NXP Semiconductors
JCOP4 P71

FIPS 140-2 Cryptographic Module
Non-Proprietary Security Policy

Document Version: 1.2
Date: 26/10/2020

Table of Contents

References **4**

Acronyms and Definitions **6**

1 Overview **7**

1.1 Versions, Configurations and Modes of Operation 7
1.2 Hardware and Physical Cryptographic Boundary 8
1.3 Firmware and Logical Cryptographic Boundary 10

2 Cryptographic Functionality **11**

2.1 Critical Security Parameters and Public Keys 12

3 Roles, Authentication and Services **13**

3.1 Secure Channel Protocol 03 Authentication Method 14
3.2 PIN authentication method 14
3.3 Services 15

4 Self-test **18**

4.1 Power-On Self-tests 18
4.2 Conditional Self-Tests 18

5 Physical Security Policy **19**

6 Mitigation of Other Attacks Policy **19**

7 Security Rules and Guidance **19**

List of Tables

Table 1: References 4
Table 2: Acronyms and Definitions 6
Table 3: Security Level of Security Requirements 7
Table 4: Operating system identification 7
Table 5: APDU command 8
Table 6: Ports and Interfaces 9
Table 7: Approved Algorithms 12
Table 8: Non-Approved but Allowed Cryptographic Functions 12
Table 9: Critical Security Parameters 13
Table 10: Public Keys 13
Table 11: Roles Supported by the Module 14
Table 12: Unauthenticated Services 15
Table 13: Authenticated Services 16
Table 14: CSPs and Public Keys Access within Services 17
Table 15: Power-On Self-Test 18
Table 16: Conditional Self-Tests 18

List of Figures

Figure 1: NXP Semiconductors JCOP4 P71 Physical Form 9
Figure 2: Module Block Diagram 10

References

Table 1: References

Acronym	Full Specification Name
References used in Approved Algorithms Table	
[38A]	NIST, Special Publication 800-38A, *Recommendation for Block Cipher Modes of Operation: Methods and Techniques*, December, 2001
[38B]	NIST, Special Publication 800-38B, *Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication*, May, 2005
[38F]	NIST, Special Publication 800-38F, *Recommendation for Block Cipher Modes of Operation: Methods for Key Wrapping*, December, 2012
[56A]	NIST, Special Publication 800-56A, *Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography (Revised)*, June, 2010
[56Arev3]	NIST, Special Publication 800-56A, *Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography*, Revision 3, April, 2018
[67]	NIST Special Publication 800-67, *Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher*, Revision 2, July, 2017
[90A]	NIST, Special Publication 800-90A, *Recommendation for Random Number Generation Using Deterministic Random Bit Generators*, Revision 1, June, 2015
[108]	NIST, *Recommendation for Key Derivation Using Pseudorandom Functions (Revised)*, FIPS Publication 108, October, 2009
[133]	NIST Special Publication SP800-133, *Recommendation for Cryptographic Key Generation*, Revision 2, June 2020
[180-4]	NIST, *Secure Hash Standard*, FIPS Publication 180-4, August, 2015
[186-4]	NIST, *Digital Signature Standard (DSS)*, FIPS Publication 186-4, July, 2013
[197]	NIST, *Advanced Encryption Standard (AES)*, FIPS Publication 197, November 26, 2001

Other References	
[FIPS140-2]	NIST, *Security Requirements for Cryptographic Modules*, May 25, 2001
[GlobalPlatform]	*GlobalPlatform Card Specification 2.3, GlobalPlatform Inc., December 2015* *GlobalPlatform Consortium: GlobalPlatform Card -- Confidential Card Content Management -- Card Specification 2.2 -- Amendment A*, January 2011 *GlobalPlatform Consortium: GlobalPlatform Card Technology -- Contactless Services -- Card Specification v2.2 -- Amendment C*, July 2014 GlobalPlatform Consortium: GlobalPlatform Card Technology -- Secure Channel Protocol '03' – Card Specification v2.2 – Amendment D, May 2009
[IG]	NIST, *Implementation Guidance for FIPS PUB 140-2 and the Cryptographic Module Validation Program,* last updated October 23, 2019
[ISO 7816]	ISO/IEC 7816-1: 2011 *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*

Other References	
	ISO/IEC 7816-4:2013 *Identification cards -- Integrated circuit cards -- Part 4: Organization, security and commands for interchange* ISO/IEC 7816-6:2016 *Identification cards -- Integrated circuit cards -- Part 6: Interindustry data elements for interchange* ISO/IEC 7816-8:2016 *Identification cards -- Integrated circuit cards – Part 8: Commands and mechanisms for security operations* ISO/IEC 7816-12:2005 *Identification cards -- Integrated circuit cards -- Part 12: Cards with contacts -- USB electrical interface and operating procedures* ISO/IEC 7816-15:2016 *Identification cards – Integrated circuit cards – Part 15: Cryptographic Information application*
[ISO 14443]	ISO/IEC 14443-3:2016 *Identification cards -- Contactless integrated circuit cards -- Proximity cards -- Part 3: Initialization and anticollision* ISO/IEC 14443-4:2016 *Identification cards -- Contactless integrated circuit cards – Proximity cards – Part 4: Transmission protocol*
[JavaCard]	*Java Card 3.0.5 Runtime Environment (JCRE) Specification*, *May 2015* *Java Card 3.0.5 Virtual Machine (JCVM) Specification*, *May 2015* *Java Card 3.0.5 Application Programming Interface* Published by Oracle
[PKCS#1]	*PKCS #1 v2.1: RSA Cryptography Standard*, RSA Laboratories, June 14, 2002
[SP800-131A]	*Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths*, Revision 2, March 2019
[DTR]	NIST, *Derived Test Requirements for FIPS PUB 140-2, Security Requirements for Cryptographic Modules*, January 2011

Acronyms and Definitions

Table 2: Acronyms and Definitions

Acronym	Definition
APDU	Application Protocol Data Unit, see [ISO 7816]
API	Application Programming Interface
CM	Card Manager, see [GlobalPlatform]
CRNGT	Continuous Random Number Generator Test, see [DTR] AS09.42
CSP	Critical Security Parameter, see [FIPS 140-2]
DAP	Data Authentication Pattern, see [GlobalPlatform]
DPA	Differential Power Analysis
GP	GlobalPlatform
HID	Human Interface Device (Microsoftism)
IC	Integrated Circuit
ISD	Issuer Security Domain, see [GlobalPlatform]
KAT	Known Answer Test
NVM	Non-Volatile Memory (e.g., EEPROM, Flash)
OP	Open Platform (predecessor to GlobalPlatform)
PCT	Pairwise Consistency Test
PKI	Public Key Infrastructure
SCP	Secure Channel Protocol, see [GlobalPlatform]
SPA	Simple Power Analysis
TPDU	Transaction Protocol Data Unit, see [ISO 7816]

1 Overview

This document defines the Security Policy for the NXP Semiconductors JCOP4 P71 cryptographic module, hereafter denoted *the Module*. The Module, validated to FIPS 140-2 overall Level 3, is a single chip module (P71D321 so known as "P71") implementing the Global Platform operational environment, with a Card Manager and an application, the FIPS_Applet v1.0 (RC2).

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.

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

Table 3: Security Level of Security Requirements

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

1.1 Versions, Configurations and Modes of Operation

The JCOP4 P71 module is composed of a platform operational environment and a Java Card applet running on the P71 chip, see Section 1.3 for further detail on the logical architecture of the Module. The platform operational environment is identified by the ROM ID, Platform ID, and Patch ID. The Java Card applet is identified with its name and version.

The JCOP4 P71 platform component can be identified by using the IDENTIFY APDU command (Info service). This command returns the card identification data, which includes the ROM ID, Platform ID, and Patch ID.

Part number	Interface	Hardware Version	Platform ID	ROM ID	Patch ID
P71D321	Dual	N7121 B1	4A335233353130323336333130343030DCE5C19CFE6D0DCF	2E5AD88409C9BADB	1

Table 4: Operating system identification

The IDENTIFY APDU command is formatted as follow:

Code	Value	Parameter settings
CLA	'80'	GlobalPlatform
INS	'CA'	GET DATA (IDENTIFY) - ISD
P1	'00'	High order tag value
P2	'FE'	Low order tag value - proprietary data
Lc	'02'	Length of data field
Data	'DF28'	Module identification data
Le	'00'	Length of response data

Table 5: APDU command

The command answers the content of the DF28 file. The platform shall return the following information to confirm that the Module operates in an Approved mode of operation:

- Tag '03' identifies the platform ID version; the value will be 4A335233353130323336333130343030DCE5C19CFE6D0DCF.
- Tag 02 identifies the patch ID version; the value will be 0000000000000001.
- Tag 05 identifies the mode of operation; the value will be '01' - FIPS mode active
- Tag 08 identified the ROM ID: 2E5AD88409C9BADB.

The FIPS_Applet version 1.0 (RC2) always runs in an Approved mode of operation.

The personalized product shall have the following applet identification:

- Package ID: A00000000001H
- Applet ID: A0000000000101H
- Instance ID: A0000000000101H

The Module (composition of the platform and applet) as defined above will always be in an Approved mode of operation.

The Approved configuration of the product identified here has exactly one applet instance: the FIPS_Applet applet instance identified above. No other applet instance is allowed. The module's validation to FIPS 140-2 will no longer be valid once a non-validated applet is loaded.

1.2 Hardware and Physical Cryptographic Boundary

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

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

The contactless ports of the module require connection to an antenna. The Module relies on [ISO 7816] and [ISO 14443] card readers as input/output devices.

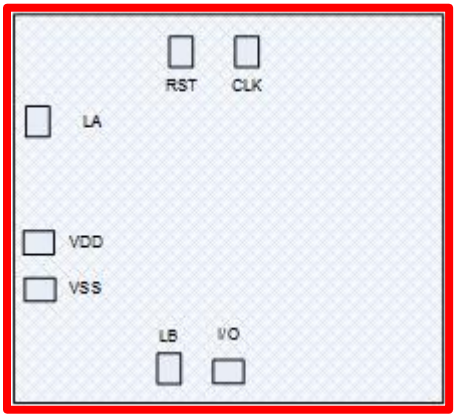

Figure 1: NXP Semiconductors JCOP4 P71 Physical Form

Port	Description	Logical Interface Type	Ct	Cl
VSS, VDD	ISO 7816: Supply voltage	Power	X	
RST	ISO 7816: Reset	Control in	X	
CLK	ISO 7816: Clock	Control in	X	
I/O	ISO 7816: Input/Output	Control in, Data in, Data out, Status out	X	
LA, LB	ISO 14443: Antenna	Power, Control in, Data in, Data out, Status out		X

Table 6: Ports and Interfaces

In the table above, an “X” in the Ct column indicates the port is active in the contact mode; an “X” in the Cl column indicates the port is active in the contactless mode.

1.3 Firmware and Logical Cryptographic Boundary

Figure 2 depicts the Module operational environment.

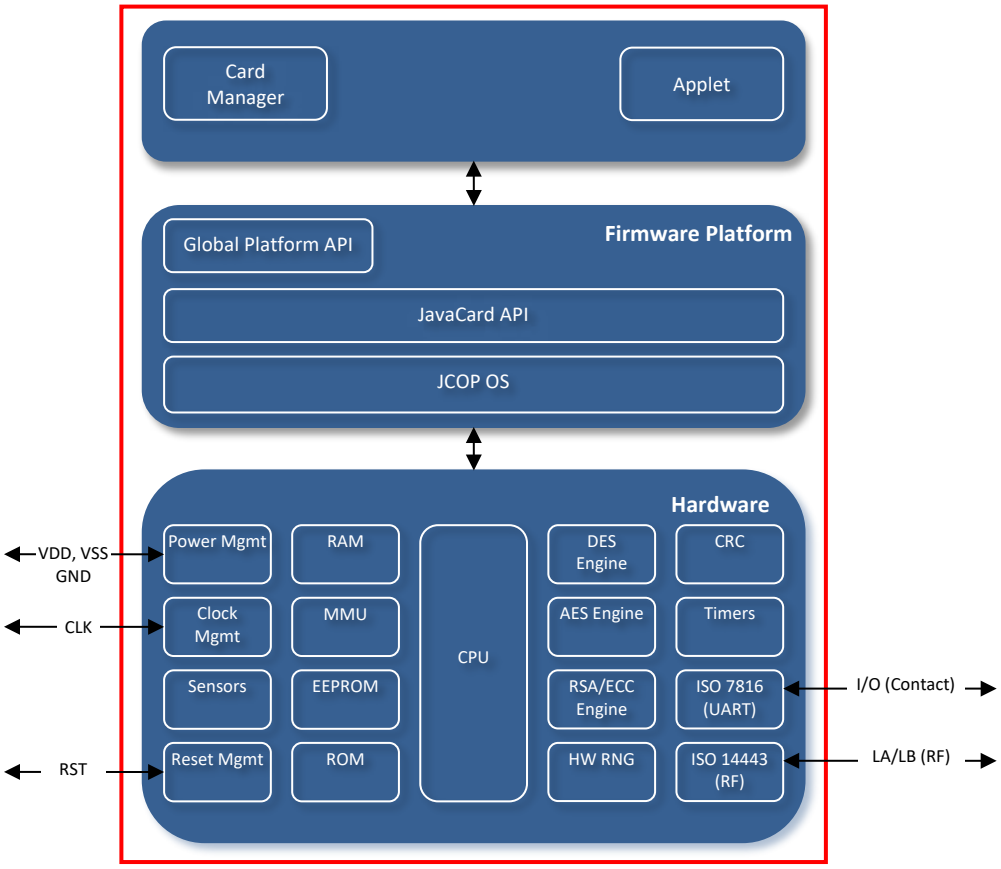

Figure 2: Module Block Diagram

The JavaCard and Global Platform APIs are internal interfaces available to applets. Only applet and Card Manager services are available at the card edge (the interfaces that cross the cryptographic boundary). The product is delivered personalized with a defined PIN and Secure Messaging Key. Those are set during wafer test operation before product's delivery to customer.

2 Cryptographic Functionality

The module implements the Approved and Allowed cryptographic functions listed below only[1].

CAVP Cert	Algorithm	Standard	Mode/ Method	Description	Use
C880	AES	[197], [38A]	CBC, ECB	AES-128, AES-192, AES-256	Data Encryption/ Decryption
Vendor Affirmed	AES-CBC-CS	[197], [38A]	CBC-CS3	AES-128	Data protection
C880	AES CMAC	[197], [38B]	CMAC	AES-128, AES-192, AES-256	Message Authentication; generation and verification
Vendor Affirmed	CKG	[133]	§4: Using the Output of a Random Bit Generator		Asymmetric Key Generation seed is based on an unmodified output of the DRBG cert. #C886
C887	CVL	[56Arev3]	ECC CDH Primitive	P-224, P-256, P-384, P-521	Shared Secret Computation
C886	DRBG	[90A]	CTR_DRBG	AES-128, AES-256	Deterministic Random Bit Generation AES-128: RSA key generation AES-256: ECDSA key generation Derivation function is used
C887	ECDSA	[186-4]	P-224, P-256, P-384, P-521		ECC Key Generation
			P-224: (SHA-224, SHA-256, SHA-384, SHA-512), P-256: (SHA-256, SHA-384, SHA-512), P-384: (SHA-384, SHA-512), P-521: (SHA-512)		Digital Signature Generation
			P-224: (SHA-224, SHA-256, SHA-384, SHA-512), P-256: (SHA-256, SHA-384, SHA-512), P-384: (SHA-384, SHA-512), P-521: (SHA-512)		Digital Signature Verification
C1289	KBKDF	[108]	Counter	AES-128, AES-192, AES-256	Deriving keys from existing keys
C880	KTS	[38F]	AES CBC / AES CMAC	AES-128, AES-192, AES-256	Meets the SP 800-38F §3.1 ¶3 requirements for symmetric key wrapping, using Cert. #C880 AES and AES CMAC. Key establishment methodology provides between 128 and 256 bits of encryption strength.
C888	RSA	[186-4]	n=2048, 3072		Key Generation

[1] The cryptographic implementation might have been tested with additional modes of operation or key size but only the cryptographic algorithms listed in the table are used by the module.

CAVP Cert	Algorithm	Standard	Mode/ Method	Description	Use
C838	RSA	[186-4]	n=2048, 3072 with PKCS v1.5 and PKCSPSS and SHA-(224, 256, 384, 512)		Digital Signature Generation Note, 4096-bit RSA Key Generation and Verification implementation was tested but it is not reachable.
			n=2048, 3072 with PKCS v1.5 and PKCSPSS and SHA-(1[2], 224, 256, 384, 512)		Digital Signature Verification
C837	SHS	[180-4]	SHA-1, SHA-224, SHA-256, SHA-384, SHA-512		Message Digest Generation
C880	Triple-DES[3]	[67]	CBC, ECB	3-Key	Data Encryption and Decryption

Table 7: Approved Algorithms

Algorithm	Description
NDRNG	Hardware RNG; used as entropy input to the FIPS approved (Cert. #C886) DRBG. The non-deterministic RNG provides a minimum entropy of 128 bits for AES-128 CTR_DRBG and 256 bits for AES-256 CTR_DRBG.

Table 8: Non-Approved but Allowed Cryptographic Functions

2.1 Critical Security Parameters and Public Keys

All CSPs used by the Module are described in this section. All usage of these CSPs is described in the services detailed in Section 3.3. In the tables below, the following prefixes are used:

- OS prefix denotes operating system.
- SD prefix denotes a GlobalPlatform Security Domain.
- DAP prefix denotes the GlobalPlatform Data Authentication Protocol.
- APP prefix denotes an Applet CSP or a Public Key.

CSP	Description/Usage
	Card Manager
OS-DRBG-EI	NDRNG entropy input to CTR_DRBG.
OS-DRBG-STATE	Current AES-128 and AES-256 CTR_DRBG states (V and Key).
OS-SKEK	128-bit key stored in NVM, used to derive OS-MKEK.
OS-MKEK	AES-128/192/256 key used to encrypt all secret and private key data stored in NVM.
SD-KENC	AES (128-bit, 192-bit, 256-bit) Master key used to derive SD-SENC.
SD-KMAC	AES (128-bit, 192-bit, 256-bit) Master key used to derive SD-SMAC.

[2] This algorithm is Approved for legacy use.

[3] The same Triple-DES key is not used more than either 2^{16} per IG A.13. When the block limit is reached the key value is cleared and the key is set to un-initialized automatically by the JCOP4 OS.

CSP	Description/Usage
	Card Manager
SD-KDEK	AES (128-bit, 192-bit, 256-bit) Sensitive data decryption key used to decrypt CSPs.
SD-SENC	AES (128-bit, 192-bit, 256-bit) Session encryption key used to encrypt / decrypt secure channel data.
SD-SMAC	AES (128-bit, 192-bit, 256-bit) Session MAC key used to verify inbound secure channel data integrity.
SD-RMAC	AES (128-bit, 192-bit, 256-bit) Session MAC key used to generate response secure channel data MAC.
	Applet
APP-SC-KENC	AES (256-bit) encryption key used to encrypt / decrypt secure channel data.
APP-SC-KMAC	AES (256-bit) MAC key used to verify inbound secure channel data integrity.
APP-DES	3-Key Triple-DES key used by Symmetric cipher.
APP-AES	AES (128, 192 or 256) key used by Symmetric cipher.
APP-RSA	RSA (n=2048, n=3072) private key used by Digital signature service.
APP-ECDSA	ECDSA (P-224, P-256, P-384, P-521) private key used by Digital signature service.
APP-ECSSG	ECC CDH (P-224, P-256, P-384, P-521) private key used for testing the shared secret generation.
APP-PIN	Application PIN for user authentication.
APP-SS	Application Shared Secret.

Table 9: Critical Security Parameters

Public Key	Description/Usage
	Card Manager
DAP-PUB	RSA (2048-bit) or ECC (P-256) new firmware signature verification key.
	Applet
APP-RSAPUB	RSA public key of size 2048 or 3072 for testing RSA signature generation.
APP-ECDSAPUB	ECDSA (P-224, P-256, P-384, P-521) public key for testing ECDSA signature verification.
APP-ECDHPUB	ECC CDH (P-224, P-256, P-384, P-521) public key, used to generate a shared secret.

Table 10: Public Keys

3 Roles, Authentication and Services

The Module:

- Does not support a maintenance role.
- Clears previous authentications on power cycle.
- Supports Global Platform SCP logical channels, allowing concurrent operators in a limited fashion.

Table 11 lists all operator roles supported by the Module.

Role ID	Role Description
CO	Cryptographic Officer – manages Module content and configuration, including issuance and management of Module data via the ISD. Authenticated as described in *Secure Channel Protocol 03 Authentication* in sub-section below.
User	The Card Holder (applet user) – performs FIPS approved cryptographic operations. Authenticated as described in *PIN authentication method* in sub-section below.

Table 11: Roles Supported by the Module

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

- Only one operator at a time is permitted on a channel.
- Applet and Card Manager de-selection, card reset, or power down terminates the current authentication. Re-authentication is required after any of these events for access to authenticated services.
- CO authentication method does not exchange plaintext CSP.
- User authentication data is encrypted during entry (by APP-SC-KENC), is stored encrypted with OS-MKEK, and is only accessible by authenticated services.

3.1 Secure Channel Protocol 03 Authentication Method

The Secure Channel Protocol authentication method is provided by the SECURE CHANNEL service. The SD-KENC and SD-KMAC keys are used to derive the SD-SENC and SD-SMAC keys, respectively. The off-card entity participating in the mutual authentication sends a 64-bit challenge to the Smart Card. The Smart Card generates its own challenge and computes a 64-bit cryptogram with SD-SMAC key and both challenges. The Smart Card cryptogram and challenge are sent to the off-card entity which checks the Smart Card cryptogram and creates its own 64-bit cryptogram with both challenges. A 64-bit message authentication code (MAC) is also computed on the command containing the off-card entity cryptogram with AES-CMAC and SD-SMAC key, the MAC is concatenated to the command, and the command is sent to the Smart Card. The Smart Card checks the message authentication code and compares the received cryptogram to the calculated cryptogram. If all of this succeeds, the two participants are mutually authenticated (the external entity is authenticated to the Module in the CO role).

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

- 1/(2^128) = 2.9E-39 (MAC||cryptogram, using a 128-bit block for authentication)

This authentication method 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 enforces a maximum of 60 failed SCP03 authentication attempts before blocking permanently the card. The probability that a random attempt will succeed over a one-minute interval is:

- 60/2^128 = 1.7E-37 (MAC||cryptogram, using a 128-bit block for authentication)

3.2 PIN authentication method

The PIN verification method is used to authenticate a user at the applet level. The user must enter his PIN and call the Verify PIN service. This service is performed over a secure messaging (approved KTS) established between the external entity and the Module, see Section 3.3.

The PIN value is set during pre-personalization of the product, before product delivery.
The probability that a random attempt will succeed using this authentication method is:

- 1/2^48 = 3.5E-15 (for any of 48-bit PIN)

The Module enforces a maximum of three (3) failed PIN based authentication attempts. The probability that a random attempt will succeed over a one-minute interval is:

- 3/2^48 = 1.1E-14 (for any of 48-bit PIN)

If the user fails to authenticate, access to the command handler is rejected and an exception is thrown.

3.3 Services

All services implemented by the Module are listed in the tables below. The *ISD Services* are provided by the Card Manager and are available to off card entities. Such services are related to card content management (e.g., applet loading, installation, deletion, card data access or storage) accessed via communication protocols like ISO7816. The *API Services* are available to on card entities, i.e., Java Card applets. These services are typically cryptographic services available via the Java Card API.

Service	Description
Card Reset	Power cycle or reset the Module. Includes Power-On Self-Test.
Context	Select an applet or manage logical channels.
Info	Read unprivileged data objects, e.g., module configuration or status information (Show Status).

Table 12: Unauthenticated Services

Service	Description	CO	User
	ISD (OS/Card Manager) Services		
Lifecycle	Modify the card or applet life cycle status.	X	
Manage Content	Load and install application packages and associated keys and data.	X	
Privileged Info	Read module data (privileged data objects, but no CSPs).	X	
Secure Channel	Establish and use a secure communications channel.	X	
	Applet Services		
Asymmetric key generation	Trigger OS API for generation of RSA and ECDSA keys.		X
Digital signature	Trigger OS API for ECDSA and RSA signature generation and verification.		X
Secure hash	Trigger OS API for [FIPS 180-4] compliant hash algorithms.		X
Shared secret generation	Trigger OS API for [SP 800-56A] §5.7.1.2 conformant ECC CDH.		X
Symmetric cipher	Trigger OS API for AES and Triple-DES encryption and decryption.		X
Verify PIN	Verify the user's PIN (authenticate the user) through the OS OwnerPIN object and associated methods.		X

Service	Description	CO	User
	ISD (OS/Card Manager) Services		
Open secure messaging	Initialize the OS secure messaging functions and establish a secure messaging channel for communicating with the applet.		X
Import key	Initialize the OS key object with a key value that will be required for Triple-DES, AES, RSA, and/or ECC cryptographic operations.		X
Import domain parameters	Import parameters (initialize the OS Key Object) that will be required and used by further cryptographic commands related to Elliptic Curve.[4]		X

Table 13: Authenticated Services

Table 14 below describes the access to CSPs by service with brief descriptions, which are intended to help readers understand the patterns of access. Explanations are provided in groups of services and/or keys (as best suited to explain the pattern of access), describing those aspects that have commonality across services or keys/CSPs.

Lifecycle: must be used with Secure Channel active (hence SD Session keys are 'E'); zeroizes all keys except session keys when Lifecycle is used for card termination.

OS-MKEK: generated on first power-up of the Module in a manufacturing setting; used whenever any private or secret key is accessed; zeroized on Lifecycle card termination.

OS-DRBG CSPs: OS-DRBG-EI is the NDRNG entropy input to the DRBG instantiation at power-on (Module Reset), zeroized after use. OS-DRBG-STATE is generated at startup (Module Reset), zeroized at shutdown as part of Module Reset, or by LifeCycle card termination. Each 'E' in the OS-DRBG-STATE column indicates the use of the DRBG to generate keys (or nonces), as the value is used and the state is updated.

Secure Channel Master Keys (SD-KENC, SD-KMAC): 'E' when a secure channel is initialized (GP Secure Channel). May be updated ('I') using the Manage Content service; zeroized by Lifecycle card termination.

SD-KDEK: is used to decrypt CSPs entered into the module during the applet personalization.

Secure Channel Session Keys (SD-SENC, SD-SMAC, SD-RMAC): 'E' for any service that can be used with secure channel active. 'GE' on GP Secure Channel as a consequence of secure channel initialization and usage; however, while the SD-RMAC key is generated by default. 'Z' on Module Reset is a consequence of RAM clearing/garbage collection.

DAP-PUB: is imported into the module at the factory, but may be updated using the Manage Content service. It is used by the Manage Content for signature verification of patch or applet code.

All applet services, with the exception of the import of public domain parameters service, are used with an active secure messaging (logical Trusted Path). The data is sent encrypted with AES-256 CBC and AES-CMAC (Cert. #C880), the secure messaging provides 256 bits of encryption strength. To initiate the secure messaging, the User will call the *Open secure messaging* service. Then, all applet services will have to be protected as specified in [GlobalPlatform] Amendment D.

The Asymmetric key generation service is used for ECC or RSA key generation; public keys are output in the service response. The Digital signature service provides ECDSA or RSA signature generation and verification; ECDSA signature generation utilizes a random value. The Shared secret generation provides the SP 800-56A §5.7.1.2 ECC CDH function, using the card private key and the external participant's public key to generate the shared secret; the shared secret is not used by the Module and it is output from the Module encrypted and protected in integrity with application secure messaging; this service is available

[4] See guidance 15

for demonstration purpose only. The Symmetric cipher service provides AES and Triple-DES encryption and decryption. The applet keys can be imported with the dedicated service.

Services	CSPs																			Public Keys			
	OS-DRBG-EI	OS-DRBG-STATE	OS-SKEK	OS-MKEK	SD-KENC	SD-KMAC	SD-KDEK	SD-SENC	SD-SMAC	SD-RMAC	APP-SC-KENC	APP-SC-KMAC	APP-DES	APP-AES	APP-RSA	APP-ECDSA	APP-ECSSG	APP-PIN	APP-SS	DAP-PUB	APP-RSAPUB	APP-ECDSAPUB	APP-ECDHPUB
Unauthenticated Role	*Card Manager*										*Applet*									*CM*	*Applet*		
Card Reset	GEZ	GEZ	E	G	--	--	--	Z	Z	Z	--	--	--	--	--	--	Z	--	Z	--	--	--	Z
Context	--	--	--	--	--	--	--	EZ	EZ	EZ	--	--	--	--	--	--	--	--	--	--	--	--	--
Info	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--
ISD Role	*Card Manager*										*Applet*									*CM*	*Applet*		
Lifecycle	Z	Z	Z	Z	Z	Z	Z	E	E	E	--	--	--	--	--	--	--	Z	--	--	--	--	--
Manage Content	Z	Z	IZ	EZ	IEZ	IEZ	IEZ	E	E	E	IZ	IZ	Z	Z	Z	Z	--	IZ	--	EZ	Z	Z	--
Privileged Info	--	--	--	E	E	E	--	E	E	E	--	--	--	--	--	--	--	--	--	--	--	--	--
Secure Channel	--	--	--	E	E	E	--	GE	GE	GE	--	--	--	--	--	--	--	--	--	--	--	--	--
API Role	*Card Manager*										*Applet*									*CM*	*Applet*		
Asymmetric key generation	--	GE	--	E	--	--	--	--	--	--	E	E	--	--	G	G	--	--	--	--	GO	GO	--
Digital signature	--	GE	--	E	--	--	--	--	--	--	E	E	--	--	E	E	--	--	--	--	E	E	--
Secure hash	--	--	--	E	--	--	--	--	--	--	E	E	--	--	--	--	--	--	--	--	--	--	--
Shared secret generation	--	E	--	E	--	--	--	--	--	--	E	E	--	--	--	--	GE	--	GO	--	--	--	GEO
Symmetric cipher	--	--	--	E	--	--	--	--	--	--	E	E	E	E	--	--	--	--	--	--	--	--	--
Verify PIN	--	--	--	E	--	--	--	--	--	--	E	E	--	--	--	--	--	E	--	--	--	--	--
Open secure messaging	--	--	--	E	--	--	--	--	--	--	E	E	--	--	--	--	--	--	--	--	--	--	--
Import key	--	--	--	E	--	--	--	--	--	--	E	E	I	I	I	I	--	--	--	--	I	I	--
Import domain parameters	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--

Table 14: CSPs and Public Keys Access within Services

- G = Generate: The service generates or derives the CSP.
- I = Input: The service inputs the CSP.
- E = Execute: The Module executes using the CSP.
- O = Output: The service outputs the CSP.
- Z = Zeroize: The module zeroizes the CSP. For the Context service, SD session keys are destroyed on applet deselect (channel closure).
- -- = Not accessed by the service.

4 Self-test

4.1 Power-On Self-tests

On power-on or reset, the Module performs self-tests as described in Table 15 below. All self-tests must be completed successfully prior to any other use of cryptography by the Module. If the power-on self-tests or the CRNGT fail, the system will halt and will start again after a reset of the module. The other conditional self-tests will return an error status. The on-demand Power-On Self-tests can be executed by restarting the module.

Test Target	Description
AES	Performs separate encrypt and decrypt KATs using an AES-128 key in CBC mode.
DRBG	Performs a fixed input KAT and all SP 800-90A health test monitoring functions.
ECC CDH	Performs with the separate ECDSA signature generation and verification KATs using the P-521 curve.
ECDSA	Performs ECDSA signature generation and verification KATs using the P-521 curve and SHA-256; this self-test is inclusive of the ECC CDH self-test.
Firmware Integrity	32-bit CRC performed over all code located in NVM and ROM.
RSA	Performs separate RSA signature generation and verification KATs using a2048-bit key and SHA-256.
SHA-1	Performs a fixed input KAT
SHA-256	Performs a fixed input KAT (inclusive of SHA-224, per IG 9.4)
SHA-512	Performs a fixed input KAT (inclusive of SHA-384, per IG 9.4).
Triple-DES	Performs encrypt and decrypt KATs using 3-Key Triple-DES in CBC mode.
CMAC	Performs an AES-CMAC KAT with AES-128
KBKDF	Performs a KBKDF KAT with AES-128

Table 15: Power-On Self-Test

4.2 Conditional Self-Tests

Test Target	Description
DRBG CRNGT	On every call to the DRBG, the Module performs the AS09.42 continuous RNG test to assure that the output is different than the previous value.
FW Load	When new firmware is loaded into the Module using the LOAD (after authentication to the ISD) command (Manage Content service), the Module verifies the integrity of the new firmware (applet) using RSA and ECDSA Signature Verification with the DAP-PUB public key; the new firmware in this scenario is signed by an external entity using the private key corresponding to DAP-PUB.
Generate PCT	Pairwise consistency test performed when an asymmetric key pair is generated for RSA or ECC. The conditional test is implemented at the applet level.
NDRNG RCT	The NDRNG is tested by performing an RCT on raw data (amongst other continuously running tests). Per IG 9.8, this is an alternative to the NDRNG CRNGT.
Signature PCT	Pairwise consistency test performed when a signature is generated for RSA or ECDSA.

Table 16: Conditional Self-Tests

5 Physical Security Policy

The Module is a single-chip implementation that meets commercial-grade specifications for power, temperature, reliability, and shock/vibrations. The Module uses standard passivation techniques and is protected by 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 includes also Environmental Failure Protection features, see section 6 below.

The Module is intended to be mounted in additional packaging; physical inspection of the die is typically not practical after packaging.

6 Mitigation of Other Attacks Policy

The module is protected against SPA, DPA, Timing Analysis and Fault Induction using a combination of firmware and hardware counter-measures. Protection features include detection of out-of-range supply voltages, frequencies or temperatures, and detection of illegal address or instruction. All cryptographic computations and sensitive operations such as PIN comparison provided by the 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.

7 Security Rules and Guidance

The Module implementation also enforces the following security rules:

1. The Module provides two distinct operator roles: User and Cryptographic Officer.
2. The Module does not support a maintenance interface or role.
3. The Module provides identity-based authentication.
4. The Module clears previous authentications on power cycle.
5. Power up self-tests do not require any operator action.
6. The Module allows the operator to initiate self-tests on-demand on by power cycling power or resetting the Module.
7. Data output is inhibited during key generation, self-tests, zeroization, and error states.
8. Status information does not contain CSPs or sensitive data that if misused could lead to a compromise of the Module.
9. The Module does not enter or output plaintext CSPs.
10. There are no restrictions on which CSPs are zeroized by the zeroization service.
11. The Module does not support manual key entry.
12. The Module does not output intermediate key values.
13. The module does not provide bypass services or ports/interfaces.
14. No additional interface or service is implemented by the Module which would provide access to CSPs.

In addition, the following guidance shall be followed:

15. It is the operator’s responsibility to either use a NIST-Approved parameter as specified in FIPS 186-4 Appendix D or to generate the parameter according to FIPS 186-4 Section 6.1.1 and [IG] A.2