ActivIdentity® Digital Identity Applet v2 on Gemalto's IDCore 3020 (v2)

FIPS 140-2 Cryptographic Module Security Policy

Version: 1.2
Date: September 13, 2013

Table of Contents

List of Tables

List of Figures

1 Introduction

This document defines the Security Policy for the ActivIdentity Digital Identity Applet v2 (v2.7) on Gemalto's IDCore 3020 (v2) cryptographic module, hereafter denoted *the Module*. The Module, validated to FIPS 140-2 overall Level 2, is a single chip smartcard module implementing the JavaCard platform, Global Platform operational environment, with Card Manager as well as the Digital Identity applet suite (including the PIV Applet 2.7).

The Module is intended for use by US Federal agencies and other markets that require smartcards with a [SP 800-73-3] conformant PIV End Point applet.

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	2
Roles, Services, and Authentication	3
Finite State Model	2
Physical Security	3
Operational Environment	N/A
Cryptographic Key Management	2
EMI/EMC	3
Self-Tests	2
Design Assurance	3
Mitigation of Other Attacks	2

Table 1 – Security Level of Security Requirements

The Module implementation is compliant with:

- [ISO 7816] Parts 1-4
- [ISO 14443] Parts 1-4
- [JavaCard]
- [GlobalPlatform]
- [SP 800-73-3] Interfaces for Personal Identity Verification, Parts 1-4
- [SP 800-78-3] Cryptographic Algorithms and Key Sizes for Personal Identity Verification

1.1 Hardware and Physical Cryptographic Boundary

The Module is designed to be embedded into plastic card bodies, USB tokens, key fobs, Secure SD cards or SIMs, with a contact plate and contactless antenna connections. The physical form of the Module is depicted in Figure 1 (to scale); below diagram depicts the physical cryptographic boundary, representing the surface of the chip and the bond pads. In production use, the module is wire-bonded to a frame connected to a contact plate, enclosed in epoxy and mounted in a card body. The contactless ports of the module are electrically connected to an antenna embedded in the card body. The Module relies on [ISO7816] and [ISO14443] card readers as input/output devices.

The Cryptographic Boundary is defined to be the 'ICC module edge' of the Cryptographic Module (**CM)** , comprising a set of "embedded" hardware and software that implements cryptographic functions and processes, including cryptographic algorithms and key generation and applications services. The FIPS 140-2 embodiment of the **CM** is single chip. The micro-module is designed to be embedded in a plastic card body to provide an **ISO-7816** compliant smart card.

The TOP DL v2 Cryptographic Module (now marketed as IDCore 3020 (v2) and referred to as such throughout this document) has already achieved FIPS 140-2 Level 3 validation. NIST Certificate #1450 provides detail information on the FIPS validation:

http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm#1450

Depending on the market and the end-customer requirements, PK [Public Key] support (i.e. PK enabled or PK disabled) and Secure Channel Protocol can be configured during the manufacturing in order to answer as precisely as possible to the market and the end-customer requirements:

- **CONFIGURATION 1**: The product is initialized in dual interface mode; it means that both contact and contact-less mode are operated, with FIPS PK self-tests and PK services enabled. The secure channel protocol is based on AES keys : GP-SCP03-00 (option i=00 as per **GP specification** [15]**)**.
- **CONFIGURATION 2**: The product is initialized in dual interface mode; it means that both contact and contact-less mode are operated, with FIPS PK self-tests and PK services enabled. The secure channel protocol is based on AES keys : GP-SCP03-10 (option i=10 as per **GP specification** [15]).
- **CONFIGURATION 3**: The product is initialized in dual interface mode; it means that both contact and contact-less mode are operated, with FIPS PK self-tests and PK services enabled. The secure channel protocol is based on Triple-DES : GP-SCP01

During the Gemalto manufacturing process, the chip (ICC) is wire-bonded on the inner side of a contact plate, then globe-topped with resin. **The resulting Micro-Module meets the physical security requirements of FIPS140-2 Level 3.**

The contact-less antenna is not within the cryptographic boundaries of the module.

All the components of the **IDCore 3020 (v2) - Micro-Module** that are included in the cryptographic module boundaries are those as shown in the following figure:

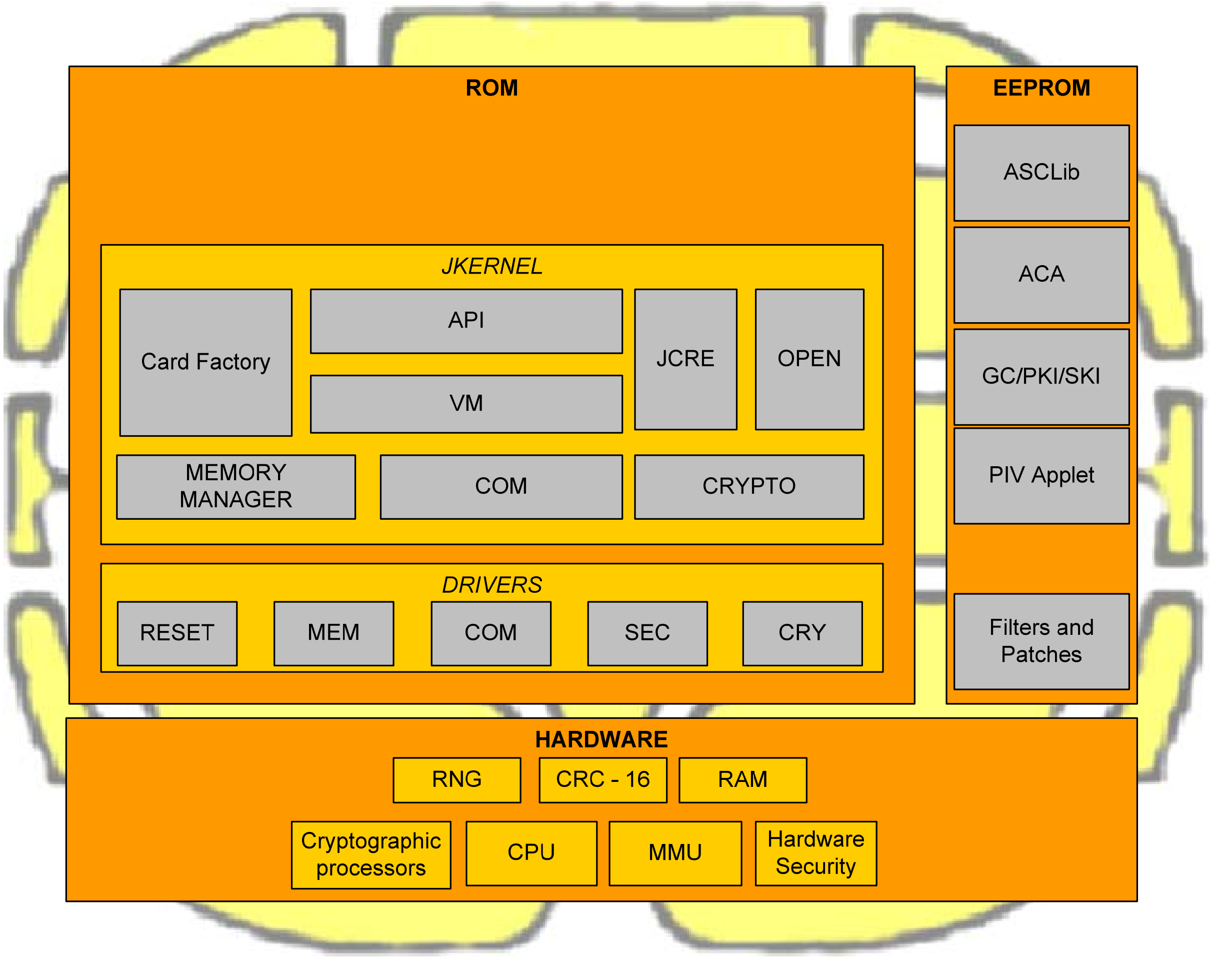

Figure 1 – Physical Form and Cryptographic Boundary

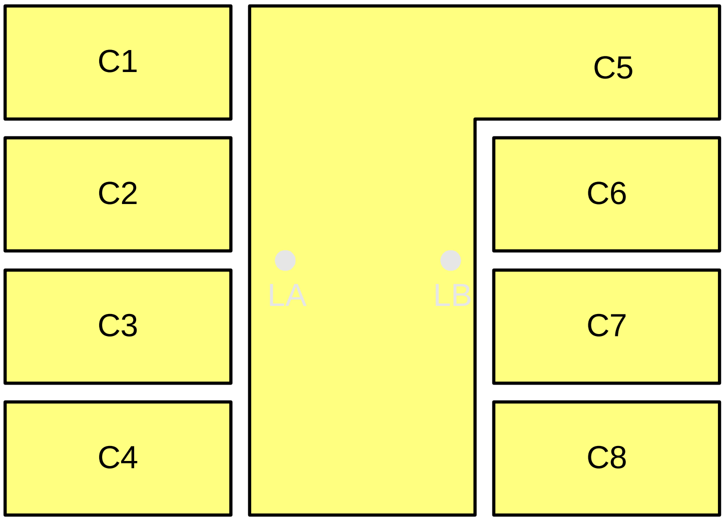

Figure 2 - Contact plate example – Contact physical interface

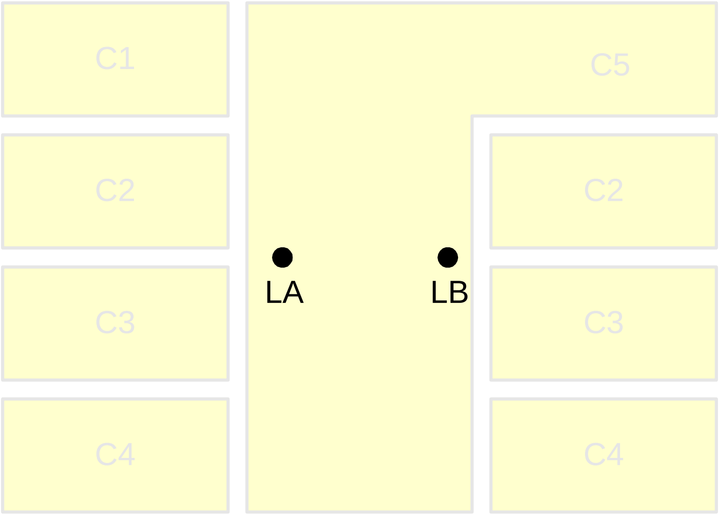

Figure 3 - Contact plate example - Contact-less antenna contacts

Pad	Description	Logical interface type
VSS, VDD	ISO 7816: Power and ground	Power
CLK	ISO 7816: Clock	Control in
RST_N	ISO 7816: Reset	Control in
IO	ISO 7816: Serial interface	Data in, data out, control in, status out
LA, LB	ISO 14443: Antenna	Data in, data out, control in, status out
NC	No connect	Not used

Table 2 – Ports and Interfaces

1.2 Firmware and Logical Cryptographic Boundary

Figure 1 above depicts the Module operational environment and applets.

- The ISO 7816 UART supports the T=0 and T=1 communications protocol variations
- The ISO 14443 communications block supports 13.56 MHz Type A signaling (106 kbps; 212 kbps; 424 kbps; 848 kpbs using T=CL protocol)
- 144 KB EEPROM; 240 KB ROM; 6 KB XRAM

List of Applets loaded in the module:

- **ASC Library package** – This is the library package that implements functions required by other applets. The library functions are not directly accessible via the cryptographic module command interface.
- **Access Control Applet (ACA)** – This applet is responsible for Access Control Rules (ACR) definition, access control rules enforcement and secure-messaging processing for all card services. Three off-card entity authentication methods – GP secure messaging, PIN, and ActivIdentity External Authentication are included by default in the ACA applet.
- **PKI/Generic Container/ SKI (PKI/GC/SKI) Applet** – The PKI/GC/SKI Applet can be used to provide secure storage for PKI credentials, and other data that are required for implementation of card services including single sign-on applications, identity, and benefits information. This applet is responsible for RSA-based cryptographic operations using the RSA private key stored in the PKI buffers. The applet also exposes services for OTP (One Time Password) through a synchronous or asynchronous authentication.
- **PIV EP Wrapper Applet -** This Applet implements SP800-73-3 (both at card-edge and data model levels). The Applet is a wrapper on top of v2.7 applets (ASCLIB, ACA and GC/PKI/SKI above). Its purpose is to access the PIV card-edge and objects although objects are physically stored in the GC/PKI/SKI applet instances. This PIV applet cannot operate in standalone mode, it must interface with the ACA and GC/PKI/SKI applet to operate properly. This applet can only be instantiated in a strictly compliant mode to SP800-73-3 meaning the applet doesn't support extensions as PIV EP Extended applet below does.
- **PIV EP Extended (Ext) Applet** – This Applet implements SP800-73-3 (both at card-edge and data model levels) and is extended to support additional features on top of native PIV such as support of additional PKI RSA keys (example: PKI Key Encryption Key, SSO (single sign-on) storage, SKI authentication mechanisms, etc). This applet can be instantiated in PIV EP mode (native PIV features) or in PIV Ext mode (extensions are accessible through the 800-73-3 card edge.)

Section 3 describes applet functionality in greater detail. The JavaCard API is an internal interface, available to applets. Only applet services are available at the card edge (the interfaces that cross the cryptographic boundary).

1.3 Versions and mode of operation

Hardware: A1023378
Firmware: Build#11 - M1005011+ Softmask V03, Applet Version: Digital Identity Applet Suite 2.7

The Digital Identity Applet Suite 2.7 includes the following applet versions:

- ASCLIB: 2.7.0.6
- ACA: 2.7.0.5
- GC/PKI/SKI: 2.7.0.4
- PIV Extended: 2.7.0.5
- PIV Wrapper: 2.7.0.3

The module provides only a FIPS 140-2 Approved mode. To verify that a module is in the approved mode of operation, an operator sends the commands shown below. The Module responds with the following information:

Command and associated elements	Expected Response
GET DATA command with Tag 01 01h	16 bytes of data broken down as follows: Card serial number: 8 bytes Reserved bytes: 3 bytes **Flow identification: 1 byte** Reserved bytes: 4 bytes The 12th Flow id bytes are: 0x = Non FIPS mode 1x = FIPS mode 11 = FIPS + SCP01 13 = FIPS + SCP03 17 = FIPS + SCP03-10
GET PROPERTIES command (tag 24) *(with ACA applet selected)*	01 (For FIPS 140-2 L2 mode)

Table 3 –Versions and Mode of Operations Indicators

2 Roles, authentication and services

Table 4 - Roles description lists all operator roles supported by the module. This Module does not support a maintenance role. The Module supports multiple concurrent operators via MANAGE CHANNEL, but permits only one role to be authenticated at any time, and clears previous authentications on power cycle.

Role ID	Role Description
CO	Cryptographic Officer: This role is responsible for card issuance and management of card data via the Card Manager and Digital Identity Applet Suite. Authenticated using the SCP authentication method with SD-SENC and SD-SMAC.
CH	Card Holder (the User role for FIPS 140-2 validation purposes). The Card Holder uses the Module for an identity token. Authenticated in the PIV applet using the VERIFY authentication method with PIV-LPIN.
AA	Applet Administrator. The AA role is responsible for configuration of the PIV data using the PIV applet PUT DATA and GENERATE ASYMMETRIC KEY PAIR services. - Authenticated in the PIV applet using the PIV CMK authentication method with PIV-SCMK.
PU	PIN Unblocking User – this role is associated with a single PIV service, RESET RETRY COUNTER, which requires knowledge of PIV-PUK.

Table 4 - Roles description

2.1 Secure Channel Protocol (SCP) Authentication

The Global Platform Secure Channel Protocol authentication method is performed when the EXTERNAL AUTHENTICATE service is invoked after successful execution of the INITIALIZE UPDATE command. These two commands operate as described next. In the description below, the process is identical regardless of domain, e.g. Issuer Security Domain (ISD) or Application Security Domain (ASD).

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

Note that the only use of the any of the domain keys for encryption is for a total of 1 block over the life of the associated SD-SENC session key. The Module's designed encryption limitation using SD-SENC prevents the meet-in-the-middle attack described in [SP800-131A]. In accordance with [SP800-131A], the Module's 2-Key TRIPLE-DES security strength is determined to be 112 bits. Based on this strength and a 64 bit authentication data block size:

- The probability that a random attempt at authentication will succeed is 1/2^64, meeting the FIPS requirement of 1/1,000,000.
- Based on the maximum count value of the failed authentication blocking mechanism, the probability that a random attempt will succeed over a one minute period is 255/2^64, meeting the FIPS requirement of 1/100,000 in a one minute period.

2.2 PIV Applet PIN Comparison Authentication

This authentication method compares a PIN value sent to the Module to the stored PIV-LPIN or PIV-PUK values; if the two values are equal, the operator is authenticated. This method is used in the VERIFY and CHANGE REFERENCE DATA services to authenticate to the CH role, and by the RESET RETRY COUNTER service to authenticate to the PU role.

The strength of authentication for this authentication method depends on both internal and external factors. The Module compares all 8 characters of the PIV-LPIN or PIV-PUK value and the PIN authentication strength is based on the fact that PIN value is encoded on eight bytes (eight bit for each byte) on the assumption that the values span the entire spectrum of characters represented by an 8-bit values. Based on this, the strength of this authentication method is as follows:

- The probability that a random attempt at authentication will succeed is 1/256^8, meeting the FIPS requirement of 1/1,000,000.
- Based on the [SP800-73-3] defined maximum count of 15 for failed VERIFY or CHANGE REFERENCE DATA attempts, the probability that a random attempt will succeed over a one minute period is 15/256^8, meeting the FIPS requirement of 1/100,000 in a one minute period.

Please see Section 9 for guidance on required external security procedures associated with the PIV Applet PIN Comparison authentication method.

2.3 PIV Applet Symmetric Cryptographic Authentication

This authentication method decrypts (using PIV-SCMK) an encrypted challenge sent to the module by an external entity and compares the challenge to the expected value.

The strength of authentication for this authentication method is based on the strength of PIV-SCMK; only 3-Key TRIPLE-DES are allowed for this key, with a security strength of 112 bits, hence the associated strength of this authentication methods is:

- The probability that a random attempt at authentication will succeed is 1/2^64, meeting the FIPS requirement of 1/1,000,000.
- The execution of this authentication mechanism is rate limited – the module can perform no more than 2^16 attempts per minute. Therefore, the probability that a random attempt will succeed over a one minute period is 2^16/2^64, meeting the FIPS requirement of 1/100,000 in a one minute period.

2.4 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.

Service	Description
Card Reset (Self-test)	Power cycle the Module by removing and reinserting it into the contact reader slot, or by reader assertion of the RST signal. The *Card Reset* service invokes the power on self-tests as described in Section 4. On any card reset, the Module overwrites OS-SEED, OS-SEED-KEY and OS-RNG_STATE. On any card reset, the card overwrites all volatile memory.
GET RESPONSE	Fetch remaining data to read from the Card (e.g in response to GET ACR command). **CSP Usage**: Does not use CSPs. **Interface availability**: Contact-Contactless
SELECT	Select an applet. **CSP Usage**: Does not use CSPs. **Interface availability**: Contact-Contactless

Table 5 - Unauthenticated Services Available to Any Applet

The UN column in the tables below indicates unauthenticated commands available in that applet.

Service	Description	CO	UN
DELETE	Delete an applet instance or package from EEPROM. **CSP usage**: Destroys all CSPs associated with the deleted applet or package by overwriting memory. **Interface availability**: Contact-Contactless	X	
EXTERNAL AUTHENTICATE	Authenticates the operator and establishes a secure channel. Must be preceded by a successful INITIALIZE UPDATE. **CSP Usage**: Executes using SD-SENC, SD-SMAC. **Interface availability**: Contact-Contactless		X
GET DATA	Retrieve a single data object. **CSP Usage**: Does not use CSPs. **Interface availability**: Contact-Contactless		X
GET STATUS	Retrieve information about the card. **CSP Usage**: Does not use CSPs. **Interface availability**: Contact-Contactless	X	
INSTALL	Perform Card Content management. **CSP Usage**: Does not use CSPs. **Interface availability**: Contact-Contactless	X	
INITIALIZE UPDATE	Initialize the Secure Channel; to be followed by EXTERNAL AUTHENTICATE. **CSP Usage**: Executes using SD-KENC, SD-KMAC. Writes SD-SENC, SD-SMAC. **Interface availability**: Contact-Contactless		X
LOAD	Load a load file (e.g. an applet). **CSP Usage**: Executes using SD-SENC, SD-SMAC.	X	

Service	Description	CO	UN
	Interface availability: Contact-Contactless		
MANAGE CHANNEL	Opens and closes supplementary logical channels. **CSP Usage**: Does not use CSPs. **Interface availability**: Contact-Contactless		X
PUT KEY	Load Card Manager keys as well as the XAUT keys (like used to unblock the PIN), the RSA private key component or the SKI key for One Time Password generation. **CSP Usage**: SD-KKEK. Writes SD-KENC, SD-KMAC, SD-KKEK. **Interface availability**: Contact-Contactless	X	
SET STATUS	Modify the card or applet life cycle status. **CSP Usage**: Does not use CSPs. **Interface availability**: Contact-Contactless	X	
STORE DATA	Transfer data to an application during command processing. **CSP Usage**: Does not use CSPs. **Interface availability**: Contact-Contactless	X	

Table 6 – Card Manager Services and CSP Usage

Service	Description	CO	CH	PU	AA	UN
AC EXTERNAL AUTHENTICATE	Used in combination with a GET CHALLENGE to authenticate the AA using the AC external authenticate protocol. **CSP Usage:** Execute with ACA-SPAK **Interface availability:** Contact-Contactless					X
CHANGE REFERENCE DATA	Create the PIN (PIV-LPIN) and PUK (PIV-PUK) in the card. It is also used to update the PUK value. **CSP Usage**: Write PIV-LPIN, PIV-PUK **Interface availability**: Contact only	X	X			
EXTERNAL AUTHENTICATE	Authenticates the operator and establishes a secure channel. Must be preceded by a successful INITIALIZE UPDATE. **CSP Usage**: Execute with SD-SENC, SD-SMAC. **Interface availability**: Contact only					X
GET ACR	Extract the public ACR (Access Control Rule) or ACR-ID-INS or Applet table properties as configured during the card issuance process **CSP Usage**: Does not use CSPs. **Interface availability**: Contact-Contactless					X
GET CHALLENGE	Retrieve a challenge from the card too perform a host authentication: first step of the AC EXTERNAL AUTHENTICATION process **CSP Usage**: Does not use CSPs. **Interface availability**: Contact-Contactless					X
GET PROPERTIES	Retrieve Applet instance properties (marked only with "public" attribute) **CSP Usage**: Does not use CSPs. **Interface availability**: Contact-Contactless					X
INITIALIZE UPDATE	Initialize the Secure Channel; to be followed by EXTERNAL					X

Service	Description	CO	CH	PU	AA	UN
	AUTHENTICATE. **CSP Usage**: Executes using SD-KENC, SD-KMAC. Writes SD-SENC, SD-SMAC. **Interface availability**: Contact only					
LOGOUT	Logout all previously authenticated roles **CSP Usage**: Does not use CSPs. **Interface availability**: Contact-Contactless					X
PUT KEY	Load XAUT keys (like used to unblock the PIN) **CSP Usage**: Write ACA-SPAK. Execute using SD_KKEK **Interface availability**: Contact only	X			X	
REGISTER ACR	Manages the mapping between ACR-ID and actual APDU instruction as well as record the ACR definition for the applet services **CSP Usage**: Does not use CSPs. **Interface availability**: Contact only	X				
REGISTER APPLET	Record applet instances to the ACA instance so that the access control and secure message service can be provided. **CSP Usage**: Does not use CSPs. **Interface availability**: Contact only	X				
RESET CARD	Reset the card content (buffer content, PKI credentials, SKI keys as well the PIN/PUK) **CSP Usage**: Destroy ACA-SPAK, PIV-LPIN, PIV-PUK, PKI-GPK and PKI-GPKPUB **Interface availability**: Contact only		X		X	X
RESET RETRY COUNTER	Used to unblock the cardholder PIN (PIV-LPIN) and restore the VERIFY service with a new counter value if the CM role is authenticated successfully. The command operates as long as the unblock counter has not expired. **CSP Usage**: Write PIV-LPIN **Interface availability**: Contact only	X		X		
SET APPLICATION UID	Initialize the UID (unique identifier) associated with the applet instance **CSP Usage**: Does not use CSPs. **Interface availability**: Contact only	X				
SET STATUS	Modify the card or applet life cycle status **CSP Usage**: Does not use CSPs. **Interface availability**: Contact only	X				
UPDATE PROPERTIES	Updates the Applet properties **CSP Usage**: Does not use CSPs. **Interface availability**: Contact only	X	X		X	X
VERIFY	Check the PIN presented by the cardholder against the current PIN. **CSP Usage**: Execute with PIV-LPIN **Interface availability**: Contact-Contactless		X			

Table 7 – ACA Applet Services and CSP Usage

Service	Description	CO	CH	AA	UN
AC EXTERNAL AUTHENTICATE	APDU is used in combination with a GET CHALLENGE to authenticate the AA using the AC external authenticate protocol. **CSP Usage**: Use ACA-SPAK **Interface availability**: Contact only			X	
EXTERNAL AUTHENTICATE	Authenticates the operator and establishes a secure channel. Must be preceded by a successful INITIALIZE UPDATE. **CSP Usage**: Execute with SD-SENC, SD-SMAC. **Interface availability**: Contact only				X
GENERATE KEY	Generate an RSA Key Pair in the cryptographic module. The Private Key is associated with a PKI Applet instance. **CSP Usage**: Write PKI-RGPK and PKI-RGPKPUB **Interface availability**: Contact only	X	X	X	
GET CHALLENGE	Retrieve a challenge from the card too perform a host authentication: first step of the AC EXTERNAL AUTHENTICATION process) **CSP Usage**: Does not use CSPs. **Interface availability**: Contact only				X
GET DATA	Retrieve a single data object **CSP Usage**: Does not use CSPs. **Interface availability**: Contact-Contactless		X		X
GET PROPERTIES	Retrieve Applet instance properties (marked only with "public" attribute) **CSP Usage**: Does not use CSPs. **Interface availability**: Contact-Contactless				X
INITIALIZE UPDATE	Initialize the Secure Channel; to be followed by EXTERNAL AUTHENTICATE. **CSP Usage**: Executes using SD-KENC, SD-KMAC. Writes SD-SENC, SD-SMAC. **Interface availability**: Contact only				X
INTERNAL AUTHENTICATE	Perform SKI operations to generate a cryptogram from the card for verification by the calling application. **CSP Usage**: Execute with SKI-OTP **Interface availability**: Contact-Contactless		X		X
PRIVATE SIGN/DECRYPT	Use the RSA private key in the PKI buffer to sign data. **CSP Usage**: Execute with PKI-RGPK and PKI-RGPKPUB **Interface availability**: Contact-Contactless		X	X	
PUT KEY	Inject the RSA private key component to the module **CSP Usage**: Write PKI-RGPK and PKI-RGPKPUB **Interface availability**: Contact only	X		X	
READ BINARY	Reads binary data stored on the card **CSP Usage**: Does not use CSPs **Interface availability**: Contact only				X

Service	Description	CO	CH	AA	UN
SET PROPERTIES	Load Applet properties **CSP Usage**: Does not use CSPs **Interface availability**: Contact only	X	X		X
SET STATUS	Modify the card or applet life cycle status **CSP Usage**: Does not use CSPs. **Interface availability**: Contact only	X			
READ CERTIFICATE BUFFER / READ BUFFER	Read the data from the selected buffer **CSP Usage**: Does not use CSPs **Interface availability**: Contact-Contactless		X	X	X
UPDATE CERTIFICATE BUFFER / UPDATE BUFFER	Write data into the selected buffer **CSP Usage**: Does not use CSPs **Interface availability**: Contact-Contactless	X	X	X	X
VERIFY	Performs VERIFY authentication; executes using PIV-LPIN as specified in the APDU. **CSP Usage**: Execute with PIV-LPIN **Interface availability**: Contact-Contactless		X		

Table 8 – GC/PKI/SKI Applet Services and CSP Usage

Service	Description	CO	CH	PU	AA	UN
CHANGE REFERENCE DATA	**Used for**: change the PIV-LPIN. Successful execution of this service is an instance of the VERIFY authentication method; that is, the CH holder has been authenticated. **CSP usage**: PIV-LPIN: execute, update. **Interface availability**: Contact only.		X			
GENERAL AUTHENTICATE	As defined in [SP 800-73-3], this service has several different usages depending on the command tags embedded in the APDU, and also on the prior execution of other commands in a protocol. **Used for**: AA role (9B) authentication. Does not require prior authentication. **CSP usage**: PIV-SCMK: execute. **Interface availability**: Contact only. **Used for**: authentication of the card to the external system. **CSP usage**: PIV-RCAK: execute. **Interface availability**: Contact or Contactless only. **Used for**: authentication of the PIV Applet to the external system. Requires prior authentication to the CH role. **CSP usage**: PIV-RPAK: execute. **Interface availability**: Contact only. **Used for**: decryption of the key provided by an external system (the key provided by the external system in the command message has been encrypted by an external system using the PIV-RKEK). Requires prior authentication to the CH role.		X		X	

Service	Description	CO	CH	PU	AA	UN
	CSP usage: PIV-RKDK: execute. **Interface availability**: Contact only. **Used for:** Signing a hashed message provided by an external system. Requires authentication to the CH role in the message *immediately preceding* this command. **CSP usage**: PIV-RDSK: execute. **Interface availability**: Contact only. **Used for**: nonce generation for use as a challenge. **CSP usage**: OS RNG-STATE: execute. **Interface availability**: Contact only.					X
GENERATE ASYMMETRIC KEY PAIR	**Used for**: When authenticated to the AA role, generates new PIV RSA keys. Writes the PIV-RPAK, PIV-RDSK, PIV-RKDK, PIV-RCAK, as designated in the APDU. When used with the PIV-RKDK only the current key location may be specified; the retired key locations '82' through '95' cannot be overwritten with this command. **CSP Usage**: Execute. **Interface availability**: Contact only.	X			X	
GET DATA (PIV Variant)	**Used for**: Retrieve a single data object managed by the PIV applet access control conditions. If the VERIFY(PIN) security condition is met, access to containers with the PIN condition are allowed. Containers with the ALWAYS access control condition are always allowed. **CSP Usage**: This service does not use any CSPs. **Interface availability**: Contact-Contactless		X			X
PUT DATA	**Used for**: An operator authenticated to the AA role can replace the contents of PIV Data objects using this APDU command. **CPS Usage**: This service does not use any CSPs. **Interface availability**: Contact only	X			X	
RESET RETRY COUNTER	**Used for**: Change the PIV-LPIN. This service requires authentication of the current PIV-PUK value (i.e. authentication of the PU role) to succeed. **CSP Usage**: Executes using PIV-PUK, updates the counter associated with PIV-LPIN. **Interface availability**: Contact only			X		
VERIFY	**Used for**: Performs VERIFY authentication; **CSP Usage**: Executes using PIV-LPIN as specified in the APDU. **Interface availability**: Contact only					X

Table 9 – PIV Extended Applet Services and CSP Usage

Service	Description	CO	CH	PU	AA	UN
CHANGE REFERENCE DATA	**Used for**: change the PIV-LPIN. Successful execution of this service is an instance of the VERIFY authentication method;		X			

Service	Description	CO	CH	PU	AA	UN
	that is, the CH holder has been authenticated. **CSP usage**: PIV-LPIN: execute, update. **Interface availability**: Contact only.					
GENERAL AUTHENTICATE	As defined in [SP 800-73-3], this service has several different usages depending on the command tags embedded in the APDU, and also on the prior execution of other commands in a protocol. **Used for**: AA role (9B) authentication. Does not require prior authentication. **CSP usage**: PIV-SCMK: execute. **Interface availability**: Contact only. **Used for**: authentication of the card to the external system. **CSP usage**: PIV-RCAK: execute. **Interface availability**: Contact or Contactless only. **Used for**: authentication of the PIV Applet to the external system. Requires prior authentication to the CH role. **CSP usage**: PIV-RPAK: execute. **Interface availability**: Contact only. **Used for**: decryption of the key provided by an external system (the key provided by the external system in the command message has been encrypted by an external system using the PIV-RKEK). Requires prior authentication to the CH role. **CSP usage**: PIV-RKDK: execute. **Interface availability**: Contact only. **Used for:** Signing a hashed message provided by an external system. Requires authentication to the CH role in the message *immediately preceding* this command. **CSP usage**: PIV-RDSK: execute. **Interface availability**: Contact only. **Used for**: nonce generation for use as a challenge. **CSP usage**: OS RNG-STATE: execute. **Interface availability**: Contact only.		X		X	X
GENERATE ASYMMETRIC KEY PAIR	**Used for**: In this version, the applet only returns an exception as the RSA key generation is done from the GC/PKI/SKI applet. **CSP Usage**: Execute. **Interface availability**: Contact only.	X			X	
GET DATA (PIV Variant)	**Used for**: Retrieve a single data object managed by the PIV applet access control conditions. If the VERIFY(PIN) security condition is met, access to containers with the PIN condition are allowed. Containers with the ALWAYS access control condition are always allowed. **CSP Usage**: This service does not use any CSPs. **Interface availability**: Contact-Contactless		X			X
PUT DATA	**Used for**: In this version, the applet only returns an exception as the injection of PIV data is done from the GC/PKI/SKI applet	X			X	

Service	Description	CO	CH	PU	AA	UN
	CPS Usage: This service does not use any CSPs. **Interface availability**: Contact only					
RESET RETRY COUNTER	**Used for**: Change the PIV-LPIN. This service requires authentication of the current PIV-PUK value (i.e. authentication of the PU role) to succeed. **CSP Usage**: Executes using PIV-PUK, updates the counter associated with PIV-LPIN. **Interface availability**: Contact only			X		
VERIFY	**Used for**: Performs VERIFY authentication; **CSP Usage**: Executes using PIV-LPIN as specified in the APDU. **Interface availability**: Contact only					X

Table 10 – PIV Wrapper Applet Services and CSP Usage

3 Finite State Model

The Module is designed using a finite state machine model that explicitly specifies every operational and error state. The Module includes Power on/off states, Cryptographic Officer states, User services states, applet loading states, Key/PIN loading states, Self-test states, Error states, and the GP life cycle states.

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

4 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 SYSTEM HALTED error state. Furthermore, attempts to attack the chip or micro-module will result in signs of tampering such as scratches and deformation.

The Module is intended to be mounted in a plastic smartcard or other package as described in Section 1; physical inspection of the module boundary is not practical after mounting. Physical inspection of modules for tamper evidence is performed using a lot sampling technique during the card assembly process.

5 Operational Environment

The Module is designated as a limited operational environment under the FIPS 140-2 definitions. Therefore, this section does not apply.

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 require a separate FIPS 140-2 validation.

6 Cryptographic Key Management

The Module operating system implements the FIPS Approved and cryptographic function listed in Table 11 below.

Algorithm	Description	Cert #
AES	CBC and ECB modes.	1363
ECDSA	[ANSI X9.62] ECDSA signature generation/verification/key pair generation. P-192, P-224, P-384, P-512	172
RNG	[ANSI X9.31] RNG, based on the TRIPLE-DES algorithm.	749
SHS	Hashing operation	1243
TRIPLE-DES	[SP 800-67] Triple Data Encryption Algorithm. The module supports the 2-Key and 3-Key options; CBC and ECB modes.	938
TRIPLE-DES MAC	[FIPS113] TRIPLE-DES Message Authentication Code. Vendor affirmed, based on the validated TRIPLE-DES above.	Vendor affirmed

RSA	[PKCS#1] RSA signature generation. The module follows PKCS#1 and supports 1024- and 2048-bit RSA keys. Note that all uses of RSA follow PIV specifications, requiring hash off-card.	664

Table 11 – FIPS Approved Cryptographic Functions

Note that the module supports 2-Key TRIPLE-DES. [SP 800-131A] Section A.1 provides the NIST rationale for 2-Key TRIPLE-DES security strength. 2-Key TRIPLE-DES is used exclusively for Global Platform secure channel operations, in which the module derives session keys from the master keys and a handshake process, performs mutual authentication, and decrypts data for internal use only. The Module encrypts a total of one block (the mutual authentication cryptogram) over the life of the session encryption key; no decrypted data is output by the module. The Module claims 112-bit security strength for its 2-Key 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.

2-Key TDEA key establishment in this context provides 112 bits of security strength. The module uses the SD-SKEK keys to decrypt critical security parameters, and does not perform encryption with this key or output data decrypted with this key.

6.1 Critical Security Parameters

All CSPs used by the Module are described in this section. All usage of these CSPs by the Module, including all CSP lifecycle states, are described in the services detailed in Section 4.

Note that the OS-SEED, OS-SEED-KEY, and OS-MKEK CSPs are all generated by an HSM and input into the Module in the factory during initialization process.

Key	Description / Usage
OS-SEED	64 bit random value from HW RNG used to seed the [ANSI X9.31] RNG.
OS-SEED-KEY	3-key TRIPLE-DES key generated by HW RNG, used for the RNG seed key
OS-RNG_STATE	32 bit value; Current RNG state
OS-MKEK	2-Key TRIPLE-DES Master key used to encrypt all key data stored in the EEPROM.
Domain Key Set (ISD or ASD)	
SD-KENC	2-Key TRIPLE-DES Master key used by the CM role to generate SD-SENC
SD-KMAC	2-Key TRIPLE-DES Master key used by the CM role to generate SD-SMAC.
SD-KKEK	2-Key TRIPLE-DES Sensitive data decryption key used by the Module role to decrypt CSPs.
SD-SENC	2-Key TRIPLE-DES Session encryption key used by the Module role to encrypt / decrypt secure channel data.
SD-SMAC	2-Key TRIPLE-DES Session MAC key used by the Module role to verify inbound secure channel data integrity.
ACA Applet Keys	
ACA-SPAK	2-Key or 3-Key TRIPLE-DES key used by the ACA applet to authenticate the AA role (0-7 keys)
GC/PKI/SKI Applet Keys	
PKI-GPK	RSA 1024, 2048 for general purpose Key with usage determined outside the module scope
SKI-OTP	2-Key or 3-Key TRIPLE-DES key used by the GC/PKI/SKI applet for one time password generation (0-2 keys)
PIV Keys for PIV Extended Applet	
PIV-LPIN	8 character string PIV application Local PIN
PIV-PUK	8 character string PIV PIN Unblocking Key
PIV-RPAK	RSA 1024, 2048 PIV Authentication (9A) RSA Authentication Key
PIV-SCMK	3-Key Triple DES PIV Card Management (9B) Symmetric Authentication Key
PIV-RDSK	RSA 2048 PIV Digital Signature (9C) RSA Private Signature Key
PIV-RKDK	RSA 2048 PIV Key Management (9D) RSA Key Decryption Key Up to 20 copies of this key may be stored in retired key locations '82' though '95'.
PIV-RCAK	RSA 1024, 2048 Card Authentication (9E) RSA Authentication Key

PIV Keys for PIV Wrapper Applet	
PIV-LPIN	8 character string PIV application Local PIN
PIV-RPAK	RSA 1024, 2048 PIV Authentication (9A) RSA Authentication Key
PIV-RDSK	RSA 2048 PIV Digital Signature (9C) RSA Private Signature Key
PIV-RKDK	RSA 2048 PIV Key Management (9D) RSA Key Decryption Key Up to 5 copies of this key may be stored in retired key locations '82' though '86'.
PIV-RCAK	RSA 1024, 2048 Card Authentication (9E) RSA Authentication Key

Table 12 - Module Critical Security Parameters

6.2 Public keys

Key	Description / Usage
GC/PKI/SKI and PIV Public Keys	
PKI-RGPKPUB	RSA 1024, 2048 for general purpose Key with usage determined outside the module scope
PIV-RPAKPUB	RSA 1024, 2048 PIV Authentication (9A) RSA Authentication Public Key
PIV-RDSKPUB	RSA 2048 PIV Digital Signature (9C) RSA Signature Verification Key
PIV-RKDKPUB	RSA 2048 PIV Authentication (9D) RSA Key Decryption Key
PIV-RCAKPUB	RSA 1024, 2048 Card Authentication (9E) RSA Authentication Public Key

Table 13 - Public Keys

The PIV applet specification defines the generation of asymmetric key pairs for PIV authentication (9A), digital signature (9C), key management (9D, with retired copies in 82-95 for PIV Extended and in 82-86 for the PIV Wrapper Applet) and card authentication (9E). When the GENERATE ASYMMETRIC KEY PAIR service is called, the public keys listed above are returned by the PIV applet. An external entity (e.g., a card management system) is responsible for packaging the public key in an X509 certificate and storing it in the corresponding X509 certificate container in the PIV applet. The PIV applet does not make use of the public key after generation, and does not define any other usage of public keys.

7 Electromagnetic Interference/Electromagnetic 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 Self-Tests

8.1 Power-on self-test

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

On power on or reset, the Module performs the self-tests described in Table 14 below. All KATs must be completed successfully prior to any other use of cryptography by the Module.

Test Target	Description
Firmware Integrity	16 bit CRC performed over all code located in EEPROM.
RNG	Performs the [ANS X9.31] RNG KAT.
TRIPLE-DES	Performs separate encrypt and decrypt KATs using 2-Key TRIPLE-DES in ECB mode.
RSA	Performs separate RSA PKCS#1 signature and verification KATs using an RSA 1024 bit key. Note that all uses of RSA follow PIV specifications, requiring hash off-card.

Table 14 – Power-On Self-Test

8.2 Conditional self-tests

On every call to the HW RNG or [ANSI X9.31] RNG, the Module performs a continuous random number generator test to assure that the output is different than the previous value.

The Module performs a pairwise consistency test when any asymmetric key pair is generated.

When new firmware is loaded into the module using the LOAD command, the module verifies the integrity of the new firmware using a TRIPLE-DES MAC process and the SD-SMAC key.

9 Design Assurance

The **CM** meets the Level 3 Design Assurance section requirements.

9.1 Configuration Management

The **CM** is designed and developed using a configuration management system that is operated with clear rules.

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

9.2 Delivery and Operation

The **CM** is designed and developed using a configuration management system that is operated with clear rules.

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

10 Mitigation of other attacks

The Module implements defenses against:

- Timing Attacks
- Differential Power Analysis
- Simple Power Analysis
- Electromagnetic Analysis
- Fault Attack
- Card Tearing

In these cases the main major task of the countermeasures is to remove the dependencies that exist between processed data and the current and/or time, electromagnetic consumption/processing/emission. To mitigate these side channel attacks the platforms implements countermeasures in order to make blurring instrumentation & signal analysis and a wide variety of numerical/logical tricks that decorrelate the side channel from the secret data.
Software countermeasures are random order execution, random delay, parallel processing to add noise, usage of encrypted logical data to remove correlation between current consumption and logical data and hardware countermeasures is desynchronized as dummy cycles, unstable clocking, noise (current scrambling, smoothing) and sensors activation, memory ciphering.

Fault Attacks:
The fault attacks are semi-invasive attacks. The goal of this kind of attacks is to perturb the 'normal' execution of the chip in order to find out or corrupt sensitive or critical parameters. Faults may be used to create exploitable vulnerabilities.
Card Tearing is a fault attack. Card tearing (or power failure) may cause inconsistency data.

To mitigate fault attacks countermeasures implemented are the activation of the hardware sensors before sensitive processes, the detection of repetitive fault attacks using detection counter and putting the cryptographic module in terminated state once the number of detection has reached its maximum quota, the backup for operations on sensitive data, the redundancy to check consistency of secure processes, the check of data integrity, the usage of non-reversible life cycle states, the memory ciphering and bus protection.

A separate and proprietary document from Gemalto describes the mitigation of attacks policy provided by the Module.

11 Security Rules and Guidance

The Module implementation also enforces the following security rules:

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

In addition, the following guidance must be followed to operate the Module within the conditions describes any further rules for using the module in accordance with the conditions of the FIPS 140-2 validation.

- PIV Applet administrators are required to procedurally enforce usage policy that ensures end user's PIV PIN values meet the conditions as described in [SP80073-3-3] and that the selected PIN values also meet the FIPS 140-2 security strength of 1/1,000,000.

12 References

The following standards are referred to in this Security Policy.

Acronym	Full Specification Name
[FIPS140-2]	*Security Requirements for Cryptographic Modules*, May 25, 2001
[FIPS201-1]	*Personal Identity Verification (PIV) Of Federal Employees and Contractors*, March 2006
[ISO 7816]	ISO/IEC 7816-1: 1998 *Identification cards -- Integrated circuit(s) cards with contacts -- Part 1: Physical characteristics* ISO/IEC 7816-2:2007 *Identification cards -- Integrated circuit cards -- Part 2: Cards with contacts -- Dimensions and location of the contacts* ISO/IEC 7816-3:2006 *Identification cards -- Integrated circuit cards -- Part 3: Cards with contacts -- Electrical interface and transmission protocols* ISO/IEC 7816-4:2005 *Identification cards -- Integrated circuit cards -- Part 4: Organization, security and commands for interchange*
[ISO 14443]	ISO/IEC 14443-1:2008 Identification cards -- Contactless integrated circuit cards -- Proximity cards -- Part 1: Physical characteristics ISO/IEC 14443-2:2001 Identification cards -- Contactless integrated circuit(s) cards -- Proximity cards -- Part 2: Radio frequency power and signal interface ISO/IEC 14443-3:2001 Identification cards -- Contactless integrated circuit(s) cards -- Proximity cards -- Part 3: Initialization and anticollision ISO/IEC 14443-4:2008 Identification cards -- Contactless integrated circuit cards -- Proximity cards -- Part 4: Transmission protocol
[JavaCard]	Please cite the correct document
[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
[SP800-131A]	*Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths*, January 2011
[SP800-73-3]	*Interfaces for Personal Identity Verification - Part 1: End-Point PIV Card Application Namespace, Data Model and Representation,* February 2010 *Interfaces for Personal Identity Verification - Part 2: End-Point PIV Card Application Card Command Interface,* February 2010
[SP800-78-3]	*Cryptographic Algorithms and Key Sizes for Personal Identity Verification*, December 2010
[FIPS 140-2 IG]	*Implementation Guidance for FIPS PUB 140-2 and the Cryptographic Module Validation Program,* March 2011
[AES Key Wrap]	*AES Key Wrap Specification, 16 November 2001, NIST*

Table 15 – References

13 Acronyms and definitions

Acronym	Definition
ACA	Access Control Applet
APDU	Application Protocol Data Unit
GP	Global Platform
KAT	Known Answer Test
MMU	Memory Management Unit
PUK	Pin Unblocking Key
OPACITY	Open Protocol for Access Control Identification and Ticketing
RSA	Rivest Shamir and Adelman
XAUT	External Authentication

Table 16 – Acronyms and Definitions