THALES

IDCore 3230 / 230 Platform
FIPS 140-3 Cryptographic Module
Non-Proprietary Security Policy Level 3

Document Information

Release Date	July 24, 2024

Trademarks, Copyrights, and Third-Party Software

Disclaimer

All information herein is either public information or is the property of and owned solely by Thales and/or its subsidiaries who shall have and keep the sole right to file patent applications or any other kind of intellectual property protection in connection with such information.

Nothing herein shall be construed as implying or granting to you any rights, by license, grant or otherwise, under any intellectual and/or industrial property rights of or concerning any of Thales's information.

This document can be copied or distributed for informational, non-commercial, internal and personal use only provided that:

> The copyright notice below, the confidentiality and proprietary legend and this full warning notice appear in all copies.

> This document shall not be posted on any network computer or broadcast in any media other than on the NIST CMVP validation list and no modification of any part of this document shall be made.

Use for any other purpose is expressly prohibited and may result in severe civil and criminal liabilities.

The information contained in this document is provided "AS IS" without any warranty of any kind. Unless otherwise expressly agreed in writing, Thales makes no warranty as to the value or accuracy of information contained herein.

Thales hereby disclaims all warranties and conditions with regard to the information contained herein, including all implied warranties of merchantability, fitness for a particular purpose, title and non-infringement. In no event shall Thales be liable, whether in contract, tort or otherwise, for any indirect, special or consequential damages or any damages whatsoever including but not limited to damages resulting from loss of use, data, profits, revenues, or customers, arising out of or in connection with the use or performance of information contained in this document.

Thales does not and shall not warrant that this product will be resistant to all possible attacks and shall not incur, and disclaims, any liability in this respect. Even if each product is compliant with

current security standards in force on the date of their design, security mechanisms' resistance necessarily evolves according to the state of the art in security and notably under the emergence of new attacks. Under no circumstances, shall Thales be held liable for any third party actions and in particular in case of any successful attack against systems or equipment incorporating Thales products. Thales disclaims any liability with respect to security for direct, indirect, incidental or consequential damages that result from any use of its products. It is further stressed that independent testing and verification by the person using the product is particularly encouraged, especially in any application in which defective, incorrect or insecure functioning could result in damage to persons or property, denial of service or loss of privacy.

References

Acronym	Full Specification Name
[GlobalPlatform]	GlobalPlatform Consortium: GlobalPlatform Card Specification 2.2.1, January 2011, http://www.globalplatform.org
[ISO 7816]	ISO/IEC 7816-1:1998 *Identification cards -- Integrated circuit(s) cards with contacts -- Part 1: Physical characteristics* ISO/IEC 7816-2:2007 *Identification cards -- Integrated circuit cards -- Part 2: Cards with contacts -- Dimensions and location of the contacts* ISO/IEC 7816-3:2006 *Identification cards -- Integrated circuit cards -- Part 3: Cards with contacts -- Electrical interface and transmission protocols* ISO/IEC 7816-4:2005 *Identification cards -- Integrated circuit cards -- Part 4: Organization, security and commands for interchange*
[ISO 14443]	*Identification cards – Contactless integrated circuit cards – Proximity cards* ISO/IEC 14443-1:2008 Part 1*: Physical characteristics* ISO/IEC 14443-2:2010 Part 2: *Radio frequency power and signal interface* ISO/IEC 14443-3:2011 Part 3: *Initialization and anticollision* ISO/IEC 14443-4:2008 Part 4: *Transmission protocol*
[JavaCard]	*Java Card 3.1.0 Runtime Environment (JCRE) Specification* *Java Card 3.1.0 Virtual Machine (JCVM) Specification* *Java Card 3.1.0 Application Programming Interface* Published by Sun Microsystems, February 2021.
[FIPS 140-3]	Federal Information Processing Standards Publication 140-3, Security Requirements for Cryptographic Modules, March 2019
[IG]	NIST, Implementation Guidance for FIPS 140-3 and the Cryptographic Module Validation Program, January 2024.
[FIPS 180-4]	NIST, *Secure Hash Standard*, FIPS Publication 180-4, August 2015
[FIPS 186-4]	NIST, Digital Signature Standard (DSS), FIPS Publication 186-4, July 2013.
[FIPS 186-5]	NIST, Digital Signature Standard (DSS), FIPS Publication 186-5, February 2023.
[FIPS 197]	NIST, *Advanced Encryption Standard (AES)*, FIPS Publication 197, November 26, 2001.
[FIPS 198-1]	Federal Information Processing Standards Publication 198-1, The Keyed-Hash Message Authentication Code (HMAC), July 2008.
[FIPS 202]	Federal Information Processing Standards Publication 202, SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions, August 2015.
[FIPS 113]	NIST, *Computer Data Authentication*, FIPS Publication 113, 30 May 1985.
[ISO 19790:2012]	ISO/IEC 19790:2012 (Corrected 2015-12-15, IDT) Information technology – Security techniques – Security requirements for cryptographic modules, 2015-12-15.

[ISO 24759:2017]	ISO/IEC 24759:2017 (Corrected 2017-03, IDT) Information technology – Security techniques – Test requirements for cryptographic modules, 2017-03.
[PKCS#1]	PKCS #1 v2.1: RSA Cryptography Standard, RSA Laboratories, June 14, 2002
[SP 800-108r1]	NIST Special Publication 800-108 Revision 1, Recommendation for Key Derivation Using Pseudorandom Functions, August 2022.
[SP 800-131Ar2]	NIST Special Publication 800-131A Revision 2, Transitioning the Use of Cryptographic Algorithms and Key Lengths, March 2019.
[SP 800-132]	NIST Special Publication 800-132, Recommendation for Password-Based Key Derivation: Part 1: Storage Applications, December 2010.
[SP 800-133r2]	NIST Special Publication 800-133 Revision 2, Recommendation for Cryptographic Key Generation, June 2020.
[SP 800-140Cr2]	NIST Special Publication 800-140C Revision 2, CMVP Approved Security Functions: CMVP Validation Authority Updates to ISO/IEC 24759, July 2023.
[SP 800-140Dr2]	NIST Special Publication 800-140D Revision 2, CMVP Approved Sensitive Security Parameter Generation and Establishment Methods: CMVP Validation Authority Updates to ISO/IEC 24759, July 2023.
[SP 800-140E]	NIST Special Publication 800-140E, CMVP Approved Authentication Mechanisms: CMVP Validation Authority Requirements for ISO/IEC 19790:2012 Annex E and ISO/IEC 24759 Section 6.17, March 2020.
[SP 800-140F]	NIST Special Publication 800-140F, CMVP Approved Non-Invasive Attack Mitigation Test Metrics: CMVP Validation Authority Updates to ISO/IEC 24759, March 2020.
[SP 800-38A]	NIST Special Publication 800-38A, Recommendation for Block Cipher Modes of Operation – Methods and Techniques, December 2001.
[SP 800-38B]	NIST Special Publication 800-38B, Recommendation for Block Cipher Modes of Operation: the CMAC Mode for Authentication, May 2005 (with October 2016 updates).
[SP 800-38D]	NIST Special Publication 800-38D, Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC, November 2007.
[SP 800-38E]	NIST Special Publication 800-38E, Recommendation for Block Cipher Modes of Operation: the XTS-AES Mode for Confidentiality on Storage Devices, January 2010.
[SP 800-38F]	NIST Special Publication 800-38F, Recommendation for Block Cipher Modes of Operation: Methods for Key Wrapping, December 2012.
[SP 800-56Ar3]	NIST Special Publication 800-56A, Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography, Revision 3, April 2018.
[SP 800-56Br2]	NIST Special Publication 800-56B, Recommendation for Pair-Wise Key-Establishment Schemes Using Integer Factorization Cryptography, Revision 2, March 2019.
[SP 800-56Cr2]	NIST Special Publication 800-56C, Recommendation for Key-Derivation Methods in Key-Establishment Schemes, Revision 2, August 2020.
[SP 800-67r2]	NIST Special Publication 800-67, Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher, Revision 2, November 2017.
[SP 800-90Ar1]	NIST Special Publication SP 800-90A, Recommendation for Random Number Generation Using Deterministic Bit Generators, Revision 1, June 2015.

[SP 800-90B]	NIST, SP 800-90B, “Recommendation for the Entropy Sources Used for Random Bit Generation”, January 2018.

Table 1 – References

Term	Definition
AES	Advanced Encryption Standard
API	Application Programming Interface
CBC	Cipher Block Chaining
CKG	Cryptographic Key Generation
CLK	CLocK
CM	Cryptographic Module
CMAC	Cipher-based Message Authentication Code
CMVP	Cryptographic Module Validation Program
CO	Crypto Officer
CRC	Cyclic Redundancy Check
CS	Cipher Suite
DAP	Data Authentication Pattern
DES	Data Encryption Standard
DRBG	Deterministic Random Bit Generator
DM	Delegated Management
ECB	Electronic Code Book
ECC	Elliptic Curve Cryptography
ECDSA	Elliptic Curve Digital Signature Algorithm
EDC	Error Detection Code
EFP	Environmental Failure Protection
ESV	Entropy Source Validation
FIPS	Federal Information Processing Standards
GND	Ground (electrical connection)
GP	Global Platform
HKDF	HMAC Key Derivation Function

HMAC	Hash-based keyed Message Authentication Code
HW	Hardware
I/O	Input Output
ISO	International Standards Organisation
JCAPI	JavaCard API
JCRE	JavaCard Runtime Environment
KAS	Key Agreement Scheme
KAT	Known Answer Test
KBKDF	Key Based Key Derivation Function
KC	Key Confirmation
KDF	Key Derivation Function
MAC	Message Authentication Code
MMU	Memory Management Unit
OPACITY	Open Protocol for Access Control, Identity, Ticketing with privacY
PIN	Personal Identification Number
PIV	Personal Identity Verification
PKCS	Public Key Cryptographic Standards
PRI	PRIvate (key)
PSS	Probabilistic Signature Scheme
PST	Periodic Self Test
PUB	PUblic (key)
RAM	Random Access Memory
SCP	Secure Channel Protocol
SD	Security Domain
SHA	Secure Hash Algorithm
SSD	Supplementary Security Domain
SSP	Sensitive Security Parameter
SYM	SYMmetric (key)
RF	Radio Frequency
RLC	Reinforced Low Cost
RLT	RLC Thin

RSA	Rivest Shamir Adleman
SCP	Secure Channel Protocol
TRNG	True Random Number Generator
UA	Unauthenticated User
UART	Universal Asynchronous Receiver Transceiver
USB	Universal Serial Bus
USR	USeR
VCC	Voltage Common Collector
VM	Virtual Machine

Table 2 – Acronyms and Definitions

Table of Contents

Table of Tables

Table of Figures

1 General

This document defines the Security Policy for the Thales **IDCore 3230 / 230 Platform** cryptographic module, herein denoted the *Module*. The *Module*, validated to FIPS 140-3 overall Level 3, is a single-chip "contact" or "contact and contactless" module implementing the Global Platform operational environment, with Card Manager and Demonstration Applet.

The Demonstration Applet is available only to demonstrate the complete cryptographic capabilities of the Module for FIPS 140-3 validation and is not intended for general use. The term *platform* herein is used to describe the chip and operational environment, not inclusive of the Demonstration Applet.

The *Module* has a limited operational environment. The *Module* includes a firmware load function to support necessary updates. New firmware versions within the scope of this Security Policy and certificate must be validated through the FIPS 140-3 CMVP. Any other firmware loaded onto this module is out of the scope of this validation and requires a separate FIPS 140-3 validation.

The FIPS 140-3 security levels for the *Module* are as follows:

ISO/IEC 24759 Section 6. [Number Below]	FIPS 140-3 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	N/A

Table 3 – Security Levels

2 Cryptographic Module Specification

The IDCore 3230/230 platform cryptographic module is a single chip hardware module.

The platform is available in both 'contact' or 'contact and contactless' variants implementing the Global Platform operational environment, with Card Manager and a Demonstration Applet.

Figure 1 below depicts the Module's block diagram, with a red outline highlighting the cryptographic boundary. The cryptographic boundary encompasses all the components included on the single chip.

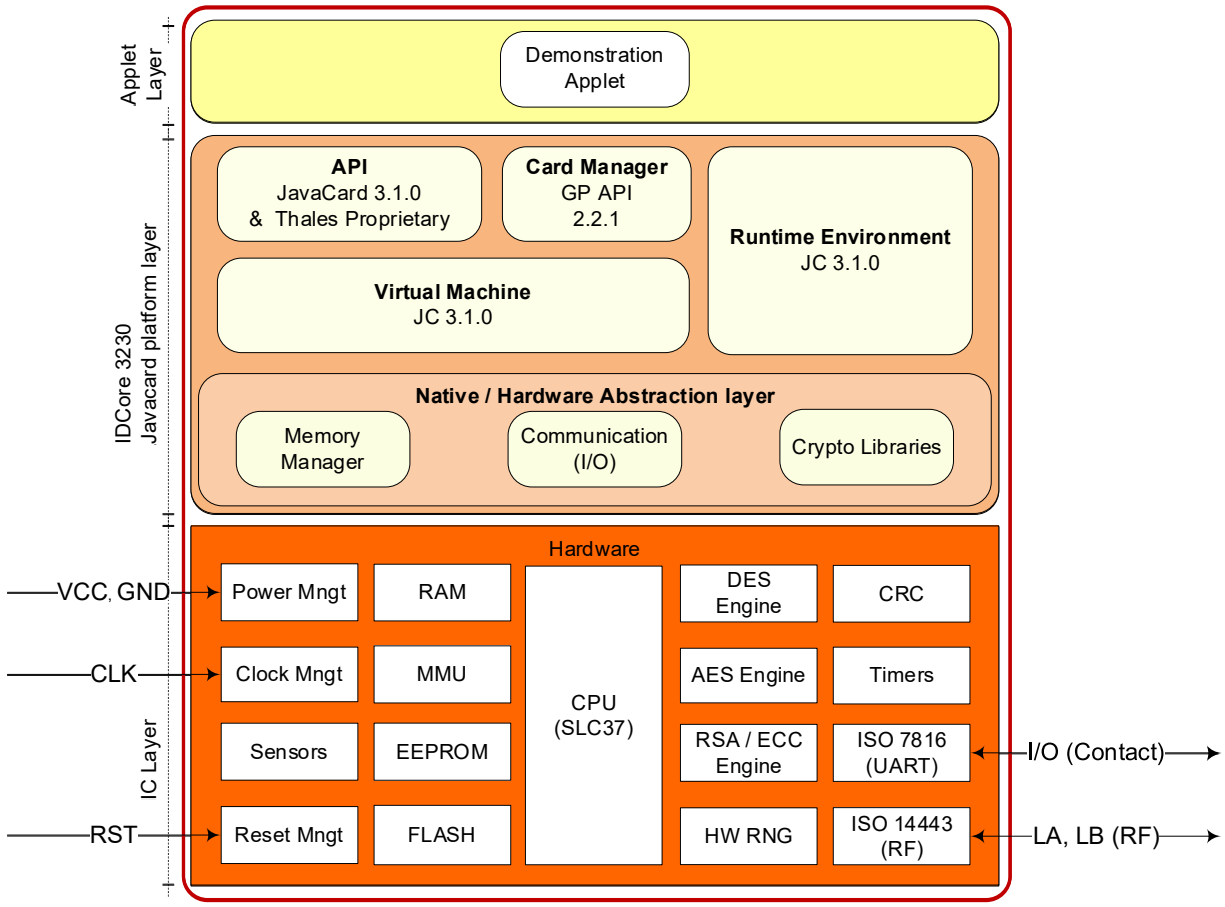


Figure 1 – Cryptographic Boundary

The CM is fully compliant with two major cards industry standards: Oracle Java Card 3.1.0 Classic Edition and GlobalPlatform (GP) Card Specification version 2.2.1.

The CM supports [ISO7816] T=0, T=1 and T=CL 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.

The *JavaCard API (JCAPI)* 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 (JCRE)* implements the dispatcher, registry, loader, and logical channel functionalities.

The *Virtual Machine (VM)* 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 Card Manager behaves similarly to an applet but is properly represented as a constituent of the platform. In case of delegated management (DM), the Supplementary Security Domain (SSD) behaves similarly to the Card Manager in term of card content, keys and life cycle states.

The *Memory Manager* implements functions such as memory access, allocation, deletion and garbage collection.

The *Communication* handler implements the ISO 7816 and ISO 14443 communications protocols in contactless mode and dual mode.

The *Cryptography Libraries* implement the Approved services listed in Section 2.2.

The Module is designed to be embedded into a plastic card body, passport, USB key, secure element etc., with a contact plate connection and/or RF antenna.

The Module's single chip is the SLC37GDA512. It can be presented in three different form factors:

- WORLD RLT module (contact)
- WORLD Combi RLT module (contact and contactless)
- PICO RLV module (contact)

2.1 Test Configuration

The following tested configurations are covered in this security policy:

Model	Hardware [Part Number and Version]	Firmware Version	Distinguishing Features
World RLT module	**Hardware:** SLC37GDA512 **Mask number:** G322 **Part Number**: A2848377	**Firmware:** IDCore 230-BUILD6.11 Demonstration Applet version V1.D	Java Card 3.1.0 GlobalPlatform (GP) 2.2.1 Interface: contact with protocol communication T=0 and T=1
World Combi RLT module	**Hardware:** SLC37GDA512 **Mask number:** G322 **Part Number**: A2848344	**Firmware:** IDCore 3230-BUILD6.11 Demonstration Applet version V1.D	Java Card 3.1.0 GlobalPlatform (GP) 2.2.1 Interface: contact with protocol communication T=0 and T=1 Contactless with protocol communication T=CL
PICO RLV Module	**Hardware:** SLC37GDA512 **Mask number:** G322 **Part Number**: A3138921	**Firmware:** IDCore 230-BUILD6.11 Demonstration Applet version V1.D	Java Card 3.1.0 GlobalPlatform (GP) 2.2.1 Interface: contact with protocol communication T=0 and T=1

Table 4 – Cryptographic Module Tested Configuration

2.1 Tested Operational Environment Physical Perimeter

The physical form of the Module is depicted in Figure . The Tested Operational Environment's Physical Perimeter (TOEPP) is defined as the surfaces and edges of the packages. The Module relies on [ISO 7816] and/or [ISO 14443] card readers as input/output devices.

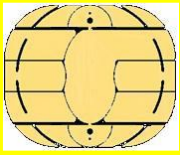
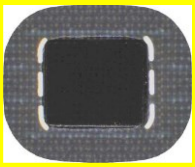
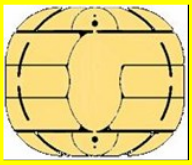
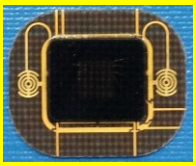
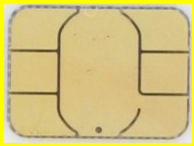
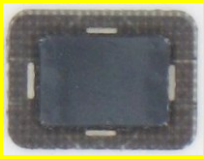
WORLD RLT module (SLC37GDA512)	
 Oblong punching **Top View – Contact Plate**	 **Bottom View - Black Epoxy with RLT technology**
WORLD Combi RLT module (SLC37GDA512)	
 Oblong punching **Top View – Combi Plate**	 **Bottom View - Black Epoxy with RLT technology**
PICO RLV module (SLC37GDA512)	
 **Top View – Contact Plate**	 **Bottom View - Black Epoxy with RLV technology**

Figure 2 - Models

2.2 CM Identification

The CM is always in the approved mode of operation, it does not support a non-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	2Dh	Get CPLC data (tag 9F 7F)
			01-03	1Dh	Get Identification data (tag 01 03)
			01-2F	10h	Get Approved mode parameters (tag 01 2F):

Table 5 – Tags for Tracking Data (Approved Mode)

The CM production life cycle data can be checked using GET DATA command with tag '9F7F'. The Module responds with 42 bytes composed of:

IDCore 3230/230 - CPLC data (tag 9F7F)			
Byte	**Description**	**Value**	**Value meaning**
1-2	IC fabricator	**4090h**	Infineon
3-4	IC type	**0039h**	SLC37GDA512
5-6	Operating system identifier	**1291h**	Thales
7-8	Operating system release date (YDDD) – Y=Year, DDD=Day in the year	**YDDDh**	Operating System release Date
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

Table 6 – Card Production Life Cycle Data

The CM identification data can be checked using GET DATA command with tag '0103'. The Module responds with 29 bytes composed of:

IDCORE 3230/230 - Identification data (tag 0103)			
Byte	**Description**	**Value**	**Value meaning**
1	Thales Family Name	**B0**	Javacard
2	Thales OS Name	**84**	IDCore family
3	Thales Mask Number	**66**	G322
4	Thales Product Name	**6B**	IDCore3230 / 230
5	Thales Version	**06**	Major Version
6	Thales Version (Minor)	**11**	Minor Version[1]
7-8	Chip Manufacturer	**4090**	Infineon
9-10	Chip Version	**7305**	SLC37GDA512
11-12	Operational Mode	**8900**	Approved mode
13	FIPS Level for product	**03**	03 = FIPS Level 3
14-15	Specific chip ID	**32 30**	32 30 = Contact and Contactless 2 30 = Contact
16-29	RFU	**xx..xxh**	RFU

Table 7 – Versions and Operations Indicators

The status of the Approved mode of operation can be checked using GET DATA command with tag '012F'. The Module responds with 16 bytes composed of:

- 4 bytes for CAST status

1 Bytes 5 and 6, as indicated in Table 7 above collective indicate the validated Firmware version number, "IDCore 3230-BUILD6.11".

- 2 bytes for Error log
- 4 bytes for Periodic Self-Test counter
- 4 bytes for Periodic Self-Test maximum counter value
- 1 byte for Operational Mode
- 1 byte for Flag

The Demonstration Applet version can be checked using GET VERSION command, after having selected the applet:

Field	CLA	INS	P1-P2 (Tag)	Le (Expected response length)	Purpose
Value	**00**	**AA**	**00 00**	**01**	**1Dh (version)**

Table 8 – get data command to output Demonstration applet version (Approved Mode)

2.3 Approved Algorithms

The CM implements the following approved services:

CAVP Cert	Algorithm and Standard	Mode / Method	Description / Key Size(s) / Key Strength(s)	Use / Function
Cert. #A2877	**Algorithm**: AES-CBC **Standard**: [SP 800-38A]	**Mode**: CBC **Method**: encryption and decryption	**Key size**: 128, 192 and 256-bits	Manage Content Module Info (Auth) Secure Channel Symmetric Cipher Opacity Secure Channel
Cert. #A2877	**Algorithm**: AES-CMAC **Standard**: [SP 800-38B]	**Method**: generation and verification	**Key size**: 128, 192 and 256-bits **MAC Length**: 128 **Message Length**: 128-256 Increment 8	Life cycle Manage Content Module Info (Auth) Secure channel Symmetric Cipher Message Authentication Opacity Secure Channel
Cert. #A2877	**Algorithm**: AES-ECB **Standard**: [SP 800-38A]	**Mode**: ECB **Method**: encryption and decryption	**Key size**: 128, 192 and 256-bits	Manage Content Symmetric Cipher Verify OS-GLOBALPIN

CAVP Cert	Algorithm and Standard	Mode / Method	Description / Key Size(s) / Key Strength(s)	Use / Function
Cert. #A2877	**Algorithm**: Counter DRBG **Standard**: [SP 800-90Ar1]	**Mode**: Counter mode based on AES-256.	**Security strength**: 256-bits Derivation Function Enabled: Yes Additional Input: 0 Entropy Input: 1024 Nonce: 384 Personalization String Length: 0 Returned Bits: 128.	Secure Channel Digital Signature Generate Key Pair Opacity Secure Channel
Cert #E107	**Algorithm**: ESV **Standard**: [SP 800-90B]	**Method**: Hardware TRNG includes conditioning (based on compression) and SP 800-90B required health tests.	Security strength: min-entropy is 13.376 per 32-bit blocks	Entropy source for DRBG [SP 800-90Ar1]
Cert. #A2877	**Algorithm**: ECDSA KeyGen **Standard**: [FIPS 186-5]	**Method**: Key Generation Secret Generation Mode: Extra Bits	Key pair generation using P-224, P-256, P-384, P-521 curves. Security Strength: between 112 bits (P-224) and 256 bits (P-521)	Generate Key Pair
Cert. #A2877	**Algorithm**: ECDSA SigGen **Standard**: [FIPS 186-5]	**Method**: Signature Generation **Hash options**: SHA2-224, SHA2-256, SHA2-384, SHA2-512	Capabilities: Curve: P-224, P-256, P-384, P-521 Hash Algorithm: SHA2-224, SHA2-256, SHA2-384, SHA2-512	Digital Signature
Cert. #A2877	**Algorithm**: ECDSA SigVer. **Standard**: [FIPS 186-5]	**Method**: Signature Verification. **Hash options**: SHA2-224, SHA2-256, SHA2-384, SHA2-512	Capabilities: Curve: P-224, P-256, P-384, P-521 Hash Algorithm: SHA2-224, SHA2-256, SHA2-384, SHA2-512 Security Strength: between 112 bits (P-224) and 256 bits (P-521)	Digital Signature

CAVP Cert	Algorithm and Standard	Mode / Method	Description / Key Size(s) / Key Strength(s)	Use / Function
Cert. #A2877	**Algorithm:** HMAC-SHA2-256 **Standard**: [FIPS 198-1]	**Method**: HMAC-SHA2-256	**Key size**: 16 bytes **MAC**: 256 **Key Length**: 128, 256	Compute HashMac
Cert. #A2877	**Algorithm**: KAS-ECC **Standard**: [SP 800-56Ar3]	**Method**: OnePassDH is a One Step KDF with partial key validation and Unilateral key confirmation (KC) using CMAC-AES	**Curves:** P-256 using SHA-256 with KC CMAC-AES128 bits **Key length**: 512 bits **Curves**: P-384, using SHA-384, with KC CMAC-AES 256 bits **Key length**: 1024 bits	Opacity Secure Channel
Cert. #A2877	**Algorithm**: KAS-ECC-SSC **Standard**: [SP 800-56Ar3]	**Method**: ephemeralUnified KAS Role: initiator, responder	**Curves**: P-224, P-256, P-384, P-521.	ECC CDH Primitive
Cert. #A2877	**Algorithm**: KDA OneStep **Standard**: [SP800-56Cr2]	**Method**: One Step Key derivation using approved hash (SHA2-256)	Fixed Info Pattern: uPartyInfo||vPartyInfo Fixed Info Encoding: concatenation Derived Key Length: 256 Shared Secret Length: 256	Key-Derivation Functions (KDF) Opacity Secure Channel
Cert. #A2877	**Algorithm**: KDA HKDF **Standard**: [SP800-56Cr2]	**Method**: HMAC -based KDF (RFC5869)	Fixed Info Pattern: uPartyInfo||vPartyInfo Fixed Info Encoding: concatenation Derived Key Length: 512 Shared Secret Length: 256 HMAC Algorithm: SHA2-256	Key-Derivation Functions (KDF)

CAVP Cert	Algorithm and Standard	Mode / Method	Description / Key Size(s) / Key Strength(s)	Use / Function
Cert. #A2877	**Algorithm**: KBKDF **Standard**: [SP 800-108r1]	**Mode**: Counter KDF **MAC Mode**: CMAC-AES128, CMAC-AES192, CMAC-AES256	**Description**: Derive session key from existing static secret key for SCP03 establishment **Key size**: 128, 192 and 256-bits Supported Lengths: 128-256 Increment 64 Fixed Data Order: In the Middle of Fixed Data Counter Length: 8 Custom Key In Length: 0	Secure Channel
Cert. #A2877	**Algorithm**: KTS **Standards**: [SP 800-38F] AES ENC + AES CMAC	**Mode:** AES (CBC or ECB) encryption with AES CMAC authentication **Method:** Key Transport Scheme/Key Wrapping AES	**Description:** Use of approved AES encryption method (SP 800-38A) with the combination of approved Authentication method AES CMAC [SP 800-38B] **Key size:** 128, 192 and 256-bits.	Secure Channel
Cert. #A2877	**Algorithm**: RSA KeyGen (CRT) **Standard:** [FIPS 186-5]	**Method**: Key Generation Mode probable Hash options: SHA2-224, SHA2-256, SHA2-384, SHA2-512	**Key sizes**: 2048, 3072, 4096 bit keys Private Key Format: crt	Generate Key Pair
Cert. #A2877	**Algorithm**: RSA KeyGen **Standard**: [FIPS 186-5]	**Method**: Key Generation Mode probable Hash options: SHA2-224, SHA2-256, SHA2-384, SHA2-512	**Key sizes**: 2048 bit keys Private Key Format: std	Generate Key Pair

CAVP Cert	Algorithm and Standard	Mode / Method	Description / Key Size(s) / Key Strength(s)	Use / Function
Cert. #A2877	**Algorithm**: RSA SigGen **Standard**: [FIPS 186-5]	**Method**: Signature Generation Signature Type: PKCS #1-v1.5, PKCS-PSS. Hash options: (PKCS #1-v1.5 and PKCS-PSS): SHA2-224, SHA2-256, SHA2-384, SHA2-512	**Key sizes**: 2048, 3072, 4096 bit keys Private Key Format: crt and std	Digital Signature
Cert. #A2877	**Algorithm**: RSA SigVer **Standard**: [FIPS 186-5]	**Method**: Signature Verification Signature Type: PKCS #1-v1.5 1.5, PKCS-PSS. Hash options: (PKCS #1-v1.5 and PKCS-PSS): SHA2-224, SHA2-256, SHA2-384, SHA2-512	**Key sizes**: 2048, 3072, 4096 bit keys	Digital Signature Manage Content
Cert. #A2877	**Algorithm**: SHA2 **Standard**: [FIPS 180-4]	**Method**: SHA2-224, SHA2-256, SHA2-384, SHA2-512 Message Length: 8-65536 Increment 8	N/A.	Digital Signature Compute Hash Key Derivation Functions Manage Content
Cert. #A2877	**Algorithm**: SHA3 **Standard**: [FIPS 202]	**Methods:** SHA3-224, SHA3-256, SHA3-384, SHA3-512. Message Length: 0-65536 Increment 8	N/A.	Compute Hash
Cert. #A2877	**Algorithm**: TDES-CBC **Standard**: [SP 800-67r2]	**Mode**: CBC **Method:** Decrypt (legacy use)	Description: The Module supports the 3-Key, with CBC decrypt mode for legacy use only. Key size: 168-bits (3-key).	Symmetric Cipher (decrypt only)

CAVP Cert	Algorithm and Standard	Mode / Method	Description / Key Size(s) / Key Strength(s)	Use / Function
Cert. #A2877	**Algorithm**: TDES-ECB **Standard**: [SP 800-67r2]	**Mode**: ECB **Method:** Decrypt (legacy use)	Description: The Module supports the 3-Key, with ECB decrypt mode for legacy use only. Key size: 168-bits (3-key).	Symmetric Cipher (decrypt only)
Vendor Affirmed	**Algorithm**: CKG **Standard**: [SP 800-133r2]	**Method**: Sections 4, 5.1 and 5.2	Description: The seeds used for asymmetric key pair generation are produced using the unmodified/direct output of the DRBG. Security Strength: 256-bits	Generate Key Pair

Table 9: Approved Algorithms

NOTE The following algorithms are present in the module and have completed CAVP testing (under CAVP #A2877) but this code is not executed for the validated configuration of the module.

- ECDSA KeyGen (FIPS 186-4), ECDSA SigGen (FIPS 186-4), ECDSA SigVer (FIPS 186-4), KTS-IFC (KTS-OAEP-basic, rsa std 2048), KTS-IFC (KTS-OAEP-basic, rsa CRT 2048, 3072, 4096), RSA KeyGen (FIPS 186-4), RSA SigGen (FIPS 186-4), RSA SigVer (FIPS 186-4), RSA Decryption Primitive (SP 800-56B), SHA1

2.4 Non-Approved Algorithms

The module only implements approved services/algorithms and does not support any non-approved algorithms.

3 Cryptographic Module Interfaces

The Module is designed to be embedded into a plastic card body, passport, USB key, secure element etc., with a contact plate connection and/or RF antenna.

3.1 PIN Assignments and Contact Dimensions

The WORLD Combi RLT module has access to contact and contactless interfaces.

The WORLD RLT module and the PICO RLV module have only access to a contact interface. The contact interface is the same for all the module variants.

Figure 3 - Contact and Contactless Interfaces

The Module does not support a Control Output interface.

Physical port	Logical interface	Data that passes over port/interface
VCC	Supply voltage	Power
RST	Reset signal	Control in
CLK	Clock signal	Control in
GND	Ground	Power
I/O	Input/output	Data in, data out, control in, status out
LA	Antenna coil connection	Power, Data in, Data out, Control in, Status out
LB	Antenna coil connection	Power, Data in, Data out, Control in, Status out

Table 10 – Ports and Interfaces

For contact interface operation, the *Module* conforms to [ISO 7816] part 1 and part 2. The electrical signals and transmission protocols follow the [ISO 7816] part 3.

The operating conditions for the contact interfaces of this module are:

Conditions	Range
Voltage	1.8V, 3 V and 5.5 V DC
Frequency[2]	1MHz to 10MHz

Table 11 - Voltage and Frequency Ranges

For contactless interface operation, the *Module* conforms to [ISO 14443] part 1 for physical connections, and to [ISO 14443] parts 2, 3 and 4 for radio frequencies and transmission protocols.

The operating conditions for the contactless interfaces of this module are:

Conditions	Range
Supported bit rate	106 Kbits/s, 212 Kbits/s, 424 Kbits/s, 848 Kbits/s
Operating field	Between 1.5 A/m and 7.5 A/m rms
Frequency	13.56 MHz +- 7kHz

Table 12 – Contactless voltage and Frequency Ranges

[2] Frequency of the internal clock as supplied by the CLK physical interface.

4 Roles, Services, and Authentication

4.1 Roles

The module supports two authenticated roles, the Cryptographic Officer (CO) and the User (USR). The CO is responsible for card issuance and management of card data via the Card Manager Authenticated using the SCP authentication method with SD-SENC. The USR is for FIPS 140-3 validation purposes, authenticated as described in *Demonstration Applet Authentication* below. The module also supports unauthenticated services, which are implicitly invoked by the Unauthenticated Role (UA).

Authentication of each operator and their access to roles and services is as described below, independent of logical channel usage. Only one operator at a time is permitted on a channel.

Applet 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.

Applet reselection (except Card Manager that close systematically the GlobalPlatform secure channel) is leaving the secure channel unchanged and it is up to the applet policy to close it or not.

The module clears previous authentications on each power cycle. It also supports Global Platform SCP logical channels, allowing concurrent operators in a limited fashion.

4.2 Approved Services

All approved services implemented by the Module are listed in the tables below. The module does not support any non-approved services.

Role	Service	Input	Output
CO	Lifecycle: Modify the card or applet life cycle status	Set / Get Status: life cycle state to update/ empty	return Status Word / life cycle state and package list
CO	Manage Content: -Load, install, and delete application packages and associated keys and data -Manage keys: SD-KENC, SD-KDEK,SD-KMAC, DAP-SYM, DAP-ASYM, DM-TOKEN-SYM, DM-TOKEN-ASYM, DM-RECEIPT-SYM (Put key) -Update Pin to change the OS-GLOBALPIN	- applications and associated data - keys - OS-GLOBALPIN	return Status Word
CO	Module Info (Auth): Read module configuration or status information (privileged data objects).	Tags and module information	module configuration status information return Status Word

Role	Service	Input	Output
CO	Secure Channel: Establish and use a secure communications channel (AES CMAC with KBKDF)	random, diversification data	authentication data, return Status Word
USR	Digital Signature: Demonstrate RSA and ECDSA digital signature generation and verification	session, algorithm, algorithm parameters, data to sign.	signature, return Status Word
USR	Generate Key Pair: Demonstrate RSA and ECC key generation	None	public and private key generated return Status Word
USR	ECC CDH Primitive: Demonstrate ECC Diffie-Hellman primitive Generate a shared secret from ECC-CDH scheme	algorithm, algorithm parameters, Ecc public key	shared secret, return Status Word
USR	Symmetric Cipher: Demonstrate use of AES for encryption and decryption.. Demonstrate use of Triple-DES for decryption only.	session, algorithm, algorithm parameters, data to encrypt/decrypt	encrypted / decrypted data, return Status Word.
USR	Message Authentication: Demonstrate AES CMAC	Data	CMAC return Status Word
USR	Key-Derivation Functions (KDF): Demonstrate use of Keys diversification service • KDA HKDF • KDA OneStep	ikm (“input key material”) salt, fixed info counter, shared secret and Other info	okm: Output keys material return Status Word
USR	Compute Hash: compute the hash value	message	Hash return Status Word
USR	Compute HashMac: compute the hashmac value	Message Key	HashMac return Status Word
UA	Context – Select an applet or manage logical channels.	data	return Status Word
UA	Module Info - Read unprivileged data objects, e.g., module configuration or status information.	Data	return Status Word

Role	Service	Input	Output
UA	Module Reset - Power cycle or reset the Module. Includes Integrity Self-Test, periodic self-test counter set up and self-test flag is reset	N/A	ATR (Answer To Reset)
UA	Run Cryptographic KAT - Sets a flag to that a specific cryptographic KATs has been performed on demand via Module Reset.	Data	return Status Word
UA	Get Approved mode parameters - Get information of the approved mode of operation	N/A	data return Status Word
UA	Verify the OS-GLOBALPIN	OS-GLOBALPIN	return Status Word
UA	OPACITY Secure Channel - Establishes a secure channel based on opacity to protect confidentiality and integrity of transmitted information and allows the off-card entity initiating the Opacity Secure Messaging to authenticate the module	Data	control byte + nonce + cryptogram + cert return Status Word

Table 13 - Roles, Service Commands, Input and Output

Opacity Secure Channel service:

OPACITY (**O**pen **P**rotocol for **A**ccess **C**ontrol **I**dentification and **T**icketing with privac**Y**) is a compact flexible secure and fast authentication protocol with secure messaging capability.
This secure messaging is based on symmetric session keys derived using the key establishment protocol. The key establishment protocol authenticates the card application to the client application and establishes a set of session keys that may be subsequently used to protect the communication channel between the two parties. Once session keys are established and the card is authenticated, subsequent communication with the card can be performed using secure messaging.

This is a one way authentication protocol. The reader is not authenticated by the card. This secure channel is based on the card key: DEM-OPACITY-PRI and an ephemeral key generated by the host.
The section 4.1 of SP 800-73-4 specification describes the key establishment protocol used to support secure messaging in the PIV Card Application.

The strength depends on cipher suite CS2 and CS7:

- Cipher Suite 2 (AES 128, ECDSA with SHA-256 using an ECDSA (Curve P-256) key) provides 128 bits of channel strength.
- Cipher Suite 7 (AES 256, ECDSA with SHA-384 using an ECDSA (CurveP-384) key) provides 192 bits of channel strength.

All usage of SSPs by the services implemented by the Module are listed in the table below:

All of the above commands use the SD-SENC and SD-SMAC keys for secure channel communications, and SD-SMAC for firmware load integrity.

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.

The provided demonstration applet enforces the restrictions of algorithms, modes, and key sizes per NIST SP 800-131A Revision 1.

In the ‘Access Rights to Keys and/or SSPs’ column:

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.

E = Execute: The module uses the SSP in performing a cryptographic operation.

Z = Zeroize: The module zeroizes the SSP.

In the ‘Indicator Column’:

IND_1: The status conditions for successfully completed execution is 90 00

Service	Description	Approved Security Functions	Keys and/or SSPs	Roles	Access rights to Keys and/or SSPs	Indicator
Lifecycle	Modify the card or applet life cycle status	AES-CMAC	OS-DRBG-EI OS-DRBG-S OS-DRBG-V OS-DRBG-KEY OS-GLOBALPIN OS-MKDK SD-KENC SD-KMAC SD-KDEK SD-SENC SD-SMAC DAP-SYM	CO	**Z** : for all SSPs When setting the card state to terminated	IND_1

Service	Description	Approved Security Functions	Keys and/or SSPs	Roles	Access rights to Keys and/or SSPs	Indicator
			DM-TOKEN-SYM DM-RECEIPT-SYM DAP-ASYM DM-TOKEN-ASYM DEM-EDK DEM-MAC DEM-COM-EDK DEM-COM-MAC DEM-SGV-PRI DEM-KAP-PRI DEM-KGS-PRI DEM-DEM-SGV-PUB DEM-KAP-PUB DEM-KGS-PUB			
Manage Content1	Load, install, and delete application packages and associated keys and data	AES-CBC AES-CMAC AES-ECB RSA SigVer SHA2	SD-KENC SD-KMAC OS-MKDK SD-KDEK SD-SENC SD-SMAC DAP-SYM DM-TOKEN-SYM	CO	**W** : SD-KENC, SD-KMAC, SD-KDEK, DAP-SYM, DM-TOKEN-SYM, DM-RECEIPT-SYM, DAP-ASYM, DM-TOKEN-ASYM, DEM-COM-EDK, DEM-COM-MAC **E** :	IND_1

Service	Description	Approved Security Functions	Keys and/or SSPs	Roles	Access rights to Keys and/or SSPs	Indicator
			DM-RECEIPT-SYM DAP-ASYM DM-TOKEN-ASYM DEM-COM-EDK DEM-COM-MAC		OS-MKDK, SD-KMAC, SD-KDEK, SD-SENC, SD-SMAC, DAP-SYM, DM-TOKEN-SYM, DM-RECEIPT-SYM, DAP-ASYM, DM-TOKEN-ASYM **Z**: DEM-COM-EDK, DEM-COM-MAC	
Manage Content2	Manage keys: SD-KENC, SD-KDEK, SD-KMAC, DAP-SYM, DAP-ASYM, DM-TOKEN-SYM, DM-TOKEN-ASYM, DM-RECEIPT-SYM (Put key)	AES-CBC AES-CMAC AES-ECB	SD-KENC SD-KDEK SD-KMAC DAP-SYM DAP-ASYM DM-TOKEN-SYM DM-TOKEN-ASYM DM-RECEIPT-SYM OS-MKDK	CO	**W** : SD-KENC, SD-KMAC, SD-KDEK, DAP-SYM, DAP-ASYM; DM-TOKEN-SYM, DM-TOKEN-ASYM, DM-RECEIPT-SYM **E** : OS-MKDK, SD-KMAC, SD-KDEK, SD-SENC, SD-SMAC	IND_1
Manage Content3	Update Pin to change the OS-GLOBALPIN	AES-CBC AES-CMAC	OS-GLOBALPIN OS-MKDK	CO	**W** : OS-GLOBALPIN **E** :	IND_1

Service	Description	Approved Security Functions	Keys and/or SSPs	Roles	Access rights to Keys and/or SSPs	Indicator
		AES-ECB	DEM-COM-EDK DEM-COM-MAC		OS-MKDK, DEM-COM-EDK, DEM-COM-MAC	
Module Info (Auth)	Read module configuration or status information (privileged data objects).	AES-CBC AES-CMAC	SD-SENC SD-SMAC	CO	**E** : SD-SENC, SD-SMAC	IND_1
Secure Channel	Establish and use a secure communications channel (AES CMAC with KBKDF)	AES-CBC AES-CMAC KTS Counter DRBG ESV KBKDF	OS-DRBG-EI OS-DRBG-S OS-DRBG-V OS-DRBG-KEY SD-KENC SD-KMAC SD-SENC SD-SMAC	CO	**E** : OS-DRBG-EI, OS-DRBG-S, OS-DRBG-V, OS-DRBG-KEY, SD-KENC, SD-KMAC, , SD-SENC, SD-SMAC **G**: SD-SENC, SD-SMAC **W**: OS-DRBG-V, OS-DRBG-KEY	IND_1
Digital Signature	Demonstrate RSA and ECDSA digital signature generation and verification	SHA2 RSA SigGen RSA SigVer ECDSA SigGen ECDSA SigVer Counter DRBG	OS-GLOBALPIN OS-DRBG-EI OS-DRBG-S OS-DRBG-V OS-DRBG-KEY OS-MKDK	USR	**E** : OS-DRBG-EI, OS-DRBG-S, OS-DRBG-V, OS-DRBG-KEY, OS-GLOBALPIN OS-MKDK DEM-SGV-PRI DEM-SGV-PUB	IND_1

Service	Description	Approved Security Functions	Keys and/or SSPs	Roles	Access rights to Keys and/or SSPs	Indicator
		ESV	DEM-SGV-PRI DEM-SGV-PUB		**W** :, OS-DRBG-S, OS-DRBG-V **R**: DEM-SGV-PRI DEM-SGV-PUB	
Generate Key Pair	Demonstrate RSA and ECC key generation	RSA KeyGen RSA KeyGen (CRT) ECDSA KeyGen Counter DRBG ESV CKG	OS-GLOBALPIN DEM-KGS-PUB DEM-KGS-PRI OS-DRBG-EI OS-DRBG-S OS-DRBG-V OS-DRBG-KEY OS-MKDK	USR	**E** : OS-GLOBALPIN DEM-KGS-PUB DEM-KGS-PRI OS-DRBG-KEY OS-MKDK OS-DRBG-EI, OS-DRBG-S, OS-DRBG-V, OS-DRBG-KEY **G** : DEM-KGS-PUB DEM-KGS-PRI **R** : DEM-KGS-PUB DEM-KGS-PRI **W**: DEM-KGS-PUB DEM-KGS-PRI OS-DRBG-S, OS-DRBG-V	IND_1

Service	Description	Approved Security Functions	Keys and/or SSPs	Roles	Access rights to Keys and/or SSPs	Indicator
					Z : DEM-KGS-PUB DEM-KGS-PRI	
ECC CDH Primitive	Demonstrate ECC Diffie-Hellman primitive	KAS-ECC-SSC	OS-GLOBALPIN DEM-KAP-PUB DEM-KAP-PRI OS-MKDK	USR	**E** : OS-GLOBALPIN DEM-KAP-PUB DEM-KAP-PRI OS-MKDK OS-DRBG-KEY **R** : DEM-KAP-PUB DEM-KAP-PRI :	IND_1
Symmetric Cipher	Demonstrate use of AES for encryption and decryption Demonstrate use of Triple-DES 3k for decryption for legacy	AES-CBC AES-ECB AES-CMAC TDES-CBC TDES-ECB	OS-GLOBALPIN OS-MKDK DEM-EDK	USR	**E** : OS-GLOBALPIN DEM-EDK OS-MKDK **R** : DEM-EDK **Z** : DEM-EDK	IND_1
Message Authentication	Demonstrate AES CMAC	AES CMAC	OS-GLOBALPIN OS-MKDK DEM-MAC	USR	**E** : OS-GLOBALPIN OS-MKDK DEM-MAC	IND_1
Key-Derivation Functions (KDF)	Demonstrate use of Keys diversification service	KDA HKDF SHA2	OS-GLOBALPIN	USR	**E** : OS-GLOBALPIN	IND_1

Service	Description	Approved Security Functions	Keys and/or SSPs	Roles	Access rights to Keys and/or SSPs	Indicator
	KDA HKDF KDA OneStep	KDA OneStep	OS-MKDK		OS-MKDK	
Compute HASH	Compute the hash value	SHA2 SHA3	OS-GLOBALPIN OS-MKDK	USR	**E** : OS-GLOBALPIN OS-MKDK	IND_1
Compute HashMac	Compute the hash mac value	HMAC-SHA2-256	OS-GLOBALPIN OS-MKDK	USR	**E** : OS-GLOBALPIN OS-MKDK	IND_1
Context	Select an applet or manage logical channels.	N/A	N/A	UA	N/A	IND_1
Module Info (Unauth)	Read unprivileged data objects, e.g., module configuration or status information.	N/A	N/A	UA	N/A	IND_1
Module Reset	Power cycle or reset the Module. Includes Integrity Self-Test, periodic self-test counter set up and self-test flag is reset	N/A	SD-SENC SD-SMAC	UA	**Z** : SD-SENC, SD-SMAC	IND_1
Run Cryptographic KAT	Sets a flag to that a specific cryptographic KATs has been performed on demand via Module Reset.	N/A	N/A	UA	N/A	IND_1

Service	Description	Approved Security Functions	Keys and/or SSPs	Roles	Access rights to Keys and/or SSPs	Indicator
Get Approved mode parameters	Get information on the approved mode of operation	N/A	N/A	UA	N/A	IND_1
Verify OS-GLOBALPIN	Verify the OS-GLOBALPIN	AES-ECB	OS-GLOBALPIN OS-MKDK	UA	**E** : OS-GLOBALPIN OS-MKDK	IND_1
Opacity Secure Channel	Establish a secure communications channel based on opacity	AES-CBC AES-CMAC SHA2 KDA OneStep KAS-ECC Counter DRBG	OS-DRBG-EI OS-DRBG-S OS-DRBG-V OS-DRBG-KEY OPACITY-SENC OPACITY-SMAC OPACITY-SRMAC OPACITY-SCONFIRMATION	UA	**E** : OS-DRBG-EI, OS-DRBG-S, OS-DRBG-V, OS-DRBG-KEY, OPACITY-SENC OPACITY-SMAC OPACITY-SRMAC OPACITY-SCONFIRMATION **G**: OPACITY-SENC OPACITY-SMAC OPACITY-SRMAC OPACITY-SCONFIRMATION **W**: OS-DRBG-S, OS-DRBG-V **Z** :	IND_1

Service	Description	Approved Security Functions	Keys and/or SSPs	Roles	Access rights to Keys and/or SSPs	Indicator
					OPACITY-SCONFIRMATION	

Table 14 –Approved Services

4.3 Authentication Methods

The module provides Identity-based authentication using either the Security Channel Protocol Authentication or the Demonstration Applet Authentication Method below.

The following table lists the roles supported by the cryptographic module as well as how they are authenticated:

Role ID	Authentication Method	Authentication Strength
CO	Secure Channel Protocol authentication method (Identity-based)	See below
USR	Demonstration applet Authentication Method (Identity-based)	See below
UA	N/A	N/A

Table 15 – Roles and Authentication

The Module does not support a maintenance role.

4.3.1 Secure Channel Protocol (SCP) Authentication (CO)

The CO role is authenticated to the module by an Open Platform Secure Channel Protocol authentication method. This method is performed when the EXTERNAL AUTHENTICATE command is invoked after successful execution of the INITIALIZE UPDATE command. The CO is individually and uniquely identified.

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). In accordance with SP 800-63B, this Authenticator type is best described as Single-Factor Cryptographic Software (Section 5.1.6).

The strength of Global Platform mutual authentication relies on AES key length, and the probability that a random attempt at authentication will succeed is:

- $\left(\frac{1}{2^{128}}\right)$ 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

The probability that a single random attempt will succeed with the smallest (16-byte long key) is $1/(2^{128})$. Additionally, the module also enforces a maximum count of 15 consecutive failed authentication attempts. After 15 consecutive unsuccessful attempts, the secure channel authentication is permanently blocked. All services that require the secure channel authentication return the status word: SW_SECURITY_STATUS_NOT_SATISFIED.

4.3.2 Demonstration Applet Authentication Method (USR)

The USR role is authenticate to the module by verifying a PIN value. This authentication method compares a PIN value sent to the Module over an encrypted channel to the stored OS-GLOBALPIN value; if the two values are equal, the operator is authenticated.

In accordance to SP 800-63B, this Authenticator type is best described as Memorized Secrets (Section 5.1.1).

The module enforces OS-GLOBALPIN string length of 8 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 $1/256^{8}$.
- Additionally, the module also enforces a maximum count of 15 consecutive failed authentication attempts of the Global PIN. After 15 consecutive unsuccessful attempts, the Global PIN verification is blocked permanently. All services that require the Global PIN verification will return the status word: SW_AUTHENTICATION_METHOD_BLOCKED.

5 Software/Firmware Security

The CM's firmware integrity is checked on startup and when periodic self-test period is over.

Periodic Self-Tests (PST) are performed and run the firmware integrity tests.

The integrity technique is based on EDC (CRC-16), which is approved for a hardware module. The firmware image size covered by the integrity technique is roughly 200 KB.

The integrity test can be triggered on demand by setting the specific flag with the proprietary command "autotest management".

Failure of firmware integrity self-tests during Periodic Self-Tests (PST) will trigger a module halt. Recovery from this state will require the module to be restarted and for the detected fault to have cleared. Otherwise, the module will re-halt during POST following restart. The module's FIPS error log is updated regarding the encountered issue and the card goes into an error state.

6 Operational Environment

The module includes a limited Operating Environment.

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.

7 Physical Security

The module is a hardware module claiming level 3 **physical security** and of embodiment single-chip.

The CM 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 *Module* is designed to be mounted in a plastic smartcard or similar package; physical inspection of the epoxy side of the Module is not practical after mounting.

Module Inspection:

Physical Security Mechanism	Recommended Frequency of Inspection/Test	Inspection/Test Guidance Details
Physical inspection of module surfaces for signs of tamper.	On receipt of module following transport. Before each module use	In the event of any observed damage, photograph the card and contact Thales to confirm whether observed anomalies are to be expected or are confirmed signs of potential tampering

Table 16 - Physical Security Inspection Guidelines

The normal operating conditions of use are the following:

Conditions	Range
Voltage	1.8V-5V
Temperature	-25°C/+85°C

Table 17 - Voltage and Temperature Ranges

The module's hardware is designed to sense and respond to out-of-range temperature conditions as well as out-of-range voltage conditions. The temperature and voltage conditions are only monitored in the powered-on state.

The module supports an EFP mechanism that will trigger module shutdown if low or high temperature extremes and out-of-range voltage conditions are detected whilst the module is active.

In the event that the module senses an out-of-range temperature or over voltage the module will reset itself, clearing all working memory.

The module can be reset and placed back into operation when in-bound operating conditions have been restored .

The following table covers the limits enforced by the module:

	Temperature or voltage measurement	Specify EFP or EFT	Specify if this condition results in a shutdown or zeroisation
Low Temperature	-45°C	EFP	Shutdown
High Temperature	+130°C	EFP	Shutdown
Low Voltage	1.6 V	EFP	Shutdown
High Voltage	5.5 V	EFP	Shutdown

Table 18 - EFP/EFT

The following table lists the temperature tested during the assessment of the module:

	Hardness tested temperature measurement
Low Temperature	-45°C, -25°C
High Temperature	+85ºC, +130°C

Table 19 - Hardness testing temperature ranges

8 Non-invasive security

No assured mitigations to ‘other attacks’ are covered in this security policy.

9 Sensitive security parameter management

All SSPs used by the CM are described in this section. All usages of these SSPs by the CM are described in the services. In addition, all keys stored in RAM are zeroized upon power-cycle of the CM.

The following table lists Sensitive Security Parameters (SSP) used to perform approved security function supported by the cryptographic module.

The following notes should be observed when reading the table:

- Keys with the “SD” prefix pertains 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
- The “PRI” suffix indicates that this is a private key
- The “PUB” suffix indicates that this is a public key
- The “SYM” suffix indicates that this is a symmetric key
- The “ASYM” suffix indicates that this is an asymmetric key
- Keys with the “DEM” prefix are used by the demonstration applet

The methods to zeroise SSPs, using the relevant CM services, are described below:

-Power-cycling the module: Explicit zeroization method using the Module Reset service, the CM is able to destroy the SSPs by overwriting with zero values (in RAM memory).

-Closing SCP secure channel: Explicit zeroization method using the Secure Channel service of the CO, the CM is able to destroy the SSPs of this service, at the closing of SCP secure channel by overwriting with zero values.

-**Module entering TERMINATED state**: Explicit zeroization method using the Manage Content / Lifecycle service of the CO, the CM is able to enter the TERMINATED state, through the Set Status command, destroying the SSPs by overwriting with zero values.

-Uninstallation of demonstration applet: Explicit zeroization method using the Manage Content / Delete service of the CO, the CM is able to destroy the SSPs of the demonstration applet, through the Delete command (uninstall method).

Indication of success is determined by the status response 90 00.

As per FIPS 140-3 IG D.L, the DRBG parameters Entropy Input String (“OS-DRBG-EI”), Seed (“OS-DRBG-S”), DRBG Internal State values V and Key (“OS-DRBG-V” and “OS-DRBG-KEY”) are considered CSPs by the module.

9.1 Sensitive Security Parameters Summary

Key / SSP Name / Type	Strength	Security Function and Cert Number	Generation	Import/ Export	Establishment	Storage	Zeroisation	Use and Related Keys
OS-DRBG-EI / Entropy Input / CSP	256 bits	ESV Cert. #E107	Generated on module using ESV	N/A	N/A	plaintext in RAM	Module entering TERMINATED state	1024-bit random drawn by the approved entropy source described in section 9.2 of the SP and used as entropy input for the [SP 800-90A] DRBG implementation Used by the SCP authentication
OS-DRBG-S / Seed / CSP	256 bits	DRBG Cert. #A2877	Constructed as per SP 800-90A	N/A	N/A	plaintext in RAM	Power-cycling the module Module entering TERMINATED state	48 byte seed output from AES_DF used for instantiation of the [SP800-90A] DRBG implementation Used by the SCP authentication

Key / SSP Name / Type	Strength	Security Function and Cert Number	Generation	Import/ Export	Establishment	Storage	Zeroisation	Use and Related Keys
OS-DRBG-V / DRBG "V" value / CSP	128 bits	DRBG Cert. #A2877	Constructed as per SP 800-90A	N/A	N/A	plaintext in RAM	Power-cycling the module Module entering TERMINATED state	16-byte AES state V used in the [SP 800-90A] CTR DRBG implementation Used by the SCP authentication
OS-DRBG-KEY / DRBG "Key" value / CSP	256 bits	DRBG Cert. #A2877	Constructed as per SP 800-90A	N/A	N/A	plaintext in RAM	Power-cycling the module Module entering TERMINATED state	32-byte AES key used in the [SP 800-90A] CTR DRBG implementation Used by the SCP authentication

Key / SSP Name / Type	Strength	Security Function and Cert Number	Generation	Import/ Export	Establishment	Storage	Zeroisation	Use and Related Keys
OS-GLOBALPIN / global PIN / CSP	N/A	N/A	Pre-loaded during manufacturing	Input using Manage Content service, encrypted by SD-KDEK	N/A	Stored encrypted (AES-ECB) by OS-MKDK in FLASH	Module entering TERMINATED state by OS-MKDK zeroisation	8 to 16 byte Global PIN value managed by the CO. Character space is not restricted by the module. The PIN Policy is managed by the applet. Used by the Demonstration Applet Authentication Method (USR role)
OS-MKDK / Encryption key / CSP	128 bits	AES-ECB Cert. #A2877	Pre-loaded during manufacturing using chip-internal data	N/A	N/A	Stored in plaintext in FLASH	Module entering TERMINATED state	Encrypts OS-GLOBALPIN Used by the Demonstration Applet Authentication Method (USR role)

Key / SSP Name / Type	Strength	Security Function and Cert Number	Generation	Import/ Export	Establishment	Storage	Zeroisation	Use and Related Keys
SD-KENC / Decryption Key / CSP	128, 192, 256 bits	AES-CBC Cert. #A2877	N/A	Entered using PUT KEY, encrypted by SD-KDEK; key identifier entity association. An initial value is loaded during manufacturing	N/A	Stored in plaintext in FLASH	Module entering TERMINATED state	AES-128/192/256 master key used by the CO role to derive SD-SENC Used by the SCP authentication
SD-KMAC / Signature verification Key / CSP	128, 192, 256 bits	AES-CMAC Cert. #A2877	N/A	Entered using PUT KEY, encrypted by SD-KDEK; key identifier entity association. An initial value is loaded during manufacturing	N/A	Stored in plaintext in FLASH	Module entering TERMINATED state	AES-128/192/256 master key used by the CO role to derive SD-SMAC Used by the SCP authentication

Key / SSP Name / Type	Strength	Security Function and Cert Number	Generation	Import/ Export	Establishment	Storage	Zeroisation	Use and Related Keys
SD-KDEK / Encryption Decryption Key / CSP	128, 192, 256 bits	AES-CBC Cert. #A2877	N/A	Entered using PUT KEY, encrypted by SD-KDEK; key identifier entity association. An initial value is loaded during manufacturing	N/A	Stored in plaintext in FLASH	Module entering TERMINATED state	AES-128/192/256 decryption encryption key used by the CO role to decrypt/encrypt sensitive data Can be used to wrap SD-KENC, SD-KDEK, SD-KMAC, DAP-SYM, DM-TOKEN-SYM, DM-RECEIPT-SYM, DAP-ASYM and DM-TOKEN-ASYM SSPs
SD-SENC / Session Decryption Key / CSP	128, 192, 256 bits	AES-CBC Cert. #A2877	Derived on module using KBKDF, in accordance with SCP03 specification	N/A	N/A	plaintext in RAM	Power-cycling the module Closing SCP secure channel	AES-128/192/256 (SCP03) Session encryption key used by the CO role to encrypt / decrypt secure channel data Used by the SCP authentication

Key / SSP Name / Type	Strength	Security Function and Cert Number	Generation	Import/ Export	Establishment	Storage	Zeroisation	Use and Related Keys
SD-SMAC / Session Signature verification Key / CSP	128, 192, 256 bits	AES-CMAC Cert. #A2877	Derived on module using KBKDF, in accordance with SCP03 specification	N/A	N/A	plaintext in RAM	Power-cycling the module Closing SCP secure channel	AES-128/192/256 (SCP03) Session MAC key used by the CO role to verify secure channel data integrity Used by the SCP authentication
DAP-SYM / Signature verification key / CSP	128, 192, 256 bits	AES-CMAC Cert. #A2877	N/A	Entered using PUT KEY, encrypted by SD-KDEK; key identifier entity association. An initial value is loaded during manufacturing	N/A	Stored in plaintext in FLASH	Module entering TERMINATED state	AES-128/192/256 DAP key optionally loaded in the field and used to verify the CMAC signature of packages loaded into the Module
DM-TOKEN-SYM / Delegate Management Signature verification key / CSP	128, 192, 256 bits	AES-CMAC Cert. #A2877	N/A	Entered using PUT KEY, encrypted by SD-KDEK; key identifier entity association. An initial value is loaded during manufacturing	N/A	Stored in plaintext in FLASH	Module entering TERMINATED state	AES-128/192/256 Delegate Management Token symmetric key

Key / SSP Name / Type	Strength	Security Function and Cert Number	Generation	Import/ Export	Establishment	Storage	Zeroisation	Use and Related Keys
DM-RECEIPT-SYM / Delegate Management Signature generation Key / CSP	128, 192, 256 bits	AES-CMAC Cert. #A2877	N/A	Entered using PUT KEY, encrypted by SD-KDEK; key identifier entity association. An initial value is loaded during manufacturing	N/A	Stored in plaintext in FLASH	Module entering TERMINATED state	AES-128/192/256 Delegate Management symmetric key to compute receipt
DAP-ASYM / Signature verification Key / PSP	112 bits (2048 bits length)	RSA SigVer Cert. #A2877	N/A	Entered using PUT KEY, encrypted by SD-KDEK; key identifier entity association. An initial value (if necessary) is loaded during manufacturing	N/A	Stored in plaintext in FLASH	Module entering TERMINATED state	2048-bit public part of RSA key pair used for Asymmetric Signature verification used to verify the signature of packages loaded into the Module

Key / SSP Name / Type	Strength	Security Function and Cert Number	Generation	Import/ Export	Establishment	Storage	Zeroisation	Use and Related Keys
OPACITY-SENC / OPACITY session Encryption Decryption Key / CSP	128 bits	AES-CBC Cert. # A2877	Derived using KDA OneStep	N/A	N/A	Stored in plaintext in RAM	Power-cycling the module Closing SCP secure channel	Card OPACITY Secure Messaging Session Encryption Key: Symmetric AES-128/256 used during Secure Messaging session for data encryption
OPACITY-SMAC / OPACITY session Signature verification key/ CSP	128 bits 256 bits	AES CMAC Cert. # A2877	Derived using KDA OneStep	N/A	N/A	Stored in plaintext in RAM	Power-cycling the module Closing SCP secure channel	Card OPACITY Secure Messaging Session MAC Key: Symmetric AES-128/256 used during Secure Messaging session for input MAC verification

Key / SSP Name / Type	Strength	Security Function and Cert Number	Generation	Import/ Export	Establishment	Storage	Zeroisation	Use and Related Keys
OPACITY-SRMAC / OPACITY session Signature generation key / CSP	128 bits 256 bits	AES-CMAC Cert. # A2877	Derived using KDA OneStep	N/A	N/A	Stored in plaintext in RAM	Power-cycling the module Closing SCP secure channel	Card OPACITY Secure Messaging Session Response MAC Key: Symmetric AES-128/256 used during Secure Messaging session for response MAC computation
OPACITY-SCONFIRMATION / OPACITY session Signature generation confirmation key / CSP	128 bits 256 bits	AES-CMAC Cert. # A2877	Derived using KDA OneStep	N/A	N/A	Stored in plaintext in RAM	Power-cycling the module Automatically zeroised after cryptogram computation occurring during secure channel establishment	Card OPACITY Secure Messaging Session Confirmation Key: Symmetric AES-128/256 used during Secure Messaging session establishment.

Key / SSP Name / Type	Strength	Security Function and Cert Number	Generation	Import/ Export	Establishment	Storage	Zeroisation	Use and Related Keys
DM-TOKEN-ASYM / Delegate Management Signature verification Key / CSP	112 bits (2048 bits length)	RSA SigVer Cert. #A2877	N/A	Entered using PUT KEY, encrypted by SD-KDEK; key identifier entity association. An initial value (if necessary) is loaded during manufacturing	N/A	Stored in plaintext in FLASH	Module entering TERMINATED state	RSA 2048-bit Asymmetric key for Delegate Management for token verification

Key / SSP Name / Type	Strength	Security Function and Cert Number	Generation	Import/ Export	Establishment	Storage	Zeroisation	Use and Related Keys
DEM-EDK / Demonstration Applet Encryption Decryption Key / CSP	128, 192, and 256 bits 168-bits for TDES (decrypt only)	AES-ECB AES-CBC TDES-ECB (decrypt only) TDES-CBC (decrypt only) Cert. #A2877	N/A	SP 800-38F KTS. Entered or exported encrypted by DEM-EDK and authenticated with DEM-MAC	N/A	Stored in plaintext in FLASH	Uninstallation of demonstration applet	Demonstration Applet: AES-128 encryption / decryption key, or Triple-DES decryption key used by the Demonstration Applet for Symmetric Cipher service used to encrypt/decrypt DEM-EDK, DEM-MAC, DEM-SGV-PRI, DEM-KAP-PRI, DEM-KGS-PRI, DEM-KAP-PUB, DEB-KGS-PUB and DEM-SGV-PUB

Key / SSP Name / Type	Strength	Security Function and Cert Number	Generation	Import/ Export	Establishment	Storage	Zeroisation	Use and Related Keys
DEM-MAC / Demonstration Applet Signature & Verification key / CSP	128, 192, and 256 bits	AES-CMAC Cert. #A2877	N/A	SP 800-38F KTS. Entered or exported encrypted by DEM-EDK and authenticated with DEM-MAC	N/A	Stored in plaintext in FLASH	Uninstallation of demonstration applet	Demonstration Applet: AES-128 key used by Demonstration Applet for Message Authentication service. used to authenticate SSPs encrypted using DEM-EDK, like DEM-EDK, DEM-MAC, DEM-SGV-PRI, DEM-KAP-PRI, DEM-KGS-PRI, DEM-KAP-PUB, DEB-KGS-PUB and DEM-SGV-PUB
DEM-COM-EDK / Demonstration Applet Secure Channel Encryption & Decryption Key / CSP	128, 192, and 256 bits	AES-ECB AES-CBC Cert. #A2877	N/A	SP 800-38F KTS. Entered during manufacturing (initial value), using Manage Content service. Not exported	N/A	Stored in plaintext in FLASH	Uninstallation of demonstration applet	Demonstration Applet: AES-128 encryption / decryption key used by the Demonstration Applet for secure communication

Key / SSP Name / Type	Strength	Security Function and Cert Number	Generation	Import/ Export	Establishment	Storage	Zeroisation	Use and Related Keys
DEM-COM-MAC / Demonstration Applet Secure Channel Signature & Verification key / CSP	128, 192, and 256 bits	AES-CMAC Cert. #A2877	N/A	SP 800-38F KTS. Entered during manufacturing (initial value), using Manage Content service. Not exported	N/A	Stored in plaintext in FLASH	Uninstallation of demonstration applet	Demonstration applet: AES-128 key used by Demonstration Applet to compute signature for secure communication
DEM-SGV-PRI / Demonstration Applet Signature generation – Private key/ CSP	RSA: 112, 128, 150 bits (2048-, 3072-, 4096-bit length) ECDSA: 112, 128, 192, 256 bits (P-224, P-256, P-384, P-521)	RSA SigGen, ECDSA SigGen Cert. #A2877	Generated on module using approved Key Generation	SP 800-38F KTS. Entered or exported encrypted by DEM-EDK and authenticated with DEM-MAC	N/A	Stored in plaintext in FLASH	Uninstallation of demonstration applet	Demonstration applet: 2048-, 3072-, 4096-bit RSA or P-224, P-256, P-384, P-521 ECDSA private key used by Demonstration Applet for Digital Signature service

Key / SSP Name / Type	Strength	Security Function and Cert Number	Generation	Import/ Export	Establishment	Storage	Zeroisation	Use and Related Keys
DEM-KAP-PRI / Demonstration Applet – Key generation – Private key / CSP	112, 128, 192, 256 bits (P-224, P-256, P-384, P-521)	KAS-ECC Cert. #A2877	Generated on module using approved Key Generation	SP 800-38F KTS. Entered or exported encrypted by DEM-EDK and authenticated with DEM-MAC	N/A	Stored in plaintext in FLASH	Uninstallation of demonstration applet	Demonstration applet: P-224, P-256, P-384, P-521 ECC private key used by the Demonstration Applet Generate Key Pair and Key Agreement Primitive Services
DEM-KGS-PRI / Demonstration Applet Key generation – Private key / CSP	112 bits (2048-bit length)	RSA SigGen Cert. #A2877	Generated on module using approved Key Generation	SP 800-38F KTS. Entered or exported encrypted by DEM-EDK and authenticated with DEM-MAC	N/A	Stored in plaintext in FLASH	Uninstallation of demonstration applet	Demonstration applet: 2048-bit RSA used by Demonstration Applet Generate Key Pair
DEM-KAP-PUB / Demonstration Applet Key generation – Public key / PSP	112, 128, 150 bits (P-224, P-256, P-384, P-521)	KAS-ECC Cert. #A2877	Generated on module using approved Key Generation	SP 800-38F KTS. Entered or exported encrypted by DEM-EDK and authenticated with DEM-MAC	N/A	Stored in plaintext in FLASH	Uninstallation of demonstration applet	Demonstration applet : P-224, P-256, P-384, P-521 ECC public key used by the Demonstration Applet Key Agreement Service

Key / SSP Name / Type	Strength	Security Function and Cert Number	Generation	Import/ Export	Establishment	Storage	Zeroisation	Use and Related Keys
DEM-KGS-PUB / Demonstration Applet Key generation – Public key / PSP	112 bits (2048-bit length)	RSA SigVer Cert. #A2877	Generated on module using approved Key Generation	SP 800-38F KTS. Exported from the module encrypted by DEM-EDK and authenticated with DEM-MAC	N/A	Stored in plaintext in FLASH	Uninstallation of demonstration applet	Demonstration applet : 2048-bit RSA public key used by Demonstration Applet Generate Asymmetric Key Pair
DEM-SGV-PUB / Demonstration Applet Signature generation – Public key / PSP	RSA: 112, 128, 150 bits (2048-, 3072-, 4096-bit length); ECDSA: 112, 128, 192, 256 bits (P-224, P-256, P-384, P-521)	RSA SigVer, ECDSA SigVer Cert. #A2877	Generated on module using approved Key Generation	SP 800-38F KTS. Exported from the module encrypted by DEM-EDK and authenticated with DEM-MAC	N/A	Stored in plaintext in FLASH	Uninstallation of demonstration applet	Demonstration applet: 2048-, 3072-, 4096-bit RSA or P-224, P-256, P-384, P-521 ECDSA public key used by Demonstration Applet Asymmetric Signature service

Table 20 – SSPs

9.2 Random bit generator entropy sources

The module includes a non-deterministic Random Number Generator within the cryptographic boundary. This non-deterministic RNG (also called TRNG) is used exclusively to feed the approved DRBG with entropy:

Entropy sources	Minimum number of bits of entropy	Details
SLC37 32-bit Security Controller	Min-entropy claimed: 13.376 bits per 32-bit blocks.	Provided by the hardware TRNG of the SLC37 chip from Infineon.

Table 21 – Non-Deterministic Random Number Generation Specification

ESV certificate (#E107) has been procured for this entropy source. As per the Public Use Document for #E107, the settings under the Configuration Settings section are followed to by the factory prior to delivery of the module for operating the entropy source in a compliant manner.

The output of the entropy source is used to directly feed the DRBG. The DRBG uses CTR_DRBG from [SP800-90Ar1] with Derivation Function (DF) enabled. 1024-bits of entropy at 13.376 bits per 32-bits min-entropy are fed to the DF which accounts for 428.032 -bits of entropy which exceed the 256-bits required by CTR_DRBG to claim full entropy output of the DRBG. A separate nonce is created for the DRBG based on output from entropy source.

10 Self-tests

10.1 Pre-Operational Self-Tests

On power-on or reset, the *Module* performs integrity testing using an EDC (16-bit CRC) performed over all code located in FLASH and EEPROM memory (for OS and Applets).

All flags for cryptographic algorithm self-tests are cleared.

10.2 Conditional Self-Tests

10.2.1 Conditional Cryptographic Algorithm Tests

The module maintains a flag in RAM memory that stores the state (self-test passed or not) for each Cryptographic algorithm that is approved.

This flag indicates if an algorithm has been already self-tested.

The Module performs self-test of an algorithm prior the first operational use (corresponding flag is not set) and if the self-test succeeds, the corresponding flag is set otherwise the card logs the self-test error and entered into a *Card Is Mute* error state or *Card is Killed* error state, depending on number of failures.

On each reset of the CM, it performs only “Firmware Integrity test”. The cryptographic KATs are executed automatically, in a mode named “on demand”, when a cryptographic service is requested.

Self-tests can be also played by any operator using the “autotests management” APDU command, corresponding to the “Run Cryptographic KAT” service. The operator can choose the list of self-test execution giving in data of the APDU the self-test flag.

Self-Tests are based on known answer tests (KATs):

Test Target	Description
AES	ECB decrypt KAT with 128-bit key. Encrypt is self-tested as a part of KBKDF KAT.
DRBG	Counter DRBG KAT as per SP 800-90A section 11.3 with nonce (48 bytes) and entropy (128 bytes).
ECDSA Signature Generation	Signature generation KAT using an ECC P-224 key.
ECDSA Signature Verification	Signature verification KAT using an ECC P-224 key.
ESV	SP 800-90B Repetition Count Test and Adaptive Proportion Test
HMAC-SHA2-256	HMAC-SHA2-256 KAT.
KAS-ECC	OnePassDH CS2 shared secret computation KAT using an ECC P-256 key with SHA2-256.

Test Target	Description
KAS-ECC	OnePassDH CS7 shared secret computation KAT using an ECC P-384 key with SHA2-384.
KAS-ECC-SSC	Primitive 'Z' Computation KAT using an ECC P-224 key.
KBKDF	KBKDF KAT using AES-CMAC 128-bit key and 32-byte derivation data.
KDA OneStep	SP 800-56Cr2 One Step KDF KAT.
KDA HKDF	SP 800-56Cr2/RFC5869 HKDF KAT.
RSA Signature Generation	RSA PKCS#1 v1.5 signature generation KAT using an RSA 2048-bit key RSA PKCS#1 v1.5 signature generation KAT using the RSA CRT implementation with a 2048-bit key.
RSA Signature Verification	RSA PKCS#1 v1.5 signature verification KAT using an RSA 2048-bit key RSA PKCS#1 v1.5 signature verification KAT using the RSA CRT implementation with a 2048-bit key. RSA PKCS#1 v1.5 decryption KAT with a 2048-bit key is also performed
SHA2-256	SHA2-256 KAT.
SHA2-512	SHA2-512 KAT.
SHA3-224	SHA3-224 KAT.
Triple-DES	ECB decrypt KAT.

Table 22 –Conditional Algorithm Self-Tests

10.2.2 Conditional Pair-wise Consistency Tests

When any asymmetric key pair is generated, the CM performs a pairwise consistency test. For RSA keys, the pairwise consistency test is based on keys encryption / decryption. For ECC keys, the pairwise consistency test is based on signature / verify.

10.2.3 Conditional Firmware Load Tests

When new firmware (applet) is loaded into the CM (or into a SSD having the Delegated Management privilege) using the Manage content service, the CM (or the SSD) verifies the authenticity (MAC or signature) of the new firmware (applet) using respectively the DAP-SYM key or DAP-ASYM key. The signature or MAC in this scenario is generated by an external entity using the key corresponding to the asymmetric key DAP-ASYM or the secret key DAP-SYM.

10.2.4 Conditional Critical Functions Tests

The module performs a validity check of the public static key and the ephemeral keys according to the SP 800-56Ar3 specification.

10.3 Periodic Self-tests

The Module supports an internal counter and an associated maximum value. The counter is set to its maximum value on power on and it is decremented when receiving an APDU.

When the counter reaches its zero, the integrity test is executed (see 10.1), the counter is reset to its maximum value again and the flag for on-demand tests is also reset so that at next cryptographic algorithm usage, the self-tests are executed again (see 10.2.1). No interruption to the module's operation is expected while the self-tests are executed.

11 Life-cycle assurance

The CM meets the Level 3 Design Assurance section requirements.

11.1 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. Once the module has been delivered outside of the factory, the CM is always in the Compliant state. Once the module has been powered on, it always functions in the approved mode of operation. There are no additional steps for installation, initialization, and configuration required for the CM after delivery. The configuration cannot be changed outside the factory.

11.2 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, Services, and Authentication chapter.

11.3 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 SSPs.
- Data output is inhibited during key generation, self-tests, zeroisation, and error states.
- The zeroisation service is applied with no restrictions on all keys or SSPs of the CM.
- The *Module* does not support manual key entry, output plaintext SSPs or output intermediate key values.
- Status information does not contain SSPs or sensitive data that if misused could lead to a compromise of the Module.

12 Mitigation of Other Attacks

No assured mitigations to ‘other attacks’ are covered in this security policy.

END OF DOCUMENT