Watchdata Technologies Pte Ltd.
7F Qiming International Mansion, No.101, Wangjing Lize Middle Park,
Chaoyang District, Beijing, P.R.China, 100102

Phone :（8610）6472 2288
（8610）8047 8166
Email : marketing@watchdata.com
Website : http://www.watchdata.com

WatchKey ProX USB Token Cryptographic Module

Hardware Version: K023314A

Firmware Version: 36410101

FIPS 140-2 Non-Proprietary Security Policy

Policy Version 1.0.2

Last Updated: 2015-06-11

Table of contents

1 Introduction

This document is the non-proprietary FIPS 140-2 Security Policy for the WatchKey ProX USB Token (“WatchKey”, “module” or “token”) 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 3 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 module must operate in order to be in the 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 ProX users and its application developers, testers at the Cryptographic Services Testing (CST) lab, and reviewers from CMVP.

The WatchKey ProX 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. The WatchKey ProX USB Token is used as the carrier of keys and certificates, and the processor of cryptographic algorithms. The WatchKey ProX USB Token communicates with the 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 ProX USB Token is a hardware cryptographic module validated against the FIPS 140-2 at security level 3. 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 100K FLASH for the on-card file system. The user's key pairs reside in the FLASH. 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 a 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 2.0 (full speed) specifications and USB CCID (Circuit(s) Cards Interface Device) protocol which enables communicating with ISO/IEC 7816 smart cards over USB. The Module also embodies an internal SPI Flash simulating CD-ROM, which provides the software package of mini-driver and allows the user to have a convenient experience.

2.2 Cryptographic Module Description

The cryptographic boundary of the module is defined as the entire WatchKey ProX USB Token itself.

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

Figure 1. WatchKey ProX USB Token-4 angles

The weight of the module is 7g and three dimension sizes of the module are approximately 52.1mm * 16.8mm * 7.9mm.

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

Component Type	Part Number or File Name and Version
Hardware	Smart Card Chip AS518, K023314A
Module Number	K8
Firmware	36410101.bin(include Watchdata-FIPS-TimeCOS Hardware Cryptographic Library V1.0.0.2)
Documentation	Security Policy for WatchKey ProX USB Token V1.0.2
	TimeCOS_PK Technique Manual V4.2
	WatchKey ProX USB Token_User Guidance V1.0.1
	WatchKey ProX USB Token _Finite State Module V1.10
	WatchKey ProX USB Token_High Level Design V1.7
	WatchKey ProX USB Token_Key Management Design V1.5
	WatchKey ProX USB Token_Configuration Management Overview V1.1
	WatchKey ProX USB Token_Configuration Output Detail List V1.0.0

Table 1. WatchKey ProX USB Token Cryptographic Module Components

2.3 Block Diagram

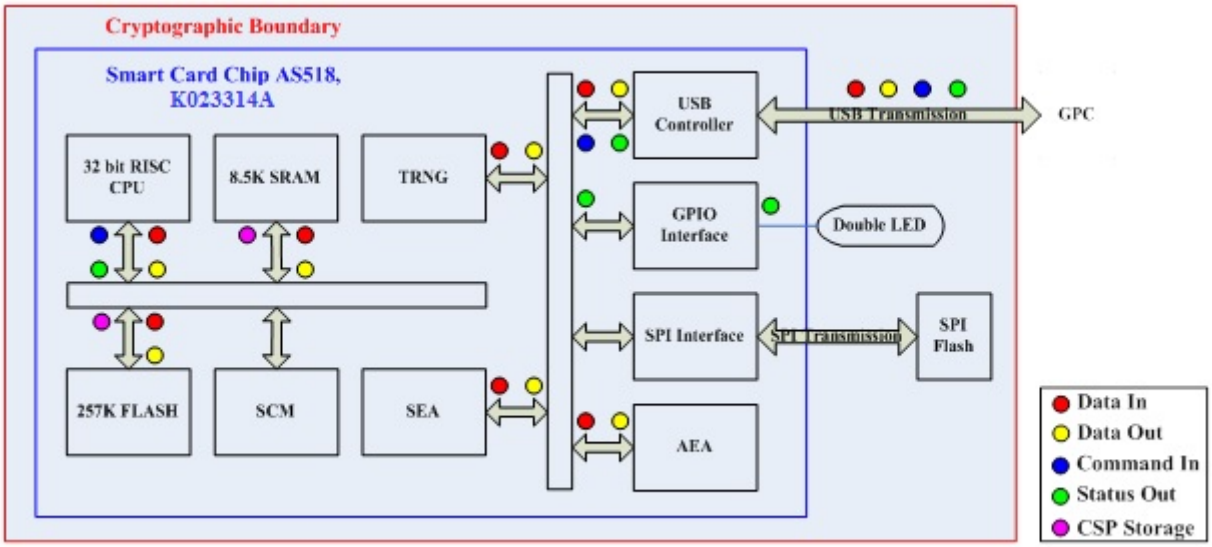

Figure 2. WatchKey ProX USB Token Hardware Block Diagram

Note: 100 K of 257K Flash is used for file system, and 157 K left is used for code storage.

Figure 3. WatchKey ProX 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 an overall Security Level 3. 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	3
Cryptographic Module Ports and Interfaces	3
Roles, Services and Authentication	3
Finite State Model	3
Physical Security	3
Operational Environment	N/A
Cryptographic Key Management	3
EMI/EMC	3
Self Tests	3
Design Assurance	3
Mitigation of Other Attacks	N/A

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

2.5 Approved Mode(s) of operation

When the WatchKey ProX USB Token is plugged-in to a host PC, the module performs power-up self-test automatically. Once the successful completion of the power-up self-test, the module will enter FIPS mode automatically.

In FIPS mode, the module provides the FIPS-Approved algorithms, along with RSA encrypt/decrypt with 2048-bit keys and HW RNG. RSA encrypt/decrypt are FIPS-Allowed algorithms to be used in FIPS mode for key wrapping (also known as key transport) as a method of key establishment. WatchKey uses RSA encrypt/decrypt to wrap data in transit. The HW RNG is a Non-Approved nondeterministic RNG implemented in the module for seeding the Approved DRBG.

The WatchKey ProX USB Token implements the list of FIPS-Approved algorithms shown in Table 3 when operated in FIPS-mode.

Algorithm w/modes	Keys/CSPs	Usage	Standards	Algorithm Certificate #
AES (ECB, CBC,OFB)	128, 192, 256 bit keys	Encryption/ Decryption	FIPS 197	3196
Triple-DES (ECB,CBC,OFB)	3-key 168 bits	Encryption/ Decryption	SP 800-67	1822
CMAC (AES)	128, 192, 256 bit AES keys	Calculate MAC (Generation/ Verification)	SP 800-38B	3196
CMAC (Triple-DES)	3-key Triple-DES 168 bits	Calculate MAC (Generation/ Verification)	SP 800-38B	1822
RSA Key Generation	Modulus sizes: 2048 Public Key values: 65537	Generate 2048 bits RSA Key pairs	FIPS 186-4	1630
RSA (PKCS#1 1.5) Signature Generation	Modulus sizes: 2048 Public Key values: 65537	Generate RSA signature with SHA-256, SHA-384 or SHA-512		
RSA (PKCS#1 1.5) Signature Verification	Modulus sizes: 1024, 2048 Public Key values: 65537	Verify RSA signature with SHA-1, SHA-256, SHA-384 or SHA-512		
ECDSA Key Generation	P-256	Generate ECDSA Key pairs	FIPS 186-4	585
ECDSA Public Key Validation	P-192, P-256	Public Key Validation		
ECDSA Signautre Generation	P-256	Generate ECDSA signature with SHA-256, SHA-384 or SHA-512		
ECDSA Signautre Verification	P-192, P-256	Verify ECDSA signature with SHA-1, SHA-256, SHA-384 or SHA-512		

Algorithm w/modes	Keys/CSPs	Usage	Standards	Algorithm Certificate #
SHA-1, SHA-256, SHA-384, SHA-512 (BYTE-only)	N/A	Hashing	FIPS 180-4	2647
DRBG (Hash based with SHA-256)	Entropy input string, seed, V and C	Random number generation	SP 800-90A	673

Table 3. FIPS-Approved Cryptographic Algorithms

The module also supports non-compliant key size of FIPS-Approved algorithms in Non-FIPS Mode. When the Non-Approved services are called, the module will enter the Non-FIPS mode automatically with the Red LED on and Green LED off as Non-FIPS mode indicators. The module cannot switch back to FIPS mode unless the power-up self-tests is called again (i.e. the token is unplugged and then plug in the host again, or on-demand self-test APDU command is called.) The module does not share the non-compliant key pairs between FIPS and Non-FIPS mode, and the non-compliant key pairs are generated by the non-Approved HW RNG in non-FIPS mode. The Non-FIPS-Approved algorithms implemented by the WatchKey ProX USB Token are listed in Table 4.

Algorithm w/modes	Keys/CSPs	Usage	Operate in FIPS-mode
HW RNG	N/A	Generate entropy bits for seeding the Approved DRBG	Yes and No
RSA Key Generation	Modulus sizes: 1024 Public Key values: 65537	Generate 1024 RSA Key pairs	No
RSA (PKCS #1 1.5) Signature Generation	Modulus sizes: 1024 Public Key values: 65537	Generate RSA signature with SHA-1, SHA-256, SHA-384 or SHA-512	No

Algorithm w/modes	Keys/CSPs	Usage	Operate in FIPS-mode
RSA Encryption and Decryption	Modulus sizes: 1024 Public Key values: 65537	RSA Key Wrapping and Unwrapping	No
	Modulus sizes: 2048 Public Key values: 65537		Yes
RSA (PKCS #1 1.5) Signature Generation	Modulus sizes: 1024 Public Key values: 65537	Generate RSA signature with SHA-1, SHA-256, SHA-384 or SHA-512	No
ECDSA Key Generation	P-192	Generate ECDSA Key pairs	No
ECDSA Signature Generation	P-192	Generate ECDSA signature with SHA-1, SHA-256, SHA-384 or SHA-512	No
ECDSA Encryption	P-192	Calculate ECDSA encryption	No
ECDSA Decryption	P-192	Calculate ECDSA decryption	No

Table 4. Non-FIPS-Approved Cryptographic Algorithms

Note: The module supports 2048 bits RSA Key Wrapping and Unwrapping in FIPS mode which provides 112 bits of encryption strength, and 1024 bits non-compliant RSA Key Wrapping and Unwrapping in non-FIPS mode.

The module uses 2 LEDs (red and green) to differentiate the FIPS relevant state. The module also provides an APDU command (i.e. APDU 808A000003) for the user (through the host PC application) to query the state which the module is in at any time. The module returned three bytes in response to indicate its current state. The interpretation of the response values is documented in detail in TimeCOS_PK Technique Manual V4.2.

Red LED	Green LED	State
off	off	Power off
off	blink	Self Test
on	off	Non-FIPS
off	on	FIPS
blink	off	Error

Table 5. LED for Current State Indicator

3 Cryptographic Module Ports and Interfaces

The interfaces for the cryptographic module include the physical ports of the WatchKey ProX 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 ProX 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 6. Ports and Interface of the WatchKey ProX USB Token

The USB 2.0 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 ProX USB Token refer to Chapter 8 Command and Response of TimeCOS_PK Technique Manual V4.2.

4 Roles, Services and Authentication

The module has an embedded smart card chip, which has an on-Card Operating System (COS) and on-Card File System (CFS). The CFS of the module complies with ISO/IEC 7816-4 and supports multiple levels of directory structure. Basically, there are three types of file: Master File (MF), Dedicated File (DF) and Elementary File (EF). MF is the root directory of the entire file system, DF is the directory file that contains child directory files or EF, and EF is the file that storage the data.

The life cycle of the module is described in order: Manufacture stage, Issue stage and Application stage. Manufacture stage is only available in the factory to setup the file structure and generate default keys and authentication data. Issue stage is available to the token issuers (e.g. banks) to change the keys and CSPs. Application stage is available to end user to perform the services provided by the module. Once the module moves from one stage to another which requires Security Office authentication, it cannot go back to the previous stage(s).

4.1 Roles

The WatchKey ProX USB Token supports two types of roles: User Role and Security Officer Role. The Security Officer role is equivalent to the Crypto Officer role in FIPS 140-2 validation.

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

In Application stage, the Security Officer Role can create files, read and update the Security Officer files, unblock the User PIN and manage the token in Application stage. In addition to the services available in Application stage, the Security Officer Role can also initialize the application, initialize the Module, import and update keys, configure the Module, set Life Cycle and serial number of the token in the Manufacturer stage and Issue stage.

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

4.2 Services

Available services for an operator depend on the type of role he or she is authenticated and the identity he or she is verified.

Each operator does not have access right to the files that belong to other operators.

The services provided by the WatchKey ProX USB Token are through the documented APDU commands. They are invoked by the host application toolkit (i.e. WatchSafe 4.2.0).

All services that required authentication provided by the WatchKey ProX USB Token are listed in Table 7 below, along with their associated CSPs and modes.

Service	Description	Keys/CSPs	Mode
User Login	A successful external entity authentication and verification of USER PIN	User PIN	FIPS/ Non-FIPS

Service	Description	Keys/CSPs	Mode
Change User PIN	Verify and change PIN	User PIN	FIPS
Unblock User PIN	Unblock PIN	Security Officer PIN User PIN	FIPS
Security Officer Login	A successful external entity authentication and verification of Security Officer PIN	Security Officer PIN	FIPS/ Non-FIPS
Change Security Officer PIN	Verify and change PIN	Security Officer PIN	FIPS
Security Officer File Read	Read Binary	Security Officer PIN Secure Messaging Key Secure Messaging Mac Key	FIPS/Non-FIPS
Security Officer File Update	Update Binary	Security Officer PIN Secure Messaging Key Secure Messaging Mac Key	FIPS/ Non-FIPS
User File Read	Read Binary	User PIN Secure Messaging Key Secure Messaging Mac Key	FIPS/ Non-FIPS
User File Update	Update Binary	User PIN Secure Messaging Key Secure Messaging Mac Key	FIPS/ Non-FIPS
Initialize the Application	Erase DF that holds application in order for the application related files to be re-created	Initializing Application Key	FIPS
Restore Default Application	Clear the content for all the files under the DF that holds application, except for secret key files, and restore Security Officer PIN and User PIN to default value.	Security Officer PIN	FIPS

Service	Description	Keys/CSPs	Mode
Initialize the Module	Erase MF	Initializing Module Key	FIPS
RSA Signature Verification (1024/2048)	Verify Signatures	User PIN RSA Public Key	FIPS
RSA Signature Generation (2048)	Generate Signatures with SHA-256, SHA-384 or SHA-512	User PIN RSA Private Key	FIPS
RSA Signature Generation (1024)	Generate Signatures	User PIN RSA Private Key	Non-FIPS
RSA Encrypt/Decrypt (2048)	RSA encryption/decryption for data transit	User PIN RSA Public Key RSA Private Key	FIPS
RSA Encrypt/Decrypt (1024)	RSA encryption/decryption for data transit	User PIN RSA Public Key RSA Private Key	Non-FIPS
ECDSA Signature Verification (P-192/P-256)	Verify Signatures	User PIN ECDSA Public Key	FIPS
ECDSA Signature Generation (P-256)	Generate Signatures with SHA-256, SHA-384 or SHA-512	User PIN ECDSA Private Key	FIPS
ECDSA Signature Generation (P-192)	Generate Signatures	User PIN ECDSA Private Key	Non-FIPS
ECDSA Encrypt/Decrypt (P-192)	ECDSA encryption/decryption for data transit	User PIN ECDSA Public Key ECDSA Private Key	Non-FIPS
Generate RSA Key(2048)	Generate RSA Key	User PIN RSA Public Key RSA Private Key	FIPS

Service	Description	Keys/CSPs	Mode
Generate RSA Key(1024)	Generate RSA Key	User PIN RSA Public Key RSA Private Key	Non-FIPS
Generate ECDSA Key(P-256)	Generate ECDSA Key	User PIN ECDSA Public Key ECDSA Private Key	FIPS
Generate ECDSA Key(P-192)	Generate ECDSA Key	User PIN ECDSA Public Key ECDSA Private Key	Non-FIPS
Import RSA Key Pair (1024/2048)	Import RSA key pair	User PIN RSA Public Key RSA Private Key	FIPS
Import Key	Write key	User PIN Security Officer PIN KEK Secure Messaging Key Secure Messaging Mac Key Initializing Module Key Initializing Application Key Device Encryption Key Encryption/Decryption Key External Entity Authentication Key	FIPS
Update key	Modify key	User PIN Security Officer PIN KEK	FIPS

Service	Description	Keys/CSPs	Mode
		Secure Messaging Key Secure Messaging Mac Key Initializing Module Key Initializing Application Key Device Encryption Key Encryption/Decryption Key External Entity Authentication Key	
Create Application	Create Application related files	Initializing Application Key	FIPS
Create User File	Create file that owned by User	User PIN	FIPS
Delete User File	Delete file that owned by User	User PIN	FIPS
Create SO File	Create file that owned by Security Officer	Security Officer PIN	FIPS
Delete SO File	Delete file that owned by Security Officer	Security Officer PIN	FIPS
Data Encrypt/Decrypt	AES /Triple-DES Algorithm	Encryption/Decryption Key User PIN Security Office PIN	FIPS
Set Life Cycle	Set the life cycle of module	Security Officer PIN	FIPS
Erase RSA Key	Destruct the key value	User PIN RSA Public Key RSA Private Key	FIPS
Erase ECDSA Key	Destruct the key value	User PIN ECDSA Public Key ECDSA Private Key	FIPS

Service	Description	Keys/CSPs	Mode
Set Serial Number	Set the unique serial number	Security Officer PIN	FIPS
Initiate Configuration Information	Initiate non-security relevant configuration information of module in Manufacture stage only.	N/A	FIPS

Table 7. Authenticated Services with CSPs and modes

All services that do not require any authentication provided by WatchKey ProX USB Token are listed in Table 8 below, along with their associated CSPs and modes.

Service	Description	Keys/CSPs	Mode
Get Challenge	Get random digits	Seed, Entropy Input String, V and C	FIPS/ Non-FIPS
External entity Authentication	External entity authentication is used for the Token to authenticate the external entity.	External Entity Authentication Key KEK	FIPS/ Non-FIPS
Internal Authentication	Internal Authentication is used for the external entity to authenticate the Token	Encryption/Decryption Key Secure Messaging Mac Key	FIPS/ Non-FIPS
Select File	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.	N/A	FIPS/ Non-FIPS
Data Compress	Data Compress（SHA-1/SHA-256/SHA-384/SHA-512）	N/A	FIPS/ Non-FIPS
Restart	Reset the state	N/A	FIPS/ Non-FIPS
Self Test	Self-test	N/A	FIPS/ Non-FIPS
Get State	Get the operational state	N/A	FIPS/ Non-FIPS
Inquire Life Cycle	Inquire the life cycle of module	N/A	FIPS/ Non-FIPS

Service	Description	Keys/CSPs	Mode
Inquire Serial Number	Inquire serial number of module	N/A	FIPS/ Non-FIPS
Get COS Information	Get the information about the security functions that the Token supports	N/A	FIPS/ Non-FIPS
Get Release Space	Get the size of space left in the Token	N/A	FIPS/ Non-FIPS
Get Device Information	Get the device descriptor or the firmware check code of the Token	N/A	FIPS/ Non-FIPS
Session Key Management	Create a security channel between module and GPC	Device Encryption Key Session Key	FIPS/ Non-FIPS

Table 8. Un-authenticated Services with CSPs and modes

For details regarding service inputs, corresponding service outputs and description of each service, please refer to Chapter 9, 10 and 11 of TimeCOS_PK Technique Manual V4.2.

The relations between services, role of operator and life cycle are listed in Table 9 below.

Service	User	Security Officer	Manu-facture Stage	Issue Stage	Appli-cation Stage
User Login	√		√	√	√
Change User PIN	√		√	√	√
Unblock User PIN		√	√	√	√
Security Officer Login		√	√	√	√
Change Security Officer PIN		√	√	√	√
Get Challenge*			√	√	√
External entity Authentication*			√	√	√
Internal Authentication*			√	√	√
Select File*			√	√	√

Service	User	Security Officer	Manu-facture Stage	Issue Stage	Appli-cation Stage
Security Officer File Read		√	√	√	√
Security Officer File Update		√	√	√	√
User File Read	√		√	√	√
User File Update	√		√	√	√
Initialize the Application		√	√		
Restore Default Application		√	√	√	√
Initialize the Module		√	√		
RSA Signature Verification (1024/2048)	√				√
RSA Signature Generation (2048)	√				√
RSA Signature Generation (1024)	√				√
RSA Encrypt/Decrypt (2048)	√				√
RSA Encrypt/Decrypt (1024)	√				√
ECDSA Signature Verification (P-192/P-256)	√				√
ECDSA Signature Generation (P-256)	√				√
ECDSA Signature Generation (P-192)	√				√
ECDSA Encrypt/Decrypt (P-192)	√				√
Data Compress*			√	√	√

Service	User	Security Officer	Manu-facture Stage	Issue Stage	Appli-cation Stage
Generate RSA Key(2048)	√				√
Generate RSA Key(1024)	√				√
Generate ECDSA Key(P-256)	√				√
Generate ECDSA Key(P-192)	√				√
Import RSA Key Pair (1024/2048)	√				√
Import Key		√	√		
Update key		√	√	√	
Create Application		√	√		
Create User File	√				√
Delete User File	√				√
Create SO File		√		√	√
Delete SO File		√		√	√
Restart*			√	√	√
Data Encrypt/Decrypt	√	√	√	√	√
Self Test*			√	√	√
Get State*			√	√	√
Set Life Cycle		√	√	√	
Inquire Life Cycle*			√	√	√
Erase RSA Key	√				√
Erase ECDSA Key	√				√
Set Serial Number		√	√		

Service	User	Security Officer	Manu-facture Stage	Issue Stage	Appli-cation Stage
Inquire Serial Number*			√	√	√
Get COS Information*			√	√	√
Get Release Space*			√	√	√
Get Device Information*			√	√	√
Session Key Management*			√	√	√
Initiate Configuration Information		√	√		

Table 9. Services Authorized for Roles and Life Cycle

Note: A * indicates that the service does not require any authentication.

4.3 Operator Authentication

The WatchKey ProX USB Token supports identity-based authentication to authenticate different identities. The authentication method in Manufacture stage, Issue stage and Application stage is described in the following sections.

Only one operator can login to the WatchKey ProX USB Token at the same time. The module does not support concurrent operators.

The module ensures that there is no visible display of the authentication data. 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 power of module 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 7 are available only to operators with the authenticated role(s).

4.3.1 Authentication in Manufacture stage

Only Security Officer is allowed in Manufacture stage. The operator is required to perform external authentication with the Initializing Module Key or Initializing Application Key to grant their Security Officer role. These two keys are only known by the manufacturer.

4.3.2 Authentication in Issue stage

Only Security Officer is allowed in Issue stage. The operator can authenticate his or her identity by entering the Security Officer PIN to perform Update Key or Restore Default Application at Issue Stage.

4.3.3 Authentication in Application Stage

Identities of operators of the WatchKey ProX USB Token with the User Role or the Security Officer Role are authenticated by successful verifying the corresponding password (i.e. User PIN or Security Officer PIN.)

Each operator of the Token has his or her unique PIN, while files in the Token are assigned to each operator when created during the initialization phase at the factory. The operator can only perform services with files assigned to him or her after authenticating their identity.

4.3.4 Security Rules for PINs

The initial Security Officer Passwords and default User Password are written into the WatchKey ProX USB Tokens when they are manufactured. The initial Security Officer Passwords are for token issuers (e.g. banks) who use the Security Officer Role to initialize the Application before they are issued to the final users. Both the initial Security Officer Password and default User Password are distributed via a User Guide brochure in a secure manner, which is compliant to the corporation security handling process and procedure of manufacturer and the token issuers.

When the Security Officer and User receive the WatchKey ProX USB Token at the first time, he or she should change their Password immediately by using the ‘Verify and Change PIN’ command.

4.4 Password Strength

4.4.1 Initializing Module/Application Key

The Initializing Module Key and the Initializing Application Key are either an AES 128/192/256 Key or a 3–key Triple-DES key. The minimum length of the key is 128 bits. The probability that a random attempt will succeed using this authentication method is $1/2^{128}$, which is less than 1/1,000,000. The probability that a random attempt will succeed over a one minute interval is definitely less than 1/100,000.

4.4.2 User and Security Officer Password

Passwords for User and Security Officer Role authentication must be in the range of 6-32 characters. The Password must contain a mix of letters, numeric characters, and special characters. Assuming a mix of lower case letters, upper case letters, numeric characters, 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 $1/62^6$, which is less than 1/1,000,000. Assuming 10 attempts per second via a scripted or automatic attack, the probability of a success with multiple attempts in a one minute period is $600/62^6$, 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 $15/62^6$, which is less than 1/100,000.

The password will be turned into a 24 byte PIN by an algorithm (SHA-256 hashed calculation to get first 24 bytes of 32 bytes).

PINs are stored in the WatchKey ProX USB Token in a hashed form with 32-byte fixed length, while the first 24 bytes are used as PIN.

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 with standard passivation (a sealing coat applied over the chip circuitry to protect it against environmental and other physical damage) and is housed in a sealed, hard plastic enclosure that has no openings, vents or doors. It cannot be opened without damage.

6 Operational Environment

The module operates in a limited operational environment and does not implement a General Purpose Operating System. Once the firmware of the module is loaded on the WatchKey ProX USB Token, it cannot be modified or erased. The operational environment requirements do not apply to the module.

7 Key Management

The module supports keys for normal usages and a key encryption key (KEK).

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

Key/CSP	Key Type	Description
KEK	AES 128/192/256 Key, 3–key Triple-DES key	Used to wrap the other keys
External entity Authentication Key	AES 128/192/256 Key, 3–key Triple-DES key	Involved in authenticating to the further use of Roles
Initializing Module Key	AES 128/192/256 Key, 3–key Triple-DES key	To Erase MF in factory ONLY
Initializing Application Key	AES 128/192/256 Key, 3–key Triple-DES key	To Delete DF in factory ONLY
Device Encryption Key	AES 128/192/256 Key, 3–key Triple-DES key	Used to generate Session Key by encrypting a random number generated by SP 800-90A DRBG
Secure Messaging Key	AES 128/192/256 Key, 3–key Triple-DES key	Used for secure transmission of files between module and the external entity
Secure Messaging Mac Key	AES 128/192/256 Key, 3–key Triple-DES key	For computing the MAC
Encryption/ Decryption Key	AES 128/192/256 Key, 3–key Triple-DES key	Cryptographic operation with AES/Triple-DES
Session Key	AES 128 Key, 3–key Triple-DES key	Do cryptographic operation with AES/Triple-DES on the data transmitted between module and GPC
RSA Private Key	1024/2048 RSA private key	Generates Signatures, Decryption User Role only

Key/CSP	Key Type	Description
RSA Public Key	1024/2048 RSA public key e = 010001	Verifies Signature, Encryption User Role only
ECDSA Private Key	P-192/P-256 ECDSA private key	Generates Signatures, User Role only
ECDSA Public Key	P-192/P-256 ECDSA public key	Verifies Signature, User Role only
User PIN	24 bytes PIN	Involved in authenticating User Role
Security Officer PIN	24 bytes PIN	Involved in authenticating Security Officer Role or unblocking User PIN
Seed for SP 800-90A DRBG	256 bits random number	Seeding the SP 800-90A DRBG

Table 10. Keys and CSPs

7.1 Random Number Generator

The WatchKey ProX USB Token uses a FIPS-Approved Deterministic Random Bit Generator (DRBG) based on SP 800-90A for random number generation and asymmetric key generation. The module implements a hash based DRBG, Hash_DRBG, which generates 256-bits random value per request.

The 256-bit seeds for SP 800-90A DRBG are provided by the IC hardware-based non-deterministic random number generator (HW RNG). The module also implements the health checks described in section 11.3 of SP 800-90A and Continuous Random Number Generator Test to ensure that two consecutively seeds are not identical before the later one is used as a valid input to seed the SP 800-90A DRBG.

7.2 Key Generation

The module uses an FIPS-Approved SP 800-90A DRBG as inputs to create the following keys/CSPs:

- RSA key pairs
- ECDSA key pairs
- Session key

RSA key pairs can be generated inside the module by using the Generate RSA Key service. They can also be imported by a User who uses the Import RSA Key Pair service.

The ECDSA key pair can only be generated inside the module by using the Generate ECDSA Key service.

The Session Key is generated automatically at the Application stage of the life cycle for each secure channel. It is generated by using the FIPS-Approved 3-keyed Triple-DES or AES 128-bit algorithm to encrypt a random number provided by SP 800-90A DRBG with the Device Encryption Key.

When generating a pair of RSA Keys, the module uses the algorithm specified in SP 800-90A DRBG to generate a group of random numbers as prime numbers, and then uses these random numbers to generate the key pair in accordance with the RSA key generation algorithm described in the standard FIPS 186-4.

When generating a pair of ECDSA Keys, the module uses the algorithm specified in SP 800-90A DRBG to generate a random numbers as prime numbers, and then uses the random number to generate the key pair in accordance with the ECDSA key generation algorithm described in the standard FIPS 186-4.

7.3 Key Entry and Output

Columns “Generate/Input” and “Output” in Table 11 show the key entry and output for all keys and CSPs used by the WatchKey ProX. All keys except the RSA key, ECDSA key and Session Key are imported in the factory. 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, the device manager that runs on the host GPC turns the password into a 24-byte PIN and sends it using the Verify PIN & Change PIN APDU command to WatchKey for verification or changing of the PIN stored on the device.

In the Issue and Application stage, all the data transactions between the module and external entity such as host PC are protected by a secure channel. When connecting the WatchKey ProX USB Token to an external entity, the “Session Key Management” service is required by the module to establish a secure channel before performing cryptographic or security service. All the APDU commands in the secure channel are protected by the Session Key. The Session Key between the Token and the external entity is a 3-key Triple-DES key or AES 128/192/256 Key. This is a diversified key obtained by using the Device Encryption Key to encrypt a random number. The Device Encryption Keys for all tokens are diversified keys obtained from the unique serial number of the Token, and 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 algorithm used for the key diversification. When the external entity establishes a secure channel with the Token, it retrieves the serial number from the Token and calculates the Device Encryption Key for this Token. Then the external entity uses the Device Encryption Key to encrypt the random number to get the Session Key. The external entity uses the Session Key to encrypt the random number and send the result to the Token for authentication. If the calculated key matches with the Session key stored on the Token, then the secure channel is established successfully.

If the “Session Key Management” service is not preformed, no cryptographic or security function is allowed. Only the non-security relevant services such as Get Response, Inquire Life Cycle, Self-Test, Get Device Information and Restart can be executed.

7.4 Key Storage, Protection and Destruction

The module stores the keys in the FLASH of the embedded Smart Card chip. Data in the FLASH is protected by the secure design of the Smart Card chip. The memory is scrambled and obfuscated.

In the Manufacture stage, all the keys under the Application DF can be deleted by the Security Officer using the erase EF/DF APDU command (i.e. Initialize the Application.) All the keys under the MF file structure can be deleted by the Security Officer using the erase MF APDU command (i.e. Initialize the Module.) In the Application stage, only the RSA key pair and ECDSA key pair can be deleted by the User using the erase File Content APDU command.

The zeroization is performed by filling the memory area with “FF”. It is performed immediately after the zeroization APDU commands are called.

The following table describes key generation, key input, key output, key storage and key zeroization for each key and KEK in the module.

Key/CSP	**Generate/** **Input**	**Output**	**Storage**	**Zeroization**
Key Encryption Key (KEK)	Externally generated and initially entered in plaintext form in factory by Security officer The key is encrypted by Initializing Application Key to enter the module for services.	Never exits the module	Stored in plaintext in FLASH Stored under DF	By Erase DF/EF APDU command “00E4000002Data” or by Erase MF APDU command “800E000000”
External entity Authentication Key	Externally generated and initially entered in plaintext form in factory by Security officer The key is encrypted by KEK to enter the module for services.	Never exits the module	Stored in plaintext in FLASH Stored under DF	By Erase DF/EF APDU command “00E4000002Data” or by Erase MF APDU command “800E000000”
Initializing Module Key	Externally generated and initially entered in plaintext form in factory by Security officer The key is encrypted by Initializing Application Key to enter the module for services.	Never exits the module	Stored in plaintext in FLASH Stored under MF	By Erase MF APDU command “800E000000”

Key/CSP	Generate/ Input	Output	Storage	Zeroization
Initializing Application Key	Externally generated and initially entered in plaintext form in factory by Security officer	Never exits the module	Stored in plaintext in FLASH Stored under MF	By Erase MF APDU command “800E000000”
Device Encryption Key	Externally generated and initially entered in plaintext form in factory by Security officer The key is encrypted by Initializing Application Key to enter the module for services.	Never exits the module	Stored in plaintext in FLASH Stored under MF	By Erase MF APDU command “800E000000”
Secure Messaging Key	Externally generated and initially entered in plaintext form in factory by Security officer If this key is stored under MF, it is encrypted by Initializing Application Key. If this key is stored under DF, it is encrypted by KEK to enter the module for services.	Never exits the module	Stored in plaintext in FLASH Stored under MF or DF	By Erase DF/EF APDU command “00E4000002Data” or by Erase MF APDU command “800E000000”
Secure Messaging Mac Key	If this key is stored under MF, it is externally generated and initially entered in plaintext form in factory by Security officer If this key is stored under DF, it is encrypted by KEK to enter the module for services.	Never exits the module	Stored in plaintext in FLASH Stored under MF or DF	By Erase DF/EF APDU command “00E4000002Data” or by Erase MF APDU command “800E000000”
Session Key	Generated by the module using Triple-DES or AES encryption on a random number generated by SP 800-90A DRBG with Device Encryption Key	Never exits the module	Stored in plaintext in volatile memory	Power off or by Session Key Management APDU command “84EF020005Data”

Key/CSP	Generate/ Input	Output	Storage	Zeroization
Encryption/ Decryption Key	Externally generated and initially entered in plaintext form in factory by Security officer The key is encrypted by KEK to enter the module for services.	Never exits the module	Stored in plaintext in FLASH Stored DF	By Erase DF/EF APDU command “00E4000002Data” or by Erase MF APDU command “800E000000”
RSA Private Key	Generated by the module using RSA Key Generation APDU command or Imported by User using Import RSA Key Pair APDU command.	Never exits the module	Stored in plaintext in FLASH Stored under EF	By Erase DF/EF APDU command “00E4000002Data” or by Erase MF APDU command “800E000000”or by Erase File Content APDU command “807AP1P200”
RSA Public Key	Generated by the module using RSA Key Generation APDU command or Imported by User using Import RSA Key Pair APDU command.	By Read Binary APDU command “00B00000Le”	Stored in plaintext in FLASH Stored under EF	By Erase DF/EF APDU command “00E4000002Data” or by Erase MF APDU command “800E000000” or by Erase File Content APDU command “807AP1P200”
ECDSA Private Key	Generated by the module using ECDSA Key Generation APDU command	Never exits the module	Stored in plaintext in FLASH Stored under EF	By Erase DF/EF APDU command “00E4000002Data” or by Erase MF APDU command “800E000000” or by Erase File Content APDU command “807AP1P200”
ECDSA Public Key	Generated by the module using ECDSA Key Generation APDU command	By Read Binary APDU command “00B00000Le”	Stored in plaintext in FLASH Stored under EF	By Erase DF/EF APDU command “00E4000002Data” or by Erase MF APDU command “800E000000” or by Erase File Content APDU

Key/CSP	Generate/ Input	Output	Storage	Zeroization
				command “807AP1P200”
User PIN	Externally generated and initially entered in plaintext form in factory by Security officer The hashed and truncated User PIN is encrypted by KEK to enter the module for authentication.	Never exits the module	Stored in SHA-256 hashed form in FLASH Stored under DF	By Erase DF/EF APDU command “00E4000002Data” or by Erase MF APDU command “800E000000”
Security Officer PIN	Externally generated and initially entered in plaintext form in factory by Security officer The hashed and truncated Security Officer PIN is encrypted by KEK to enter the module for authentication.	Never exits the module	Stored in SHA-256 hashed form in FLASH Stored under DF	By Erase DF/EF APDU command “00E4000002Data” or by Erase MF APDU command “800E000000”
Seed for SP800-90A DRBG	Internally generated by the HW RNG within the module.	Never exists the module	Stored in plaintext in volatile memory	Internal API function call

Table 11. Key Generation, Input/Output, Storage and Zeroization

Note:
1. 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.
2. The “P1P2” field in the Erase File Content APDU command “807AP1P200” is a 2-byte file identifier of an EF to be erased.
3. The “Data” field in the Session Key Management APDU command “84EF020005Data is combination of one byte channel number and four bytes process ID encrypted with Session Key.

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: Y97-PROXKEY001.

9 Self-Tests

The WatchKey ProX 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 ProX USB Token into a USB port of a GPC. The on-demand self-test can be invoked by the Self-Test APDU command, or unplugging the token and plugging it back to reinitiated the power-up self-test.

If the self-test is successful, then the module enters the FIPS-Approved operational state and it is indicated by a steady green LED indicator. If any self-test fails, the module enters an error state and returns an error code with a description of the error. The error state is indicated by a blinking 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 the self-tests are successfully completed.

9.1 Power-Up Tests

The WatchKey ProX USB Token performs power-up self-tests automatically without any operator intervention when it is plugged into a USB port of a GPC.

Whenever the power-up self-tests is initiated, the module performs the integrity test and the cryptographic algorithm Known Answer Test (KAT). If the self-test result does not match with the expected result, the self-test fails. If any of these tests fails, the module enters the error state.

9.1.1 Integrity Test

The WatchKey ProX USB Token uses CRC-16 for the integrity test of its firmware. Cyclic Redundancy Check (CRC) is an error detecting code to calculate a check value that is based on the remainder of a polynomial division of the input content. CRC-16 means the polynomial length is 17 bits. When the module is power-up, the module will generate the check value of the memory that stores the executing code and compare with the existing value stores in the FLASH memory. If the values do not match, the integrity test fails and the module enters the error state.

9.1.2 Cryptographic algorithm KAT

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

- AES encryption and decryption tested separately
- Triple-DES encryption and decryption tested separately
- CMAC for Triple-DES and AES
- RSA signature generation and verification tested separately
- RSA encryption and decryption tested separately

- ECDSA signature generation and verification tested separately
- SP 800-90A DRBG
- SHA-1
- SHA-256
- SHA-512

9.2 Conditional Tests

9.2.1 Pair-wise consistency test

The WatchKey ProX USB Token performs the pair-wise consistency test for each pair of RSA keys and ECDSA keys that it generates. The consistency of the key pair used for signature generation and verification is tested by calculating and verifying a digital signature. The consistency of the key pair used for encryption and decryption is tested by encrypting and decrypting a given data.

9.2.2 Continuous DRBG test

The WatchKey ProX USB Token implements a continuous test for the DRBG based on NIST SP 800-90A. 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 for 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 SP 800-90A implemented in the module, two internal 32 bytes cycles are performed and the generated data are compared.

The SP 800-90A DRBG is seeded by the output of the IC hardware-based non-deterministic random number generator (HW RNG). 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 the DRBG accepts it as a valid input.

10 Design Assurance

10.1 Configuration Management

The WatchKey ProX 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 ProX USB Token and subject to ClearCase control is detailed in the ***WatchKey ProX USB Token_Configuration Output Detail List V1.0.0*** 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 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 of the module as soon as he or she 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 ProX USB Token_User Guidance V1.0.1***.

10.2.2 User Guidance

The details about the initialization procedures are described in the dedicated document ***WatchKey ProX USB Token_User Guidance V1.0.1***.

As soon as the correctly initialized WatchKey token is plugged into a USB port of a host GPC, the red LED will remain off while the 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 remain 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 in the upperleft corner of its GUI window.

If a user invokes RSA signature generation/verification with a 1024-bit key or ECDSA signature generation/verification with a P-192 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 Prox USB 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
GPC	General Purpose Computer
INS	Instruction code in a command APDU indicates the specific command
KEK	Key Encryption Key
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

Reference

[1] FIPS 140-2 Standard, http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf
[2] FIPS 140-2 Implementation Guidance, http://csrc.nist.gov/groups/STM/cmvp/documents/fips140-2/FIPS1402IG.pdf
[3] FIPS 140-2 Derived Test Requirements, http://csrc.nist.gov/groups/STM/cmvp/documents/fips140-2/FIPS1402DTR.pdf
[4] FIPS 197, Advanced Encryption Standard (AES), http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf
[5] FIPS 180-4 Secure Hash Standard, http://csrc.nist.gov/publications/fips/fips180-4/fips-180-4.pdf
[6] FIPS 186-4, Digital Signature Standard, http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf
[7] NIST SP 800-67 Revision 1, Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher, http://csrc.nist.gov/publications/nistpubs/800-67-Rev1/SP-800-67-Rev1.pdf
[8] NIST SP 800-90A, Recommendation for Random Number Generation Using Deterministic Random Bit Generators, http://csrc.nist.gov/publications/nistpubs/800-90A/SP800-90A.pdf
[9] NIST SP 800-38B, Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication, http://csrc.nist.gov/publications/PubsFIPS.html

