NetApp Cryptographic Security Module

3.0.8

FIPS 140-2 Non-Proprietary Security Policy

v1.1

NetApp, Inc.
October 21, 2024

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

1 Introduction

This document is the non-proprietary Cryptographic Module Security Policy for the NetApp Cryptographic Security Module (NCSM). This security policy describes how the NCSM (Software Version: 3.0.8) meets the security requirements of FIPS 140-2, and how to operate it in a secure FIPS 140-2 mode. This policy was prepared as part of the Level 1 FIPS 140-2 validation of the NetApp Cryptographic Security Module.

This document provides an overview of the NetApp Cryptographic Security Module and explains the secure configuration and operation of the module. Apart from this Non-Proprietary Security Policy, the FIPS 140-2 Validation Submission Documentation is NetApp-proprietary and is releasable only under appropriate non- disclosure agreements. For access to these documents, please contact NetApp Inc.

FIPS 140-2 (Federal Information Processing Standards Publication 140-2 — *Security Requirements for Cryptographic Modules*) details the U.S. Government requirements for cryptographic modules. More information about the FIPS 140-2 standard and the FIPS 140-2 validation program is available on the NIST website at http://csrc.nist.gov/groups/STM/index.html.

2 Cryptographic Module Description

The NetApp Cryptographic Security Module is a software library that provides cryptographic services to a vast array of NetApp's storage and networking products.

The module provides FIPS 140-2 validated cryptographic algorithms for services such as IPSEC, SRTP, SSH, TLS, 802.1x, etc. The module does not directly implement any of these protocols, instead it provides the cryptographic primitives and functions to allow a developer to implement the various protocols.

In this document, the NetApp Cryptographic Security Module is variously referred to as NCSM, the Library, or the Module.

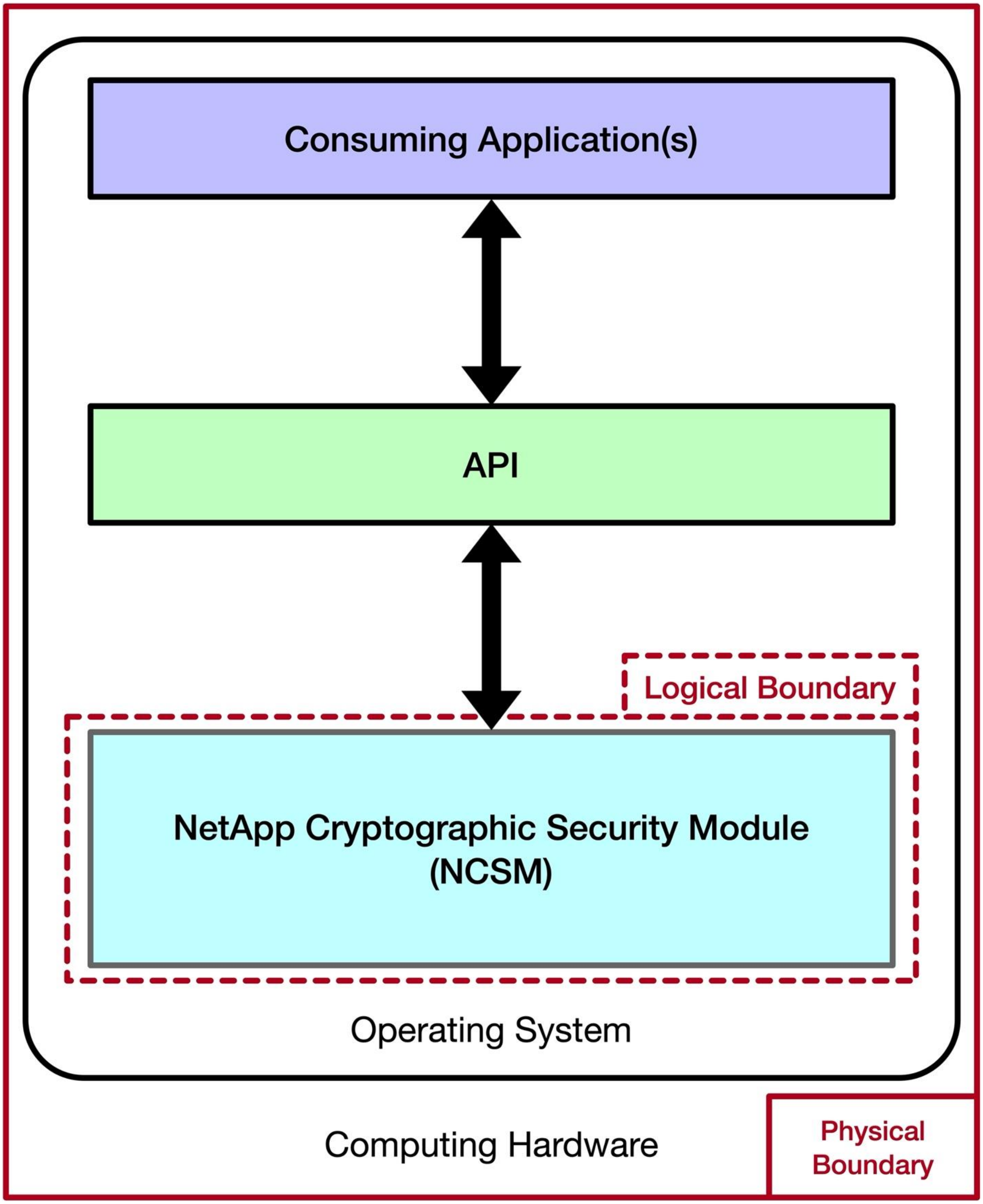
2.1 Module Overview

The Module is a multi-chip standalone cryptographic module. For the purposes of the FIPS 140-2 level 1 validation, the NCSM cryptographic module is a single dynamically loadable library named *fips.so*. The Module performs no communications other than with the calling application (the process that invokes the Module services via the Module's API).

2.2 Module Boundary

The module's logical block diagram is shown in Figure 1 below. The dashed red border denotes the logical cryptographic boundary of the module. The physical cryptographic boundary of the module is the enclosure of the system on which it is executing and is denoted by the solid red boundary.

Figure 1) NCSMv3 block diagram



2.3 Validation Level

The following table lists the FIPS 140-2 security level associated with each of the FIPS 140-2 requirements.

Table 1) Security Levels

FIPS 140-2 Security Requirement Levels	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
Cryptographic Key Management	1
EMI/EMC	1
Self-Tests	1
Design Assurance	1
Mitigation of Other Attacks	1
Overall Level	1

2.4 Tested Configurations

The Module has been tested on the NetApp platforms listed below in Table 2.

Table 2) Tested Operational Environments

#	Operating System	Hardware Platform	Processor	PAA/Acceleration
1	ONTAP 9.14.1	AFF A150	Intel® Xeon® D-1557	PAA (AES-NI)
2	ONTAP 9.14.1	AFF A150	Intel® Xeon® D-1557	None
3	ONTAP 9.14.1	AFF A320	Intel® Xeon® Silver 4114	PAA (AES-NI)
4	ONTAP 9.14.1	AFF A320	Intel® Xeon® Silver 4114	None
5	ONTAP 9.14.1	AFF A400	Intel® Xeon® Silver 4210	PAA (AES-NI)
6	ONTAP 9.14.1	AFF A400	Intel® Xeon® Silver 4210	None
7	ONTAP 9.14.1	FAS9500	Intel® Xeon® Platinum 8352Y	PAA (AES-NI)
8	ONTAP 9.14.1	FAS9500	Intel® Xeon® Platinum 8352Y	None
9	ONTAP 9.14.1	AFF C250	Intel® Xeon® D-2164IT	PAA (AES-NI)
10	ONTAP 9.14.1	AFF C250	Intel® Xeon® D-2164IT	None

#	Operating System	Hardware Platform	Processor	PAA/Acceleration
11	ONTAP 9.14.1	FAS2820	Intel® Xeon® D-1735TR	PAA (AES-NI)
12	ONTAP 9.14.1	FAS2820	Intel® Xeon® D-1735TR	None
13	StorageGRID 11.8	SG6160	Intel® Xeon® Gold 5318Y	PAA (AES-NI)
14	StorageGRID 11.8	SG6160	Intel® Xeon® Gold 5318Y	None
15	StorageGRID 11.8	SG110	Intel® Xeon® Silver 4310	PAA (AES-NI)
16	StorageGRID 11.8	SG110	Intel® Xeon® Silver 4310	None
17	StorageGRID 11.8	SG5812	Intel® Xeon® D-1735TR	PAA (AES-NI)
18	StorageGRID 11.8	SG5812	Intel® Xeon® D-1735TR	None

2.5 Vendor-affirmed Configurations

This module is vendor-affirmed to operate on the following platforms in Table 3. The CMVP makes no claim as to the correct operation of the module or the security strengths of the generated keys when ported to an operational environment which is not listed on the validation certificate.

Table 3) Vendor Affirmed Operational Environments

#	Operating System	Hardware Platform
1	ONTAP 9.15, 9.16	AFF A1K
2	ONTAP 9.14.1, 9.15, 9.16	AFF A220
3	ONTAP 9.14.1, 9.15, 9.16	AFF A250
4	ONTAP 9.14.1, 9.15, 9.16	AFF A300
5	ONTAP 9.15, 9.16	AFF A90
6	ONTAP 9.14.1, 9.15, 9.16	AFF A700
7	ONTAP 9.14.1, 9.15, 9.16	AFF A700s
8	ONTAP 9.14.1, 9.15, 9.16	AFF A800
9	ONTAP 9.14.1, 9.15, 9.16	AFF A900
10	ONTAP 9.14.1, 9.15, 9.16	AFF C190
11	ONTAP 9.14.1, 9.15, 9.16	AFF C400
12	ONTAP 9.14.1, 9.15, 9.16	AFF C800
13	ONTAP 9.14.1, 9.15, 9.16	ASA A150
14	ONTAP 9.14.1, 9.15, 9.16	ASA A250
15	ONTAP 9.14.1, 9.15, 9.16	ASA A400
16	ONTAP 9.14.1, 9.15, 9.16	ASA A800
17	ONTAP 9.14.1, 9.15, 9.16	ASA A900
18	ONTAP 9.14.1, 9.15, 9.16	ASA AFF A220
19	ONTAP 9.14.1, 9.15, 9.16	ASA AFF A250

#	Operating System	Hardware Platform
20	ONTAP 9.14.1, 9.15, 9.16	ASA AFF A400
21	ONTAP 9.14.1, 9.15, 9.16	ASA AFF A700
22	ONTAP 9.14.1, 9.15, 9.16	ASA AFF A800
23	ONTAP 9.14.1, 9.15, 9.16	ASA C250
24	ONTAP 9.14.1, 9.15, 9.16	ASA C400
25	ONTAP 9.14.1, 9.15, 9.16	ASA C800
26	ONTAP 9.14.1, 9.15, 9.16	FAS2720
27	ONTAP 9.14.1, 9.15, 9.16	FAS2750
28	ONTAP 9.14.1, 9.15, 9.16	FAS500f
29	ONTAP 9.14.1, 9.15, 9.16	FAS8200
30	ONTAP 9.14.1, 9.15, 9.16	FAS8300
31	ONTAP 9.14.1, 9.15, 9.16	FAS8700
32	ONTAP 9.14.1, 9.15, 9.16	FAS9000
33	Data ONTAP Select 9.14.1, 9.15, 9.16 with VMware ESXi 7/8	FDvM300-16GB
34	Data ONTAP Select 9.14.1, 9.15, 9.16 with VMware ESXi 7/8	FDvM300-64GB
35	Data ONTAP Select 9.14.1, 9.15, 9.16 with VMware ESXi 7/8	FDvM300-128GB
36	Amazon FSx for NetApp ONTAP 9.14.1, 9.15, 9.16	AWS EC2 Nitro[1]
37	Cloud Volumes ONTAP 9.14.1, 9.15, 9.16	Microsoft Azure Compute[2]
38	Cloud Volumes ONTAP 9.14.1, 9.15, 9.16	Google Compute Engine[3]
39	StorageGRID 11.8, 11.9	SG100
40	StorageGRID 11.9	SG110
41	StorageGRID 11.8, 11.9	SG1000
42	StorageGRID 11.8, 11.9	SG1100
43	StorageGRID 11.8, 11.9	SG5712
44	StorageGRID 11.8, 11.9	SG5760
45	StorageGRID 11.9	SG5812
46	StorageGRID 11.8, 11.9	SG5860
47	StorageGRID 11.8, 11.9	SG6060
48	StorageGRID 11.8, 11.9	SG6024
49	StorageGRID 11.9	SG6160
50	StorageGRID 11.8, 11.9	SGF6112

[1] See https://docs.netapp.com/us-en/cloud-volumes/ontap-relnotes/reference-configs-aws.html
[2] See https://docs.netapp.com/us-en/cloud-volumes/ontap-relnotes/reference-configs-azure.html
[3] See https://docs.netapp.com/us-en/cloud-volumes/ontap-relnotes/reference-configs-gcp.html

3 Ports and Interfaces

The physical ports of the Module are the same as the system on which it is executing. The logical interface is a C-language application program interface (API). The logical interfaces and their mapping are described in the following table:

Table 4) Ports and Interfaces

Logical Interface Type	Data that passes over port/interface
Data Input	API entry point data input stack parameters
Data Output	API entry point output stack parameters
Control Input	API entry point and corresponding stack parameters
Status Output	API entry point return values and status stack parameters

Since the Module is a software module, control of the physical ports is outside of the Module's scope. Whenever the Module is performing self-tests, or is in an error state, all output on the logical data output interface is inhibited. On encountering an error, the Module will return an error value—it will not output any data on the Data Output logical port.

4 Roles, Services and Authentication

4.1 Roles

The Module meets all FIPS 140-2 level 1 requirements for Roles and Services, implementing both Crypto-User and Crypto-Officer roles. The User and Crypto Officer roles are implicitly assumed by the entity accessing services implemented by the Module.

4.2 Services

The Crypto Officer can install and initialize the Module. The Crypto Officer role is implicitly entered when installing the Module or performing system administration functions on the host operating system.

- User Role: Loading the Module and calling any of the API functions. This role has access to all services provided by the Module.
- Crypto-Officer Role: Includes all services associated with the User Role as well as the ability to install the Module on the host computer system. This role is assumed implicitly when the system administrator installs the Module library file.

Table 5) Service, Role(s), and Description

Service	Role(s)	Description
Initialize	User Crypto-Officer	Initialization of the Module. Does not access CSPs.
Self-Test	User Crypto-Officer	Perform Power-On Self-Tests (POST) on demand. Does not access CSPs.
Show Status	User Crypto-Officer	Show's the Module's status. Does not access CSPs.
CSP/Key Zeroization	User Crypto-Officer	Overwrite CSPs stored in allocated memory.

Service	Role(s)	Description
Random Number Generation	User Crypto-Officer	Used for random number and symmetric key generation. For random number generation includes the ability to • Seed or reseed a DRBG instance • Obtain random data Functionality is associated with CSPs associated with the following: • CTR_DRBG • Hash_DRBG • HMAC_DRBG
Asymmetric Key Generation	User Crypto-Officer	Used to generate DH, DSA, ECDH, ECDSA, Ed25519, RSA, X25519, and X448 keys, including the following key types: DH Public/Private, DSA SGK/SVK, ECDH Public/Private, ECDSA SGK/SVK, Ed25519 SGK/SVK, RSA SGK/SVK, X25519 Public/Private, and X448 Public/Private. The maximum entropy strength specified in SP 800-90Ar1 is the supported entropy strength for each mechanism and algorithm type.
Key Derivation	User Crypto-Officer	Used to derive keys using one of the following algorithms: • ANSI X9.6-2001 KDF • ANSI X9.42-2001 KDF • HKDF • KBKDF • PBKDF2 • SP 800-56Cr2 One-Step KDF (KDA) • SP 800-135 TLS 1.2 • SSHv2 • TLS 1.3 KDF
Symmetric Encrypt/Decrypt	User Crypto-Officer	Used to encrypt or decrypt data. Calling application passes in either AES Encryption/Decryption Key or the TDES Encryption/Decryption Key
Symmetric Digest	User Crypto-Officer	Used to generate or verify data integrity with CMAC. Calling application passes in the AES CMAC Key.
Message Digest	User Crypto-Officer	Used to generate a SHA-1, SHA-2, or SHA-3 message digest. Does not access CSPs.
Keyed Hash	User Crypto-Officer	Used to generate or verify data integrity with HMAC or KMAC. Calling application passes in the HMAC or KMAC Key

Service	Role(s)	Description
Key Transport	User Crypto-Officer	Used to encrypt or decrypt a key on behalf of the calling application. The calling application will also pass in the RSA KDK or KEK.
Key Wrapping	User Crypto-Officer	Used to encrypt or decrypt a key on behalf of the calling application. The calling application will also pass in the AES KEK.
Key Agreement	User Crypto-Officer	Used to perform key agreement primitives on behalf of the calling application. The calling application will pass in the appropriate DH Public/Private, ECDH Public/Private, RSA SGK/SVK, X25519 Public/Private, or X448 Public/Private keys.
Digital Signature	User Crypto-Officer	Used to generate or verify DSA, ECDSA, Ed25519, Ed448, or RSA digital signatures. The calling application will pass in the appropriate DSA SGK/SVK, ECDSA SKG/SVK, Ed25519 SGK/SVK, Ed448 SGK/SVK, or RSA SGK/SVK key.
Utility functions	User Crypto-Officer	Miscellaneous utility functions provided by the Module. Does not access CSPs

4.3 Authentication

As allowed by FIPS 140-2 at Security Level 1, the Module does not support user authentication for the provided roles. Only one role may be active at a time and the Module does not allow concurrent operators.

5 Physical Security

The module is comprised of software only and thus does not claim any physical security.

6 Operational Environment

The Module operates in a modifiable operational environment.

The tested operating systems segregate user processes into separate process spaces. Each process space is an independent virtual memory area that is logically separated from all other processes by the operating system software and hardware. The Module functions entirely within the process space of the process that invokes it, and thus satisfies the FIPS 140-2 requirement for a single-user mode of operation.

7 Cryptographic Algorithms and Key Management

7.1 Cryptographic Algorithms

The module implements a variety of approved and allowed algorithms.

7.2 Approved Cryptographic Algorithms

The module supports the following FIPS 140-2 approved algorithms:

Table 6) Approved Algorithms

CAVP Cert #	Algorithm	Standard	Sizes/Curves	Mode/Method	Use
A4858	AES [FIPS 197]	SP 800-38A	128, 192, 256 bits	EBC, CBC, CBC-CS1, CBC-CS2, CBC-CS3, OFB, CFB1, CFB8, CFB128, CTR	Encryption, Decryption
		SP 800-38B	128, 192, 256 bits	CMAC	Generate/Verify
		SP 800-38C	128, 192, 256 bits	CCM	Encryption, Decryption
		SP 800-38D	128, 192, 256 bits	GCM, GMAC	Encryption, Decryption GMAC Generate/Verify
		SP 800-38F	128, 192, 256 bits	KW, KWP (cipher, inverse)	Encryption, Decryption
		SP 800-38E	128, 256 bits	XTS	Encryption, Decryption
A4858	Triple-DES	SP 800-67r2	3-Key TDES	ECB, CBC	Encryption, Decryption
A4858	DSA	FIPS 186-4	L = 2048, N = 224 L = 2048, N = 256 L = 3072, N = 256	Key Pair Gen	Digital signature and asymmetric key generation
			L = 2048, N = 224 L = 2048, N = 256 L = 3072, N = 256 (All SHA sizes)	PQG Gen Sig Gen	
			L = 1024, N = 160 L = 2048, N = 224 L = 2048, N = 256 L = 3072, N = 256	PQG Ver Sig Ver	

CAVP Cert #	Algorithm	Standard	Sizes/Curves	Mode/Method	Use
A4858	ECDSA	FIPS 186-4	P-224, 256, 384, 521 K-233, 283, 409, 571 B-233, 283, 409, 571 Testing candidates	Key Gen	Digital signature and asymmetric key generation
			P-192, 224, 256, 384, 521 K-163, 233, 283, 409, 571 B-163, 233, 283, 409, 571	PKV	
			P-224, 256, 384, 521 K-233, 283, 409, 571 B-233, 283, 409, 571 (SHA2-224, 256, 384, 512, 512/224, 512/256)	Sig Gen	
			P-192, 224, 256, 384, 521 K-163, 233, 283, 409, 571 B-163, 233, 283, 409, 571 (SHA-1, SHA2-224, 256, 384, 512, 512/224, 512/256)	Sig Ver	
A4858	CVL	FIPS 186-4	2048, 3072, 4096	Gen Key 9.31	Digital Signature and Asymmetric Key Generation
			1024, 2048, 3072, 4096 (SHA-1, SHA2-224, 256, 384, 512, 512/224, 512/256)	Sig Ver 9.31	
			2048, 3072, 4096 (SHA2-256, 384, 512)	Sig Gen 9.31	
			2048, 3072, 4096 (SHA2-224, 256, 384, 512)	Sig Gen PKCS 1.5	
			1024, 2048, 3072, 4096 (SHA-1, SHA2-224, 256, 384, 512, 512/224, 512/256)	Sig Ver PKCS 1.5	
			2048, 3072 (SHA2-224, 256, 384, 512, 512/224, 512/256) 4096 (SHA2-224, 256, 384, 512)	Sig Gen PSS	

CAVP Cert #	Algorithm	Standard	Sizes/Curves	Mode/Method	Use
			1024, 2048, 3072, 4096 (SHA-1, SHA2-224, 256, 384, 512, 512/224, 512/256)	Sig Ver PSS	
A4858	CVL	FIPS 186-4	RSASP1 (mod 2048)		Signature Generation Primitive
A4858	KAS-FFC-SSC	SP 800-56Ar3	ffdhe2048, ffdhe3072, ffdhe4096, ffdhe6144, and ffdhe8192 safe prime groups per SP 800-56Ar3	dhEphem Domain Parameter Generation Domain Parameter Validation Key Pair Generation Full Public Key Validation Partial Public Key Validation	Key Agreement
	KAS-ECC-SSC		All P, B, and K curves (per Appendix D of SP 800-56Ar3) with all SHA sizes	Ephemeral Unified Domain Parameter Generation Domain Parameter Validation Key Pair Generation Full Public Key Validation	

CAVP Cert #	Algorithm	Standard	Sizes/Curves	Mode/Method	Use
A4858	KAS-RSA-SSC	SP 800-56Br2	2048, 3072, 4096, 6144, 8192 with SHA2-224, 256, 384, 512, 512/224, 512/256, SHA-3-224, 256, 384, 512	KAS1, KAS2 Key Generation methods: rsakpg1-crt, rsakpg2-crt, rsakpg1-basic, rsakpg2-basic, rsakpg1-prime-factor, rsakpg2-prime-factor	Key Agreement
A4858	CVL	SP 800-56Ar3	KAS ECC CDH with P-224, 256, 384, 521, K-233, 283, 409, 571, B-233, 283, 409, 571		Section 5.7.1.2: “ECC CDH Primitive used in Shared Secret Computation”
A4858	KTS	SP 800-38F	KTS (AES Cert #A4858; key establishment methodology provides between 128 and 256 bits of encryption strength)	AES KW, KWP AES CCM AES GCM	Key Transport
			KTS (AES Cert #A4858 and HMAC Cert #A4858; key establishment methodology provides between 128 and 256 bits of encryption strength)	AES (any mode) and HMAC	
			KTS (AES Cert #A4858; key establishment methodology provides between 128 and 256 bits of encryption strength)	AES (any node) and CMAC, GMAC	
			KTS (Triple-DES Cert #A4858 and HMAC Cert. #A4858; key establishment methodology provides 112 bits of encryption strength)	Triple-DES (ECB, CBC) and HMAC	

CAVP Cert #	Algorithm	Standard	Sizes/Curves	Mode/Method	Use
A4858	KTS-RSA	SP 800-56Br2	2048, 3072, 4096 KTS-RSA (Cert #A4858; key establishment methodology provides between 112 and 128 bits of encryption strength)	RSA-OAEP RSADP RSAEP	Key Transport
A4858	KDA	SP 800-56Cr2	One-Step KDF (Section 4), Two-Step KDF (Section 5)		Key Derivation Function
A4858	HKDF	SP 800-56Cr2	HMAC-based “Extract-and-Expand” Key Derivation Function		Key Derivation Function
A4858	PBKDF2	SP 800-132	HMAC-SHA-1, HMAC-SHA2-224, 256, 384, 512, 512/224, 512/256 (C = 1–10,000; sLen = 16–512 bytes)	Option 1a	Password-based Key Derivation
A4858	KBKDF	SP 800-108	CMAC AES128, CMAC AES192, CMAC AES256, HMAC-SHA-1, HMAC-SHA2-224, 256, 384, 512	Counter, Feedback	Key Derivation Function
A4858	CVL	SP 800-135	TLS 1.2 KDF (SHA2-256, 384, 512) SSHv2 KDF (SHA-1, SHA2-224, 256, 384, 512) ANSI X9.63-2001 KDF (SHA2-224, 384, 512) ANSI X9.42-2001 KDF (SHA-1, SHA2-224, 256, 384, 512, 512/224, 512/256, SHA3-224, 256, 384, 512)		Key Derivation Function
A4858	CVL	RFC 8446 (Section 7.1)	TLS 1.3 KDF (SHA2-256, 384)		Key Derivation Function
A4858	SHA-3, SHAKE	FIPS 202	SHA3-224, 256, 512 SHAK-128, 256	SHA-3	Message Digests
A4858	SHS	FIPS 180-4	SHA-1 SHA2-224, 256, 384, 512, 512/224, 512/256	SHA-1 SHA-2	Message Digests

CAVP Cert #	Algorithm	Standard	Sizes/Curves	Mode/Method	Use
A4858	HMAC	FIPS 198-1	SHA-1 SHA2-224, 256, 384, 512, 512/224, 512/256 SHA3-224, 256, 384, 512	SHA-1 SHA-2 SHA-3	Keyed Hash
A4858	KMAC	SP 800-185	KMAC-128 KMAC-256		Keyed Hash
A4858	CKG	SP 800-133r2	Cryptographic Key Generation		Key Generation Section 4 ("Using the Output of a Random Bit Generator") Section 6.1 ("Direct Generation of Symmetric Keys") Section 6.2 ("Derivation of Symmetric Keys")
A4858	DRBG	SP 800-90A	SHA-1 SHA2-224, 256, 384, 512, 512/224, 5112/256 SHA3-224, 256, 384, 512	Hash DRBG	Random Number Generation Symmetric Key Generation
			SHA-1 SHA2-224, 256, 384, 512, 512/224, 5112/256 SHA3-224, 256, 384, 512	HMAC DRBG	
			AES-128, 192, 256	CTR DRBG	

7.3 Allowed Cryptographic Algorithms

The module supports the following FIPS 140-2 allowed algorithms:

Table 7) Allowed Algorithms

Algorithm	Use/Function
X25519 (curve 25519 with 128 bits of security strength)	Key Agreement
X448 (curve 448 with 224 bits of security strength)	Key Agreement

The module implements the following non-Approved algorithms:

Table 8) Non-Approved Algorithms

Algorithm	Use/Function
Ed448 (curve Ed448 with 224 bits of security strength)	Digital Signature Generation
Ed25519 (curve Ed25519 with 128 bits of security strength)	Digital Signature Generation
SHA-1	Digital Signature Generation
RSA PKCS1.5 padding	Key Transport

Algorithms listed above shall not be used when operating in the FIPS Approved mode of operation. Use of the non-Approved algorithms listed in the table above will place the module in the non-Approved mode of operation.

7.4 Critical Security Parameters (CSPs) and Public Keys

The module supports the following CSPs listed in Table 9. The CSP access policies were listed previously in Table 4) Ports and Interfaces.

Table 9) Critical Security Parameters

Key or CSP Name	Description
RSA SGK	RSA (2048 to 16384 bits) signature generation key
RSA KDK	RSA (2048 to 16384 bits) key decryption key used for private key transport
DSA SGK	DSA (2048 or 3072) signature generation key
ECDSA SGK	ECDSA signature generation keys using all NIST defined B, K, and P-curves
DH Private	DH (256 to 512 bits) private key agreement key
EC DH Private	EC DH private key agreement key using all NIST defined B, K, and P-curves
X22519 Private	X22519 private key agreement key
X448 Private	X448 private key agreement key
AES EDK	AES (128, 192, 256 bit) encrypt/decrypt key
AES CMAC	AES (128, 192, 256 bit) CMAC generate/verify key

Key or CSP Name	Description
AES GCM	AES (128, 192, 256 bit) encrypt/decrypt key
AES XTS	AES (128, 256 bit) encrypt/decrypt key
AES Key Wrapping	AES (128, 192, 256 bit) key wrapping key
TDES EDK	TDES (3-key) encrypt/decrypt key
HMAC Key	Keyed hash key (160, 224, 256, 384, 512 bit)
KMAC key	Keyed hash key (128 to 1024 bit)
HASH_DRBG CSPs	V (440 and 888 bit) C (440 and 888 bit) Entropy input (depends on security strength)
HMAC_DRBG CSPs	V (160, 224, 256, 384, 512 bit) Key (AES 128, 192, 256 bit) Entropy input (depends on security strength)
CTR_DRBG CSPs	V (128 bit) Key (AES 128, 192, 256 bit) Entropy input (depends on security strength)
KDF secret	Secret value used for constructing the PRF key used for SP 800-108 KBKDF, SP 800-132 PBKDF, HKDF, KDA, SP 800-135 KDFs and TLS 1.3 KDF) key derivation functions

The Module does not output any intermediate key generation values. The Module supports the following Public Keys listed in Table 10.

Table 10) Public Keys

Key or CSP Name	Description
RSA SVK	RSA (2048 to 16384 bits) signature verification key
RSA KEK	RSA (2048 to 16384 bits) key encryption key used for public key transport
DSA SVK	DSA (1024, 2048, or 3072 bits) signature verification key
ECDSA SVK	ECDSA signature verification keys using all NIST defined B, K, and P-curves
DH Public	DH (2048, 3072, 4096, 6144, or 8192 bits) public key agreement key
EC DH Public	EC DH public key agreement key using all NIST defined B, K, and P-curves
X22519 Public	X22519 public key agreement key
X448 Public	X448 public key agreement key

For all CSPs and Public Keys:

- **Storage:** RAM, associated to entities by memory location. The Module stores DRBG state values for the lifetime of the DRBG instance. The module uses CSPs passed in by the calling application on the stack. The Module does not store any CSP persistently (beyond the lifetime of an API call), except for DRBG state values used for the Module's default key generation service.
- **Generation:** The Module implements SP 800-90 compliant DRBG services for creation of symmetric keys, and for generation of DSA, elliptic curve, and RSA keys as shown in Table 4. The calling application is responsible for storage of generated keys returned by the module.
- **Entry:** All CSPs enter the Module's logical boundary in plaintext as API parameters, associated by memory location. However, none cross the physical boundary.

- **Output:** The Module does not output CSPs, other than as explicit results of key generation services or keys passed into the module by the calling application. However, none cross the physical boundary.
- **Destruction:** Zeroization of sensitive data is performed automatically by API function calls for temporarily stored CSPs. The calling application is responsible for parameters passed in and out of the module.

7.5 Key Generation and Entropy

Private and secret keys as well as seeds and entropy input are provided to the Module by the calling application and are destroyed when released by the appropriate API function calls. Keys residing in internally allocated data structures (during the lifetime of an API call) can only be accessed using the Module defined API. The operating system protects application space from unauthorized access. Only the calling application that creates or imports keys can use or export such keys. All API functions (Module Services) are executed by the calling application invoking an API. Each API either succeeds or fails and is logically non-interruptible from the point of view of the calling application.

The module supports generation of ECDSA, RSA, DSA, EC Diffie-Hellman, and Diffie-Hellman key pairs per Section 5 in NIST SP 800-133r2. A NIST SP 800-90Ar1 random bit generator is used for generating the seed used in asymmetric key generation.

Applications shall use entropy sources that meet the security strength required for the random number generation mechanism as shown in [SP 800-90Ar1] Table 2 (Hash_DRBG, HMAC_DRBG, or CTR_DRBG). A minimum of 112-bits of entropy must be supplied. This entropy is supplied by means of callback functions. Those functions must return an error if the minimum entropy strength cannot be met.

8 Electromagnetic Interference/Electromagnetic Compatibility (EMI/EMC)

The only electromagnetic interference produced is that of the host platform on which the Module resides and executes. Pursuant to FIPS 140-2, all host systems on which FIPS 140-2 testing is performed meet the Federal Communications Commission (FCC) EMI and EMC requirements for business use as defined in Subpart B, Class A of FCC 47 Code of Federal Regulations Part 15.

9 Self-Tests

FIPS 140-2 requires self-tests to test the integrity of the operational environment at start-up. In addition, FIPS 140-2 requires the Module to perform additional conditional self-tests during normal operation of the Module.

9.1 Power-On Self-Tests

The power-on self-tests are run when the Module is initialized. These tests do not require operator intervention. The module will not output any data, nor will the Module initialize, if any of the required power-on self-tests fails.

The power-on self-tests implemented by the Module are listed in Table 11.

Table 11) Power-On Self-Tests

Algorithm	Type of Self-Test	Description
AES	KAT	Decrypt, ECB mode, 128-bit key
AES GCM	KAT	Encrypt, Decrypt, 256-bit key

Algorithm	Type of Self-Test	Description	
DRBG	KAT	CTR_DRBG	AES, 128-bit with derivation function
		HASH_DRBG	SHA2-256
		HMAC_DRBG	SHA-1 Generate, Reseed, Instantiate functions (per Section 11.3 of SP 800-90Ar1)
DSA	PCT	Sign and Verify using 2048-bit key with SHA-256	
ECDSA	PCT	Sign and Verify using P-224 and K-233	
KAS ECC-SSC	KAT	Ephemeral Unified Share Secret (Z) Computation (Section 6 of SP 800-56Ar3) with P-256	
KAS FFC-SSC	KAT	dhEphem Share Secret (Z) Computation (Section 6 of SP 800-56Ar3)	
KAS RSA-SSC	KAT	RSA Primitive Computation (Scenario 2 of IG D.8 and Section 6 of SP 800-56Br2)	
KBKDF	KAT	Counter Mode using HMAC-SHA2-256	
KDA	KAT	One-step KDF (Section 4 of SP 80-56Cr2) and Two-step KDF (Section 5 of SP 800-56Cr2)	
KTS RSA	KAT	Encrypt and Decrypt for Basic	
		Decrypt for CRT (IG D.9 and SP 800-56Br2)	
PBKDF2	KAT	Derivation of the Master Key (MK) (Section 5.3 of SP 800-132)	
RSA	KAT	Sign and Verify using 2048-bit key with SHA-256 with PKCS#1	
SHS	KAT	SHA-1, SHA2-512, SHA3-256	
Software Integrity	KAT	HMAC-SHA2-256	
SP 800-135 KDFs	KAT	TLS v1.2, SSHv2, ANSI X9.63-2001, and ANSI X9.42-2001 KDFs	
TLS v1.3 KDF	KAT	TLS v1.3 KDF (Section 7.1 of RFC 8446)	
Triple-DES	KAT	Encrypt, Decrypt using 3-key in CBC mode	

The SELF_TEST_post() function performs all power-up self-tests listed above with no operator intervention required when the module loads, returning a “1” if all power-up self-tests succeed, and a “0” otherwise. The power-up self-tests may also be performed on-demand by calling this function and interpretation of the return code is the responsibility of the calling application.

If any component of the power-up self-test fails, an internal flag is set to prevent subsequent invocation of any cryptographic function calls. The module will only enter the FIPS Approved mode if the module is reloaded and the call to SELF_TEST_post() succeeds.

9.2 Conditional Self-Tests

Conditional self-tests are run under specific conditions as indicated in Table 12.

Table 12) Conditional Self-Tests

Algorithm	Test
DSA	Pairwise consistency test on generation of a key pair
ECDSA	Pairwise consistency test on generation of a key pair
Entropy Source	FIPS 140-2 continuous test for a stuck fault
RSA	Pairwise consistency test on generation of a key pair

In the event of a DRBG self-test failure, the calling application must uninstantiate and re-instantiate the DRBG per the requirements of [SP 800-90]; this is not something the Module can do itself.

9.3 Assurances

The Module obtains the following assurances per SP 800-56Ar3 and SP 800-56Br2:

Table 13) Assurances

Standard	Description
SP 800-56Ar3	Per Section 5.6.2 of SP 800-56Ar3, required per IG D.8
SP 800-56Br2	Per Section 6.4 of SP 800-56Br2, required per IG D.8

9.4 Critical Function Tests

The Module does not implement any specific critical function tests.

10 Mitigation of Other Attacks

The Module implements two mitigations against timing-based side-channel attacks, namely Constant-time Implementations and Blinding.

Constant-time Implementations protect cryptographic implementations in the Module against timing analysis since such attacks exploit differences in execution time depending on the cryptographic

operation, and constant-time implementations ensure that the variations in execution time cannot be traced back to the key, CSP or secret data.

Numeric Blinding protects the RSA, DSA and ECDSA algorithms from timing attacks. These algorithms are vulnerable to such attacks since attackers can measure the time of signature operations or RSA decryption. To mitigate this the Module generates a random blinding factor which is provided as an input to the decryption/signature operation and is discarded once the operation has completed and resulted in an output. This makes it difficult for attackers to attempt timing attacks on such operations without the knowledge of the blinding factor and therefore the execution time cannot be correlated to the RSA/DSA/ECDSA key.

11 Crypto Officer and User Guidance

Please see Appendix A for installation and usage guidance for module operators.

11.1 AES-GCM Usage

The Module does not implement the TLS protocol itself, however, it provides the cryptographic functions required for implementing the protocol. AES GCM encryption is used in the context of the TLS protocol versions 1.2 and 1.3 (per Scenario 1 and Scenario 5 in FIPS 140-2 A.5 respectively). For TLS v1.2, the mechanism for IV generation is compliant with RFC 5288. The counter portion of the IV is strictly increasing. When the IV exhausts the maximum number of possible values for a given session key, this results in a failure in encryption and a handshake to establish a new encryption key will be required. It is the responsibility of the user of the module i.e., the first party, client or server, to encounter this condition, to trigger this handshake in accordance with RFC 5246. For TLS v1.3, the mechanism for IV generation is compliant with RFC 8446.

The Module also supports internal IV generation using the module's Approved DRBG. The IV is at least 96-bits in length per NIST SP 800-38D, Section 8.2.2. Per FIPS 140-2 IG A.5 Scenario 2 and NIST SP

800-38D, the approved DRBG generates outputs such that the (key, IV) pair collision probability is less than 2^{-32}.

If the Module power is lost and restored the user must ensure that the AES-GCM encryption/decryption keys are re-distributed.

The Module also supports importing of GCM IVs when an IV is not generated within the Module. In the FIPS approved mode, an IV must not be imported for encryption from outside the cryptographic boundary of the Module as this will result in a non-conformance.

11.2 Triple-DES Usage

The calling application shall ensure that a given Triple-DES key is used to encrypt no more than 2^{16} 64-bit blocks of data.

11.3 Miscellaneous

The module performs run-time checks related to enforcement of security parameters such as the minimum-security strength of keys, valid key sizes, and usage of approved curves.

Validation of domain parameters prior to generating keys using functions provided by the module is the responsibility of the Cryptographic Officer and not enforced by the module itself.

Appendix A: Installation and Usage Guidance

A.1 Installation and Usage Guidance

The module comes pre-installed on various NetApp products. No customer installation is necessary.

A.2 Installation and Usage Guidance

The module is architected to be compliant with all FIPS 140-2 power-on requirements. Upon invocation of the shared library or application into which the object module has been compiled, the module begins to execute a prescribed set of startup tasks including both an integrity test and the POSTs described in section 9.1 above.

To enable NCSM in FIPS mode, ONTAP users need to run the "security config modify -interface SSL -is-fips-enabled true" command.

To enable use of NCSM in FIPS mode, StorageGRID users should review the StorageGRID 11.8 documentation section, *Manage the TLS and SSH policy,* and the follow one of the procedures below:

a) Select the *FIPS strict* policy from the *Use Policy* setting under *CONFIGURATION > Security > Security settings* Grid Manager page. A rolling reboot might be required after making this configuration change.

b) Create a custom policy on the *CONFIGURATION > Security > Security settings* Grid Manager page. Ensure that the *fipsMode* property is set to *true*. A rolling reboot might be required after making this configuration change.

The SELF_TEST_post() function performs all power-on self-tests listed above with no operator intervention required when the module loads or when FIPS mode is enabled, returning a "1" if all power-on self-tests succeed, and a "0" otherwise. The power-on self-tests can also be performed on demand by calling this function. Interpretation of the return code is the responsibility of the calling application.

If any component of the power-on self-test fails, an internal flag is set to prevent subsequent invocation of any cryptographic function calls. The module will only enter the FIPS Approved mode if the module is reloaded and the call to SELF_TEST_post() succeeds.

The module is in the Approved mode of operation when only the algorithms listed in Table 6 and Table 7 are being used. If any of the algorithms listed in Table 8 are used, the module enters the non-Approved mode of operation.

No operator intervention is required during the running of the self-tests.

Appendix B: Acronyms

This section describes the acronyms used throughout the document.

Table 14) Acronyms

Acronym	Definition
AES	Advanced Encryption Standard
API	Application Program Interface
CAVP	Cryptographic Algorithm Validation Program
CMVP	Cryptographic Module Validation Program
CMAC	Cipher-based Message Authentication Code
CSP	Critical Security Parameter
CTR	Counter mode
DH	Diffie-Hellman
DSA	Digital Signature Algorithm
ECDSA	Elliptic Curve Digital Signature Algorithm
ECDH	Elliptic Curve Diffie-Hellman
EDK	Encrypt/Decrypt Key
FIPS	Federal Information Processing Standards
GCM	Galois/Counter Mode
GMAC	Galois Message Authentication Code
HKDF	HMAC-based Extract-and-Expand Key Derivation Function
HMAC	Hashed Message Authentication Code
IG	Implementation Guidance
IV	Initialization Vector
KAT	Known Answer Test
KBKDF	Key Based Key Derivation Function
KDA	Key Derivation Algorithm
KDK	Key Derivation Key
KDF	Key Derivation Function
KEK	Key Encryption Key
KMAC	KECCAK Message Authentication Code
NIST	National Institute of Standards and Technology
PAA	Processor Algorithm Acceleration
PBKDF2	Password Based Key Derivation Function
PCT	Pairwise Consistency Test
PKG	Private Key Generator
RSA	Rivest Shamir Adleman
SHA	Secure Hash Algorithm
SHAKE	Secure Hash Algorithm Keccak
SGK	Signature Generation Key
SVK	Signature Verification Key

Acronym	Definition
TDES	Triple Data Encryption Algorithm

Appendix C: References

[ANSI X9.42-2001] Public Key Cryptography for the Financial Services Industry: Agreement of Symmetric Keys Using Discrete Logarithm Cryptography

[ANSI X9.63-2001] Public Key Cryptography for the Financial Services Industry: Key Agreement and Key Transport Using Elliptic Curve Cryptography

[FIPS 140-2] Security Requirements for Cryptographic Modules, May 25, 2001

https://csrc.nist.gov/files/pubs/fips/140-2/upd2/final/docs/fips1402.pdf

[FIPS 180-4] Secure Hash Standard (SHS)

https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.180-4.pdf

[FIPS 186-4] Digital Signature Standard

https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf

[FIPS 197] Advanced Encryption Standard

https://csrc.nist.gov/publications/fips/fips197/fips-197.pdf

[FIPS 198-1] The Keyed Hash Message Authentication Code (HMAC)

https://csrc.nist.gov/csrc/media/publications/fips/198/1/final/documents/fips-198-_final.pdf

[FIPS 202] SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions

https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.202.pdf

[PKCS#1] Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1

https://www.rfc-editor.org/info/rfc3447

[RFC 5288] AES Galois Counter Mode (GCM) Cipher Suites for TLS

https://datatracker.ietf.org/doc/html/rfc5288

[RFC 8446] The Transport Layer Security (TLS) Protocol Version 1.3

https://datatracker.ietf.org/doc/html/rfc8446

[SP 800-38A] NIST Special Publication 800-38A – Recommendation for Block Cipher Modes of Operation: Methods and Techniques

https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-38a.pdf

[SP 800-38B] NIST Special Publication 800-38B – Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication

https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-38b.pdf

[SP 800-38C] NIST Special Publication 800-38C – Recommendation for Block Cipher Modes of Operation: The CCM Mode for Authentication and Confidentiality

https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-38c.pdf

[SP 800-38D] NIST Special Publication 800-38D – Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC

https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-38d.pdf

[SP 800-38E] NIST Special Publication 800-38E – Recommendation for Block Cipher Modes of Operation: The XTS AES Mode for Confidentiality on Storage Devices

https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-38e.pdf

[SP 800-38F] NIST Special Publication 800-38F – Recommendation for Block Cipher Modes of Operation: Methods for Key Wrapping

https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-38F.pdf

[SP 800-56Ar3] NIST Special Publication 800-56A Revision 3 – Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography

https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-56Ar3.pdf

[SP 800-56Br2] NIST Special Publication 800-56B Revision 2 – Recommendation for Pair-Wise Key Establishment Using Integer Factorization Cryptography

https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-56Br2.pdf

[SP 800-56Cr2] NIST Special Publication 800-56C Revision 2 – Recommendation for Key-Derivation Methods in Key-Establishment Schemes

https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-56Cr2.pdf

[SP 800-67r2] NIST Special Publication 800-67 Revision 2 – Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher

https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-67r2.pdf

[SP 800-90Ar1] NIST Special Publication 800-9A Revision 1 – Recommendation for Random Number Generation Using Deterministic Random Bit Generators

https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-90Ar1.pdf

[SP 800-108] NIST Special Publication 800-108 (Revised) – Recommendation for Key Derivation Using Pseudorandom Functions

https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-108.pdf

[SP 800-132] NIST Special Publication 800-132– Recommendation for Password-Based Key Derivation

https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-132.pdf

[SP 800-133r2] NIST Special Publication 800-133 Revision 2 – Recommendation for Cryptographic Key Generation

https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-133r2.pdf

[SP 800-135r1] NIST Special Publication 800-135 Revision 1 – Recommendation for Existing Application-Specific Key Derivation Functions

https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-135r1.pdf

12 Version history

Version history is only for drafts. Remove before final submission.

Version	Date	Document version history
Version 1.0	12/20/2023	Initial version
Version 1.1	09/13/2024	Updated version Added AFF C250 (PAA and non-PAA) to tested configurations Added FAS2828 (PAA and non-PAA) to tested configurations Updated “vendor affirmed” table