HYPERSECU®

HyperOTP Token

FIPS 140-2 Non-Proprietary Security Policy

Document Version: 1.0.0
Date: October 27, 2022

HYPERSECU INFORMATION SYSTEMS INC

200-6191 Westminster Hwy, Richmond BC, V7C 4V4 Canada
1-604-279-2000 | hypersecu.com

Table of Contents

List of Tables

List of Figures

Document History

Version	Release Date	Description of Changes	Document Owner	Approved By
1.0.0	2022-10-27	Initial Release	NB	JL

1. Purpose

This non-Propriety Security Policy for the HyperOTP Token, a one-time password token module by Hypersecu Information Systems Inc describes how the module meets the security requirements of FIPS 140-2.

The HyperOTP Token enables strong authentication by positively identifying the user with a one-time password. Pressing the button on the HyperOTP Token generates a secure event-based or time-based one-time password, ensuring proper identification and allowing only authorized access to critical applications and sensitive data.

The HyperOTP Token is a connectionless device offering users true zero-footprint authentication. The token is embedded within a Hypersecu HyperOTP HOTP or a HyperOTP TOTP. The HyperOTP HOTP complies with IEFT RFC4226 event-based authentication methods and the HyperOTP TOTP complies with IETF RFC6238 time-based authentication methods, which was submitted by OATH (Open Authentication) providing compatibility with 3rd party software.

The HyperOTP Token works with OATH OTP authentication compatible servers, 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 HyperOTP HOTP, “02” for HyperOTP TOTP.
- X: Fixed value. “5” for HyperOTP HOTP, “2” for HyperOTP TOTP.
- Y: “0” for SHA-1, “2” for SHA-256
- ZZ: 1.0.

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

Table 1 - Cryptographic Module Configurations

The module is intended for use by U.S. federal agencies or other industries that require a FIPS 140-2 validated OTP token product.

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

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

Table 2 - Security Level of Security Requirements

1.1 Module Description and Cryptographic Boundary

The physical form of the module is depicted in Figure 2. The module is a multi-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.

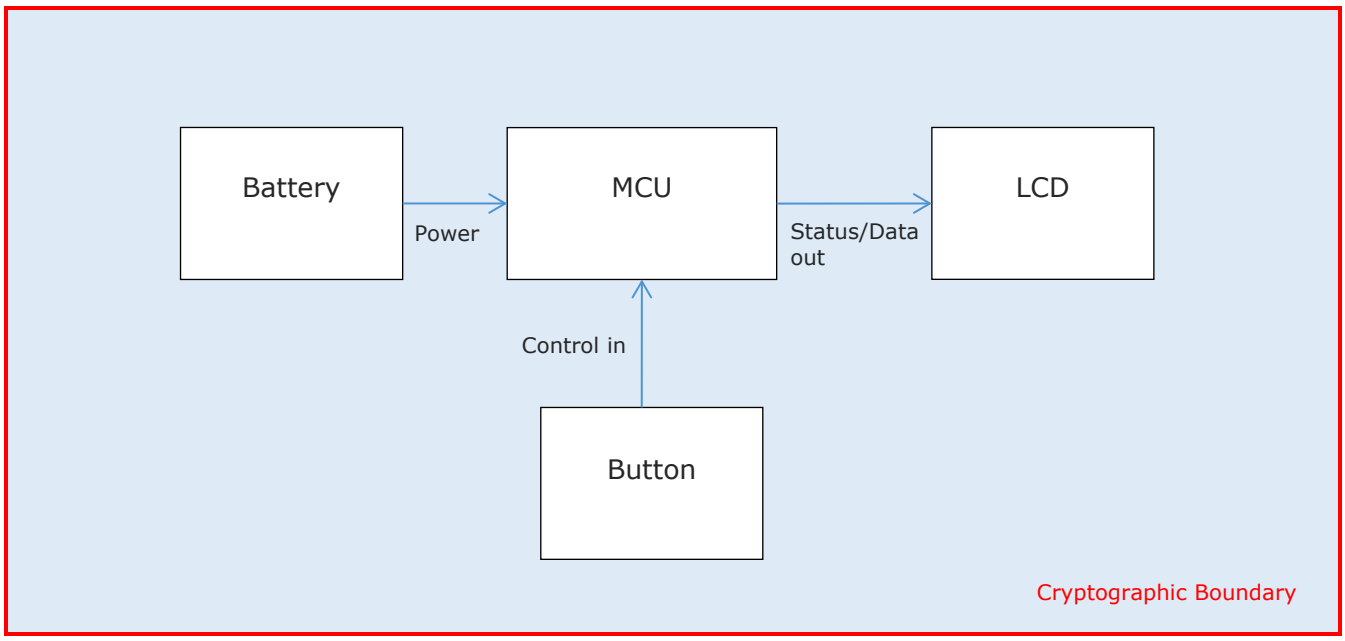

Figure 1 - Module Crypto Boundary

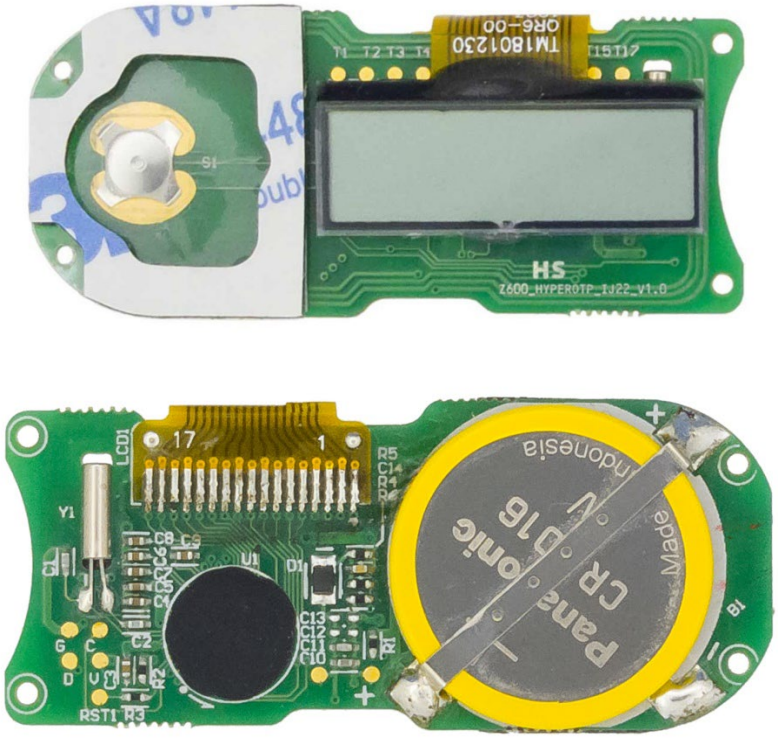

Figure 2 - HyperOTP Token (Front and Back)

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

Port	Description	Logical Interface Type
LCD screen	Displays one-time password and device status	Data/status output interface
Button	Push the button to power on the device or activate the device's standby mode	Control input
Battery	Power source	Power source

Table 3 - Ports and Interfaces

1.2 Modes of Operation

The HyperOTP 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.

Cert	Algorithm	Mode	Description	Functions/Caveats
A2875	HMAC	SHA-1, SHA-256	Generate HMAC w/ 160-bit or 256-bit keys	Keyed-Message Authentication Code
A2875	SHS	SHA-1, SHA-256	Generate event-based and time-based OTPs	Hash

Table 4 - Approved Algorithms

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.

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

CSP	Description/Usage	Generation	Storage	Entry/Output	Destruction
	SHA-256) value based on configuration				

Table 5 - Critical Security Parameters (CSPs)

2.2 Public Security Parameters

PSP	Description/Usage
None	N/A

Table 6 - Public Security Parameters (PSPs)

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 (CO) 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.

Role ID	Role Description	Authentication Type	Authentication Data
User	Everyday operator of the device	N/A	N/A
Cryptographic Officer (CO)	Everyday operator of the device	N/A	N/A

Table 7 - Description of Roles

3.2 Services

All services implemented by the module are listed in Table 8.

Service	Description	CO	U
Generate passcode	When pushing the button while the OTP token is under standby mode, the module calculates and displays a passcode.	X	X

Service	Description	CO	U
	When pushing the button while the OTP token's display is on, the module enters standby mode.		
Standby/Sleep	The OTP token can perform timing function according to the display time defined in production. When the display times out, the OTP token will shut down the LCD and enter standby/sleep mode. Pressing the button while the display is on will also enable standby/sleep mode.	X	X
Show Status	Output error messages on the LCD are as follows: ERR 1 or ERR 2. Upon initial power-on, the module will display the build version. When the battery is low, the LCD will indicate this 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 when the button is pressed. This serves as the required Power-On Self-Tests, as well as provides the on demand self-tests.	X	X

Table 8 - Description of Services

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

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

Table 9 - Security Parameters Access by Service

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 the firmware (16-bit EDC) to ensure that the firmware has no loss or damage. The module will then perform algorithm self-test by doing a 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 operations can be performed in the error state, and the LCD displays "ERR". Otherwise, it indicates successful completion of the KAT 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 multi-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 will be rendered inoperable.

9. References and Definitions

The following standards are referred to in this Security Policy.

Abbreviation	Full Specification Name
FIPS 140-2	*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 10 - References

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

Table 11 - Acronyms and Definitions