FEITIAN Technologies Co., LTD

FEITIAN Biometric FIDO Key Module

Non-Proprietary FIPS 140-2 Security Policy

Document Version: V1.0

Date: April 27, 2021

Table of Contents

List of Tables

1 Introduction

This document defines the Security Policy for the FEITIAN Biometric FIDO Key Module, hereafter denoted the Module. The FEITIAN Biometric FIDO Key Module is built on FIDO2 and U2F specifications which are issued and promoted by the FIDO Alliance to drive and enable a real password-less multi-factor authentication. The module does not implement any of the biometric features or store any biometric data, but instead communicates with an external fingerprint module within the FEITIAN Biometric FIDO Key fob. For enterprises who use passwords today and have a shared PC environment, security keys for Windows Hello provide a more seamless way for employees to authenticate without entering a username or password. Unlike passwords, using a security hardware device equipped with FEITIAN Biometric FIDO Key Module will provide lower IT management costs, improved productivity, enhanced security, and privacy for both employees and employers.

Table 1 – Cryptographic Module Configurations

	Module	HW P/N and Version	FW Version
1	FEITIAN Biometric FIDO Key Module	Z32HUB	1.0.03

The Module is intended for use by US Federal agencies or other markets that require FIPS 140-2 validated FIDO Authenticator.

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	2
Operational Environment	N/A
Cryptographic Key Management	2
EMI/EMC	3
Self-Tests	2
Design Assurance	2
Mitigation of Other Attacks	N/A
Overall	2

1.1 Module Description and Cryptographic Boundary

The Module is a single-chip embodiment. The cryptographic boundary is defined as the outer perimeter of the IC as shown in Figure 1.

The physical form of the module is depicted in Figure 1. The FEITIAN Biometric FIDO Key Module is a hardware type module with a single-chip embodiment that meets overall level 2 FIPS 140-2 requirements. The module consists of two major components, a 32-bit Integrated Circuit (IC) and a COS. The cryptographic boundary of FEITIAN Biometric FIDO Key Module is the outer IC packaging, which encompasses all module components.

The physical ports provided by the module are shown on the right in Figure 1.

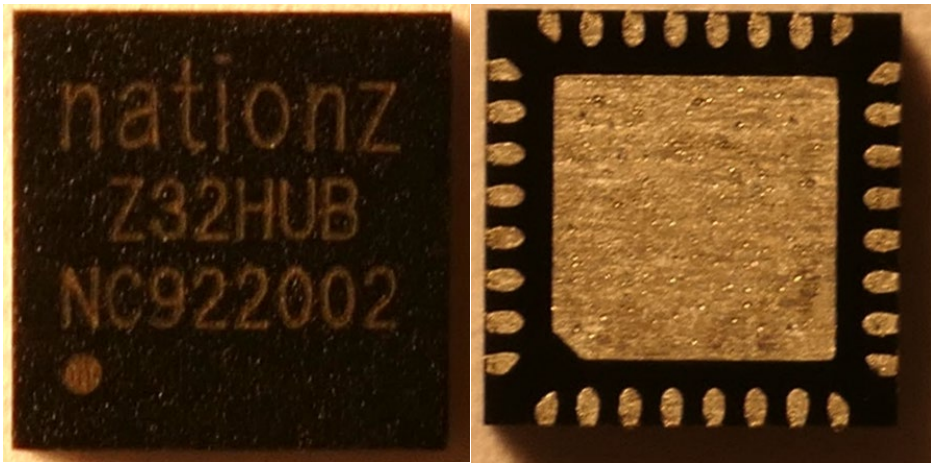

Figure 1 – FEITIAN Biometric FIDO Key Module (Top and Bottom)

It should be noted that although the module provides 32 physical pins, only 8 pins are enabled. The module's pins are described in Table 3.

Table 3 – Ports and Interfaces

Port/Pin	Description	Logical Interface Type
VDD33	Provides power to the module	Power in
USBDP – USB D+ USBDM – USB D-	Data transfer through USB	Data in Data out Control in Status out
USB_VDD33	Provides power to the module	Power in
GPIO8	RX, Serial port input, get data from fingerprint module (Biometric functionality not available in Approved mode)	Data in Control in
GPIO9	TX, Serial port output, send data to fingerprint module (Biometric functionality not available in Approved mode)	Data out Status out
GPIO1	Output to external red LED (Only used with biometric functionality, not available in Approved mode)	Status out
GPIO2	Output to external green LED	Status out

1.2 Mode of Operation

The Module supports an Approved and a non-Approved mode of operation. The module can switch between Approved mode and non-Approved mode by the “Switch mode” service, which zeroizes all plaintext CSPs. In order to confirm the Approved mode of operation has been selected, the operator may invoke the “Get Device Information” service; the third byte of the return value specifies the mode of operation (0x01 for Approved and 0x00 for non-Approved). The operator must also update the CO PIN from its default value.

1.2.1 Non-Approved Mode

When configured for the non-Approved mode, no CO PIN or pinToken are supported and non-Approved security functions are available (Table 6). All biometric services (enrollment, remove enrollment, enum enrollment, etc.) are only available in the non-Approved mode, as well. Please see Section 3.3 for a full list of services available in the non-Approved mode.

2 Cryptographic Functionality

The Module implements the FIPS Approved and Non-Approved but Allowed cryptographic functions listed in the tables below. Non-Approved cryptographic functions only available in the non-Approved mode of operation are specified in Table 6.

Table 4 – Approved Algorithms

Cert	Algorithm	Mode	Description	Functions/Caveats
C1901	AES [197]	ECB [38A]	Key Sizes: 128, 256	Encrypt, Decrypt
		CMAC [38B]	Key Sizes: 128, 256 Tag Len: 64, 128	Message Authentication
VA	CKG [133]		[133] Section 6.1: Direct symmetric key generation using unmodified DRBG output	Key Generation
C1901	DRBG [90A]	CTR	Use_df AES-128	Deterministic Random Bit Generation Security Strength = 112 bits. Key strength is modified by available entropy.
C1901	ECDSA [186]	P-256		KeyGen
		P-256 SHA-256		SigGen
C1901	HMAC [198]	SHA-256	Key Size: 128, 256	Message Authentication; KDF Primitive
VA	KAS-SSC [56Ar3]	ECDH using P-256 only	Ephemeral Unified	Key Establishment; Key Agreement

Cert	Algorithm	Mode	Description	Functions/Caveats
VA	KDA [56Cr1]	SHA-256	One-Step	Key Derivation Function
C1901	KTS [IG D.9]	AES and CMAC	AES-ECB w/ 128 or 256-bit keys with CMAC using 128 or 256-bit keys	Key Transport (AES Cert.#C1901 and AES Cert. #C1901; key establishment methodology provides 128 or 256 bits of security strength)
C1901	KTS [IG D.9]	AES and HMAC	AES-ECB w/ 128-bit keys with HMAC SHA-256 using 128 or 256-bit keys	Key Transport (AES Cert.#C1901 and HMAC Cert. #C1901; key establishment methodology provides 128 bits of security strength)
C1901	SHS [180]	SHA-256		Message Digest Generation, Password Obfuscation

Table 5 – Non-Approved but Allowed Cryptographic Functions

Algorithm	Description
NDRNG	[Annex C] Non-Deterministic RNG; minimum of 8 bits per access. The NDRNG output is used to seed the FIPS Approved DRBG to a security strength of 112-bits.

Table 6 – Non-Approved Cryptographic Functions available in Non-Approved Mode only

Algorithm	Description
AES	CBC mode (non-compliant)
ECDH	Non-SP800-56a-rev3 conformant ECDH
KDF	Non-compliant SHA-256 based KDF
Triple-DES	Triple-DES (non-compliant)

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 3.3.

Table 7 – Critical Security Parameters (CSPs)

CSP	Usage	Storage	Generation	Input	Output	Zeroization
DRBG EI	128-bit entropy and 64bit nonce input collected from the NDRNG, used to derive the DRBG seed	RAM plaintext	Internally generated using the NDRNG	No	No	Overwritten with new values after power cycle
DRBG V Value	Internal CTR_DRBG state value is used for SP 800-90A CTR_DRBG (consists of 128 bits)	RAM plaintext	Internally generated using the NDRNG	No	No	Overwritten with new values after power cycle
DRBG Key Value	Internal CTR_DRBG state value is used for SP 800-90A CTR_DRBG (Consists of 128 bits)	RAM plaintext	Internally generated using the NDRNG	No	No	Overwritten with new values after power cycle

CSP	Usage	Storage	Generation	Input	Output	Zeroization
Agreement ECC private key	ECDH P-256 private key, used for ECDH Key agreement with client to get sharedSecret	RAM plaintext	Internally, using the DRBG during power on, ReFactory, AuthenticatorClientPIN, AuthenticatorAdminPIN, or Switch Mode service	No	No	Overwritten with new values after power cycle
U2F Device ECDSA private key	ECDSA P-256 private key. Used for signature in U2F registration	Flash ciphertext, encrypted by Managing Key	Installed during production	No	No	N/A - Encrypted by Managing Key
FIDO2 device ECDSA private key	ECDSA P-256 private key. Used for signature in FIDO2 registration	Flash ciphertext, encrypted by managing key	Installed during production	No	No	N/A - Encrypted by Managing Key
User ECDSA private key	ECDSA P-256 private key. Used for signature in U2F and FIDO2 authentication	Flash ciphertext, encrypted by managing key	Internally using the DRBG and ECDSA Key Generation algorithm during U2F_Registration or FIDO2_ MakeCredential service	Encrypted by Init_Keyenc & Init_keymac	Encrypted by Init_Keyenc & Init_keymac	Zeroized by Switch Mode and ReFactory services

CSP	Usage	Storage	Generation	Input	Output	Zeroization
Managing Key	128-bit AES-ECB key, used to encrypt CSPs and keys	Flash plaintext	Generated during production using the DRBG, Switch Mode, or ReFactory service	No	No	Overwritten in Switch Mode and ReFactory services
Init_Keyenc	128-bit AES-ECB key, used for encrypting the User ECDSA Private key info generated and returned to server by U2F and FIDO2	Flash ciphertext, encrypted by managing key	Internally, using the DRBG during production, Switch Mode, or ReFactory service	No	No	Overwritten in Switch Mode and ReFactory services
Init_keymac	AES128-CMAC (U2F) and SHA256-HMAC (FIDO2) calculation against User ECDSA Private key info returned by U2F and FIDO2	Flash ciphertext, encrypted by managing key	Internally, using the DRBG during production, Switch Mode, or ReFactory service	No	No	Overwritten in Switch Mode and ReFactory services
SharedSecret key	256-bit AES key, used for ECB mode encryption and CMAC calculation of pin related operations	RAM plaintext	N/A. Established via KAS-SSC and KDA	No	No	Zeroized after each use and by Switch Mode and ReFactory services

CSP	Usage	Storage	Generation	Input	Output	Zeroization
User pinToken	256-bit HMAC key for FIDO2 and U2F operations	RAM plaintext	Internally, using the DRBG by AuthenticatorClientPIN service	No	Encrypted and authenticated by SharedSecret key	Zeroized when power cycle and by Switch Mode and ReFactory services
CO pinToken	256-bit HMAC key for FIDO2 and U2F operations	RAM plaintext	Internally, using the DRBG in AuthenticatorAdminPIN command	No	Encrypted and authenticated by SharedSecret key	Zeroized when power cycle and by Switch Mode and ReFactory services
User PIN	Authenticate the User	Flash SHA-256 hash of PIN encrypted by Managing Key	No	Encrypted and authenticated by SharedSecret Key	No	Overwritten with new values after PIN update, zeroized by ReFactory and Switch Mode services
CO PIN	Authenticate the CO	Flash SHA-256 hash of PIN encrypted by Managing Key	No	Encrypted and authenticated by SharedSecret Key	No	Overwritten with new values after PIN update, set to factory default by ReFactory and Switch Mode services

2.2 Public Keys

Table 8 – Public Keys

Key	Usage	Storage	Generation	Input	Output
Agreement ECC public key	Agreement ECC P-256 public key returned to Client for key agreement	Plaintext in RAM	DRBG	No	Plaintext during KAS-SSC

Key	Usage	Storage	Generation	Input	Output
Client ECC public key	Client ECC P-256 public key for key agreement	Plaintext in RAM	No	Plaintext during KAS-SSC	No
U2F device ECC public key	ECC P-256; In U2F registration, the module returns it to the Client via attestation for verification of the signature returned during U2F registration	Plaintext in Flash	Installed during production	No	Plaintext
FIDO2 device ECC public key	ECC P-256; In FIDO2 registration, the module returns it to the Client via attestation for verification of the signature returned during FIDO2 registration	Plaintext in Flash	Installed during production	No	Plaintext
User ECDSA public Key	ECC P-256; Returned to Client in U2F and FIDO2 registration, for verifying signature returned in U2F and FIDO2 authentication	Plaintext in RAM	DRBG	No	Plaintext

3 Roles, Authentication and Services

3.1 Assumption of Roles

The module supports two distinct operator roles, User and Cryptographic Officer (CO). The CO is the role responsible for U2F and FIDO2 registration, resetting module and credential management. The user is allowed to perform cryptographic authentication operation with the U2F key handles and FIDO2 credentials.

Table 9 lists all operator roles supported by the module. The Module does not support a maintenance role and bypass capability. The Module does not support concurrent operators.

Table 9 – Roles Description

Role ID	Role Description	Authentication Type	Authentication Data
1	CO (Cryptographic-Officer)	Role-based	CO PIN
2	User	Role-based	User PIN

3.2 Authentication Methods

Please see Table 10 for details regarding the authentication mechanisms.

Table 10 – Authentication Mechanisms

Authentication Method	Probability	Justification
User PIN 6 - 63 bytes	The PIN is 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 1/2^48 which is less than 1/1,000,000.	The module is limited by the retry counter of 3 tries before it power cycles. After 8 total failed attempts, it will block further authentication attempts. Therefore, the probability of successfully authenticating to the module within one minute through random attempts is 8/2^48, which is less than 1/100,000.
Admin PIN 6 - 63 bytes	The PIN is 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 1/2^48 which is less than 1/1,000,000.	The module is limited by the retry counter of 3 tries before it power cycles. After 8 total failed attempts, it will block further authentication attempts. Therefore, the probability of successfully authenticating to the module within one minute through random attempts is 8/2^48, which is less than 1/100,000.

3.3 Services

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

Table 11 – Authenticated Services

Service	Description	CO	U
MakeCredential(0x01)	This service is used to generate a new credential in the module.	X	
GetAssertion(0x02)	This service is used to generate a cryptographic proof of user authentication.		X
GetNextAssertion(0x08)	The client calls this service when the GetAssertion response contains the numberOfCredentials and the number of credentials exceeds 1.		X
ReFactory(0x07)	This service is used by the client to zeroized all plaintext CSPs, reset the module back to a factory default state, invalidating all generated credentials and key handles, and regenerating the Managing Key.	X	

Service	Description	CO	U
AuthenticatorClientPIN(0x06)	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
AuthenticatorAdminPIN(0x46)	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	
CredentialManagement(0x41)	This service is used by the platform to manage resident credentials on the module.	X	
U2F_Registration(0x01)	This service is used to generate a new key handle from the module. (AES ECB encrypt with Init_Kenc and AES CMAC with Init_Kmac of User ECDSA Private Key).	X	
U2F_Authentication(0x02)	This service is used to verify a cryptographic proof by the key handle of user authentication (signing with User ECDSA Private Key.		X
Switch mode(0x47)	This service is used to switch between Approved and non-Approved mode and zeroizes all plaintext CSPs	X	

Table 12 – Unauthenticated Services

Service	Description
GetInfo(0x04)	Using this service, the host can request that the module report a list of all supported protocol versions, supported extensions, AAGUID of the device, and capabilities.
U2F_GetVersion(0x03)	This service is used to get the U2F version.
Get Challenge(0xF2)	This service is used to get a challenge.
Get Device Information(0xE3)	This service is used to get device information.
Self-Tests	Self-tests may be invoked by power cycling the module.
Show Status	Provided by return codes for each service, as well as the external LED

FIDO2 proprietary services are: MakeCredential(0x01), GetAssertion(0x02), GetnextAssertion(0x08), GetInfo(0x04), Refactory(0x07), AuthenticatorClientPIN(0x06), CredentialManagement(0x41).

U2F proprietary services are: U2F_Registration(0x01), U2F_Authentication(0x02), U2F_GetVersion(0x03). The above services are provided in both the FIPS Approved mode and non-Approved mode; in non-Approved mode, the services are available with non-Approved security functions. In addition, the non-

Approved mode supports biometric services (enrollment, remove enrollment, enum enrollment) and does not support a CO PIN or pinToken.

The FIDO2 instruction format uses the CBOR encoding method, and the other instructions use the APDU encoding format.

The command and response formats are as follows.

Table 13 – FIDO2 Command Format

Offset	Field	Size	Description
0	CMD	1	Command byte
1-N	DATA	N	Command data in CBOR encoding format

Table 14 – FIDO2 Response Format

Offset	Field	Size	Description
0	STATUS	1	Response byte
1-N	DATA	N	Response data in CBOR encoding format

Table 15 – APDU Command Format

Header					Lc Field	Data Field	Le Field
CLA	INS	P1	P2	(P3)	1 or 2 bytes	Input Data	1 or 2 bytes

APDU command structure descriptions:

CLA – The Class byte indicates the class of the command.

INS – The Instruction byte indicates the command to process.

P1\P2 –The command parameters.

P3 –When the length of Lc or Le is two bytes, P3 exist and a value of '0'.

Lc – Length in bytes of the data field

Data Field – Data input with command for processing

Le – Maximum number of bytes expected in the response

Table 16 – APDU Response Format

Data Field	Trailer
Response data	Status word

Table 17 defines the relationship between access to Security Parameters and the different module services. The ReFactory service is used to clear and invalidate all keys. 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 17 – Security Parameters Access by Service

Service	CSPs and Public Keys																			
	DRBG EI	DRBG V Value	DRBG Key Value	Agreement ECC private key	U2F device ECDSA private key	FIDO2 device ECDSA private key	User ECDSA private key	Managing Key	Init_Keyenc	Init_keymac	sharedSecret	User pinToken	CO pinToken	User PIN	CO PIN	Agreement ECC public key	Client ECC public key	U2F device ECC public key	FIDO2 device ECC public key	User ECDSA public key
MakeCredential(0x01)	G/E	G/E	G/E	-	-	E	G/O	E	E	E	-	-	E	-	-	-	-	-	O	G/O
GetAssertion(0x02)	G/E	G/E	G/E	-	-	-	I/E	E	E	E	-	E	-	-	-	-	-	-	-	-
GetNextAssertion(0x08)	G/E	G/E	G/E	-	-	-	E	E	-	-	-	-	-	-	-	-	-	-	-	-
ReFactory(0x07)	G/E	G/E	G/E	G	-	-	Z	GZ	GZ	GZ	Z	Z	Z	Z	Z	G	-	-	-	-
AuthenticatorClientPIN(0x06)	G/E	G/E	G/E	G/E	-	-	-	E	-	-	G/E	G/O	-	I/E	-	O/G	I	-	-	-
AuthenticatorAdminPIN(0x46)	G/E	G/E	G/E	G/E	-	-	-	E	-	-	G/E	-	G/O	-	I/E	O/G	I	-	-	-
CredentialManagement(0x41)	-	-	-	-	-	-	E	E	-	-	-	-	E	-	-	-	-	-	-	G/O
U2F_Registration(0x01)	G/E	G/E	G/E	-	E	-	G/O	E	E	E	-	-	-	-	-	-	-	O	-	G/O
U2F_Authentication(0x02)	-	-	-	-	-	-	I/E	E	E	E	-	-	-	-	-	-	-	-	-	-
Switch Mode(0x47)	G/E	G/E	G/E	G	-	-	Z	GZ	GZ	GZ	Z	Z	Z	Z	Z	G	-	-	-	-
GetInfo(0x04)	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
U2F_GetVersion(0x03)	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Get Challenge(0xF2)	G/E	G/E	G/E	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Get Device Information(0xE3)	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Self-Tests	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Show Status	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-

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-on self-tests or conditional self-tests. Power-on self–tests are available on demand by power cycling the module.

Power-on self-tests must be completed successfully prior to any other use of cryptography by the Module. If one test fails, the Module enters the error state.

When receiving an instruction, the module first checks whether it is currently in an error state. If it is in an error state, it directly returns an error code (6F00), otherwise it processes the instruction. The module must be power cycled to exit the error state.

The module performs the following algorithm self-tests at power-on.

- Firmware Integrity: 16-bit CRC
- AES-ECB 128 and 256-bit Encrypt/Decrypt KAT
- AES-CMAC 128 and 256-bit KAT
- CTR_DRBG KAT
- HMAC SHA-256 KAT
- SHA-256 KAT
- KAS-SSC KAT
- KDA KAT
- ECDSA Signature Generation/Verification PCT

The module performs the following conditional self-tests as indicated.

- NDRNG Continuous Random Number Generator Test
- DRBG Continuous Random Number Generator Test
- SP800-90A DRBG Health Tests
- ECDSA Pairwise consistency test on ECDSA key pair generation
- EC-DH Pairwise consistency test on EC-DH key pair generation

5 Physical Security Policy

The Module is opaque and meets Level 2 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 operational environment requirements do not apply to FEITIAN Biometric FIDO Key Module as it only supports a non-modifiable operational environment.

7 Mitigation of Other Attacks Policy

FEITIAN Biometric FIDO Key Module is not designed to mitigate any specific attacks outside of those required by FIPS 140-2, including but not limited to power consumption, timing, fault induction, or TEMPEST attacks.

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 allows the operator to initiate power-up self-tests by power cycling the module.
4. Power up self-tests do not require any operator action.
5. Data output are inhibited during key generation, self-tests, zeroization, and error states.
6. Status information does not contain CSPs or sensitive data that if misused could lead to a compromise of the module.
7. There are no restrictions on which plaintext keys or CSPs are zeroized by the zeroization service.
8. The module does not support concurrent operators.
9. The module does not support a maintenance interface or role.
10. The module does not support manual key entry.
11. The module does not have any proprietary external input/output devices used for entry/output of data.
12. The module does not enter or output plaintext CSPs.
13. The module does not output intermediate key values.
14. The module must be configured to operate in the Approved mode of operation. By default, the module is configured in the Approved mode. If it is not, then the Switch Mode service may be used to invoke the Approved mode of operation.

9 References and Definitions

The following standards are referred to in this Security Policy.

Table 18 – 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, 28 August 2020*
[133]	*NIST Special Publication 800-133, Recommendation for Cryptographic Key Generation, Revision 2 June 2020*
[186]	*National Institute of Standards and Technology, Digital Signature Standard (DSS), Federal Information Processing Standards Publication 186-4, July, 2013.*
[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*
[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*
[38F]	*National Institute of Standards and Technology, Recommendation for Block Cipher Modes of Operation: Methods for Key Wrapping, Special Publication 800-38F, December 2012*
[56Ar3]	*NIST Special Publication 800-56A Revision 3, Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography, April 2018*
[56Cr1]	*NIST Special Publication 800-56C Revision 1, Recommendation for Key-Derivation Methods in Key-Establishment Schemes, April 2018*
[90A]	*National Institute of Standards and Technology, Recommendation for Random Number Generation Using Deterministic Random Bit Generators, Special Publication 800-90A, June 2015.*

Table 19 – Acronyms and Definitions

Acronym	Definition
AAGUID	Authenticator Attestation Globally Unique Identifier
APDU	Application Protocol Data Unit
CBOR	Concise Binary Object Representation
CBC	Cipher Block Chaining
COS	Chip Operating System
CPU	Core Processing Unit
CRC	Cyclic Redundancy Check
DRBG	Deterministic Random Bit Generator
ECB	Electronic Codebook
FIDO	Fast IDentity Online
FIPS	Federal Information processing Standard
U2F	Universal Second Factor