VASCO Data Security International, Inc.

DIGIPASS GO-7

FIPS 140-2 Non-Proprietary Cryptographic Module Security Policy

Security Level: 2

Version: 1.7

Date: August 12, 2015

Table of Contents

List of Figures

List of Tables

1 Introduction

1.1 Purpose

This document defines the non-proprietary Security Policy for the DIGIPASS GO-7 cryptographic module from VASCO Data Security International, Inc. hereafter denoted the Module.

The Module is a hardware Time-based One-Time Password (OTP) Token.

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 Security Policy.

Table 1: References

Abbreviation	Full Name
[FIPS140-2]	*Security Requirements for Cryptographic Modules*, May 25, 2001
[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*

1.4 Acronyms

Table 2 defines the acronyms found in this document.

Table 2: Acronyms

Acronym	Definition
AES	Advanced Encryption Standard
CMAC	Cipher-based MAC
CO	Cryptographic Officer
ECB	Electronic Codebook mode of operation
EMI	Electromagnetic Interference
EMC	Electromagnetic Compatibility
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
OTP	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 GO-7	DIGIPASS GO-7 FIPS 140-2	0355

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 Hardware and Physical Cryptographic Boundary

The physical form of the Module is depicted in Figure 1. 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.

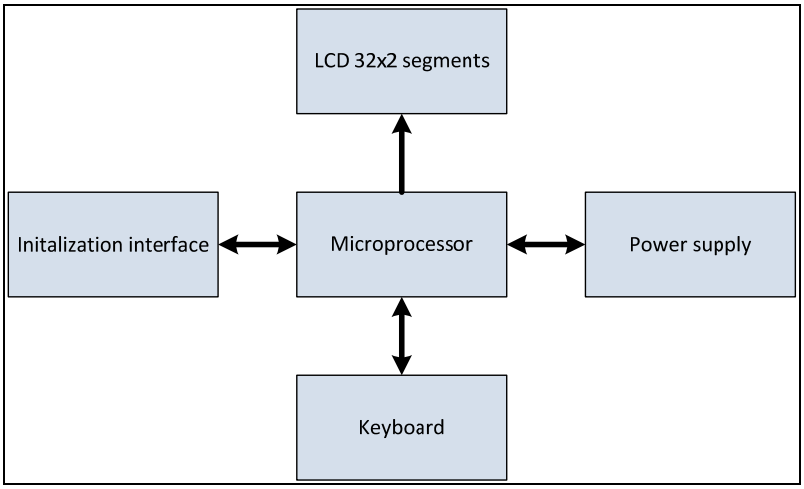

Figure 2: Hardware block diagram of the Module

The Module consists of the following hardware components:

- **Microprocessor**. This is a general-purpose low power micro controller with following characteristics:
  - 4 Kbyte One-Time-Programmable code memory
  - 128 bytes static RAM
  - LCD controller
  - Clocks
  - General purpose I/O ports
- **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.

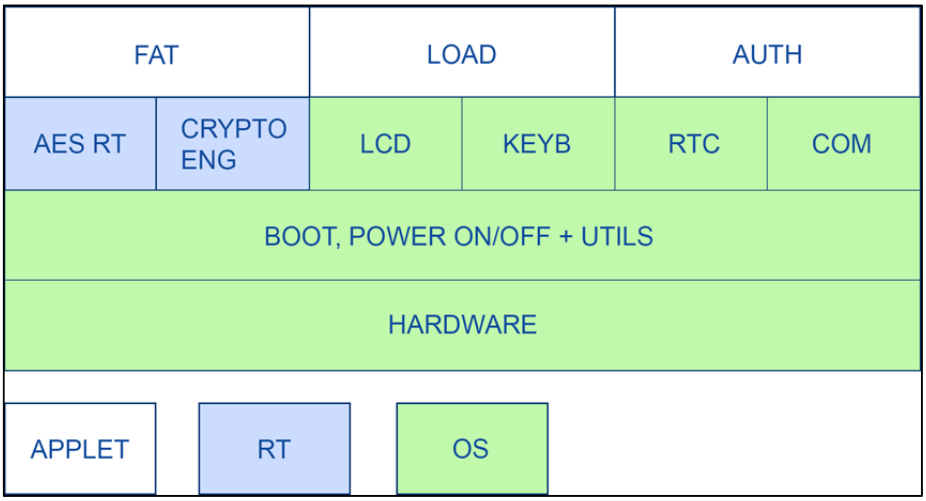

Figure 3: Logical block diagram of the Module

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 to generate One-Time Passwords.

2.4 Mode of Operation

The Module only supports an 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 following 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 #3216
AES	CMAC Standard: [SP 800-38B] Functions: Generation Key sizes: AES with 128-bits	AES #3217
KDF, using Pseudorandom Functions	Standard: [SP 800-108] Modes: Counter Mode Functions: CMAC-based KDF with AES 128-bits	KBKDF #44

3.2 Critical Security Parameters

The table 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 4.

Table 7: Critical Security Parameters (CSPs)

CSP	Description / Usage
Master Device Key	128-bit AES key, used to derive the Device Authentication Key and Device Application Keys.
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 and the Cryptographic Officer role, as defined in Section 4.1.
Device Application Key	128-bit AES keys used to generate One-Time Passwords, derived from the Master Device Key.

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

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 reset. Re-authentication is not supported.

Table 9 lists all operator roles 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	Authentication Data
Cryptographic Officer (CO)	Initialize the module and set the time.	Role-based	Knowledge of the Factory Authentication Key (during initialization) or Master Device Key proven by creating an OTP
User	Set the time.	Role-based	Knowledge of the Factory Authentication Key (during initialization) or Master Device Key proven by creating an OTP

The Factory Authentication Key is embedded inside the firmware of the Module and is considered default authentication data. The firmware is stored within the processor, inside the Module's tamper-evident casing. The Master Device Key is loaded into the Module's processor RAM during initialization of the Module.

4.2 Services

All services implemented by the Module are listed in the tables below. Each service description also describes all usage of CSPs by the service.

Table 10: Authenticated Services

Service	Description	CO	User
Authenticate Operator	Knowledge of the Factory Authentication Key (during initialization) or Master Device Key proven by creating an OTP	X	X
Load Master Device Key	Writes the Master Device Key.	X	X
Set time	Sets the time for the module's internal real-time clock.	X	X

Table 11: Unauthenticated Services

Service	Description
Power-Up Module / Execute Self-Tests / Show Status	Power-up the module by pressing the Push Button. The module performs the self-tests and shows the state of the module (uninitialized, error, operational).
Retrieve Module status	Retrieves status information from the Module, such as its battery status, current time, firmware version, and Serial Number.
Generate OTP	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.

Service	Description
Reset to Factory Defaults	Destroys all CSPs by writing zeros over the Static RAM locations of the Master Device Key, Device Application Keys, and Device Authentication Keys.

In order to perform the authenticated services, the Cryptographic Officer or User puts the Module onto a so-called DIGILINK device. This device is used to load the Master Device Key and set the time 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
Authenticate Operator	RE	GE	
Load Master Device Key	W		
Set Time			
Power Up Module / Execute Self-Tests / Show Status			
Retrieve Module status			
Generate OTP	RE		GE
Reset to Factory Defaults	Z	Z	Z

4.3 Authentication Methods

Both authenticated services described in Section 4.2 use 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. 4 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 Factory Authentication Key or the Device Authentication Key, and therefore always 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, 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.

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	• 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	• Same as for one (1) attempt • Additionally, the authentication process takes about one (1) second

5 Electromagnetic Interference/Electromagnetic Compatibility (EMI / EMC)

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 performed over all code.
KDF, using Pseudorandom Functions	KATs: CMAC Generation which includes AES ECB Encrypt. Key size: 128-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.
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.

