WatchKey USB Token Cryptographic Module

Model Number: K6

Smart Card Chip: Z32L256D32U

PCB: K003010A

Firmware Version: 360C6702

FIPS 140-2 Non-Proprietary Security Policy

Policy Version 1.0.3

Last Updated: 2011-11-14

Note: This document was initially developed based on atsec's security policy questionnaire, template, and the answers that Watchdata provided, which described the design and implementation of WatchKey USB Token.

Table of contents

1 Introduction

This document is a non-proprietary FIPS 140-2 Security Policy for the WatchKey USB Token ("WatchKey" or "module") cryptographic module manufactured by WatchData Technologies Pte Ltd. It describes how the token meets the requirements as specified in FIPS PUB 140-2 (Federal Information Processing Standards Publication 140-2) for a Security Level 2 multi-chip standalone hardware module.

The security policy is required for FIPS 140-2 validation and is intended to be part of the package of documents that are submitted to Crypto Module Validation Program (CMVP). It describes the capabilities, protection, and access rights provided by the cryptographic module. It also contains a specification of the rules under which the token must operate in order to be in FIPS mode. This security policy allows individuals and organizations to determine whether the cryptographic token meet their security requirements and to determine whether the module, as implemented, satisfies the stated security policy.

The targeted audience of this document consists of, but not limited to, the WatchKey and its application developers, testers at the Cryptographic Services Testing (CST) lab, and reviewers from CMVP.

WatchKey USB Token is a PKI-based client network security suite which contains both software and hardware to balance security with ease-to-use. It is a combination of cryptography, smartcard, and other advanced technologies. WatchKey USB Token is used as the carrier of keys and certificates, and the processor of cryptographic algorithm. WatchKey USB Token communicates with computer via its USB interface and is opened to various applications including software protection, ID authentication, online transaction, digital security, etc.

2 Cryptographic Module Specification

2.1 Module Overview

The WatchKey USB Token is a hardware cryptographic module validated against the FIPS 140-2 at security level 2. It is a USB-based PKI, two-factor authentication token device. It provides digital signature generation/verification for online authentications and data encryption/decryption for online transactions. The user's private and public key pairs can be generated and stored on the embedded chip. WatchKey has 32K EEPROM and 64K FLASH for the on-card file system divided into the basic areas and extended area. The user's key pairs reside in the EEPROM. The private key can never be exported. The implementation of FIPS-Approved cryptographic algorithms are tested under the Cryptographic Algorithm Validation Program (CAVP) and have certificate numbers as specified in section 2.5 of this document.

The WatchKey provides the USB interface that can connect the module to a General Purpose Computer (GPC) in a "plug and play" manner, which eliminates the need to install Smart Card Reader drivers. The WatchKey implements type A USB 1.1 (full speed) specifications and USB CCID (Circuit(s) Cards Interface Device) protocol which enables communication with ISO/IEC 7816 smart cards over USB.

2.2 Cryptographic Module Description

The physical boundary of the WatchKey USB Token cryptographic module is defined as the opaque enclosure surrounding the token device as shown in the picture below.

There are 6 colors of the module that have passed the physical security analysis.

Figure 1. WatchKey USB Token - 6 colors

Figure 2. WatchKey USB Token - 4 angles

The weight of the module is 35g. The dimensions of the module are approximately 59.5mm * 19mm * 10.5mm.

The module components within the logical boundary of the WatchKey USB Token are specified in Table 1.

Component Type	Part Number or File Name and Version
Hardware	Smart Card Chip Z32L256D32U and PCB K003010A
Model Number	K6
Firmware	360C6702.bin (includes Watchdata-FIPS-TimeCOS Hardware Cryptographic Library V1.0.0.1)
Documentation	TimeCOSPK General Technique Manual V4.0.0
	TimeCOSPK Specific Technique Manual V4.0.0
	WatchKey USB Token User Guidance V1.0.0
	Z32_FIPS_Validation_FSM V1.0.0
	Z32_FIPS_Validation_Firm General Design V1.0.0
	Security Policy for WatchKey USB Token V1.0.1
	WatchKey USB Token Configuration Management Overview V1.0.0
	WatchKey USB Token Configuration Output Detail List V1.0.0

Table 1. WatchKey USB Token Cryptographic Module Components

Note：For source code associated with Watchdata-FIPS-TimeCOS Hardware Cryptographic Library V1.0.0.1, please refer to ***WatchKey USB Token Configuration Output Detail List*.**

2.3 Block Diagram

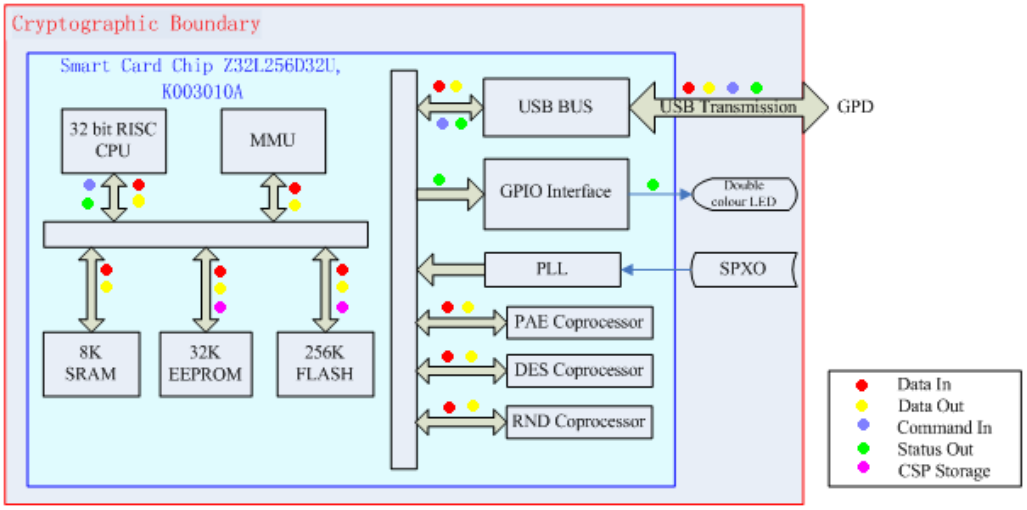

Figure 3. WatchKey USB Token Hardware Block Diagram

Note: 64K of 256K Flash is used for extended area of file system, and 192K left is used for code storage.

Figure 4. WatchKey USB Token Logic Cryptographic Component Block Diagram

2.4 Cryptographic Module Security Level

The module is validated as a multi-chip standalone hardware module against FIPS 140-2 at the overall Security Level 2 cryptographic module. 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
Cryptographic Module Specification	2
Cryptographic Module Ports and Interfaces	2
Roles, Services and Authentication	2
Finite State Model	2

FIPS 140-2 Sections	Security Level
Physical Security	3
Operational Environment	N/A
Cryptographic Key Management	2
EMI/EMC	3
Self-Tests	2
Design Assurance	2
Mitigation of Other Attacks	N/A

Table 2. Security Levels for Eleven Sections of the FIPS 140-2 Requirements

2.5 FIPS and non-FIPS Modes of operation

The WatchKey USB Token implements a list of FIPS-Approved algorithms as shown in Table 3.

Algorithm w/modes	Keys/CSPs	Usage	FIPS-Approved algorithm	Algorithm Certificate #	Operate in FIPS-mode
AES (ECB, CBC)	128, 192, 256 bit keys	Encryption/decryption	Yes	#1616	Yes
Triple DES (ECB, CBC, CMAC) (based on NIST SP 800-38A)	3-key 168 bits	Encryption/decryption	Yes	#1057	Yes
RSA Key Gen (based on ANSI X9.31)	Module sizes: 2048, Public Key sizes: 65537	Generate 2048 RSA Key pairs	Yes	#794	Yes
RSA (PKCS #1.5 (SIG(gen), SIG(ver)))	Module sizes: 2048, Public Key sizes: 65537	Generate and Verify signature	Yes	#794	Yes
DRBG(based on SP 800-90)	Deterministic RNG	Random number generation	Yes	#85	Yes
SHA256 (BYTE-only)	N/A	Hashing	Yes	#1425	Yes

Table 3. FIPS-Approved Cryptographic Algorithms

In FIPS mode, the module provides the FIPS-Approved algorithms listed in Table 3. The module also uses RSA Encrypt for wrapping a session key for transport between the module and the host application toolkit (i.e. WatchSAFE 3.4.1) with which it communicates. RSA Encrypt is not a FIPS-Approved algorithm, but it is allowed to be used in FIPS-mode for key wrapping only.

In the non-FIPS mode, the module provides the RSA signature and verification with 1024 bit keys and the SHA-1 operation.

The module uses 2 LEDs (red and green) to differentiate the FIPS relevant state as shown in Table 4, below. The module also provides an APDU command (i.e. APDU 808A000002) for the user (through the host PC application) to query the state in which the module is in at any time. The module returned two bytes in response to indicate its current state. The interpretation of the response values is documented in detail in TimeCOSPK General Technique Manual V4.0.0.

Red LED	Green LED	State
Off	Off	Power off
Blink	Blink	Self-Test
On	Off	Non-FIPS
Off	On	FIPS
Blink	Off	Error

Table 4. LED for Current State Indicator

3 Cryptographic Module Ports and Interfaces

The interfaces for the cryptographic module include the physical ports of WatchKey USB Token and APDU command fields. The physical ports of the module and APDU command fields are mapped to four FIPS 140-2 logical interfaces: Data Input, Data Output, Control Input, and Status Output. The mapping between the logical interfaces, the module physical ports, and APDU command fields is provided in the following table:

FIPS 140-2 Required Logical Interface	WatchKey USB Token Physical Ports	APDU Command Fields
Data Input	Data pins within the USB Port	Lc, Command Data Field
Data Output	Data pins within the USB Port	Response Data Field
Control Input	Data pins within the USB Port	CLA, INS, P1, P2, Le
Status Output	Data pins within the USB Port LED	SW1, SW2
Power Input	Power pin within the USB Port	

Table 5. Ports and Interface of the WatchKey USB Token

The USB 1.1 specification with CCID protocol ensures that these logical interfaces are distinct. The module does not support bypass capability.

For details about structure of APDU commands applied by WatchKey USB Token, please refer to Chapter 6, Command and Response in the TimeCOSPK General Technique Manual V4.0.0.

4 Roles, Services, and Authentication

4.1 Roles

WatchKey USB Token supports two types of roles: User Role and Security Officer Role.

The module supports role-based authentication. Available services for a user depends on which type of roles he or she is authenticated.

The User Role can execute all of the approved algorithms, create files, read and update User files, delete files, change the User PIN, and update the Encryption keys.

The Security Officer Role can create files, read and update the Security Officer files, import and update keys, unblock the User PIN, initialize the application, and read and update the applications that reside on the token.

WatchKey USB Token does not support concurrent operators.

The details of the available services for each role are given in the following sections.

4.2 Services

The services provided by WatchKey USB Token are through the documented APDU commands. They are invoked by the host application toolkit (i.e., WatchSAFE 3.4.1).

All services listed in Table 6 below, except for RSA signature generation and verification using 1024-bit key and SHA-1, can be used in the FIPS-approved mode. The WatchKey can perform a digital signature with RSA 1024-bit key and SHA-1 only while in non-FIPS mode.

Service	Description	Security Officer	User	CSP
User Login	A successful external entity authentication and verification of USER PIN		√	User PIN
Change Security Officer PIN	Verify and change PIN	√		Security Officer PIN
Unblock User PIN	Unblock PIN	√		Security Officer PIN Unblock PIN
Change User PIN	Verify and change PIN		√	User PIN
Security Officer Login	A successful external entity authentication and verification of Security Officer PIN	√		Security Officer PIN
Get Challenge (Note 1)	Get random digits	√	√	Random Number
External entity Authentication (Note 1)	External entity authentication is used for the Token to authenticate the external entity	√	√	External Entity Authentication Key KEK

Service	Description	Security Officer	User	CSP
Internal Authentication (Note 1)	Internal authentication is used for the external entity to authenticate the token	√	√	Encryption Key SM Mac Key
Select File (Note 1)	The file access rights will be effective only when the DF is re-selected after the file is created for the first time. When the DF is selected successfully, the current operation state will be reset.	√	√	
Security Officer File Read	Read Binary, Read Record	√		Security Officer PIN SM Key SM Mac Key
Security Officer File update	Update Binary, Update Record	√		Security Officer PIN SM Key SM Mac Key
User File Read	Read Binary, Read Record		√	User PIN SM Key SM Mac Key
User File Update	Update Binary, Update Record		√	User PIN SM Key SM Mac Key
Initialize the Application	Erase DF that holds application in order for the application related files to be re-created	√		Security Officer PIN
RSA Signature Verification (1024/2048)	Verify signatures		√	User PIN RSA Private Key
RSA Signature Generation (1024/2048)	Generate signatures		√	User PIN RSA Public Key
RSA Encrypt	RSA encryption/decryption for wrapping a session key		√	User PIN RSA Public Key RSA Private Key
Data Compress (Note 1)	Data compress（SHA-1/SHA-256）	√	√	
Generate RSA Key Pair (2048)	Generate RSA key pair		√	User PIN RSA Public Key

Service	Description	Security Officer	User	CSP
				RSA Private Key
Import RSA Key Pair (1024/2048)	Import RSA key pair		√	User PIN RSA Public Key RSA Private Key
Import Key	Write key	√		User PIN Security Officer PIN KEK SM Key SM Mac Key Encryption Key External Entity Authentication Key Unblock PIN
Update Key	Modify key	√	√	User PIN Security Officer PIN KEK SM Key SM Mac Key Encryption Key External Entity Authentication Key
Create File	Create file	√	√	User PIN Security Officer PIN
Restart (Note 1)	Reset the state	√	√	
Data Encrypt/Decrypt	AES /TDES algorithm	√	√	Encryption Key
Self-Test (Note 1)	Self-test	√	√	
Get State (Note 1)	Get the operational state	√	√	
Erase RSA Key	Destruct the key value		√	User PIN RSA Public Key RSA Private Key
Set Serial Number	Set the unique serial number	√	√	

Service	Description	Security Officer	User	CSP
(Note 1)				
Get COS Information (Note 1)	Get the information about the function that the Token supports	√	√	
Get Release Space (Note 1)	Get the size of space left in the Token	√	√	
Append Record	Append record to cycle record file and variable-length record file	√	√	User PIN Security Officer PIN SM Key SM Mac Key

Table 6. Services Authorized for Roles

Note 1: The service does not need role authentication.

4.3 Operator Authentication

WatchKey USB Token uses two authentication mechanisms to authenticate different roles. The User Role and the Security Officer Role are authenticated by successful external entity authentication and verifying the corresponding password.

The Token provides the basics for a challenge-response style authentication using a shared secret key between the Token and the external entity. The mutual authentication between the Token and the external entity depends on the correct implementation of the authentication mechanism within the external entity as well.

The shared secret key between the Token and the external entity for mutual authentication is a 3-key TDES key. This is a diversified key obtained from a master 3-key TDES key and the unique serial number of the Token. The master key is securely kept at the manufacturing facility. The diversified keys for all tokens are pre-computed and entered into tokens during the initialization phase at the factory. The external entity (e.g., the backend server, the application running on the host GPC, or a combination of both) knows the master key and algorithm used for the key diversification. When the external entity starts a mutual authentication process with the Token, it retrieves the serial number from the Token and calculates the diversified key for this Token. If the calculated key matches with the external entity authentication key stored on the Token, then the authentication is successful.

The module ensures that there is no visible display of the authentication data, such as User password. The authentication data is stored in the key file which can never be exported outside the Token. All of the authentication states are stored in the RAM area. When the module's power is off, all of the states will be cleared and when the module is powered on again, all of the states will be initialized to zero. While the status information indicated by the LEDs is available to all operators, the services described in Table 6 are available only to operators with the authenticated role(s).

There is an initial Security Officer Password written into the WatchKey USB Tokens when they are manufactured. This initial Security Officer Password is for token issuers (e.g., banks) who use the Security Officer Role to initialize the Application before they are issued to the final users. The initial Security Officer Password to token issuers are distributed via a

User Guide brochure in a secure manner, which is compliant to the corporation security handling process and procedure of the token issuers.

There is a default User Password in the Token. When the User takes the Token for the first time, he or she should change the User Password by using the 'Verify and Change PIN' command.

If a User wants to switch to the Security Officer Role, he or she should verify the Security Officer Password. Only when the Security Officer Password is verified successfully, will the state be switched to the Security Officer Role.

4.4 Password Strength

Passwords for User and Security Officer Role authentication must be in the range of 8-32 characters. The Password must contain a mix of letters, numeric characters, and special characters. Assuming that a mix of lower case letters, upper case letters, and numeric characters is used, the password can consist of the following set: [a-zA-Z0-9], yielding 62 choices per character.

The probability of a successful random attempt is $1/62^8$, which is less than 1/1,000,000. Assuming 10 attempts per second are made via a scripted or automatic attack, the probability of a success with multiple attempts in a one minute period is $600/62^8$, which is less than 1/100,000.

The module will lock an account after, at most, 15 consecutive failed authentication attempts; thus, the maximum number of attempts in one minute is 15. Therefore, the probability of a success with multiple consecutive attempts in a one-minute period is $15/62^{8,}$ which is less than 1/100,000.

The password will be turned into 24 bytes PIN by an algorithm (SHA-1 hashed calculation plus 4 bytes serial number).

PINs are stored in the WatchKey USB Token in a hashed form with a 24-byte fixed length.

5 Physical Security

The module is a multiple-chip standalone module and conforms to Level 3 requirements for physical security. The module is composed of production-grade components and is housed in a sealed, hard plastic enclosure that has no openings, vents, or doors. It cannot be opened without noticeable damage.

6 Operational Environment

The module operates in a limited operational environment and does not implement a General Purpose Operating System. The operational environment requirements do not apply to the module.

7 Key Management

7.1 Random Number Generator

WatchKey USB Token uses a FIPS-Approved Deterministic Random Bit Generator (DRBG) based on SP 800-90.

Seeds are provided by the IC hardware-based non-deterministic random number generator. The module checks to ensure that two consecutively provided seeds are not identical before the later one is used as a valid input to seed the DRNG SP 800-90.

7.2 Key Generation

The module uses a FIPS-Approved DRBG (SP 800-90) as input to create the following keys/CSPs:

- RSA key pairs
- Session keys for protecting read/write on-card files
- Session keys for encrypting external data/files

When generating a pair of RSA Keys, the module uses the algorithm specified in DRBG SP 800-90 to generate a group of random numbers, and then uses these random numbers to generate the key pair in accordance with the RSA key generation algorithm described in the standard ANSI X9.31.

There are two types of session keys. The first type of session key is used for the protection of the read/write operations on the files residing on the WatchKey USB Token. This type of session key is generated by using the FIPS-Approved TDES algorithm to encrypt a random number provided by DRBG with the Secure Messaging Key.

The second type of session key is used for encrypting emails or files not located on the token. When the token is plugged into its host GPC, the host application toolkit WatchSAFE can request the connected token to encrypt an email or file by providing the token an RSA public key, the data to be encrypted, and the encryption method (i.e. AES or TDES). The token first generates a session key by DRBG SP 800-90. Then it encrypts the session key with the provided RSA public key using RSA encryption, and encrypts the provided data with the session key using AES or TDES as indicated in the request from WatchSAFE. Lastly, it replies to the WatchSAFE by providing the encrypted session key together with the encrypted data.

Both types of session keys are either AES keys, or 3-key TDES keys. They only exist in the volatile memory and do not survive across power cycles.

The KEK, Initializing key, External entity Authentication key, Secure Messaging Key, Secure Messaging Mac Key, Encryption Key, User PIN, Security Officer PIN, and Unblock PIN are imported as input parameters to the APDU commands in the factory or in the initializing of the application process.

7.3 Key Entry and Output

Columns “Generate/Input” and “Output” in Table 7 show the key entry and output for all keys and CSPs used by the WatchKey. Other than the passwords, the module does not support manual key entry. In addition, the module does not output keys/CSPs or their intermediate values in plaintext format outside its physical boundary.

When a user or security officer enters his or her password manually using the keyboard of the host GPC to which the WatchKey is connected to, the device manager that runs on the

host GPC turns the password into a 24-byte PIN and sends it using the Verify & Change PIN APDU command to WatchKey for verification or changing of the PIN stored on the device.

7.4 Key Storage, Protection, and Destruction

The module stores the keys mentioned below in the EEPROM of the embedded Smart Card chip. Data in the EEPROM is protected by the secure design of the Smart Card chip. The memory is scrambled and encrypted.

There are key and key encryption key (KEK) in general.

The keys include Initializing key, External entity authentication key, Secure Messaging Key, Secure Messaging Mac Key, Encryption Key, User PIN, Security Officer PIN, Unblock PIN, Session key, RSA private key, and RSA public key.

The KEK is used to encrypt the other key in the initialization. It is imported in plaintext form in the factory.

All keys except the RSA key and session key are imported in the factory.

There are two ways that the RSA key pair is generated. The first is by generating RSA Key pairs internally by the User. The second way is by being imported by a trusted third-party of the Client and Watchdata after the factory.

All the keys are effective after they are initialized in the factory.

All the keys under the Application DF can be deleted by the Security Officer using the erase EF/DF APDU command. The WatchKey USB Token can only be reloaded in the factory by authenticating the initializing key.

The following table lists all keys, including the key encryption key (KEK) and CSPs, that reside within the WatchKey USB Token:

Key/CSP	Key Type	Generate/ Input	Output	Storage	Zeroization	Privileges
KEK	3-key TDES key	Externally generated, entered in plaintext in factory	Never exits the module	Stored in Plaintext	By Erase MF APDU command “800E000000”	Used to wrap the other key
Security Officer PIN	24 bytes Pin	Externally generated, entered in encrypted form in factory or by Security officer (encrypted with TDES)	Never exits the module	Stored in Plaintext	By Erase DF/EF APDU command “00E4000002 Data” or by Erase MF APDU command	Involved in authenticating Security Officer Role
External entity Authenticat ion key	3-key TDES key	Externally generated, entered in encrypted form in factory or by Security	Never exits the module	Stored in Plaintext	By Erase DF/EF APDU command “00E4000002 Data” or by Erase MF APDU	Involved in authenticating to the further use of Roles

Key/CSP	Key Type	Generate/ Input	Output	Storage	Zeroization	Privileges
		officer (encrypted with TDES)			command	
Secure Messaging Key	3-key TDES key	Externally generated, entered in encrypted form in factory or by Security officer (encrypted with TDES)	Never exits the module	Stored in plaintext	By Erase DF/EF APDU command "00E4000002 Data" or by Erase MF APDU command	Used as a master key to derive a session key for the secure transition of files between the module and the external entity with which the module is communicating
Secure Messaging Mac Key	3-key MAC key	Externally generated, entered in encrypted form in factory or by Security officer (encrypted with TDES)	Never exits the module	Stored in plaintext	By Erase DF/EF APDU command "00E4000002 Data" or by Erase MF APDU command	For computing the MAC
Initializing Key	3-key TDES key	Externally generated, entered in encrypted form in factory (encrypted with TDES)	Never exits the module	Stored in plaintext	by Erase MF APDU command	To Erase MF and reload the Firmware in factory ONLY
Encryption Key	AES 128/192/256 Key, 3 –key TDES key	Externally generated, entered in encrypted form in factory or by Security officer (encrypted with TDES)	Never exits the module	Stored in plaintext	By Erase DF/EF APDU command "00E4000002 Data" or by Erase MF APDU command	Crypt operation with AES/TDES User Role only
Session key for protecting	AES 128/192/2	Internally generated using TDES	Never exits the module encrypted by	Stored in plaintext in volatile	Power off or updated by another	Do cryptographic operation with

Key/CSP	Key Type	Generate/ Input	Output	Storage	Zeroization	Privileges
read/write on-card files	56 Key, 3 –key TDES key	encryption on a random number from DRBG SP 800-90 with the Secure Messaging Key	RSA encryption	memory	session key, or mode switch	AES/TDES on the data to be read from/write into on-card files
Session Key for encrypting external data/files	AES 128/192/256 Key, 3 –key TDES key	Internally generated using DRBG SP 800-90	Sent to the host application WatchSAFE encrypted by RSA encryption under an externally imported RSA public key	Stored in plaintext in volatile memory	Power off or updated by another session key, or mode switch	Do cryptographic operation with AES/TDES on the data/files to be encrypted upon the request of WatchSAFE
RSA private key	1024/2048 RSA private key	Internally generated by User or Imported by trusted third-party	Never exits the module	Stored in plaintext	By Erase DF/EF APDU command “00E4000002 Data” or by Erase MF APDU command	Generates signatures User Role only
RSA public key	e = 010001	Internally generated by User or Imported by trusted third-party	Never exits the module	Stored in plaintext	By Erase DF/EF APDU command “00E4000002 Data” or by Erase MF APDU command	Verifies signature, encrypts session keys User Role only
User PIN	24 bytes Pin	Externally generated, entered in encrypted form in factory or by Security officer (encrypted with TDES)	Never exits the module	Stored in Plaintext	By Erase DF/EF APDU command “00E4000002 Data” or by Erase MF APDU command	Only use for User Role
Unblock PIN	8~32 bytes	Externally generated,	Never exits the module	Stored in plaintext	By Erase DF/EF APDU	Crypto Security

Key/CSP	Key Type	Generate/ Input	Output	Storage	Zeroization	Privileges
		entered in encrypted form in factory or by Security officer (encrypted with TDES)			command “00E4000002 Data” or by Erase MF APDU command	Officer Role

Table 7. Keys and CSPs

Note: The “Data” field in the Erase DF/EF APDU command “00E4000002 Data” is a 2-byte file identifier of a DF/EF to be erased.

8 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, with FCC ID: Y97WATCHKEY509 and FCC test report number: I11MQ0278-FCC-PART15B.

9 Self-Tests

The WatchKey USB Token implements a number of self-tests to ensure proper functioning of the module. This includes power-up and on-demand self-tests, as well as conditional self-tests.

The power-up self-test can be initiated by inserting the WatchKey USB Token into a USB port of a GPC. The on-demand self-test can be invoked by the Self-Test APDU command.

If the self-test is successful, then the module enters the FIPS-Approved operational state. If the self-test is unsuccessful, the module enters an error state and returns an error code with a description of the error. The error state is indicated by the red LED indicator, as well as the Get State APDU command. Once in the error state, no services are available and no data output is possible from the module. Only self-test can be executed in the error state to return FIPS Mode.

In addition, when the module is performing self-tests, no APDU commands are available and no data output is possible until self-tests are successfully completed.

9.1 Power-Up Tests

The WatchKey USB Token performs self-tests automatically when it is plugged into a USB port of a GPC. The on-demand self-test is performed when the APDU command is invoked.

Whenever the power-up tests are initiated, the module performs the integrity test and the cryptographic algorithm Known Answer Test (KAT). If any of these tests fail, the module enters into an error state.

9.1.1 Integrity test

The WatchKey USB Token uses CRC32 for the integrity test of its firmware.

9.1.2 Cryptographic algorithm KAT

Upon power-up, a KAT is performed for the following FIPS-Approved algorithms:

- AES encryption/decryption
- Triple-DES encryption/decryption
- CMAC
- RSA Key Generation with key size 2048
- RSA signature generation/verification
- DRBG SP 800-90
- SHA-256

9.2 Conditional Tests

9.2.1 Pair-wise consistency test

The WatchKey USB Token performs the pair-wise consistency test for each pair of RSA keys that it generates. The consistency of the key pair is tested by calculating and verifying a digital signature.

9.2.2 Continuous DRBG test

The WatchKey USB Token implements a continuous test for the DRBG based on NIST SP800-90. The token generates a minimum of 4 bytes per request. The n($4 \leqslant n \leqslant 128$) bytes data generated for every request is compared with the n bytes data generated from the previous request. If the generated data for two requests are identical, a conditional test error flag is raised. For the first request made to any instantiation of the DRBG SP800-90 implemented in the module, two internal 32 bytes cycles are performed and the generated data is compared.

The DRBG SP800-90 is seeded by the output of the IC hardware-based non-deterministic random number generator. Each new seed is compared with the previously saved generated seed. When two seeds have the same value, the module enters an error state. If the new seed is not identical to the previous one, DRBG accepts it as a valid input.

10 Design Assurance

10.1 Configuration Management

The WatchKey USB Token development team utilizes ClearCase and ClearQuest, 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.

ClearCase and ClearQuest integrate 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 details 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 WatchKey USB Token and subject to ClearCase control is detailed in the ***WatchKey USB Token Configuration Output Detail List*** provided by Watchdata.

10.2 Guidance and Secure Operation

This section describes how to configure the module for FIPS-Approved mode of operation. Operating the module without maintaining the following settings will remove the module from the FIPS-Approved mode of operation.

10.2.1 Cryptographic officer guidance

The initial login Password and unlock Password must be delivered to the Security Officer in a secure manner (e.g., in a sealed envelope via a trusted carrier).

The Security Officer must change the initial login Password and unlock Password of the module as soon as s/he receives the module.

The Security Officer must not disclose the Password and must store passwords in a safe location adhering to his/her organization’s systems security policies for Password storage.

The Security Officer must initialize the file structure and configure the cryptographic operations in accordance to the guidance given in WatchKey USB Token User Guidance.

10.2.2 User guidance

The details about the initialization procedures are described in the dedicated document “WatchKey USB Token User Guidance.”

As soon as the correctly initialized WatchKey token is plugged into an USB port of a host GPC, both red LED and green LED will blink, indicating the ongoing self-test. When the power-on self-test completes successfully, the green LED will remain on while the red LED will be off, indicating that the token is in FIPS mode. If the power-on self-test fails, then the token enters the error state.

Assuming that the user has also correctly installed the WatchSAFE Manager Tools on the host GPC by following instructions given in the User Guidance, he or she can confirm FIPS-

mode status by invoking WatchSAFE Manager Tools and observe the FIPS icon on the upper-left corner of its GUI window.

If a user invokes RSA signature generation/verification with 1024-bit key, the token enters into the non-FIPS mode. The non-FIPS mode is indicated by the red LED. The user can also observe the non-FIPS icon on the upper-left corner of WatchSAFE Manager Tools GUI window.

If the WatchKey token enters the non-FIPS mode, or is in an error state (which can be observed either by the status of LEDs or through the WatchSAFE Manager Tools), the token can be unplugged from its host GPC and re-plugged back into the GPC to enforce a power-up self-test. If the self-test completes successfully, the token will enter FIPS mode.

11 Mitigation of Other Attacks

No other attacks are mitigated.

Glossary

Term	Explanation
APDU	Application Protocol Data Unit and is the standard logical packet to communicate with a smartcard
CLA	Instruction class in a command APDU indicates the type of command
DF	Dedicated File in a smart card file structure, equivalent to an intermediate directory
EF	Elementary File in a smart card file structure, equivalent to a file
INS	Instruction code in a command APDU indicates the specific command
Lc	The number of bytes of command data in a command APDU to follow
Le	The maximum number of response bytes to expected after a command APDU
MF	Master File in a smart card file structure, equivalent to the root directory of a file system
P1, P2	Instruction parameters for a command APDU
PCB	Printed Circuit Board
SW1,SW2	Status words in a response APDU indicates the command processing status