HID Global ActivID Applet Suite v2.6.2B on Oberthur Technologies ID-One Cosmo v7

FIPS 140-2 L3 Security Policy

Product Version 2.6.2b
August 24, 2015

Table of Contents

List of Figures

List of Tables

1.0 Introduction

This document defines the Security Policy for the HID Global ActivID Applet Suite v2.6.2B on Oberthur ID-One Cosmo v7 cryptographic module. The module, a single chip embodiment validated to FIPS 140-2 Overall Security Level 3, is the combination of the HID Global ActivID Applet Suite v2.6.2B (denoted *ActivID Applet Suite* below) running on the Oberthur ID-One Cosmo v7-n (denoted *platform* below). The platform has been previously validated as Cert. #1236.

This module is bound to the Cert. #1236 module - a binding caveat similar to the following is expected to be present in the listing:

> *When operated with module Oberthur ID-One Cosmo V7-n validated to FIPS 140-2 under Cert. #1236 operating in FIPS mode.*

The platform provides an operational environment for the ActivID Applet Suite: all cryptographic algorithm implementations and associated self-tests, random number and key generation, card lifecycle management, and key storage and protection are provided by platform. The code for this functionality is contained in the platform ROM, unchanged from Cert. #1236. However, the factory configuration of the module constrains the module to the set of services provided by the platform's Card Manager (implementing a standard set of GlobalPlatform services) and the ActivID Applet Suite. As such, some functionality and options present on the platform are not usable on this module. Unusable functionality is not discussed further in this document; see the Cert. #1236 Security Policy for more details of the platform and platform configurability.

Figure 1 depicts the ActivID Applet Suite in the platform operational enviroment.

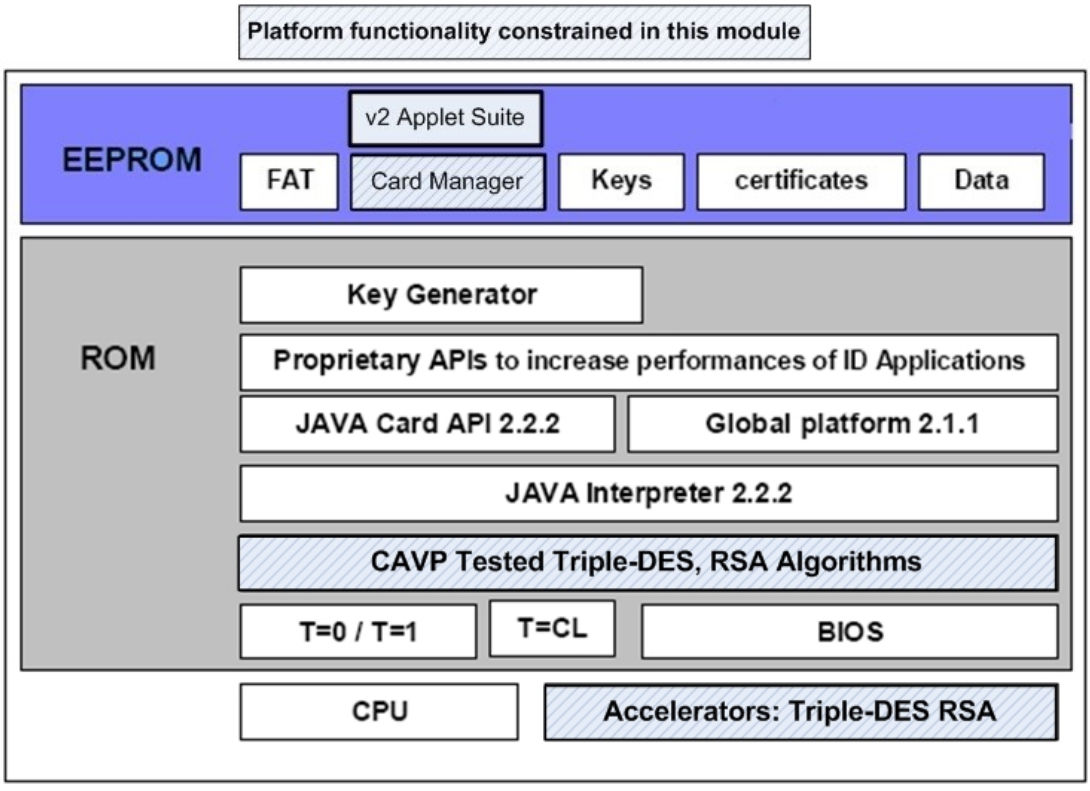

FIGURE 1: Logical Block Diagram of the module

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.

Table 1 summarizes the FIPS 140-2 Security Levels for all requirements areas.

TABLE 1: Module Security Level Specification

Security Requirements Section	Level
Cryptographic Module Specification	3
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

The module is available as the ActivID Applet Suite loaded on any of the platform configurations in Table 2.

TABLE 2: Module Platform Configurations

Platform Product Name	Hardware P/N	Firmware version/ Op Code	Available EEPROM	Interfaces
ID-One Cosmo V7-n Standard	C7	FC10 / 069778	~80K	Contact only
ID-One Cosmo V7-n Standard Dual	BA	FC10 / 069778	~80K	Dual: Contact, Contactless
ID-One Cosmo V7-n Large	C4	FC10 / 069778	~128K	Contact only
ID-One Cosmo V7-n Large Dual	B0	FC10 / 069778	~128K	Dual: Contact, Contactless

ISO 7816 compliant (contact) and ISO 14443 compliant (contactless) communications occur over contact plate and antenna connections. The mode of operation is determined at power-up, depending on the reader type (contact or contactless) that the module is operated within, and cannot be changed until the module is reset.

Table 3 lists all ports and the corresponding FIPS 140-2 logical interfaces for the module.

TABLE 3: Ports and Interfaces

PIN	FIPS 140-2 Designation	Description
Vcc	Power	Both Class A (5V) and Class B (3V) supported
RST	Control input	External Reset Signal
CLK	Control input	External Clock Signal (1 to 10Mhz) to transmit data over I/O line. Internally the card relies on an uninterrupted internal oscillator to drive the main processor and all cryptographic co-processors independently of the external clock.
I/O	Control input, Data input, Data output, Status output	See transmission parameters below
GND	Ground (power interface)	Reference Voltage
LA, LB	Power, Control input, Data input, Data output, Status output	Antenna (Dual interface configurations only)

The cryptographic module boundary are the surfaces and edges of the die, with die bond pads connected to contact plates and contactless antenna connections. The module will typically be embedded into a plastic card body and connected to a contact plate and for dual interface, an external antenna loop. The physical form of the module is depicted in Figure 2, with the cryptographic boundary outlined in red. The image at left in Figure 2 depicts the contact plate of the module when packaged in final form.

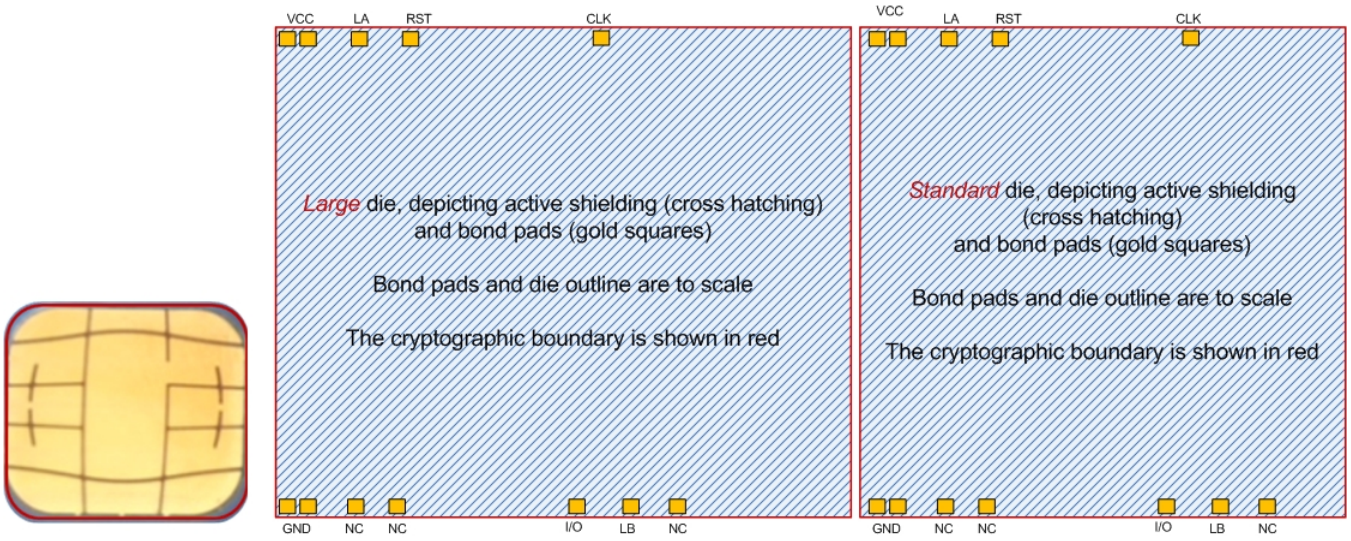

FIGURE 2: Module Physical form
Contact plate (left); Depictions of Large and Standard module configurations

The module is configured in the factory to operate exclusively in the Approved mode. The explicit indicator of the Approved mode of operation is obtained by issuing the following commands:

TABLE 4: Commands to Obtain Approved Mode Indicator

Command and associated elements	Expected Response
GET DATA (tag '05') with Card Manager selected	'01'
GET PROPERTIES (tag 24) with ACA applet selected	0x24 0x01 0x02

2.0 HID Global ActivID Applet Suite

The ActivID Applet Suite (version 2.6.2B.7) comprises:

- ASCLib Library Interfaces: version 2.6.2B.7
- ASC library: version 2.6.2B.6
- ACA applet interfaces: version 2.6.2B.7
- ACA applet: version 2.6.2B.6
- PKI/GC/SKI applet: version 2.6.2B.6
- SMA applet: version 2.6.2B.6

Access Control Applet (ACA) – Manages Access Control Rules (ACR) definition, access control rules enforcement and secure-messaging processing for all card services. The authentication methods detailed in Section 5.0 are implemented in this applet.

PKI/Generic Container/SKI (PKI/GC/SKI) Applet – Manages PKI credentials and other data required for implementation of card services including single sign-on applications, identity, and benefits information. This applet also manages the keys and command handling for applet RSA and OTP services.

ASC Library Package – Provides utility functions accessible only to callers within the domain (not accessible via the module's ports and interfaces).

Secure Messaging Anonymous (SMA) Plug-In Applet – Provides secure messaging services to the ACA applet to automate secure messaging integratin with access control rules. The SMA protocol uses RSA key decapsulation to establish session key material into the module, derives 2-Key Triple-DES message confidentiality and integrity keys from the session key material, and uses these keys for bi-directional message confidentiality and integrity.

3.0 Cryptographic Functionality

The module uses the FIPS Approved and Non-FIPS Approved but allowed cryptographic functions listed next.

TABLE 5: FIPS Approved Cryptographic Functions

Algorithm	Description	Cert #
RNG	[FIPS 186-2] Random Number Generator.	#480
Triple-DES	[SP 800-67] Triple Data Encryption Algorithm. The module supports the 2-Key and 3-Key options CBC and ECB modes. (Note: The module does not use 2-Key Triple-DES to encrypt or to wrap keys.)	#698
Triple-DES MAC	[FIPS113] Triple-DES Message Authentication Code. Vendor affirmed, based on Cert. #698.	#698
RSA	[PKCS#1] RSA key generation and signature generation. The module supports 2048-bit RSA keys. All uses of RSA signature generation require hash off-card.	#403

TABLE 6: non-FIPS Approved but Allowed Cryptographic Functions

Algorithm	Description
NDRNG	Hardware RNG used to seed the Approved RNG.
RSA Key Decapsulation	The module supports RSA key decapsulation using 2048-bit keys; key establishment method provides 112 bits of encryption strength.
Symmetric Key Unwrap (2-Key Triple-DES)	Symmetric key unwrap allowed by IG D2 and SP 800-38F for key transport; key establishment method provides 112 bits encryption strength.

4.0 Critical Security Parameters and Public Keys

Table 17 summarizes all CSPs and public keys used in the module; access to CSPs and public keys by service is described in Section 6.1. The module does not output secret or private keys. All keys may be zeroized using the SET STATUS(TERMINATE) command and removing the card from the reader.

TABLE 7: Critical Security Parameters and Public Keys

CSP	Description / Usage
Platform CSPs (CDK prefix: Card Administrator (Issuer Security Domain) key set; ADK prefix: Application Provider (Application Security Domain) key set.	
RNG Seed	20-byte seeding data for use by the onboard FIPS 186-2 RNG
CDKENC, ADKENC	2-Key Triple-DES Master key used in the Secure Channel Protocol to generate CDSENC and ADSENC, respectively.
CDKMAC, ADKMAC	2-Key Triple-DES Master key used in the Secure Channel Protocol to generate CDSMAC and ADSMAC, respectively.
CDKKEK, ADKKEK	2-Key Triple-DES sensitive data decryption key used in Secure Channel Protocol to decrypt CSPs.
CDSENC, ADSENC	2-Key Triple-DES Session decryption key used to decrypt secure channel data.
CDSMAC, ADSMAC	2-Key Triple-DES Session MAC key used to verify inbound secure channel data integrity.
ActivID Applet Suite CSPs (CDK prefix: Card Administrator (Issuer Security Domain) key set; ADK prefix: Application Provider (Application Security Domain) key set.	
ACA PIN	6 to 127 byte alpha-numeric character string used for Card Holder authentication.
OTP	2-Key or 3-Key Triple-DES Secret Key for One time Password – used to generate a unique password.
RSA Private Keys	2048-bit RSA private keys used for PKI/GC/SKI applet signature generation and authentication.
SMA-ENC	2-Key Triple-DES Session decryption key used for SMA channel decrypt.
SMA-MAC	2-Key Triple-DES Session decryption key used for SMA channel MAC generation and verification.
SMA Private Keys	2048-bit RSA private keys used for SMA session key transport.
XAUT	3-Key Triple-DES External Authentication keys, 1 to 8 instances.
ActivID Applet Suite Public Keys	
RSA Public Keys	2048-bit RSA public keys held in the module for retrieval by external users through the PKI/GC/SKI applet.

5.0 Roles

The module does not support concurrent operators. Table 7 lists the roles available in the module.

TABLE 8: Roles and Required Identification and Authentication

Cryptographic Officer Roles	
CA	Card Administrator - Manages module content and security configuration. Authenticated using the Secure Channel Protocol or XAUT authentication methods.
User Roles	
AP	Application Provider - Manages application security configuration. Authenticated using the Secure Channel Protocol authentication method.
CH	Card Holder – The human user of the module. Authenticated using the PIN Verification Method.
AO	Application Operator - An external application requesting applet services. Authenticated using the XAUT Authentication Method.
Unauthenticated Roles	
PO	Public Operator - Represents unauthenticated services.

Secure Channel Protocol Authentication Method

The Secure Channel Protocol authentication method uses the security domain KENC (CDKENC and ADKENC) and KMAC (CDKMAC and ADKMAC) keys to derive the SENC (CDSENC and ADSENC) and SMAC (CDSMAC, ADSMAC) keys, respectively, in the Secure Channel Protocol implementation. The SENC key is used to create a cryptogram; the external entity participating in the mutual authentication, identified by key identifier, 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 CO role).

[SP 800-131A] Section A.1 provides the NIST rationale for 2-Key Triple-DES security strength. The module encrypts a total of one block (the mutual authentication cryptogram) over the life of the session encryption key; no decrypted data is output by the Module. The Module claims 112-bit security strength for its 2-Key Triple-DES operations, as the meet-in-the-middle attack rationale described in [SP 800-131A] does not apply unless the attacker has access to encrypt/decrypt pairs.

The probability that a random attempt will succeed using this authentication method is:

- 1/2^64 = 5.4E-20 (based on the Triple-DES block size)

The module enforces an exponential delay mechanism on failed attempts, limiting the rate of authentication attempts to 50 in a one minute period. The probability that a random attempt will succeed over a one minute interval is:

- 50/2^64 = 2.7E-18

XAUT External Authentication Method

The XAUT uses the XAUT key in a challenge response exchange to verify an encrypted nonce. The key identifier corresponds to a specific operator identity. The probability that a random attempt will succeed using this authentication method is:

- 1/2^64 = 5.4E-20 (based on the Triple-DES block size)

The module enforces an exponential delay mechanism on failed attempts, limiting the rate of authentication attempts to 50 in a one minute period. The probability that a random attempt will succeed over a one minute interval is:

- 50/2^64 = 2.7E-18

PIN Verification Authentication Method

The external entity submits an identifier and corresponding PIN. The PIN is compared to the stored reference for that identifier. The character space for PINs is enforced by the module to be in the alphanumeric range (62 possible values). The minimum PIN length of 6 characters is enforced by the module. The probability that a random attempt will succeed using this authentication method is:

- 1/(62^6) = 1.8E-11

The module restricts authentication attempts to 15 tries, so the probability that a random attempt will succeed over a one minute interval is:

- 15/(62^6) = 2.6E-10

6.0 Services

Table 8 list the services implemented by the module, separated into the services implemented by the platform and by the ActivID Applet Suite, respectively. All services are available via the contact interface. Services available via the contactless interface are marked in the CL column.

TABLE 9: Module Services by Role

Platform Services		Roles					CL
		CA	AP	CH	AO	PO	
Module Reset (power cycle)	Powering on or resetting the module; reinitializes the module, including invoking all power-on self-tests described in Section 7.0.					X	
DELETE	This command is used by the CA to delete a uniquely identifiable object. The object may be an Application, a load file, or a key set.	X	X				X
EXTERNAL AUTHENTICATE	This command is used by the CA to open a Global Platform Secure Channel Session with the Issuer Security Domain.	X	X				X
GET DATA	The GET DATA command is used to retrieve public data from the selected application. No CSP can be read using this service.	X	X	X	X	X	X
GET STATUS	This command is used by the CA to retrieve identification and life cycle status information for all applications, executable load files, and security domains present in the module.	X	X				X
INITIALIZE UPDATE	This command is used by the CA to initiate a Global Platform Secure Channel Session, setting the key set version and index.	X	X				X
INSTALL	This command is used by the CA to add an application to the module.	X					X
LOAD	This command is used by the CA to load patch or applet code.	X					X
PUT KEY	This command is used by the CA to add or replace Security Domain keys. Keys are loaded protected by the double encryption of the global Platform Secure Channel and a KCV is included in the transmission to ensure integrity of the key loading operation. This command is also used by the CA to load RSA public keys such as the Token Verification Key or the DAP Verification Key. These keys are used for Delegated Management and DAP verification as specified by Global Platform.	X	X				X
SELECT	This command is used for selecting an application on a specific logical channel. A successful selection logs out the role currently active on the same logical channel, if any. In the applet suite context SELECT can be used to select a Load File.	X	X	X	X	X	X
SET STATUS	This command is used to manage the lifecycle state of the card. The use of SET STATUS with the TERMINATE qualifier provides the required Zeroization service, along with removal and reinsertion of the card into the reader.	X	X				X
STORE DATA	This command is used by the CA to transfer data to the module. It is also used to clear the audit log and to modify the contactless capabilities (activate/deactivate a contactless stealth mode, or to allow only non-identifiable information to leak out of the contactless interface until the terminal can be authenticated) to increase the privacy protection of the user.	X	X				X

ActivID Applet Suite Services		Roles					CL
		CA	AP	CH	AO	PO	
AC EXTERNAL AUTHENTICATE	Used in combination with GET CHALLENGE for AO authentication.				X		
CHANGE REFERENCE DATA	Change the (ACA) PIN value.	X		X			
GENERAL AUTHENTICATE	Perform PKI operations when opening a SMA session.	X	X	X	X	X	X
GENERATE KEY PAIR	Generate an RSA Key Pair, outputting public key.	X		X	X		
GET ACR	Retrieve the ACR definition for the services.	X	X	X	X	X	
GET CHALLENGE	Used in combination with AC EXTERNAL AUTHENTICATE for AO authentication, or when opening a SMA session.	X	X	X	X	X	X
GET DATA	Used to retrieve a single data object.	X	X	X	X	X	X
GET PROPERTIES	Used to obtain applet instance configuration information.	X	X	X	X	X	X
GET RESPONSE	Used to retrieve remaining data in the output buffer (T=0 only).	X	X	X	X	X	X
INTERNAL AUTHENTICATE	The APDU is for SKI operations (One Time Password) and to generate a cryptogram from the card for verification by the calling application.			X			X
LOGOUT	To logout all authenticated roles. The APDU is accessible from ACA applet.	X	X	X	X	X	
MANAGE SMA	The APDU is used to explicitly close the SMA secure session	X	X	X	X	X	X
PRIVATE SIGN / DECRYPT	This APDU uses the RSA private key in the PKI buffer to sign data	X		X			X
PUT KEY	This APDU is used to either enter the XAUT keys (like used to unblock the PIN), the RSA private key component, SMA private key or the SKI key for One Time Password generation. The APDU must be used with a secure channel established by CA role. The APDU format is compliant with GP specifications.	X		X			X
READ BINARY	This APDU reads binary data stored on the card.	X	X	X	X	X	X
READ CERTIFICATE / STATIC BUFFER	This APDU is used to read the data from the selected buffer	X	X	X	X	X	X
REGISTER ACR	This APDU manages the mapping between ACRID and actual APDU instruction as well as record the ACR definition for the applet services.	X					
REGISTER APPLET	This APDU is to register applet instances to the ACA instance so that the access control and GP secure message service can be provided.	X					
RESET CARD	This command resets the card content (buffer content, PKI credentials, SKI keys as well the PIN)				X		
RESET RETRY COUNTER	This APDU is used to unblock the Card Holder PIN and restore the VERIFY service with a new counter value if the CA role is authenticated successfully. The command operates as long as the unblock counter has not expired.	X			X		
SET APPLICATION UID	This APDU is sent when the UID associated with the applet instance needs to be changed	X					
SET PROPERTIES	This APDU creates and sets the object properties for GC/PKI/SKI applet.	X					
SET STATUS	This APDU is sent when the applet instance life cycle needs to be changed. The applet instance life cycle can be: SELECTABLE, BLOCKED, and PERSONALIZED.	X					
UPDATE CERTIFICATE / STATIC BUFFER	This APDU is used to update the data stored in the selected buffer.	X	X	X	X	X	
UPDATE PROPERTIES	Update ACA properties.	X	X	X	X	X	
VERIFY	This APDU checks the PIN presented by the Card Holder against the current PIN.			X			X

6.1 Service Access to CSPs

Table 9 describes access to CSPs by module services. The following codes are used to indicate access type:

- 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.

TABLE 10: Relationship between Roles, Services and CSP Access

Services \ CSPs	RNG Seed	CDKENC	CDKMAC	CDKKEK	CDSENC	CDSMAC	ADKENC	ADKMAC	ADKKEK	ADSENC	ADSMAC	ACA PIN	XAUT	OTP	RSA Private	SMA-ENC	SMA-MAC	SMA Private
Platform																		
Module reset (power cycle)	ZGE	--	--	--	Z	Z	--	--	--	Z	Z	--	--	--	--	--	--	--
DELETE	--	--	--	--	E[1]	E	--	--	--	E	E	Z	Z	Z	Z	Z	Z	Z
EXTERNAL AUTHENTICATE	--	--	--	--	E	E	--	--	--	E	E	--	--	--	--	--	--	--
GET DATA	--	--	--	--	E	E	--	--	--	E	E	--	--	--	--	--	--	--
GET STATUS	--	--	--	--	E	E	--	--	--	E	E	--	--	--	--	--	--	--
INITIALIZE UPDATE	--	E	E	--	G	G	E	E	--	G	G	--	--	--	--	--	--	--
INSTALL	--	--	--	--	E	E	--	--	--	E	E	--	--	--	--	--	--	--
LOAD	--	--	--	--	E	E	--	--	--	E	E	--	--	--	--	--	--	--
PUT KEY	--	W	W	W	E	E	W	W	W	E	E	--	--	--	--	--	--	--
SELECT	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--
SET STATUS[2]	Z	Z	Z	Z	E	E	Z	Z	Z	E	E	Z	Z	Z	Z	Z	Z	Z
STORE DATA	--	--	--	--	E	E	--	--	--	E	E	--	--	--	--	--	--	--

[1] In the CDSENC, CDSMAC, ADSENC and ADSMAC columns, E indicates possible usage of the secure channel.

[2] As a consequence of SET STATUS (TERMINATE).

Services \ CSPs	DRNG Seed	CDKENC	CDKMAC	CDKKEK	CDSENC	CDSMAC	ADKENC	ADKMAC	ADKKEK	ADSENC	ADSMAC	ACA PIN	XAUT	OTP	RSA Private	SMA-ENC	SMA-MAC	SMA Private
ActivID Applet Suite																		
AC EXTERNAL AUTHENTICATE	--	--	--	--	--	--	--	--	--	--	--	--	E	--	--	--[3]	--	--
CHANGE REFERENCE DATA	--	--	--	--	--	--	--	--	--	--	--	WE	--	--	--	E	E	--
GENERAL AUTHENTICATE	--	--	--	--	--	--	--	--	--	--	--	--	--	--	E	G	G	E
GENERATE KEY PAIR	--	--	--	--	E	E	--	--	--	E	E	--	--	--	G	--	--	G
GET ACR	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--
GET CHALLENGE	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--
GET DATA	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--
GET PROPERTIES	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--
GET RESPONSE	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--
INTERNAL AUTHENTICATE	--	--	--	--	--	--	--	--	--	--	--	--	--	E	--	--	--	--
LOGOUT	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--
MANAGE SMA	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	E	E	--
PRIVATE SIGN / DECRYPT	--	--	--	--	--	--	--	--	--	--	--	--	--	--	E	--	--	--
PUT KEY	--	--	--	--	E	E	--	--	--	E	E	--	W	W	W	--	--	W
READ BINARY	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--
READ CERTIFICATE / STATIC BUFFER	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--
REGISTER ACR	--	--	--	--	E	E	--	--	--	E	E	--	--	--	--	--	--	--
REGISTER APPLET	--	--	--	--	E	E	--	--	--	E	E	--	--	--	--	--	--	--
RESET CARD	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--
RESET RETRY COUNTER	--	--	--	--	E	E	--	--	--	E	E	--	--	--	--	E	E	--
SET APPLICATION UID	--	--	--	--	E	E	--	--	--	E	E	--	--	--	--	--	--	--
SET PROPERTIES	--	--	--	--	E	E	--	--	--	E	E	--	--	--	--	--	--	--
SET STATUS	--	--	--	--	E	E	--	--	--	E	E	--	--	--	--	--	--	--
UPDATE CERTIFICATE / STATIC BUFFER	--	--	--	--	E	E	--	--	--	E	E	--	--	--	--	--	--	--
UPDATE PROPERTIES	--	--	--	--	E	E	--	--	--	E	E	--	--	--	--	--	--	--
VERIFY	--	--	--	--	--	--	--	--	--	--	--	E	--	--	--	E	E	--

[3] In the SMA-ENC and SMA-MAC columns, E indicates usage of the SMA secure channel, used based on ACR configuration.

7.0 Self-Tests

On power-on or reset, the module performs self-tests as described below. All KATs must be completed successfully prior to any other use of cryptography by the module. The module does not respond to any commands while self-tests are being performed. If any of these tests fail, the card returns an error status before entering the Power up and Conditional Self-test Failure state in which further commands are not processed until the card is power-cycled or reset. The module also performs self-tests for other unused algorithms present in the module; these are not relevant to this module's validation and as such are not listed below.

- EEPROM code integrity check (CRC 16)
- Cryptographic algorithm tests (KAT)
  - Random Generator.
  - Triple-DES – separate encrypt and decrypt KATs.
  - RSA – signature generation KAT.

The module also perform the conditional self-tests required by FIPS 140-2:

- On generation of an RSA key pair, the module performs a double pair-wise consistency check to validate that the newly generated key pair for both signature/verification and encryption/decryption.
- Continuous testing is performed on every output of both the Approved RNG and the non-Approved hardware RNG. Additional statistical testing is also performed to ensure the highest possible quality of the generated random numbers.
- When new firmware is loaded (using the LOAD and INSTALL commands) the module verifies all code using Triple-DES MAC.

8.0 Security Rules

This section documents the security rules not already listed above that are enforced by the cryptographic module to implement the security requirements of this FIPS 140-2 Level 3 module.

- No additional interface or service is implemented by the module that provides 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.
- The module does not support manual key entry, output plaintext CSPs or output intermediate key values.
- Status information does not contain CSPs or sensitive data that if misused could lead to a compromise of the module.

9.0 Physical Security

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

The module is intended to be mounted in additional packaging; physical inspection of the die is typically not practical after packaging. Physical inspection of modules for tamper evidence is performed using a lot sampling technique during the card assembly process.

Note: Hardness testing was only performed at ambient temperature; no assurance is provided for Level 4 hardness conformance at any other temperature.

10.0 Mitigation of Other Attacks

The module implements the following attack detection and mitigation methods:

- Power Analysis
- Timing Analysis
- Fault Induction
- Flash Gun
- Electromagnetic Attacks
- Card Tearing

Power analysis - the module includes protections against SPA and DPA attacks for all embedded cryptographic algorithms involving secret elements, using a combination of hardware and software design that makes differentiation of key values impractical by equalizing or scrambling current consumption of the card during algorithm cryptographic computation. Based on the algorithm used, the defense mechanisms vary, as the internal hardware implementations of these algorithms do not use the same underlying hardware.

Timing attacks are non-invasive attacks that rely on the variation in computation time required for the microprocessor to perform its secret calculation. The module's algorithm implementations are written to mitigate timing attacks. All cryptographic algorithms, as well as Java Card API comparison functions offered by the chip, are designed to be protected against Timing Analysis. This is done by enforcing the fact that any sensitive operation is achieved in a constant time regardless of the value of keys or data involved.

Fault induction - the module includes protections to prevent operation in extreme conditions that might cause processing errors that could lead to revealing the values of cryptographic keys or secret elements. Extreme Conditions refer to abnormal temperature, external power supply and external clock supply. In addition, all keys and PINs are inegrity checked prior to use.

Flash gun - the module includes a combination of software and hardware protections in order to detect "Flash Gun" type of attacks and mitigates the attack by aborting current processing then becoming mute.

Electromagnetic attacks - the module includes a combination of software and hardware protections in order to detect "EMI" type of attacks and mitigate the attack by aborting current processing and then becoming mute.

Card Tearing - the module includes a combination of software and hardware protections in order to protect the card against damages potentially caused by a discontinued power (or RF for contactless) supply during an operation. Roll back mechanisms restore the card memory to a safe previous stable state during the next power-on sequence.

11.0 References

[1] ISO/IEC 7816-3 – Information Technology – Identification Cards – Integrated Circuit(s) with Contacts – Part 3: Electronic Signals and Transmission Protocols, December 1997 – Amendment, June 2002.
[2] ISO/IEC 7816-4 – Information Technology – Identification Cards – Integrated Circuit(s) with Contacts – Part 4: Interindustry Commands for Interchange, September 1995 – Amendment, December 1997.
[3] ISO/IEC 7816-5 – Information Technology – Identification Cards – Integrated Circuit(s) with Contacts – Part 5: Numbering system and registration procedure for application identifiers, June 1994 - Amendment, December 1996.
[4] ISO/IEC 14443-3 – Information Technology – Identification Cards – Contactless Integrated Circuit(s) Cards – Proximity Cards – Part 3: Initialization and Anti-collision, February 2001.
[5] ISO/IEC 14443-4 – Information Technology – Identification Cards – Contactless Integrated Circuit(s) Cards – Proximity Cards – Part 4: Transmission Protocols, February 2001.
[6] GlobalPlatform Card Specification, version 2.1.1, March 2003.
[7] GlobalPlatform Card Specification, Amendment A, February 2004.
[8] Visa GlobalPlatform 2.1.1 Card Implementation Requirements, May 2003.
[9] Java Card 2.2.2 Application Programming Interface, March 2006.

[10] Java Card 2.2.2 Run-time Environment Specification, March 2006.
[11] Java Card 2.2.2 Virtual Machine Specification, March 2006
[12] “Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher”, NIST January 2012

12.0 Definitions and Acronyms

Acronym	Definition
ACA	Access Control Applet
AP	Application Provider
APDU	Application Protocol Data Unit
API	Application Programming Interface
ATR	Answer To Reset (contact mode)
CBC	Cipher Block Chaining
CRC	Cyclic Redundancy Check
CSP	Critical Security Parameter
DES	Data Encryption Standard
DPA	Differential Power Analysis
ECB	Electronic Code Book
EEPROM	Electrically Erasable and Programmable Read Only Memory
EMI	Electromagnetic Interference
EMC	Electromagnetic Compatibility
GC	Generic Container
MAC	Message Authentication Code
OTP	One-Time Password
PIN	Personal Identification Number
PKCS	Public Key Cryptographic Standards
PKI	Public Key Infrastructure
RAM	Random Access Memory
RNG	Random Number Generator
ROM	Read only Memory
RSA	Public key cryptographic algorithm invented by Rivest, Shamir and Adleman
SPA	Simple Power Analysis
XAUT	External Authentication