Cryptographic Officer.
2. The Module provides identity-based authentication.
3. The Module clears previous authentications on power cycle.
4. An operator does not have access to any cryptographic services prior to assuming an authorized role.
5. The Module allows the operator to initiate power-up self-tests by power cycling or resetting the Module.
6. All self-tests do not require any operator action.
7. Data output is inhibited during key generation, self-tests, zeroization, and error states.
8. Status information does not contain CSPs or sensitive data that if misused could lead to a compromise of the Module.
9. There are no restrictions on which keys or SSPs are zeroized by the zeroization service.
10. The Module does not support concurrent operators.
11. The Module does not support a maintenance interface or role.
12. The Module does not support manual SSP establishment method.
13. The Module does not have any proprietary external input/output devices used for entry/output of data.
14. The Module does not enter or output plaintext CSPs.
15. The Module stores CSPs in plaintext.
16. The Module does not output intermediate key values.
17. The Module does not provide bypass services for ports/interfaces.

11.6 End of Life

The term end-of-life of the module describes the secure cleanup of the module in a way that it cannot be used any longer. There are 2 separate ways a module can enter the end-of-life state.

1. The Crypto officer decides that the module needs to be destroyed. In order to do that, the CO has to authenticate to the module (AM1) and issue a SET STATUS (TERMINATE). This will use

the zeroization method Z2, which destroys all sensitive data on the module (see section SSP Zeroization).

2. The module detects multiple attacks. After a predefined number of attacks the card will terminate the card by using the zeroization method Z2 (see section SSP Zeroization).

The module shall be returned to the CO for secure physical destruction e.g. by shredding or cutting the chip in small pieces.

12 Mitigation of Other Attacks

The Module implements the following mitigation methods against other attacks.

12.1 Attack List

The Module implement the following mitigation methods against other attacks.

Attack	Method	Method Effectiveness description
Power Analysis	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.	The countermeasure implemented in hardware were already tested in an independent Common Criteria evaluation of the chip platform (ANSSI-CC-2022/21) with the highest vulnerability assessment possible (AVA_VAN.5). The counter-measures implemented in the OS software were tested in the G+D SPA/DPA/DFA/LFI test laboratories with state-of-the-art equipment and methods that revealed no vulnerabilities for the cryptographic algorithms of the module. All requirements of the hardware security guidance [AN_SECU] were implemented.
Electromagnetic analysis		
Timing analysis		

Table 28 – Attack List

The Module detects physical tampering with sensors for operating voltage, clock frequency, temperature and electromagnetic radiation. It is resistant to physical tampering. If the COS detects with the above mentioned sensors that it is not supplied within the specified limits, a security reset is initiated and the Module is not operable until the supply is back in the specified limits. The design of the hardware protects it against analyzing and physical tampering.

This Module provides resistance to side channel attacks and enforces protection of its secret data during cryptographic operations, comparison operations and key generation against state-of-the-art attacks that are based on external observable physical phenomena of the Module.
The Module hides information about IC power consumptions and command execution time such that no confidential information can be derived from this data.

The card is muted upon detection of a potential security violation such that the Module preserves a secure state.

References and Definitions

The following standards are referred to in this Security Policy.

Table 29 – References

Abbreviation	Full Specification Name
[FIPS140-3]	*Security Requirements for Cryptographic Modules*, March 22, 2019
[ISO19790]	*International Standard, ISO/IEC 19790, Information technology — Security techniques — Test requirements for cryptographic modules, Second edition, 2012-08-15, corrected version: 2015-12-15*
[ISO24759]	*International Standard, ISO/IEC 24759, Information technology — Security techniques — Test requirements for cryptographic modules, Third edition, 2017-03*
[IG]	*Implementation Guidance for FIPS PUB 140-3 and the Cryptographic Module Validation Program, March 26, 2024*
[108]	*NIST Special Publication 800-108, NIST SP 800-108r1, Recommendation for Key Derivation Using Pseudorandom Functions, August 2022*
[131A]	*NIST Special Publication 800-131A, for Transitioning the Use of Cryptographic Algorithms and Key Lengths, Revision 2, March 2019*
[132]	*NIST Special Publication 800-132, Recommendation for Password-Based Key Derivation, Part 1: Storage Applications, December 2010*
[133]	*NIST Special Publication 800-133, Recommendation for Cryptographic Key Generation, Revision 2, June 2020*
[135]	*NIST Special Publication 800-135, Recommendation for Existing Application-Specific Key Derivation Functions, Revision 1, December 2011.*
[186-4]	*FIPS PUB 186-4, FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION, Digital Signature Standard (DSS), July, 2013.*
[186-5]	*FIPS PUB 186-5, FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION, Digital Signature Standard (DSS), February 3, 2023.*
[197]	*FIPS PUB 197, FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION, Advanced Encryption Standard (AES), November 26, 2001, Updated May 9, 2023*
[198]	*FIPS PUB 198, FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION, The Keyed-Hash Message Authentication Code (HMAC), July, 2008*
[180]	*FIPS PUB 180-4, FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION, Secure Hash Standard, August, 2015*
[202]	*FIPS PUB 202, FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION, SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions, August 2015*
[38A]	*NIST Special Publication 800-38A, National Institute of Standards and Technology, Recommendation for Block Cipher Modes of Operation, Methods and Techniques, December 2001*

Abbreviation	Full Specification Name
[38B]	*NIST Special Publication 800-38B, National Institute of Standards and Technology, Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication, May 2005*
[38C]	*NIST Special Publication 800-38C, National Institute of Standards and Technology, Recommendation for Block Cipher Modes of Operation: The CCM Mode for Authentication and Confidentiality, May 2004 (errata update 07-20-2007)*
[38D]	*NIST Special Publication 800-38D, National Institute of Standards and Technology, Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC, November 2007*
[38E]	*NIST Special Publication 800-38E, National Institute of Standards and Technology, Recommendation for Block Cipher Modes of Operation: The XTS-AES Mode for Confidentiality on Storage Devices, January 2010*
[38F]	*NIST Special Publication 800-38F, National Institute of Standards and Technology, Recommendation for Block Cipher Modes of Operation: Methods for Key Wrapping, December 2012*
[56Ar3]	*NIST Special Publication 800-56A Revision 3, National Institute of Standards and Technology, Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography, April 2018*
[56Br2]	*NIST Special Publication 800-56B Revision 2, National Institute of Standards and Technology, Recommendation for Pair-Wise Key Establishment Schemes Using Finite Field Cryptography, March 2019*
[56Cr2]	*NIST Special Publication 800-56C Revision 2, National Institute of Standards and Technology, Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography, August 2020*
[67]	*NIST Special Publication 800-67 Revision 2, National Institute of Standards and Technology, Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher, May 2004*
[90A]	*NIST Special Publication 800-90A Revision 1, National Institute of Standards and Technology, Recommendation for Random Number Generation Using Deterministic Random Bit Generators, June 2015.*
[90B]	*NIST Special Publication 800-90B, National Institute of Standards and Technology, Recommendation for the Entropy Sources Used for Random Bit Generation, January 2018.*
[GPCS]	*GlobalPlatform Technology Card Specification, Version 2.3.1, Public Release, March 2018*
[GP Amd D]	*GlobalPlatform Card Technology, Secure Channel Protocol '03', Card Specification v2.2 – Amendment D, Version 1.1.1, July 2014, GPC_SPE_014*
[GP Amd E]	*GlobalPlatform Card Technology, Security Upgrade for Card Content Management Card Specification v2.3 – Amendment E, Version 1.1, October 2016*
[JCRE]	*Java Card Platform Runtime Environment Specification, Classic Edition v3.1, January 2019, Oracle*

Abbreviation	Full Specification Name
[JCVM]	*Java Card Platform Virtual Machine Specification, Classic Edition, v3.1, January 2019, Oracle*
[JCAPI]	*Java Card Platform Application Programming Interface, Classic Edition, v3.1.0, Oracle*
[PKCS#1]	*PKCS#1 v2.1: RSA Cryptography Standard, RSA Laboratories, June 14, 2002*
[AN_SECU]	*AN_SECU_ST31N Security Guidance of the ST31N secure MCU platform, Rev 1 – September 2021*
[DS_ST31N]	*ST31N platform ST31N600 Datasheet, DS_ST31N – Rev 2 – July 2022*
[REF_MAN]	*Sm@rtCafé Expert 8.1 Reference Manual, Giesecke+Devrient ePayments GmbH*

Table 30 – Acronyms and Definitions

Acronym	Definition
APT	Adaptative Proportion Test
COS	Card Operating System
KAT	Known Answer Test
RCT	Repetition Count Test
SSP	Sensitive Security Parameter
PCT	Pairwise consistency test
ATR	Answer to reset