赞嘉电子科技(北京)有限公司

Zanjia Electronic Science & Technology (Beijing) Co., LTD

HSM-ZJ2014

FIPS 140-2 Non-Proprietary

Security Policy

Document Version: 1.1

Last Update: 2016-06-15

Prepared by:

atsec information security corporation

9130 Jollyville Road, Suite 260

Austin, TX 78759

www.atsec.com

Table of Contents

1 Introduction ... 1
1.1 Purpose of the Security Policy ... 1
1.2 Target Audience ... 1
2 Cryptographic Module Specification ... 2
2.1 Module Overview ... 2
2.2 Cryptographic Module Description ... 3
2.3 Approved Mode of Operation ... 4
2.4 Cryptographic Module Block Diagram ... 6
3 Cryptographic Module Ports and Interfaces ... 7
3.1 Physical Ports ... 7
3.2 Module Interfaces ... 8
4 Roles, Services and Authentication ... 9
4.1 Roles ... 9
4.2 Services ... 10
4.3 Operator Authentication ... 13
4.4 Authentication Strength ... 15
5 Physical Security ... 16
5.1 Static Protection ... 16
5.2 Dynamic Protection ... 18
6 Operational Environment ... 19
7 Cryptographic Key Management ... 20
7.1 Key Life Cycle Table ... 20
7.2 Split Knowledge Procedure ... 23
7.3 Random Number Generation ... 23
8 EMI/EMC ... 24
9 Self-Test ... 25
9.1 Power-Up Self-Tests ... 25

9.2 Conditional Tests....26
10 Design Assurance....27
10.1 Configuration Management....27
10.2 Crypto Officer Guidance....27
10.3 User Guidance....28
11 Mitigation of Other Attacks....29
12 Acronyms and Abbreviations....30
13 References....31

1 Introduction

This document is the non-proprietary FIPS 140-2 Security Policy for the HSM-ZJ2014 cryptographic module. It contains specific 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) for a Security Level 3 module.

For more information about the FIPS 140-2 standard and validation program, please refer to the NIST website at http://csrc.nist.gov/groups/STM/cmvp/index.html.

In this document, the terms "HSM", "cryptographic module" and "module" are used interchangeably to refer to the HSM-ZJ2014.

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 is part of the package of documents submitted for FIPS 140-2 conformance validation of the module. It is intended for the following people:

- Those specifying cryptographic modules
- Administrators of the cryptographic module(s)
- Users of the cryptographic module(s)

2 Cryptographic Module Specification

This section describes the cryptographic module and how it conforms to the FIPS 140-2 specification in each of the required areas.

2.1 Module Overview

The HSM-ZJ2014 is a multi-chip standalone hardware cryptographic module that can be connected to a data center or business system via its ethernet and fiber optic channels, providing its users data encryption, decryption, signature generation, signature verification and key management services. The Hardware Security Module (HSM) provides a hardened, tamper-resistant environment for secure cryptographic processing, key protection, and key management. The HSM is enclosed entirely within an opaque secure steel chassis which deters physical tampering and is guarded at all times with a tamper response circuitry in the event the enclosure is ever opened.

The modular design of the HSM makes it convenient to integrate HSM-ZJ2014 with existing information systems. A typical usage scenario of HSM-ZJ2014 is shown in Figure 1. The module connects data center, business system and other clients via Ethernet to provide cryptographic services. After authenticating, the clients can send service requests to the HSM, and HSM provides cryptographic services.

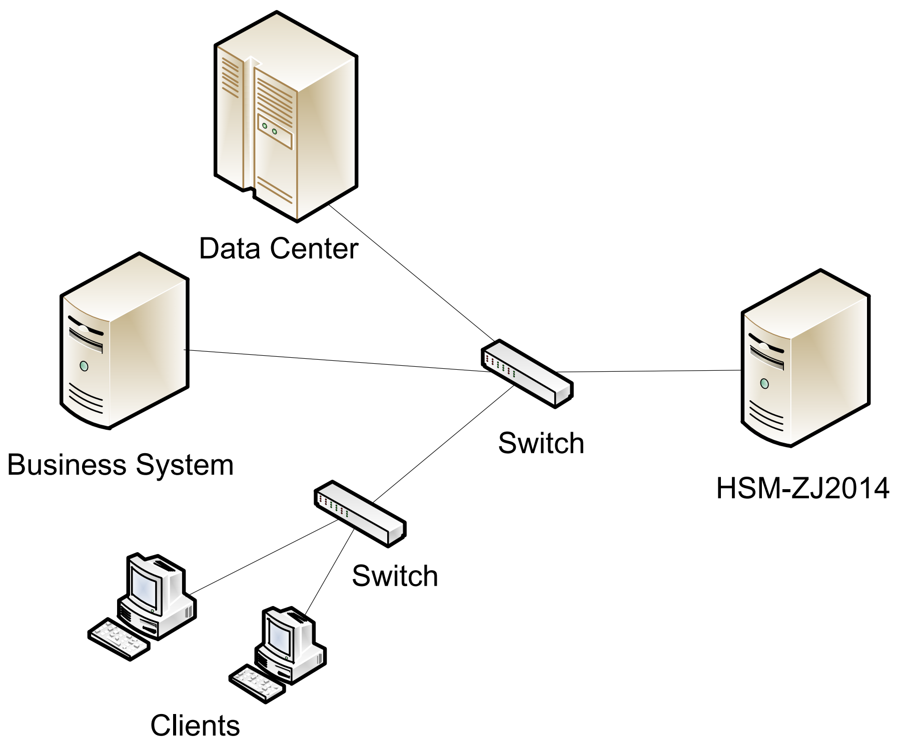


Figure 1: Typical Usage Scenario of HSM-ZJ2014

2.2 Cryptographic Module Description

The module is validated as a multi-chip standalone hardware module against FIPS 140-2 at an overall Security Level 3. The table below 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 and Services and Authentication	3
Finite State Machine 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 1: Security Levels

The cryptographic boundary of the module is defined as the entire HSM-ZJ2014. The physical boundary of the cryptographic module is defined by the hard metal chassis, which surrounds all the hardware and firmware components of HSM-ZJ2014 as shown in Figure 2. The dimension (Width× Height× Length) of the HSM hard metal chassis is 400mm×177mm×490mm.

Figure 2: HSM-ZJ2014

The module components within the logical boundary of HSM-ZJ2014 are specified in the table below:

Component Type	Part Number / Version
Hardware	ZJ2014-2697v2-680-32G
Firmware	1.0.0.1

Table 2: HSM-2014 Module Components

2.3 Approved Mode of Operation

The HSM is shipped by the manufacturer with the FIPS Approved mode as the only operational mode. After successful completion of the module's power on self-tests, the touchscreen displays the message "FIPS Approved Mode" to indicate the module is ready for use. Please refer to Table 6 for the details of the status indicator shown on the touch screen of the HSM.

HSM-ZJ2014 implements the following FIPS 140-2 Approved algorithms:

Algorithms	Keys / CSPs	Standard	Usage	CAVS Cert.
AES (ECB and CBC mode)	AES 128,192 and 256-bit keys	FIPS 197 NIST SP 800-38A	Encryption and Decryption	#3912
SHA-256	N/A	FIPS 180-4	Hashing	#3224
CTR_DRBG	Entropy input string, Nonce, V and Key	NIST SP 800-90A	Random Number Generation	#1128

ECDSA	ECDSA public and private key pair according to P-256 curve	FIPS 186-4	Key Pair Generation, Public Key Verification, Signature Generation and Signature Verification	#855
RSA	RSA private key with 2048-bit modulus size	FIPS 186-4	Key Pair Generation, PKCS#1 v1.5 Signature Generation and Signature Verification	#1996
HMAC	256-bit HMAC key	FIPS 198-1	Message Integrity	#2541

Table 3: Approved Algorithms

The module also implements the following FIPS 140-2 non-Approved algorithm but allowed to be used in FIPS Approved mode.

Algorithms	Keys / CSPs	Standard	Usage
AES key wrapping using AES CBC mode (not compliant with NIST SP 800-38F, but allowed in FIPS mode through December 31st 2017 according to IG D.9)	256-bit Master Key	FIPS 197	Used in “Export User File from current HSM to another HSM” and “Restore User Account” services in Table 9
RSA decryption (used as part of key transport scheme)	RSA private key with 2048-bit modulus size	NIST SP 800-56B	Used in “Modify User PIN” service in Table 9 to modify User PIN
NDRNG	seed	N/A	Used to seed the SP800-90A CTR_DRBG

Table 4: Non-Approved but Allowed Algorithm

Please refer to section 4.2 for the services that use the Approved or non-Approved but allowed algorithms.

2.4 Cryptographic Module Block Diagram

Figure 3 shows a hardware block diagram of the module. The red bold line surrounding the hardware components represents the physical boundary of the module.

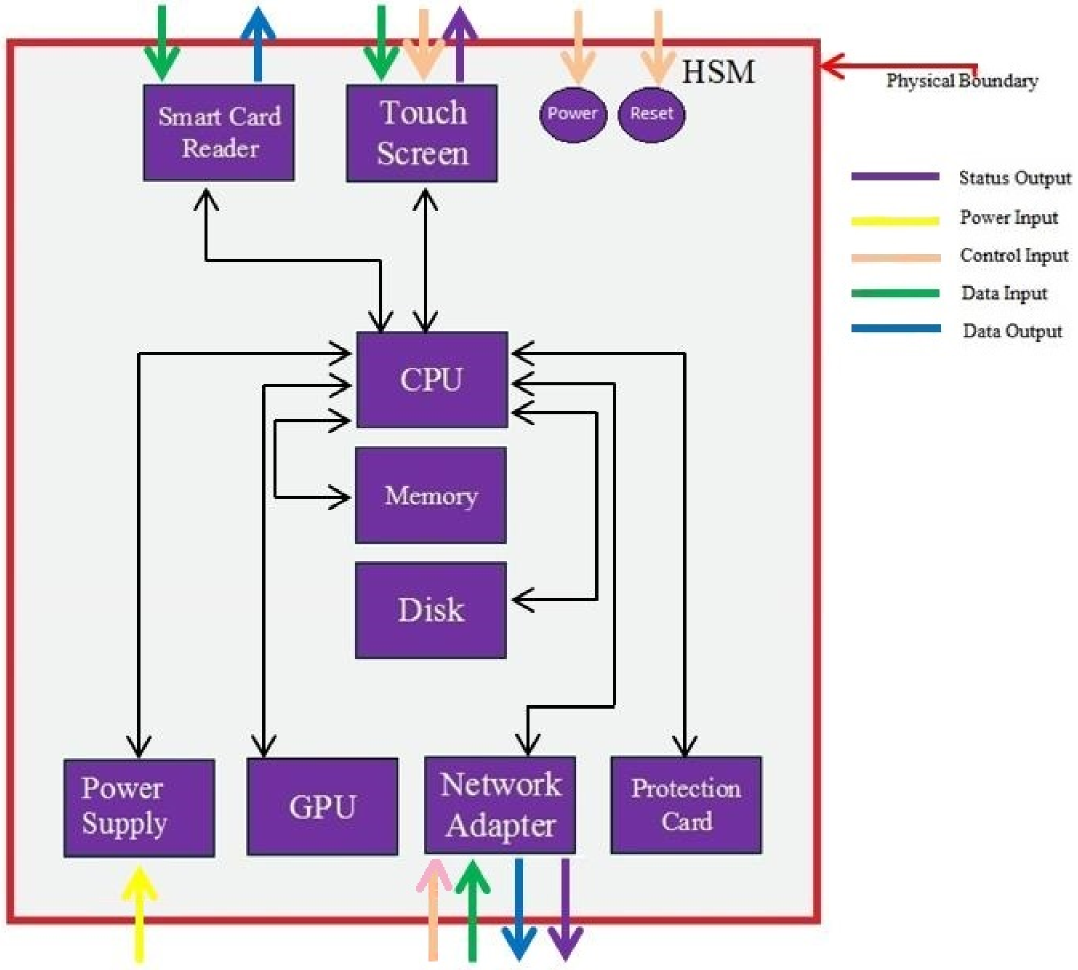


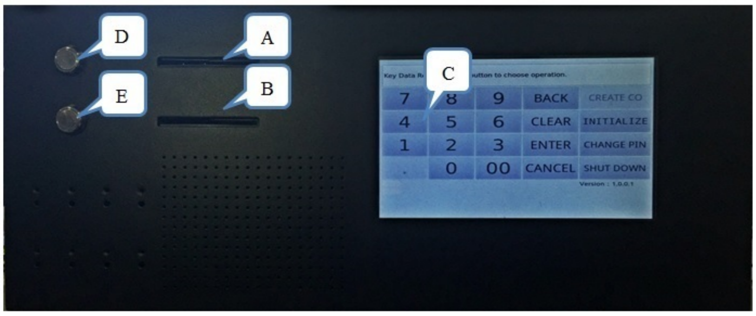
Figure 3: Hardware Block Diagram of HSM-ZJ2014

3 Cryptographic Module Ports and Interfaces

This section describes physical ports and logical interfaces of the module.

3.1 Physical Ports

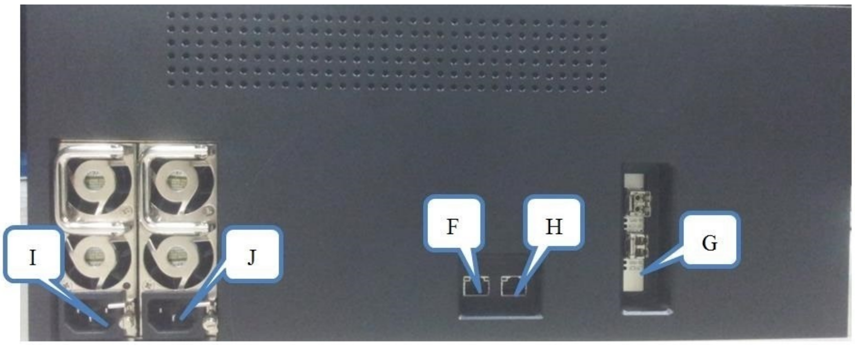
Figure 4 shows front panel of the HSM. The smart card reader for ID is used to authenticate the crypto officer by using the smart card and to update the smart card PIN of the crypto officers. The smart card reader for key is used to read the master key component from the smart card and write the master key component to the smart card. The touch screen provides a keypad to enter the smart card PIN and provides several buttons to enter the command. The touch screen can also show the firmware version, the FIPS approved mode and the self-test status. The power button is used to power on or off the module. The reset button is used to restart the HSM.



A – smart card reader for ID
B – smart card reader for key
C – touch screen
D – power button
E – reset button

Figure 4: Front View of HSM-ZJ2014

Figure 5 shows rear panel of the HSM. The two Ethernet ports and the fiber optic ports provide network interface to receive the requests of cryptographic services, provide the cryptographic services, and output the status. The module is powered through two redundant power supplies which provide a constant source of power to the module through either of the power ports.



F – Ethernet port
G – fiber optic port
H – Ethernet port
I – power port
J – power port

Figure 5: Rear View of HSM-ZJ2014

3.2 Module Interfaces

The following table provides the mapping between the FIPS interfaces, physical ports and the logical interfaces.

FIPS Interfaces	Physical Ports	Logical Interfaces
Data Input	Touch screen, smart card reader for ID, smart card reader for key, Ethernet and fiber optic ports	The input parameters of the service functions.
Data Output	Smart card reader for key, smart card reader for ID, Ethernet and fiber optic ports	The output parameters of the service functions
Control Input	Touch screen, Ethernet and fiber optic ports, power button and reset button	The input command
Status Output	Touch screen, Ethernet and fiber optic ports	The status output from the service functions
Power Input	Power ports	N/A

Table 5: Ports and Interfaces

The following table describes the status indicator shown on the touch screen for the corresponding FIPS states:

FIPS States	Messages displayed on touch screen
Power Off	(none)
Self-Tests	Status message of the result of each self-test
Error	Error message of the specific self-test
FIPS mode	Status message of “FIPS Approved Mode”

Table 6: Touch Screen Status Indicator

4 Roles, Services and Authentication

This section defines the roles, services and authentication mechanisms with respect to the applicable FIPS 140-2 requirements.

Identity-Based Authentication is required to authenticate the operator accessing the module and to verify that the operator is authorized to assume the requested role and perform the services within that role.

The module does not support concurrent operators.

4.1 Roles

The module supports four types of roles: Device Manager, Authorizer, Auditor, and User. For the purpose of FIPS 140-2 validation, the Device Manager role, Authorizer role, and Auditor role are considered as the Crypto Officer (CO) role. The following table shows the authorized roles and description:

Roles in FIPS 140-2 term	Roles defined in the module	Description
CO	Device Manager	Perform device management services including generating, importing, exporting the master key, system configuration, viewing non-sensitive information of user account and user key. The module only supports one operator for Device Manager role. The device manager account is created during module initialization.
	Authorizer	Perform user management services including creating, deleting, updating user account and user key, and managing the user file. The module only supports one operator for Authorizer role. The authorizer account is created during module initialization.
	Auditor	Perform audit management services including viewing and exporting the audit log, and inspecting the tamper seals. The module only supports one operator for Auditor role. The auditor account is created during module initialization.
User	User	Perform general security services including encryption, decryption, signature generation and signature verification. The module supports multiple operators for User role. The individual user account is created by the Authorizer role.

Table 7: Description of Roles

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

4.2 Services

The module only supports FIPS mode. The following two tables list all the services provided by the module. Table 8 contains all of the services that do not need authentication. There may be some keys or CSPs used by these non-Authenticated services, but these services do not create, modify, disclose, or substitute keys and CSPs. The non-Authenticated services are available to all roles. Table 9 contains all the services that require identity-based authentication.

Services	Description	Keys/CSPs	Access
Display FIPS Mode	View FIPS mode status	N/A	N/A
Display Module Version	Show module version	N/A	N/A
Self-Tests	Perform the self-tests automatically when the module is powered on or restarted	HMAC key for module integrity test. 256-bit Device Key is used as the HMAC key.	Read

Table 8: Non-Authenticated Services

Services	Authentic-ated Roles	Description	Keys/CSPs	Access
Import Master Key (When the module is restarted)	Device Manager	Import Master Key into the HSM from 3 out of the 5 key components stored on the smart cards. Decrypt the user file using AES decryption with Master Key to restore the user accounts in memory. Encrypt the user file after decryption	Master Key	Write Read
			Authentication data of Device Manager, PINs of the 3 smart cards that are used to store the Master Key components	Read
View User Account	Device Manager	View user ID and key ID	Authentication data of Device Manager	Read
View User Key	Device Manager	View non-sensitive information of user key including key ID, name, usage and size	Authentication data of Device Manager	Read
System Configuration	Device Manager	Perform network configuration	Authentication data of Device Manager	Read

Services	Authenticated Roles	Description	Keys/CSPs	Access
Update Smart Card PIN	Device Manager, Authorizer, Auditor	Modify the smart card PIN. The smart card could be the one for Device Manager, Authorizer, Auditor or the one to store the Master Key component	The new smart card PIN, the old smart card PIN (Note: the smart card PIN is used for the operator to authenticate to the smart card and the PIN is stored on the smart card only)	Write
Create User Account	Authorizer[1]	Create a user account with default User PIN. Generate user's default RSA or ECDSA key pair. Update the user file with the encrypted user account information by using AES encryption with Master Key	Default User PIN, user's default RSA or ECDSA key pair	Write
			Authentication data of Authorizer, Master Key	Read
Create User Key	Authorizer[1]	Generate AES key, RSA key pair or ECDSA key pair for a user. Update the user file with the encrypted user account information by using AES encryption with Master Key	User's AES key, RSA key pair or ECDSA key pair	Write
			Authentication data of Authorizer, Master Key	Read
Update User Key	Authorizer[1]	Regenerate AES key, RSA key pair or ECDSA key pair for a user. Update the user file with the encrypted user account information by using AES encryption with Master Key	User's AES key, RSA key pair or ECDSA key pair	Write
			Authentication data of Authorizer, Master Key	Read
Backup User File	Authorizer[1]	Copy the user file to a backup file	Authentication data of Authorizer	Read

[1] Note: The Device Manager must first be authenticated before the Authorizer can perform these services.

Services	Authenticated Roles	Description	Keys/CSPs	Access
Export User File from current HSM to another HSM (denoted as HSM_other)	Authorizer[1]	Import Master Key of HSM_other from 3 out of 5 key components stored on the smart cards. Wrap the user account information to a backup file using AES key wrapping with AES CBC mode and Master Key of HSM_other	Master Key of HSM_other User's AES key, RSA key pair or ECDSA key pair Authentication data of Authorizer, PINs of 3 smart cards that are used to store the Master Key components of HSM_other	Read
Restore User Account	Authorizer[1]	Unwrap the backup file encrypted by Master Key. Restore the user's account information in memory and then encrypt the user file	User's AES key, RSA key pair or ECDSA key pair	Write
			Authentication data of Authorizer, Master Key	Read
Delete User Key	Authorizer[1]	Delete user's AES key, RSA key pair or ECDSA key pair. Update the user file with the encrypted user account information by using AES encryption with Master Key	User's AES key, RSA key pair or ECDSA key pair	Zeroize
			Authentication data of Authorizer, Master Key	Read
Delete User Account	Authorizer[1]	Delete a user account. Update the user file with the encrypted user account information by using AES encryption with Master Key	User PIN, user's AES key, RSA key pair or ECDSA key pair	Zeroize
			Authentication data of Authorizer	Read
Delete All User Accounts	Authorizer[1]	Delete all of the user accounts. Delete all information in the user file	Each user's User PIN, each user's AES key, RSA key pair or ECDSA key pair	Zeroize
			Authentication data of Authorizer	Read
View Audit Log	Auditor	Show event log	Authentication data of Auditor	Read

Services	Authenticated Roles	Description	Keys/CSPs	Access
Export Audit Log	Auditor	Output event log file	Authentication data of Auditor	Read
Modify User PIN	User	Modify User PIN by using RSA decryption to decrypt the old PIN and new PIN which are sent and encrypted by the user using RSA encryption	The new User PIN, the old User PIN, RSA private key for RSA decryption	Read
AES Encryption	User	Perform AES encryption operation	User's AES key, User PIN	Read
AES Decryption	User	Perform AES decryption operation	User's AES key, User PIN	Read
RSA Signature Generation	User	Compute a digital signature using RSA	User's RSA private key, User PIN	Read
RSA Signature Verification	User	Verify a digital signature using RSA	User's RSA public key, User PIN	Read
ECDSA Signature Generation	User	Compute a digital signature using ECDSA	User's ECDSA private key, User PIN	Read
ECDSA Signature Verification	User	Verify a digital signature using ECDSA	User's ECDSA public key, User PIN	Read

Table 9: Authenticated Services

4.3 Operator Authentication

The HSM-ZJ2014 uses Identity-Based Authentication to authenticate different roles.

The Device Manager role, Authorizer role and Auditor role are identified by the Device Manager ID, Authorizer ID and Auditor ID, respectively. The module performs two-factor authentication. First the CO must provide a valid PIN to authenticate to the smart card which is assigned to him. Next the smart card must provide a valid signature to the HSM based on the ID stored in the smart card. The authentication of these roles is based on RSA signature verification via the smart card.

During module initialization, each of the Cryptographic Officers (CO) is assigned a smart card. The ID and RSA public key are read from the smart cards to create the Device Manager account, Authorizer account and Auditor account, respectively. All of these CO accounts are stored on the HSM in encrypted form using AES encryption with Device Key. The Device Key is generated in factory and stored in the protection card of the HSM.

The User role is identified by the User ID created by the Authorizer and stored on the HSM. The module uses the “challenge-response” method for User authentication.

The following table explains the authentication methods for different roles.

Roles	Authentication Methods
Crypto Officer (CO)	1. Authenticate CO to the smart card by inserting the smart card to the smart card reader for ID and providing an 8-digit smart card PIN. 2. The HSM decrypts all of the CO accounts stored in the hard disk, uses the type index to locate the CO account that the smart card shall be associated with, and then obtains the ID and RSA public key of the respective CO. 3. The HSM reads ID’ from smart card and compares whether ID=ID’. 4. The HSM sends a random message M to smart card and receives a RSA signature S generated by smart card. 5. The HSM uses the RSA public key to verify S. If S is valid, the authentication succeeds. Otherwise it fails.
User	1. The user generates a random value R1 and sends R1 and User ID to the HSM. 2. The HSM generates a random value R2 and sends it to the user. 3. The user generates a SHA-256 hash value H1 of the concatenation of R1, R2 and the User PIN provided by the user. The user sends H1 to the HSM. 4. The HSM generates the SHA-256 hash value H2 of the concatenation of R1, R2 and the User PIN stored on the HSM. The HSM checks if H1= H2. If yes, the User role is authenticated successfully.

Table 10: Authentication Methods

The module ensures that there is no visible display of the authentication data, such as smart card PIN or User PIN. The smart card PIN is only stored on the smart card and is used to authenticate the operator to the smart card in order to read its ID. The ID and RSA public key of Device Manager, Authorizer or Auditor are stored in the disk and encrypted by Device Key. The User PIN is stored in the disk and encrypted by Master Key. The current operator status is stored temporarily in memory and will be cleared when the operator logs out. When the HSM is powered off, the authentication data will be automatically zeroized due to the volatile feature of memory.

4.4 Authentication Strength

For Device Manager, Authorizer or Auditor role, the module only allows 6 unsuccessful attempts for authentication. If the authentication fails for 6 attempts, the specific CO role will be blocked and the module will need to be returned to the factory to unblock it.

For User role, the module will block the User role after 15 attempts of unsuccessful authentication. It will be unblocked automatically after 3 minutes.

The strength of the authentication mechanisms is listed in Table 11.

Authentication Mechanism	Strength
Authentication of Device Manager, Authorizer or Auditor role: Smart card PIN to authenticate the operator to the smart card. The RSA public key for signature verification.	Smart Card PIN includes 8 digits. This yields 10^8 possible combinations. For each attempt to use this authentication mechanism, the probability that a random attempt will succeed is $1/10^8$, which is less than $1/10^6$. For multiple attempts to use this authentication mechanism, the probability that a random attempt will succeed in one minute is $6/10^8$, which is less than $1/10^5$. The RSA public key is 2048-bit, which provides 112 bit of security strength. For each attempt to use this authentication mechanism, the probability that a random attempt will succeed is $1/2^{112}$, which is less than $1/10^6$. For multiple attempts to use this authentication mechanism, the probability that a random attempt will succeed in one minute is $6/2^{112}$, which is less than $1/10^5$.
User Authentication: User PIN	User PIN includes 8 digits. This yields a minimum of 10^8 possible combinations. For each attempt to use this authentication mechanism, the probability that a random attempt will succeed is $1/10^8$, which is less than $1/10^6$. For multiple attempts to use this authentication mechanism, the probability that a random attempt will succeed in one minute by is $15/10^8$, which is less than $1/10^5$.

Table 11: Authentication Mechanism and Strength

5 Physical Security

This section describes the physical security mechanisms that the module employs in order to restrict unauthorized physical access to the contents of the module and to deter unauthorized use or modification of the module.

5.1 Static Protection

All the components of HSM-ZJ2014 are enclosed by the 2-millimeter steel chassis, opaque to the visible spectrum. The input and output ports of the HSM are listed in Section 3. The interspace between each port and the chassis and the ventilation holes are fitted with baffles to obscure visual access and to prevent undetected physical probing inside the chassis.

The HSM is designed to resist physical attack. The red rectangle in Figure 6 shows the primary area to be protected. This area is isolated from other area by wire mesh filter over the power supply housing and air circulating fans and a baffle covering the ventilation openings.

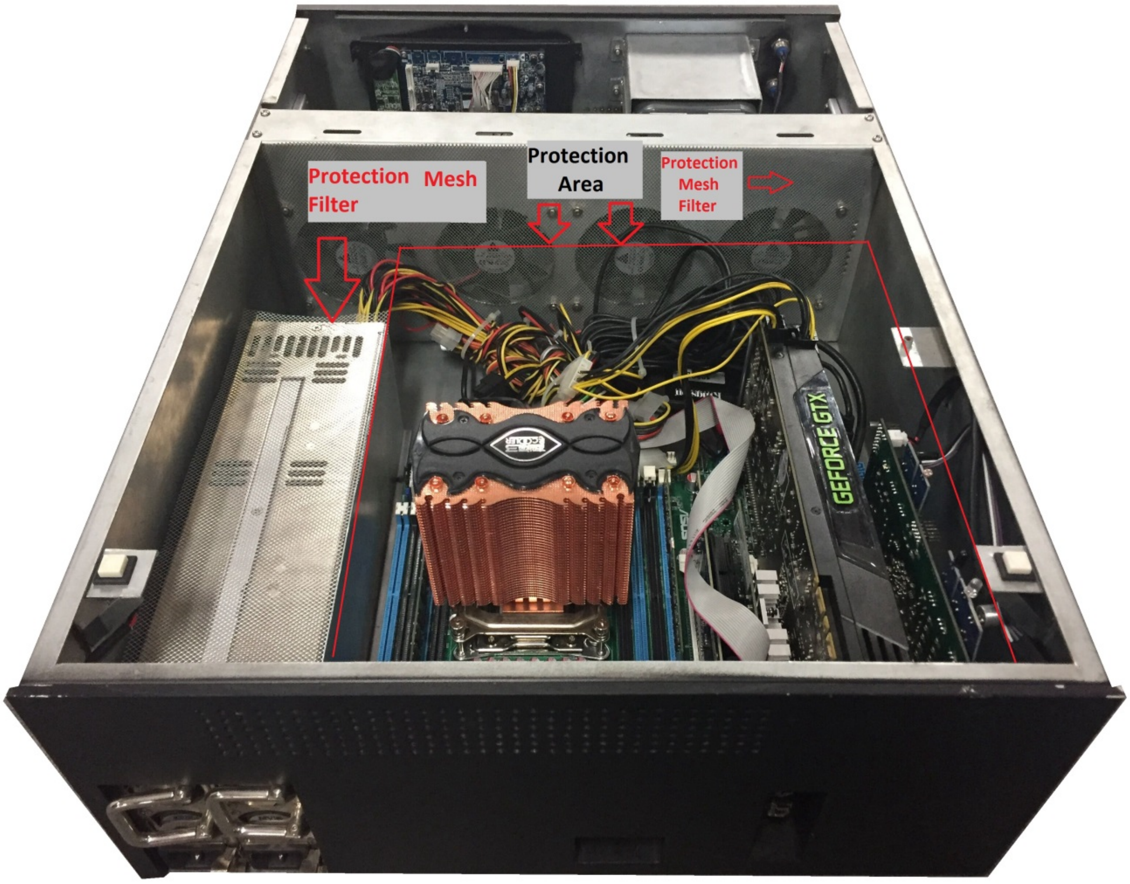


Figure 6: Resist Physical Attack from the front and left

The back is isolated by filter2, as shown in Figure 7 and Figure 8.

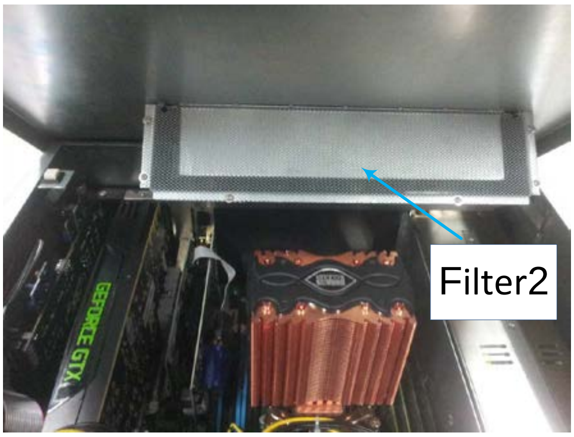


Figure 7: Resist Physical Attack from the back

Figure 8: Backend Vents

Furthermore, there are tamper evident seals placed around the chassis cover before the HSM leaves the factory, as shown in Figure 9. Any attempts to remove the cover will leave tamper evidence. The Crypto Officer (Auditor) is responsible for inspecting the tamper-evident labels on the HSM at monthly intervals to verify that the labels have not been altered in any way.

Figure 9: Tamper Evident Seals

5.2 Dynamic Protection

HSM-ZJ2014 employs a protection card to protect the integrity of the module from physical attacks. The protection card is equipped with a battery and volatile RAM to store the Device Key, no matter whether the HSM is connected to the power or not. Once the Device Key is broken, the HSM will no longer function. There are two chassis-open tamper switches connected to the protection card as shown in Figure 10. If the chassis cover is open when the HSM is powered on or powered off, the tamper switch will trigger the protection card to instantaneously zeroize the Device Key and all User's sensitive information. In addition, the module will delete the operating system's kernel and all the cryptographic services shall become unavailable. Ultimately, the HSM will be in an unrecoverable state which requires it to be returned the manufacturer for reconfiguration. The tamper switch is activated mandatorily before the HSM leaves the factory, and cannot be deactivated.

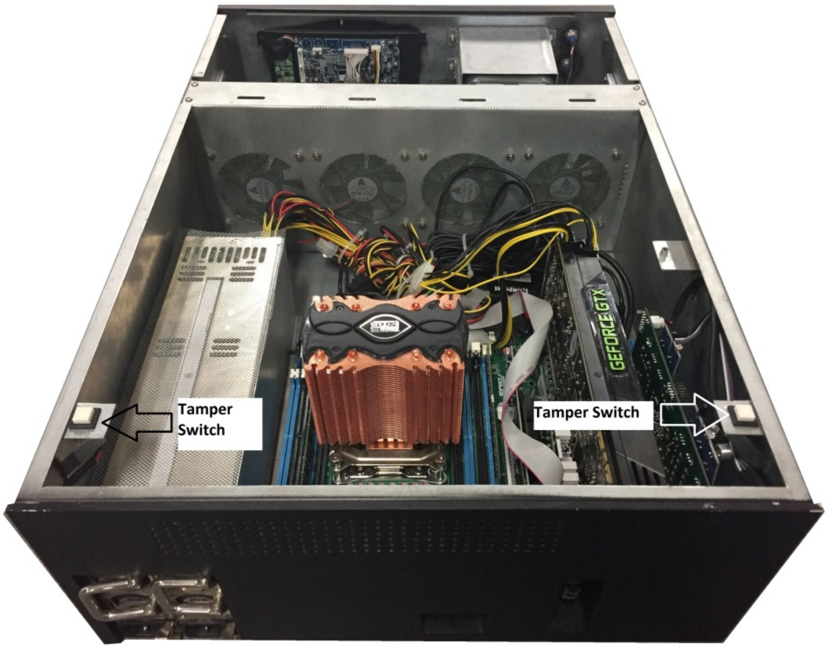


Figure 10: tamper switch

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 HSM-ZJ2014, it cannot be modified or erased. The operational environment requirements do not apply to the module.

7 Cryptographic Key Management

7.1 Key Life Cycle Table

The following table provides a summary of the keys and CSPs that are employed by the module:

Key/CSP	Generation	Entry and Output	Storage	Zeroization
Master Key (256-bit random number)	Generated by CTR_DRBG during module initialization	Split into 5 key components and written to 5 smart cards during module initialization. In the next power cycle, 3 of the 5 key components are imported from 3 of the 5 smart cards to recover the Master Key	Stored temporarily in volatile memory	Zeroized when the module is powered off or the tamper switch is triggered
Device Key (256-bit random number)	Generated in factory	N/A	Stored in protection card	Zeroized when the tamper switch is triggered
Smart Card PIN of Device Manager (8-digit PIN)	N/A	Input manually by Device Manager; Output through API parameter to the smart card of Device Manager	Stored in smart card of Device Manager	N/A
Smart Card PIN of Authorizer (8-digit PIN)	N/A	Input manually by Authorizer; Output through API parameter to the smart card of Authorizer	Stored in smart card of Authorizer	N/A
Smart Card PIN of Auditor	N/A	Input manually by Auditor; Output through API parameter to	Stored in smart card of Auditor	N/A

(8-digit PIN)		the smart card of Auditor		
RSA public key to authenticate Device Manager (2048-bit)	N/A	During module initialization, RSA public key is read from the smart card of Device Manager by API call	Encrypted by Device Key and Stored in hard disk	Zeroized when the tamper switch is triggered
RSA public key to authenticate Authorizer (2048-bit)	N/A	During module initialization, RSA public key is read from the smart card of Authorizer by API call	Encrypted by Device Key and Stored in hard disk	Zeroized when the tamper switch is triggered
RSA public key to authenticate Auditor (2048-bit)	N/A	During module initialization, RSA public key is read from the smart card of Auditor by API call	Encrypted by Device Key and Stored in hard disk	Zeroized when the tamper switch is triggered
User PIN (8-digit PIN)	Default User PIN is created during Create User Account service (must be updated at first use by user)	Entered and output in user file which is encrypted with Master Key or entered encrypted with RSA Public key during Modify User PIN service	Stored temporarily in volatile memory and stored in user file which is encrypted by Master Key	The value stored in memory is zeroized when the user account is deleted, the module is powered off or the tamper switch is triggered. The user file is zeroized when the tamper switch is triggered.
RSA public key to modify User PIN (2048-bit)	Generated by CTR_DRBG	Entered and output in user file which is encrypted with Master Key. Sent to the user during Modify User PIN service	Stored temporarily in volatile memory and stored in user file which is encrypted by Master Key	The value stored in memory is zeroized when the user account with ID 0 is deleted, the module is powered off or the tamper switch is triggered. The user file is zeroized when the tamper switch is triggered.
RSA private key to modify User	Generated by CTR_DRBG	Entered and output in user file which is	Stored temporarily in volatile	The value stored in memory is zeroized when the user account

PIN (2048-bit)		encrypted with Master Key	memory and stored in user file which is encrypted by Master Key	with ID 0 is deleted, the module is powered off or the tamper switch is triggered. The user file is zeroized when the tamper switch is triggered.
User's AES key (128/192/256 –bit)	Generated by CTR_DRBG	Entered and output in user file which is encrypted with Master Key	Stored temporarily in volatile memory and stored in user file which is encrypted by Master Key	The value stored in memory is zeroized when the user account is deleted, the module is powered off or the tamper switch is triggered. The user file is zeroized when the tamper switch is triggered.
User's ECDSA key pair according to P-256	Generated by CTR_DRBG	Entered and output in user file which is encrypted with Master Key	Stored temporarily in volatile memory and stored in user file which is encrypted by Master Key	The value stored in memory is zeroized when the user account is deleted, the module is powered off or the tamper switch is triggered. The user file is zeroized when the tamper switch is triggered.
User's RSA key pair (2048-bit)	Generated by CTR_DRBG	Entered and output in user file which is encrypted with Master Key	Stored temporarily in volatile memory and stored in user file which is encrypted by Master Key	The value stored in memory is zeroized when the user account is deleted, the module is powered off or the tamper switch is triggered. The user file is zeroized when the tamper switch is triggered.
CTR_DRBG entropy input string	Obtained from NDRNG	N/A	Stored temporarily in volatile memory	Zeroized when the module is powered off or the tamper switch is triggered
CTR_DRBG nonce, V and K	Derived from entropy string as defined in	N/A	Stored temporarily in volatile	Zeroized when the module is powered off or the tamper switch is

	NIST SP 800-90A		memory	triggered

Table 12: Key Life Cycle

7.2 Split Knowledge Procedure

The HSM-ZJ2014 uses the split knowledge procedure for Master Key entry and output. This scheme is based on Shamir's Threshold Secret. The HSM splits the Master Key into 5 components, and stored them individually in 5 smart cards. Any 3 of these 5 components must be transmitted to the HSM in order to reconstruct the Master Key. To read each of the key components, the operator has to insert the corresponding smart card into the smart card reader for key and authenticate to the smart card by providing the correct PIN.

For more information about Shamir's Threshold Secret Scheme, please see *How to Share a Secret* which can be acquired from http://dl.acm.org/citation.cfm?id=359176.

7.3 Random Number Generation

A FIPS-Approved Deterministic Random Bit Generator (DRBG) based on a block cipher as specified in NIST SP 800-90A is used. It is a CTR_DRBG using AES-256 with derivation function and without prediction resistance. The CTR_DRBG produces a 128-bit random number block for one request and will be reseeded when it has produced 2^{24} random number blocks.

The module uses a Non-Deterministic Random Number Generator (NDRNG) as the entropy source to seed the Approved CTR_DRBG. The NDRNG is provided by Intel's Ivy Bridge RNG implemented as an instruction in the CPU called RDRand. The NDRNG provides sufficient entropy to support 256-bit of security strength.

8 EMI/EMC

The HSM-ZJ2014 conforms to the EMI/EMC requirements as specified by 47 Code of Federal Regulations, Part 15, Subpart B, Unintentional Radiators, Digital Devices, Class B (i.e., for home use).

9 Self-Test

The HSM-ZJ2014 implements a series of self-tests to ensure that proper cryptographic algorithm calculations are implemented in the module. Self-tests include power-up self-tests and conditional tests.

If any self-test fails, the module enters into the Error state. When the module is in the Error state, the touch screen will show error message to indicate the failure of self-tests. When the module is performing self-tests or in the Error state, all data output is prohibited and no cryptographic operation is allowed.

To recover from the Error state, the module needs to be restarted and the power-up self-tests will be reinitiated.

9.1 Power-Up Self-Tests

When the HSM-ZJ2014 is powered on, the power-up self-tests are executed automatically without any operator intervention. If the module completes the power-up self-tests successfully, the module will enter FIPS approved mode and a message "FIPS Approved Mode" will be observed on the touch screen. On demand self-tests can be initiated by rebooting the HSM.

The module implements the following Known Answer Tests (KATs), Pair-wise Consistency Tests (PCTs) and the Integrity Test during the power-up of the module:

Algorithm	Test
AES	KAT: encryption and decryption are tested separately
SHA-256	KAT
CTR_DRBG	KAT
ECDSA signature generation and verification	PCT
RSA signature generation and verification	KAT: signature generation and verification are tested separately
HMAC-SHA-256	KAT, integrity test of the module
RSA decryption	KAT

Table 13: Power-Up Self-Tests

HSM-ZJ2014 uses HMAC-SHA-256 for the integrity test of its firmware. HMAC is an Approved algorithm that is provided by the module. The known HMAC value of the firmware is calculated in the factory as part of the binary of the firmware. When the module is powered-up, it will generate the HMAC value of the firmware of the module. The module then compares the generated HMAC value and the known HMAC value stored in the firmware binary. If the values do not match, the integrity test fails and the module enters the Error state.

9.2 Conditional Tests

HSM-ZJ2014 performs conditional tests when the module generates random numbers or public/private key pairs.

The module implements the following Pair-wise Consistency Tests (PCTs) for public-private key pair generation and the Continuous Random Number Generator Test (CRNGT):

Algorithm	Test
ECDSA Key Generation	PCT
RSA Key Generation	PCT
CTR_DRBG	CRNGT
NDRNG	CRNGT

Table 14: Conditional Tests

For CTR_DRBG, the module also performs the health tests as specified in section 11.3 of NIST SP 800-90A.

10 Design Assurance

10.1 Configuration Management

The module is maintained by using the revision control system called “Git”.

The source code and documentations of HSM-ZJ2014 including design document, develop environment, guidance, process, specifications of hardware components are managed and recorded. Additionally, configuration management is provided for the module’s FIPS documentation.

Document management utilities provide access control, versioning and logging. Access to the Git repository (source tree) is granted or denied by the server administrator in accordance with company and team policy.

10.2 Crypto Officer Guidance

The module is non-modifiable and it does not provide any access ports, such as USBs, which can be used to modify the system. The auto-update function of the OS has been shut down and it does not provide any function to modify the system. The product which is delivered to the consumer includes the HSM and its accessories. The accessories are smart cards, power cables, network cables and guidance documents.

Before the module is ready for use, the following steps need to be performed during module initialization:

1) Create the Crypto Officers (COs). The operator powers on the HSM and selects “Create CO” from the touchscreen. The operator then inserts the Device Manager smart card into smart card reader for ID and enters the smart cards default PIN which is provided in the guidance documents. The HSM reads the ID and RSA public key (used for CO authentication) from the smart card and then creates the account of Device Manager. Similarly, the operator creates the accounts of Authorizer and Auditor. The CO account information includes the smart card ID, RSA public key and the type of the CO. All the CO accounts are encrypted with AES encryption using Device Key and stored in cipher text in the hard disk.

2) Generate Master Key, export Master Key components and generate RSA key pair for User PIN modification. The operator selects “INITIALIZE” from the touch screen. The HSM will require the operator to authenticate as Device Manager. The HSM generates Master Key and split it into 5 components. It requires the Device Manager to insert 5 smart cards separately into smart card reader for key and enter the default smart card PIN. Then the HSM will write the Master Key components into each of the smart cards. In addition, the HSM will generate a RSA key pair (used in “Modify User PIN” service). A special user account with user ID 0 and this RSA key pair is created. A user file is created with the

encrypted information of this user account by using AES encryption with Master Key.

Once the module initialization is done, the HSM is ready for use and the smarts cards shall be distributed to the appropriate personnel.

It is highly recommended that the default smart card PIN shall be modified immediately after the module initialization. The smart card used for authentication of Device Manager, Authorizer or Auditor cannot be used to store the Master Key component, vice versa.

When the module is restarted and the Master Key has already been generated, the Device Manager is required to be authenticated to the HSM to import Master Key from 3 of the 5 Master Key components. The Device Manager needs to provide the PIN to get authenticated to each of the 3 smart cards.

The CO operators have the responsibilities to protect the smart cards and the PINs from theft. The PINs should be complex and only used in one place.

10.3 User Guidance

The user can access the cryptographic services only when the User PIN is verified. When Authorizer creates the user account, a default User PIN is generated. However, the default User PIN cannot be used for user authentication. During initial login, the user must modify the User PIN in order to get authenticated to the HSM successfully.

The user has the responsibilities to protect the User PIN from theft.

11 Mitigation of Other Attacks

No other attacks are mitigated.

12 Acronyms and Abbreviations

AES	Advanced Encryption Standard
API	Application Programming Interface
CBC	Cipher Block Chaining
CMVP	Cryptographic Module Validation Program
CRNGT	Continuous Random Number Generator Test
CSP	Critical Security Parameter
CTR	Counter
DRBG	Deterministic Random Bit Generator
ECB	Electronic Codebook
ECDSA	Elliptic Curve Digital Signature Algorithm
EMI	Electromagnetic Interference
EMC	Electromagnetic Compatibility
FIPS	Federal Information Processing Standard
HMAC	Hash Message Authentication Code
HSM	Hardware Security Module
KAT	Known Answer Test
MAC	Message Authentication Code
NDRNG	Non-Deterministic Random Number Generator
NIST	National Institute of Standards and Technology
OS	Operating System
PC	Personal Computer
PIN	Personal Identification Number
PCT	Pairwise Consistency Test
PKCS	Public-Key Cryptography Standards
RAM	Random Access Memory
RNG	Random Number Generator
RSA	Rivest-Shamir-Adleman
SP	NIST Special Publication
SHA	Secure Hash Algorithm

13 References

[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 180-4, Secure Hash Standard (SHS),
http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.180-4.pdf

[5] FIPS 186-4, Digital Signature Standard,
http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf

[6] FIPS 197, Advanced Encryption Standard (AES),
http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf

[7] FIPS 198-1, The Keyed-Hash Message Authentication Code (HMAC),
http://csrc.nist.gov/publications/fips/fips198-1/FIPS-198-1_final.pdf

[8] NIST SP 800-38A, Recommendation for Block Cipher Modes of Operation,
http://csrc.nist.gov/publications/nistpubs/800-38a/sp800-38a.pdf

[9] NIST SP 800-56B, Revision 1, Recommendation for Pair-Wise Key-Establishment Schemes Using Integer Factorization Cryptography,
http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-56Br1.pdf

[10] 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

