Tendyron
天地融科技

FIPS 140-2 Level 3 Validation

Security Policy

OnKey193 USB Token

Tendyron Corporation

May 29, 2014

Contents

1 Introduction

This document describes the cryptographic module security policy for the OnKey193 USB Token. It contains specification of the security rules, under which the cryptographic module operates, including the security rules derived from the requirements of the FIPS 140-2 standard. This document is non-proprietary.

The OnKey193 cryptographic module is a USB 1.1/2.0 compliant token which is a multi-chip standalone module. The chip platform operating system is based on OnCOS that manages all the low level resources, cryptographic algorithms implementation, object access control and applications life cycle.

The hardware version tested for this module is version 122.V102. The software version tested for this module is DBFips-V0.1.12-120313-C000.

2 Glossary

Application Initiation	Operation initiated by CO to reset the module to a known specific state, in which the RAT of User Pin is set to MAT, and User PIN is set to the newly supplied one, and User's security related objects such as private file and RSA key pairs is cleared or deleted.
Authentication Object	CSPs such as PIN or Authentication Key used to validate the identity of a specific role.
Auth Key	Symmetric Key used to authenticate the identity of a specific role.
CM	Cryptographic Module.
CO	Crypto-officer whose main responsibility is to reset the RAT of User PIN, if blocked after too much attempt with wrong PIN, change User PIN to the newly supplied one, and clear the content of user's private file and delete RSA key pairs.
MAC	Message authentication code..
MAT	Max Attempt Times of a specific Authentication Object such as PIN or Authentication Key.
OTP	One Time Programmable
PIN	Personal Identification Number**.**
PKCS	Public Key Cryptography Standard
RAT	Remained Attempt Times of a specific Authentication Object such as PIN or Authentication Key.
RNG	Random Number Generator
Terminal	The device used in conjunction with the CM at the point of transaction
User	Person who legitimately possesses the cryptographic module.

3 Security Levels

The OnKey193 meets all requirements for FIPS 140-2 level 3*. Refer to the following table for individual security requirements:

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

*The FIPS mode will be indicated on user’s PC screen by the Client software through reading the product version info stored in the module.

4 SPECIFICATION

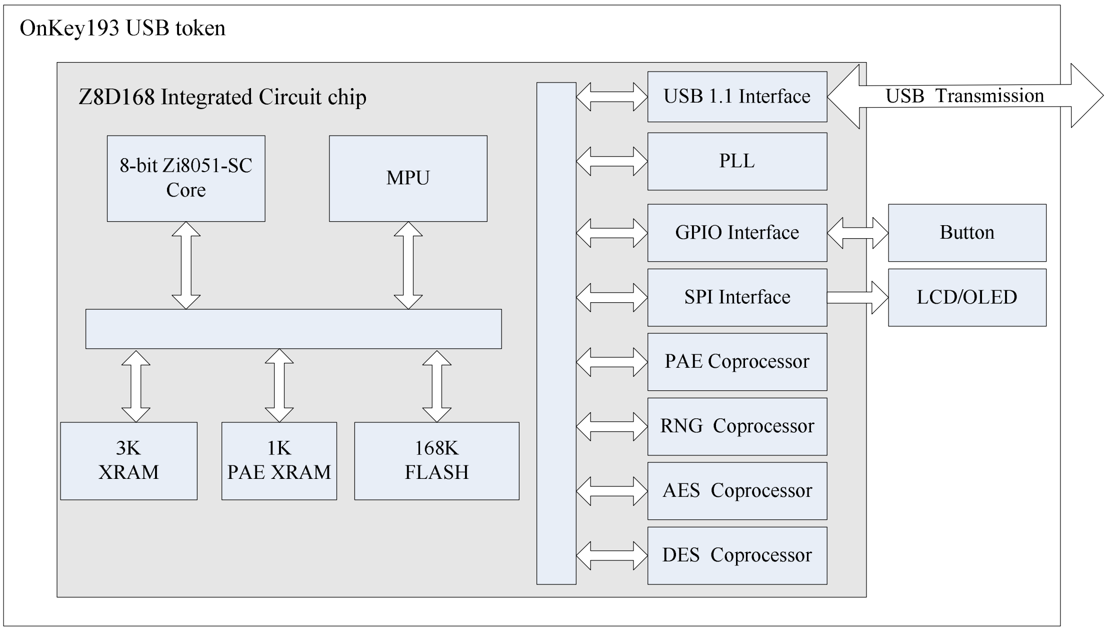
4.1 Cryptographic Boundary

The cryptographic boundary for the OnKey193 Token is the physical boundary of the token itself. The boundary includes the hard plastic enclosure and all components contained within the enclosure. The token provides utility basing on a chip of high security as a standalone cryptographic module component and enhances the tamper evidence of the cryptographic module.

The chip contains the following hardware components:

- Zi8051-Secure Core
- Triple DES cryptographic accelerator
- AES cryptographic accelerator
- Public Arithmetic Engine(support RSA)
- 168K Byte + 512 Byte Flash（Code Flash/ Data Flash + OTP Block）.
- 256 bytes internal RAM for register and data.
- 3K bytes external RAM for data and code.
- 1K bytes external PAE (Public Arithmetic Engine) RAM for data and code.
- Hardware RNG.

Block diagram：



4.2 Hardware Communication Interface

- UART controller
- SPI controller
- GPIO
- Full-speed USB 1.1 interface.
- ISO7816 master and slave controller

4.3 Physical Interfaces

The OnKey193 Token module supports four pins that lead to the PCB board.

• VSS — Ground (reference voltage).
• VDD — Power supply voltage input.
• DP — USB D+ connection.
• DM — USB D- connection.

The above four electronic signals are in full compliance with the USB interface specification..

The OnKey193 Token module supply voltage is 4.5V~5.5V.
The OnKey193 Token module supply current is less than 100mA.

The OnKey193 Token module supports seven pins for LCD/OLED screen function.

•LCD1 — Power supply voltage input
•LCD2 — SDA，SPI MOSI Pin

- LCD3 — SCK，SPI SCK Pin
- LCD4 — A0，Data/Command Control Pin
- LCD5 — RST，LCD Hardware Reset Pin
- LCD6 — CS，LCD Chip Select Pin
- LCD7 — Ground (reference voltage)

The LCD supply voltage is 2.7V~3.6V.
The LCD supply current:
Maximum value: 5mA at 3.3V
Typical value: 1mA at 3.3V

The OnKey193 Token module supports four pins for button function

- KEY1 — the "OK" button
- KEY2 — the "C" button
- KEY3 — the "Down" button
- KEY4 — the "Up" button

4.4 Logical Interfaces

The operation system on OnKey193 Token is a file system based operating system that controls the logical interface thru a well-defined set of Application Protocol Data Unit (APDU) commands. Communications between the host applications and the device is accomplished using a BOT driver that converts back and forth between USB and 7816-4 command APDUs. It manages the secure object storage system, interface protocol and parameters, interprets and executes external commands.
The details of these commands are defined in [OCS] and ISO 7816-4.

OnKey193 USB Token provides the following 4 logic interfaces.

Logic Interface	Corresponding Physical Interface	Description
Data In	DP/DM	The input data field of the command APDU to USB Token
Data Out	DP/DM	The output data field of the response APDU from USB Token
Control In	DP/DM	The command APDU header consisting of the CLA, INS, P1, P2 and LC fields comprises the control in interface used by User Application Tool.
	KEY1 pin KEY2 pin	The 4 buttons comprise the control in interface directly

	KEY3 pin KEY4 pin	used by User to interact on CM.
Status Out	DP/DM	The status word SW1 and SW2 of the response APDU comprise the status out interface, out of which the status can only be understood by user with the help of User Application Tool.
	LCD pins	The screen comprises the status out interface, out of which the status can give user intuitionistic meanings.

4.5 Operation System

The embedded operation system (OnCOS) on The OnKey193 Token module is developed in standard C-language based on Z8D168 Integrated Circuit chip. It is downloaded to the token in the factory (a secure environment) in plaintext. The module does not support software updates as this function is performed at the factory. The embedded operation system is provided in [OCS].

4.5.1 OnCOS File System Architecture

OnCOS file system is hierarchical, with file types MF (master file), DF (directory file), and EF (element file). If the hierarchical file structure is represented as a tree, the MF is the root of the file/directory tree. At manufacturing time, the card is initialized with the MF to contain PKI DF.
The general use application DF contains Tendyron’s PKI DF to be used with Tenryron’s PKCS #11 or windows CSP(Cryptographic Service Provider) middleware. In the Tendyron’s PKI DF, there are two types of EF, configuration files and application files. The configuration files are initialized at manufacture fatocry(a secure environment) and used only by the OnCOS internal. The configuration files are ‘ invisible’ from the outside and can’t be accessed by the outside with Read and Update commands in the application mode.
The Token file system is organized as described in [OCS].

4.5.2 OnCOS Security Architecture

The OnKey 193 USB token implements an access control rule consisting of an access type and a security condition called access right. The access type defines which operation can be performed on the application data file such as Read and Update and it is controlled by the permission bytes of each file.
In the OnKey 193 USB token, keys and CSPs are stored in separate files and OnCOS will not only check file id to prevent keys and CSPs output but also use the access control mechanism to ensure unwanted output of the sensitive information never occour.
The details of these commands are defined in [OCS].

5 Roles, Services, and Authentication

5.1 Identity Based Authentication

The OnKey 193 USB token performs identity-based authentication using PIN, cryptographic keys. A specific access right is assigned to each PIN and cryptographic key to identify each role associated with the token. The following section describes roles and access rights assigned.

5.2 Roles

The OnKey 193 USB token provides three independent roles, namely the Crypto-officer Roles, the User Roles and non-authenticated.

1 The Crypto-officer Role is responsible for initializing the application. When the token is initialized, all key pairs generated by user and all data in the user file will be deleted, and the PIN will be reset to the specified value. The token authenticates this Crypto-officer role by successfully executing External Authenticate challenge-response protocol using an AES key.
2 The User Role is essentially the end user and has access to all of the cryptographic functions of the token. The token authenticates this User Role by verifying the PIN value.
3 a non-authenticated operator is any unauthenticated operator who can only access non-security relevant application and data.

5.3 Services

5.3.1 Crypto Officer Services

This Role must execute the External Auth command with the secret response (challenge encrypted using an AES key) verification data to fulfill the access condition to initialize application.

The table below discrible the available service.

Role	**Service**	**Discription**
Crypto-Officer	External Authenticate +	used by the module to authenticate the crypto officer.A previous and successful execution of the GetChallenge command is required prior to processing this command
	AppInit	The data in the token are cleared, except the file system frame.
	SecureUpdateKey +	update the authentication key by using secure messaging ways
	EncTransGetKey +	Generate Communication Protection Key and establish security communication channel
	EncTransOperation +	Encrypt command header and data
Non-Authenticated	ReadPK	Read the readable information of the specified public key
	GetChallenge	Get the expected number of random bytes
	SelectFile	Select the given file for use in subsequent commands
	ReadBinary	Read binary data from a Transparent EF (elementary file)
	GetAppSystemInfo	Get attribute of PIN or Symmetric Key
	CardGetInfo	Get the serial number and manufacturer information on the smart card chip
	Query Language/Encoding Info	Query the current configuration of language and encoding, or query the list of supported languages and encodings
	Configure Language/Encoding	Configure displaying language and data coding
	Cancel Operation	Cancel the current operation from PC, and the function is the same as user

		pressing the ‘C’ button on the token

+ The service indicated must have the 2048 bit RSA keying option selected when signature generation or encryption is performed. The service indicated must have either the 168 bit Triple-DES, 128, 192, or 256 bit AES keying option selected when encrypt operations are performed.

5.3.2 User Services

This Role must execute the Verify PIN command with the correct 128 or 256 byte secret, response (challenge and PIN value encrypted using a RSA public key) verification data to transmit the state to User authenticated state. The user PIN value is encrypted by RSA public key, and the ciphertext is sent to the token via Verify PIN command. In this state, the User can access services provided by the token that require User authentication.

.

Role	**Service**	**Description**
User	Change PIN +	change the PIN CODE stored in the token
	Verify PIN	check the input PIN CODE , comparing it with the value stored in the token
	GenerateRSAKey +	Generates a RSA key pair into the internal private key and public key files with the referring key ID
	Secure Export Public Key +	Export the encrypted public key generated in the module
	Verify Signature	Verifies the signature with the referring public key
	Encipher +	Encrypts the given plaintext with the referring public RSA key
	Decipher	Decrypts the given ciphertext with the referring private RSA key
	DelRSAKey	Delete the referring RSA key pair
	UpdateBinary	update binary data to a Transparent EF(elementary file)
	GetUsrChoise	Gets the status of the pressed button
	Manage Secure Enviroment +	Prepares security commands (e.g.Computation of a digital signature, Verification of a digital signature, Encipher, Decipher)

	Compute Digital Signature +	Using private RSA key designated in previous MSE command, compute digital signature with data field in previous MSE command as digest
	Critical Data Signature +	Compute the digital signature of critical message with constraints of being in visiable ASCII encoding or other multibyte character encoding supported by COS
	EncTransGetKey +	Generate Communication Protection Key and establish security communication channel
	EncTransOperation +	Encrypt command header and data
Non-Authenticated	ReadPK	Read the readable information of the specified public key
	GetChallenge	Get the expected number of random bytes
	SelectFile	Select the given file for use in subsequent commands
	ReadBinary	Read binary data from a Transparent EF (elementary file)
	GetAppSystemInfo	Get attribute of PIN or Symmetric Key
	CardGetInfo	Get the serial number and manufacturer information on the smart card chip
	Query Language/Encoding Info	Query the current configuration of language and encoding, or query the list of supported languages and encodings
	Configure Language/Encoding	Configure displaying language and data coding
	Cancel Operation	Cancel the current operation from PC, and the function is the same as user pressing the ‘C’ button on the token

+ The service indicated must have the 2048 bit RSA keying option selected when signature generation or encryption is performed. The service indicated must have either the 168 bit Triple-DES, 128, 192, or 256 bit AES keying option selected when encrypt operations are performed.

5.3.3 Non Authenticated Service

This Role does not need to execute any authentication.

Role	**Service**	**Discription**
Non-Authenticated	ReadPK	Read the readable information of the specified public key
	GetChallenge	Get the expected number of random bytes
	SelectFile	Select the given file for use in subsequent commands
	ReadBinary	Read binary data from a Transparent EF (elementary file)
	GetAppSystemInfo	Get attribute of PIN or Symmetric Key
	CardGetInfo	Get the serial number and manufacturer information on the smart card chip
	Query Language/Encoding Info	Query the current configuration of language and encoding, or query the list of supported languages and encodings
	Configure Language/Encoding	Configure displaying language and data coding
	Cancel Operation	Cancel the current operation from PC, and the function is the same as user pressing the 'C' button on the token

5.4 Authentication

All access rights are application security based which means the status of the access right will be false when an application DF is selected.
Concurrent operators are not supported. For all role authentications the following properties stand:

- The minimum PIN length in OnKey193 is 6 bytes, and one-byte can be one of the “0-9” numbers and “A-Z” characters. In the worse situation user use the minimum length pin (6 bytes), if a random access succeeds, all the 6 bytes must be matched which means a probability of one in 36^6 , or less than one in 1,000,000.
- the probability is less than one in 1,000,000 that a random attempt at authentication will succeed
- during any one minute period, the probability is less than 1 in 100,000 that a random authentication attempt will succeed

To discourage an attacker from guessing the User PIN or Challenge-response key, this mechanism includes a counter of failed authentication and a blocking mechanism. The counter is decremented prior to any attempt to authenticate and is only reset to its threshold (maximum value) upon successful authentication. The authentication mechanism is blocked when the associated counter reaches zero, and an error response will be returned. The PIN can be reload by initialize function. The key authentication method cannot be unblocked. If the key is blocked, the PIN will never be reloaded.

5.4.1 Crypto Officer Authentication

.
The Crypto-officer authenticates by executing the Authentication command with the secret response verification data to fulfill the access condition to initialize application.

5.4.2 User Authentication

The User authenticates by executing the Verify PIN command with the secret response verification data to transmit the state to User authenticated state. In this state, the User can access services provided by the token that require User authentication.

6 FIPS-Approved Mode of Operation

The module is shipped from the factory in the FIPS approved mode of operation. The end user can confirm that the module is in the FIPS approved mode by reading the product version info stored in the module.

7 Cryptographic Functions

The purpose of the OnKey193 Token module is to provide a FIPS validated module that may provide cryptographic services to end-user applications. Cryptographic keys and PIN represent the roles involved in controlling the token. A variety of FIPS 140-2 validated algorithms are used in the OnKey193 Token module to provide cryptographic services.

7.1 Random Number Generator

The Onkey193 Token module supports a hardware random number generator.
Val. Cert. #509

7.2 Cryptographic Algorithms

The Onkey193 Token module includes the following cryptographic algorithms:

- Triple-DES
  FIPS-Approved, Val. Cert. #725
  Encrypt and Decrypt
  MAC
  112-bit and 168-bit key length (112 bit is not to be used to encrypt in the approved mode of operation)
  To use the two-key Triple-DES algorithm to encrypt data or wrap keys in an Approved mode of operation, the module operator shall ensure that the same two-key Triple-DES key is not used for encrypting data (or wrapping keys) with more than 2^{20} plaintext data (or plaintext keys).
  Triple-DES key wrapping; key establishment methodology provides 112 bits of encryption strength; non-compliant less than 112 bits of encryption strength
- AES
  FIPS-Approved, Val. Cert. #889
  Encrypt and Decrypt
  MAC
  128-bit, 192-bit and 256-bit key length
  AES key wrapping; key establishment methodology provides between 128 and 256 bits of encryption strength
- RSA
  FIPS-Approved, Val. Cert. #430
  FIPS-Approved, Val. Cert. #1138
  sign and verify
  encrypt and decrypt
  1024-bit and 2048-bit key length (1024 bit is not to be used to sign or encrypt in the approved mode of operation)
  RSA key wrapping; key establishment methodology provides 112 bits of encryption strength; non-compliant less than 112 bits of encryption strength
- SHA
  FIPS-Approved, Val. Cert. #879
  FIPS-Approved, Val. Cert. #1735
  SHA-1 (Not to be used for sign operations in the approved mode)
  SHA-256
  SHA-384
  SHA-512

7.3 Critical Security Parameters

This module includes the following CSPs. CSPs used as authentication method have default value initialized by vendor. User or issuer can authenticate his identity with the provided default value upon accessing the module for the first time. He may and should change the value to his private one with corresponding commands.

Name	Abbreviation	Type	Description	Storage
RSA Key‘s Secure Storage Key	KSSK	128-bit AES key	Used to encrypt all private components of RSA key pairs.. It is generated in the factory (a secure environment) using the hardware RNG	Embedded in FLASH
Application Initialization Key	AIK	128-bit AES key	Authentication Key used by the Crypto Officer to complete the Application Initiation operation	Stored at the FLASH in plaintext.
Communication Protection Key	CPK	128-bit AES key	Used to protect the communication channel between the token and the Terminal(e.g. Application Software on PC), generated temporarily within each power cycle.	Stored at the RAM in plaintext
Critical Message Signing Key (Private)	CMSK	1024/2048-bit RSA key	Used to sign the critical Message. **	Stored at the FLASH in ciphertext.
Normal Message Signing Key (Private)	NMSK	1024/2048-bit RSA key	Used to sign the Normal Message. **	Stored at the FLASH in ciphertext.
Encryption/Decryption Key	EDK	1024/2048-bit RSA key	Used to encrypt and decrypt. **	Stored at the FLASH in ciphertext.
Public Key Export Protection Key (Private)	PKEPK	1024/2048-bit RSA key	Used to protect the export of public component of RSA key pairs. **	Stored at the FLASH in ciphertext.
User Pin Protection Key (Private)	UPPK*	1024/2048-bit RSA key	Used to decrypt the cipher pin in Verify PIN or Change PIN command. **	Stored at the FLASH in ciphertext.
CPK Exchange Key	CPKEK*	1024/2048-bit RSA key	Used to exchange CPK with terminal(e.g. Application Software on PC). **	Stored at the FLASH in ciphertext.
User Pin	PIN	N/A	Used to authenticate the	Stored at the

			identity of the legal holder.	FLASH in plaintext.
RNG Seed Key	RSK	168-bit TDES Key	Used to generate RNG.	Embedded in FLASH

*The module is designed to support both UPPK and CPKEK which are differentiated by ID, but generally this two CSPs use the same key pair.

** 1024 bit RSA key is not to be used in the approved mode of operation for sign or encrypt operations.

8 Self Tests

8.1 Power-Up Self-Tests

8.1.1 Integrity Self-Test

Each time this cryptographic module is powered up self-test will automatically run to check if the firmware on the module is still in integrity.
If the integrity self-test fails, the LED on the module will flash to warn the user.

8.1.2 Algorithm Self-Test

Each time this cryptographic module is powered up it tests that the cryptographic algorithms still operate correctly. Known Answer Tests (KATs) are conducted for each cryptographic algorithm in one mode of operation. The following KATs are performed:

RSA PKCS#1(sign and verify with 1024-bit private key and public key)
TDES(encrypt and decrypt with 112-bit ,168-bit key in ECB mode)
SHA-1
SHA-256
SHA-384
SHA-512
AES(encrypt and decrypt with 128-bit,192-bit,256bit key in ECB mode)
RNG

If one of the KATs fails the module will be mute(performs no further data or status input or output and must be reset)and record the failure time. If the KATs succeeds next time, the count will be reset. When the count reaches 8, the module will be locked permanently.

8.2 Conditional Self-Tests

- RSA Key generation:

A pair wise consistency check is performed during key generation which consists of encrypt/decrypt operation if the parameter in the APDU command requires the check. The pair wise consistency check for encrypt/decrypt calculates and verifies that the cipher differs from the plain text, and that the decrypted result is equal to the original plain text. If the test fails and an error message “⚠”will be returned.

- Random number generation:

A continuous RNG test is performed during each use of the hardware random generator to verify that it is not generating the same value. If the test fails an error message will be returned.

- RSA Calculation:

A pair wise consistency check is performed during RSA calculation which consists of encrypt/decrypt or sign/verify operation. The pair wise consistency check for encrypt/decrypt or sign/verify calculates and verifies that the cipher differs from the plain text, and that the decrypted result is equal to the original plain text. If the test fails an error message will be returned.

- Functionality of buttons:

OnCOS checks status of buttons periodically to ensure that the buttons is not stuck. If the test fails an error message will be returned.

9 Security Rules

9.1 Access Control Security Rules

All sensitive information, symmetric keys, RSA Key Pairs and PIN are stored in the FLASH, which can be accessed by the following rules:

For every restricted service, verifying that authentication security status is granted for each role,

The sensitive information is imported which is protected by Secure Message using the protect key to ensure their integrity and confidentiality.

9.2 Key and PIN Management Security Rules

The module contains a set of symmetric keys, PIN and a variety of RSA key pairs. The module protects these keys from unauthorized disclosure, export, modification, and substitution

9.2.1 Key Generation

- RSA Key's Secure Storage Key(AES)

This key is generated in the factory (a secure environment) using the hardware RNG.

- Critical Message Signing Key(RSA)
- Normal Message Signing Key(RSA)
- Encryption/Decryption Key(RSA)
- Public Key Export Protection Key(RSA)
- UserPin Protection Key(RSA)
- CPK Exchange Key(RSA)

RSA key pairs are generated upon application using the GenerateRSAKey service after authentication.

9.2.2 Key and PIN Storage

- Application Initialization Key(AES)
- RSA Key's Secure Storage Key(AES)
- Critical Message Signing Key(RSA)
- Normal Message Signing Key(RSA)
- Encryption/Decryption Key(RSA)
- Public Key Export Protection Key(RSA)
- UserPin Protection Key(RSA)
- CPK Exchange Key(RSA)
- Secure Channel Establishing Key(RSA)

These keys are stored in FLASH. The module uses the key ID to associate each key with the correct entity.

The User Pin is stored in FLASH

9.2.3 Key and PIN Entry

- Application Initialization Key(AES)

This key is first imported in the factory (a secure environment) in plaintext.

- User Pin

The User Pin is encrypted by UserPin Protection Key (RSA), and imported after

successful user authentication.
All RSA private keys cannot be imported from the outside environment.

9.2.4 Key and PIN Output

The public keys can be read from the module.
All RSA private keys cannot be exported from the module in any way.
All symmetric keys and user PIN are not allowed to be exported from the module in any way.
The OnKey193 Token don’t provides any secret keys and CSPs output service.

9.2.5 Key and PIN Zeroization

The OnKey193 Token supports zeroizing all the application keys and PIN:

the data stored in the token are cleared , except the file system frame by using the AppInit service after successful crypto officer authentication.

The OnKey193 Token also supports zeroizing all the session keys:

When the OnKey193 Token is closed due to power-off, the session keys are lost as they are stored in RAM. The RAM is actively cleared to zero on the next power-on.

10 References

The following standards are referred to in this Security Policy.

Acronym	**Full Specification Name**
[OCS]	OnCOS Specification, Version 1.0
[USB 1.1]	Universal Serial Bus Revision 1.1 specification
[USB 2.0]	Universal Serial Bus Revision 2.0 specification
[BOT]	Universal Serial Bus Mass Storage ClassBulk-Only Transport Revision 1.0
[7816-4]	ISO/IEC 7816-4, Second edition 2005-01-15, Identification cards — Integrated circuit(s) cards with contacts — Part 4: Interindustry commands for interchange
[FIPS140-2]	FIPS 140-2 Security Requirements for Cryptographic modules, May 25, 2001