GoldKey Security Token Cryptographic Module

FIPS 140-2 Security Policy

Version 1.10

Last Update: May 2, 2019

[1]

CybrSecurity Corporation
10220 North Ambassador Drive, Kansas City, MO 64153, USA

[1] The actual module is a single chip within the depicted package

Table of Contents

Trademarks

GoldKey is a registered trademark of **CybrSecurity Corporation.**

1. Introduction

This document is the non-proprietary FIPS 140-2 Security Policy for the GoldKey Security Token Cryptographic Module. It contains a specification of the rules under which the module must operate and describes how this module meets the requirements as specified in FIPS PUB 140-2 (Federal Information Processing Standards Publication 140-2 FIPS PUB 140-2 CHANGE NOTICES (12-03-2002)) for a Security Level 2 single-chip standalone cryptographic module.

1.1. Purpose of the Security Policy

There are two major reasons that a security policy is needed:

- To provide a specification of the cryptographic security that will allow individuals and organizations to determine whether a cryptographic module, as implemented, satisfies a stated security policy.
- To describe to individuals and organizations the capabilities, protection, and access rights provided by the cryptographic module, thereby allowing an assessment of whether the module will adequately serve the individual or organizational security requirements.

1.2. Target Audience

This document has the following audience:

- Administrators of the cryptographic module
- Those specifying cryptographic module
- Users of the cryptographic module.

2. Cryptographic Module Specification

2.1. Module Overview

The following table shows the security level claimed for each of the eleven sections that comprise the FIPS 140-2:

FIPS 140-2 Sections		Security Level				
		N/A	1	2	3	4
1	Cryptographic Module Specification			✓		
2	Cryptographic Module Ports and Interfaces			✓		
3	Roles, Services and Authentication			✓		
4	Finite State Model			✓		
5	Physical Security				✓	
6	Operational Environment	✓				
7	Cryptographic Key Management			✓		
8	EMI/EMC				✓	
9	Self-Tests			✓		
10	Design Assurance				✓	
11	Mitigation of Other Attacks	✓				

Table 1: Security Levels

The overall security level for the cryptographic module is security level 2. The GoldKey Security Token Cryptographic Module (referred to hereafter as “GoldKey”) is a single chip cryptographic module capable of protecting information on a user’s computer or network storage. The protected data can only be accessed if the correct GoldKey is attached to the computer and the authorized user is authenticated by the GoldKey device. This product also allows secure authentication and communication over the network or Internet. In addition, it offers the full capabilities of a PIV smart card, including provisioning and use of the PIV digital credentials on the GoldKey.

2.2. Description of Module

The GoldKey hardware is a customized Security Controller Chip. The chip is housed in a standard surface-mount IC package (64-pin QFN). This chip includes an Arca2S 32-bit RISC processor, which executes the GoldKey firmware. All the memory for the firmware execution and code storage is included within the chip.

The module component list of the GoldKey is specified in the following table:

Component Type	Part Number or File Name and Version with Description
Hardware	GoldKey USB Security Token Controller IC: USB-CONTROLLER-2LF Processor: Arca2S 32-bit RISC
Firmware	Binary image of the module: goldkey.bin v7.13
Documentation	Security Policy: GoldKey_SP_v1.10.pdf
	GoldKey User Manual: GoldKeyManual.pdf v7.1
	Finite State Model: GoldKey_FSM_v1.1.docx
	GoldKey API Specification: GoldKey_API_Spec_v1.0.docx
	GoldKey Master Component List: GoldKey_Master_Comp_List_v1.4.docx
	GoldKey Firmware Design Document: DesDoc_GoldKeyFirmware 7.doc

Table 2: GoldKey Security Token Cryptographic Module Components

Note: For source code associated with GoldKey Cryptographic Library V7.13 and the Master Component List, please refer to the GoldKey Security Token Configuration Output Detail List documented in GoldKey_Master_Comp_List_v1.4.docx.

2.3. Modes of Operation

The GoldKey supports FIPS approved and Non-approved modes of operation. After completing all the self-tests, the module enters FIPS mode without any operator intervention. The module implicitly transitions to Non-approved mode if the RSA algorithm with 1024-bit key size is requested, which is the only non-approved algorithm for this module.

The GoldKey provides the following FIPS 140-2 Approved algorithms:

Algorithm and CAVS cert #	Description	Use
DRBG cert #297	SP 800-90A CTR_DRBG, AES-256 (seeded with the hardware NDRNG)	Random Number Generation
AES cert #2347	FIPS 197 AES-256, CBC, CTR, and ECB modes	Encrypt/Decrypt
Triple-DES cert #1470	SP 800-67 Three-Key, Triple-DES, ECB and CBC modes	Encrypt/Decrypt
RSA CVL cert # 234	FIPS 186-4 RSA PKCS#1 v2.1 2048-bit Modulus (External Hash)	Signature Primitive RSASP1
RSA cert #1210	FIPS 186-4 RSA Key Generation, 2048-bits	KEY(gen)
ECDSA cert #384	FIPS 186-4 ECDSA, P-256 and P-384 Curves (External Hash)	SIG(gen) KEY(gen)
ECDSA CVL cert # 235	FIPS 186-4 ECDSA SigGen Component: CURVES (P-256 P-384)	Signature Generation of hash sized messages
EC Diffie-Hellman CVL cert # 54	SP 800-56A All of SP800-56A EXCEPT KDF	Shared Secret Computation
SHA cert #2024	FIPS 180-4 SHA-256	Secure Hash

Table 3: FIPS Approved Algorithms

2.4. Cryptographic Module Boundary

2.4.1. Hardware block diagram

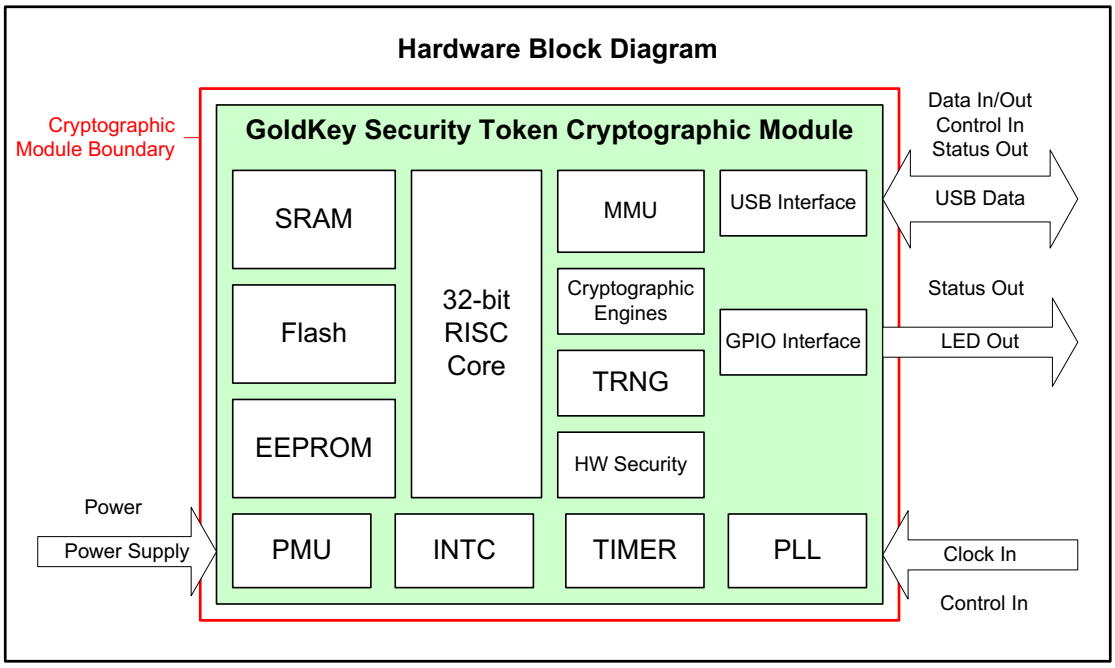

Figure 1: Hardware Block Diagram

Both the physical and logical cryptographic boundaries of the GoldKey Security Token Cryptographic Module are defined as the IC package.

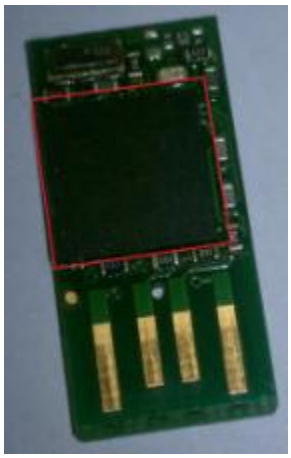

Figure 2: Physical Module Boundary

Figure 2 shows the physical module within the red outline.

3. Cryptographic Module Ports and Interfaces

FIPS 140-2 Required Logical Interface	GoldKey Physical Ports	USB Data Command Fields
Data Input	USB Data (DM, DP)	Command Data Field
Data Output	USB Data (DM, DP)	Response Data Field
Control Input	USB Data (DM, DP), Clock In (XIN, XOUT), Mode[0:2], POR	CLA, INS, P1, P2n, Lc, Le
Status Output	USB Data (DM, DP), LED Output (LED Out)	SW1, SW2
Power Input	Power Supply (VDD5, VSS)	

Table 4: Ports and Interfaces

The GoldKey Status can be determined by the "LED Out" status output. When connected to an external LED circuit the status is indicated as follows:

LED State	Status	Mode of Operation
Off	Power Off	Off
On	Operational	FIPS Approved or Non Approved depending on the requested service
Slow Blink	Active (indicates cryptographic operation in process)	FIPS Approved or Non Approved depending on the requested service
Fast Blink	Error	Error

Table 5: LED Status

4. Roles, Services and Authentication

4.1. Roles and Authentication Mechanism

GoldKey supports role based authentication.

User Roles	Authentication Criteria/Mechanism	Description
Registered Master	Registered Secret	The Registered Master is the Cryptographic Officer role. This role is responsible initialization and management functions of the GoldKey.
Non-Registered Master	Registration Secret	The Non-Registered Master role can perform a limited set of management functions on the GoldKey, which includes key zeroization and registering a GoldKey to become the Registered Master.
PIV Administrator	Card Management Key (CMK)	The PIV Administrator role is the PIV Card Administrator defined in the PIV specification. This role is responsible for configuration of the PIV data using the PIV services.
User	User PIN	The primary User role. This role is assumed to perform general security services, including cryptographic operations and remote authentication.
Owner	User PIN, Personal Question Answer (PQA)	The Owner role is assumed to perform limited management functions that are available to the user, such as changing the PIN and PQA.
PIN Unblock	PIN Unblock Key (PUK)	The PIN Unblock User role is used for PIV applications and is associated with the RESET RETRY COUNTER service.

Table 6: Roles

This Module uses password authentication for the verification of the User, Owner, and PIN Unblock User, and symmetric-key authentication for verification of the Registered Master, PIV Administrator, and Non-Registered Master roles. Please refer to the above table for the authentication criteria of each role. The module ensures that there is no visible display of the authentication data, such as User PIN. All authentication status related information is stored in the RAM area and this information is cleared when the module is powered off.

The strength of various CSPs used in the authentication mechanism is discussed below.

The User PIN used for authentication of the User and Owner roles must be in the range of 4-8 characters. The minimum length of a Personal Question Answer (PQA) is four (4) characters.

The User PIN and the Personal Question Answer may contain a mix of alphabet letters, numeric characters, and special characters. Assuming a mix of lower case alphabet letters, upper case alphabet letters, and numeric characters, the User PIN/PQA can consist of the following set: [a-z, A-Z, 0-9, 33 special characters], yielding 95 choices per character.

The total number of possibilities for guessing the User PIN/PQA is 95^4 = 81450625.

The probability of a successful random attempt is 1/81450625, which is less than 1/1,000,000.

Please note that the module will lock an account after, at most, ten consecutive failed authentication attempts.

The Card Management Key (CMK) is a Triple-DES key. This key is used for challenge/response authentication of the PIV Administrator role. The minimum length of the CMK is 48 hexadecimal characters. The probability of guessing the CMK key will be same as guessing a 192 bits Triple-DES key. A Triple-DES key of size 192 bits provides 112 bits of security.

The minimum length of the PIN UNBLOCK Key (PUK) is 4 ASCII (entered in hexadecimal), yielding 255 choices per character.

The total number of possibilities for guessing the PUK is $255^4 = 4228250625$.

The probability of a successful random attempt is 1/4228250625, which is less than 1/1,000,000.The Registered Secret and Registration Secret, used for authentication of the Registered and Non-registered Master roles, are 256-bit AES keys. The probability of guessing these keys will be same as guessing a 256-bit AES key. An AES key of size 256 bits provides 256 bits of security.

4.2. Services

The following table shows all the cryptographic algorithms implemented by the module along with corresponding roles, CSPs, modes of the algorithm and access rights:

Service	Roles	CSP	Modes	FIPS Approved (cert #)	Access	Notes
Symmetric Algorithms						
AES Encryption and Decryption	User, Registered Master, Non-registered Master	256-bit AES Key	ECB, CBC, CTR	Yes, cert #2347	W, X	FIPS 197
Triple-DES 3-Key Encryption and Decryption	All Roles	192-bit TDES Key	ECB, CBC	Yes, cert #1470	W, X	SP 800-67; Used for challenge/ response authentication of PIV Admin
Asymmetric Algorithms						
RSA key Generation	Registered Master, PIV Admin	RSA Private Key	2048-bit key size	Yes, cert #1210	W	FIPS 186-4
RSA Signature Generation	All Roles	RSA Private Key	PKCS#1 v2.1 (External Hash)	Yes, (2048-bit only) CVL cert #234	X	FIPS 186-4
ECDSA Key Generation	Registered Master, PIV Admin	ECC Private Key	P-256, P-384 Curves	Yes, cert #384	W	FIPS 186-4
ECDSA Signature Generation	All Roles	ECC Private Key	P-256, P-384 Curves (External Hash)	Yes, cert #384	X	FIPS 186-4

Service	Roles	CSP	Modes	FIPS Approved (cert #)	Access	Notes
ECDSA Signature Generation of hash sized messages	All Roles	ECC Private Key	SigGen Component: CURVES (P-256 P-384)	Yes, CVL cert #235	X	FIPS 186-4
Hash Functions						
SHA-256	All Roles	N/A	N/A	Yes, cert #2024	X	FIPS 180-4; Used internally by Firmware for integrity check
Random Number Generation						
DRBG	All Roles	V, seed, Key	AES-256 No derivation function	Yes, cert #297	X	SP 800-90A CTR_DRBG, AES-256 (seeded with the hardware NDRNG); Key generation
NDRNG	All Roles	Seed, Seed key	N/A	N/A	W	Hardware-based NDRNG, which supplies Seed to the DRBG
Shared Secret Computation						
EC Diffie-Hellman	All Roles	ECC Private Key	P256, P384 Curves	Yes, CVL cert #54	X	SP 800-56A (EC Diffie-Hellman Primitive Only)
Non approved algorithm						
RSA key Generation	Registered Master, PIV Admin	RSA Private Key	1024-bit key size	cert #1210	W	Due to transitions in SP 800-131A, the validation with 1024 bits is no longer approved.

Users should refer to SP 800-131-A for the validity of the algorithms and key sizes over time.

Table 7: Algorithms

The following table shows services and APDU commands offered by the module, their description, corresponding roles, and the associated Keys/CSPs.

Services/APDU Commands	Description	Roles	Keys/CSPs
Module Initialization	Initializes module	N/A (module initializes before the roles are authenticated)	N/A
Self-Test	Performs self-test	N/A (module performs self-tests before the roles are authenticated)	N/A
Show Status	Determines the status of the module by observing the LEDs	N/A (Does not require authentication)	N/A
RAM Zeroization	Zeroizes all CPSs from RAM	All Roles	All applicable CSPs
SELECT	Used for identification of GoldKey device by the OS	N/A (Does not require authentication)	N/A
GET DATA	Used for operations that read public data from the GoldKey, including: any operation that displays public GoldKey info. Please refer to the design specification document for a listing of data objects within the GoldKey.	N/A (Does not require authentication)	N/A
VERIFY	Used to verify a password, such as the PIN or personal question answer. This command is used to authenticate the User and Owner Roles.	N/A (Does not require authentication)	User PIN, Personal Question Answers
CHANGE REFERENCE DATA	Used for operations that write/change CSPs in the GoldKey, including: Master registration and management operations, GoldKey personalization, change PIN or PUK, and importing private keys.	Registered Master	All (except CSPs that can only be written at Factory). The complete list of CSPs is provided in section 8.
		Non-registered Master	Group Secrets, Registered Secret (AES keys (256-bit))
		Owner	User PIN, PQA

Services/APDU Commands	Description	Roles	Keys/CSPs
		PIV Admin	ECDSA Keys, RSA Keys, EC Diffie-Hellman Keys
	Used to change the PIN or PUK after verifying the current PIN/PUK	N/A (Does not require authentication)	User PIN, PIN Unblock Key (PUK)
	Used to zeroize CSPs stored in NV memory	Registered Master, Non-registered Master	All (except CSPs that can only be written at Factory)
RESET RETRY COUNTER	Used to reset a PIN, using the PIN Unblock Role	PIN Unblock User	User PIN, PIN Unblock Key (PUK)
GENERAL AUTHENTICATE	Used for challenge/response and public/private key operations including: authentication of the PIV Admin role, and signature generation.	N/A (Does not require authentication)	CMK (Triple-DES 192 bits), Card Authentication Key (RSA 2048, ECC P256/P384 Private Key), Remote Approval Key(AES key (256 bits)) Session Secret (generated by ASSOCIATE command) (AES key (256 bits))
		User	All Private Keys (RSA 2048, ECC P256/P384), except Card Authentication Key
PUT DATA	Used for any operation that writes data objects to the GoldKey, including: registering GoldKey, personalizing GoldKey, and PIV provisioning. Refer to the design specification document for a listing of data objects within the GoldKey.	Owner, PIV Admin, Registered Master	N/A
GENERATE ASYMMETRIC KEY	Used to generate and save a new public/private key pair (RSA 2048 and ECC P256/P384 are supported).	PIV Admin, Registered Master	Private Keys (RSA 2048, ECC P256/P384)
RANDOM	Used for operations that require random data, including: Network authentication, and creating a Secure Drive.	N/A (Does not require authentication)	DRBG V, seed, key

Services/APDU Commands	Description	Roles	Keys/CSPs
UVS RESET	Used to un-authenticate the current role after performing an authenticated operation. It can also be used to output current authentication status.	N/A (Does not require authentication)	N/A
ASSOCIATE	Used to set up a secure channel, for operations including: Authentication of the Registered and Non-registered Master roles, network authentication, external data encryption/decryption. Generates a session secret that can be used by other commands (stored in RAM). For detailed information refer to the design specification.	N/A (Does not require authentication)	Remote Approval Key (Sacred Secret), Registration Secret, Registered Secret, Session Secret (generated by ASSOCIATE command), (AES keys (256 bits))
		Any* (except PIN Unblock Role)	All AES keys (other than above) (256 bits) *Required role for each key can be set when key is written.
PROVE ID	Used to generate an Identifier Proof for setting up a network authentication (used for accessing GoldKeyVault and other servers that support "GoldKey Secure Web Login"). For detailed information please refer to the design specification.	N/A (Does not require authentication)	Session Secret (generated by ASSOCIATE command) (AES key (256 bits))
SECURE CMD	Used as a gateway to perform other commands through a secure channel. This is used for operations including: Master registration and management, and GoldKey personalization. For detailed information please refer to the design specification.	N/A (Does not require authentication)	Session Secret (generated by ASSOCIATE command) (AES key (256 bits))
Non Approved Services			
GENERATE ASYMMETRIC KEY	Used to generate and save a new public/private key pair for RSA 1024.	PIV Admin, Registered Master	Private Key (RSA 1024)
GENERAL AUTHENTICATE	Used for challenge/response and public/private key operations including: authentication of the PIV Admin role, and signature	N/A (Does not require authentication)	Card Authentication Key (RSA 1024)

Services/APDU Commands	Description	Roles	Keys/CSPs
	generation.	User	Private Key (RSA 1024), except Card Authentication Key
CRYPTO	Used for AES-256 data Encryption/Decryption and key wrapping. For detailed information please refer to the design specification.	N/A (Does not require authentication)	Session Secret (generated by ASSOCIATE command) (AES key (256 bits))

Table 8: Services

5. Physical Security

The module is a single-chip standalone module and conforms to Level 3 requirements for physical security.

The module is completely enclosed within the external GoldKey case (please see the cover page of this document for a picture of the GoldKey). It is a single chip encased in a standard black, opaque epoxy IC package that prevents any access to the interior of the module (please see Figure 2). It is never visible to the user if the module is un-tampered. If the external case has been cut open or removed, the user is cautioned that the module may have been compromised and should return the module to a security administrator for evaluation. The hardness testing was performed on the module with a high temperature +78 C and a low temperature of -10C. The testing had no effect on the physical security or operation of the module.

6. Operational Environment

The module operates in a non-modifiable environment and does not implement a General Purpose Operating System.

7. Cryptographic Key Management

The module uses the following keys/CSPs:

- AES keys - used for AES encryption/decryption operations, as well as authentication of the Registered and Non-registered Master roles. (Session Secret, Remote Approval Key, Registered Secret and Registration Secret are AES keys.)
- RSA key-pair - used in RSA signature generation operations.
- ECDSA key-pair - used in ECDSA signature generation.
- EC Diffie-Hellman key pair - used for the shared secret computation operations.
- DRBG V, key, and seed - used to generate DRBG based random numbers.
- User PIN - required for the authentication of the User and Owner roles. (The Owner role also requires the PQA).
- Personal Question Answer (PQA) - required for the authentication of the Owner role, along with the User PIN.
- Card Management Key (CMK) - required for the authentication of the PIV administrator role.
- PIN Unblock Key (PUK) - required for the authentication of PIN Unblock role.

7.1. Random Number Generation and Key/CSP Generation

The Modules provides an SP800-90A-compliant Deterministic Random Bit Generator (DRBG) for creation of key components of asymmetric keys, and random number generation.

The underlying NDRNG provides 384 bits of seed to the DRBG. The module performs a continuous self-test on the output of SP800-90A DRBG to ensure that consecutive random numbers do not repeat.

The Key Generation methods implemented in the module for Approved services in FIPS mode is compliant with [SP800-133].

For generating RSA and ECDSA keys the module implements asymmetric key generation services compliant with [FIPS186-4]. A seed (i.e. the random value) used in asymmetric key generation is directly obtained from the [SP800-90A] DRBG.

The public and private key pairs used in the EC Diffie-Hellman shared secret computation are generated internally by the module using the same ECDSA key generation compliant with [FIPS186-4] which is compliant with [SP800-56A].

The module does not output intermediate values of keys/CSPs.

7.2. Key Establishment

The module uses SP 800-56A based on the EC Diffie-Hellman (primitive only, P-256, P-384 curves) shared secret computation. It is used to for the secure communication between a PIV compliant client application on the GPC (when connected to the GoldKey), and a remote host (for example, the server).

As per IG section 7.5, the EC Diffie-Hellman Curve P-256 provides 128 bits of security and P-384 provides 192 bits of security strength.

7.3. Key/CSP Entry and Output

Electronic key entry method is used to import the private/secret keys/CSPs in a plaintext form. This method is used for all the CSPs listed in table 8 (i.e. User PIN, Personal Question Answers, Group Secrets, Registered Secret, PIN Unblock Key, Card Authentication Key, Card Management Key, Session Secret), except the Registration Secret and Remote Approval Key, which are written at the factory. The CSPs and keys are never exported. There is no manual key import or export method used in the module.

Please note that the resulting shared key of the shared secret computation operation is

never used internally by the module.

7.4. Key Transport/Key Wrapping

The module does not support Key Transport or Key Wrapping.

7.5. Key/CSP Storage

Keys and CSPs are stored in the internal non-volatile memory, in plaintext. The keys and CSPs are not accessible from outside of the module.

7.6. Key/CSP Zeroization

The key zeroization is implemented using the following functions:

- ClearToken() - zeroizes the EEPROM and flash data where the keys are stored. This function is used to zeroize all the keys/CSPs stored in the module, including CSPs listed in table 8 (i.e. User PIN, Personal Question Answers, Group Secrets, Registered Secret, PIN Unblock Key, Card Authentication Key, Card Management Key, Remote Approval Key, Session Secret and Registration Secret).

- zeromem() - zeroizes the entire block of RAM memory. It is used to zeroize all the intermediated CSP values/buffers and the cryptographic keys and other CSPs.

7.7. Triple-DES Keying Requirements

According to IG A.13, the same Triple-DES key shall not be used to encrypt more than 2^{16} 64-bit blocks of data.

8. Electromagnetic Interference/Electromagnetic Compatibility (EMI/EMC)

The module meets the requirements of 47 CFR PART 15 regulation & ANSI C63.4 and ICES-003 for the evaluation of Class B of electromagnetic compatibility. This device complies with Part 15 of FCC Class B rules for home or office use. FCC test report number: HBCS Report # EMC_12029.

9. Self Tests

The GoldKey implements a number of self-tests to check proper functioning of the module. This includes power-up and conditional self-tests.

The power-up self-test can be initiated by connecting the GoldKey to a USB port of a GPC. The on-demand self-test can be invoked by restarting the module.

If the set of self-tests are successful, then the module enters the FIPS-Approved operational state. Otherwise, the module enters an error state and returns an error code with the applicable description of the error. The error state is indicated by the fast blinking LED indicator. Once in the error state, no services are available and no data output is possible from the module. The GoldKey must be reset to recover from the error state.

In addition, when the module is performing self-tests, no cryptographic services or APDU commands are available and no data output is possible until self-tests are successfully completed. The module will implicitly transition to Non-approved mode if the RSA algorithm with 1024-bit key size is requested, which is the only non-approved algorithm for this module, as stated in table 7.

9.1. Power-Up Tests

A series of startup tests that run every time the GoldKey is powered up in include:

- The entire firmware code base is verified with an integrity test using SHA-256 hash
- Every cryptographic algorithm is verified with the following Known Answer Test (KAT):

Algorithm	Test
AES (encryption/decryption tested separately)	KAT
Triple-DES (encryption/decryption tested separately)	KAT
RSA (signature generation/verification tested separately)	KAT
ECDSA (signature generation/verification)	Pair-wise consistency test
EC Diffie–Hellman	Primitive “Z” Computation KAT
DRBG	KAT
SHA-256	KAT

Table 9: Power-up Tests

9.2. Conditional Tests

- Continuous Random Number Generation Test is implemented for the DRBG
- A pair-wise test is implemented for RSA and ECDSA key generation.

If any of the conditional tests fail, the module enters Error state, indicated by the fast blinking LED. Once in the error state, no services are available and no data output is possible from the module. The module must be reset to recover from the error state.

10. Design Assurance

10.1. Configuration Management

The GoldKey development team utilizes Subversion, a software versioning and a revision control system, to maintain current and historical versions of files, such as source code and design documentation that contribute to the formation of the module.

Subversion integrates several aspects of the software development process in a distributed development environment to facilitate project-wide coordination of development activities across all phases of the product development life cycle:

- Configuration Management – the process of identifying, managing, and controlling software modules as they change over time
- Version Control – the storage of multiple versions of a single file along with information about each version
- Change control – centralizes the storage of files and controls changes to files through the process of checking files in and out

The list of files that are relevant to the GoldKey and subject to Subversion control is detailed in the GoldKey Configuration Output Detail List provided by **CybrSecurity Corporation**.

10.2. Guidance and Secure Operations

The GoldKey Security Token Cryptographic Module v7.13 is by default designed to operate in the FIPS approved mode. As soon as the GoldKey connected to the GPC, a series of power-up self-tests are performed. Upon successful completion of the self-tests, the module enters the FIPS- Approved mode.

No special settings are required by the User or other roles to operate the module in the FIPS-Approved mode of operation. The module implicitly transitions to Non-approved mode if the RSA algorithm with 1024-bit key size is requested, which is the only non-approved algorithm for this module.

The SELECT command can be used to obtain the version information.

10.2.1. Cryptographic Officer Guidance

The services performed by the Crypto Officer/Registered-Master role listed in section 4 and the operations required to perform these services are described in the GoldKey User Manual.

10.2.2. User Guidance

The details about the procedures such as personalization and registration of the GoldKey are described in the GoldKey User Manual.

11. Mitigation of Other Attacks

The module does not claim mitigation of other attacks.

12. Additional Information

For information on the Finite State Model diagram and the state transition table, please refer to the FSM document (GoldKey_FSM_v1.1.docx). This is available by contacting the point of contact for the validated module available from the CMVP website at:

http://csrc.nist.gov/groups/STM/cmvp/validation.html.

Appendix A. Glossary and Abbreviations

AES	Advanced Encryption Standard
AES-NI	Advanced Encryption Standard New Instructions
API	Application Program Interface
CAVP	Cryptographic Algorithm Validation Program
CAVS	Cryptographic Algorithm Validation System
CBC	Cipher Block Chaining
CMAC	Cipher-based Message Authentication Code
CMVP	Cryptographic Module Validation Program
CRNGT	Continuous Random Number Generator Test
CSP	Critical Security Parameter
CTR	Counter Mode
DES	Data Encryption Standard
DRBG	Deterministic Random Bit Generator
ECB	Electronic Code Book
ECC	Elliptic Curve Cryptography
EMI/EMC	Electromagnetic Interference/Electromagnetic Compatibility
FCC	Federal Communications Commission
FFC	Finite Field Cryptography
FIPS	Federal Information Processing Standards Publication
HMAC	Hash Message Authentication Code
IG	Implementation Guidance
KAS	Key Agreement Scheme
KAT	Known Answer Test
KW	Key Wrap
MAC	Message Authentication Code
NIST	National Institute of Science and Technology
NDRNG	Non-Deterministic Random Number Generator
PCT	Pair-wise Consistency Test
RSA	Rivest, Shamir, Addleman
SHA	Secure Hash Algorithm
SHS	Secure Hash Standard

Appendix B. References

FIPS140-2 **FIPS PUB 140-2 - Security Requirements For Cryptographic Modules**
May 2001
http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf

FIPS140-2 IG **Implementation Guidance for FIPS PUB 140-2 and the Cryptographic Module Validation Program**
June 17, 2016
http://csrc.nist.gov/groups/STM/cmvp/documents/fips140-2/FIPS1402IG.pdf

FIPS180-4 **Secure Hash Standard (SHS)**
March 2012
http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.180-4.pdf

FIPS186-4 **Digital Signature Standard (DSS)**
July 2013
http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf

FIPS197 **Advanced Encryption Standard**
November 2001
http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf

FIPS198-1 **The Keyed Hash Message Authentication Code (HMAC)**
July 2008
http://csrc.nist.gov/publications/fips/fips198-1/FIPS-198-1_final.pdf

SP800-38A **NIST Special Publication 800-38A - Recommendation for Block Cipher Modes of Operation Methods and Techniques**
December 2001
http://csrc.nist.gov/publications/nistpubs/800-38a/sp800-38a.pdf

SP800-38B **NIST Special Publication 800-38B - Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication**
May 2005
http://csrc.nist.gov/publications/nistpubs/800-38B/SP_800-38B.pdf

SP800-38C **NIST Special Publication 800-38C - Recommendation for Block Cipher Modes of Operation: the CCM Mode for Authentication and Confidentiality**
May 2004
http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-38c.pdf

SP800-38F **NIST Special Publication 800-38F - Recommendation for Block Cipher Modes of Operation: Methods for Key Wrapping**
December 2012
http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-38F.pdf

SP800-56A	**NIST Special Publication 800-56A - Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography (Revised)** March, 2007 http://csrc.nist.gov/publications/nistpubs/800-56A/SP800-56A_Revision1_Mar08-2007.pdf
SP800-57	**NIST Special Publication 800-57 Part 1 Revision 4 - Recommendation for Key Management Part 1: General** January 2016 http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-57pt1r4.pdf
SP800-67	**NIST Special Publication 800-67 Revision 1 - Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher** January 2012 http://csrc.nist.gov/publications/nistpubs/800-67-Rev1/SP-800-67-Rev1.pdf
SP800-90A	**NIST Special Publication 800-90A - Revision 1 - Recommendation for Random Number Generation Using Deterministic Random Bit Generators** June 2015 http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-90Ar1.pdf
SP800-131A	**NIST Special Publication 800-131A Revision 1- Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths** November 2015 http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-131Ar1.pdf

