Juniper Networks, Inc.

Juniper CryptoCore Cryptographic Module

FIPS 140-2 Cryptographic Module
Non-Proprietary Security Policy

Document Version: 1.3

Date: April 29, 2019

Table of Contents

List of Tables

List of Figures

1 Introduction

This document defines the Security Policy for the Juniper Networks, Inc. Juniper CryptoCore Cryptographic Module, hereafter denoted the Module. The Module is a library of cryptographic algorithms that are employed in numerous Juniper Networks products. The Module meets FIPS 140-2 overall Level 1 requirements.

Table 1 – Cryptographic Module Configurations

	Module	SW Version	Processor	Operating Environment	Platform
1	CryptoCore	1.0	Intel Xeon E5	Ubuntu Linux 14.04	Juniper JATP700
2	CryptoCore	1.0	Intel Core i5	Ubuntu Linux 14.04	Apple Mac mini
3	CryptoCore	1.0	Intel Xeon E5	Ubuntu Linux 14.04 on VMWare ESXi 6.0	Dell PowerEdge R320

The Module is intended for use by US Federal agencies and other markets that require FIPS 140-2 validated cryptography. The Module is a software only module that executes on a general purpose computer. The module may be ported per IG G.5 to operating environments not listed in Table 1 and retain compliance to FIPS 140-2; however, the CMVP makes no statement as to the correct operation of the module or the security strengths of the generated keys when so ported if the specific environment is not listed on the validation certificate. The module is also supported on the following, untested platforms:

- Juniper JATP400
- Dell R330
- Dell R430
- Dell R730

For the purposes of the validation, the embodiment is considered multi-chip standalone; the cryptographic boundary is the object module with filename, fipscanister.o.

The FIPS 140-2 security levels for the Module are as follows:

Table 2 – Security Level of Security Requirements

Security Requirement	Security Level
Cryptographic Module Specification	1
Cryptographic Module Ports and Interfaces	1
Roles, Services, and Authentication	1
Finite State Model	1
Physical Security	N/A
Operational Environment	1

Security Requirement	Security Level
Cryptographic Key Management	1
EMI/EMC	1
Self-Tests	1
Design Assurance	1
Mitigation of Other Attacks	N/A

1.1 Cryptographic Boundary & Interfaces

The physical form of the Module is the general purpose computer on which the Module operates. The logical boundary is defined as the Module's API, which provides all logical interfaces as described in Table 3.

Figure 1 – Module Block Diagram

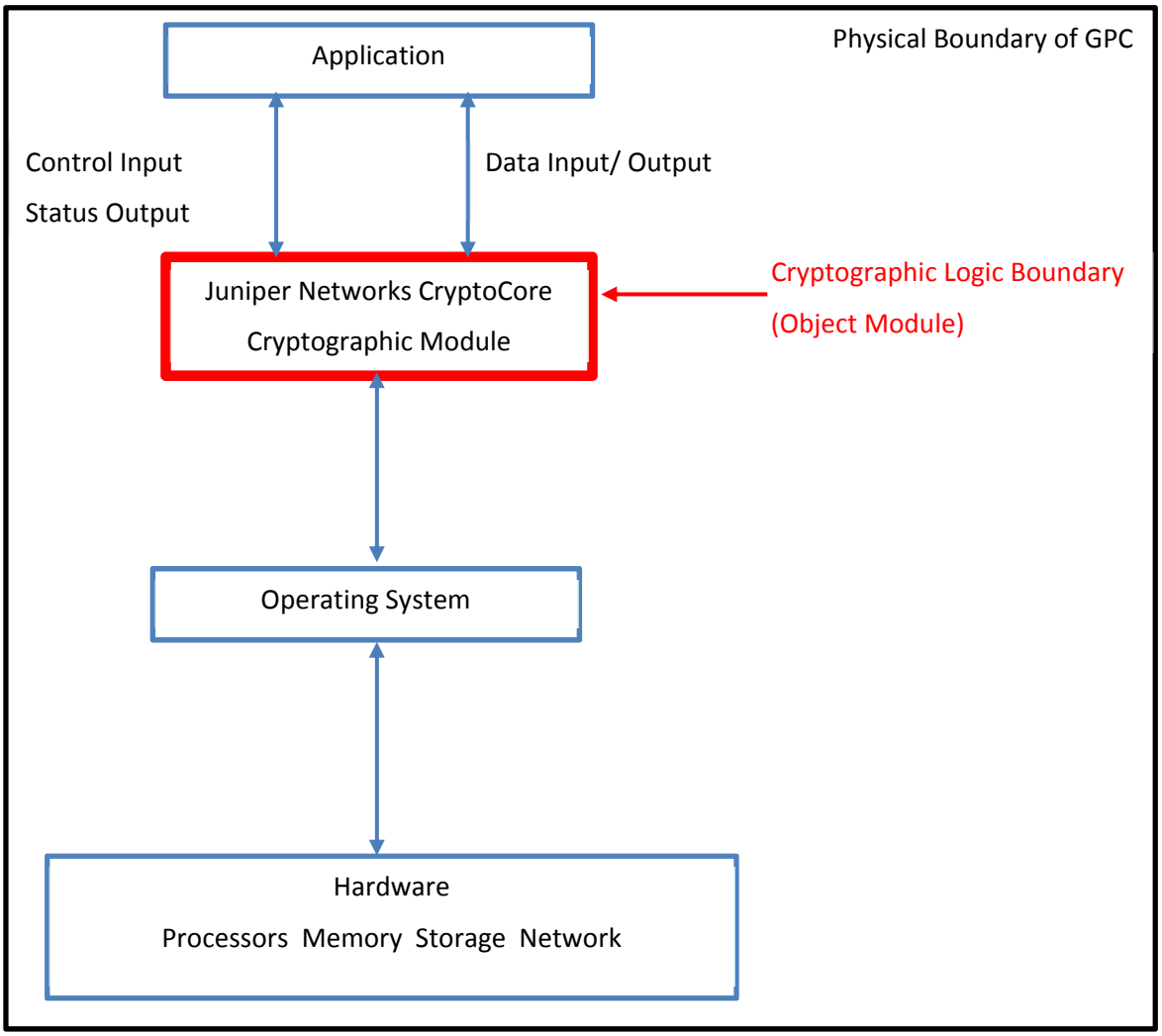

Table 3 – Interfaces

Logical Interface Type	Description
Control in	API function calls
Data in	API input parameters
Data out	API output parameters and return values
Status out	API output parameters and return values

1.2 Mode of Operation

The Module supports both an Approved mode of operation and non-Approved mode. To configure the module in the Approved mode of operation, the operator must invoke the "Set FIPS" service and only employ Approved algorithms listed in Table 4 and Table 5.

2 Cryptographic Functionality

The Module implements the FIPS Approved and Non-Approved but Allowed cryptographic functions listed in the tables below.

Table 4 – Approved Cryptographic Functions

Cert	Algorithm	Mode	Description	Functions/Caveats
5540	AES [197]	CBC [38A]	Key Sizes: 128, 192, 256	Encrypt, Decrypt
		CTR [38A]	Key Sizes: 128, 192, 256	Encrypt, Decrypt
		ECB [38A]	Key Sizes: 128, 192, 256	Encrypt, Decrypt
		GCM [38D][1]	Key Sizes: 128, 192, 256 Tag Len: 32, 64, 96, 104, 112, 120, 128	Authenticated Encrypt, Authenticated Decrypt, Message Authentication
Vendor Affirmed	CKG [IG D.12]	[133] Section 6.1 Asymmetric signature key generation using unmodified DRBG output		Key Generation
		[133] Section 6.2 Asymmetric key establishment key generation using unmodified DRBG output		
		[133] Section 7.1 Direct symmetric key generation using unmodified DRBG output		
1980	CVL: ECC CDH [56A]		All NIST defined B, K, and P curves: P-224, P-256, P-384, P-521, K-233, K-283, K-409, K-571, B-233, B-283, B-409, B-571	Shared Secret Establishment
2195	DRBG [90A]	CTR	Use_df, Prediction Resistance Enabled, No Reseed, AES-256	Deterministic Random Bit Generation
1422	DSA [186]		(L = 2048, N = 224) (L = 2048, N = 256) (L = 3072, N= 256)	KeyGen

[1] The IV is generated internally within the GCM algorithm boundary per SP800-38D, Section 8.2.1. If power is lost, operator can set the IV to the last value used.

Cert	Algorithm	Mode	Description	Functions/Caveats
			(L = 2048, N = 224) SHA(224, 256, 384, 512) (L = 2048, N = 256) SHA(256, 384, 512) (L = 3072, N = 256) SHA(256, 384, 512)	PQG Gen
			(L = 1024, N = 160) SHA(1, 224, 256, 384, 512) (L = 2048, N = 224) SHA(224, 256, 384, 512) (L = 2048, N = 256) SHA(256, 384, 512) (L = 3072, N= 256) SHA(256, 384, 512)	PQG Ver
			(L = 2048, N = 224) SHA(224, 256, 384, 512) (L = 2048, N = 256) SHA(224, 256, 384, 512) (L = 3072, N= 256) SHA(224, 256, 384, 512)	SigGen
			(L = 1024, N = 160) SHA(1, 224, 256, 384, 512,) (L = 2048, N = 224) SHA(1, 224, 256, 384, 512) (L = 2048, N = 256) SHA(1, 224, 256, 384, 512) (L = 3072, N= 256) SHA(1, 224, 256, 384, 512)	SigVer
1491	ECDSA [186]		P-224, K-233, B-233, P-256, K-283, B-283, P-384, K-409, B-409, P-521, K-571, B-571	KeyGen
			P-192, K-163, B-163, P-224, K-233, B-233, P-256, K-283, B-283, P-384, K-409, B-409, P-521, K-571, B-571	PKV
			P-224 SHA(224, 256, 384, 512) P-256 SHA(224, 256, 384, 512) P-384 SHA(224, 256, 384, 512) P-521 SHA(224, 256, 384, 512) K-233 SHA(224, 256, 384, 512) K-283 SHA(224, 256, 384, 512) K-409 SHA(224, 256, 384, 512) K-571 SHA(224, 256, 384, 512) B-233 SHA(224, 256, 384, 512) B-283 SHA(224, 256, 384, 512) B-409 SHA(224, 256, 384, 512) B-571 SHA(224, 256, 384, 512)	SigGen
			P-192 SHA(1, 224, 256, 384, 512) P-224 SHA(1, 224, 256, 384, 512) P-256 SHA(1, 224, 256, 384, 512) P-384 SHA(1, 224, 256, 384, 512) P-521 SHA(1, 224, 256, 384, 512) K-233 SHA(1, 224, 256, 384, 512) K-283 SHA(1, 224, 256, 384, 512) K-409 SHA(1, 224, 256, 384, 512)	SigVer

Cert	Algorithm	Mode	Description	Functions/Caveats
			K-571 SHA(1, 224, 256, 384, 512) B-233 SHA(1, 224, 256, 384, 512) B-283 SHA(1, 224, 256, 384, 512) B-409 SHA(1, 224, 256, 384, 512) B-571 SHA(1, 224, 256, 384, 512)	
3691	HMAC [198]	SHA-1	Key Sizes: λ = *32 to 256 bytes*	Message Authentication
		SHA-224	Key Sizes: λ = *32 to* 256 *bytes*	
		SHA-256	Key Sizes: λ = *32 to 256 bytes*	
		SHA-384	Key Sizes: λ = *32 to 256 bytes*	
		SHA-512	Key Sizes: λ = *32 to 256*	
2973	RSA [186]	X9.31	n = 2048 SHA(256, 384, 512) n = 3072 SHA(256, 384, 512)	SigGen
		PKCS1_v1.5	n = 2048 SHA(224, 256, 384, 512) n = 3072 SHA(224, 256, 384, 512)	SigGen
		X9.31	n = 1024 SHA(1, 256, 384, 512) n = 2048 SHA(1, 256, 384, 512) n = 3072 SHA(1, 256, 384, 512)	SigVer
		PKCS1_v1.5	n = 1024 SHA(1, 224, 256, 384, 512) n = 2048 SHA(1, 224, 256, 384, 512) n = 3072 SHA(1, 224, 256, 384, 512)	SigVer
4446	SHS [180]	SHA-1 SHA-224 SHA-256 SHA-384 SHA-512		Message Digest Generation

Table 5 – Non-Approved but Allowed Cryptographic Functions

Algorithm	Description
Non-SP 800-56A Compliant EC Diffie-Hellman	[IG D.8] EC Diffie-Hellman (CVL Cert. #1980 ; shared secret computation provides between 112 and 256 bits of encryption strength)
Non-SP 800-56B Compliant RSA Key Transport (Encapsulation)	[IG D.9] RSA (key wrapping; key establishment methodology provides 112 bits of encryption strength)

Table 6 – Non-Approved Cryptographic Functions

Non-compliant Algorithm	Description
AES	[FIPS 197, SP 800-38A, SP 800-38B, SP 800-38C, SP 800-38E] Functions: Encryption, Decryption Modes:, CCM, CMAC, OFB, CFB1, CFB8, CFB128, XTS Key sizes: 128, 192, 256 bits
DRBG	[SP 800-90A] Functions: Hash DRBG, HMAC DRBG, Dual EC DRBG, CTR_DRBG w/ AES-128, AES-192, no_df, or Prediction Resistance disabled
DRNG	[ANSI X9.31] Functions: Random Number Generation
DSA	[FIPS 186-2] Functions: Key Pair Generation, Signature Generation, Signature Verification Key sizes: All Hashes: All
ECDH	len(n) < 224, which provides less than 112 bits of security strength
ECDSA	[FIPS 186-2] Functions: Key Pair Generation, Signature Generation, Signature Verification Key sizes: All Hashes: All [FIPS 186-4] Functions: PKG: Curves P192, K163, B163 SigGen: Curves(P192: (SHA1, 224, 256, 384, 512), P224:(SHA1), P256:(SHA1), P384: (SHA1), P521:(SHA1), K163: (SHA1, 224, 256, 384, 512), K233:(SHA1), K283:(SHA1), K409:(SHA1), K571:(SHA1), B163: (SHA1, 224, 256, 384, 512), B233:(SHA1), B283: (SHA1), B409:(SHA1), B571:(SHA1))

Non-compliant Algorithm	Description
RSA	Scheme: RSA Key Transport Key sizes: Less than 2048 bits Scheme: PSS [FIPS 186-2 and PKCS #1 v2.1], All [FIPS 186-2] Functions: Key Pair Generation, Signature Generation, Signature Verification Key sizes: All Hashes: All Schemes: PKCS1_v1.5 and X9.31 Functions: Signature Generation Key sizes: All Hashes: SHA1
Triple-DES	[SP800-67, SP800-20, SP 800-38B] Functions: Encryption, Decryption, MAC Generation, MAC Verification Modes: All Key sizes: All

2.1 Critical Security Parameters

All CSPs used by the Module are described in this section. All usage of these CSPs by the Module is described in the services detailed in Section 3.

Table 7 – Critical Security Parameters (CSPs)

CSP	Description / Usage
DRBG EI	DRBG entropy input[2]
DRBG State	DRBG secret values: V and Key
Encryption Key	AES key used for confidentiality
Private Key	RSA, DSA, or ECDSA key used for asymmetric cryptography
Integrity Key	HMAC key used for data integrity
ECDH Private Key	Private ECDH components used for key agreement

[2] The calling applications shall use entropy sources with at least 112 bits of entropy. There is no assurance of the minimum strength of generated keys.

CSP	Description / Usage
Shared Secret	Shared secret established via ECDH

2.2 Public Keys

Table 8 – Public Keys

Key	Description / Usage
Public Key	Public component of an RSA, DSA, or ECDSA key pair used
ECDH Public Component	Public component of an ECDH key pair.

3 Roles, Authentication and Services

3.1 Assumption of Roles

The module supports two operator roles, User and Cryptographic Officer (CO). Roles are selected implicitly based on the services invoked. No authentication is supported.

Table 9 lists all operator roles supported by the module. The Module does not support a maintenance role, bypass capability, or concurrent operators.

Table 9 – Roles Description

Role ID	Role Description	Authentication Type
CO	Responsible for loading the module and setting the FIPS mode.	None
User	Operational usage of the module.	None

3.2 Services

All services implemented by the Module are listed in the table below. The non-Approved mode provides the same list of services, but includes the non-Approved algorithms listed in Table 6.

Table 10 – Services

Service	Description	CO	U
Library Loading	Load the module into memory	X	
Set FIPS	Configure the module for FIPS mode	X	
Encryption	Symmetric encryption		X
Decryption	Symmetric decryption		X
Message Digest	Hash and Keyed-Hash algorithms, which include HMAC and SHA		X
Random Number Generation	Generate a random number or cryptographic key		X
Signature Generation	RSA, DSA, or ECDSA signature generation		X
Signature Verification	RSA, DSA, or ECDSA signature verification		X
Key Establishment	RSA Key Transport or EC DH		X
Zeroize	Destruction of all plaintext CSPs by power cycling		X
Show Status	Provided by return codes	X	X
Self-Tests	Invokes the FIPS 140-2 Power-On Self-Tests; performed on demand by re-loading the module	X	X
Utility	Miscellaneous helper functions		X

Table 11 defines the relationship between access to CSPs and the different module services. The modes of access shown in the table are defined as:

- R = Read: The module reads the CSP. The read access is typically performed before the module uses the CSP.
- W = Write: The module writes the CSP. The write access is typically performed after a CSP is imported into the module, when the module generates a CSP, or when the module overwrites an existing CSP.
- Z = Zeroize: The module zeroizes the CSP.

Table 11 – CSP & Cryptographic Key Access Rights within Services

		CSPs & Cryptographic Keys							
Services	DRBG EI	DRBG State	Encryption Key	Private Key	Integrity Key	ECDH Private Key	Shared Secret	Public Key	ECDH Public Component
Library Loading									
Set FIPS									
Encryption			RW						
Message Digest					RW				
Random Number Generation	RW	RW		RW				RW	RW
Signature Generation		RW		RW					
Signature Verification								RW	RW
Key Establishment				RW		RW	RW	RW	RW
Zeroize	Z	Z	Z	Z	Z	Z	Z	Z	Z
Show Status									
Self-Tests									
Utility									

4 Self-tests

Each time the Module is powered up it tests that the cryptographic algorithms still operate correctly. Power up self-tests are available on demand by power cycling the module.

On power up or reset, the Module performs the self-tests described in Table 12 below. All KATs must be completed successfully prior to any other use of cryptography by the Module. If one of the KATs fails, the Module enters an error state.

Table 12 – Power Up Self-tests

Test Target	Description
Software Integrity	HMAC SHA-1 integrity test performed at power-up
AES	KATs: Encryption, Decryption Modes: ECB Key sizes: 128 bits
DRBG	KATs: CTR DRBG, Security Strengths: 256 bits
DSA	PCT: Signature Generation, Signature Verification Key size: 2048 bit key Hash: SHA-384
EC CDH	KAT: Shared secret calculation Curves: P-224
ECDSA	PCT: Signature Generation, Signature Verification Curves: P-224, K-233 Hash: SHA-512
GCM	KATs: GMAC Generation, GMAC Verification Key sizes: 256 bits
HMAC	KATs: Generation, Verification SHA sizes: SHA-1, SHA-224, SHA-256, SHA-384, SHA-512
RSA	KATs: Signature Generation, Signature Verification (PKCS#1 w/ SHA-256) Key sizes: 2048 bits
SHS	KATs: SHA-1, SHA-224, SHA-256, SHA-384, SHA-512

Table 13 – Conditional Self-tests

Test Target	Description
DRBG	DRBG Continuous Test performed when a random value is requested from the DRBG.
DRBG Health Checks	Performed conditionally per SP 800-90 Section 11.3. Required per IG C.1.
DSA	DSA Pairwise Consistency Test performed on every DSA key pair generation.
ECDSA	ECDSA Pairwise Consistency Test performed on every ECDSA key pair generation.

5 Physical Security Policy

Not applicable. The module is software only.

6 Operational Environment

The Module is designated to operate on Ubuntu 14.04. Please see Table 1.

7 Mitigation of Other Attacks Policy

Not applicable. The Module has not been tested to support mitigation of attacks beyond the scope of FIPS 140-2 requirements.

8 Security Rules and Guidance

The Module design corresponds to the Module security rules. This section documents the security rules enforced by the cryptographic module to implement the security requirements of this FIPS 140-2 Level 1 module.

1. The operator shall be capable of commanding the module to perform the power up self-tests by cycling power or resetting the module.
2. Power up self-tests do not require any operator action.
3. Data output shall be inhibited during key generation, self-tests, zeroization, and error states.
4. Status information does not contain CSPs or sensitive data that if misused could lead to a compromise of the module.
5. There are no restrictions on which keys or CSPs are zeroized by the zeroization service.
6. The module does not support concurrent operators.
7. The module does not support a maintenance interface or role.
8. The module does not support manual key entry.
9. The module does not have any external input/output devices used for entry/output of data.
10. The module does not output intermediate key values.

9 Secure Distribution and Operation

The Module is designed for the sole consumption of Juniper Networks, Inc. and is only available internally to Juniper Networks.

10 EMI/EMC

The module is software-only, but the GPC on which the module is installed shall (at a minimum) conform to the EMI/EMC requirements specified by 47 Code of Federal Regulations, Part 15, Subpart B, Unintentional Radiators, Digital Devices, Class A (i.e., for business use).

11 User Guide

For AES GCM, the IV is generated internally within the GCM algorithm boundary per SP 800-38D, Section 8.2.1. If power is lost, the operator can set the IV to the last value used.

> Note: SP 800-38D, Section 8.2.1 is used for AES GCM IV Construction (i.e., IVs are generated deterministically and IG A.5 Scenario #3 applies). Deterministic IV generation is performed as follows. The IV fixed field size will have a minimum size of 4 bytes in approved mode. The contents are supplied by the caller based on the invocation. The IV fixed field contents (e.g., the module's name) allows for at least 2^{32} different names. The IV invocation field has a minimum size of 64 bits in approved mode. The contents are initially from an approved PRNG source, with the alternative of all zeros or a value supplied by the caller. The IV's invocation field increments by 1. It will take 2^{64} increments for the IV invocation field to wrap.

12 References and Definitions

The following standards are referred to in this Security Policy.

Table 14 – References

Abbreviation	Full Specification Name
[FIPS140-2]	*Security Requirements for Cryptographic Modules*, May 25, 2001
[IG]	*Implementation Guidance for FIPS PUB 140-2 and the Cryptographic Module Validation Program*
[131A]	*Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths*, *January 2011*
[133]	*NIST Special Publication 800-133, Recommendation for Cryptographic Key Generation, December 2012*
[186]	*National Institute of Standards and Technology, Digital Signature Standard (DSS), Federal Information Processing Standards Publication 186-4, July, 2013.*
[197]	*National Institute of Standards and Technology, Advanced Encryption Standard (AES), Federal Information Processing Standards Publication 197, November 26, 2001*

Abbreviation	Full Specification Name
[198]	*National Institute of Standards and Technology, The Keyed-Hash Message Authentication Code (HMAC), Federal Information Processing Standards Publication 198-1, July, 2008*
[180]	*National Institute of Standards and Technology, Secure Hash Standard, Federal Information Processing Standards Publication 180-4, August, 2015*
[38A]	*National Institute of Standards and Technology, Recommendation for Block Cipher Modes of Operation, Methods and Techniques, Special Publication 800-38A, December 2001*
[38B]	*National Institute of Standards and Technology, Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication, Special Publication 800-38B, May 2005*
[38C]	*National Institute of Standards and Technology, Recommendation for Block Cipher Modes of Operation: The CCM Mode for Authentication and Confidentiality, Special Publication 800-38C, May 2004 (errata update 07-20-2007)*
[38D]	*National Institute of Standards and Technology, Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC, Special Publication 800-38D, November 2007*
[38E]	*National Institute of Standards and Technology, Recommendation for Block Cipher Modes of Operation: The XTS-AES Mode for Confidentiality on Storage Devices, Special Publication 800-38E, January 2010*
[56Ar3]	*NIST Special Publication 800-56A Revision 3, Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography, April 2018*
[56Ar2]	*NIST Special Publication 800-56A Revision 2, Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography, May 2013*
[56A]	*NIST Special Publication 800-56A, Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography, March 2006.*
[56Br1]	*NIST Special Publication 800-56A Revision 1, Recommendation for Pair-Wise Key Establishment Schemes Using Integer Factorization Cryptography, September 2014*
[67]	*National Institute of Standards and Technology, Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher, Special Publication 800-67, May 2004*
[90A]	*National Institute of Standards and Technology, Recommendation for Random Number Generation Using Deterministic Random Bit Generators, Special Publication 800-90A, June 2015.*