HiCOS PKI Applet and Taiwan TWNID Applet

on NXP JCOP 3 SecID P60 (OSA)

FIPS 140-2 Cryptographic Module

Non-Proprietary Security Policy

Version: 1.2
Date: 2/6/2017

Table of Contents

List of Tables

List of Figures

References

Acronym	Full Specification Name
[Annex_A]	NIST, *Approved Security Functions*, September 2015.
[Annex_C]	NIST, *Approved Random Number Generators*, February 2012.
[Annex_D]	NIST, Approved Key Establishment Techniques, October, 2014.
[DTR]	NIST, *Derived Test Requirements [DTR] for FIPS PUB 140-2, Security Requirements for Cryptographic Modules*, January 2011.
[FIPS 180]	NIST, *Secure Hash Standard (SHS)*, FIPS Publication 180-4, August 2015.
[FIPS 186]	NIST, *Digital Signature Standard (DSS)*, FIPS Publication 186-4, July 2013.
[FIPS140-2]	NIST, *Security Requirements for Cryptographic Modules*, May 25, 2001
[FIPS197]	NIST, *Advanced Encryption Standard (AES)*, FIPS Publication 197, November 26, 2001.
[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
[IG]	NIST, *Implementation Guidance for FIPS PUB 140-2 and the Cryptographic module Validation Program*, December 28 2015.
[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 14443-1:2016 Part 1: Physical characteristics[1]* *ISO/IEC 14443-2:2016 Part 2: Radio frequency power and signal interface[2]* *ISO/IEC 14443-3:2016 Part 3: Initialization and anticollision[3]* *ISO/IEC 14443-4:2016 Part 4: Transmission protocol[4]*
[JavaCard]	*Java Card 2.2.2 Runtime Environment (JCRE) Specification* *Java Card 2.2.2 Virtual Machine (JCVM) Specification* *Java Card 2.2.2 Application Programming Interface* Published by Sun Microsystems, March 2006
[PKCS#1]	PKCS #1 (IETF RFC3447): *Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1*, February 2003.
[SP 800-67]	NIST Special Publication 800-67, *Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher*, version 1.2, July 2011
[SP800-108]	NIST, *Recommendation for Key Derivation Using Pseudorandom Functions*, October 2009.
[SP800-131A]	*Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths*, November 2015.
[SP800-38A]	NIST, *Recommendation for Block Cipher Modes of Operation - Methods and Techniques*, December 2001.
[SP800-38B]	NIST, *Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication*, May 2005.
[SP800-38F]	NIST, *Recommendation for Block Cipher Modes of Operation: Methods for Key Wrapping*, December 2012.
[SP800-56A]	NIST, *Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography*, Revision 2, May 2013.
[SP800-67]	NIST, *Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher*, January 2012.
[SP800-90A]	NIST, *Recommendation for Random Number Generation Using Deterministic Random Bit Generators*, June 2015.

Table 1: References

Acronyms and definitions

Acronym	Definition
APDU	Application Protocol Data Unit, the messaging structure - see [ISO 7816]
API	Application Programming Interface
CHT	Chungwa Telecom
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	Global Platform
HiCOS	Chungwa Telecom smartcard product trade name
HID	Human Interface Device (Microsoftism)
IC	Integrated Circuit
ISD	Issuer Security Domain, see [GlobalPlatform]. Associated with Card Manager functionality.
JCOP	JavaCard Open Platform
KAT	Known Answer Test
NDRNG	Non-deterministic random number generator
NXP	The hardware and OS supplier, NXP Semiconductors
NVM	Non-Volatile Memory (e.g., EEPROM, Flash)
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]
TWNID	Taiwan ID (identity applet)

Table 2: Acronyms and Definitions

1 Introduction

This document defines the Security Policy for the Chunghwa Telecom Co., Ltd. and NXP Semiconductors HiCOS PKI Applet and TWNID Applet on NXP JCOP 3 SecID P60 (OSA) cryptographic module, hereafter denoted *the module*. The module, a single chip embodiment validated to FIPS 140-2 Overall Security Level 2, is the combination of the HiCOS PKI Applet and the TWNID Applet running on the NXP JCOP 3 SecID P60 (OSA) (denoted platform below).

The platform provides an operational environment for the PKI Applet and TWNID Applet: 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. Unusable functionality is not discussed further in this document.

The TWNID Applet is a Javacard applet that stores the personal information related to the card holder. It allows governmental organizations to retrieve these pieces of data. The PKI Applet is a Javacard applet that provides security for stored user data and credentials and an easy to use interface to PKI services (e.g., for strong authentication, encryption and digital signatures).

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

Security Requirement	Security Level
Cryptographic module Specification	2
Cryptographic module Ports and Interfaces	2
Roles, Services, and Authentication	2
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 3: Security Level of Security Requirements

1.1 Versions, Configurations and Modes of operation

Hardware: P6022y VB (IC designation; commercial part number P60D145)
Firmware: JCOP 3 SECID P60 (OSA) version 0x0503.8211
Applets: HiCOS PKI Applet V1.0, TWNID Applet V1.1

The module is available in three hardware configurations:

- Contact Only
- Contactless Only
- Dual Interface

The module always runs in the Approved mode of operation. The explicit indicator of the Approved mode of operation is obtained in two steps.

1. Use the *Context* service to select the Card Manager and the *Info* service (GET DATA APDU, tag '9F7F' and tag '88') to verify the fields shown in Table 4 below.
2. Use the *Context* service to select the PKI Applet selected, use the *PKI Applet Info (Unauthenticated)* service (GET DATA APDU, tag '0105'), which is expected to return '03020101'.

Data Element	Length	Value	Associated Version
GET DATA tag 9F7F			
IC fabricator	2	0x4790	NXP P6022y VB
IC type	2	0x0503	Firmware Version Part 1
Operating system identifier	2	0x8211	Firmware Version Part 2
Operating system release date	2	0x6057	Firmware release date
Operating system release level	2	0x0002	Firmware release level; first byte is the patch level
GET DATA tag 88			
FIPS Mode Indicator	2	0xA5F0	The module is configured for FIPS compliance. Any other value does not indicate the FIPS Approved mode.

Table 4: Versions and Mode of Operations Indicators

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 and edges of the integrated circuit die and the associated bond pads. The cross-hatching indicates the presence of active tamper shields. In production use, the module is delivered wire bonded and encapsulated by epoxy, packaged into a smart card.

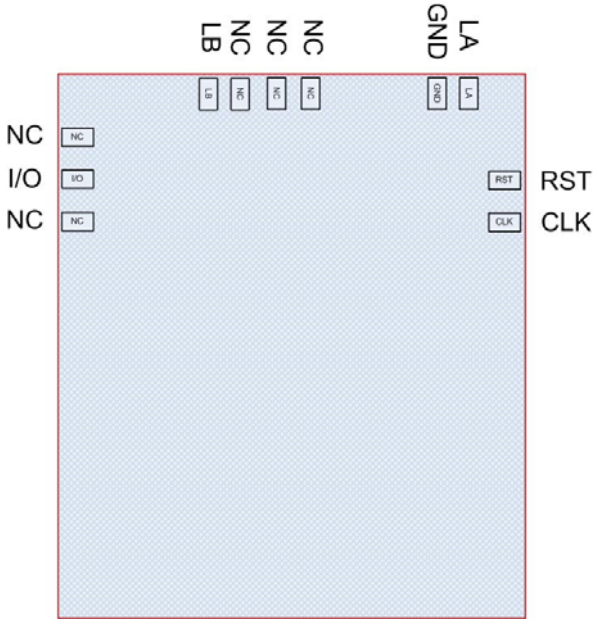

Figure 1: NXP Semiconductors P6022y VB

The contactless ports of the module require connection to an antenna. The module relies on [ISO7816] and [ISO14443] card readers as input/output devices.

Port	Description	Logical Interface Type
$V_{CC,}$ GND	ISO 7816: Supply voltage	Power (Contact Only or Dual Interface)
RST	ISO 7816: Reset	Control in (Contact Only or Dual Interface)
CLK	ISO 7816: Clock	Control in (Contact Only or Dual Interface)
I/O	ISO 7816: Input/Output	Control in, Data in, Data out, Status out (Contact Only or Dual Interface)
LA, LB	ISO 14443: Antenna	Power, Control in, Data in, Data out, Status out (Contactless Only or Dual Interface)
NC	Not connected	Not connected

Table 5: Ports and Interfaces

1.3 Firmware and Logical Cryptographic Boundary

Figure 2 depicts the module operational environment.

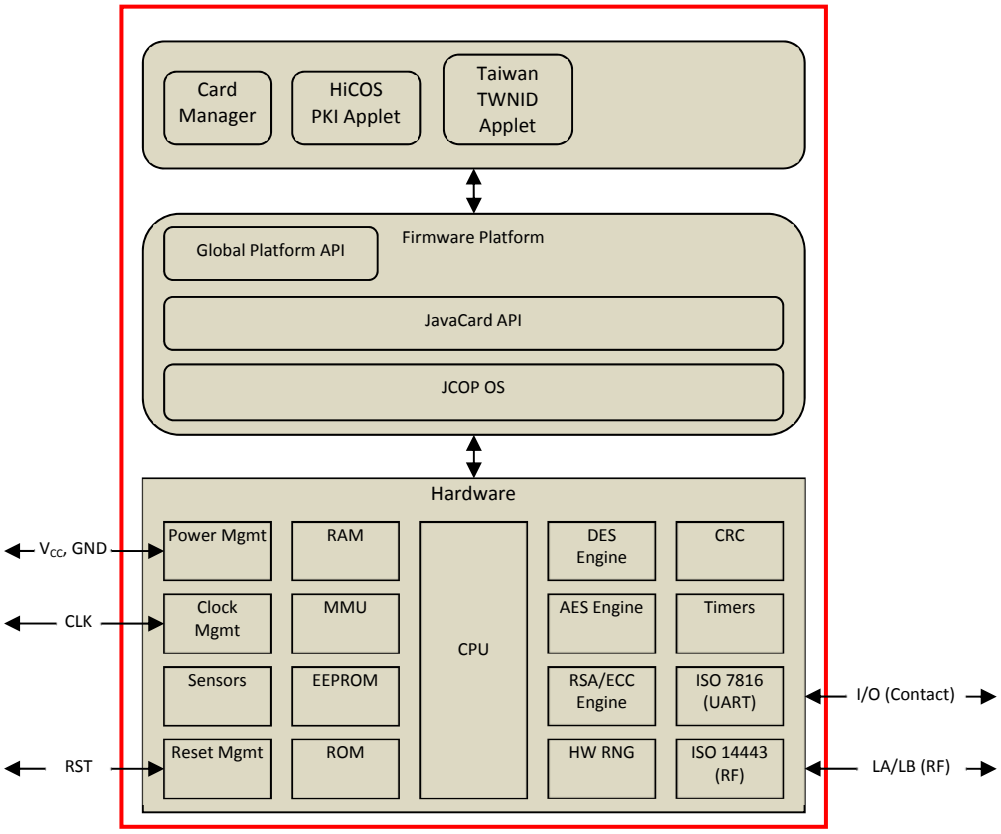

Figure 2: Module Block Diagram

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

2 Cryptographic Functionality

The module implements the Approved and Allowed cryptographic functions listed below. *Note: any item in curly braces { } is CAVP tested but not used by the module.*

CAVP Cert #	Standard	Mode/ Method	Strength[1]	Use
AES #3997	FIPS 197, SP 800-38A	CBC, ECB	128, 192, 256	Data Encryption/ Decryption
AES #3997	FIPS 197, SP 800-38B	CMAC	128,192,256	Message Authentication; SP 800-108 KDF
CVL #824	SP 800-56A	ECC CDH Primitive	P-224 , P-256, P-384, P-521	Shared Secret Computation
DRBG #1187	SP 800-90Ar1	HASH_based	256	Deterministic Random Bit Generation
ECDSA #890	FIPS 186-4		P-224 and P-256 P-384, P-521 {P-192 (Sig Ver)}	Digital Signature Generation, Verification and ECC Key Generation.
KBKDF #91	SP 800-108	AES CMAC	128,192,256	Deriving keys from existing keys, using Cert. #3397 AES CMAC
RSA #2053	FIPS 186-4 PKCS#1	SigGen and SigVer (n=2048) with SHA-256 {All other modes, methods and strengths listed on this cert are not used by this module}		Digital signature generation and verification.
RSA #2086	FIPS 186-4		n=2048 {n=3072}	Key generation
SHS #3299	FIPS 180-4	{SHA-1}, SHA-224, SHA-256, SHA-384, SHA-512		Message Digest
Triple-DES #2195	SP 800-67	TCBC, TECB	3-Key	Data Encryption/ Decryption
KTS	SP800-38F	AES/CMAC	(128, 192, 256)	Meets the SP 800-38F §3.1 ¶3 requirements for symmetric key wrapping, using Cert. #3397 AES/AES CMAC.

Table 6: Approved Algorithms

[1] Strength indicates DRBG Strength, Key Lengths, Curves or Moduli

Algorithm	Establishment Strength	Use
EC Diffie-Hellman (CVL Cert. #824 ECC CDH; ECDSA Cert. #890 Key Generation)	Provides 112, 128, 192 or 256 bits of encryption strength.	Key establishment
NDRNG	384 bits of entropy input at 7.976 min_entropy (382 effective bits of entropy are provided; 256 are required).	DRBG (Cert. #1187) seeding

Table 7: Allowed Algorithms

2.1 Critical Security Parameters

All CSPs used by the module are described in this section.

CSP	Type	Length (bits) Or Curve	Description / Usage
OS-DRBG-EI		384	Entropy input to Hash_DRBG (from NDRNG output).
OS-DRBG-STATE		880	880-bit value; the current DRBG state.
OS-MKEK	AES	128	Encrypt / decrypt all secret, private key data in NVM.
OS-PEK	AES	128	Encrypt / decrypt all PIN data in NVM.
SD-KENC	AES	128, 192, 256	Master key for SD-SENC generation.
SD-KMAC	AES	128, 192, 256	Master key for SD-SMAC generation.
SD-KDEK	AES	128, 192, 256	Sensitive data decryption.
SD-SENC	AES	128, 192, 256	Session encryption key to encrypt / decrypt secure channel data.
SD-SMAC	AES	128, 192, 256	Session MAC key to verify inbound secure channel data integrity.
SD-RMAC	AES	128, 192, 256	Session MAC key to generate response secure channel data MAC.

Table 8: JCOP Critical Security Parameters

CSP	Type	Length (bits) Or Curve	Description / Usage
PKI-KXAUTH	AES, Triple-DES	128, 192, 256 3-Key	PKI applet External Authentication key.
PKI-KIAUTH	AES, Triple-DES	128, 192, 256 3-Key	PKI applet Internal Authentication key.
PKI-KRSA-PRI	RSA	2048	PKI applet signature generation private keys.
PKI-KECC-PRI	ECC	P-224, P-256, P-384, P-521	PKI applet ECDSA signature generation private keys.
PKI-AUTH	Secret	10-byte	Two instances: Card holder PIN verification; PIN unblocking.

Table 9: PKI Applet Critical Security Parameters

CSP	Type	Length (bits) Or Curve	Description / Usage
TWNID-SENC	AES	128, 192, 256	Secure channel session data encryption / decryption.
TWNID-SMAC	AES	128, 192, 256	Secure channel session data integrity.
TWNID-EKAK-PRI	ECC	Brainpool P256r1 (256-bit curve, 128-bit equivalent strength)	Secure channel key agreement ephemeral private key.

Table 10: TWNID Applet Critical Security Parameters

2.2 Public Keys

Key	Type	Length (bits) Or Curve	Description / Usage
DAP-PUB	RSA ECC	2048 P-256	Firmware load test signature verification key.
PKI-KRSA-PUB	RSA	2048	Public keys held in the module for retrieval by external users through the PKI applet.
PKI-KECC-PUB	ECC	P-224, P-256, P-384, P-521	Public keys held in the module for retrieval by external users through the PKI applet.
TWNID-EKAK-PUB	ECC	Brainpool P256r1	Secure channel key agreement ephemeral public key.
TWNID-EKAK-PEER	ECC	Brainpool P256r1	Secure channel key agreement ephemeral public key, provided by peer.

Table 11: 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.
- Implements security conditions which must be satisfied to access specific features, not necessarily as a separate role.

Authentication of each operator and their access to roles and services is as described below. Only one operator at a time is permitted on a channel. Applet de-selection (including Card Manager), card reset or power down terminates the current authentication; re-authentication is required after any of these events for access to authenticated services. Authentication data is encrypted during entry (by SD-KDEK), and is only accessible by authenticated services. The module supports access by the TWNID Basic Inspection System (BIS), which requires use of the [PACE] secure channel to protect against contactless skimming.

Table 12 lists all operator roles supported by the module.

Role ID	Role Description
CO	Cryptographic Officer - role that manages module configuration, including issuance and management of module data via the ISD. Authenticated as described in GP Secure Channel Protocol Authentication Method below.
AA	Application Administrator - a role that manages TWNID and PKI application-related content and configuration. Authenticated using the GP Secure Channel Protocol Authentication method or PKI Applet Symmetric Key Authentication method.
User	Card Holder – The human user of the module, authenticated by PKI Applet Secret Value authentication with PKI applet or TWNID applet selected.

Table 12: Roles Supported by the module

3.1 GP Secure Channel Protocol Authentication Method

The GP Secure Channel Protocol provides confidentiality, integrity and mutual authentication. The module supports this mechanism in three services: the *GP Secure Channel* service, the *PKI Applet Secure Channel* service or the *TWNID Applet GP Secure Channel* service. These services each invoke the same underlying library calls, but from the Card Manager, PKI Applet and TWNID Applets, respectively.

The SD-KENC and SD-KMAC keys are used 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 probability that a random attempt will succeed using this authentication method is:

- 1/(2^128) = 2.9E-39 (for any of AES-128/192/256 SD-KENC/SD-SENC, assuming a 128-bit block)

The module enforces a maximum of 80 failed SCP authentication attempts. The probability that a random attempt will succeed over a one minute interval is:

- 80/(2^128) = 2.4E-37 (for any of AES-128/192/256 SD-KENC/SD-SENC, assuming a 128-bit block)

3.2 PKI Applet Symmetric Key Authentication Method

The external entity obtains a 16-byte challenge from PKI applet, encrypts the challenge and sends the cryptogram to PKI applet, along with a key ID. PKI applet decrypts the cryptogram, and the external entity is authenticated if the decrypted value matches the challenge.

The strength of authentication using this method is dependent on the challenge size and key size used: the minimum in both cases is 128 bits.

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

- 1/(2^128)= 2.9E-39

Based on the module's maximum communication rate and the sizes of command and response APDU, the maximum number of authentication attempts is 1.2E5 attempts per minute. The probability that a random attempt will succeed over a one minute interval is:

- 1.2E5/(2^128) = 2.8E-32

3.3 PKI Applet Secret Value Authentication Method

The external entity submits an identifier and corresponding secret value. The module enforces a minimum length of 6 characters, with the character space of all printable characters (95 possible characters).

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

- 1/(95^6) = 1.4E-12

Based on the module's maximum communication rate and the sizes of command and response APDU, the maximum number of authentication attempts is 3.6E5 attempts per minute. The probability that a random attempt will succeed over a one minute interval is:

- 3.6E5/(95^6) = 4.9E-7

3.4 Services

All services implemented by the module are listed in the tables below.

Service	Description
Card Manager	
Context	Select an application or manage logical channels.
Module Info (Unauthenticated)	Read unprivileged data objects, e.g., module configuration or status information.
Module Reset	Power cycle or reset the module. Includes Power-On Self-Test.
PKI Applet	
PKI Applet Info (Unauthenticated)	Read unprivileged PKI applet data objects.
TWNID Applet	
Establish PACE Channel	Establish secure channel between terminal and TWNID applet using EC Diffie-Hellman (not tested for compliance to SP 800-56A).
TWNID Applet (requires active PACE channel)	
TWNID Applet Info (Unauthenticated)	Read low sensitivity TWNID applet date objects.

Table 13: Unauthenticated Services

Service	Description	CO	AA	User
Platform				
GP Secure Channel	Establish and use a Global Platform secure communications channel.	X		
Lifecycle	Modify the card or applet life cycle status.	X		
Manage Content	Load and install application packages and associated keys and data.	X		
Module Info (Authenticated)	Read module configuration or status information (privileged data objects).	X		
PKI Applet				
PKI Applet Secure Channel	Establish and use a PKI Applet secure communications channel.		X	X
PKI Applet preparation	Manage PKI applet authentication data and PKI Applet lifecycle.		X	
Entity authentication with symmetric key	Authenticate AA role to the module.		X	
Entity authentication with password	Authenticate User role to the module (PIN verification).			X
Change PIN	Allows the User to change their PIN.			X
Unblock PIN	Mechanism to reset the retry counter when the card is blocked after too many failed PIN verify attempts.		X	
File Content Manage	Read or update binary data stored in the applets ISO 7816 file system.		X	X
Generate asymmetric key pair	Generate an RSA or EC key pair.		X	X
Digital Signature	Sign provided data with the specified key.		X	X
Get public key	Retrieve the specified public key.		X	X
Key Management	Update PKI applet keys.		X	
Register Client Applet	Registration required to enable use of PKI credentials by the TWNID applet.		X	
TWNID Applet				
TWNID Applet GP Secure Channel	Establish and use TWNID Applet GP secure communications channel.		X	
TWNID Applet preparation	Manage TWNID applet authentication data and keys.		X	
TWNID User Authentication with password	Authenticate User or BIS role to the module (PIN verification).			X
Read Taiwan TWNID Data Groups	Read the TWNID data groups.			X
Update Data Groups	Update TWNID applet data.		X	

Table 14: Authenticated Services

Service	Platform CSPs	CSPs and Public Keys																								
		OS-DRBG-EI	OS-DRBG-STATE	OS-MKEK	OS-PEK	SD-KENC	SD-KMAC	SD-KDEK	SD-SENC	SD-SMAC	SD-RMAC	PKI Applet CSPs	PKI-KXAUTH	PKI-KIAUTH	PKI-KRSA-PRI	PKI-KECC-PRI	PKI-AUTH	TWNID Applet CSPs	TWNID-SENC	TWNID-SMAC	TWNID-EKAK-PRI	Public Keys	DAP-PUB	PKI-KRSA-PUB	PKI-KECC-PUB	TWNID-EKAK-PUB	TWNID-EKAK-PEER
Unauthenticated Services																										
Context		–	–	–	–	–	–	–	E	E	E		–	–	–	–	–		–	–	–		–	–	–	–	–
Module Info (Unauthenticated)		–	–	–	–	–	–	–	E	E	E		–	–	–	–	–		–	–	–		–	–	–	–	–
Module Reset		GE Z	GE WZ	–	–	–	–	--	Z	Z	Z		–	–	–	–	–		–	–	–		–	–	–	–	–
PKI Applet Info (Unauthenticated)		–	–	–	–	–	–	–	–	–	–		–	–	–	–	–		–	–	–		–	–	–	–	–
Establish PACE Channel		–	–	–	–	–	–	–	–	–	–		–	–	–	–	–		GE	GE	GEZ		–	–	–	GRZ	WEZ
TWNID Applet Info (Unauthenticated)		–	–	–	–	–	–	–	–	–	–		–	–	–	–	–		–	–	–		–	–	–	–	–
Platform Services																										
GP Secure Channel		–	EW	E	–	E	E	E	GE	GE	GE		–	–	–	–	–		–	–	–		–	–	–	–	–
Lifecycle		Z	Z	GZ	Z	Z	Z	Z	E	E	E		Z	Z	Z	Z	Z		Z	Z	Z		–	–	–	–	–
Manage Content		–	–	–	–	W	W	EW	E	E	E		–	–	–	–	–		–	–	–		WE	–	–	–	–
Module Info (Authenticated)		–	–	–	–	–	–	–	E	E	E		–	–	–	–	–		–	–	–		–	–	–	–	–
PKI Applet Services																										
PKI Applet Secure Channel		–	EW	E	–	E	E	–	GE	GE	G		–	–	–	–	–		–	–	–		–	–	–	–	–
PKI Applet preparation		–	–	E	E	–	–	–	E	E	–		W	W	–	–	W		–	–	–		–	–	–	–	–
Entity authentication with symmetric key		–	–	E	–	–	–	–	E	E	–		E	E	–	–	–		–	–	–		–	–	–	–	–
Entity authentication with password		–	–	–	E	–	–	–	E	E	–		–	–	–	–	E		–	–	–		–	–	–	–	–
Change PIN		–	–	–	E	–	–	–	E	E	–		–	–	–	–	W		–	–	–		–	–	–	–	–
Unblock PIN		–	–	–	E	–	–	–	E	E	–		–	–	–	–	W		–	–	–		–	–	–	–	–
File Content Manage		–	–	–	–	–	–	–	E	E	–		–	–	–	–	–		–	–	–		–	–	–	–	–
Generate asymmetric key pair		–	EW	E	–	–	–	–	E	E	–		–	–	G	G	–		–	–	–		–	–	–	–	–
Digital Signature		–	EW	E	–	–	–	–	E	E	–		–	–	E	E	–		–	–	–		–	–	–	–	–
Get public key		–	–	E	–	–	–	–	–	–	–		–	–	–	–	–		–	–	–		–	R	R	–	–
Key Management		–	–	E	–	–	–	–	E	E	–		W	W	W	W	–		–	–	–		–	W	W	–	–
Register Client Applet		–	–	–	–	–	–	–	E	E	–		–	–	–	–	–		–	–	–		–	–	–	–	–
TWNID Applet Services																										
TWNID Applet GP Secure Channel		–	EW	E	–	E	E	–	GE	GE	G		–	–	–	–	–		–	–	–		–	–	–	–	–
TWNID Applet preparation		–	–	–	–	–	–	–	E	E	–		–	–	–	–	–		–	–	–		–	–	–	–	–
TWNID User Authentication with password		–	–	–	E	–	–	–	–	–	–		–	–	–	–	E		E	E	–		–	–	–	–	–
Read TWNID Data Groups		–	–	–	–	–	–	–	–	–	–		–	–	–	–	–		E	E	–		–	–	–	–	–
Update Data Groups		–	–	–	–	–	–	–	E	E	–		–	–	–	–	–		–	–	–		–	–	–	–	–

Table 15: Access to CSPs by Service

The table is organized to correspond to the set of unauthenticated services, then authenticated services.

- 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 CSP is imported into the module.
- 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.

Below are brief descriptions to help readers understand Table 15. Explanations are provided in groups of services and/or keys (as best suited to explain the pattern of access), describing first 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: used whenever any private or secret key is accessed, zeroized on *Lifecycle* card termination.

OS-PEK: used whenever any PIN is accessed, zeroized on *Lifecycle* card termination.

OS-DRBG CSPs: OS-DRBG-EI is the NDRNG entropy input to the DRBG instantiation *block_cipher_df* 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 'EW' in the OS-DRBG-STATE column indicates the use of the DRBG to generate keys, 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*, *PKI Applet Secure Channel*, *TWNID Applet GP Secure Channel*). May be updated ('W') using the *Manage Content* service; zeroized by *Lifecycle* card termination. SD-KDEK is used to decrypt CSPs entered into the module.

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*, *PKI Applet Secure Channel* and *TWNID Applet GP Secure Channel* as a consequence of secure channel initialization and usage; however, while the SD-RMAC key is generated by default, the *PKI Applet Secure Channel* and *TWNID Applet GP Secure Channel* services do not use it). 'Z' on *Module Reset* as 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.

Establish PACE Channel (TWNID-SENC, TWNID-SMAC, TWNID-EKAK-PRI/PUB/PEER): PACE channel establishment through a Diffie-Hellman key agreement generates a shared secret by providing the ephemeral public key to the peer, and using the ephemeral private key (TWNID-EKAK-PRI) and peer public key (TWNID-EKAK-PEER) to derive TWNID-SENC and TWNID-SMAC. Use of the TWNID secure channel for other services is indicated by an 'E' in the TWNID-SENC and TWNID-SMAC columns. The ephemeral key pair (TWNID-EKAK-PRI\PUB) and peer public key (TWNID-EKAK-PEER) are zeroized after the secure channel is established.

Entity authentication services: PKI-KXAUTH, PKI-KIAUTH, PKI-AUTH enters the module via *PKI Applet preparation.* PKI-AUTH is used ('E') by *Entity Authentication with Password* and *TWNID User Authentication with password*, and may be updated by *Change PIN* or *Unblock PIN* ('W'). Entity authentication with symmetric key uses PKI-KXAUTH and PKI-KIAUTH for external and internal authentication, respectively.

Digital Signature: uses PKI-KRSA-PRI/PKI-KRSA-PUB or PKI-KECC-PRI/PKI-KECC-PUB for digital signature ('E'). These key pairs may be generated on card, with the public keys exported to the host, or may be imported into the module using the Key Management service.

4 Self-test

4.1 Power-On Self-tests

On power-on or reset, the module performs self-tests as described in Table 16 below. All KATs must be completed successfully prior to any other use of cryptography by the module. If one of the KATs fails, the system is halted and will start again after a reset (the *CM is Mute* error state).

Test Target	Cert	Description
AES	3997	Performs separate encrypt and decrypt KATs using an AES-128 key in CBC mode.
AES CMAC	3997	Performs AES CMAC generate and verify KATs using an AES-128 key.
DRBG	1187	Performs a fixed input KAT and all SP 800-90A health test monitoring functions.
ECC CDH	824	Performs a fixed input KAT using the P-256 curve.
ECDSA	890	Performs ECDSA signature and verify KAT using the P-256 curve.
FW Integrity	N/A	16 bit CRC performed over all code located in NVM. This integrity test is not required or performed for code stored in ROM.
KBKDF	91	Performs a fixed input KAT on SP 800-108 AES CMAC based KBKDF
RSA	2053	Performs separate RSA CRT signature and verify KATs using an RSA 2048-bit key.
SHA-1	3299	Performs a fixed input KAT.
SHA-256	3299	Performs a fixed input KAT.
SHA-512	3299	Performs a fixed input KAT.
Triple-DES	2195	Performs encrypt and decrypt KATs using 3-Key Triple-DES in CBC mode.

Table 16: Power-On Self-Tests

4.2 Conditional self-tests

Test Target	Cert	Description
DRBG CRNGT	1187	On every call to the NDRNG or DRBG, the module performs the AS09.42 continuous RNG test to assure that the output is different than the previous value.
ECDSA PCT	890	Pairwise consistency test performed when an ECDSA key pair is generated.
FW Load	N/A	Firmware loaded into the module using the *Manage Content* command is verified using the DAP-PUB public key.
NDRNG CRNGT	N/A	AS09.42 continuous RNG test performed on every call to the NDRNG to assure that the output is different than the previous value.
RSA PCT	2086	Pairwise consistency test performed when an RSA key pair is generated.

Table 17: 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). Detection of an active shield tamper event places the module permanently into the *Tamper Is Detected* error state.

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

6 Operational Environment

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

7 Electromagnetic interference and compatibility (EMI/EMC)

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

8 Mitigation of Other Attacks Policy

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[2], 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.

The platform (chip and operating system) is Common Criteria validated; more information is available here: http://www.commoncriteriaportal.org/products/.

9 Security Rules and Guidance

The module implementation also enforces the following security rules:

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

[2] FIPS 140-2 defines EFP in Level 4; in this submission, the platform vendor declined to perform additional testing beyond Level 3 and what was already performed for Common Criteria validation.