gemalto

security to be free

IDCore 30
FIPS 140-2 Cryptographic Module Security Policy

Table of Contents

References....4
Acronyms and definitions....5
1 Introduction....6
2 Cryptographic Module Ports and Interfaces....7
2.1 Hardware and Physical Cryptographic Boundary....7
2.1.1 PIN assignments and contact dimensions....7
3 Cryptographic Module Specification....9
3.1 Firmware and Logical Cryptographic Boundary....9
3.2 Versions and mode of operation....10
3.3 Cryptographic functionality....14
4 Platform Critical Security Parameters....16
4.1 Platform Public key....16
4.2 Demonstration Applet Critical Security Parameters....17
4.3 Demonstration Applet Public Keys....17
5 Roles, authentication and services....18
5.1 Secure Channel Protocol (SCP) Authentication....19
5.2 USR Authentication....20
5.3 Services....20
6 Finite State Model....23
7 Physical security policy....23
8 Operational Environment....23
9 Electromagnetic interference and compatibility (EMI/EMC)....23
10 Self-test....24
10.1 Power-on self-test....24
10.2 Conditional self-tests....24
11 Design Assurance....25
11.1 Configuration Management....25
11.2 Delivery and Operation....25
11.3 Guidance Documents....25
11.4 Language level....25
12 Mitigation of other attacks policy....25
13 Security Rules and Guidance....26

© Copyright Gemalto 2016. May be reproduced only in its entirety [without revision].

Table of Tables

Table 1 – References 5
Table 2 – Acronyms and Definitions 5
Table 3 – Security Level of Security Requirements 6
Table 4 - Contact plate pad list – Interfaces 8
Table 5 - Voltage and frequency ranges 8
Table 6 –Versions and Mode of Operations Indicators 13
Table 7 – FIPS Approved Cryptographic Functions 14
Table 8 – Non-FIPS Approved But Allowed Cryptographic Functions 14
Table 9 – Non-Approved Functions (Disallowed per NIST SP 800-131A Transitions) 15
Table 9 - Platform Critical Security Parameters 16
Table 10 – Platform Public Keys 16
Table 11 – Demonstration Applet Critical Security Parameters 17
Table 12 – Demonstration Applet Public Keys 17
Table 13 - Role description 18
Table 14 - Unauthenticated Services and CSP Usage 20
Table 15 – Authenticated Card Manager Services and CSP Usage 21
Table 16 – Demonstration Applet Services and CSP Usage 22
Table 17 – Power-On Self-Test 24

Table of Figures

Figure 1- Module Physical Form 7
Figure 2 – Contact plate example – Contact physical interface 7
Figure 3 - Module Block Diagram 9

© Copyright Gemalto 2016. May be reproduced only in its entirety [without revision].

References

Acronym	Full Specification Name
[FIPS140-2]	NIST, *Security Requirements for Cryptographic Modules*, May 25, 2001 CHANGE NOTICES (12-03-2002)
[GlobalPlatform]	*GlobalPlatform Consortium: GlobalPlatform Card Specification 2.1.1,* March 2003, http://www.globalplatform.org *GlobalPlatform Consortium: GlobalPlatform Card Specification 2.1.1* Amendment A, March 2004 *GlobalPlatform Consortium: GlobalPlatform Card Specification 2.2* Amendment D, Sept 2009
[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*
[JavaCard]	*Java Card 2.2.2 Runtime Environment (JCRE) Specification* *Java Card 2.2.2 Virtual Machine (JCVM) Specification* *Java Card 2.2.2 Application Programming Interface* *Java Card 3.0.1 Application Programming Interface [only for algos ECDSA, SHA2]* Published by Sun Microsystems, March 2006
[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.
[FIPS 197]	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 186-2]	NIST, *Digital Signature Standard (DSS)*, FIPS Publication 186-2, January, 2000 with Change Notice 1. (DSA, RSA and ECDSA)
[SP 800-56A]	NIST Special Publication 800-56A, *Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography*, March 2007
[FIPS 180-3]	NIST, *Secure Hash Standard*, FIPS Publication 180-3, October 2008
[AESKeyWrap]	NIST, *AES Key Wrap Specification*, 16 November 2001. This document defines symmetric key wrapping, Use of 2-Key TDES in lieu of AES is described in [IG] D.2.
[IG]	NIST, *Implementation Guidance for FIPS PUB 140-2 and the Cryptographic Module Validation Program,* last updated 29 June 2012.

© Copyright Gemalto 2016. May be reproduced only in its entirety [without revision].

Table 1 – References

Acronyms and definitions

Acronym	Definition
GP	Global Platform
MMU	Memory Management Unit
OP	Open Platform
RMI	Remote Method Invocation

Table 2 – Acronyms and Definitions

© Copyright Gemalto 2016. May be reproduced only in its entirety [without revision].

1 Introduction

This document defines the Security Policy for the Gemalto IDCore 30 module herein denoted as Cryptographic Module. The Cryptographic Module or CM, validated to FIPS 140-2 overall Level 3, is a single chip embodiment, “contact-only” secure controller module implementing the Global Platform 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 CM is a limited operational environment under the FIPS 140-2 definitions. The CM includes a firmware load service 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 loading of non-validated firmware within the validated cryptographic module invalidates the module’s validation.

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

Security Requirement	**Security Level**
Cryptographic Module Specification	3
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

The CM implementation is compliant with:

- [ISO 7816] Parts 1-4
- [JavaCard]
- [GlobalPlatform]

© Copyright Gemalto 2016. May be reproduced only in its entirety [without revision].

2 Cryptographic Module Ports and Interfaces

2.1 Hardware and Physical Cryptographic Boundary

The CM is designed to be embedded into plastic card bodies, with a contact plate connection. The physical form of the CM is depicted in Figure 1 (to scale), with the cryptographic boundary indicated by the red outline. The module, intended for use in a plastic card body, is a single integrated circuit die wire-bonded to a frame connected to a contact plate, enclosed in epoxy. The cryptographic boundary is the contact plate surface on the top side, and the surface of the epoxy on the bottom side. The Module relies on [ISO7816] card readers as input/output devices.

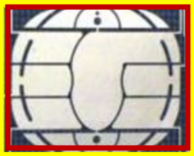
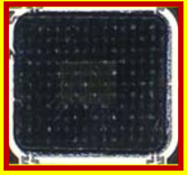
WORLD RLC module	
 Top View – Contact Plate	 Bottom View - Epoxy

Figure 1- Module Physical Form

2.1.1 PIN assignments and contact dimensions

The CM conforms to the ISO 7816-1 and ISO 7816-2 specifications for physical characteristics, dimensions and contact location. The contact plate pads are assigned as shown below, with the corresponding interfaces given in Table 4.

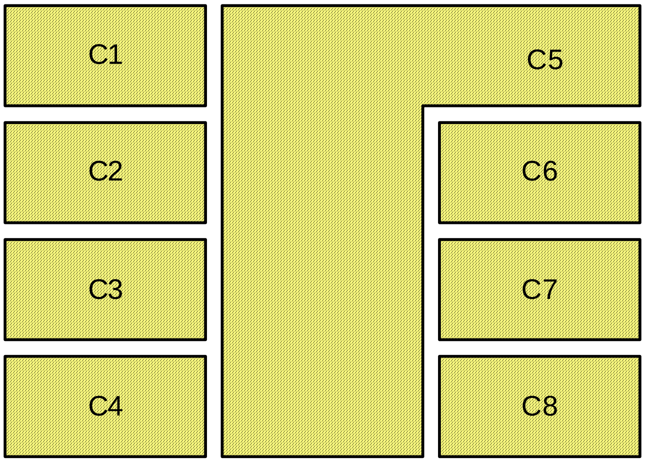


Figure 2 – Contact plate example – Contact physical interface

Contact No.	Logical interface type	Contact No.	Logical interface type
C1	VCC (Supply voltage)	C5	GND (Ground)
C2	RST (Reset signal) control In	C6	Not connected
C3	CLK (Clock signal) control In	C7	I/O : Data in, data out, control in, status out
C4	Not connected	C8	Not connected

Table 4 - Contact plate pad list – Interfaces

The CM conforms to the ISO 7816-3 specifications for electrical signals and transmission protocols, with voltage and frequency operating ranges as shown in Table 5.

Conditions	Range
Voltage	1.62 V and 5.5 V
Frequency	1MHz to 10MHz

Table 5 - Voltage and frequency ranges

© Copyright Gemalto 2016. May be reproduced only in its entirety [without revision].

3 Cryptographic Module Specification

3.1 Firmware and Logical Cryptographic Boundary

Figure 2 depicts the Module operational environment and applets.

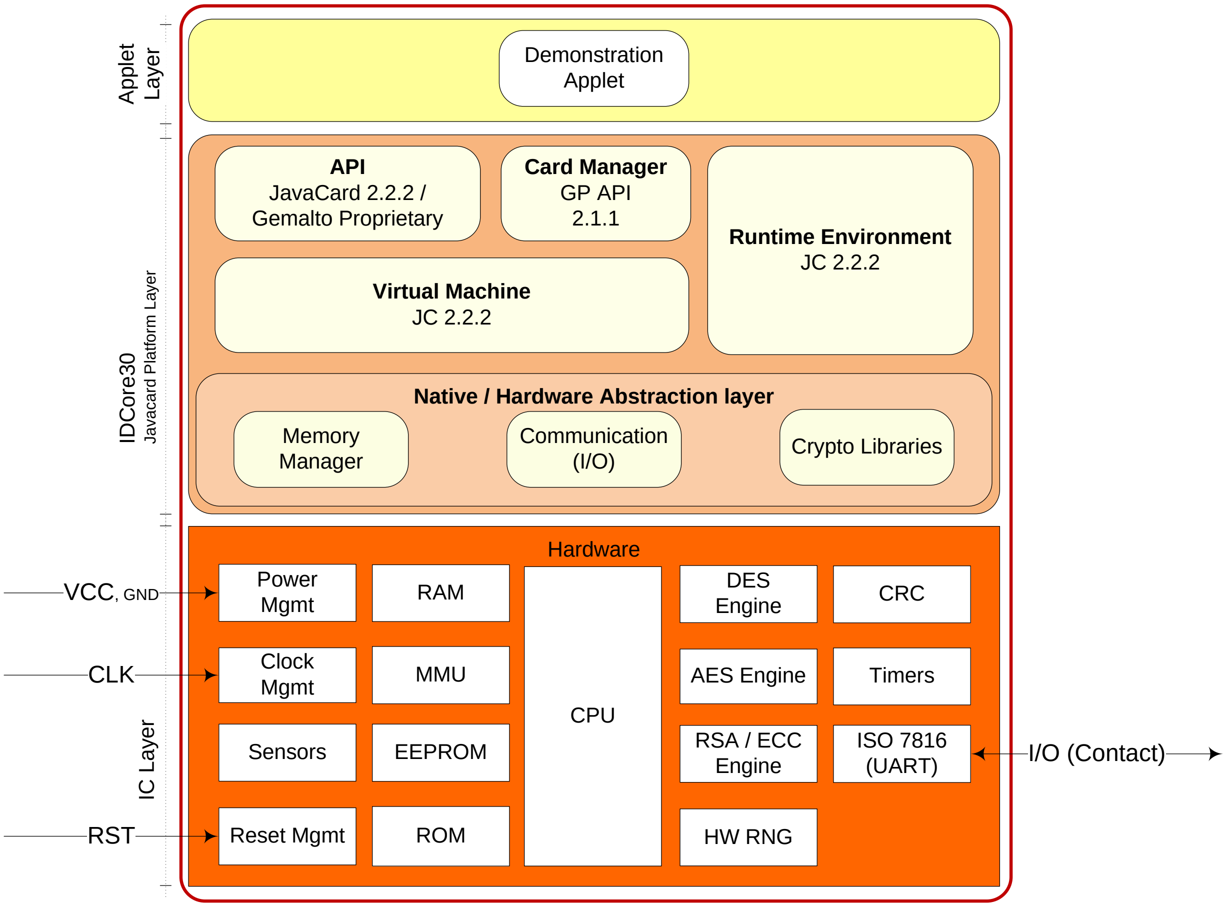


Figure 3 - Module Block Diagram

The CM supports [ISO7816] T=0 and T=1 communication protocols.

The CM provides an execution sandbox for Applets, performing the requested services as described in this security policy. Applets access module functionality via internal API entry points that are not exposed to external entities. External devices have access to CM services by sending APDU commands.

The CM inhibits all data output via the data output interface while the module is in error state and during self-tests.

© Copyright Gemalto 2016. May be reproduced only in its entirety [without revision].

The *JavaCard API* is an internal interface, available to applets. Only applet services are available at the card edge (the interfaces that cross the cryptographic boundary).

The *Javacard Runtime Environment* implements the dispatcher, registry, loader, logical channel and RMI functionalities.

The *Virtual Machine* implements the byte code interpreter, firewall, exception management and byte code optimizer functionalities.

The *Card Manager* is the card administration entity – allowing authorized users to manage the card content, keys, and life cycle states.

The *Memory Manager* implements services such as memory access, allocation, deletion, garbage collector.

The *Communication* handler deals with the implementation of ATR, PSS, T=0 and T=1 protocols.

The *Cryptography Libraries* implement the algorithms listed in section 2.

3.2 Versions and mode of operation

Hardware: SLE78CFX3009P
Firmware: IDCore 30 Build 1.17, Demonstration Applet version V1.0

The Demonstration Applet AID (application identifier) value is 464950535F546573744170706C657401. It can be retrieved using the GET STATUS command - available after a successful Card Manager authentication – which provides the AIDs of all the packages loaded in the card.

Field	CLA	INS	P1-P2 (Tag)	Lc-Le	Purpose
Value	**80**	**F2**	**20-00**	**02-00**	Get AID list – first command
Value	**80**	**F2**	**20-01**	**02-00**	Get AID list, continued (to get the end of the list, if previous command returned '6310 SW)

The CM is always in the approved mode of operation. To verify that a CM is in the approved mode of operation, select the Card Manager and send the GET DATA commands shown below:

Field	CLA	INS	P1-P2 (Tag)	Le (Expected response length)	Purpose
Value	**00**	**CA**	**9F-7F**	**2A**	Get CPLC data
			01-03	**1D**	Identification information (proprietary tag)

© Copyright Gemalto 2016. May be reproduced only in its entirety [without revision].

The CM responds with the following information:

G259 Mask - CPLC data (tag 9F7F)			
Byte	**Description**	**Value**	**Value meaning**
1-2	IC fabricator	**4090h**	Infineon
3-4	IC type	**7871h**	SLE78CFX3009P
5-6	Operating system identifier	**1291h**	Gemalto
7-8	Operating system release date (YDDD) – Y=Year, DDD=Day in the year	**2121h**	2012 – 30th of April
9-10	Operating system release level	**0100h**	V1.0
11-12	IC fabrication date	xxxxh	Filled in during IC manufacturing
13-16	IC serial number	xxxxxxxxh	Filled in during IC manufacturing
17-18	IC batch identifier	xxxxh	Filled in during IC manufacturing
19-20	IC module fabricator	xxxxh	Filled in during module manufacturing
21-22	IC module packaging date	xxxxh	Filled in during module manufacturing
23-24	ICC manufacturer	xxxxh	Filled in during module embedding
25-26	IC embedding date	xxxxh	Filled in during module embedding
27-28	IC pre-personalizer	xxxxh	Filled in during smartcard preperso
29-30	IC pre-personalization date	xxxxh	Filled in during smartcard preperso
31-34	IC pre-personalization equipment identifier	xxxxxxxxh	Filled in during smartcard preperso
35-36	IC personalizer	xxxxh	Filled in during smartcard personalization
37-38	IC personalization date	xxxxh	Filled in during smartcard personalization
39-42	IC personalization equipment identifier	xxxxxxxxh	Filled in during smartcard personalization

© Copyright Gemalto 2016. May be reproduced only in its entirety [without revision].

G259 Mask - Identification data (tag 0103)			
Byte	**Description**	**Value**	**Value meaning**
1	Gemalto Family Name	**B0h**	Javacard
2	Gemalto OS Name	**84h**	IDCore family (OA)
3	Gemalto Mask Number	**41h**	G259
4	Gemalto Product Name	**3Dh**	IDCore 30
5	Gemalto Flow Version	**XYh**	**X** is the type of SCP: ▪ 1xh for SCP0105 flows ▪ 2xh for SCP0300 flows ▪ 3xh for SCP0310 flows **Y**: is the version of the flow (x=1 for version 01). <u>For instance:</u> **11h** = SCP0105 - flow 01 (version 01) **21h** = SCP0300 - flow 01 (version 01) Carriage Return **31h** = SCP0310 - flow 01 (version 01)
6	Gemalto Filter Set	**00h**	▪ Major nibble: filter family = 00h ▪ Lower nibble: version of the filter = 00h
7-8	Chip Manufacturer	**4090h**	Infineon
9-10	Chip Version	**7871h**	SLE78CFX3009P
11-12	FIPS config	**8x00h**	MSByte: b8 : 1 = **conformity to FIPS certificate** b7 : 0 = RFU b6 : 0 = RFU b5 : 0 = RFU b4 : 1 = ECC supported b3 : 1 = RSA CRT supported b2 : 1 = RSA STD supported b1 : 1 = AES supported LSByte: b8 .. b5 : 0 = non applicable b4 : 0 = non applicable (ECC in contactless) b3 : 0 = non applicable (RSA CRT in contactless) b2 : 0 = non applicable (RSA STD in contactless) b1 : 0 = non applicable (AES in contactless)

© Copyright Gemalto 2016. May be reproduced only in its entirety [without revision].

			For instance: **8F 00** = FIPS enable (CT only)–AES-RSA CRT/STD-ECC **(Full FIPS)** **8D 00** = FIPS enable (CT only)–AES-RSA CRT-ECC **(FIPS PK CRT) *** **85 00** = FIPS enable (CT only)–AES-RSA CRT **(FIPS RSA CRT)** **00 00** = FIPS disable (CT only)–No FIPS mode **(No FIPS)** **(* default configuration)**
13-18	RFU	**xx..xxh**	-
19-29	RFU	**xx..xxh**	-

Table 6 –Versions and Mode of Operations Indicators

© Copyright Gemalto 2016. May be reproduced only in its entirety [without revision].

3.3 Cryptographic functionality

The Module operating system implements the FIPS Approved and Non-FIPS Approved but Allowed cryptographic functions listed in Tables 7 and 8 below.

Algorithm	Description	Cert #
TDES	[SP 800-67] Triple Data Encryption Algorithm. The Module supports the 3-Key options; CBC and ECB modes. Note that the Module does not support a mechanism that would allow collection of plaintext / ciphertext pairs aside from authentication, limited in use by a counter.	1413
TDES MAC	[FIPS 113] TDES Message Authentication Code. Vendor affirmed, based on validated TDES.	1413
AES	[FIPS 197] Advanced Encryption Standard algorithm. The Module supports 128-, 192- and 256-bit key lengths with ECB and CBC modes.	2261
AES CMAC	AES CMAC The Module supports 128-, 192- and 256-bit key lengths.	2261
RSA	[[FIPS 186-3] RSA signature generation and verification. The Module follows PKCS#1 and is CAVP validated: Signature generation uses 2048 bit key length with SHA-224 to SHA-512. Signature verification uses 1024 or 2048 bit key length with SHA-1 to SHA-512.	1158
RSA CRT	[FIPS 186-3] RSA signature generation and verification. The Module follows PKCS#1 and is CAVP validated: Signature generation uses 2048 bit key length with SHA-224 to SHA-512. Signature verification uses 1024 or 2048 bit key length with SHA-1 to SHA-512.	1163
ECDSA	[FIPS 186-3] Elliptic Curve Digital Signature Algorithm : Signature generation uses curves P-224, P-256, P-384 and P-521 with SHA-224 to SHA-512. Signature verification uses curves P-192, P-224, P-256, P-384 and P-521 with SHA-1 to SHA-512.	363
ECC-CDH	[SP 800-56A] The Section 5.7.1.2 ECC CDH Primitive. The Module is CAVP validated for the NIST defined P-224, P-256, P-384 and P-521 curves.	41
SHA-1, SHA-224, SHA-256, SHA-384, SHA-512	[FIPS 180-4] Secure Hash Standard compliant one-way (hash) algorithms.	1946

Table 7 – FIPS Approved Cryptographic Functions

Algorithm	Description
EC Diffie-Hellman	SP 800-56A; non-compliant - NIST defined P-224, P-256, P-384 and P-521 curves.

Table 8 – Non-FIPS Approved But Allowed Cryptographic Functions

The CM includes an uncallable DES implementation. This algorithm is not used and no security claims are made for its presence in the Module.

© Copyright Gemalto 2016. May be reproduced only in its entirety [without revision].

The functions in Table 9 are Now Disallowed and cannot be used in the Approved mode.

FUNCTION	DETAILS
Triple-DES	2-key ECB mode in encryption (*)
	2-key CBC mode in encryption (*)
Triple-DES MAC	2-key ECB and CBC modes for generation (*)
RSA	Key generation following X9.31 (*)
	Signature generation following PKCS#1 using 1024 bit key length with any SHA size or 2048 bit key length with SHA-1 hashing (*)
PRNG	Pseudo Random Number Generation (*)
ECDSA	Signature Generation (*) following FIPS186-3 using P-192 with any SHA size or P-224, P-256, P-384, P-521 with SHA-1
	Key pair generation (*) following FIPS186-3
ECC-CDH	EC secret value derivation primitive, Diffie-Hellman version: P-192 (*)

Table 9 - Non-Approved Functions (Disallowed per NIST SP 800-131A Transitions)

Note (*): Services/CSPs using disallowed functions are not allowed in the Approved mode.

© Copyright Gemalto 2016. May be reproduced only in its entirety [without revision].

4 Platform Critical Security Parameters

All CSPs used by the CM are described in this section. All usage of these CSPs by the CM are described in the services detailed in Section 5.

Note (*): Services/CSPs using disallowed functions are not allowed in the Approved mode.

Key	Description / Usage
OS-RNG-SEED-KEY	AES-128 random key loaded into the card during pre-personalization of the card used as a seed key for the [ANS X9.31] RNG implementation (*).
OS-RNG-STATE	16-byte random value and 16-byte counter value used in the [ANS X9.31] RNG implementation (*).
OS-GLOBALPIN	6 to 16 byte Global PIN value managed by the ISD. Character space is not restricted by the module.
OS-MKDK	2-Key TDES (SCP01/02) (*) or AES-128/192/256 (SCP03) key used to encrypt OS-GLOBALPIN value
SD-KENC	2-Key TDES (SCP01/02) (*) or AES-128/192/256 (SCP03) Master key used by the CO role to generate SD-SENC
SD-KMAC	2-Key TDES (SCP01/02) (*) or AES-128/192/256 (SCP03) Master key used by the CO role operator to generate SD-SMAC
SD-KDEK	2-Key TDES (SCP01/02) (*) or AES-128/192/256 (SCP03) Sensitive data decryption key used by the USR role to decrypt CSPs for SCP01/03, and used to generate SD-SDEK in case of SCP02.
SD-SENC	2-Key TDES (SCP01/02) (*) or AES-128/192/256 (SCP03) Session encryption key used by the CO role to encrypt / decrypt secure channel data.
SD-SMAC	2-Key TDES (SCP01/02) (*) or AES-128/192/256 (SCP03) Session MAC key used by the CO role to verify inbound secure channel data integrity.
SD-SDEK	2-Key TDES (SCP01) (*) or AES-128/192/256 (SCP03) Session DEK key used by the CO role to decrypt CSPs.
DAP-SYM	2-Key TDES (SCP01/02) (*) or AES-128/192/256 (SCP03) key optionally loaded in the field and used to verify the signature of packages loaded into the Module.

Table 10 - Platform Critical Security Parameters

Keys with the “SD-“ prefix pertain to a Global Platform Security Domain key set. The module supports the Issuer Security Domain at minimum, and can be configured to support Supplemental Security Domains.

4.1 Platform Public key

Key	Description / Usage
DAP-SVK	RSA 1024 Global Platform Data Authentication Public Key. Optionally used to verify the signature of packages loaded into the Module.

Table 11 – Platform Public Keys

© Copyright Gemalto 2016. May be reproduced only in its entirety [without revision].

4.2 Demonstration Applet Critical Security Parameters

Note (*): Services/CSPs using disallowed functions are not allowed in the Approved mode.

Key	Description / Usage
DSC-AES	AES 128/192/256 key used by Demonstrate Symmetric Cipher
DSC-TDEA	2-Key (*) or 3-Key TDES key used by Demonstrate Symmetric Cipher
DSS-TDEA	2-Key (*) or 3-Key TDES key used by Demonstrate Symmetric Signature (MAC generation and verify)
DAS-RSA	1024 (*)-, 2048- RSA private key used by Demonstrate Asymmetric Signature (signature generation and verify)
DAS-ECDSA	P-192 (*), P-224, P-256, P-384, P-521 ECDSA private key used by Demonstrate Asymmetric Signature (signature generation and verify)
ECDH-ECC	P-192 (*), P-224, P-256, P-384, P-521 ECDSA private key used by Demonstrate ECC CDH (shared secret primitive)
DKG-RSA	1024(*)-, 2048- RSA private key generated by Demonstrate Asymmetric Key Generation
DKG-ECDSA	P-192 (*), P-224, P-256, P-384, P-521 ECDSA private key generated by Demonstrate Asymmetric Key Generation
DMK	Demonstration master key, 2-Key TDES key (*) used to encrypt or decrypt CSPs exported out of or imported into the module for use by the demonstration applet.

Table 12 – Demonstration Applet Critical Security Parameters

4.3 Demonstration Applet Public Keys

Key	Description / Usage
DAS-RSA-SVK	1024-, 2048- RSA public key used by Demonstrate Asymmetric Signature (signature generation and verify)
DAS-ECDSA-SVK	P-192, P-224, P-256, P-384, P-521 ECDSA public key used by Demonstrate Asymmetric Signature (signature generation and verify)
DKG-RSA-PUB	1024-, 2048- RSA public key generated by Demonstrate Asymmetric Key Generation
DKG-ECDSA-PUB	P-192, P-224, P-256, P-384, P-521 ECC public key generated by Demonstrate Asymmetric Key Generation
DKG-ECDH-PUB	P-192, P-224, P-256, P-384, P-521 ECC public key entered into the module for EC Diffie-Hellman demonstration.

Table 13 – Demonstration Applet Public Keys

© Copyright Gemalto 2016. May be reproduced only in its entirety [without revision].

5 Roles, authentication and services

Table 14 lists all operator roles supported by the Module. This Module does not support a maintenance role. The Module clears previous authentications on power cycle. The Module supports GP logical channels, allowing multiple concurrent operators. Authentication of each operator and their access to roles and services is as described in this section, independent of logical channel usage. Only one operator at a time is permitted on a channel. Applet deselection (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-SDEK), is stored encrypted (by OS-MKDK) and is only accessible by authenticated services.

Role ID	Role Description
CO	(Cryptographic Officer) This role is responsible for card issuance and management of card data via the Card Manager applet. Authenticated using the SCP authentication method with SD-SENC.
USR	(User) This role has the privilege to use the cryptographic services provided by the demonstration applet. Authenticated using the GLOBAL PIN verification.

Table 14 - Role description

© Copyright Gemalto 2016. May be reproduced only in its entirety [without revision].

5.1 Secure Channel Protocol (SCP) Authentication

Note (*): Services/CSPs using disallowed functions are not allowed in the Approved mode.

The Open Platform Secure Channel Protocol authentication method is performed when the EXTERNAL AUTHENTICATE service is invoked after successful execution of the INITIALIZE UPDATE command. These two commands operate as described next.

The SD-KENC and SD-KMAC keys are used along with other information to derive the SD-SENC and SD-SMAC keys, respectively. The SD-SENC key is used to create a cryptogram; the external entity participating in the mutual authentication also creates this cryptogram. Each participant compares the received cryptogram to the calculated cryptogram and if this succeeds, the two participants are mutually authenticated (the external entity is authenticated to the Module in the COrole).

For SCP01 or SCP02 [SP 800-131A] Section A.1 provides the NIST rationale for 2-Key TDES security strength. 2-Key TDES is used for Global Platform secure channel operations, in which the Module derives session keys from the master keys and a handshake process, performs mutual authentication, and decrypts data for internal use only. The Module encrypts a total of one block (the mutual authentication cryptogram) over the life of the session encryption key; no decrypted data is output by the Module. The Module claims 112-bit security strength for its 2-Key TDES operations, as the meet-in-the-middle attack rationale described in [SP 800-131A] does not apply unless the attacker has access to encrypt/decrypt pairs.

2-Key TDES key (*) establishment provides 112 bits of security strength. The Module uses the SD-KDEK key to decrypt critical security parameters, and does not perform encryption with this key or output data decrypted with this key.

- The probability that a random attempt at authentication will succeed is 1/2^64 (based on block size)
- Based on the maximum count value of the failed authentication blocking mechanism, the probability that a random attempt will succeed over a one minute period is 255/2^64

For SCP03, AES-128, AES-192 or AES-256 keys are used instead of 2-key TDES. Operations are identical to those previously described. Therefore, AES key establishment provides a minimum of 128 bits of security strength. The Module uses the SD-KDEK key to decrypt critical security parameters, and does not perform encryption with this key or output data decrypted with this key.

The strength of GP mutual authentication relies on AES key length:

- $\left(\frac{1}{2^{128}}\right)$ for AES 16-byte-long keys;
- $\left(\frac{1}{2^{192}}\right)$ for AES 24-byte-long keys;
- $\left(\frac{1}{2^{256}}\right)$ for AES 32-byte-long keys;

Based on the maximum count value of the failed authentication blocking mechanism, the probability that a random attempt will succeed over a one minute period is 255/2^128.

© Copyright Gemalto 2016. May be reproduced only in its entirety [without revision].

5.2 USR Authentication

This authentication method compares a PIN value sent to the Module to the stored OS-GLOBALPIN values if the two values are equal, the operator is authenticated. This method is used in the Demonstration Applet services to authenticate to the USR role.

The module enforces OS-GLOBALPIN string length of 6 bytes minimum (16 bytes maximum), allowing all characters, so the strength of this authentication method is as follows:

- The probability that a random attempt at authentication will succeed is 1/256^6
- Based on a maximum count of 15 for consecutive failed service authentication attempts, the probability that a random attempt will succeed over a one minute period is 15/256^6

5.3 Services

Note (*): Services/CSPs using disallowed functions are not allowed in the Approved mode.

All services implemented by the Module are listed in the tables below. Each service description also describes all usage of CSPs by the service. The SD-SENC and SD-SMAC keys are used by every Card Manager service when a secure channel has been established, for decryption and MAC verification (packet integrity and authenticity), respectively. This is noted below as “Optionally uses SD-SENC, SD-SMAC (SCP)”. Unauthenticated commands listed below function whether or not a secure channel has been established.

Service	Description
Card Reset (Self-test)	Power cycle the Module by removing and reinserting it into the contact reader slot, or by reader assertion of the RST signal. The *Card Reset* service will invoke the power on self-tests described in Section 10. Moreover, on any card reset, the Module overwrites with zeros the RAM copy of, OS-RNG-STATE, SD-SENC, SD-SMAC and SD-SDEK. The Module can also write the values of all CSPs stored in EEPROM as a consequence of restoring values in the event of card tearing or a similar event. During the self-tests the module generates the RAM copy of OS-RNG-STATE and updates the EEPROM copy of OS-RNG-STATE.
EXTERNAL AUTHENTICATE (*)	Authenticates the operator and establishes a secure channel. Must be preceded by a successful INITIALIZE UPDATE. Uses SD-SENC and SD-SMAC.
INITIALIZE UPDATE (*)	Initializes the Secure Channel; to be followed by EXTERNAL AUTHENTICATE. Uses the SD-KENC, SD-KMAC and SD-KDEK master keys to generate the SD-SENC, SD-SMAC and SD-SDEK session keys, respectively.
GET DATA	Retrieve a single data object. Optionally uses SD-SENC, SD-SMAC (SCP).
MANAGE CHANNEL	Open and close supplementary logical channels. Optionally uses SD-SENC, SD-SMAC (SCP).
SELECT	Select an applet. Does not use CSPs.

Table 15 - Unauthenticated Services and CSP Usage

© Copyright Gemalto 2016. May be reproduced only in its entirety [without revision].

Service	Description	CO
DELETE	Delete an applet from EEPROM. This service is provided for the situation where an applet exists on the card, and does not impact platform CSPs. Optionally uses SD-SENC, SD-SMAC (SCP).	X
GET STATUS	Retrieve information about the card. Optionally uses SD-SENC, SD-SMAC (SCP).	X
INSTALL	Perform Card Content management. Optionally uses SD-SENC, SD-SMAC (SCP). Optionally, the Module uses the DAP-SYM key to verify the package signature.	X
LOAD	Load a load file (e.g. an applet). Optionally uses SD-SENC, SD-SMAC (SCP).	X
PUT DATA	Transfer data to an application during command processing. Optionally uses SD-SENC, SD-SMAC (SCP).	X
PUT KEY (*)	Load Card Manager keys The Module uses the SD-KDEK key to decrypt the keys to be loaded. Optionally uses SD-SENC, SD-SMAC (SCP).	X
SET STATUS	Modify the card or applet life cycle status. Optionally uses SD-SENC, SD-SMAC (SCP).	X
STORE DATA	Transfer data to an application or the security domain (ISD) processing the command. Optionally, updates OS-GLOBALPIN. Optionally uses SD-SENC, SD-SMAC (SCP).	X
GET MEMORY SPACE	Monitor the memory space available on the card. Does not use CSPs. Optionally uses SD-SENC, SD-SMAC (SCP).	X
SET ATR	Change the card ATR. Optionally uses SD-SENC, SD-SMAC (SCP).	X

Table 16 – Authenticated Card Manager Services and CSP Usage

The card life cycle state determines which modes are available for the secure channel. In the SECURED card life cycle state, all command data must be secured by at least a MAC. As specified in the GP specification, there exist earlier states (before card issuance) in which a MAC might not be necessary to send Issuer Security Domain commands. Note that the LOAD service enforces MAC usage.

© Copyright Gemalto 2016. May be reproduced only in its entirety [without revision].

Note (*): Services/CSPs using disallowed functions are not allowed in the Approved mode.

Service	Description	USR
Demonstrate RNG (*)	Generates a random value. Does not use CSPs.	X
Demonstrate Hash	Hashes a provided value using SHA-1, SHA-224, SHA-256, SHA-384, SHA-512. Does not use CSPs.	X
Demonstrate Symmetric Cipher (*)	Encrypts or decrypts a provided value using DSC-AES or DSC-TDEA provided in encrypted form with the service.	X
Demonstrate Symmetric Signature (*)	Generates or verifies a TDES MAC using DSS-TDEA provided in encrypted form during service invocation.	X
Demonstrate Asymmetric Signature (*)	Generates or verifies a signature using DAS-RSA or DAS-ECDSA provided to the module in encrypted form during service invocation,	X
Demonstrate EC DH (*)	Generates a shared secret value in accordance with SP 800-56A Section 5.7.1.2, and as well with non-SP 800-56A EC DH, using DECC-CDH.	X
Demonstrate Asymmetric Key Generation (*)	Demonstrates RSA, RSA CRT and ECC key generation, generating DKG-RSA and DKG-ECDSA.	X

Table 17 – Demonstration Applet Services and CSP Usage

All services include an authentication sequence – no service can be performed without successful authentication.

© Copyright Gemalto 2016. May be reproduced only in its entirety [without revision].

6 Finite State Model

The CM is designed using a finite state machine model that explicitly specifies every operational and error state.

The CM includes Power on/off states, Cryptographic Officer states, User services states, applet loading states, Key/PIN loading states, Self-test states, Error states, and the GP life cycle states.

An additional document (Finite State Machine document) identifies and describes all the states of the module including all corresponding state transitions.

7 Physical security policy

The CM is a single-chip implementation that meets commercial-grade specifications for power, temperature, reliability, and shock/vibrations. The CM uses standard passivation techniques and is protected by passive shielding (metal layer coverings opaque to the circuitry below) and active shielding (a grid of top metal layer wires with tamper response). A tamper event detected by the active shield places the Module permanently into the Card Is Killed error state.

The CM is mounted in a plastic smartcard; physical inspection of the Module boundaries is not practical after mounting. Physical inspection of modules for tamper evidence is performed using a lot sampling technique during the card assembly process. The Module also provides a key to protect the Module from tamper during transport and the additional physical protections listed in Section 12 below.

8 Operational Environment

This section does not apply to CM. No code modifying the behavior of the CM operating system can be added after its manufacturing process.

Only authorized applets can be loaded at post-issuance under control of the Cryptographic Officer. Their execution is controlled by the CM operating system following its security policy rules.

9 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.

© Copyright Gemalto 2016. May be reproduced only in its entirety [without revision].

10 Self-test

Note (*): Services/CSPs using disallowed functions are not allowed in the Approved mode.

10.1 Power-on self-test

Each time the CM is powered up it tests that the cryptographic algorithms still operate correctly and that sensitive data have not been damaged. Power-on self–tests are available on demand by power cycling the CM.

On power on or reset, the CM performs the self-tests described in Table 17. All KATs must be completed successfully prior to any other use of cryptography by the CM. If one of the KATs fails, the CM enters the Card Is Mute error state.

Test Target	Description
Firmware Integrity	16 bit CRC performed over all code located in Flash memory (for OS, Applets and filters).
RNG	Performs ANSI X9.31 KAT with fixed inputs (*)
TDES	Performs separate encrypt and decrypt KATs using 2-Key TDES (*) in ECB mode.
AES	Performs decrypt KAT using an AES 128 key in ECB mode. AES encrypt is self-tested as an embedded algorithm of AES-CMAC.
AES-CMAC	Performs an AES-CMAC Generate KAT using an AES 128 key. Note that AES-CMAC Verify is identical to a Generate KAT (perform Generate then compare to the input) hence a single KAT verifies both functions.
RSA	Performs separate RSA PKCS#1 signature and verification KATs using an RSA 2048 bit key, and a RSA PKCS#1 signature KAT using the RSA CRT implementation with a 2048 bit key.
ECDSA	Performs a ECDSA signature and verification KATs using an ECC P-224 key.
ECC CDH	Performs an ECC CDH KAT using an ECC P-224 key.
SHA-1	Performs a SHA-1 KAT.
SHA-256	Performs a SHA-256 KAT.
SHA-512	Performs a SHA-512 KAT.

Table 18 – Power-On Self-Test

10.2 Conditional self-tests

On every call to the [ANS X9.31] RNG, the CM performs the FIPS 140-2 Continuous RNG test (*) to assure that the output is different than the previous value.

When any asymmetric key pair is generated (for RSA or ECC keys) the CM performs a pairwise consistency test.

When new firmware is loaded into the CM using the LOAD command, the CM verifies the integrity and authenticity of the new firmware (applet) using the SD-SMAC key for MAC process. Optionally, the CM may also verify a signature of the new firmware (applet) using the DAP-RSA public key (*), the DAP-DES key (*) or the DAP-AES key; the signature block in this scenario is signed by an external entity using the private key corresponding to DAP-RSA or the symmetric DAP-DES key or the DAP-AES key.

© Copyright Gemalto 2016. May be reproduced only in its entirety [without revision].

11 Design Assurance

The CM meets the Level 3 Design Assurance section requirements.

11.1 Configuration Management

An additional document (Configuration Management Plan document) defines the methods, mechanisms and tools that allow to identify and place under control all the data and information concerning the specification, design, implementation, generation, test and validation of the card software throughout the development and validation cycle.

11.2 Delivery and Operation

Some additional documents (‘Delivery and Operation’, ‘Reference Manual’, ‘Card Initialization Specification’ documents) define and describe the steps necessary to deliver and operate the CM securely.

11.3 Guidance Documents

The Guidance document provided with CM is intended to be the ‘Reference Manual’. This document includes guidance for secure operation of the CM by its users as defined in the Roles, authentication and services chapter.

11.4 Language level

The CM operational environment is implemented using a high level language. A limited number of software modules have been written in assembler to optimize speed or size.

The Demonstration Applet is a Java applet designed for the Java Card environment.

12 Mitigation of other attacks policy

The Module implements defenses against:

- Fault attacks
- Side channel analysis (Timing Analysis, SPA/DPA, Simple/Differential Electromagnetic Analysis)
- Probing attacks
- Card tearing

© Copyright Gemalto 2016. May be reproduced only in its entirety [without revision].

13 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.

END OF DOCUMENT

© Copyright Gemalto 2016. May be reproduced only in its entirety [without revision].