HiCOS PKI Applet and Taiwan eID Applet on Oberthur Technologies ID-One Cosmo V8 FIPS 140-2 Non-Proprietary Security Policy

August 25, 2016

References

Reference	Full Specification Name
[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 ISO/IEC 7816-4:2013 Identification cards - Integrated circuit cards - Part 4: Organization, security and commands for interchange ISO/IEC 7816-5:2004 Identification cards - Integrated circuit cards - Part 5: Registration of application providers ISO/IEC 7816-6:2004 Identification cards - Integrated circuit cards - Part 6: Interindustry data elements for interchange ISO/IEC 7816-8:2004 Identification cards - Integrated circuit cards - Part 8: Commands for security operations ISO/IEC 7816-9:2004 Identification cards - Integrated circuit cards - Part 9: Commands for card management ISO/IEC 7816-11:2004 Identification cards - Integrated circuit cards - Part 11: Personal verification through biometric methods
[JavaCard]	Java Card 3.0.1 Classic – Runtime Environment (JCRE) Specifications Java Card 3.0.1 Classic – Virtual Machine (JCVM) Specifications Java Card 3.0.1 Classic – Application Programming Interface (API) Published by Sun Microsystems, May 2009
[GlobalPlatform]	GlobalPlatform Card Specification 2.2.1 – January 2011, GlobalPlatform Card Specification – Amendment E – Security Upgrade for card content management – Public Release November 2011 v1.0 GlobalPlatform Card Basic ID Configuration – Version 1.0 – December 2011 GlobalPlatform Card Technology Card Specification – ISO Framework Version 0.9.0.18 Public Review July 2013 GlobalPlatform Consortium: http://www.globalplatform.org
[PKCS#1]	PKCS #1 v2.1: RSA Cryptography Standard, RSA Laboratories, June 14, 2002
[ANS X9.31]	American Bankers Association, Digital Signatures Using Reversible Public Key Cryptography for the Financial Services Industry (rDSA), ANSI X9.31-1998 - Appendix A.2.4.
[FIPS140-2]	NIST, Security Requirements for Cryptographic Modules, May 25, 2001
[IG]	NIST, Implementation Guidance for FIPS PUB 140‐2 and the Cryptographic Module Validation Program, last updated 25 July 2013.
[FIPS113]	NIST, Computer Data Authentication, FIPS Publication 113, 30 May 1985.
[FIPS197]	NIST, Advanced Encryption Standard (AES), FIPS Publication 197, November 26, 2001.
[FIPS 186-4]	NIST, Digital Signature Standard (DSS), FIPS Publication 186-4, July, 2013
[FIPS 180-4]	NIST, Secure Hash Standard, FIPS Publication 180-4, March 2012
[SP800-38F]	NIST, Recommendation for Block Cipher Modes of Operation: Methods for Key Wrapping, December 2012
[SP 800-56A]	NIST Special Publication 800-56A, Recommendation for Pair‐Wise Key Establishment Schemes Using Discrete Logarithm Cryptography, March 2007
[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 (Revised), October 2009
[SP800-131A]	Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths, January 2011
[EAC v1]	TR-03110 Advanced Security Mechanism for Machine Readable Travel Documents, Part 1, Part 2, Part

Reference	Full Specification Name
	3, V2.10 March 2012
[PACE]	TR Supplemental Access Control for Machine Readable Travel Documents, V1.01
[ICAO]	ICAO 9303 Edition 6 Part 1, Part 2, Part 3

Table 1 – References

Acronyms and definitions

Acronym	Definition
AIS 31	A German acronym referring to standard for functionality and evaluation of random number generation
ADF	Application Dedicated File
APDU	Application Protocol Data Unit, see [ISO 7816]
API	Application Programming Interface
CHV	Card Holder Verification
CM	Card Manager, see [GlobalPlatform]
CRT	Chinese Remainder Theorem
CSP	Critical Security Parameter, see [FIPS 140-2]
DAP	Data Authentication Pattern, see [GlobalPlatform]
DPA	Differential Power Analysis
EAC	Extended Access Control
GP	Global Platform
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 Global Platform)
PACE	Password Authenticated Connection Establishment
PCT	Pairwise Consistency Test
PKI	Public Key Infrastructure
SAC	Supplemental Access Control
SCP	Secure Channel Protocol, see [GlobalPlatform]
STD	Standard, as in Standard (non-CRT) RSA
SPA	Simple Power Analysis
TPDU	Transport Protocol Data Unit, see [ISO 7816]

Table 2 – Acronyms and Definitions

1. Introduction

This document defines the Security Policy for the Chunghwa Telecom Co., Ltd. HiCOS PKI Applet and Oberthur Technologies' Taiwan eID Applet on Oberthur Technologies ID-One Cosmo v8 cryptographic module. The module, a single chip embodiment validated to FIPS 140-2 Overall Security Level 2, is the combination of the HiCOS PKI Applet (denoted PKI Applet below) and Oberthur Taiwan eID Applet (denoted LDS Applet below) running on and bound to the Oberthur ID-One Cosmo v8.0-R2 (denoted platform below).

The platform provides an operational environment for the PKI Applet and LDS 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. However, the factory configuration of the module constrains the module to the set of services provided by the platform's Card Manager (implementing a standard set of GlobalPlatform services), LDS Applet and the PKI Applet. As such, some functionality and options present on the platform are not usable on this module such as the PIV applet which is deactivated in this module. Unusable functionality is not discussed further in this document.

1.1 Functional Overview

The LDS 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 applet supports the secure channel and authentication mechanisms described in ICAO and EAC specifications [ICAO], [PACE], [EAC v1] with a fully configurable access control management over the Data Groups (DGs) allowing the applet to be used not just as MRTD and IDL but for other applications as well.

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	3
Cryptographic Module Ports and Interfaces	3
Roles, Services, and Authentication	2
Finite State Model	2
Physical Security	4
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 Requirements

1.2 Versions, Configurations and Modes of operation

Hardware: '0F'
Firmware: '5601'
Firmware Extension: '082371'
Applets: HiCOS PKI Applet V1.0, Taiwan eID Applet V1.0
The module is available in 3 hardware configurations:

- Contact Only
- Contactless Only
- Dual Interface

The module is always in the Approved mode. The associated FIPS 140-2 Level is configured in the factory to operate exclusively in the Approved mode. The explicit indicator of the Approved mode of operation is obtained by use of the Module Info (Unauthenticated) and the PKI Applet Info (Unauthenticated) services, specifically the commands and tags shown next.

Command and associated elements	Expected Response
GET DATA (tag 'DF52') with Card Manager selected (Value of FIPS Mode data objects (tag '05')	'01'
GET DATA (tag '0105') with PKI Applet selected	'03020101'

Table 4- Approved Mode Indicator

1.3 Hardware and Physical Cryptographic Boundary

The module is designed to be embedded into a plastic card body, with a contact plate and/or contactless antenna connections, or in a USB token or other standard IC packaging, such as SOIC, QFN or MicroSD.

The physical form of the module is depicted in Figure1. The cryptographic boundary of the module is the surface and edges of the die and associated bond pads, shown as circles in the figure.

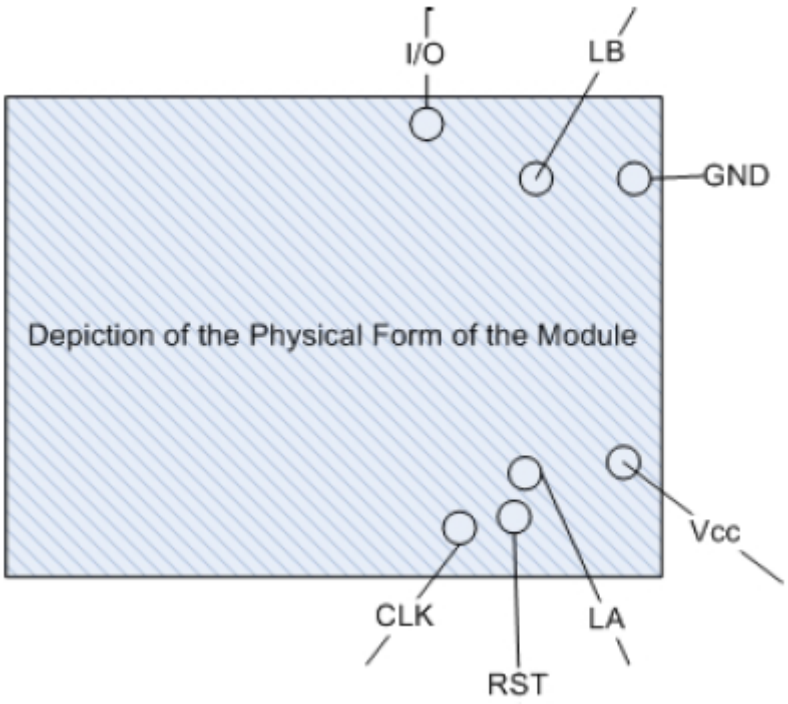

Figure 1 –Physical Form

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

Port	Description	Logical Interface Type
V_{CC}, GND	ISO 7816: Supply voltage	Power (not available in contactless-only configurations)
RST	ISO 7816:Reset	Control in (not available in contactless-only configurations)
CLK	ISO 7816: Clock	Control in (not available in contactless-only configurations)
I/O	ISO 7816: Input/ Output	Control in, Data in, Data out, Status out (not available in contactless-only configurations)
LA, LB	ISO 14443: Antenna	Power, Control in, Data in, Data out, Status out (Not available in Contact-only configurations)

Table 5 – Ports and Interfaces

1.4 Firmware and Logical Cryptographic Boundary

Figure 2 depicts the module operational environment.

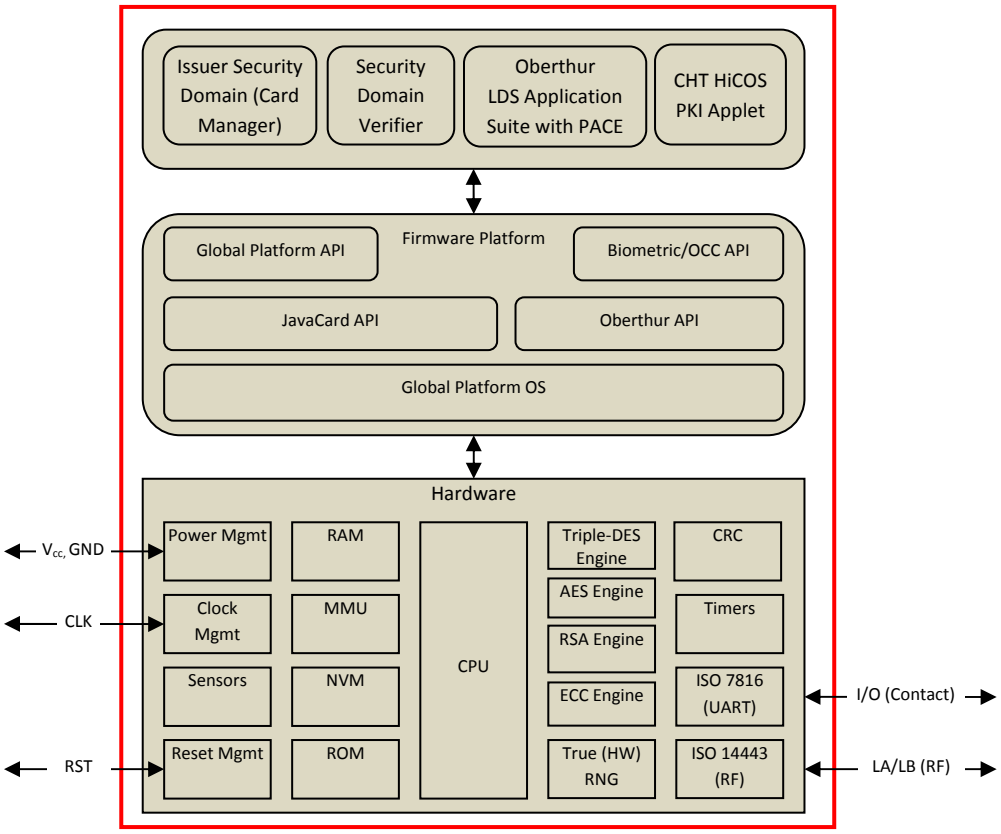

Figure 2 - Module Block Diagram
(Cryptographic Boundary Outlined in Red)

Section 3 describes applet functionality in greater detail. The Java Card and Global Platform APIs are internal interfaces available only to applets. Only applet services are available at the card edge (the interfaces that cross the cryptographic boundary). In the figure above, the Security Domain Verifier prevents loading an unauthorized (unsigned) code package into the module, and does not provide separate services.

All code is executed from ROM and NVM.

The chip family provides accelerators for AES, Triple-DES, RSA, ECC, CRC and an AIS-31 P2 class tested True (HW) RNG. The communications options for contact and contactless configurations are present in the physical circuitry of all members of the processor family, but are selectively enabled during module manufacturing.

2. Cryptographic Functionality

The module implements the Approved and Non-Approved but Allowed cryptographic functions listed in Table 6 and Table 7 below:

Algorithm	Description	Cert #
DRBG	[SP 800-90A] AES-128 CTR_DRBG. Does not support prediction resistance, supports re-seed operation and concatenation to provide security strength greater than 128 bits.	537
Triple-DES	[SP 800-67] Triple Data Encryption Algorithm. The module supports 3-Key option only, and CBC and ECB modes.	1727
AES	[FIPS 197] Advanced Encryption Standard algorithm. The module supports AES-128, AES-192- and AES-256 keys, and ECB and CBC modes.	2910
AES (Key Wrap)	[SP800-38F] AES Key Wrap (key establishment method provides 128-256 bits of encryption strength).	2910
Key wrap	Symmetric key wrap using AES 128, 192, 256 (key establishment method provides between 128 and 256 bits of encryption strength), Approved per IG D.9 and SP 800-38F §3.1 ¶3. Uses AES Cert. #2910 and AES Cert. #2911 (AES CMAC).	2910, 2911
AES (CMAC)	[SP800-38B] AES CMAC. The module supports AES-128, AES-192 and AES-256 keys.	2911
SHA-256	[FIPS 180-4] Secure Hash Standard compliant one-way (hash) algorithms: SHA-224, SHA-256.	2449
SHA-512	[FIPS 180-4] Secure Hash Standard compliant one-way (hash) algorithms: SHA-384, SHA-512.	2450
RSA STD	[FIPS 186-4] RSA signature verification. The module supports 2048-bit RSA keys.	1531
RSA CRT	[FIPS 186-4] RSA key generation and signature generation. The module supports 2048-bit RSA keys.	1532
ECDSA	[FIPS 186-4] Elliptic Curve Digital Signature Algorithm. The module supports the NIST defined P-224, P-256, P-384, and P-521 curves for key pair generation, signature generation and signature verification.	526
KBKDF	[SP 800-108] AES CMAC-based KDF with AES-128, AES-192, AES-256.	33
CVL (RSADP)	[SP 800-56B] SP 800-56B Section 7.1.2 RSA decryption primitive (as used by the PIV specification). The module supports the RSA-2048 key pair size, key decryption only.	336

Table 6 – Approved Cryptographic Functions

The CAVP certificates associated with this module include other algorithms, modes, and curves or key sizes that have been CAVP validated but are not available in this module. Only the algorithms, modes, and curves or key sizes shown in Table 6 are available in this module.

Algorithm	Description
NDRNG	[AIS 31] Class P2 Hardware True NDRNG used to seed the FIPS approved DRBG. The NDRNG provides a minimum of 264 bits of entropy as seeding material to the approved DRBG.
EC Diffie-Hellman	EC Diffie-Hellman (key establishment method provides 112, 128, 192 or 256 bits of encryption strength), allowed per IG D.8 and SP 800-131Ar1.

Table 7 – Non -Approved but Allowed Cryptographic Functions

2.1 Critical Security Parameters

All CSPs used by the module are described in this section. All usage of these CSPs by the module is described in the services detailed in Section 3. In the tables below, the OS prefix denotes operating system, the SD prefix denotes the Global Platform Security Domain, and the LDS prefix denotes a LDS Application CSP and the PKI prefix denotes a PKI Application CSP.

All CSPs, (keys and PINs) except OS-MKEK are store encrypted by OS-MKEK with a corresponding checksum.

CSP	Description / Usage
OS-DRBG-SEED	Entropy input provided by the True (HW) NDRNG, used to seed the Approved DRBG.
OS-DRBG-STATE	The current AES-128 CTR_DRBG state.
OS-MKEK	Triple-DES (3-Key) Key Encryption Key used for encrypted storage of CSPs.
SD-KENC	AES (128-bit, 192-bit, 256-bit) Master key used to generate SD-SENC.
SD-KMAC	AES (128-bit, 192-bit, 256-bit) Master key used to generate SD-SMAC.
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.

Table 8 – OS Critical Security Parameters

CSP	Description / Usage
PKI-KXAUTH	Triple-DES (3-Key) or AES (128-bit, 192-bit, 256-bit) PKI applet External Authentication key.
PKI-KIAUTH	Triple-DES (3-Key) or AES (128-bit, 192-bit, 256-bit) PKI applet Internal Authentication key.
PKI-KRSA-PRI	RSA (2048-bit) PKI applet signature generation private keys.
PKI-KECC-PRI	ECC (P-224, P-256, P-384) PKI applet ECDSA signature generation private keys.
PKI-AUTH	10-byte authentication datum, with 2 instances used for card holder PIN verification and pin unblocking.

Table 9 – PKI Applet Critical Security Parameters

CSP	Description / Usage
LDS-SENC	AES (128-bit, 192-bit, 256-bit) session encryption key used to encrypt / decrypt secure channel data.
LDS-SMAC	AES (128-bit, 192-bit, 256-bit) session MAC key used to verify inbound secure channel data integrity and to generate response secure channel data MAC.
LDS-CA	ECC (P-224, P-256, P-384, P-521) Chip Authentication Elliptic Curve Diffie-Hellman private key.
LDS-AA	RSA (2048-bit) or ECDSA (P-224, P-256, P-384, P-521) Active Authentication private key.

Table 10 – LDS Applet Critical Security Parameters

2.2 Public Keys

CSP	Description / Usage
PKI-KRSA-PUB	RSA (2048-bit) 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) public keys held in the module for retrieval by external users through the PKI applet.
LDS-AA-PUB	RSA (2048-bit) or ECC (P-224, P-256, P-384, P-521) Active Authentication public key.
LDS-CA-PUB	ECC (P-224, P-256, P-384, P-521) Chip Authentication Elliptic Curve Diffie-Hellman public key.
LDS-ROOT	RSA (2048-bit) or ECC (P-224, P-256, P-384, P-521) public key used to verify the signature of terminal certificates.
LDS-TA	RSA (2048-bit) and or ECC (P-224, P-256, P-384, P-521) Terminal Authentication temporary key.

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 ISD/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 eID 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 below.
AA	Application Administrator - a role that manages LDS 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 selected. Authenticated using the PKI Applet Secret Value authentication method with LDS selected.
EIS	Extended Inspection System – a role when the LDS Applet is selected that can read the more sensitive LDS data groups (DG3 and DG4). Authenticated using the LDS Applet Extended Access Control method with LDS selected.

Table 12 – Roles Supported by the Module

3.1 GP Secure Channel Protocol Authentication Method

The GP Secure Channel Protocol Authentication method is provided by the *GP Secure Channel* service, the *PKI Applet Secure Channel* service or the *LDS Applet GP Secure Channel* service. These services each invoke the same underlying library calls, but from the Card Manager, PKI Applet and LDS 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 “slowdown mechanism” that increases the response time between two authentications attempts following a failed authentication, such that no more than 9 attempts are possible in a one minute period. The probability that a random attempt will succeed over a one minute interval is:

- 9 /2^128 = 2.6E-38 (for any of AES-128/192/256 SD-KENC/SD-SENC, assuming a 128-bit block)

GP Secure Channel Protocol establishment provides mutual authentication service as well as establishment of a secure channel to protect confidentiality and integrity of the transmitted data.

3.2 PKI Applet Symmetric Key Authentication Method

The PKI Applet Symmetric Key Authentication method is provided by the PKI Applet *Entity authentication with symmetric key* service. The external entity obtains an 8-byte challenge from the module, encrypts the challenge and sends the cryptogram to the module. The module decrypts the cryptogram, and the external entity is authenticated if the decrypted value matches the challenge. This method is used by the PKI Applet Authentication and Administrator Authentication services. The strength of authentication using this method is dependent on the algorithm, key size and challenge size used: the minimum strength key used for this method is 3 - Key Triple- DES, using 8 bytes (a single Triple - DES block).

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

- 1/2^64 = 5.4E-20

The maximum number of consecutive failed authentication attempts is 5, so the probability that a random attempt will succeed over a one minute interval is:

- 5/2^64 = 2.7E-19

3.3 PKI Applet Secret Value Authentication Method

The PKI Applet Secret Value Authentication method is provided by the PKI Applet *Entity authentication with password* service. The external entity submits an identifier and corresponding secret value. The module compares all 10 bytes to the appropriate stored reference instance (e.g., Cardholder PIN). The enforcement of minimum number of characters before padding is not the same as a fixed minimum length for the secret. For example, a minimum of 6 characters means secrets can be created from 6 to 10 characters, determined by the user.

The worst case scenario permitted by the module is a minimum length of 6 characters allowing only numeric ASCII characters. The character space for the first 6 bytes in this scenario is 10 (the values ‘30’ through ‘39’ are permitted) and in the last 4 characters is 11 (the values ‘30’ through ‘39’ and ‘FF’ are permitted). The probability that a random attempt will succeed using this authentication method is:

- 1/(10^6 *11^2) = 8.3E-9

The applet implements a failed attempt counter, blocking after 10 failed attempts. The probability that a random attempt will succeed over a one minute interval is:

- 10/(10^6 * 11^2) = 8.3E-8

3.4 LDS Applet Extended Access Control

The LDS Applet Extended Access Control method is provided by the LDS Applet *Terminal Authentication* service. Extended Access Control (EAC) includes a mutual authentication process in which the authentication of the external entity (the terminal) to the applet uses an ECDSA (P-224, P-256, P-384 or P-521 with SHA-2) or RSA (2048 bit with SHA-2) based challenge response protocol.

The probability that a random attempt will succeed using this authentication method with either the P-224 or RSA 2048-bit keys is:

- 1/(2^112) = 1.9E-34

The applet implements a failed attempt counter, blocking after 15 failed attempts. The probability that a random attempt will succeed over a one minute interval is:

- 15/(2^112) = 2.9E-33

3.5 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.
LDS Applet	
Establish PACE Channel	Establish secure channel between terminal and LDS applet using EC Diffie-Hellman (not tested for compliance to SP 800-56A).
LDS Applet (requires active PACE channel)	
LDS Applet Info (Unauthenticated)	Read low sensitivity LDS applet data objects.
Active Authentication	Challenge-response protocol to assure chip authenticity.
Chip Authentication	Alternative mechanism to assure chip authenticity, using a DH scheme with authentication.
Terminal Authentication	Challenge-response protocol used to authenticate the terminal to the card.

Table 13 – Unauthenticated Services

Service	Description	CO	AA	User	EIS
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 LDS applet.		X		
LDS Applet					
LDS Applet GP Secure Channel	Establish and use an LDS Applet GP secure communications channel.		X		
LDS Applet preparation	Manage LDS applet authentication data and keys.		X		
LDS User Authentication with password	Authenticate User or BIS role to the module (PIN verification).			X	
Read Sensitive Data Groups	Read the more sensitive LDS data groups (DG3 & DG4).				X
Read Taiwan eID Data Groups	Read the Taiwan eID data groups.			X	
Update Data Groups	Update LDS applet data.		X		

Table 14 – Authenticated Services

Service	CSPs and Public Keys																										
	Platform CSPs	OS-DRBG-SEED	OS-DRBG-STATE	OS-MKEK	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	***LDS Applet CSPs***	LDS-SENC	LDS-SMAC	LDS-CA	LDS-AA	***Public Keys***	PKI-KRSA-PUB	PKI-KECC-PUB	LDS-AA-PUB	LDS-CA-PUB	LDS-ROOT	LDS-TA
Unauthenticated Services																											
Context		--	--	--	--	--	--	E	E	E		--	--	--	--	--		--	--	--	--		--	--			--	--
Module Info (Unauthenticated)		--	--	--	--	--	--	E	E	E		--	--	--	--	--		--	--	--	--		--	--	--	--	--	--
Module Reset		GE	GZ	--	--	--	--	Z	Z	Z		--	--	--	--	--		Z	Z	--	--		--	--	--	--	--	Z
PKI Applet Info (Unauthenticated)		--	--	--	--	--	--	--	--	--		--	--	--	--	--		--	--	--	--		--	--	--	--	--	--
Establish PACE Channel		--	--	--	--	--	--	--	--	--		--	--	--	--	--		GE	GE	--	--		--	--	--	--	--	--
LDS Applet Info (Unauthenticated)		--	--	--	--	--	--	--	--	--		--	--	--	--	--		E	E	--	--		--	--	--	--	--	--
Active Authentication		--	--	--	--	--	--	--	--	--		--	--	--	--	--		E	E	--	E		--	--	E	--	--	--
Chip Authentication		--	--	--	--	--	--	--	--	--		--	--	--	--	--		GE	GE	E	--		--	--	--	--	--	--
Terminal Authentication		--	--	--	--	--	--	--	--	--		--	--	--	--	--		E	E	--	--		--	--	--	--	E	EW
Platform Services																											
GP Secure Channel		--	EW	E	E	E	E	GE	GE	GE		--	--	--	--	--		--	--	--	--		--	--	--	--	--	--
Lifecycle		Z	Z	Z	Z	Z	Z	E	E	E		Z	Z	Z	Z	Z		--	--	Z	Z		Z	Z	Z	Z	Z	--
Manage Content		--	--	--	W	W	EW	E	E	E		--	--	--	--	--		--	--	--	--		--	--	--	--	--	--
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	--		W	W	--	--	W		--	--	--	--		--	--	--	--	--	--
Entity authentication with symmetric key		--	--	E	--	--	--	E	E	--		E	E	--	--	--		--	--	--	--		--	--	--	--	--	--
Entity authentication with password		--	--	--	--	--	--	E	E	--		--	--	--	--	E		--	--	--	--		--	--	--	--	--	--
Change PIN		--	--	--	--	--	--	E	E	--		--	--	--	--	W		--	--	--	--		--	--	--	--	--	--
Unblock PIN		--	--	--	--	--	--	E	E	--		--	--	--	--	W		--	--	--	--		--	--	--	--	--	--
File Content Manage		--	--	--	--	--	--	E	E	--		--	--	--	--	--		--	--	--	--		--	--	--	--	--	--
Generate asymmetric key pair		--	EW	E	--	--	--	E	E	--		--	--	G	G	--		--	--	--	--		G	G	--	--	--	--
Digital Signature		--	EW	E	--	--	--	E	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	--		--	--	--	--	--		--	--	--	--		--	--	--	--	--	--
LDS Applet Services																											
LDS Applet GP Secure Channel		--	EW	E	E	E	--	GE	GE	G		--	--	--	--	--		--	--	--	--		--	--	--	--	--	--
LDS Applet preparation		--	--	--	--	--	--	E	E	--		--	--	--	--	--		--	--	GW	GW		--	--	GWR	GWR	W	--
LDS User Authentication with password		--	--	--	--	--	--	--	--	--		--	--	--	--	E		E	E	--	--		--	--	--	--	--	--
Read Sensitive Data Groups		--	--	--	--	--	--	--	--	--		--	--	--	--	--		E	E	--	--		--	--	--	--	--	--
Read Taiwan eID Data Groups		--	--	--	--	--	--	--	--	--		--	--	--	--	--		E	E	--	--		--	--	--	--	--	--
Update Data Groups		--	--	--	--	--	--	E	E	--		--	--	--	--	--		--	--	--	--		--	--	--	--	--	--

Table 15 – Access to CSPs by Service

Table 15 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). This module does not permit this type of access.
- 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-DRBG CSPs: OS-DRBG-SEED 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*, *LDS 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 *LDS 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 *LDS Applet GP Secure Channel* services do not use it). 'Z' on *Module Reset* as a consequence of RAM clearing/garbage collection.

Establish PACE Channel (LDS-SENC, LDS-SMAC): PACE channel establishment through a Diffie-Hellman key agreement generates a shared secret from which LDS-SENC and LDS-SMAC are derived. Use of the LDS secure channel for other services is indicated by an 'E' in the LDS-SENC and LDS-SMAC columns.

Entity authentication services: PKI-KXAUTH, PKI-KIATUH, PKI-AUTH enters the module via *PKI Applet preparation.* PKI-AUTH is used ('E') by *Entity Authentication with Password* and *LDS 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.

Active Authentication: Uses the private LDS-AA key to sign the challenge provided by the terminal. Uses LDS-AA-PUB to verify the signature generated by the host.

Chip Authentication (LDS-SENC, LDS-SMAC): *Chip Authentication* uses the LDS secure channel: 'G' in LDS-SENC and LDS-SMAC represents session key generation, 'E' represents session key use in the secure channel.

Terminal Authentication (LDS-ROOT, LDS-TA): *Terminal Authentication* uses the LDS-TA public key provided by an external entity ('W') to verify the succeeding certificates or to verify the signature provided by the terminal ('E'), and LDS-ROOT to verify the terminal certificates ('E').

Digital Signature: uses PKI-KRSA-PRI/PKI-KRSA-PUB or PKI-KECC-PRI/PKI-KECC-PUB for digital signature ('E').

LDS Applet preparation: LDS-CA/LDS-CA-PUB, LDS-AA/LDS-AA-PUB, and LDS-ROOT are loaded into the module during LDS personalization ('W'); alternatively, LDS-CA/LDS-CA-PUB and LDS-AA/LDS-AA-PUB may be generated on-card ('G'). LDS-AA-PUB and LDS-CA-PUB can be exported from the module during LDS personalization ('R').

4. Self – tests

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.

Test Target	Description
CRC-16	Compute CRC 16 from a fixed message and check the result (a critical function test).
Firmware Integrity	16 bit CRC performed over all executable code in NVM.
DRBG	Performs a fixed input KAT.
AES	Self-test of AES forward cipher is performed by the SP 800-108 self-test. Self-test of AES inverse cipher is performed by the SP 800-38F self-test.
Triple-DES	Performs separate encrypt and decrypt KATs using 3-Key Triple-DES in ECB mode.
SP 800-108 KDF	Performs a KAT of SP 800-108 KDF. This self-test is inclusive of AES CMAC and AES encrypt function self-test.
SP 800-38F	Performs a KAT of SP 800-38F key unwrapping. This self-test is inclusive of AES decrypt function self-test.
RSA STD	Performs RSA signature verify KAT using an RSA 2048-bit key.
RSA CRT	Performs RSA CRT signature generate KAT using an RSA 2048-bit key. This test is inclusive of the RSADP primitive.
ECDSA	Performs ECDSA signature generation and verification known answer tests using the P-224 curve. This self-test is inclusive of the ECC CDH function self-test.
SHA-256	Performs a fixed input KAT of SHA-256 (inclusive of the SHA-224 truncated variation).
SHA-512	Performs a fixed input KAT of SHA-512 (inclusive of the SHA-384 truncated variation).

Table 16 – Power-On Self –Test

4.2 Conditional self - tests

On every call to the DRBG or True (HW) RNG, the module performs the AS09.42 continuous RNG test to assure that the output is different than the previous value.

The module performs the SP 800-90A health monitoring tests for all DRBG functions.

When an RSA or ECC key pair is generated or loaded, the module performs a pairwise consistency test.

When new firmware is loaded into the module using the Manage Content service, the module verifies the integrity of each packet using AES CMAC.

NOTE: If any self-test fails, the system emits an error code (0x6FXX) and enters the SELF-TEST ERROR state.

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

Module hardness testing was performed at the following temperatures:

- Nominal temperature: 20°C
- Low temperature: -40°C
- High temperature: 120°C

6. Operational Environment

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

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 implements defenses against:

- Light attacks
- Invasive fault attacks
- Side-channel attacks: SPA/DPA; Timing analysis;
- Electromagnetic attacks
- Differential fault analysis (DFA)
- Card tearing attacks

9. 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 comprehensive zeroization mechanism.
- 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.