Safeword3300 Platinum V2F Cryptographic Module

FIPS 140-3 Level 1 Non-Proprietary Security Policy

Document Information

Document Part Number	002-000459-001
Release Date	October 21, 2024

Trademarks, Copyrights, and Third-Party Software

Disclaimer

All information herein is either public information or is the property of and owned solely by Thales and/or its subsidiaries who shall have and keep the sole right to file patent applications or any other kind of intellectual property protection in connection with such information.

Nothing herein shall be construed as implying or granting to you any rights, by license, grant or otherwise, under any intellectual and/or industrial property rights of or concerning any of Thales's information.

This document can be copied or distributed for informational, non-commercial, internal and personal use only provided that:

- The copyright notice below, the confidentiality and proprietary legend and this full warning notice appear in all copies.
- This document shall not be posted on any network computer or broadcast in any media other than on the NIST CMVP validation list and no modification of any part of this document shall be made.

Use for any other purpose is expressly prohibited and may result in severe civil and criminal liabilities.

The information contained in this document is provided "AS IS" without any warranty of any kind. Unless otherwise expressly agreed in writing, Thales makes no warranty as to the value or accuracy of information contained herein.

Thales hereby disclaims all warranties and conditions with regard to the information contained herein, including all implied warranties of merchantability, fitness for a particular purpose, title and non-infringement. In no event shall Thales be liable, whether in contract, tort or otherwise, for any indirect, special or consequential damages or any damages whatsoever including but not limited to damages resulting from loss of use, data, profits, revenues, or customers, arising out of or in connection with the use or performance of information contained in this document.

Thales does not and shall not warrant that this product will be resistant to all possible attacks and shall not incur, and disclaims, any liability in this respect. Even if each product is compliant with current security standards in force on the date of their design, security mechanisms' resistance necessarily evolves according to the state of the art in security and notably under the emergence of new attacks. Under no circumstances, shall Thales be held liable for any third party actions and in particular in case of any successful attack against systems or equipment incorporating Thales products. Thales disclaims any liability with respect to security for direct, indirect, incidental or consequential damages that result from any use of its products. It is further stressed that independent testing and verification by the person using the product is particularly encouraged, especially in any application in which defective, incorrect or insecure functioning could result in damage to persons or property, denial of service or loss of privacy.

CONTENTS

ACRONYMS AND ABBREVIATIONS

Term	Definition
CAVP	Cryptographic Algorithm Validation Program
CMVP	Cryptographic Module Validation Program
EDC	Error Detection Code
FIPS	Federal Information Processing Standard
HMAC	Keyed-Hash Message Authentication Code
HOTP	HMAC-based One-Time Password
IG	Implementation Guidance
ISO/IEC	International Organization for Standardization / International Electrotechnical Commission
KAT	Known Answer Test
LCD	Liquid Crystal Display
NIST	National Institute of Science and Technology
N/A	Not Applicable
OATH	Open Authentication
OCRA	Open Authentication Challenge-Response Algorithm
OTP	One-Time Password
RAM	Random Access Memory
RFC	Request for Comments
SHA	Secure Hash Algorithm
SHS	Secure Hash Standard
SSP	Sensitive Security Parameter
TOTP	Time-Based One-Time Password

REFERENCES

[FIPS 140-3] Federal Information Processing Standards Publication (Supersedes FIPS PUB 140-2), Security Requirements for Cryptographic Modules, March 22, 2019.

[FIPS 800-140C] National Institute of Science and Technology (NIST), CMVP Approved Security Functions: CMVP Validation Authority Updates to ISO/IEC 24759, March 2020.

[FIPS 800-140F] NIST, CMVP Approved Non-Invasive Attack Mitigation Test Metrics: CMVP Validation Authority Updates to ISO/IEC 24759, March 2020.

[FIPS 140-3 IG] NIST, Implementation Guidance for FIPS 140-3 and the Cryptographic Module Validation Program, October 7, 2022.

[FIPS 180-4] Federal Information Processing Standards Publication 180-4, Secure Hash Standard (SHS), NIST, August 2015.

[FIPS 198-1] Federal Information Processing Standards Publication 198-1, The Keyed-Hash Message Authentication Code (HMAC), July 2008.

[ISO/IEC 19790:2012] ISO/IEC 19790:2012 (Corrected 2015-12-15, IDT) Information technology – Security techniques – Security requirements for cryptographic modules, 2015-12-15.

[ISO/IEC 24759:2017] ISO/IEC 24759:2017 (Corrected 2017-03, IDT) Information technology – Security techniques – Test requirements for cryptographic modules, 2017-03.

[RFC 4226] HOTP: An HMAC-Based One-Time Password Algorithm, December 2005.

[RFC 6238] TOTP: Time-Based One-Time Password Algorithm, May 2011.

[RFC 6287] OCRA: OATH Challenge-Response Algorithm, June 2011.

PREFACE

This document deals only with operations and capabilities of the Safeword3300 Platinum V2F Cryptographic Module in the technical terms of [FIPS 140-3].

General information on Thales products is available from the following sources:

- the Thales internet site contains information on the full line of available products at https://cpl.thalesgroup.com
- technical or sales representatives of Thales can be contacted through one of the channels listed on https://cpl.thalesgroup.com/contact-us

1 General

1.1 Security Level

The Safeword3300 Platinum V2F Cryptographic Module meets Level 1 security requirements for [FIPS 140-3] as summarized in the table below:

Table 1-1: Security Levels

[ISO/IEC 24759:2017] Section 6 [Number Below]	FIPS 140-3 Section Title	Security Level
1	General	1
2	Cryptographic Module Specification	1
3	Cryptographic Module Interfaces	1
4	Roles, Services, and Authentication	1
5	Software/Firmware Security	1
6	Operational Environment	1
7	Physical Security	1
8	Non-Invasive Security	N/A
9	Sensitive Security Parameter Management	1
10	Self-Tests	1
11	Life-Cycle Assurance	1
12	Mitigation of Other Attacks	N/A

2 Cryptographic Module Specification

2.1 Module Overview

The Safeword3300 Platinum V2F Cryptographic Module is a multi-chip standalone hardware security module in the form of a token. The cryptographic module is contained in its own secure enclosure, which provides physical resistance to tampering. The physical resistance to tampering was not assessed during the evaluation due to the targeted security level.

The cryptographic boundary of the module is defined to encompass all components inside the secure enclosure on the token.

The module is explicitly configured to operate in an [FIPS 140-3] approved mode of operation during personalization performed at the factory. No additional configuration is required to be performed by the end user. All cryptographic operations make use of approved cryptographic functions used in an approved manner. No non-approved cryptographic algorithms, security functions or processes are available from the module. When the user selects the 'ON' button, and the LCD screen is active, only FIPS-approved cryptographic functions are available. Indication of approved status is therefore implicit for all cryptographic services.

The module only supports a single approved mode of operation.

> **NOTE** The Safeword3300 Platinum V2F Cryptographic Module does not support degraded operation as defined in [ISO/IEC 19790:2012].

The module provides a one-time password (OTP). This password is derived using the Time-Based One-Time Password (TOTP) protocol [RFC 6238] or a challenge-response based on the HMAC-based One-Time Password (HOTP) [RFC 4226] protocol.

2.2 Module Description

The cryptographic module as defined in [ISO/IEC 19790:2012] is a **hardware module** of type **multi-chip standalone**.

The cryptographic boundary of the module is shown in Figure 2-1. The cryptographic boundary is defined as the entire token.

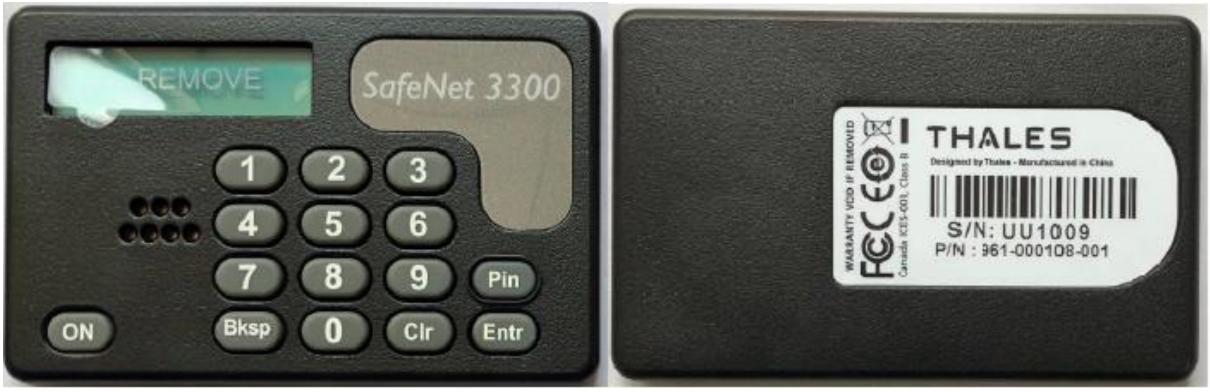

Figure 2-1: Safeword3300 Platinum V2F Cryptographic Module cryptographic boundary

The following figure highlights the cryptographic boundary of the module covered by this certification:

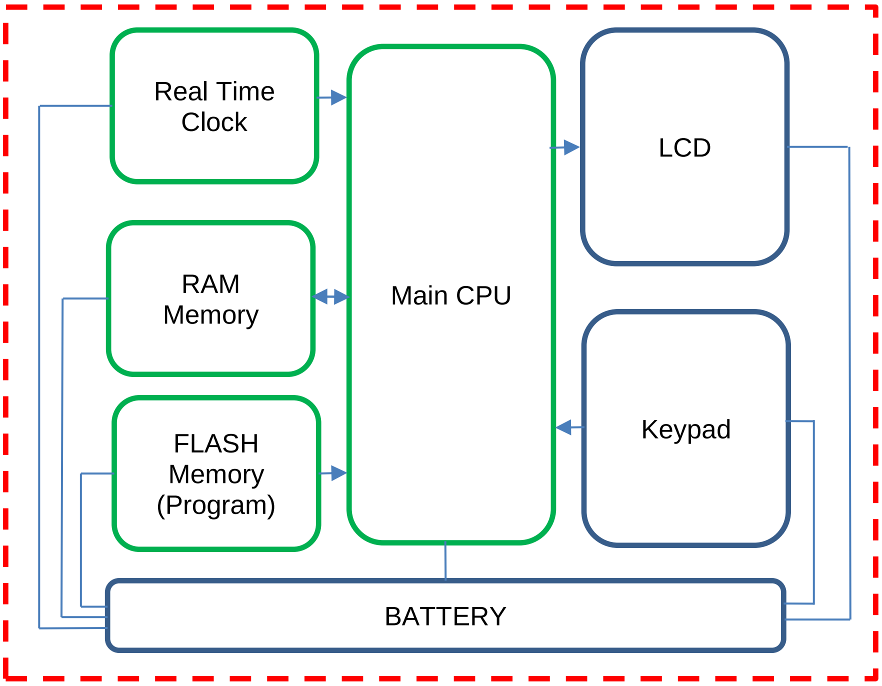

Figure 2-2 – Safeword3300 Platinum V2F Cryptographic Module, cryptographic boundary

The Safeword3300 Platinum V2F Cryptographic Module is a standalone token. The cryptographic boundary includes the hardware, firmware, battery and interfaces (Liquid Crystal Display (LCD) and keypad).

2.3 Test Configuration

The following tested configuration is covered in this security policy:

Table 2-1: Cryptographic module tested configuration.

Model	Hardware [Part Number and Version]	Firmware Version	Distinguishing Features
Safeword3300 Platinum V2F	Safeword3300 Platinum V2F HW 1.0	Version CB 20005	Standalone token with internal battery, 2 line LCD and 15-button keypad.

Figure 2-3 shows the front and back of the Safeword3300 Platinum V2F HW 1.0 with standard markings and Figure 2-4 shows the Safeword3300 Platinum V2F HW 1.0 with Citibank markings.

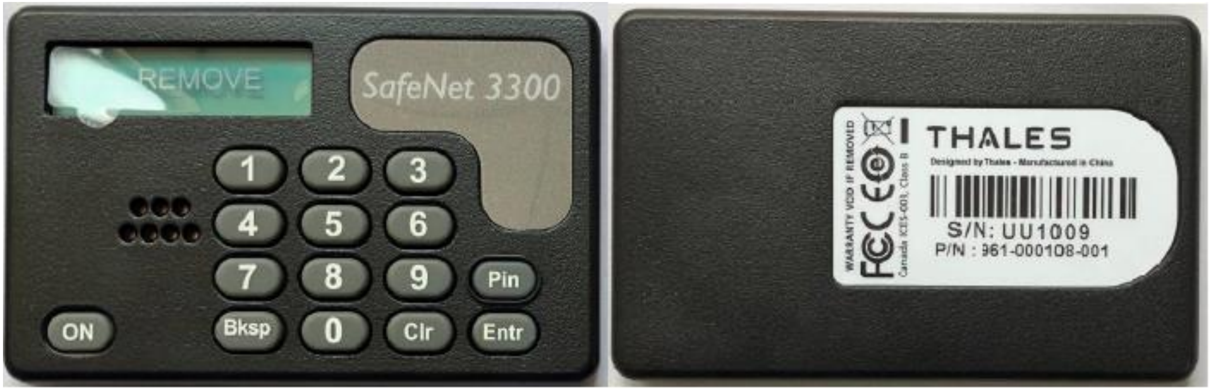

Figure 2-3: Safeword3300 Platinum V2F HW 1.0 with standard markings

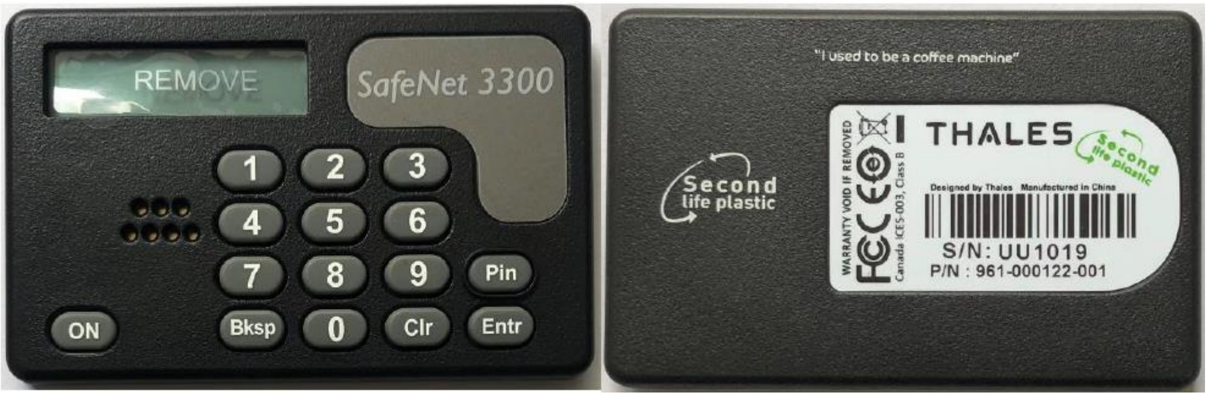

Figure 2-4: Safeword3300 Platinum V2F HW 1.0 with Citibank customization

2.4 Approved Algorithms

The following cryptographic library and associated Cryptographic Algorithm Validation Program (CAVP) certificate is used by the cryptographic module:

> Safeword3300 Platinum Cryptographic Library (Cert A2871).

The approved algorithms implemented by the module along with accompanying details are listed in the Table 2-2 below.

Table 2-2: Approved Algorithms

CAVP Cert	Algorithm and Standard	Mode / Method	Description / Key Size(s) / Key Strength(s)	Use / Function
Hashing				
A2871	**Algorithm:** SHA. **Standards:** [FIPS 180-4]	**Methods:** SHA2-256.	N/A.	Only used in conjunction with HMAC-SHA2-256 to: Request an OTP Perform OTP Challenge-Response
Message Authentication Code				
A2871	**Algorithm:** HMAC. **Standard:** [FIPS 198-1]	**Methods:** HMAC-SHA2-256.	**Mac size:** 32 bytes (256 bits). **Key size:** 32 bytes (256 bits).	Request an OTP Perform OTP Challenge-Response

2.5 Non-Approved Algorithms

Non-Approved Algorithms are not available in the Safeword3300 Platinum V2F Cryptographic Module.

3 Cryptographic Module Interfaces

3.1 Interface Overview

The following figure identifies the physical interfaces to the cryptographic module:

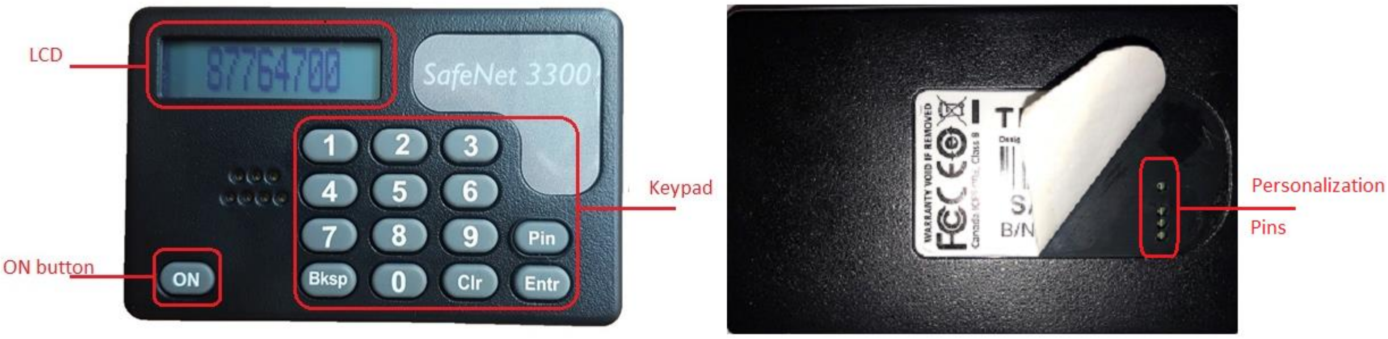

Figure 3-1: Safeword3300 Platinum V2F Cryptographic Module physical interfaces

The following table describes the physical interfaces and supported data:

Table 3-1: Ports and Interfaces

Physical Port	Logical Interface	Data that passes over the port/interface
Keypad	Control Input Data Input	The keypad supports user interaction with the module. **On button**: The device will enter sleep mode after a few seconds of inactivity in order to save power. Pressing the 'ON' button when the device is in sleep mode will put the device in active mode. Pressing the 'ON' button when the device is in active mode will cause it to enter sleep mode. The device is always on and there is no means to turn it off. **Digits (0-9)**: The digit buttons are used to access control features to request display of the hardware and firmware version. For data input, the input characters include digits (0-9). These are entered to request a One-Time Password or initiate a challenge-response.
LCD	Data Output Control Output Status Output	For data output, the display shows up to 8 characters on a single line. The displayed characters include digits (0-9) and letters (A-Z). The interface displays the One-Time Password or challenge-response (data output) as well as hardware and firmware version information (control output). Only approved cryptographic functions are permitted. Therefore, the display implicitly indicates the approved function status. For Control and Status Output, the display shows two lines, with the data type displayed on the first line and the data on the second line. The displayed characters include digits (0-9) and letters (A-Z).

Physical Port	Logical Interface	Data that passes over the port/interface
Personalization Pins (back of the token)	N/A	These are only used during manufacture and are disabled before delivery to the client. The pins neither provide nor accept data.
Power	N/A	Power is provided by an internal battery. The battery is not user replaceable. No interface is available.

4 Roles, Services, and Authentication

4.1 Roles

The Safeword3300 Platinum V2F Cryptographic Module supports the following role:

Table 4-1: Safeword3300 Platinum V2F Cryptographic Module Roles

Role	Principal Duties
Crypto Officer	A single role is provided as the operator of the device. The Crypto Officer can request an OTP, change the owner approval code and view version information.

The mapping of the cryptographic module’s roles to services can be found in the table below:

Table 4-2: Roles, Services, Input and Output

Role	Service	Service Input	Service Output
Management			
Crypto Officer	Change owner approval code	Old code, new code	The code is changed
Crypto Officer	Show module firmware version	Long press on ‘0’ key, short press on ‘1’, ‘4’, ‘5’, ‘8’, and ‘1’.	Firmware version
Crypto Officer	Show module hardware version	Long press on ‘0’ key	Hardware version of the printed circuit board
Crypto Officer	Perform HMAC-SHA2-256 KAT	Long press on ’0’ key, short press on ‘1’, ‘4’, ‘5’, ‘8’, and ‘7’.	Success or Error
Crypto Officer	Perform firmware integrity check	Long press on ’0’ key, short press on ‘1’, ‘4’, ‘5’, ‘8’, and ‘6’.	Success or Error
Crypto Officer	Display Time	Long press on ‘0’ key, short press on ‘1’, ‘4’, ‘5’, ‘8’, and ‘2’.	Displays universal time in seconds (first line) and the user friendly date/time (second line).
Crypto Officer	Display Counter	Long press on ’0’ key, short press on ‘Entr’ to toggle to counter.	Counter value
Crypto Officer	Remove battery	Remove battery	Zeroization of the SSP

Role	Service	Service Input	Service Output
OTP			
Crypto Officer	Request an OTP	Enter owner approval code, select function 1-8	OTP
Crypto Officer	Perform OTP Challenge-Response	Enter owner approval code, select function 9	Response

NOTE Only approved cryptographic functions are supported by the Safeword3300 Platinum V2F Cryptographic Module. The approved security service indicator is implicitly provided by the successful completion of a security service listed in Table 4-3.

NOTE Procedural methods are used to perform zeroization on the Safeword3300 Platinum V2F Cryptographic Module. Zeroization is performed by breaking open the device and removing the battery. Depletion of the battery will also cause the SSPs to be zeroized.

4.2 Authentication

[ISO/IEC 24759:2017] Section 6.4.4, Authentication is not claimed for this device. The operator implicitly assumes the role of Crypto Officer by virtue of physical possession of the device.

4.3 Services

All services listed in the table below can be accessed in approved mode and when in this mode exclusively use the security functions listed in Table 2-2.

As notes on the content of Table 4-3:

> In the “Approved Security Functions” column:

- ‘Algorithms’ maps the target service to cryptography from standards referenced in FIPS 800-140C with corresponding CAVP certificates from Table 2-2;

> In the “Access Rights to Keys and/or SSPs” column:

- G = Generate: The module generates or derives the SSP;
- R = Read: The SSP is read from the module (e.g. the SSP is output);
- W = Write: The SSP is updated, imported, or written to the module;
- E = Execute: The module uses the SSP in performing a cryptographic operation; and
- Z = Zeroize: The module zeroizes the SSP.

For a complete description of the SSP referenced in the “Keys / SSP” column, see Table 9-1.

Table 4-3: Approved Services

Service	Description	Approved Security Functions	Key and/or SSPs	Roles	Access Rights to Keys and/or SSPs
Show module firmware version	This service is used to retrieve the firmware version of the module.	**Algorithms:** N/A	None	Crypto Officer	None
Show module hardware version	This service is used to retrieve the hardware version of the printed circuit board.	**Algorithms:** N/A	None	Crypto Officer	None
Request a OTP [Note 1]	This service is used to request an OTP.	**Algorithms:** HMAC (Cert A2871) – HMAC-SHA2-256 SHA (Cert A2871) – SHA2-256	HMAC key Time	Crypto Officer	**E:** HMAC Key, Time
Perform OTP Challenge-Response[Note 1]	This service is used to perform an OTP challenge-response.	**Algorithms:** HMAC (Cert A2871) – HMAC-SHA2-256 SHA (Cert A2871) – SHA2-256	HMAC key Counter	Crypto Officer	**E:** HMAC Key, Counter **W**: Counter
Change owner approval code	This service is used to change the owner approval code[Note 2].	**Algorithms:** N/A	None	Crypto Officer	None
Perform firmware integrity check	This service allows the operator to initiate the firmware integrity test.	**Algorithms:** N/A	None	Crypto Officer	None
Perform HMAC-SHA2-256 KAT	This service allows the operator to initiate the HMAC KAT self-test.	**Algorithms:** N/A	None	Crypto Officer	None

Service	Description	Approved Security Functions	Key and/or SSPs	Roles	Access Rights to Keys and/or SSPs
Display Time	This service allows the operator to display the device time.	**Algorithms:** N/A	Time	Crypto Officer	**R:** Time
Display Counter	This service allows the operator to display the device's counter.	**Algorithms:** N/A	Counter	Crypto Officer	**R:** Counter

Note 1: In the case where an operator enters an incorrect owner approval code, the device will use the key and random data to create a fake OTP or Challenge-Response. After the third incorrect owner approval code, the device will display the words ‘BAD PIN’. This is displayed for n minutes, where n = (number of incorrect codes -2), and the maximum value of n = 255. It should be noted that this action is not compliant with the protocols in the RFCs referenced in Table 9-1.

Note 2 No security claims are made for authentication using the owner approval code; therefore, no SSPs are mapped to this service.

5 Software/Firmware Security

5.1 Firmware Integrity

The Safeword3300 Platinum V2F Cryptographic Module’s firmware integrity is verified using an Error Detection Code (EDC). This check is performed on all firmware components within the device.

6 Operational Environment

The module supports a **non-modifiable operating environment** as defined in [ISO/IEC 19790:2012]. The device provides no means to load firmware or reconfiguration the device following the completion of the manufacturing process.

7 Physical Security

7.1 Mechanism Summary

7.1.1 Module Construction

The token includes a production grade molded plastic enclosure with no removable parts. A label on the back of the device hides four pins. These pins are used during production and are disabled following personalization.

7.2 Module Inspection

The following routine inspections are recommended.

Table 7-1: Physical Security Inspection Guidelines

Physical Security Mechanism	Recommended Frequency of Inspection/Test	Inspection/Test Guidance Details
Physical inspection of the device.	On receipt of the token; At any point following any un-authorized access to the token; and Following any extended periods of unattended storage.	Verify that the external cover is intact; and All seams, the key pad and the LCD screen are well aligned within the device.

8 Non-invasive security

N/A: Section 6.8, Non-invasive security is Non Applicable as there are currently no requirement in FIPS 800-140F.

9 SSP Management

9.1 Sensitive Security Parameter

The following table lists Sensitive Security Parameters (SSP) used to perform approved security function supported by the cryptographic module.

Table 9-1: SSPs

Key / SSP Name / Type	Strength	Security Function and Cert Number	Import/ Export	Storage	Zeroization	Usage
CSPs						
256-bit HMAC key Function 1	256-bits	HMAC (Cert A2871).	Installed during personalization	Working RAM in plaintext	Zeroized when battery is depleted or removed.	A 256-bit key used to create an HMAC, which is then used to create an OTP in accordance with [RFC 6238].
256-bit HMAC key Function 2	256-bits	HMAC (Cert A2871).	Installed during personalization	Working RAM in plaintext	Zeroized when battery is depleted or removed.	A 256-bit key used to create an HMAC, which is then used to create an OTP in accordance with [RFC 6238].
256-bit HMAC key Function 3	256-bits	HMAC (Cert A2871).	Installed during personalization	Working RAM in plaintext	Zeroized when battery is depleted or removed.	A 256-bit key used to create an HMAC, which is then used to create an OTP in accordance with [RFC 6238].
256-bit HMAC key Function 4	256-bits	HMAC (Cert A2871).	Installed during personalization	Working RAM in plaintext	Zeroized when battery is depleted or removed.	A 256-bit key used to create an HMAC, which is then used to create an OTP in accordance with [RFC 6238].
256-bit HMAC key Function 5	256-bits	HMAC (Cert A2871).	Installed during personalization	Working RAM in plaintext	Zeroized when battery is depleted or removed.	A 256-bit key used to create an HMAC, which is then used to create an OTP in accordance with [RFC 6238].
256-bit HMAC key Function 6	256-bits	HMAC (Cert A2871).	Installed during personalization	Working RAM in plaintext	Zeroized when battery is depleted or removed.	A 256-bit key used to create an HMAC, which is then used to create an OTP in accordance with [RFC 6238].
256-bit HMAC key Function 7	256-bits	HMAC (Cert A2871).	Installed during personalization	Working RAM in plaintext	Zeroized when battery is depleted or removed.	A 256-bit key used to create an HMAC, which is then used to create an OTP in accordance with [RFC 6238].
256-bit HMAC key Function 8	256-bits	HMAC (Cert A2871).	Installed during personalization	Working RAM in plaintext	Zeroized when battery is depleted or removed.	A 256-bit key used to create an HMAC, which is then used to create an OTP in accordance with [RFC 6238].
256-bit HMAC key Function 9	256-bits	HMAC (Cert A2871).	Installed during personalization	Working RAM in plaintext	Zeroized when battery is depleted or removed.	A 256-bit key used to create an HMAC, which is then used to perform a challenge-response in accordance with [RFC 6287] and [RFC 4226].

Key / SSP Name / Type	Strength	Security Function and Cert Number	Import/ Export	Storage	Zeroization	Usage
PSPs						
Counter	N/A	N/A	Starts at zero. Incremented in the CPU, plaintext output using service ‘Display Counter’.	Stored in plaintext in RAM	Zeroized when battery is depleted or removed.	The counter is used in generation of the challenge –response in accordance with RFC 6287 and RFC 4226.
Time	N/A	N/A	Set during personalization. Plaintext output using service ‘Display Time’.	Stored in plaintext in RAM	Zeroized when battery is depleted or removed.	Time is used in generation of the OTP in accordance with RFC 6238.

10 Self-Tests

10.1 Pre-Operational tests

The module performs the pre-operational self-test to confirm the firmware integrity. This test is run at power-up following personalization.

While the module is running the self-test, all interfaces are disabled until the test reaches successful completion. If the test fails, the module halts, and data output is inhibited.

Table 10-1: Pre-operational self-test

Test	Operations Performed	Indicator
Firmware Integrity Test	EDC based on a 16-bit Cyclical Redundancy Check (CRC) calculated on the full code present on the module	Module halt on failure

10.2 Conditional Self-Tests

The module performs a conditional self-test to confirm the proper operation of the cryptographic functions.

While the module is running this self-test, all interfaces are disabled until the test reaches successful completion. If the test fails, the module halts, and data output is inhibited. The KAT is run following the pre-operational firmware integrity test.

Table 10-2: Conditional self-test

Test	Operations Performed	Indicator
HMAC-SHA2-256 KAT	MAC Generate	Module halt on failure

10.3 Periodic Self-Tests

A user may initiate the self-tests on demand for periodic testing of the module. Using the test mode options, the user may initiate the Firmware Integrity Test or the HMAC-SHA2-256 KAT at any time.

10.4 Self-Tests Failure

If a pre-operational or periodic self-test fails, the module will display “BLOCKED” on the screen for a few seconds and then enter sleep mode. The operator may then awaken the device; however, it will display “BLOCKED” on the screen for a few seconds and return to sleep mode.

11 Life-cycle Assurance

11.1 Protecting the Safeword3300 Platinum V2F

In order to maintain security throughout the life of the token, end users MUST:

> securely store the token at all times; and

> always inspect the token prior to use to check for any signs of possible tamper.

Failure of the end user to comply with these requirements could lead to subsequent compromise or malicious misuse of the token.

11.2 Zeroization

Zeroization of the SSPs is performed by breaking open the token and removing the battery. SSPs are exclusively stored in volatile RAM. Removing the battery results in irrecoverable loss of all SSPs.

The operator can verify that the procedure is successful by reattaching the battery and attempting to access the SSPs. It is most likely that the token is beyond repair after battery removal and only a blank screen will appear. In the unlikely event that the battery is reattached successfully and the device powers up, the screen will display ‘NO STATE’ indicating that there are no SSPs present, and the zeroization has been successful.

12 Mitigation of Other Attacks

No assured mitigations to ‘other attacks’ are covered in this security policy.

13 Guidance

The device is always on, but enters a low power consumption mode when not in use. The user must press the ‘ON’ button to exit this mode to make use of any service.

13.1 Identifying the Module Firmware and Hardware Version

Operators are required to verify the module firmware and hardware version prior to first use to ensure that a FIPS-validated cryptographic module is being used in the token.

A long press on the ‘0’ key will display the hardware version. The operator must then put the device into Test Mode by pressing the ‘1’, ‘4’, ‘5’ and ‘8’ buttons in sequence, and then ‘1’ to display the firmware version.

13.2 Approved Mode of Operation

The Safeword3300 Platinum V2F Cryptographic Module has a single mode of operation. This is the approved mode of operation.

13.3 Device Usage

The process to generate an OTP with the Platinum V2 token is as follows:

- The operator of the device initiates the process by pressing the ‘On’ button.
- The “Enter PIN” message is displayed of the screen. The operator enters the owner approval code and it is verified by the device. Note that this is not a cryptographic function claimed for this module.
- The operator must choose the function to execute by entering a number (1-9) after the message ‘HOST’ is displayed.
- Based on the number entered, the module selects the key to be used to generate the OTP. Entering ‘9’ selects the OTP challenge-response service, which prompts the operator to enter a challenge before generating the OTP.
- The OTP is displayed on the screen.

13.4 Status Mode

When in Status Mode, the device shows module information such as the module name. The operator requests Status Mode through a long press on the ‘0’ key.

13.5 Test Mode

From Status Mode, the operator must press the ‘1’, ‘4’, ‘5’ and ‘8’ buttons in sequence to enter Test Mode. The operator can then press ‘1’ to display the module firmware version.

13.6 End of Life

When the device has reached the end of its life, the operator returns the device to the provider for secure destruction. The provider securely destroys the device by breaking open the outer case and removing the battery.