Thales e-Security Ltd.

Authentication Token
FIPS 140-2 Cryptographic Module
Security Policy

Document Version: 0.9

Date: May 08, 2013

Prepared by:

athena Smartcard

Thales e-Security Ltd., Jupiter House, Station Road, Cambridge, CB1 2JD, UK

Table of Contents

Table of Tables

Table of Figures

1 Introduction

1.1 General

This document defines the Security Policy for the Thales e-Security Ltd. Authentication Token Cryptographic Module, hereafter denoted *the Module*. The Module is validated to FIPS 140-2 Level 3.

This document contains a description of the Module, its interfaces and services, the intended operators and the security policies enforced in the approved mode of operation.

1.2 High-Level Module Architecture

The Module is a single chip smart card micro-controller. The Module architecture consists of two High-Level architectural components:

- Platform (Card Manager and GlobalPlatform operational environment)
- Authentication Token Applet

The purpose of the GlobalPlatform operational environment is to provide common smart card operational environment facilities and services in accordance with the GlobalPlatform Specification. The Card Manager manages the Applet Life Cycle state.

The GlobalPlatform external interface and internal API allows for Applet loading and unloading, for secure communication between an Applet and a terminal and for the use of a PIN in the context of the entire Module. In particular, it allows for the loading of a special Applet called a Supplementary Security Domain that allows an Application Provider to separate their key space from the Card Manager.

The purpose of the Applet is to provide services to the end user according to the user product requirements, which are typically the requirements of Thales' Hardware Security Modules (HSMs).

According to the requirements of FIPS 140-2 both the Platform and the Applet are tested during the FIPS 140-2 conformance testing. The FIPS 140-2 conformance certificate is issued for a Cryptographic Module, which is a combination of the Platform and the Applet. Verifying the Module's Approved mode of operation necessitates verifying the Approved mode of operation of both the Platform and the Applet.

1.3 Java Card API

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.

1.4 Structure of this Security Policy

As the Module is logically separated into the Platform and the Applet, this Security Policy document logically separates FIPS 140-2 related information items into Platform-specific information (see Sections 5-7) and Applet-specific information (see Sections 8-10). The required FIPS 140-2 information should then be viewed as a superposition of the Platform-specific and Applet-specific Information Items.

2 FIPS 140-2 Security Levels

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

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

Table 1 – Security Level of Security Requirements

3 Hardware and Physical Cryptographic Boundary

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 designed to be embedded into a smart card. The physical form of the Module is represented in Figure 1. In production use, the Module is wire-bonded to a frame connected to the ports and interfaces. The Module will be enclosed in epoxy, for example, as a smart card module.

The Module hardware and physical cryptographic boundary is depicted below. The chip is approximately 2mm square.

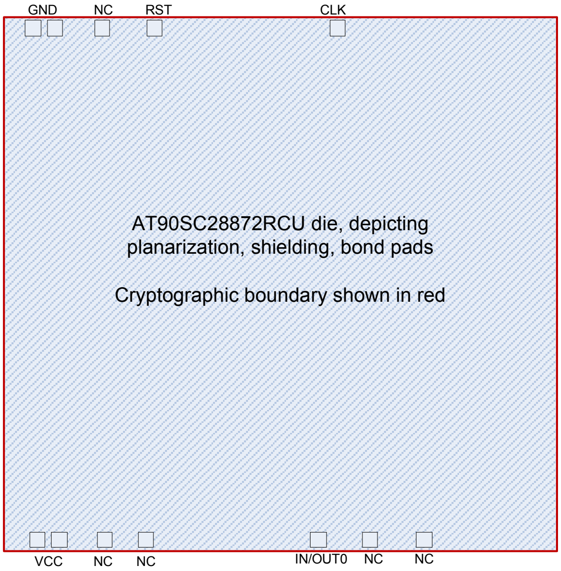
GND
NC
RST
CLK
AT90SC28872RCU die, depicting planarization, shielding, bond pads
Cryptographic boundary shown in red
VCC
NC
NC
IN/OUT0
NC
NC

Figure 1 – Hardware and Physical Cryptographic Boundary

3.1 Physical Security Policy

Physical inspection at the Module boundary is not practical after packaging. Physical inspection of Modules for tamper evidence is performed using a lot sampling technique during the assembly process. The Module also provides a transport key to protect against tampering during manufacturing and the protections listed in Section 10 below.

Module penetration testing was only performed at ambient temperature. No assurance is provided for Level 3 hardness conformance at any other temperature.

3.2 Ports and Interfaces

The Module functions as a slave processor to process and respond to commands.

3.2.1 ISO/IEC 7816

This Module provides a contact interface that is fully compliant with ISO/IEC 7816.

Interface	Description
CLK	External Clock signal
GND	Ground
VCC	Supply Voltage Power
IN/OUT0	Input/Output
RST	External Reset signal

Table 2 – ISO/IEC 7816 Physical Interfaces

This Module supports two transmission half-duplex oriented protocols: T=0 and T=1.

Up to 256 bytes of data can be exchanged through one TPDU command.

The I/O ports of the platform provide the following logical interfaces:

Interface	ISO/IEC 7816
Data In	IN/OUT0
Data Out	IN/OUT0
Status Out	IN/OUT0
Control In	IN/OUT0, CLK and RST

Table 3 – ISO/IEC 7816 Logical Interfaces

4 Firmware and Logical Cryptographic Boundary

4.1 Operational Environment

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

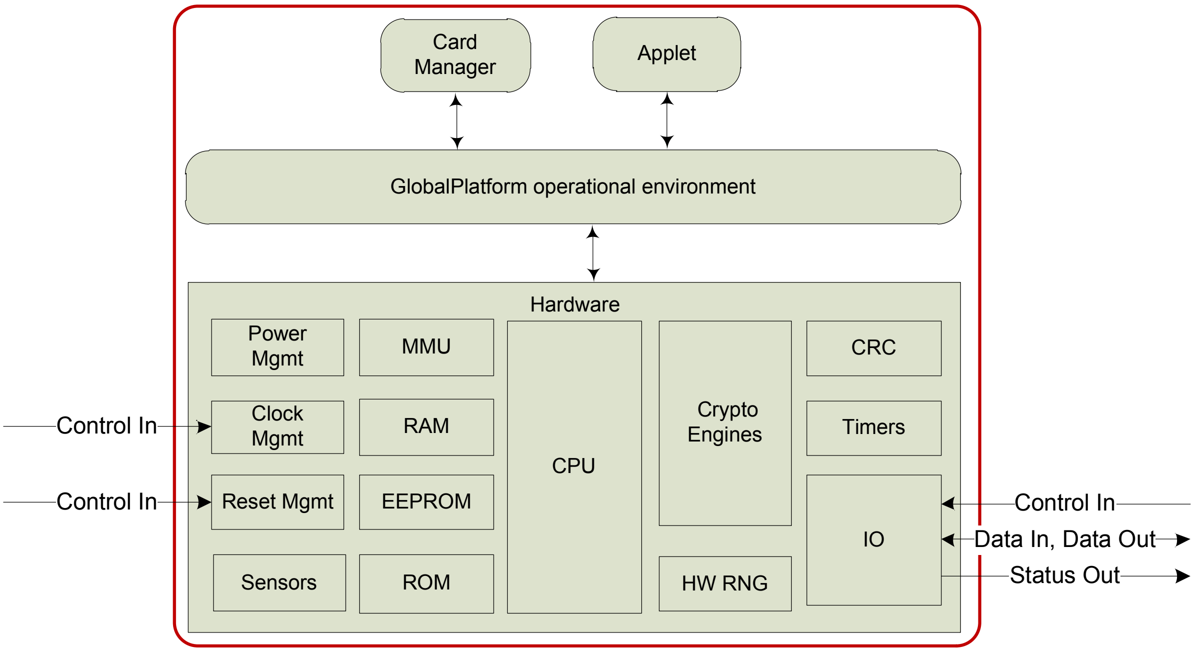

Figure 2 - Module Block Diagram

- 72 KB EEPROM; 256 KB ROM; 8 KB RAM

4.2 Versions

The hardware and firmware version numbers for the Module are provided below:

Hardware: Inside Secure AT90SC28872RCU Revision G
Firmware: Athena IDProtect 010B.0333.0004 with Authentication Token Applet 1.0

5 FIPS 140-2 Compliance (Platform)

5.1 Cryptographic Functionality

The Module implements the FIPS Approved and Non-FIPS Approved But Allowed cryptographic functions listed in tables below.

Algorithm	Description	Certificate #
DRBG	[SP800-90] DRBG. The Module supports a SHA-256 based Hash_DRBG.	98
SHA	[FIPS180-3] Secure Hash Standard compliant one-way (hash) algorithms. The Module supports SHA-1, SHA-224, SHA-256, SHA-384 and SHA-512.	1465
AES	[FIPS197] Advanced Encryption Standard algorithm. The Module supports AES-128, AES-192 and AES-256; in ECB and CBC modes.	1654
RSA	[FIPS186-2] RSA signature generation and verification. The Module supports [PKCS#1] RSASSA-PSS and RSASSA-PKCS1-v1_5 with 1024-bit and 2048-bit RSA keys.	824
ECC CDH	[SP800-56A] The Section 5.7.1.2 ECC CDH Primitive only. The Module supports NIST P-521 curve.	CVL 2

Table 4 – FIPS Approved Cryptographic Functions

Algorithm	Description
HW RNG	Hardware RNG; minimum of 64 bits per access. The HW RNG output is used to seed the FIPS approved DRBG.
AES	[SP800-38B] AES CMAC (untested). The Module supports AES CMAC with AES-128, AES-192 and AES-256 for GlobalPlatform SCP03. The AES CMAC implementation is embedded within the SCP functionality and was not CAVP validated, but is not required for secure operation of the module or to meet FIPS requirements.
AES	[AESKeyWrap] AES Key Wrap. The Module supports AES key wrapping with AES-256 for GlobalPlatform SCP03. (AES Cert. #1654, key wrapping; key establishment methodology provides 256 bits of encryption strength.)
EC Diffie-Hellman	[SP800-131A] EC Diffie-Hellman. The Module supports NIST P-521 curve with SHA-512 (key agreement; key establishment methodology provides 256 bits of encryption strength).

Table 5 – Non-FIPS Approved But Allowed Cryptographic Functions

5.2 Critical Security Parameters

Platform-specific CSPs are specified below:

Key	Description / Usage
OS-DRBG_SEED	384 bit random value from HW RNG used to seed the DRBG
OS-DRBG_STATE	880 bit value of current DRBG state
OS-MKEK	AES-128 key used to encrypt all secret and private key data stored in EEPROM Note that this is a layer of security in addition to physical security and has no relevance to the strength of mechanism of the keys it protects
OS-PKEK	AES-128 key used to encrypt all PINs
ISD-KENC	AES-256 key used by the CM role to derive ISD-SENC as specified by GlobalPlatform SCP03
ISD-KMAC	AES-256 key used by the CM role to derive ISD-SMAC and ISD-SRMAC as specified by GlobalPlatform SCP03
ISD-KDEK	AES-256 data decryption key used by the CM role to decrypt CSPs as specified by GlobalPlatform SCP03
ISD-SENC	AES-256 session encryption key used by the CM role to encrypt / decrypt Secure Channel Session data as specified by GlobalPlatform SCP03
ISD-SMAC	AES-256 session MAC key used by the CM role to verify inbound Secure Channel Session data integrity as specified by GlobalPlatform SCP03
ISD-SRMAC	AES-256 session MAC key used by the CM role to verify outbound Secure Channel Session data integrity as specified by GlobalPlatform SCP03

Table 6 - Critical Security Parameters (Platform)

5.3 Public Keys

Platform-specific public keys used by the Module are specified below:

Key	Description / Usage
ISD-DAP	RSA 1024 GlobalPlatform Data Authentication Public Key used to verify the signature of packages loaded into the Module.

Table 7 - Public Keys (Platform)

5.4 Error States

The Module has three error states:

Error state	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 GET DATA command can be processed. It is not possible to exit this state (it persists even after a reset: POWER_OFF then POWER_ON).

Table 8 – Error States

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.

5.5 Key and CSP Zeroization

The Module offers services to zeroize all CSPs in EEPROM:

- OS-MKEK and OS-PKEK are zeroized when the CM enters the “ISD is terminated” error state. The Card Manager can achieve this explicitly using the SET STATUS command, or a severe security event may occur (failure of the integrity check on code located in EEPROM or of a CSP). By zeroizing these keys all other CSPs stored in EEPROM 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-MKEK and OS-PKEK and performing a Card Reset all CSPs stored in the Module are effectively destroyed.

5.6 Self-Tests

5.6.1 Power-On Self-Tests

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

On power-on the Module performs the self-tests described in Table 9 below. Every Known Answer Test (KAT) must be completed successfully prior to any other use of cryptography by the Module.

The error state entered by the Module in case of power-on self-tests failure is “CM is mute”.

Test Target	Description
Firmware Integrity	16 bit CRC performed over all code located in EEPROM. This integrity test is not required or performed for code stored in masked ROM code memory.
DRBG	Performs the DRBG KAT.
SHS	Performs separate SHA-1, SHA-256 and SHA-512 KATs.
AES	Performs separate encrypt and decrypt KATs using an AES-128 in CBC mode.
RSA	Performs a KAT (RSA PKCS#1 sign and verify) using an RSA 2048 bit key pair.
ECC CDH	Performs an ECC CDH KAT using an ECC P-256 key pair.

Table 9 – Power-On Self-Test

5.6.2 Conditional Self-Tests

Each time the Module is powered on it performs the DRBG health test monitoring functions.

On every generation of 64 bits of random data by the HW RNG the Module performs a continuous HW RNG 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.

On every generation of 256 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.

Every CSP is protected 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 LOAD command, 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.

5.7 Standards Compliance

The Platform and the Applet are compliant with various standards.

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

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

6 Roles, Authentication and Services (Platform)

6.1 General

Table 10 lists all Platform-specific operator roles supported by the Module.

The Module does not support a maintenance role.

The Module supports concurrent operators on multiple Logical Channels. However, neither the ISD nor Authentication Token Applet are multi-selectable (they cannot be simultaneously selected on two Logical Channels). Therefore there cannot be two concurrent operators using the ISD nor two concurrent operators using the Authentication Token Applet. It is however possible to select the ISD on the Basic Channel and the Authentication Token Applet on Supplementary Channel 1 (or vice versa).

The Module clears previous authentications on power cycle.

6.2 Roles

Platform-specific roles provided by the Module are described in Table 10.

Role ID	Role Description
CM	Card Manager (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 Card Manager is able to execute the services provided by the ISD in a Secure Channel Session (see [GlobalPlatform] for more details).

Table 10 – Roles (Platform)

The Module includes the Issuer Security Domain, which allows the Card Manager to manage the operating system and content.

The Issuer Security Domain is the on-card representative of the Card Manager. 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).

6.3 Authentication

The GlobalPlatform SCP03 authentication method is performed when the EXTERNAL AUTHENTICATE service is invoked after successful execution of the INITIALIZE UPDATE command.

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, 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, less than 1 in 100,000 as required by FIPS 140-2.

6.4 Services

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

6.4.1 Unauthenticated Services

Service	Description
Card Reset (Self-test)	Power cycle the Module by removing power from the Module and then supplying it. On the first Card Reset, the Module generates OS-MKEK and OS-PKEK. On every Card Reset, the Module generates OS-DRBG_SEED and OS-DRBG_STATE from the HW RNG and invokes the Power-On Self-Tests.
INITIALIZE UPDATE	Initialize the Secure Channel Session; to be followed by EXTERNAL AUTHENTICATE. Uses OS-MKEK to decrypt ISD-KENC and ISD-KMAC for use. Uses ISD-KENC and ISD-KMAC to derive ISD-SENC and ISD-SMAC / ISD-SRMAC. Uses ISD-SENC to generate the card cryptogram.
EXTERNAL AUTHENTICATE	Authenticates the operator and establishes a Secure Channel Session. Must be preceded by a successful INITIALIZE UPDATE. Uses ISD-SMAC to verify the command MAC, and ISD-SENC to verify the host cryptogram.
GET DATA	Retrieve a single data object. Uses no CSPs.
MANAGE CHANNEL	Open a Supplementary Logical Channel. Uses no CSPs.
SELECT	Select a Java Card applet. Uses no CSPs.

Table 11 - Unauthenticated Services and CSP Usage

6.4.2 Authenticated Services

Service	Description	CM
INSTALL	Install a Java Card applet to EEPROM. Uses ISD-SENC and ISD-SMAC / ISD-SRMAC in the Secure Channel Session.	X
LOAD	Load a Java Card applet's code to EEPROM. Uses ISD-SENC and ISD-SMAC / ISD-SRMAC in the Secure Channel Session. Uses ISD-DAP to verify the integrity of the loaded firmware.	X
PUT KEY	**SCP03 key set** Load a Card Manager SCP03 key set to EEPROM. Uses ISD-SENC and ISD-SMAC / ISD-SRMAC in the Secure Channel Session. Uses OS-MKEK to decrypt ISD-KDEK for use. Uses ISD-KDEK to decrypt the loaded SCP03 key set. Creates a new or replaces the existing ISD-KENC, ISD-KMAC and ISD-KDEK SCP03 key set. Uses OS-MKEK to encrypt ISD-KENC, ISD-KMAC and ISD-KDEK for storage. **ISD DAP key** Load a Card Manager DAP key to EEPROM. Uses ISD-SENC and ISD-SMAC / ISD-SRMAC in the Secure Channel Session. Replace the existing ISD-DAP key.	X
DELETE	**Card content** Delete an Applet and/or Java Card applet code from EEPROM. Uses ISD-SENC and ISD-SMAC / ISD-SRMAC in the Secure Channel Session. **SCP03 key set** Delete a Card Manager SCP03 key set from EEPROM. Uses ISD-SENC and ISD-SMAC / ISD-SRMAC in the Secure Channel Session. Zeroizes an ISD-KENC, ISD-KMAC and ISD-KDEK SCP03 key set.	X
GET STATUS	Retrieve information about the Module. Uses ISD-SENC and ISD-SMAC / ISD-SRMAC in the Secure Channel Session.	X
SET STATUS	Modify the Card or Applet Life Cycle state. Uses ISD-SENC and ISD-SMAC / ISD-SRMAC in the Secure Channel Session.	X
STORE DATA	Add or change data in the Card Manager data store. Uses ISD-SENC and ISD-SMAC / ISD-SRMAC in the Secure Channel Session.	X

Table 12 – Authenticated Services and CSP Usage

7 Approved Mode of Operation (Platform)

The Module always runs in the Approved mode of operation.

Verifying the Module’s Approved mode of operation necessitates verifying the Approved mode of operation of both the Platform and the Applet.

7.1 Verification of Approved Mode

It is possible to verify that the Platform is in the Approved mode of operation.

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.

Data Element	Length	Value	Associated Version
IC type	2	‘010B’	Inside Secure AT90SC28872RCU Revision G
Operating system release date	2	‘0333’	Firmware Version Part 1
Operating system release level	2	‘0004’	Firmware Version Part 2

Table 13 – Versions and Mode of Operations Indicators

8 FIPS 140-2 Compliance (Applet)

8.1 Applet Description

The Module contains the Authentication Token Applet which is logically comprised of six Java Card applets each named to reflect their intended purpose relating to the credentials, keys and data of the Hardware Security Module (HSM) with which the Module will interact:

- Card admin
- Credential storage
- Key storage
- Key import
- Key export
- Data transfer

Each Java Card applet has its own command set.

The ‘Card admin’ command set is used during manufacture to set cryptographic keys and Applet data that cannot be changed post-issuance.

Post-issuance the ‘Card admin’ command set is used to interrogate non-secret Applet data, and to set/reset the Module’s intended purpose (personality). This ‘personality’ determines which of the five other mutually exclusive Java Card applets has been currently selected for that Module, each of which exposes a different command set to the HSM with which the Applet subsequently interacts.

8.2 Critical Security Parameters

Applet-specific CSPs are specified below:

Item	Byte length	Description
K_c	64	Two AES-256 keys (see [FIPS197]) for the mutual-authentication protocol.
K_c’	64	Ephemeral version of new K_c - used during key refreshment.
K_d	32	AES-256 key used by the HSM for deriving session keys.
K_d’	32	Ephemeral version of new K_d - used during key refreshment.
d_c	66	Applet’s static ECC P-521 private key for the signed EC DH (Elliptic Curve Diffie-Hellman) key exchange.
K_{dh}	32	Ephemeral AES-256 session key - derived from the EC DH key exchange.
S_{sess}	64	Two AES-256 session keys (see [FIPS197]) used to encrypt data sent from the HSM to the Module and assure its integrity.
S_{sess}’	64	Two AES-256 session keys (see [FIPS197]) used to encrypt data sent from the Module to the HSM and assure its integrity.

Table 14 - Critical Security Parameters (Applet)

The ephemeral keys used during key refreshment, K_c’ and K_d’, are the same length and type as the keys they should eventually replace.

The Applet-specific public keys and Module data are specified in the following table:

Item	Byte length	Description
ID_c	9	Thales' unique Module serial number.
Q_c	132	Applet's static ECC P-521 public key for the signed EC DH key exchange.
Q_h	132	HSM's ephemeral ECC P-521 public key for the signed EC DH key exchange.

Table 15 - Public Keys and Data (Applet)

The ID_c 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.

9 Roles, Authentication and Services (Applet)

9.1 Roles

The roles available in the Authentication Token Applet relate to the different command sets of each its six Java Card applets as described in Table 16.

Every Java Card applet has a default/unauthenticated User role.

The unauthenticated roles have access to work with non-secret data (including public keys), and to initiate or support the use of the authenticated roles.

Some Java Card applets have an additional role: 'Cryptographic/Mutually authenticated user' (C/MAU).

The cryptographic/mutually authenticated roles are intended to support the confidentiality and authenticity of transfers of secret data (in either direction) – normally between the Module and an HSM.

Where available and applicable, the holder of a personalized Module may use a passphrase to help protect their Module. This is not a security-related feature and does not involve the Module's CSPs. No FIPS related authentication is being claimed by the use of the passphrase. Table 16 also identifies the availability of this feature.

Java Card applet name	User Role ID	C/MAU Role ID	Passphrase Protection
Card admin	1a		
Credential storage	1b	2	
Key storage	1c		✓
Key import	1d	3	✓
Key export	1e	4	✓
Data transfer	1f		

Table 16 – Roles (Applet)

The use of passphrases is also intended to strengthen dependent systems (e.g. HSM management systems) against casual user errors – such as attempts to the use the wrong Module.

9.2 Authentication

Role ID	Identity Based Authentication method
1a - 1f	Unauthenticated
2	Mutual authentication using pre-shared AES-256 keys.
3	Mutual authentication using pre-shared AES-256 keys.
4	Mutual authentication using pre-shared AES-256 keys.

Table 17 – Authentication

Based on its use of keys and algorithms, the security strength of mutual authentication within the Authentication Token Applet would be 256 bits.

Of the 256 bits of authentication data encrypted by the pre-shared AES-256 keys, 240 bits are validated during mutual authentication; and this defines the security strength of the authentication:

- The probability that a random attempt at authentication will succeed is 1/2^240, less than one in 1,000,000 as required for FIPS 140-2.
- Based on the maximum speed of the authentication mechanism, the probability that a random attempt will succeed over a one minute period is 480/2^240, less than 1 in 100,000 as required by FIPS 140-2.

9.3 Services

The names and descriptions of services have the perspective of an HSM or user - rather than a 'Module' perspective.

In general, the credentials, keys, and data that a user wishes to transfer to and from the Module are not the Module's CSPs – they are the user's HSMs' data.

Service	Description	Roles	CSP usage (see Table 14)
Card administration	General Applet management and administration – including unauthenticated data storage and retrieval.	1a~1f	No non-volatile secret CSP is modified or disclosed. Non-volatile secrets are not erased by a card reset. Volatile secrets are erased by a card reset. Non-secret CSPs may be disclosed.
HSM-credential storage	Secure block-oriented data storage and retrieval (typically the user's HSM-authentication credentials) providing mutual authentication and confidential transfer.	2	Static and ephemeral keys are employed with EC DH, as are AES session keys - to protect data transfers to and from the Module.
HSM-key storage	Passphrase-protected block-oriented storage and retrieval of data - typically HSM key data.	1c	None
HSM-key import - add component	Passphrase-protected block-oriented data storage - typically HSM key components.	1d	None
HSM-key import - get component	Secure block-oriented retrieval of stored data (typically HSM key components) providing mutual authentication and confidential transfer.	3	Static and ephemeral keys are employed with EC DH, as are AES session keys - to protect data transfers from the Module.
HSM-key export - get export data	Passphrase-protected data retrieval - typically HSM key data.	1e	None
HSM-key export - set export data	Secure block-oriented storage of data (typically HSM key data) providing mutual authentication and confidential transfer.	4	Static and ephemeral keys are employed with EC DH, as are AES session keys - to protect data transfers to the Module.

Table 18 – Services and CSP Usage

10 Approved Mode of Operation (Applet)

The Module always runs in the Approved mode of operation.

Verifying the Module's Approved mode of operation necessitates verifying the Approved mode of operation of both the Platform and the Applet.

10.1 Verification of Approved Mode

It is possible to verify that the Applet is in the approved mode of operation.

SELECT the Card admin applet and send a 'Get_software_version' command as the 'Card admin applet-specific unauthenticated role' (1a) and verify that the returned data contains the field as follows. This verifies the version of the Applet.

Data Element	Length	Value	Associated Version
Software version	2	'0100'	Authentication Token Applet 1.0

Table 19 – Versions and Mode of Operations Indicators

11 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.

12 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.

13 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.

This Cryptographic Module is protected against SPA, DPA, Timing Analysis and Fault Induction by combining State of the Art firmware and hardware counter-measures.

The Cryptographic Module is protected from attacks on the operation of the IC hardware. The protection features include detection of out-of-range supply voltages, frequencies or temperatures, detection of illegal address or instruction, and physical security. This chip is Common Criteria certified; more information is available her http://www.commoncriteriaportal.org/products/.

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.

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

14 Security Rules and Guidance

14.1 Security Rules (General)

The Module implementation enforces the following security rules:

- The Module does not output CSPs (plaintext or encrypted).
- The Module does not support manual key entry.
- The Module does not output intermediate key values.
- 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 CSPs are zeroized by the zeroization service.
- Status information does not contain CSPs or sensitive data that if misused could lead to a compromise of the Module.

Additional applications can be loaded in the Module after issuance as specified in GlobalPlatform. However, any other firmware loaded into this Module is out of the scope of this validation and requires a separate FIPS 140-2 validation.

- Application loading is one of the services provided by the operating system that is restricted to the Card Manager: a Secure Channel Session must be open between the external operator (more precisely the middleware the CM is using to manage content) and the ISD. Application loading is protected by ISD-DAP.
- The application loading service is available before and after Module issuance.
- The CM is responsible for application personalization and lifecycle management following GlobalPlatform.

14.2 Acronyms

The following acronyms are referred to in this Security Policy.

Acronym	Full Specification Name
API	Application Programming Interface
CM	Card Manager, see [GlobalPlatform]
CSP	Critical Security Parameter
DAP	Data Authentication Pattern, see [GlobalPlatform]
DPA	Differential Power Analysis
ECC CDH	Elliptic Curve Cryptography Cofactor Diffie-Hellman
IC	Integrated Circuit
ISD	Issuer Security Domain, see [GlobalPlatform]
KAT	Known Answer Test
PKI	Public Key Infrastructure
SCP	Secure Channel Protocol, see [GlobalPlatform]
SPA	Simple Power Analysis

Table 20 – Acronyms

14.3 References (Cryptography)

The following Cryptography standards are referred to in this Security Policy.

Standard	Full Specification Name
[FIPS113]	Computer Data Authentication
[FIPS140-2]	Security Requirements for Cryptographic Modules
[FIPS180-3]	Secure Hash Standard (SHS)
[FIPS186-2]	Digital Signature Standard (DSS)
[FIPS186-3]	Digital Signature Standard (DSS)
[FIPS197]	Advanced Encryption Standard (AES)
[PKCS#1]	PKCS #1 v2.1: RSA Cryptography Standard June 2002
[SP800-38B]	Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication
[SP800-56A]	Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography
[SP800-89]	Recommendation for Obtaining Assurances for Digital Signature Applications
[SP800-90]	Recommendation for Random Number Generation Using Deterministic Random Bit Generators
[SP800-131A]	Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths
[AESKeyWrap]	http://csrc.nist.gov/groups/ST/toolkit/documents/kms/AES_key_wrap.pdf

Table 21 – References (Cryptography)

14.4 References (Platform)

The following Platform-related standards are referred to in this Security Policy.

Standard	Full Specification Name
[JavaCard]	Runtime Environment Specification, Java Card Platform, Version 2.2.2, March 2006 Application Programming Interface, Java Card Platform, Version 2.2.2, March 2006 Virtual Machine Specification, Java Card Platform, Version 2.2.2, March 2006
[GlobalPlatform]	GlobalPlatform Consortium: GlobalPlatform Card Specification 2.1.1, March 2003, http://www.globalplatform.org GlobalPlatform Consortium: GlobalPlatform Card Specification 2.1.1 Amendment A, March 2004 GlobalPlatform Consortium: GlobalPlatform Card Technology, Secure Channel Protocol 03, Card Specification v 2.2 - Amendment D, Version 1.1, September 2009
[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

Table 22 – References (Platform)

14.5 References (Applet)

The following Authentication Token Applet-related standards are relevant.

Standard	Full Specification Name
[ISO7816-5]	ISO/IEC 7816-5: 2004 Identification cards — Integrated circuit cards — Part 5: Registration of application providers

Table 23 – References (Applet)