Hypersecu HYP2003 MFA Cryptographic Module Non-Proprietary FIPS 140-2 Security Policy

Version: 1.0

Date: March 5, 2024

HYPERSECU INFORMATION SYSTEMS, INC

Table of Contents

List of Tables

List of Figures

1 Introduction

This document defines the Security Policy for the Hypersecu HYP2003 MFA Cryptographic Module, hereafter denoted the Module. The Module is a single chip embodiment implementing the JavaCard and Global Platform operational environment with a Card Manager, that is also considered an Issuer Security Domain (ISD), and five Applets. The Module meets FIPS 140-2 overall Level 2 requirements.

Table 1 – Cryptographic Module Configurations

	Module	HW P/N and Version	FW Version
1	Hypersecu HYP2003 MFA Cryptographic Module	SLE78CLUFX5000PH	7.04

The Module is intended for use by customers that require FIPS 140-2 validated cryptography modules.

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

Table 2 – Security Level of Security Requirements

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	N/A
Overall	2

1.1 Module Description and Cryptographic Boundary

The physical form of the Module is depicted in Figure 1. The Module is a single-chip embodiment. The cryptographic boundary is defined as the entire device.

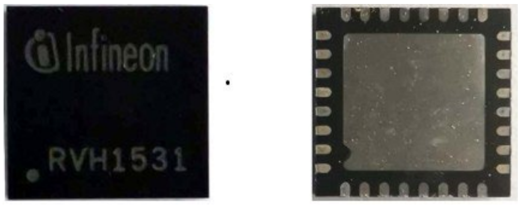

Figure 1 – Module

Figure 2 depicts the Module logical cryptographic boundary outlined in red rectangle.

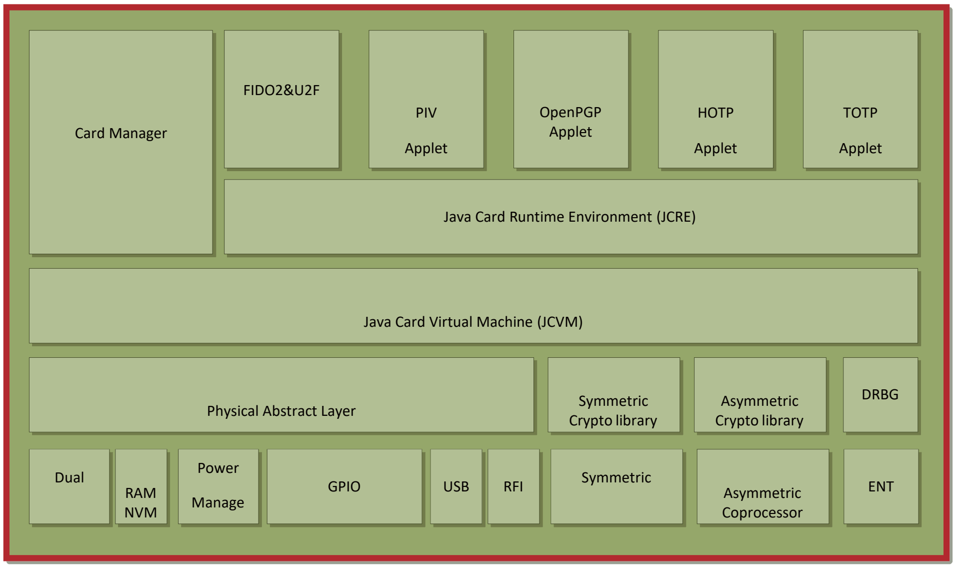

Figure 2 – The Module Cryptographic Boundary

The module's ports and associated FIPS defined logical interface categories are listed in Table 3.

Table 3 – Ports and Interfaces

Port	Description	Logical Interface Type
USB(D+/D-) 2 Pins	Primary physical interface (USB)	Control in, Data in, Data out, Status out
Power Supply 3 Pins	Vcc Vdd 1.62-5.5V	Power
I2C (SDA/SCL) 2 Pins	Primary physical interface (I2C)	Control in, Data in, Data out, Status out
Touch Button 1 Pin	Physical input	Control in
LED 1 Pin	Status LED	Status out
Contactless 2 Pins	Primary physical interface (contactless) antenna.	Control in, Data in, Data out, Status out

1.2 Mode of Operation

Each applet provides its own mode of operation, which is independent from the other applets.

The applets include: FIDO2&U2F, PIV, HOTP, TOTP, and OpenPGP. PIV only supports an Approved mode of operation, while the other applets support both an Approved and non-Approved mode of operation. To place a specific applet into the Approved or non-Approved mode of operation, follow the instructions provided below and adhere to the procedural controls outlined in Section 8 of this Security Policy. If no instructions are provided below, then only the procedural controls outlined in Section 8 of this Security Policy must be followed.

Applets do not share any keys, certificates, or CSPs between each other or between modes of operation.

1.2.1 HOTP/TOTP FIPS Approved/Non-Approved mode configuration

HOTP/TOTP can be toggled between the Approved and non-Approved mode using the “Switch Mode” service. In the non-Approved mode, this applet does not support authentication. To verify the HOTP/TOTP is in the Approved Mode, perform the ”Get FIPS mode state” service, which will return “01” for Approved mode and “00” for non-Approved mode.

Switching between modes of operation will zeroize all HOTP/TOTP Applet related CSPs by default.

In the Approved mode, no commands are available until the “SetCode” service is performed.

1.2.2 FIDO2&U2F FIPS Approved/Non-Approved mode configuration

FIDO2&U2F can be toggled between the Approved and non-Approved mode using the “Switch Mode” service with subcommand = 1 with non-Approved mode (param = 00) or Approved mode (param = 01). In the Approved mode, only FIDO2 functions are available and CTAP Pin Protocol 1 is disabled, as it uses a non-Approved KDA. In the non-Approved mode, U2F functions are supported, as well as CTAP PIN Protocol 1. The following U2F services are additionally available in the non-Approved mode:

- U2F Registration
- U2F Authentication

“Switch Mode” service with subcommand = 2, which will return “01” for Approved mode and “00” for non-Approved mode.

2 Cryptographic Functionality

The Module implements the FIPS Approved and Non-Approved but Allowed cryptographic functions listed in the table(s) below.

Table 4 – Approved Algorithms

Cert	Algorithm	Mode	Description	Functions/Caveats
A2406	AES[197]	ECB[38A]	Key Sizes: 128, 192, 256	Encrypt, Decrypt
		CBC[38A]	Key Sizes: 128, 192, 256	Encrypt, Decrypt
		CMAC[38B]	Key Sizes: 128, 192, 256 Mac Len: 32 – 128	Message Authentication
VA	CKG[IG D.12]	[133] Section 5.1 and 5.2 Asymmetric key generation using unmodified DRBG output		Key Generation
		[133] Section 6.1 Direct generation of Symmetric Key		

Cert	Algorithm	Mode	Description	Functions/Caveats
		[133] Section 6.2.1 Derivation of symmetric keys from a key agreement scheme		
A2406	CVL	EC CDH Primitive	Curves/Key sizes: P-224, P-256, P-384, P-521	Tested, but not used apart from KAS-SSC
A2406	DRBG[90A]	CTR	Use DF, AES-128	Deterministic Random Bit. Generation Security Strength = 128
A2406	ECDSA[186-4]		P-224, P-256, P-384, P-521 P-192 KeyVer Only	KeyGen, KeyVer
			P-224 SHA(224,256,384,512) P-256 SHA(224,256,384,512) P-384 SHA(224,256,384,512) P-521 SHA(224,256,384,512)	SigGen, SigGen Component
				SigVer, SigVer Component
N/A	ENT (P) [90B]			Entropy
A2406	HMAC [198]	SHA-1	Key Size: 128 bit minimum	Message Authentication
		SHA-224		
		SHA-256		
		SHA-384		
		SHA-512		
	KAS	ECDH and HKDF	KAS-SSC and KDA	KAS-SSC Cert. #A2406, KDA Cert. #A2406; key establishment methodology provides 128 bits of encryption strength.
A2406	KAS-SSC [56Ar3]	Ephemeral Unified	Curves/Key sizes: P-256	Key agreement for CTAP PIN Protocol 2
A2406	KDA[56Cr2]	HKDF	HMAC-SHA-256	HKDF for CTAP PIN Protocol 2
	KTS	AES-CBC and HMAC	128-bit AES and 128-bit HMAC-SHA-1 or 256-bit AES and 256-bit HMAC-SHA-256	Key establishment methodology provides 128 or 256-bits of encryption strength.
A2406, A2408	RSA [186-4]	FIPS186-4	n = 2048/3072/4096 Note: n = 3072/4096 only CRT mode Cert. #A2406 only tests 2048.	KeyGen
			n = 2048	RSA Decryption [SP800-56B] Tested, but not used
		PKCS1_v1.5	n = 2048/3072/4096 SHA(224, 256, 384, 512) Note: n = 3072/4096 only CRT mode Cert. #A2406 only tests 2048.	SigGen
			n = 2048/3072/4096 SHA(224, 256, 384, 512)	SigVer

Cert	Algorithm	Mode	Description	Functions/Caveats
			Cert. #A2406 only tests 2048.	
A2406	SHS [180]	SHA-1 SHA-224 SHA-256 SHA-384 SHA-512		Message Digest Generation, Password Obfuscation

2.1 Critical Security Parameters

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

Table 5 – Critical Security Parameters (CSPs)

CSP	Description	Generation	Entry	Output	Storage	Zeroization
Java Card Platform CSPs						
DRBG-EI	The input entropy and nonce for DRBG instantiation. The size of the entropy string is 51 bytes and the nonce is 26 bytes.	Internally generated using the NDRNG	N/A	N/A	Plaintext in RAM	Zeroized after reset
DRBG-State	CTR_DRBG (AES 128-bit): V (128-bit) and Key (128-bit) are the critical values of the internal state	Internally generated per SP800-90A	N/A	N/A	Plaintext in RAM	Zeroized after reset
Kos	128-bit AES key used to obfuscate all secret and private key data stored in NVM	Internally using the DRBG	N/A	N/A	Plaintext in Flash	No. The key is used for data obfuscation and cannot be destroyed.
FIDO2&U2F Applet CSPs						
FIDO2 Device ECDSA Private Key	256-bit ECC private key used to generate signature for FIDO2 registration.	N/A. Installed during production.	N/A	N/A	Encrypted by Managing Key in Flash	N/A. Encrypted by Managing Key
FIDO2 User ECDSA Private Key	256-bit ECC private key used to generate the credentialID	Internally using the DRBG during MakeCredential	KTS using Init_Keyenc and Init_Keymac during Get Assertion if RK=FALSE	KTS using Init_Keyenc and Init_Keymac	If Resident (RK=True), then stored in Flash encrypted by Init_Keyenc and Init_Keymac. Plaintext in RAM only if Transient (RK=False)	Zeroized by Switch Mode or Reset
Init Keyenc	128-bit AES CBC key used to encrypt the key handle or credentialID	Internally using the DRBG during production, Switch Mode, or Reset	N/A	N/A	Plaintext in Flash	Zeroized by Switch Mode or Reset
Init Keymac	128-bit HMAC SHA-1 key used to generate signature of the cipher key handle or credentialID	Internally using the DRBG during production, Switch Mode, or Reset	N/A	N/A	Plaintext in Flash	Zeroized by Switch Mode or Reset

CSP	Description	Generation	Entry	Output	Storage	Zeroization
Managing Key	128-bit AES-ECB key, used to encrypt CSPs and keys	Generated during production using the DRBG, Switch Mode, or Reset	N/A	N/A	Plaintext in Flash	Zeroized by Switch Mode or Reset
Agreement ECC Private Key	256-bit ECC private key used to perform key agreement with client public ECC key to get sharedSecret	Internally, using the DRBG during power on or Reset	N/A	N/A	Plaintext in RAM	Zeroized by Switch Mode or Reset
SharedSecret Key	256-bit AES CBC key used for encryption and HMAC SHA-256 calculation of pin related operations	KAS-SSC and KDA (CTAP PIN Protocol 2) during Set Pin, Change PIN, or Get pinToken	N/A	N/A	Plaintext in RAM	Zeroized by Switch Mode or Reset
User pinToken	256-bit HMAC SHA-256 Key used to authorize operator after PIN authentication	Internally using the DRBG during AuthenticatorClientPIN	N/A	KTS using SharedSecret key	Plaintext in RAM	Zeroized by Switch Mode or Reset
CO pinToken	256-bit HMAC SHA-256 Key used to authorize operator after PIN authentication	Internally using the DRBG during AuthenticatorAdminPIN	N/A	KTS using SharedSecret key	Plaintext in RAM	Zeroized by Switch Mode or Reset
PIN	Authenticate the User,4 to 63-byte PIN value	N/A	KTS using SharedSecret key	N/A	Flash, SHA-256 hash of PIN encrypted by Managing Key	Zeroized by Switch Mode or Reset
CO PIN	Authenticate the CO, 4 to 63-byte PIN value	N/A	KTS using SharedSecret key	N/A	Flash, SHA-256 hash of PIN encrypted by Managing Key	Zeroized by Switch Mode or Reset
hmacsaltKey	32-byte random value associated with the credential.	Internally using the DRBG during GetAssertion (supported hmac-secret)	N/A	N/A	Plaintext in RAM	Zeroized by Switch Mode or Reset
PIV Applet CSPs						
PIV Symmetric Key	128-bit AES ECB key, used for authentication of PIV CO. It is set with default value after personalization	N/A. Default value set during production	Plaintext during Set Management Key	N/A	Plaintext in Flash	The default value is restored after Reset
PIV Asymmetric Private Key	2048-4096 bit RSA or 256/384-bit ECC private key, used for cryptographic operations in conjunction with an external system	Internally using the DRBG during Generate Asymmetric Key	Plaintext during ImportKey	N/A	Plaintext in Flash	Zeroized by Reset
PIV Attestation Private Key	2048-4096 bit RSA or 256-bit ECC private key, used to attest internally generated public key using PKCS#1 signature	N/A. Installed during production	N/A	N/A	Plaintext in Flash	N/A
PIV User PIN	6 to 8-byte pin, used for authenticating the PIV user for Asymmetric services	N/A. Default value set during production	Plaintext during VerifyPIN, ChangePIN, GeneralAuth	N/A	Plaintext in Flash	The default value is restored after Reset

CSP	Description	Generation	Entry	Output	Storage	Zeroization
PIV PUK PIN	8-byte pin, used for unblocking the PIV user pin	N/A. Default value set during production	Plaintext during VerifyPUK, ChangePUK, UnlockPIN	N/A	Plaintext in Flash	The default value is restored after Reset
HOTP Applet CSPs						
HOTP OATH Seed Key	16 to 64-byte HMAC SHA-1/-256 key used to calculate OTP values for the User. Up to five may exist.	N/A.	Plaintext during "Put"	N/A	Plaintext in Flash	Zeroized by Switch Mode or Reset
HOTP OATH Auth Key	16 to 64-byte HMAC SHA-256 key used to authenticate operator through verification of HMAC calculated over a module generated challenge during the "Validate" service.	N/A.	Plaintext during "Set Code"	N/A	Plaintext in Flash	Zeroized by Switch Mode or Reset
TOTP Applet CSPs						
TOTP OATH Seed Key	16 to 64-byte HMAC SHA-1/-256 key, used to calculate OTP values for the User ("Calculate", "Calculate Default" services). Up to five may exist.	N/A.	Plaintext during "Put"	N/A	Plaintext in Flash	Zeroized by Switch Mode or Reset
TOTP OATH Auth Key	16 to 64-byte HMAC SHA-256 key, used to authenticate operator through verification of HMAC calculated over a module generated challenge during the "Validate" service.	N/A.	Plaintext during "Set Code"	N/A	Plaintext in Flash	Zeroized by Switch Mode or Reset
OpenPGP Applet CSPs						
OpenPGP Symmetric Key	AES-ECB 128-bit and AES-CMAC 128-bit keys (SMKey-ENC, SM-Key-MAC) for secure messaging.	N/A. Imported.	Plaintext during putData	N/A	Plaintext in Flash	Zeroized by "TERMINATE APPLET" followed by "ACTIVATE APPLET"
OpenPGP Admin PIN(PW3)	8 to 127-byte, used for authentication of the OpenPGP CO.	N/A. Default value is set by the manufacturer.	Plaintext for each Admin command	N/A	Plaintext in Flash	Reset to default by "TERMINATE APPLET" followed by "ACTIVATE APPLET"
OpenPGP User PIN(PW1)	6 to 127-byte, used for authenticating the OpenPGP user for Asymmetric services.	N/A. Default value is set by the manufacturer.	Plaintext for each User command	N/A	Plaintext in Flash	Reset to default by "TERMINATE APPLET" followed by "ACTIVATE APPLET"
OpenPGP Signature Private Key	2048-4096 bit RSA private key, used for PKCS#1 v1.5 signing operation	Internally using the DRBG during Generate Asymmetric Key	Plaintext during Import Key	N/A	Plaintext in Flash	Zeroized by "TERMINATE APPLET" followed by "ACTIVATE APPLET"

CSP	Description	Generation	Entry	Output	Storage	Zeroization
OpenPGP Authentication Private Key	2048-4096 bit RSA private key, used for authentication specified in PKCS#1 v1.5 signing operation	Internally using the DRBG during Generate Asymmetric Key	Plaintext during Import Key	N/A	Plaintext in Flash	Zeroized by "TERMINATE APPLET" followed by "ACTIVATE APPLET"
OpenPGP Resetting Code	8 to 127-byte. Used for resetting the User PIN	N/A	Plaintext during putData and "Reset Retry Counter"	N/A	Plaintext in Flash	Reset

2.2 Public Keys

Table 6 – Public Keys

Key	Description	Generation	Entry	Output	Storage
FIDO2&U2F Applet Public Keys					
FIDO2 Device ECDSA Public Key	256-bit ECC FIDO2 public key, it is returned to the server via the certificate to verify the signature generated after FIDO2 registration	N/A. Installed during production	N/A	Plaintext during MakeCredential	Plaintext In Flash
Agreement ECC Public Key	256-bit ECC public key used to perform key agreement, the Module returns it to server to derive sharedSecret	Internally, using the DRBG during power on or Reset	N/A	Plaintext during KAS-SSC	Plaintext in RAM
Client ECC Public Key	256-bit ECC Client public key for key agreement, the client sends it to applet to generate sharedSecret	N/A	Plaintext during KAS-SSC	N/A	Plaintext in RAM
FIDO2 User ECDSA Public Key	256-bit ECC FIDO2 public key, it is transmitted to the server for verifying signature generated after FIDO2 authentication	Internally using the DRBG during MakeCredential	N/A	Plaintext during MakeCredential	Plaintext in RAM
PIV Applet Public Keys					
PIV Asymmetric Public Key	2048 – 4096-bit RSA or 256/384-bit ECC public key, used for cryptographic operations in conjunction with an external system	Internally, using the DRBG during Generate Asymmetric Key	Plaintext by Import Key	Plaintext during Generate Asymmetric Key	Plaintext in Flash
OpenPGP Applet Public Keys					
OpenPGP Signature Public Key	2048-4096 bit RSA public key, used for verification specified in PKCS#1 v1.5	Internally, using the DRBG during Generate Asymmetric Key	Plaintext by Import Key	Plaintext during Generate Asymmetric Key	Plaintext in Flash

Key	Description	Generation	Entry	Output	Storage
OpenPGP Authentication Public Key	2048-4096 bit RSA public key, used for authentication specified in PKCS#1 v1.5	Internally, using the DRBG during Generate Asymmetric Key	Plaintext by Import Key	Plaintext during Generate Asymmetric Key	Plaintext in Flash
HOTP Applet Public Keys					
None					
TOTP Applet Public Keys					
None					

3 Roles, Authentication and Services

3.1 Assumption of Roles

The Module contains five functional units (i.e., applets), each with its own distinct roles and services. The listed functional units are PIV, OpenPGP, TOTP, HOTP, FIDO2&U2F. Each functional unit operates independently of the others. They do not share roles, but CSPs maintained by Java Card platform (i.e., CSPs related to DRBG).

Table 7 – Authenticated Roles Description

Role ID	Role Description	Authentication Type	Authentication Data
FIDO2&U2F Crypto Officer	This role is responsible for switch mode and changing the CO PIN	Role-based	4 to 63-byte PIN
FIDO2&U2F User	This role is allowed to perform FIDO2&U2F Registration Authentication with the PIN (FIDO2&U2F key handles)	Role-based	4 to 63-byte PIN
PIV Crypto Officer	This role is responsible for configuring the PIV CSPs and resetting the user PIN using PUK.	Role-based	16-byte KEY (AES) or 8-byte PUK
PIV User	This role is allowed to perform cryptographic operation using PIV keys, and update user PIN.	Role-based	6 to 8-byte PIN
HOTP Crypto Officer	This role is responsible for creating and using CSPs.	Role-based	16 to 64-byte HMAC-SHA256 HOTP OATH Auth Key
TOTP Crypto Officer	This role is responsible for creating and using CSPs.	Role-based	16 to 64-byte HMAC-SHA256 TOTP OATH Auth Key
OpenPGP Crypto Officer	This role is responsible for configuring CSPs and resetting PW1 (user PIN) using the PW3.	Role-based	8 to 127-byte administrator PIN or Resetting Code PIN

Role ID	Role Description	Authentication Type	Authentication Data
OpenPGP User	This role is allowed to perform cryptographic operations (encryption, signature generation and authentication) and update PW1 (user PIN).	Role-based	6 to 127-byte user PIN

Table 8 – Unauthenticated Role Description

Role ID	Role Description	Authentication Data
Unauthenticated User	This role can reset all applets to factory default settings and may also read non-read-protected objects. This role can reset the PIV to factory default settings and can read all non - read - protected objects. This role can reset the HOTP, TOTP to factory default settings.	Unauthenticated – N/A

3.2 Authentication Methods

Table lists all details regarding the authentication mechanism.

Table 9 – Authentication Description

Authentication Method	Probability	Justification
User PIN 4 to 63-byte PIN (FIDO2&U2F)	The PIN is at least 4-bytes (32-bit) binary string with no restrictions on character space. The probability that a random attempt will succeed, or a false acceptance will occur is at most $\frac{1}{2^{32}}$, which is less than $\frac{1}{1{,}000{,}000}$.	The Module is limited by retry counter of 8 tries after which the module requires a reset. Therefore, the probability of successfully authenticating to the Module within one minute through random attempts is $\frac{8}{2^{32}}$, which is less than $\frac{1}{100{,}000}$.
Admin PIN 4 to 63 bytes (FIDO2&U2F)	The PIN is at least 4-bytes (32-bit) binary string with no restrictions on character space. The probability that a random attempt will succeed, or a false acceptance will occur is at most $\frac{1}{2^{32}}$, which is less than $\frac{1}{1{,}000{,}000}$.	The Module is limited by retry counter of 8 tries after which the module requires a reset. Therefore, the probability of successfully authenticating to the Module within one minute through random attempts is $\frac{8}{2^{32}}$, which is less than $\frac{1}{100{,}000}$.
128-bit key AES mutual challenge response (PIV)	This is an AES Key which has 128 bits of security strength. The probability that a random attempt will succeed, or a false acceptance will occur is $\frac{1}{2^{128}}$ which is less than $\frac{1}{1{,}000{,}000}$.	Authentication attempts are limited to 150 per minute. Therefore, the probability of successfully authenticating to the Module within one minute through random attempts is $\frac{150}{2^{128}}$, which is less than $\frac{1}{100{,}000}$.

Authentication Method	Probability	Justification
6 to 8-byte digit PIN or 8-byte digit PUK (PIV)	The PIN is at least a 6-byte (48-bit) binary string with no restrictions on character space. The probability that a random attempt will succeed, or a false acceptance will occur is at most $\frac{1}{2^{48}}$ which is less than $\frac{1}{1{,}000{,}000}$.	The authentication is limited by the retry counter of up to 10 tries (3 by default, but 10 maximum). Therefore, the probability of successfully authenticating to the Module within one minute through random attempts is at most $\frac{10}{2^{48}}$, which is less than $\frac{1}{100{,}000}$.
Auth Key 16 to 64-byte HMAC SHA-256 key (HOTP/TOTP)	The authentication key is a at least 16-byte (128-bit) binary string with no restrictions on character space. The probability that a random attempt will succeed, or a false acceptance will occur is at most $\frac{1}{2^{128}}$ which is less than $\frac{1}{1{,}000{,}000}$.	Each authentication attempt takes approximately 12 ms which allows a maximum of 5000 attempts per minute. Therefore, the probability of successfully authenticating to the Module within one minute through random attempts is at most $\frac{5000}{2^{128}}$, which is less than $\frac{1}{100{,}000}$.
User PIN 6 to 127-byte (OpenPGP)	The PIN is at least a 6-byte (48-bit) binary string with no restrictions on character space. The probability that a random attempt will succeed, or a false acceptance will occur is at most $\frac{1}{2^{48}}$ which is less than $\frac{1}{1{,}000{,}000}$.	The authentication is limited by the retry counter of up to 10 tries (3 by default, but 10 maximum).. Therefore, the probability of successfully authenticating to the Module within one minute through random attempts is at most $\frac{3}{2^{48}}$, which is less than $\frac{1}{100{,}000}$.
Admin PIN or Resetting Code 8 to 127-byte (OpenPGP)	The PIN and Resetting Code are at least 8-byte (48-bit) binary strings with no restrictions on character space. The probability that a random attempt will succeed, or a false acceptance will occur is at most $\frac{1}{2^{48}}$ which is less than $\frac{1}{1{,}000{,}000}$.	The authentication Is limited by the retry counter of up to 10 tries (3 by default, but 10 maximum).. Therefore, the probability of successfully authenticating to the Module within one minute through random attempts is at most $\frac{3}{2^{48}}$, which is less than $\frac{1}{100{,}000}$.

3.3 Services

All services implemented by the Module are listed in the table(s) below.

Table 10 – FIDO2&U2F Authenticated Services

Service	Description	CO	U
Make Credential	This service is used to generate a new credential in the module. If the Make Credential request contains “"hmac-secre”":true}, the mac-secret:true field will be included in the Make Credential response.		X
Get Assertion	This service is used to verify the FIDO2 cryptographic proof by the credentialID of user authentication. If the GetAssertion authentication request contains an hmac-secret extension, the authenticator generates a 32-byte random number as hmacsaltkey and associates it with the Credential.		X

Service	Description	CO	U
Get Next Assertion	The client calls this service when the GetAssertion response contains the number of credentials member and the number of credentials exceeds 1.		X
Authenticator Client PIN	This service is used by the platform to establish the sharedSecret key, setting a new user PIN, changing existing user PIN, and getting User pinToken from the module		X
Credential Management	This service is used to manage resident credentials on the applet, such as retrieving or deleting.		X
Authenticator Admin PIN	This service is used by the platform to establish the sharedSecret key, setting a new CO PIN, changing existing CO PIN, and getting CO pinToken from the module.	X	
Switch Mode	This service is used to switch between FIPS and non-FIPS mode and zeroizes all plaintext CSPs and get current mode state.	X	

Table 11 – PIV Authenticated Services

Service	Description	CO	U
Set Management Key	This service is used to change management key (PIV Symmetric Key).	X	
Change PUK	This service is used to change PUK.	X	
Change PIN	This service is used to change PIN.		X
Unblock PIN (Reset retry counter)	This service is used to reset retry counter and set new user PIN with known PUK.	X	
Set PIN Retries	This service is used to set retry limit for PIN, PUK. The minimum is 3 and the maximum is 10.	X	X
Generate Asymmetric Key	This service is used to generate an asymmetric key.	X	
GeneralAuth (RSA/ECDSA)	This service is used to authenticate the applet with RSA/ECC key.		X
Put Data	This service is used to write data (certificate, ID and etc.).	X	
Import Key	This service is used to import asymmetric key.	X	

Note: PIV services are not supported over NFC, these services must be performed over USB only.

Table 12 – HOTP Authenticated Services

Service	Description	CO
Set Code	Set or update an authentication key, it is a required step for FIPS Mode.	X
Put	Add a new entry and initialize its seed key.	X
Delete	Destroy the selected HOTP OATH Seed Key.	X
List	List all the names of the entries.	X
Calculate	Calculate the HOTP value for an entry.	X
Calculate Default	Calculate the HOTP for the default entry.	X
Set Default	Set default entry.	X

Service	Description	CO
Get Default	Get default entry.	X
Switch Mode	This service is used to switch the applet from FIPS mode to non-FIPS mode and vice versa.	X

Table 13 – TOTP Authenticated Services

Service	Description	CO
Set Code	Set or update an authentication key, a required step for FIPS Mode.	X
Put	Add a new entry and initialize its seed key.	X
Delete	Remove an entry and its seed key.	X
List	List all the names of the entries.	X
List Detail Info	List detail info of the entry.	X
Calculate	Calculate the TOTP value for an entry.	X
Calculate Default	Calculate the TOTP for the default entry.	X
Calculate All	Calculate the TOTP value for all entries.	X
Set Default	Set default entry.	X
Get Default	Get default entry.	X
Switch Mode	This service is used to switch the applet from FIPS mode to non-FIPS mode and vice versa.	X

Table 14 – OpenPGP Authenticated Services

Service	Description	CO	U
Change PW1	Change user PW1.		X
Change PW3	Change administrator PW3.	X	
Reset Retry Counter	Reset user PW1 using PW3 or Resetting Code.	X	
Set PIN Retries	Set retries limit for PW1 and PW3.	X	
Generate Asymmetric Key Pair	Generate asymmetric key pair.	X	
Perform Security Operation	Compute digital signature		X
Internal Authenticate	Perform internal authentication.		X
Read Protected Data For User	Read data objects only available to user.		X
Read Protected Data For Admin	Read data objects only available to administrator.	X	
Put Data	Write data objects except user writable data objects.	X	
Import Key	This service is used to import asymmetric key.	X	
Write User Protected Data	Write user writable data objects.		X
Get Challenge	Generate a random number with the given length.	X	

Note: OpenPGP services are not supported over NFC, these services must be performed over USB only.

Table 15 – FIDO2&U2F Unauthenticated Services

Service	Description
Get Information	This service is used to get a list of all supported protocol versions, supported extensions, PIN retry count, and the mode of operation.
Select Applet	This service is used to select FIDO2&U2F.
FIDO2 Reset	This service is used by the client to zeroize all plaintext CSPs, reset the module to a factory default state, invalidating all generated credentials and key handles, and regenerating the Managing Key.

Table 16 – PIV Unauthenticated Services

Service	Description
Verify PIN	This service is used to verify the PIN.
Read Data Object	This service is used to read data.
Select Applet	This service is used to select PIV.
Reset	This service is used to reset the applet back to manufacturer default settings and invalidates all generated keys. Note: This command is also considered as the Zeroization service.
GeneralAuth (management auth)	This service is used to authenticate the applet with PIV Symmetric Key.
Attest	This service is used to attest and sign a generated key.

Note: PIV services are not supported over NFC, these services must be performed over USB only.

Table 17 – HOTP Unauthenticated Services

Service	Description
Select Applet	Selects HOTP for usage and returns version, ID and a challenge if the Module is in Approved mode.
Validate	Verify HOTP OATH Auth key.
Reset	Reset the applet to manufactory default settings. Note: This command is also considered as the Zeroization service.
Get FIPS mode state	This service is used to get the applet FIPS mode state.

Table 18 – TOTP Unauthenticated Services

Service	Description
Select Applet	Selects TOTP for usage and returns version, ID and a challenge if the Module is in Approved mode.
Validate	Verify TOTP OATH Auth key.

Service	Description
Reset	Reset the applet to manufactory default settings. Note: This command is also considered as the Zeroization service.
Get FIPS mode state	This service is used to get the applet FIPS mode state.

Table 19 – OpenPGP Unauthenticated Services

Service	Description
Select Applet	Select OpenPGP.
Verify PW1	Verify using user PW1.
Verify PW3	Verify using administrator PW3.
Read Unprotected Data Object	Read all unprotected data.
Terminate DF	Terminate OpenPGP and delete all stored data.
Activate File	Initialize to the manufactory default settings. Note: This command is also considered as the Zeroization service.

Note: OpenPGP services are not supported over NFC. These services must be performed over USB only.

Table 20 – Additional Unauthenticated Services

Service	Description
SELF-TEST (RESET)	After the module is reset, the power up self-tests are performed.
Get FW Version	Retrieves the firmware version. Bytes 08 and 09 bytes indicate the major version, while bytes 10 and 11 indicate the minor version. Example: “00 07 00 04” equates to “7.04”.
Show Status	Status information provided by return codes and optionally through the attached LED

The following defines the relationship between access to Security Parameters and the different module services. The modes of access shown in the table are defined as:

- G = Generate: The service generates the CSP.
- O = Output: The service outputs the CSP.
- E = Execute: The service uses the CSP in an algorithm.
- I = Input: The service inputs the CSP.
- Z = Zeroize: The service zeroizes the CSP.

Table 21 – FIDO2&U2F Security Parameters Access by Service

Service	CSPs and Public Keys								
	DRBG EI	DRBG-state	FIDO2 Device ECDSA Certificate	FIDO2 Device ECDSA Private Key	FIOD2 User ECDSA Private Key	Init Keyenc	Init Keymac	Managing Key	Agreement ECC Private Key
Select Applet									
Get Information									
FIDO2 Make Credential	G, E	G, E	O	E	G, O	E	E		
FIDO2 GetAssertion	G, E	G, E			E	E	E		
FIDO2 GetNext Assertion	G, E	G, E			E				
FIDO2 Reset	G, E	G, E	Z, G	Z, G	Z	Z, G	Z, G	Z, G	Z, G
FIDO2 Credential Management									
FIDO2 Authenticator ClientPIN	G, E	G, E							G, E
Authenticator AdminPIN	G, E	G, E							G, E
Switch mode	G, E	G, E	Z, G	Z, G	Z	Z, G	Z, G	Z, G	Z, G

Table 22 – FIDO2&U2F Security Parameters Access by Service Continued

Service		CSPs and Public Keys								
	SharedSecret Key	User pinToken	CO pinToken	PIN	CO PIN	hmacsaltkey	FIDO2 Device ECDSA Public Key	Agreement ECC Public Key	Client ECC Public Key	FIDO2 User ECDSA Public Key
Select Applet										
Get Information										
FIDO2 Make Credential	E	I, E		E			O			G, O
FIDO2 GetAssertion	E	I, E		E		G, E			I, E	
FIDO2 GetNext Assertion										
FIDO2 Reset	Z	Z	Z	Z	Z	Z	Z	Z, G	Z	Z
FIDO2 Credential Management		E		E						
FIDO2 Authenticator ClientPIN	G, E	G, O		E				G, O	I, E	
Authenticator AdminPIN	G, E		G, O		E			G, O	I, E	
Switch mode	Z	Z	I, E	Z	E	Z	Z	Z, G	Z	Z

Table 23 – PIV Security Parameters Access by Service

Service	CSPs and Public Keys							
	DRBG EI	DRBG-State	PIV Symmetric Key	PIV Asymmetric Private Key	PIV Attestation Private Key	PIV User PIN	PIV PUK PIN	PIV Asymmetric Public Key
Select Applet								
Verify PIN						I, E		
General Auth (management auth)		E, G	E					
General Auth (RSA/ECDSA)		E, G		E				
Read Data Object								O
Reset	Z	Z	Z	Z		Z	Z	Z
Attest					E			
Set Management Key			I, E, G					G, O
Change PUK							I, E, G	
Change PIN						I E, G		
Unblock PIN (reset retry counter)						G	I, E	
Set PIN Retries						G	G	
Generate Asymmetric Key	E, G			G				G, O
Put Data								
Import Key				I, G	I, G, Z			

Table 24 – HOTP CSP Access by Service

Service	CSPs and Public Keys			
	DRBG EI	DRBG-State	HOTP OATH Auth Key	HOTP OATH Seed Key
Select Applet		G, E	E	
List				
Put				I, G
Calculate Default				E
Calculate				E
Reset	Z	Z	Z	Z
Get Default				
Set Default				
Delete				Z
Set Code			I, E, G	
Validate			E	
Switch mode	Z	Z	Z	Z
Get FIPS mode				

Table 25 – TOTP CSP Access by Service

Service	CSPs and Public Keys			
	DRBG EI	DRBG-State	TOTP OATH Auth Key	TOTP OATH Seed Key
Select Applet		G, E	E	
Set Code			I, E, G	
Validate				
Put				I, G
Delete			Z	Z
Reset	Z	Z	Z	Z
List				
Calculate				E
Calculate All				E
Calculate Default				E
List Detail Info				
Get Default				
Set Default				
Switch mode	Z	Z	Z	Z
Get FIPS mode				

Table 26 – OpenPGP CSP Access by Service

Service	CSPs and Public Keys									
	DRBG EI	DRBG-State	Symmetric Key	OpenPGP Admin PIN (PW3)	OpenPGP Signature Private Key	OpenPGP Authentication Private Key	OpenPGP User PIN (PW1)	OpenPGP Signature Public Key	OpenPGP Authentication Public Key	Resetting Code
Select Applet										
Verify PW1							I, E			
Verify PW3				I, E						
Change PW1							I, E, G			
Change PW3				I, E, G						
Reset Retry Counter				I, E			G			I, E
Set Pin Retries				I, E, Z			Z			Z
Generate Asymmetric Key Pair		E, G		I, E	G	G		G, O	G, O	
Perform Security Operation					E					
Internal Authenticate						E	I, E			
Get Challenge		E, G	E							
Read Unprotected Data Object										
Read Protected Data For User							I, E			
Read Protected Data For Admin				I, E						

Service	CSPs and Public Keys									
	DRBG EI	DRBG-State	Symmetric Key	OpenPGP Admin PIN (PW3)	OpenPGP Signature Private Key	OpenPGP Authentication Private Key	OpenPGP User PIN (PW1)	OpenPGP Signature Public Key	OpenPGP Authentication Public Key	Resetting Code
Put Data			I	I, E			I, E			I
Write User Protected Data										
Import Key				I, E	I	I		I	I	
Terminate DF			Z							
Activate File	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z

4 Self-Tests

The module performs self-tests to ensure the proper operation of the module. Per FIPS 140-2 these are categorized as either power-up self-tests or conditional self-tests. Power up self–tests are available on demand by power cycling the module.

If one of the KATs fails, the Module is reset.

The Module performs the following algorithm KATs on power-up.

Table 27 – Power Up Self-tests

Test Target	Description
Firmware Integrity	CRC-16 over all firmware
AES	KATS: Encryption, Decryption Modes: ECB, CBC Key Size: 256-bits
CMAC	Algorithm: AES Key Size: 256-bits
DRBG	KATs: CTR_DRBG SP800-90A Section 11.3 Health Tests (covers AES Encrypt KAT) Security Strengths: 128-bits
ECDSA	PCT: Signature Generation, Signature Verification Curves/Key sizes: P-256
HMAC	KATs: Generation SHA sizes: SHA-1, SHA-256
KAS-SSC	KATs: Primitive “Z” Computation KAT per IG 9.6 Curves/Key sizes: P-256
KDA	KATs: SP800-56C HKDF
RSA-2048	KATs: PKCS#1 v1.5 Signature Generation, Signature Verification. Per IG D.9, this also satisfies the self-test requirements for RSA Decryption Primitive Key size: 2048-bits
SHA-1, SHA-256, and SHA-512	KATs: Generation

Table 28 – Conditional Self-tests

Test Target	Description
DRBG	DRBG Continuous Test performed when a random value is requested from the DRBG SP800-90A Health Tests
ECDSA	ECDSA Pairwise Consistency Test performed on every ECDSA key pair generation using sign/verify
ECDH	SP800-56A-rev3 Pairwise Consistency Tests
ENT	SP800-90A APT and RCT
RSA	RSA Pairwise Consistency Test performed on every RSA key pair generation using sign/verify

5 Physical Security Policy

The Module is opaque and meets Level 3 for tamper resistance and evidence. The Module is encased in a removal-resistant IC packaging material. The physical security mechanism is a hard, opaque tamper-evident coating. The Module should be inspected for tamper before each use. Tamper will be indicated by scratches or other damage to the coating.

6 Operational Environment

The Module is designated as a non-modifiable operational environment under the FIPS 140-2 definitions. The Module does not support firmware updates.

7 Mitigation of Other Attacks Policy

Hypersecu HYP2003 MFA Cryptographic Module is not designed to mitigate any specific attacks outside of those required by FIPS 140-2.

8 Security Rules and Guidance

This section documents the security rules for the secure operation of the cryptographic module to implement the security requirements of FIPS 140-2.

1. The Module provides two distinct operator roles: User and Cryptographic Officer.
2. The Module provides role-based authentication.
3. The Module clears previous authentication on power cycle.
4. An operator does not have access to any cryptographic services prior to assuming an authorized role.
5. The Module allows the operator to initiate power-up self-tests by power cycling power or resetting the Module.
6. Power up self-tests do not require any operator action.

7. Data outputs are 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. There are no restrictions on which keys or CSPs are zeroized by the zeroization service.
10. The Module does not support concurrent operators.
11. The Module does not support a maintenance interface or role.
12. The Module does not support manual key entry.
13. The Module does not have any proprietary external input/output devices used for entry/output of data.
14. The Module does not output intermediate key values.
15. The following procedural controls apply in order to operate in the Approved mode of operation:
    a. FIDO2&U2F:
        i. Operator shall set a PIN.
        ii. Operator shall ensure Credential Protection Level is set to 2.
    b. HOTP and TOTP:
        i. Operator shall set a Manager Key through the “Set Code” service.
        ii. Operator shall not perform “Set Code” or “Put” services over NFC.
    c. PIV and OpenPGP:
        i. PIV and OpenPGP services are not supported over NFC. These services are only available over the USB interface.
        ii. The OpenPGP service, “Perform Security Operation” must not be used to perform PKCS#1 RSA Encrypt or Decrypt.

9 References and Definitions

The following standards are referred to in this Security Policy.

Table 29 – References

Abbreviation	Full Specification Name
[FIPS140-2]	*Security Requirements for Cryptographic Modules*, May 25, 2001
[IG]	*Implementation Guidance for FIPS PUB 140-2 and the Cryptographic Module Validation Program, February 14, 2022*
[108]	*NIST Special Publication 800-108, Recommendation for Key Derivation Using Pseudorandom Functions (Revised), October 2009*
[131Ar2]	*Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths, March 2019*
[132]	*NIST Special Publication 800-132, Recommendation for Password-Based Key Derivation, Part 1: Storage Applications, December 2010*
[133r2]	*NIST Special Publication 800-133, Recommendation for Cryptographic Key Generation, June 2020*
[135]	*National Institute of Standards and Technology, Recommendation for Existing Application-Specific Key Derivation Functions, Special Publication 800-135rev1, December 2011.*
[186]	*National Institute of Standards and Technology, Digital Signature Standard (DSS), Federal Information Processing Standards Publication 186-4, July, 2013.*
[186-2]	*National Institute of Standards and Technology, Digital Signature Standard (DSS), Federal Information Processing Standards Publication 186-2, January 2000.*
[197]	*National Institute of Standards and Technology, Advanced Encryption Standard (AES), Federal Information Processing Standards Publication 197, November 26, 2001*
[198]	*National Institute of Standards and Technology, The Keyed-Hash Message Authentication Code (HMAC), Federal Information Processing Standards Publication 198-1, July, 2008*
[180]	*National Institute of Standards and Technology, Secure Hash Standard, Federal Information Processing Standards Publication 180-4, August, 2015*
[202]	*FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION, SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions, FIPS PUB 202, August 2015*
[38A]	*National Institute of Standards and Technology, Recommendation for Block Cipher Modes of Operation, Methods and Techniques, Special Publication 800-38A, December 2001*
[38B]	*National Institute of Standards and Technology, Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication, Special Publication 800-38B, May 2005*
[38C]	*National Institute of Standards and Technology, Recommendation for Block Cipher Modes of Operation: The CCM Mode for Authentication and Confidentiality, Special Publication 800-38C, May 2004*

Abbreviation	Full Specification Name
[38D]	*National Institute of Standards and Technology, Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC, Special Publication 800-38D, November 2007*
[38E]	*National Institute of Standards and Technology, Recommendation for Block Cipher Modes of Operation: The XTS-AES Mode for Confidentiality on Storage Devices, Special Publication 800-38E, January 2010*
[38F]	*National Institute of Standards and Technology, Recommendation for Block Cipher Modes of Operation: Methods for Key Wrapping, Special Publication 800-38F, December 2012*
[56A]	*NIST Special Publication 800-56A, Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography (Revised), March 2007*
[56Ar2]	*NIST Special Publication 800-56A Revision 2, Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography, May 2013*
[56Ar3]	*NIST Special Publication 800-56A Revision 3, Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography. April 2018*
[56Br1]	*NIST Special Publication 800-56A Revision 1, Recommendation for Pair-Wise Key Establishment Schemes Using Integer Factorization Cryptography, September 2014*
[90A]	*National Institute of Standards and Technology, Recommendation for Random Number Generation Using Deterministic Random Bit Generators, Special Publication 800-90A, June 2015.*
[90B]	*National Institute of Standards and Technology, Recommendation for the Entropy Sources Used for Random Bit Generation, Special Publication 800-90B, January 2018.*

Table 30 – Acronyms and Definitions

Acronym	Definition
CRC	Cyclic Redundancy Check
CTR	Counter
DRBG	Deterministic Random Bit Generator
ECB	Electronic Code Book
CBC	Cipher Block Chaining
FIPS	Federal Information processing Standard
VCC	Voltage (at the) Common Collector
PW1	User PIN
PW3	Administrator PIN
CO	Crypto Officer
PUK	PIN Unblocking Key