FEITIAN Technologies

OTP Token

Non-Proprietary FIPS 140-2 Security Policy

Document Version: 1.0

Date: 2021/4/29

Table of Contents

List of Tables

List of Figures

1 Introduction

This document defines the Security Policy for the FEITIAN Technologies OTP Token module, hereafter denoted the Module.

OTP Token enables strong authentication by positively identifying a user with one-time passwords. By simply pressing the button, OTP Token generates a secure event synchronous or time-based one-time password, ensuring proper identification and allowing only authorized access to critical applications and sensitive data.

OTP Token is a connectionless device offering the user true zero-footprint authentication. The OTP Token is embedded within a Feitian C100 or C200. The C100 OTP Token complies with OATH standards in event-based authentication methods and the C200 OTP Token complies with IETF draft of time-based authentication methods, which was submitted by OATH providing compatibility with 3rd party software. It works with the OTP authentication server, as well as other 3rd remote access and network access devices, to provide best-of-breed solutions for security needs. Table 1 lists the configurations covered by this Security Policy; note the devices are physically identical and can only be distinguished by the first half of the serial number (WWXYZZ) using the following method:

- WW: “01” for C100, “02” for C200.
- X: Fixed value. “5” for C100, “2” for C200.
- Y: “0” for SHA-1, “2” for SHA-256
- ZZ: 1.0.

Table 1 – Cryptographic Module Configurations

	HW P/N and Version	FW Version	Serial Number	Product Name
1	P449, V1.0	V1.0	build015010	OTP c100
2	P449, V1.0	V1.0	build015210	OTP c100
3	P449, V1.0	V1.0	build021010	OTP c200
4	P449, V1.0	V1.0	build021210	OTP c200

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

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	1
Cryptographic Module Ports and Interfaces	1
Roles, Services, and Authentication	1
Finite State Model	1
Physical Security	1
Operational Environment	N/A
Cryptographic Key Management	1
EMI/EMC	3
Self-Tests	1
Design Assurance	1
Mitigation of Other Attacks	N/A
Overall	1

1.1 Module Description and Cryptographic Boundary

The physical form of the Module is depicted in Figure 2. The Module is a multiple-chip embedded cryptographic module manufactured with production grade components. The cryptographic boundary is defined as the outer perimeter of the PCB as shown in Figure 2 with major components depicted below in Figure 1:

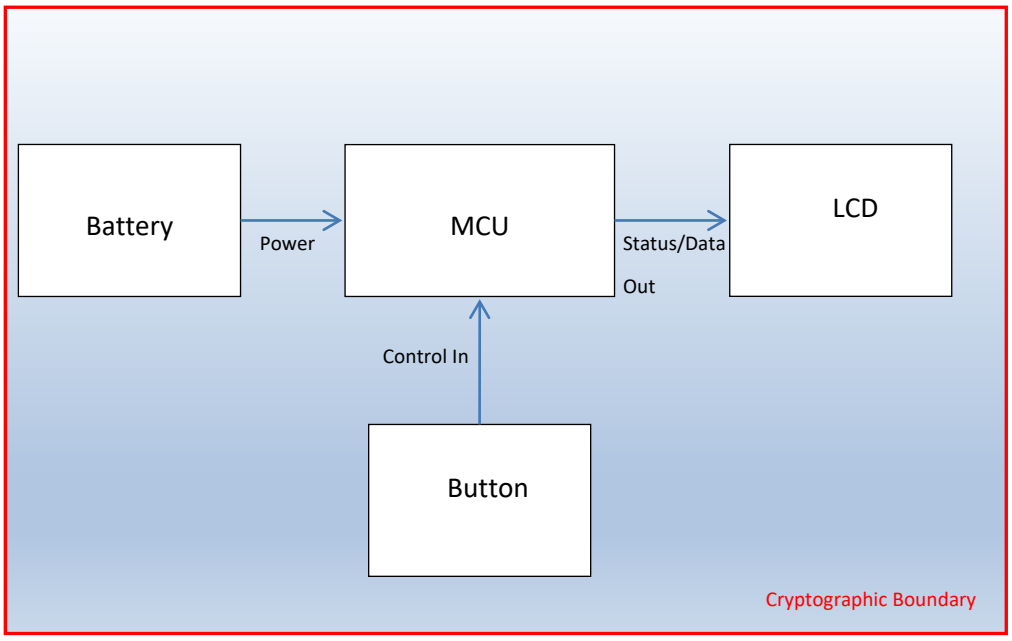

Figure 1 – Module Crypto Boundary

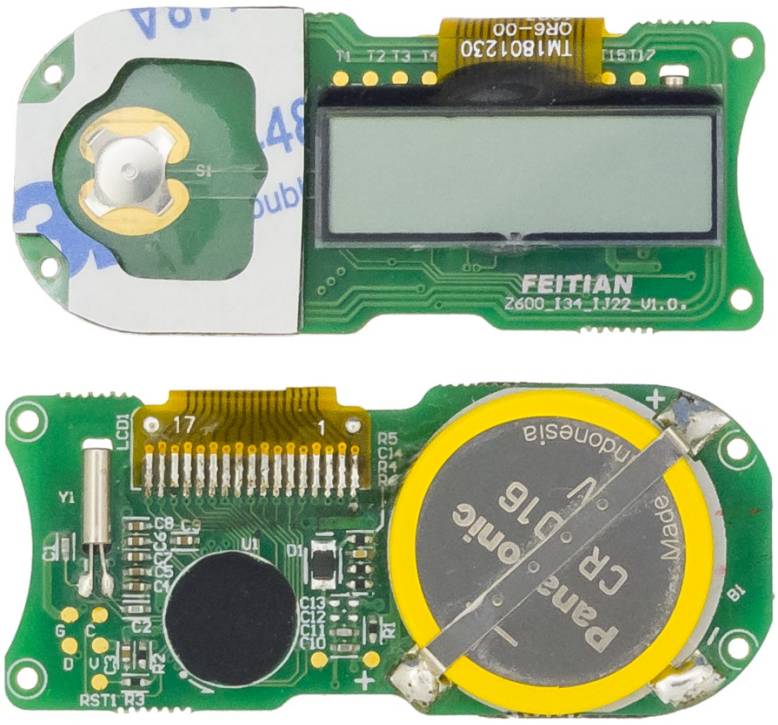

Figure 2 - Feitian OTP Token (Front and Back)

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
LCD Screen	Display password and device status	Data/Status output interface
Button	Push button to make device Switch on/stand by	Control input
Battery	Power	Power

1.2 Modes of Operation

Feitian OTP Token supports only a FIPS Approved mode of operation when the device is loaded with the firmware listed in Table 1.

2 Cryptographic Functionality

The Module implements the FIPS Approved cryptographic functions listed in the tables below.

Table 4 – Approved Algorithms

Cert	Algorithm	Mode	Description	Functions/Caveats
C1993	HMAC	SHA-1, SHA-256	Generate HMAC w/ 160-bit or 256-bit keys	Keyed-Message Authentication Code
C1993	SHS	SHA-1, SHA-256	Generate event-based and time-based OTPs	Hash

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 / Usage	Generation	Storage	Entry/Output	Destruction
HMAC Key	Defined by customer during production. 160-bit (HMAC-SHA-1) or 256-bit (HMAC SHA-256) value based on configuration	N/A. Configured during production	RAM, obfuscated (XOR'd with a random value defined during production)	Entry: N/A Output: N/A	Zeroized at Battery low power or physical battery removal.

2.2 Public Security Parameters

Table 6 – Public Security Parameters (PSPs)

PSP	Description / Usage
None	N/A

3 Roles, Authentication and Services

3.1 Assumption of Roles

The module supports only a single operator that assumes both the User and Cryptographic Officer role. The module does not support authentication and does not distinguish between the User and Cryptographic Officer role.

Table 7 lists all operator roles supported by the module.

Table 7 – Roles Description

Role ID	Role Description	Authentication Type	Authentication Data
User	The User role is the everyday operator of the device.	N/A	N/A
Crypto Officer (CO)	The CO role is the everyday operator of the device.	N/A	N/A

3.2 Services

All services implemented by the Module are listed in Table 8:

Table 8 – Services

Service	Description	CO	U
Generate passcode	Push button under power off mode, the module calculates and display passcode; under display mode, push button, display off, the module enters standby mode.	X	X
Standby/Sleep	OTP Token can perform timing function according to display time defined in production, when display time-out OTP Token will shut down LCD and enter standby/power off mode. Pressing the button will also enable standby/sleep.	X	X
Show Status	Output of error messages on the LCD: ERR 1 or ERR 2. At initial power-on, the module will display the build version. When the battery is low, the LCD will indicate with a low battery icon	X	X
Zeroize	Destruction of CSPs upon detection of a low battery state. There is no recovery from zeroization.	X	X
Self-Tests	The module will automatically perform self-tests whenever the button is pressed. This serves as the required Power-On Self-Tests and also provides the on demand self-tests.	X	X

Table 9 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 9 – Security Parameters Access by Service

Service	Security Parameters
	HMAC Key
Generate passcode	E
Standby/sleep	
Show Status	
Zeroize	Z
Self-Tests	

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 pressing the button.

The module will check the integrity of firmware (16-bit EDC) to ensure that firmware has no loss or damage; module will perform algorithm self-test by doing Known Answer Test (KAT). Note that based on configuration, the module will only test HMAC-SHA-1 or HMAC-SHA-256, as the employed algorithm is defined at build time and cannot be changed. The algorithm KAT must be completed successfully prior to any other use of cryptography by the Module. If the KAT fails, the Module will enter the error state; no operation can be performed and the LCD displays "ERR". Otherwise, it indicates successful completion by displaying a calculated passcode.

The module performs the following algorithm self-tests on power-up:

- Firmware Integrity Test (16-bit EDC)
- HMAC-SHA-1 or HMAC-SHA-256 KAT (inclusive of SHA-1 KAT or SHA-256 KAT respectively)

5 Physical Security Policy

The module is a multiple-chip embedded cryptographic module made with production grade components and standard passivation. The module conforms to EMI/EMC requirements for a FIPS 140-2, Level 3 module.

6 Operational Environment

This set of requirements is not applicable as the microcontroller firmware cannot be upgraded once the token has left production. The module does not provide a general-purpose operating system.

7 Mitigation of Other Attacks Policy

This set of requirements is not applicable.

8 Security Rules and Guidance

The following security rules and guidance apply to the module:

1. During production, an HMAC key of at least 112-bits shall be installed; the module uses 160-bit keys for HMAC-SHA-1 configurations and 256-bit keys for HMAC-SHA-256 configurations.
2. The module does not require any initialization or installation once manufactured. The module is fully functional upon delivery and the operator may invoke services via the button.
3. Upon removal of the battery, the module will zeroize the HMAC key and be rendered inoperable.

9 References and Definitions

The following standards are referred to in this Security Policy.

Table 10 – 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, August 28, 2020*
[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*
[OATH]	OATH-TOTP-rfc6238, OATH-HOTP-rfc4226, OATH-Challenge-Response-rfc6287

Table 11 – Acronyms and Definitions

Acronym	Definition
CSP	Critical Security Parameter
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
FIPS	Federal Information Processing Standard
HMAC	Hash-Based Message Authentication Code
LCD	Liquid Crystal Display
MCU	Microcontroller Unit
OATH	Open Authentication
OTP	One Time Passcode
SHA	Secure Hash Algorithm

