THALES

nShield Remote Administration Token

FIPS 140-2 Cryptographic Module Security Policy

Document Number: LSEC0508
Document Version: D6.2
Date: 2016-09-26

Prepared by:

athena Smartcard

Table of Contents

List of Tables

List of Figures

References

Table 1: References

Abbreviation	Full Specification Name
[FIPS140-2]	NIST, *Security Requirements for Cryptographic Modules*, May 25, 2001
[GlobalPlatform]	*GlobalPlatform Consortium:* http://www.globalplatform.org *GlogbalPlatform, Card Specification, Version 2.2.1, Jan2011* *Confidential Card Content Management, Amendment A, Jan2011* *Secure Channel Protocol 03, Amendment D, version 1.1, Sep2009* *Security Upgrade for Card Content Management, Amendment E version 1.0, Nov2011*
[ISO7816]	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*
[ISO7816-5]	ISO/IEC 7816-5: 2004 *Identification cards -- Integrated circuit cards -- Part 5: Registration of application providers*
[JavaCard]	*Java Card 3.0.4 Runtime Environment (JCRE) Specification* *Java Card 3.0.4 Virtual Machine (JCVM) Specification* *Java Card 3.0.4 Application Programming Interface* Published by Sun Microsystems, September 2011
[SP800-131A]	*Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths*, January 2011
[FIPS113]	NIST, *Computer Data Authentication*, FIPS Publication 113, 30 May 1985
[FIPS197]	NIST, *Advanced Encryption Standard (AES)*, FIPS Publication 197, November 26, 2001
[PKCS#1]	*PKCS #1 v2.1: RSA Cryptography Standard*, RSA Laboratories, June 14, 2002
[FIPS186-4]	NIST, *Digital Signature Standard (DSS)*, FIPS Publication 186-4, July 2013
[SP800-56A]	NIST Special Publication 800-56A, *Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography*, March 2007
[FIPS180-4]	NIST, *Secure Hash Standard*, FIPS Publication 180-4, March 2012
[SP800-90A]	NIST Special Publication 800-90A, *Recommendation for Random Number Generation Using Deterministic Random Bit Generators*, January 2012
[SP800-38B]	NIST, *Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication,* May 2005
[SP800-38F]	NIST, *Recommendation for Block Cipher Modes of Operation: Methods for Key Wrapping,* December 2012
[SP800-89]	NIST, *Recommendation for Obtaining Assurances for Digital Signature Applications,* November 2006
[IG]	NIST, *Implementation Guidance for FIPS PUB 140-2 and the Cryptographic Module Validation Program,* last updated 25 July 2013

Acronyms and Definitions

Table 2: Acronyms and Definitions

Acronym	Definition
APDU	Application Protocol Data Unit, see [ISO 7816]
API	Application Programming Interface
CM	Card Manager, see [GlobalPlatform]
CSP	Critical Security Parameter, see [FIPS 140-2]
DAP	Data Authentication Pattern, see [GlobalPlatform]
DPA	Differential Power Analysis
ECC CDH	Elliptic Curve Cryptography Cofactor Diffie-Hellman
HSM	Hardware Security Module; the secure engine associated with host processes.
IC	Integrated Circuit
ISD	Issuer Security Domain, see [GlobalPlatform]
KAT	Known Answer Test
NVM	Non-Volatile Memory (e.g., EEPROM, Flash)
OP	Open Platform (predecessor to GlobalPlatform)
PCT	Pairwise Consistency Test
PKI	Public Key Infrastructure
SCP	Secure Channel Protocol, see [GlobalPlatform]
SPA	Simple Power Analysis
TPDU	Transaction Protocol Data Unit, see [ISO7816]
Warrant	Thales proprietary certificate which links the Serial Number of the module to a public key.

1 Overview

1.1 Module Description

This document defines the Security Policy for the Thales e-Security nShield Remote Administration Token cryptographic module, hereafter denoted *the Module*. The Module, validated to FIPS 140-2 overall Level 3, is a single chip smart card micro-controller implementing the Global Platform operational environment, with Card Manager and the Authentication Token Applet.

The Authentication Token Applet provides the nShield specific authentication token functionality by supporting secure communication with an HSM and token share storage services. It is logically comprised of 2 Java Card Applets:

1. MercuryApplet: sets up the secure channel to the remote HSM
2. CardAdminApplet: card administration including production

1.2 Compliance

The Module implementation is compliant with the following standards for the Platform:

- [JavaCard]
- [GlobalPlatform]
- [ISO7816] Parts 1-4

The Java Card API is an internal API utilized by the Applet in order to execute services provided by the Platform. The Java Card API is not exposed to external applications or end users.

During the FIPS 140-2 conformance testing, the module as a whole (both the Platform and the Applet) is tested against the requirements of FIPS 140-2. Verifying the Module's Approved mode of operation necessitates verifying the Approved mode of operation of both the Platform and the Applet. (Note that the Module always runs in the Approved mode of operation.)

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

1.3 Security Levels

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

Table 3: Security Level of Security Requirements

Security Requirement	Level
Cryptographic Module Specification	3
Cryptographic Module Ports and Interfaces	3
Roles, Services, and Authentication	3
Finite State Model	3
Physical Security	4
Operational Environment	N/A
Cryptographic Key Management	3
EMI/EMC	3
Self-Tests	3
Design Assurance	3
Mitigation of Other Attacks	3

1.4 Versions, Configurations and Modes of Operation

Hardware: NXP P60D144

Firmware: Athena IDProtect 0501.5175.0001 with Authentication Token Applet 1.0

1.4.1 Mode of Operation

The Module always runs in the Approved mode of operation.

Verifying the Module's Approved Mode of Operation involves separately verifying the Approved mode of operation for both the Platform and the Applet using the Manage Content service.

To verify that the **Platform** is in the Approved mode of operation, use the Manage Content service to SELECT the ISD and send a GET DATA command with the CPLC Data tag '9F7F' and verify that the returned data contains fields as follows (other fields are not relevant here). This verifies the version of the operating system.

Table 4: Versions and Mode of Operation Indicators (Platform)

Data Element	Value (hex)	Associated Version
IC type	`0501`	TBD
Operating system release date	`5175`	Firmware Version Part 1
Operating system release level	`0001`	Firmware Version Part 2

To verify that the **Applet** is in the Approved mode of operation, use the Manage Content service to SELECT the Card admin applet and send a 'Get_software_version' command and verify that the returned data contains the field as follows. This verifies the version of the Applet.

Table 5: Versions and Mode of Operation Indicators (Applet)

Data Element	Value (hex)	Associated Version
Software Version	`0100`	Authentication Token Applet 1.0

1.5 Hardware and Physical Cryptographic Boundary

The Module is designed to be embedded into a smart card. The physical form of the Module is depicted in Figure 1; the red outline depicts the physical cryptographic boundary, representing the surface of the chip and the bond pads. The cross-hatching indicates the presence of active tamper shields. In production use, the Module is attached to a frame connected to the physical ports. The Module will be enclosed in epoxy, for example, as a smart card module.

The Module is designed to be embedded into plastic card bodies, with a contact plate. The physical form of the Module is depicted in Figure 1 (to scale); the red outline depicts the physical cryptographic boundary, representing the surface of the chip and the bond pads. The cross-hatching indicates the presence of active and passive tamper shields. In production use, the Module is delivered to either vendors or end user customers in various forms:

- As bare die in wafer form for direct chip assembly by wire bonding or flip chip assembly
- Wire bonded and encapsulated by epoxy with additional packaging (e.g., Contact only Modules; SMD packages)

The Module relies on [ISO7816] and card readers as input/output devices.

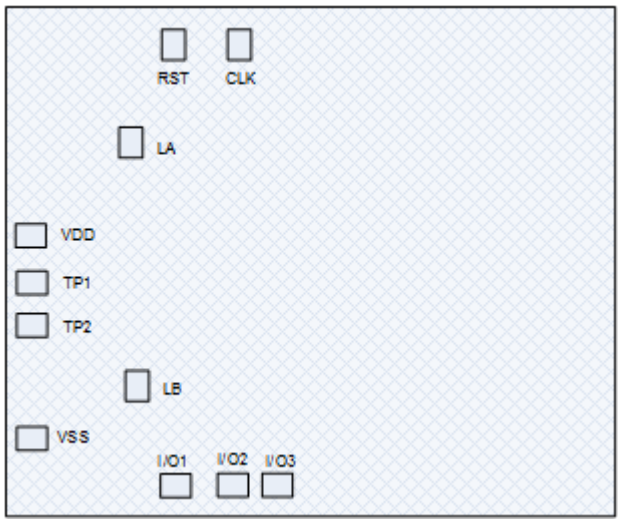

Figure 1: Thales nShield: Physical Form

1.5.1 Ports and Interfaces

The Module functions as a slave processor to process and respond to commands. Up to 256 bytes of data can be exchanged through one TPDU command.

Table 6: Ports and Interfaces

Port	Description	Logical Interface Type
VSS	ISO 7816: Ground	Power
VCC	ISO 7816: Supply voltage	Power
RST	ISO 7816: Reset	Control in
CLK	ISO 7816: Clock	Control in
I/O1	ISO 7816 communication pads: Input/Output	Control in, Data in, Data out, Status out
I/O2 and 3	Serial port (not connected)	N/A
LA, LB	RF interface antenna pads (not connected)	N/A
TP1	Programmable I/O (not connected)	N/A
TP2	Programmable I/O (not connected)	N/A

1.6 Firmware and Logical Cryptographic Boundary

Figure 2 depicts the Module operational environment. The Applet in the figure is the Authentication Token Applet.

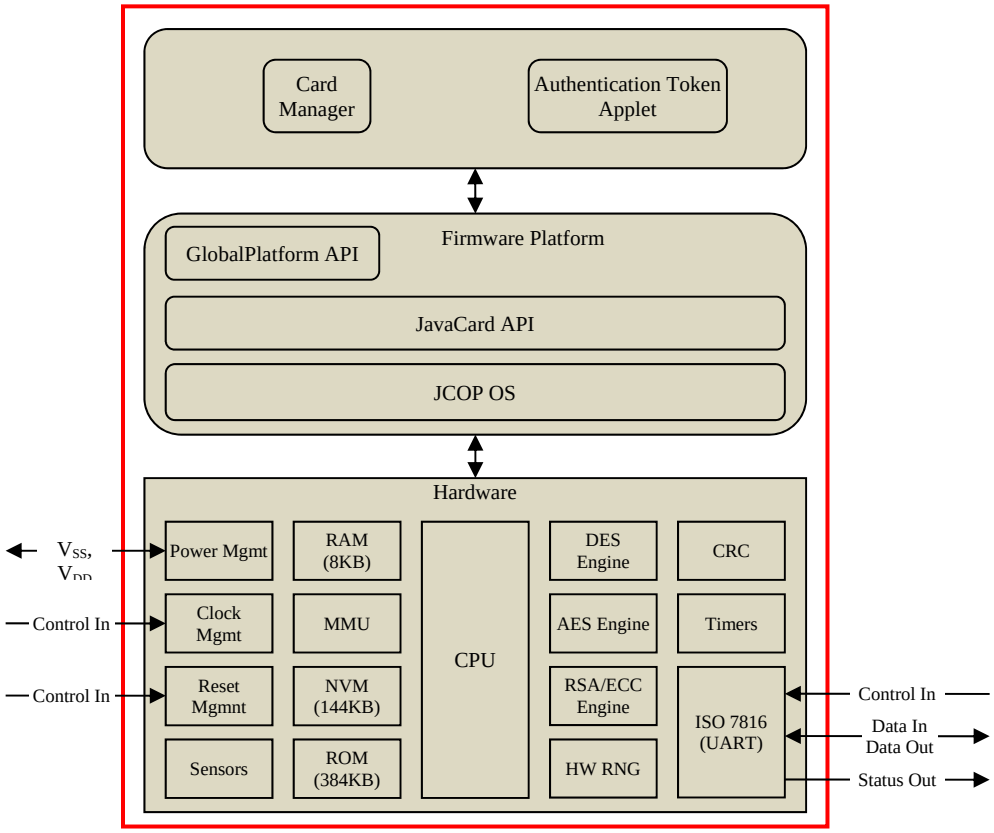

Figure 2: Module Block Diagram

- The ISO 7816 UART supports the T=0 and T=1 communications protocol variants
- The Modules has 144KB of NVM, 384KB of ROM, and 8KB of RAM.

Section 3 describes applet functionality in greater detail. The JavaCard and Global Platform APIs are internal interfaces available to applets. Only applet services are available at the card edge (the interfaces that cross the cryptographic boundary).

2 Cryptographic Functionality

The Module implements the Approved and non-Approved but allowed cryptographic functions listed in Table 7 and Table 9 below. The functions listed in Table 8 are not available for use in the module configuration under validation.

Table 7: Approved Cryptographic Functions Used in the Module

Algorithm	Description	Cert. #
AES	[FIPS 197] Advanced Encryption Standard algorithm. The module supports 128 and 256-bit key length and ECB and CBC modes.	3780
AES CMAC	[SP800-38B] AES-256 CMAC	3780
AES KDF	[SP800-108] AES-256 CMAC KDF	KBKDF 82
AES Key Wrap (KTS)	Symmetric key wrapping as allowed by [FIPS 140 IG] D2. [AESKeyWrap] [SP800-38F] Using AES-256 for encryption and AES-256 CMAC for key integrity, provides 256 bits of security strength.	3780
DRBG	[SP 800-90A] Hash_DRBG. (SHA-256)	1046
ECC CDH	[SP800-56A] The Section 5.7.1.2 ECC CDH Primitive only. The Module supports NIST P-521 curve.	CVL 721
ECDSA	[FIPS 186-4] Elliptic Curve Digital Signature Algorithm. The module supports the NIST defined P-256 and P-521 curves for key pair generation, signature generation and signature verification.	815
RSA[1]	[FIPS 186-4] RSA signature verification. The module supports [PKCS#1] RSASSA-PSS and RSASSA-PKCS1-v1_5 with 2048-bit RSA keys.	1948
SHA-2	[FIPS 180-4] Secure Hash Standard compliant one-way (hash) algorithms; SHA-256, and SHA-512.	3147

Table 8: Approved Cryptographic Functions Not Used in the Module for the Current Validation

Algorithm	Description	Cert. #
AES	[FIPS 197] Advanced Encryption Standard algorithm. 192-bit key size was tested but is not used by the module.	3780
AES CMAC	[SP800-38B] AES CMAC 128 and 192-bit key sizes were tested but are not used by the module.	3780
AES KDF	[SP800-108] AES CMAC KDF AES-128 and AES-192 CMAC options were tested but are not used by the module.	KBKDF 82
ECDSA	[FIPS 186-4] Elliptic Curve Digital Signature Algorithm The following options were tested but are not used by the module: – Key pair generation: P-224, P-384 – Signature generation: P-224 – Signature verification: P-192, P-224	815
ECC CDH	[SP800-56A] The Section 5.7.1.2 ECC CDH Primitive only. Curves P-224, P-256, P-384 were tested but are not used by the module.	CVL 721

[1] Note that RSA is never used by the Thales e-Security applets but is used for DAP.

Algorithm	Description	Cert. #
RSA	[FIPS 186-4] RSA The following options were tested but are not used by the module: – Key generation: 2048-bit – PKCS #1 V1.5 signature generation: 2048-bit – PKCS #1 V1.5 signature verification: 1024-bit – PSS signature generation: 2048-bit – PSS signature verification: 1024-bit	1948
SHA-2	[FIPS 180-4] Secure Hash Standard compliant one-way (hash) algorithms SHA-1, -224-, and -384 were tested but are not used by the module.	3147

Table 9: Non-Approved but Allowed Cryptographic Functions

Algorithm	Description
NDRNG	Hardware RNG; minimum of 64 bits per access. The NDRNG output is used to seed the FIPS approved DRBG.
ECDH	[SP800-131A] EC Diffie-Hellman; not compliant with SP 800-56A. The Module supports NIST P-521 curve with SHA-512 (key agreement; key establishment methodology provides 256 bits of encryption strength).

2.1 Critical Security Parameters

All CSPs used by the Module are described in this section. All usage of these CSPs is described in the services detailed in Section 4. In the tables below, the following prefixes are used:

- OS prefix denotes operating system.
- ISD prefix denotes the GlobalPlatform Issuer Security Domain.
- DAP prefix denotes the GlobalPlatform Data Authentication Pattern.
- K prefix denotes the MercuryApplet

Table 10: Critical Security Parameters

CSP	Description/Usage
OS-DRBG_SEED	384-bit seed (entropy input) from NDRNG to seed the SHA-256 based Hash_DRBG.
OS-DRBG_STATE	880-bit value; the current DRBG state.
OS-MKEK	AES-128 master key used to derive OS-KEK.
OS-KEK	AES-128 key used to encrypt all secret and private key data stored in NVM.
ISD-KENC	AES-256 master key used to generate ISD-SENC.
ISD-KMAC	AES-256 master key used to generate ISD-SMAC and ISD-SRMAC.
ISD-KDEK	AES-256 sensitive data decryption key used to decrypt CSPs.
ISD-SENC	AES-256 session encryption key used to encrypt/decrypt secure channel data.
ISD-SMAC	AES-256 session MAC key used to verify inbound secure channel data integrity.
ISD-SRMAC	AES-256 session MAC key used to verify outbound secure channel data integrity.
K_{C-LF}	ECDSA P-521 warrant private key. Long-term signing key (authenticity guaranteed by the warrant) using SHA-512.
K_{C-E}	AES-256 Secure Channel Session key for encrypting data to HSM
K_{C-A}	AES-256-bit Secure Channel Session key used to create CMAC of data
K_{M-E}	AES-256 Secure Channel Session key for decrypting data from HSM
K_{M-A}	AES-256-bit Secure Channel Session key for authenticating HSM data using CMAC

2.2 Public Keys

Table 11: Public Keys

Key	Description/Usage
ISD-DAP	RSA 2048 or ECC-256 GlobalPlatform Data Authentication Public Key used to verify the signature of packages loaded into the Module.
K'_{W-M}	ECC P-521 Thales' root warranting public key for HSM authentication.
K'_{C-LF}	Card's ECC P-521 warrant public key used for ECC Diffie-Hellman key agreement and ECDSA signature.
$K_{M-LF'}$	HSM's ECC P-521 public key used for ECC Diffie-Hellman

The module also includes the ID_C, which is public static data used to identify the Module. It is not intended to be used as a key or seed in securing the Module's cryptographic operations.

3 Roles, Authentication, and Services

The Module:

- Does not support a maintenance role.
- Clears previous authentications on power cycle.

Authentication of each operator and their access to roles and services is as described below, independent of logical channel usage.

- Only one operator at a time is permitted on a channel.
- Applet de-selection (including Card Manager), card reset, and power down all terminate the current authentication. Re-authentication is required after any of these events for access to authenticated services.

3.1 Roles

Table 12 lists all operator roles supported by the Module.

Table 12: Roles Supported by the Module

Role ID	Role Description	Authentication Type/Method
Card Manager (CM)	The Cryptographic Officer role for FIPS 140-2 validation purposes. This role is responsible for managing the security configuration of the Module, including issuance and management of Module data via the ISD. The CM is authenticated using ISD-SENC as specified by GlobalPlatform SCP03. Once authenticated, the CM is able to execute the services provided by the ISD in a Secure Channel Session (see [GlobalPlatform] for more details).	Identity-based authentication via the Secure Channel Protocol authentication method (see Section 3.2 below)
HSM	The User role for FIPS 140-2 validation purposes. This role represents the external entity (a Thales nShield Hardware Security Module) which is authorized to establish a secure channel with the Applet and thus is able to read and write token share data on it.	Identity-based authentication via the Security World Secure Channel authentication method (see Section 3.3 below)
Operator	Remote administration role for nShield HSM. This role is the cardholder.	N/A: The human Operator (cardholder) does not authenticate to the applet.

3.1.1 Card Manager

The Card Manager (the CO) is represented on-card by the Issuer Security Domain (ISD). The ISD allows the Card Manager to manage the operating system and content.

The ISD has Java Card applet characteristics, such as: application AID, application privileges, and Life Cycle state (the Issuer Security Domain inherits the Card Life Cycle state).

3.1.2 HSM Role

The nShield Remote Management Administration Token supports the HSM role, which is an external entity allowed to establish a secure channel with the Applet and is responsible for reading and writing token share data on the card.

Authentication of this role is done with an authenticated key exchange protocol, which establishes a secure channel with the Applet.

3.1.3 Operator Role

The nShield Remote Management Administration Token supports the Operator role, a human operator wishing to conduct (or participate in) the administration of the nShield HSM from a remote location. The applet does not provide authentication for the Operator – the system concept dictates that possession of the smartcard is the required authentication. Instead, the Module authenticates the HSM.

3.2 Secure Channel Protocol Authentication Method

The GlobalPlatform SCP03 authentication method is performed as part of the Secure Channel service.

This mechanism includes a counter of failed authentication called "velocity checking" by GlobalPlatform. The counter is decremented prior to any attempt to authenticate and is only reset to its threshold (maximum value) upon successful authentication. The Module enters the "ISD is terminated" error state when the associated counter reaches zero. The default threshold is 80.

The ISD-KENC and ISD-KMAC keys are used along with other information to derive the ISD-SENC and ISD-SMAC / ISD-SRMAC keys, respectively. The ISD-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 CM role).

The cryptogram generated by the AES-256 keys is 128 bits long; and this defines the security strength of the authentication:

- The probability that a random attempt at authentication will succeed is 1/2^128 = 2.9E-39, which is less than one in 1,000,000 as required for FIPS 140-2.
- Based on the maximum count value of the velocity checking mechanism, the probability that a random attempt will succeed over a one minute period is 255/2^128 = 7.5E-37, which is less than 1 in 100,000 as required by FIPS 140-2.

3.3 Security World Secure Channel Authentication Method

The Security World secure channel authentication method is initiated with the Security World Authentication service. The Applet validates the ECDSA P-521 certificate received from the HSM against the Thales Root Warranting key. Only authentic Thales nShield HSM's are allowed to set up a secure channel.

- The probability that a random attempt at authentication will succeed is 1/2^256 = 1.2E-77, which is less than one in 1,000,000 as required for FIPS 140-2.
- Based on the rate of at least 265 ms per ECDSA P-521 signature verification, a conservative maximum number of authentication attempts in a minute is 226. The probability that a random attempt at authentication will succeed over a one minute period is 226/2^256 = 1.1E-77, which is less than 1 in 100,000 as required by FIPS 140-2.

3.4 Services

All services implemented by the Module are listed in the tables below. Each service description also describes all usage of CSPs by the service.

Table 13: Operator Services (Unauthenticated)

Service	Description
Card Reset (Self-test)	Power cycle the Module. On the first Card Reset, the Module generates OS-KEK. On every Card Reset, the Module generates OS-DRBG_SEED and OS-DRBG_STATE from the NDRNG and invokes the Power-On Self-Tests.
Info	Retrieve a single data object.
Context	Select a Java Card applet.

Table 14: Authenticated Services

Service	Description	CM	HSM
Secure Channel	Authenticates the operator and establishes a Secure Channel Session.	X	
Manage Content	Modify the card or applet content.	X	
Privileged Info	Retrieve information about the Module.	X	
Lifecycle	Modify the Card or Applet Life Cycle state.	X	
Security World Authentication	Secure channel set up providing mutual authentication and confidential transfer of token share. Static and ephemeral keys are employed with EC DH, as are AES session keys - to protect data transfers to and from the Module.		X
HSM-credential (Token Share) storage on the card	Secure block-oriented data storage and retrieval (the user's HSM-authentication credentials)		X

It should be noted that for the "Operator" services, their names and descriptions have the perspective of an HSM or user, rather than a "Module" perspective.

Also: in general, the credentials, keys, and data that a user wishes to transfer to and from the Module are not the Module's CSPs, but rather the data of the user's HSMs.

Table 15: CSP Access within Services

Service	CSPs														
	Platform											Applet			
	OS-DRBG_SEED	OS-DRBG_STATE	OS-MKEK	OS-KEK	ISD-KENC	ISD-KMAC	ISD-KDEK	ISD-SENC	ISD-SMAC	ISD-SRMAC	K_{C-LF}	K_{C-E}	K_{C-A}	K_{M-E}	K_{M-A}
Secure Channel	--	EW	E	EZ	E	E	--	GEZ	GEZ	GEZ	--	--	--	--	--
Manage Content	--	--	E	EZ	WZ	WZ	EWZ	E	E	E	--	--	--	--	--
Privileged Info	--	--	--	--	--	--	--	E	E	E	--	--	--	--	--

Service	CSPs														
	Platform											Applet			
	OS-DRBG_SEED	OS-DRBG_STATE	OS-MKEK	OS-KEK	ISD-KENC	ISD-KMAC	ISD-KDEK	ISD-SENC	ISD-SMAC	ISD-SRMAC	K_{C-LF}	K_{C-E}	K_{C-A}	K_{M-E}	K_{M-A}
Lifecycle	--	--	Z	--	--	--	--	E	E	E	--	--	--	--	--
Security World Authentication	--	--	--	--	--	--	--	--	--	--	EZ	EZ	EZ	EZ	EZ
HSM-credential (Token Share) storage on the card	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--
Card Reset (Self-test)	GW	GW	--	--	--	--	--	--	--	--	--	--	--	--	--
Info	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--
Context	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--

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

4 Self-tests

4.1 Power-On Self-Tests

On power-on or reset, the Module performs self-tests as described in Table 16 below. All KATs must be completed successfully prior to any other use of cryptography by the Module. These tests are available on demand by power-cycling the module.

If the Firmware Integrity Test fails, the Module enters the "ISD is terminated" error state. It is not possible to exit this state (it persists even after a reset). If one of the KATs fails, the system is halted (enters "CM is mute" error state) and will start again after a reset. Error states are described in Section 10.

Table 16: Power-On Self-Tests

Test Target	Description
Firmware Integrity	16-bit CRC performed over all code located in NVM. This integrity test is not required or performed for code stored in masked ROM code memory.
DRBG	Performs a fixed input KAT.
AES	Performs decrypt KAT using an AES-128 key in CBC mode.
AES CMAC KDF	Performs a KDF KAT using AES CMAC, inclusive of AES CMAC KAT and AES encrypt KAT.
RSA	Performs a KAT (RSA PKCS#1 sign and verify) using an RSA 2048-bit key pair.
EC DSA	Performs a sign and verify pairwise consistency check.
ECC CDH	Performs an ECC CDH KAT using an ECC P-256 key pair.
SHA-256	Performs a fixed input KAT.
SHA-512	Performs a fixed input KAT.

4.2 Conditional Self-Tests

Each time the Module is powered on it performs the DRBG health test monitoring functions as specified in SP800-90A.

On every generation of bits of random data by the DRBG, the Module performs a continuous DRBG test to assure that the output is different from the previous value. In case of failure the Module enters the "CM is mute" error state.

One every asymmetric key pair generation, the module performs a pairwise consistency test. In case of failure the Module enters the "CM is mute" error state.

Every CSP is protected from unintentional corruption with a 16 bit CRC. The integrity is checked when a CSP is used. In case of failure the Module enters the "ISD is terminated" error state.

When new firmware is loaded into the Module using the Manage Content service, the Module verifies the integrity of the new firmware by verifying a signature of the new firmware using the ISD-DAP public key; the new firmware in this scenario is signed by an external entity using the private key corresponding to ISD-DAP. If the signature verification fails the Module returns an error and does not load the firmware.

5 Physical Security Policy

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

The Module is intended to be mounted in additional packaging; physical inspection of the die is typically not practical after packaging. The Module also provides a transport key to protect against tampering during manufacturing and the protections listed in Section 8 below.

Module penetration testing was performed at the following temperatures:

- Nominal temperature: 20°C
- Low temperature: -40°C
- High temperature: 120°C

6 Operational Environment

The Module is designated as a limited operational environment under the FIPS 140-2 definitions. The Module 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.

7 Electromagnetic Interference and Compatibility (EMI/EMC)

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

8 Mitigation of Other Attacks Policy

Typical smart card attacks are Simple Power Analysis, Differential Power Analysis, Timing Analysis and Fault Induction that may lead to revealing sensitive information such as PIN and Keys by monitoring the Module power consumption and timing of operations or bypass sensitive operations.

The Module implements defenses against:

- Fault induction attacks
- Side-channel attacks (SPA/DPA)
- Timing analysis
- Out-of-range frequency
- Illegal address or instruction

This chip is Common Criteria certified; see http://www.commoncriteriaportal.org/products/ for more information.

8.1 Side-channel attack mitigation

All cryptographic computations and sensitive operations such as PIN comparison provided by the Cryptographic Module are designed to be resistant to timing and power analysis. Sensitive operations are performed in constant time, regardless of the execution context (parameters, keys, etc.), owing to a combination of hardware and firmware features.

8.2 Environmental attack mitigation

The Cryptographic Module does not operate in abnormal conditions such as extreme external clock, increasing its protection against fault induction.

9 Security Rules and Guidance

The Module implementation also enforces the following security rules:

- No additional interface or service is implemented by the Module which would provide access to CSPs.
- Data output is inhibited during key generation, self-tests, zeroization, and error states.
- There are no restrictions on which keys or CSPs are zeroized by the zeroization service.
- The module does not support manual key entry.
- The module does not output plaintext CSPs or intermediate key values.
- Status information does not contain CSPs or sensitive data that if misused could lead to a compromise of the module.
- The Module does not support a maintenance role.
- The module supports concurrent operators, with caveats listed in Section 3.2 of this document.

10 Error States

The module has three error states:

Table 17: Error States

Test Target	Description
Tamper is detected	The hardware detects that it has been tampered with and will not power-on. It is not possible to exit this state (it persists even after a reset: POWER_OFF then POWER_ON).
CM is mute	CM enters a state that forbids the execution of any further code. It is possible to exit this state with a reset: POWER_OFF then POWER_ON.
ISD is terminated	The CSPs are zeroized and the Card Life Cycle state is set to TERMINATED. Only the information service can be used. It is not possible to exit this state (it persists even after a reset: POWER_OFF then POWER_ON).

There also exists a transient error state when the Module has received an unsupported, unrecognized or improperly formatted command. The Module returns an error status word as specified in ISO/IEC 7816-4, exits the error state and returns to an idle state awaiting the next command.

11 Key and CSP Zeroization

The Module offers services to zeroize all CSPs in NVM:

- OS-MKEK is zeroized when the CM enters the “ISD is terminated” error state. The Card Manager can achieve this explicitly using the Lifecycle service, or a severe security event may occur (failure of the integrity check on code located in NVM or of a CSP). By zeroizing these keys all other CSPs stored in NVM are made irreversibly undecipherable.

The Module offers services to zeroize all CSPs in RAM:

- Card Reset zeroizes all CSPs in RAM as the data values held in RAM are lost at power-off and RAM is actively cleared to zero at the next power-on.
- When a Secure Channel Session is closed for any reason other than Card Reset, the CM overwrites the session keys with zeroes.

By zeroizing OS-KEK and performing a Card Reset all CSPs stored in the Module are effectively destroyed.