GoldKey Security Token Cryptographic Module

FIPS 140-2 Security Policy

Version 1.5

Last Update: 01/15/2014

1

GoldKey Security Corporation
26900 East Pink Hill Road, Independence, MO, USA

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

Table of Contents

Trademarks

GoldKey is a registered trademark of GoldKeySecurity Corporation

1. Introduction

This document is thenon-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 GoldKeyis specified in the following table:

Component Type	Part Number or File Name and Version with Description
Hardware	GoldKeyUSB Security Token Controller IC:USB-CONTROLLER-2LF Processor: Arca2S 32-bit RISC
Firmware	Binary image of the module: goldkey.bin v7.12
Documentation	Security Policy: GoldKey_SP_v1.5.pdf
	GoldKey User Manual: GoldKeyManual.pdf v7.1
	Finite State Model: GoldKey_FSM_v1.0.docx
	GoldKey API Specification: GoldKey_API_Spec_v1.0.docx
	GoldKey Master Component List: GoldKey_Master_Comp_List-1.0.docx
	GoldKey Firmware Design Document: DesDoc_GoldKeyFirmware 7.doc

Table 2: GoldKey Security Token Cryptographic Module Components

Note: For source code associated with GoldKey CryptographicLibrary V7.12 and the Master Component List, please refer to the GoldKey Security Token Configuration Output Detail List documented in GoldKey-Master_Comp_List-1.0.docx

2.3. Modes of Operation

The GoldKey supports only one mode of operation, FIPS approved mode of operation. After completing all the self tests module enters FIPS mode without any operator intervention.

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 TRNG)	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 # 54	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 186-3 ECDSA, P-256 and P-384 Curves (External Hash)	SIG(gen) KEY(gen)
EC Diffie-Hellman, CVL cert # 54	SP 800-56A All of SP800-56A EXCEPT KDF	Key Agreement
SHA cert #2024	FIPS 180-4 SHA-256	Secure Hash

Table 3: FIPS Approved Algorithms

Note: RSA and ECDSA Signature Generation operations rely on an external hash as

specified in the PIV standard (SP-800-73-3). For Windows 7 the Enhanced Cryptographic Provider (The RSAENH Module -FIPS 140-2 cert #1330, SHS cert #1081)external hash may be used. For other platforms it may be provided using other approved software modules that support the PIV standard.

2.4. Cryptographic Module Boundary

2.4.1. Hardware block diagram

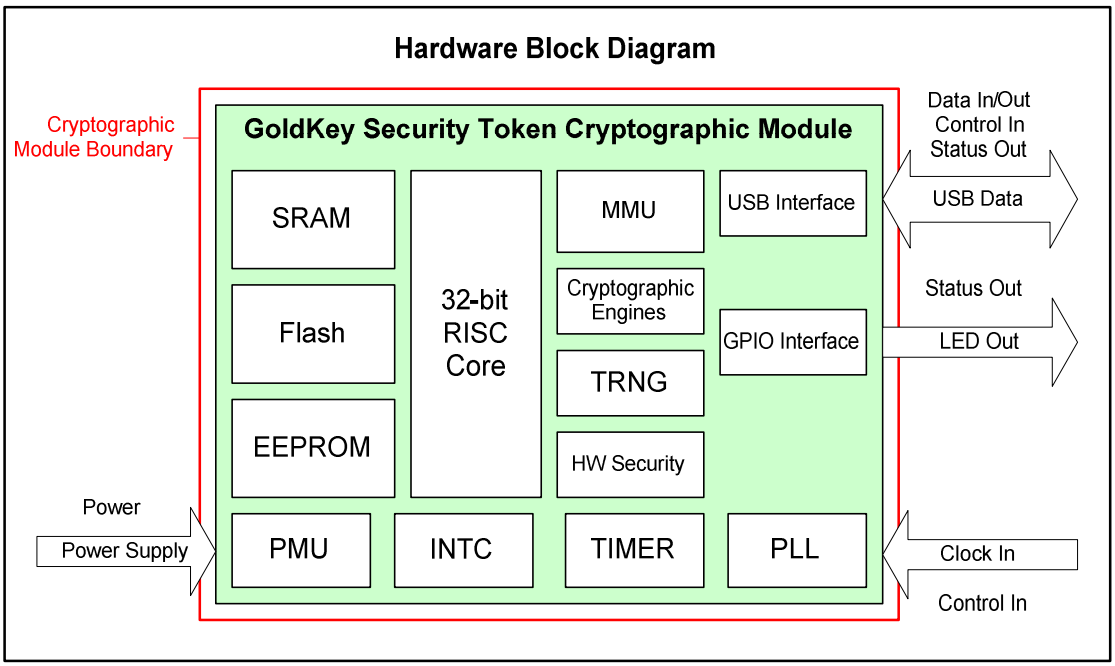

Figure 1: Hardware Block Diagram

Both the physical and logical cryptographic boundary 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
Slow Blink	Active (indicates in process cryptographic operation)	FIPS Approved
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 specialcharacters. Assuming a mix of lower case alphabet letters, upper case alphabet letters, 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

authenticationattempts.

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 bits AES keys. The probability of guessing these keys will be same as guessing a 256 bit AES key. AnAES 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 sizes	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 #54	X	FIPS 186-4
ECDSA Key Generation	Registered Master, PIV Admin	ECC Private Key	P-256, P-384 Curves	Yes, cert #384	W	FIPS 186-3

Service	Roles	CSP	Modes	FIPS Approved (cert #)	Access	Notes
ECDSA Signature Generation	All Roles	ECC Private Key	P-256, P-384 Curves (External Hash)	Yes, cert #384	X	FIPS 186-3
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	Yes, cert #297	X	SP 800-90A CTR_DRBG, AES-256 (seeded with the hardware TRNG); Key generation
TRNG	All Roles	Seed, Seed key	N/A	N/A	W	Hardware-based TRNG, which supplies Seed to the DRBG
Key Agreement						
ECDiffie-Hellman (KAS)	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 sizes	cert #1210	W	Due to transitions in SP 800-131-A, 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 CSPs.

Services/APDU Commands	Description	Roles	CSP
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 CPSsfrom 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	CSP
		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 256/384 Private Key),Remote Approval Key(AES key (256 bits)) Session Secret (generated by ASSOCIATE command) (AES key (256 bits))
		User	All Private Keys, except Card Authentication Key (RSA 2048, ECC 256/384)
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

Services/APDU Commands	Description	Roles	CSP
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 based random data for key generation
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))

Services/APDU Commands	Description	Roles	CSP
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))
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))

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 untampered. 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.

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 and key wrap/transport 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.
- ECDiffie-Hellman key pair - used for the key agreement operations.
- DRBG v,key and seed- used to generate a DRBG based random number.
- User PIN - required for the authentication of theUser 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

An SP 800-90 based Deterministic Random Bit Generator (DRBG) is used for key generation. Seed (384 bits) and seed keys (256 bits) are provided by the Hardware-based Non-deterministic RandomNumber Generator. The module checks to ensure that the seed and seed keys are not identicalbefore they are used to produce the DRNG output.

The underlying TRNG provides 384 bits of seed to the DRBG allowing generation of the random number up to 384 bits of entropy. Please note that 256 bit AES keys generated using the DRBG will have an entropy of 256 bits.

7.2. Key/CSP Generation

The module uses a FIPS-Approved DRBG as an input to create the following keys/CSPs:

- AES key
- RSA key-pair
- ECDiffie-Hellmankey-pair
- ECDSA key pair

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

7.3. Key Agreement

The module uses SP 800-56Abased on the EC Diffie-Hellman (primitive only, P-256, P-384 curves) key agreement. It is used to for the secure communication between a PIV compliantclient application on the GPC (when connected to the GoldKey), and a remote host (for example, the server). Please note that the resulting shared key is output from the module in an encrypted form. .

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.

Caveat: EC Diffie-Hellman (key agreement; key establishment methodology provides between 128 and 192 bits of encryption strength)

7.4. Key/CSP Entry and Output

Electronic key entry method is used to import the private/secret keys in an encrypted form.

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 key agreement operation is never used internally by the module. It is output from the module in an encrypted form.

7.5. Key Transport/Key Wrapping

AES (256 bits) is used for key transport or key wrapping of the following keys:

Key	Type	Strength
AES	AES 256 bits	256 bits
Triple-DES key(CMK)	Triple-DES 192 bits	112 bits
RSA keys	RSA 2048 bits	112 bits
ECDSA	ECC P256/P384	128/192 bits
EC Diffie-Hellman key-pair	ECC P256/P384	128/192 bits

Table 9: Key Strength

As specified above, the strength of the key wrapping scheme is greater than or equal to the strength of the keys being wrapped or transported.

7.6. Key/CSP Storage

Keys and CSPs are stored in the internal non-volatile memory in the form of a plain-text. The keys and CSPs are not accessible outside of the module.

7.7. Key/CSP Zeroization

The key zeroization is implemented using the following functions:

- ClearToken() -zeroizes the EEPROM and flash data where the keys are stored.
- 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.

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. FCCtest 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.

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 10: 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

10. Design Assurance

10.1. Configuration Management

The GoldKey development team utilizes Subversion, a softwareversioning 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 themodule.

Subversion integrates several aspects of the software development process ina distributed development environment to facilitate project-wide coordination ofdevelopment 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 Subversioncontrol is detailed in the GoldKey Configuration Output Detail Listprovided by GoldKey Security Corporation.

10.2. Guidance and Secure Operations

The GoldKey Security Token Cryptographic Module v 7.12 is by default designed to operate only in the FIPS approved mode. As soon as the GoldKeyconnected 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 SELECT command can be used to obtain the version information.

10.2.1. Cryptographic Officer Guidance

Theservices 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 (FSMv1.0.doc). 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:

