Digipass GO7

FIPS 140-2 Non-Proprietary Cryptographic Module Security Policy

Security Level: 2

Firmware Version: 340106

Security Policy Version: 1.9

Date: 29 November 2022

Table of Contents

1. INTRODUCTION

1.1. Purpose

This document defines the non-proprietary Security Policy for the Digipass GO7 cryptographic module from OneSpan, Inc. hereafter denoted the Module.

The Module is a hardware Time-based One-Time Password (OTP) Token. It supports generating One-Time Passwords according to OneSpan's Digipass algorithms, and according to OATH's HOTP and TOTP standards [HOTP, TOTP].

This Security Policy describes how the Module meets the requirements of Federal Information Processing Standard (FIPS) Publication 140-2 Level 2 requirements.

1.2. Copyright

1.3. References

Table 1 lists the standards referred to in this document.

Table 1: References

Abbreviation	Full Name
[FIPS 46-3]	*Data Encryption Standard (DES)*, October 25, 1999
[FIPS140-2]	*Security Requirements for Cryptographic Modules*, May 25, 2001
[FIPS 180]	*Secure Hash Standard,* August 4, 2015
[FIPS 198]	*The Keyed-Hash Message Authentication Code (HMAC),* July 2008
[HOTP]	*HOTP: An HMAC-Based One-Time Password Algorithm,* December 2005
[SP800-131A]	*Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths*, January 2011
[SP800-108]	*Recommendation for Key Derivation Using Pseudorandom Functions (Revised),* October 2009
[TOTP]	*TOTP: Time-Based One-Time Password Algorithm*, May 2011

1.4. Acronyms

Table 2 defines the acronyms used in this document.

Table 2: Acronyms

Acronym	Definition
AES	Advanced Encryption Standard
CMAC	Cipher-based MAC
CO	Cryptographic Officer
CSP	Critical Security Parameter
ECB	Electronic Codebook mode of operation
EMI	Electromagnetic Interference
EMC	Electromagnetic Compatibility
HOTP	HMAC-based One-Time Password
FIPS	Federal Information Processing Standard
FIPS PUB	FIPS Publication
FW	Firmware
HW	Hardware
KAT	Known Answer Test
KDF	Key Derivation Function
MAC	Message Authentication Code
NIST	National Institute of Standards and Technology
OATH	Initiative for Open Authentication
OTP	One-Time Password
RTC	Real-Time Clock
TOTP	Time-based One-Time Password

2. CRYPTOGRAPHIC MODULE SPECIFICATION

2.1. Module Description

2.1.1 Overview

The Module is a multi-chip standalone embodiment. The hardware part number and firmware version of the Module are as follows:

Table 3: Cryptographic Module Configuration

	Module	Hardware Part Number and Version	Firmware version
1	Digipass GO7	Digipass GO7 FIPS 140-2	340106

The Module is intended for use by US federal agencies and other markets that require FIPS 140-2 validated One-Time Password Tokens.

2.1.2 Module Validation Level

The module is intended to meet requirements of FIPS 140-2 security level 2 overall.

The following table shows the security level for each of the eleven requirement areas.

Table 4: Security Level of Security Requirements

Security Requirement Area	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	3
Mitigation of Other Attacks	N/A

2.2. Cryptographic Boundary

The physical form of the Module is depicted in Figure 1. The colour and text of the enclosure can be different. The options are described in the Appendix of this Security Policy.

The cryptographic boundary is the outer edge of the enclosure which encompasses the entire device.

Figure 1: Cover of Module (front and back)

Table 5 below defines ports and interfaces of the Module.

Table 5: Ports and Interfaces

Port	Description	Logical Interface Type
Push Button	Powers on the module and allows for the selection of OTP to display.	Control in
LCD Display	Displays OTPs, Status, and Error codes.	Data out | Status out
Digipass Initialization Interface	Allows for the loading of the Master Device Key, setting the time, and resetting to factory defaults.	Control in | Data in | Data out | Status out

2.3. Firmware and Logical Cryptographic Boundary

2.3.1 Hardware block diagram

Figure 2 depicts the hardware block diagram of the Module.

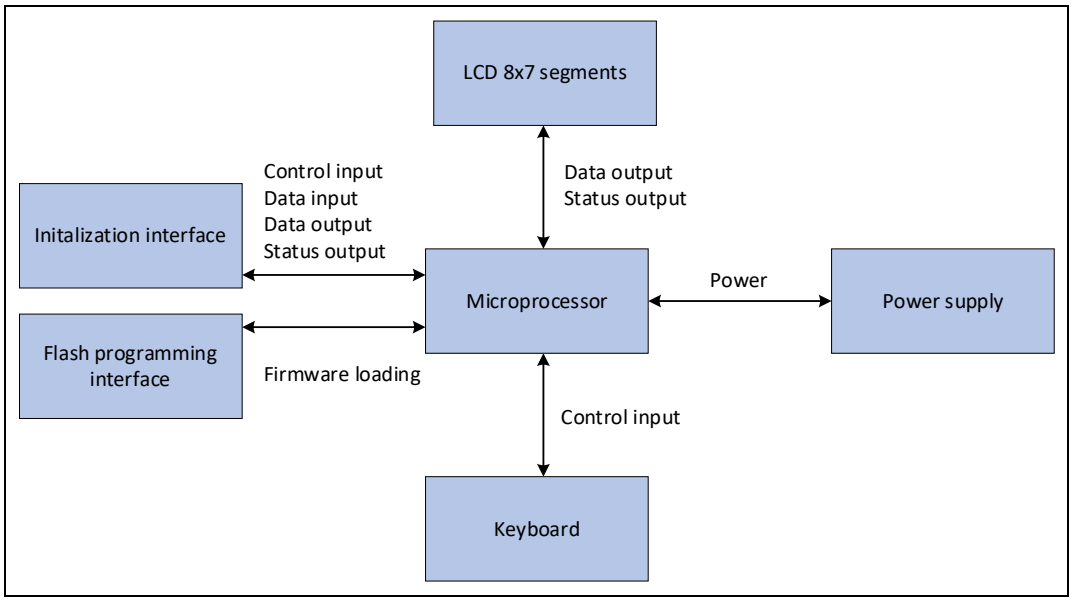

Figure 2: Hardware block diagram of the Module

The Module consists of the following hardware components:

- **Microprocessor**. This is a general-purpose low power micro controller with following main characteristics:
  - 16-bit RISC CPU core
  - 24 KB Flash ROM (program memory)
  - 2 KB embedded RAM (working memory)
  - LCD controller
  - Clocks
  - General purpose I/O ports

  The microprocessor also provides input/output buffers, plaintext/ciphertext buffers, control buffers, key storage.
- **Flash programming interface**. This interface, based on contacts via pins, is used to load the firmware of the Module's microprocessor into its flash memory.
- **Initialization interface**. This interface, based on contacts via pins, is used to load the Module's personalization data (e.g., serial number, cryptographic keys, etc.) into the RAM of the micro controller.
- **Display**. The display consists of an 8-digit seven segment glass LCD panel, directly driven by the micro controller.
- **Power supply**. The micro controller is continuously powered during its complete lifecycle, also during power off, in order to guarantee retention of data in RAM. During power off the voltage is reduced to reduce power consumption.
- **Keyboard**. The keyboard consists of a single button, directly connected to a general- purpose I/O pin.

2.3.2 Logical block diagram

Figure 3 depicts the logical block diagram of the Module. The cryptographic boundary consists of the entire Module.

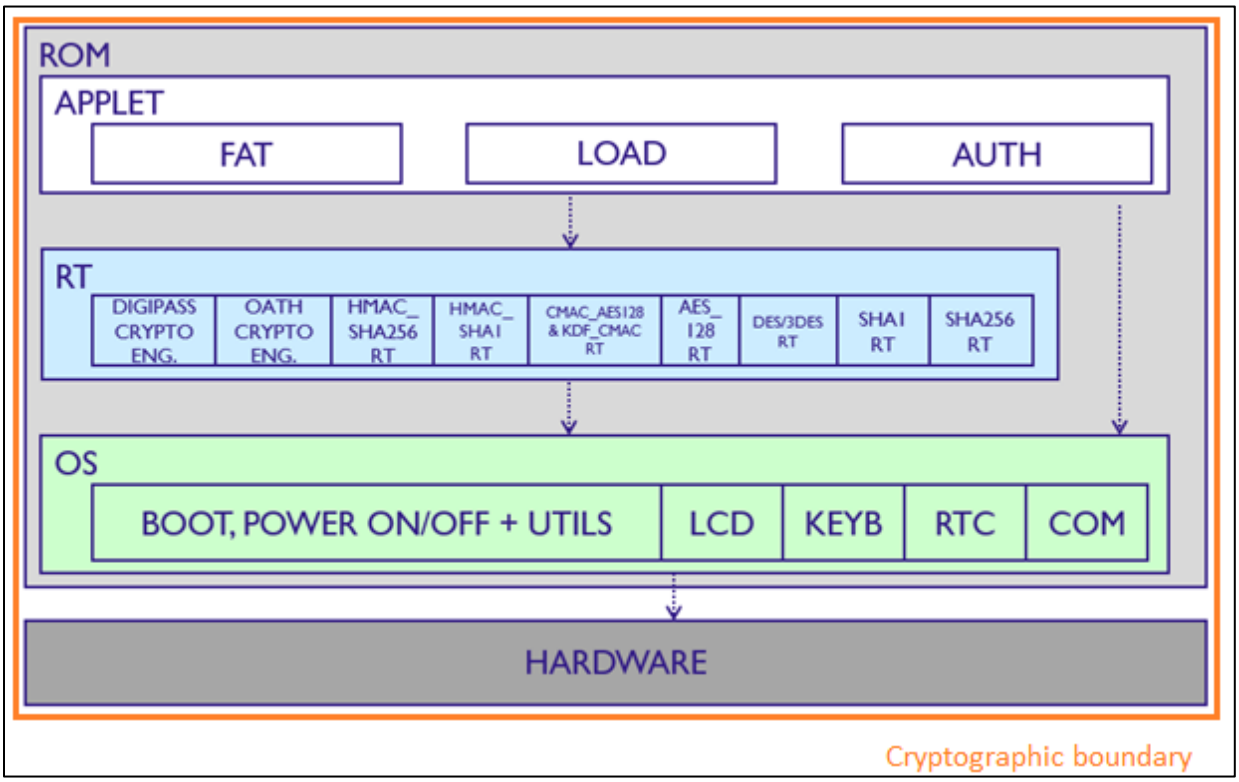

Figure 3: Logical block diagram of the Module

The Module consists of the following logical components:

- **Operating System (OS).** The OS manages the hardware peripherals, the power management and invokes the applets.
- **Runtime (RT) Libraries.** The runtime libraries implement the cryptographic algorithms and the One-Time Password (OTP) algorithm.
- **FAT Applet.** The Factory Acceptance Test Applet is a test application used during production of the Module to check the hardware during different production quality tests.
- **LOAD Applet.** The Load Applet is used during the initialization of the Module in order to load the Module's personalization data (e.g., serial number, cryptographic keys, etc.).
- **AUTHENTICATION Applet.** The Authentication Applet is used by the end-user of the Module to generate One-Time Passwords.

2.4. Mode of Operation

The Module only supports a FIPS approved mode of operation. To verify that a module is in the Approved mode of operation, the user of the Module should verify that the label of the Module contains the hardware part number and firmware version listed in Section 2.1.1.

3. CRYPTOGRAPHIC FUNCTIONALITY

3.1. Cryptographic Functions

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

Table 6: Approved and CAVP Validated Cryptographic Functions

Algorithm	Description	Cert #
AES	Standard: [FIPS 197, SP 800-38A] Functions: Encryption Modes: ECB Key sizes: 128 bits	AES #A2220
AES	CMAC Standard: [SP 800-38B] Functions: Generation Key sizes: AES with 128 bits	AES #A2220
HMAC-SHA-256	Standard: [FIPS 198] Functions: Generation Key size: 256 bits	HMAC #A2220
SHA-256	Standard: [FIPS 180] Functions: Generation	SHA-256 #A2220
KBKDF, using Pseudorandom Functions	Standard: [SP 800-108] Modes: Counter Mode Functions: CMAC-based KBKDF with AES 128 bits	KBKDF #A2220

3.2. Critical Security Parameters

Table 7 below lists and describes all CSPs used by the Module. All usage of these CSPs by the Module (including all CSP lifecycle states) is described in the services detailed in Section 0.

The Master Device Key, Counter and time are loaded into the Module's processor embedded RAM during initialization of the Module.

Table 7: Critical Security Parameters (CSPs)

CSP	Description / Usage	Public	Strength (bits)	Security Function and Cert. Number	Generation	Import/Export	Establishment	Storage	Zeroization
Master Device Key	128-bit AES key, used to derive the Device Authentication Keys and Device Application Keys.	No	128	AES, KBKDF #A2220	Generated outside the Module	Loaded into the Module during the production of the Module by the CO	Not applicable	Permanently stored in obfuscated form in the Module's RAM	Zeroized when the Module is restored to factory defaults, or when power is removed from RAM
Device Authentication Key	128-bit AES key used to authenticate operators once the module is initialized, derived from the Master Device Key. This key is used by the User role.	No	128	AES #A2220	Derived from the Master Device Key by the Module according to [SP800-108]	Not applicable	Not applicable	Temporarily stored in plaintext in the Module's RAM	This key might be overwritten by other data when it is no longer used. It is also zeroized when the Module is restored to factory defaults, or when power is removed from RAM
Device Application Key	Key used to generate One-Time Passwords, derived from the Master Device Key. It is either a 128-bit AES or a 256-bit HMAC-SHA-256 key.	No	128 or 256	AES, HMAC #A2220	Derived from the Master Device Key by the Module according to [SP800-108]	Not applicable	Not applicable	Temporarily stored in plaintext in the Module's RAM	This key might be overwritten by other data when it is no longer used. It is also zeroized when the Module is restored to factory defaults, or when power is removed from RAM

CSP	Description / Usage	Public	Strength (bits)	Security Function and Cert. Number	Generation	Import/Export	Establishment	Storage	Zeroization
Counter	An optional parameter that can be used in the generation of One-Time Passwords. If used, the parameter's value increased by one every time a new One-Time Password is generated by the Module. This parameter's integrity needs to be protected, but not its confidentiality.	Yes	Counter has a length of 32 bits	Not applicable	Generated outside the Module	Loaded into the Module during the production of the Module by the CO	Not applicable	Permanently stored in the Module's RAM	Zeroized when the Module is restored to factory defaults, or when power is removed from RAM
Time from Real-Time Clock (RTC)	The time from the Real-Time Clock (RTC), representing the current UNIX-time, in seconds. This is a parameter that can be optionally used in the generation of	Yes	Not applicable	Not applicable	Generated outside the Module	Loaded into the Module during the production of the Module by the CO	Not applicable	Permanently stored in the Module's RAM	Zeroized when the Module is restored to factory defaults, or when power is removed from RAM

CSP	Description / Usage	Public	Strength (bits)	Security Function and Cert. Number	Generation	Import/Export	Establishment	Storage	Zeroization
	One-Time Passwords. Regardless the fact if this parameter is used or not, the time is updated during each second. This parameter's integrity needs to be protected, but not its confidentiality.								

3.3. Default Authentication Data

The table below lists and describes the Default Authentication Data used by the Module.

Table 8: Default Authentication Data

Data	Description / Usage
FIPS Master Factory Key	128-bit AES key, used to derive FIPS Factory Authentication Key.
FIPS Factory Authentication Key	128-bit AES key used as default authentication data while the module is being initialized, derived from the FIPS Master Factory Key. The FIPS Factory Authentication Key is used by the Cryptographic Officer role, as defined in Section 4.1.

The FIPS Master Factory Key is embedded inside the firmware of the Module and are considered default authentication data. The firmware is stored within the processor, inside the Module's tamper-evident casing.

4. ROLES, SERVICES AND AUTHENTICATION

4.1. Roles

The module supports two distinct operator roles, **User** and **Cryptographic Officer (CO)**. The roles are assumed to be assigned to the same entity. The cryptographic module enforces the separation of roles by restricting one authentication per module power-cycle. Re-authentication under different roles is not supported.

Furthermore, the module restricts the usage of a specific role, depending on the lifecycle state of the module. Generally speaking, there are 2 lifecycle states of the module:

- **Factory State:** the module is in a state in which it contains factory defaults and must be initialized first. This is the typical state of a module during its production in the factory. During this state, the Cryptographic Officer role can be used.
- **Activated State:** the module is initialized and ready to be used by the user. This is the typical state of a module when the production is completed. During this state, the User role is used.

Table 9 lists all operator roles and also the lifecycle-state restrictions for each role, as supported by the Module. The Module does not support a maintenance role and/or bypass capability. The Module does not support concurrent operators. The module clears the authentication state when the module is power cycled.

Table 9: Roles Description

Role ID	Role Description	Authentication Type	Lifecycle-State Restrictions
Cryptographic Officer (CO)	Initialize the module and set the time.	Role-based	Only allowed in Factory State
User	Set the time.	Role-based	Only allowed in Activated State

4.2. Services

The services implemented by the Module and available are listed in the tables below. Each service description describes all usage of CSPs by the service, and lists the approved algorithms used by that service.

Table 10: Authenticated Services

Service	Description	CO (Only in Factory State)	User (Only in Activated State)	Approved algorithms
Authenticate Operator	• For **CO**: Knowledge of the Factory Authentication Key (during initialization), proven by creating an OTP, is required. • For **User**: Knowledge of the Master Device Key (after factory initialization), proven by creating an OTP, is required.	X	X	• KBKDF • AES
Load Master Device Key	Writes the Master Device Key.	X		None
Set time	Sets the time for the module's internal real-time clock.	X	X	None

Table 11: Unauthenticated Services

Service	Description	Approved algorithms
Perform Self-Tests	The Module performs the self-tests and shows the state of the module (uninitialized, error, operational). The self-tests are initiated by powering-up the Module by pressing the Push Button.	• KBKDF • AES • HMAC
Show Status	Retrieves status information from the Module, such as its battery status, current time, counter value, firmware version, and Serial Number. The Module needs to be powered-up first by pressing the Push Button.	None
Generate OTP	• For **Digipass** One-Time Passwords: reads the Master Device Key, derives a Device Application Key, reads the Time, and uses the Device Application Key and Time to calculate a One-Time Password. • For **OATH** One-Time Passwords: reads the Master Device Key, derives a Device Application Key, reads the Time and/or Counter, and uses the Device Application Key and Time and/or Counter to calculate a One-Time Password.	• KBKDF • AES • HMAC
Reset to Factory Defaults	Performs a Hardware (HW) or Software (SW) reset of the module. • A Hardware Reset can be performed by removing the serial number label and access the HW_Reset interface. A shortcut between the Ground- and HW_Reset-pad is sufficient to perform a HW-reset. • A Software Reset can be done by placing the module on a DIGILINK-device and sending a dedicated "RESET" command (see below). The reset destroys all CSPs by writing zeros over the Static RAM locations of the Master Device Key, Device Application Keys, and Device Authentication Keys, and resets the lifecycle-state to Factory State.	None

In order to perform the authenticated services or to perform a Software Reset, the Cryptographic Officer or User uses appropriate software tooling and puts the Module onto a so-called DIGILINK device. Any serial number label present on the Module should be removed before placing the Module onto the DIGILINK device. More specifically the following actions are performed:

- **For Module in Blank/Factory state and CO role**: authenticate towards the module, and load the Master Device Key and set the time of the Module
- **For Module in Activated state and User role**: Authenticate towards the module and change the time of the Module
- **For Module in any state**: perform a Software Reset of the Module

Table 12 defines the relationship between access to CSPs and the different module services. The modes of access shown in the table are defined as:

- Generate (G): The module generates the CSP.
- Read (R): The module reads the CSP. The read access is typically performed before the module uses the CSP.
- Execute (E): The module executes using the CSP.
- Write (W): The module writes the CSP. The write access is typically performed after a CSP is imported into the module, when the module generates a CSP, or when the module overwrites an existing CSP.
- Zeroize (Z): The module zeroizes the CSP.

Table 12: CSP and SSP Access Rights within Services

Service	CSPs				
	Master Device Key	Device Authentication Keys	Device Application Keys	Counter	Time from Real-Time Clock (RTC)
Authenticate Operator	RE	GE			RE
Load Master Device Key	W				
Set Time					W
Perform Self-Tests					
Show Status				R	R
Generate OTP	RE		GE	RWE	RE
Reset to Factory Defaults	Z	Z	Z	Z	Z

4.3. Authentication Methods

The authenticated services described in Section **Error! Reference source not found.** use the following authentication method:

1) The User or Cryptographic Officer obtains the current time from the Module.
2) The User or Cryptographic Officer calculates a One-Time Password by encrypting the time stamp from the Module with AES using the appropriate cryptographic key, and selecting 64 bits from the output of AES. The 4 leftmost bits of the 64-bit One-Time Password are replaced by a time synchronization digit, represented using 4 bits, which is calculated as the remainder of the time stamp mod 10. The time synchronization digit helps the Module to verify the time stamp used by the User or Cryptographic Officer. The cryptographic key is either the FIPS Factory Authentication Key or the Device Authentication Key, and therefore has a length of 128 bits.
3) The User or Cryptographic Officer provides the One-Time Password to the Module.
4) The Module verifies the One-Time Password by repeating the calculation process and verifying whether the provided OTP matches the expected OTP.

The above process takes approximately one (1) second. This amount of time is mainly the result of the speed of the interface that the User and Cryptographic Officer use to communicate with the Module.

The strength of the authentication method is based on the following:

- The usage of AES in the generation of One-Time Passwords ensures that One-Time Passwords are unpredictable and occur with uniform probability.
- The probability to guess a One-Time Password in one (1) attempt equals 1 / 2^60 (i.e. less than 1/1,000,000), as the length of a One-Time Password, excluding the time synchronization digit, equals 60 bits.
- The probability to guess a One-Time Password in one (1) minute equals 60 / 2^60 (i.e. less than 1/100,000).

Note: The security of the module is dependent on controlling access to any copies of the Master Device Key that reside outside of the module. The User or Cryptographic Officer is responsible for ensuring an attacker does not obtain the Master Device Key.

Table 13: Authentication Description

Authentication Method	False Acceptance Probability	Justification
One-Time Password	For one attempt: 1/2^60 (i.e. less than 1/1,000,000)	• The usage of AES ensures One-Time Passwords are unpredictable and occur with uniform probability. • The length of a One-Time Password, excluding the time synchronization digit, equals 60 bits
	For multiple attempts during 60 seconds: 60/2^60 (i.e. less than 1/100,000)	• Same as for one (1) attempt • Additionally, the authentication process takes about one (1) second

5. ELECTROMAGNETIC INTERFERENCE AND ELECTROMAGNETIC COMPATIBILITY

The Module is compliant with Title 47 of the Code of Federal Regulations (CFR) Part 15, Subpart B, Class B (Home use).

6. SELF-TESTS

Each time the Module is powered up, it tests that the cryptographic algorithms still operate correctly and that the module has not been modified. Power up self–tests are available on demand by power cycling the module.

On power up or reset, the Module performs the self-tests described in Table 14 below. All KATs must be completed successfully prior to any other use of cryptography by the Module. If one of the KATs fails, the Module enters the error state.

Table 14: Power Up Self-tests

Test Target	Description
Firmware Integrity	16-bit checksum calculation and verification over the ROM-mask firmware code
Firmware Integrity	16-bit checksum calculation and verification over the Non-Volatile Storage (NVS) patch firmware code
CMAC-based KBKDF with AES 128 bits	KAT: Counter Mode with CMAC AES, including Include CMAC generate and AES ECB encrypt self-test. Key size: 128 bits
HMAC-SHA256	KAT: HMAC Generation which includes SHA-256 Key size: 256 bits

7. PHYSICAL SECURITY POLICY

The Module is a multi-chip stand-alone module that is housed in a production grade plastic enclosure. The parts of the enclosure are shear welded together, so they are non-removable. Any attempts to open the enclosure will show clear tamper evidence. In the event of tamper evidence, please contact the organization or company that provided the Module immediately.

Table 15: Physical Security Inspection Guidelines

Physical Security Mechanism	Recommended Frequency of Inspection/Test	Inspection/Test Guidance Details
Enclosure	Upon every usage of the device	Verify that the enclosure is intact and the token does not show evidence of prying or cutting attempts. Verify that the size of the holes, covered by the label at the back of the Module, has not increased, as this would provide evidence of tampering.

8. OPERATIONAL ENVIRONMENT

The Module is designated as a non-modifiable operational environment under the FIPS 140-2 definitions. The Module does not support loading new firmware.

9. MITIGATION OF OTHER ATTACKS POLICY

The module does not implement mitigation of other attacks.

10.SECURITY RULES AND GUIDANCE

The Module design corresponds to the Module security rules. This section documents the security rules enforced by the cryptographic module to implement the security requirements of this FIPS 140-2 Level 2 module.

The Module enforces following security rules:

1. The module provides two distinct operator roles: User and Cryptographic Officer.
2. The module provides role-based authentication.
3. The module clears previous authentications on power cycle.
4. When the module has not been placed in a valid role, the operator can use the Module to generate One-Time Passwords.
5. The operator shall be capable of commanding the module to perform the power up self-tests by cycling power or resetting the module.
6. Power up self-tests do not require any operator action.
7. Data output shall be inhibited during key generation, self-tests, zeroization, and error states.
8. Status information does not contain CSPs or sensitive data that if misused could lead to a compromise of the module.
9. There are no restrictions on which keys or CSPs are zeroized by the zeroization service.
10. The module does not support concurrent operators.
11. The module does not support a maintenance interface or role.
12. The module does not support manual key entry.
13. The module has external input/output devices used for entry/output of data.
14. The module enters plaintext CSPs.
15. The module does not output plaintext CSPs, except for the Counter and time.
16. The module does not output intermediate key values.
17. The Cryptographic Officer must ensure that the Master Device Key provides 128 bits of security strength.

11.APPENDIX

11.1.Module enclosures

This Appendix lists the various enclosures in which the module is available. The following options exist:

1. The back enclosure of the module can contain the text "OneSpan.com", or the text "www.vasco.com" and two US patent numbers.
2. The enclosure is available in three colours (white, blue, and black).

In addition, the enclosure might contain additional text or logos referring to the customer. The lens (which is present on top of the front enclosure) might be available in other colours and might contain text.

The figures below depict the various options for the enclosure. The lens is depicted in grey in all pictures.

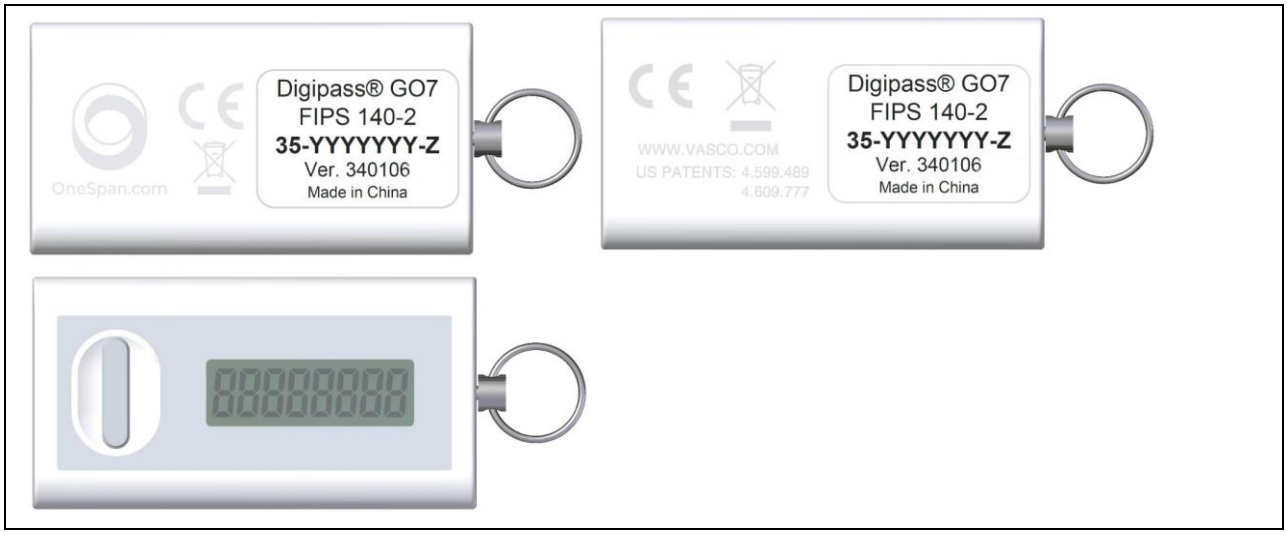

Figure 4: White enclosure (two options for back, and front)

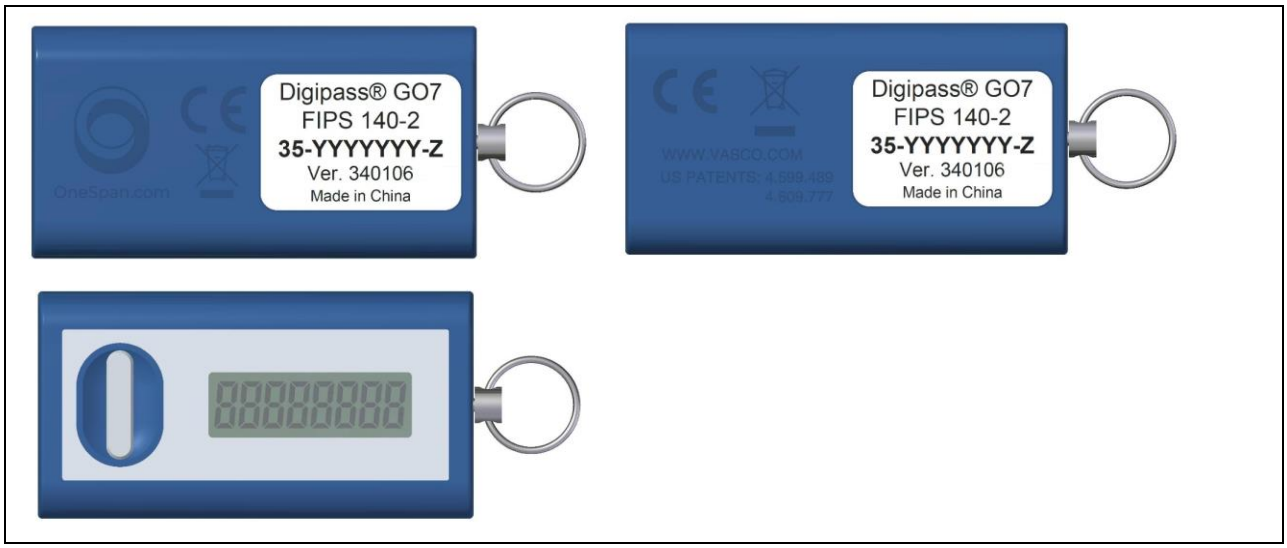

Figure 5: Blue enclosure (two options for back, and front)

Figure 6: Black enclosure (two options for back, and front)

11.2. Interfaces involved in Module's services

This section details physical and logical interfaced involved in the various services of the Module. More specifically, Table 16 specifies the following:

- The physical component involved in transit of data related to the service, and
- The physical component involved in storage of data related to the service, and
- The logical interface involved in the service.

Table 16: Data path for Module's services

Service	Physical component transit	Physical component storage	Logical interface
Authenticate Operator	Initialization Interface	RAM of processor	LOAD_Applet : Digilink command DL MSG 8: (MSG_FIPS_EXTERNAL_AUTHENTICATE)
Load Master Device Key	Initialization Interface	RAM of processor	LOAD_Applet: 4 Digilink commands are needed: • DL MSG 3: (MSG_SECZ) • DL MSG 4: (MSG_MULTI_OTP_APPZ1) • DL MSG 5: (MSG_MULTI_OTP_APPZ2) • DL MSG 6: (MSG_MULTI_OTP_APPZ3) Each command writes a part of the key.
Set time	Initialization Interface	RTC of processor	LOAD_Applet. : Digilink command DL MSG 7: (MSG_FIPS_UPDATE_TIME)
Perform Self-Tests	Button	Not applicable	Not applicable
Show Status	• Button and display, or • Initialization Interface	RAM	• AUTH_Applet:Extra Function Menu, or • LOAD_Applet. Digilink command DL MSG 0: (TEST)
Generate OTP	Button and display	RAM, and optionally RTC of processor	AUTH_Applet:Calculate and Display Appli OTP(n)
Reset to factory defaults	• Initialization interface, or • Initialization interface	RAM and RTC of processor	• LOAD_Applet. Digilink command DL MSG 1:(RESET), or • LOAD_Applet. Digilink command DL MSG 1:(RESET)

OneSpan is a global leader in delivering trust and business productivity solutions to the digital market. OneSpan develops next generation technologies that enable more than 10,000 customers in 100 countries in financial, enterprise, government, healthcare and other segments to achieve their digital agenda, deliver an enhanced customer experience and meet regulatory requirements. More than half of the top 100 global banks rely on OneSpan solutions to protect their online, mobile, and ATM channels. OneSpan's solutions combine to form a powerful trust platform that empower businesses by incorporating identity, fraud prevention, electronic signatures, mobile application protection and risk analysis. Learn more at **OneSpan.com**.

Last Update June 2018