Hewlett Packard
Enterprise

Voltage Cryptographic Module v.5.0

FIPS 140-2 Non-Proprietary Security Policy

Document Version 1.0

HPE Data Security

August 5, 2016

Revision History

The following table presents the history of changes to this document.

Document History

Date	Version	Changes
07/08/2016	1.0	Initial public release
07/29/2016	1.1	Adding NonStop operating systems
08/05/2016	1.2	Adding Windows operating systems

TABLE OF CONTENTS

1. Module Overview

The following summarize key features of the Module:

- The Voltage Cryptographic Module v.5.0 (Version 5.0) is a software-only cryptographic module embodied as a shared library binary that executes on general-purpose computer systems. The specific operating systems and versions that were validated are specified in the "Operational Environment" section of this document.
- The Module is accessible to client applications through an application-programming interface (API).
- The Module provides a FIPS mode of operation, which is described in the "Approved Mode of Operation" section of this document.
- For the purposes of FIPS 140-2, the Module is classified as a multichip standalone module.
- The Module provides program interfaces for data input and output. Figure 1 below illustrates these interfaces as well as defining the cryptographic boundary.

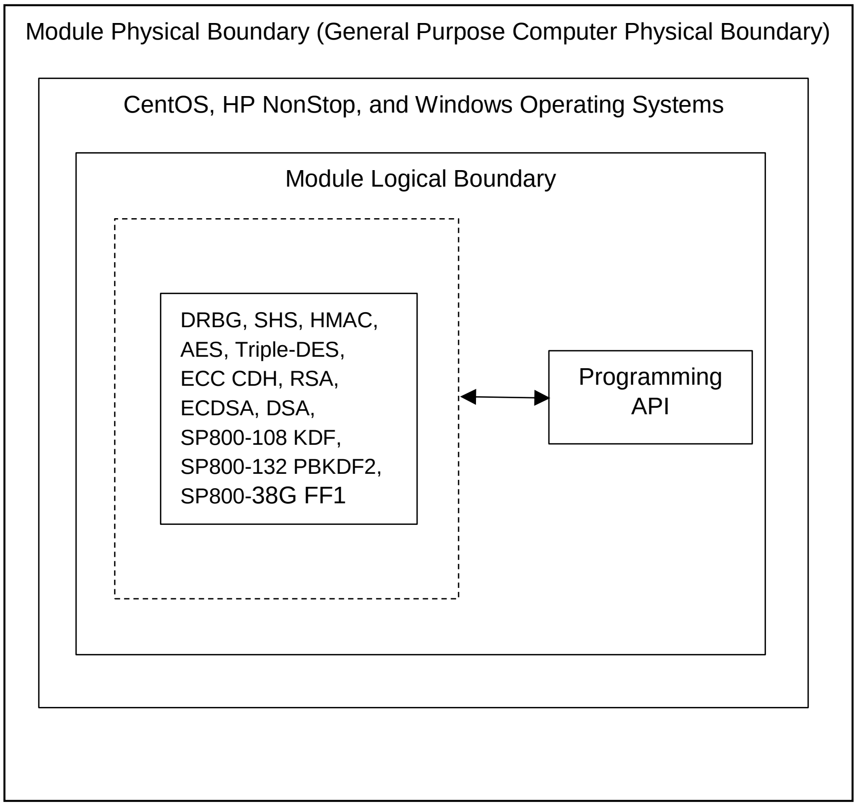
Module Physical Boundary (General Purpose Computer Physical Boundary)
CentOS, HP NonStop, and Windows Operating Systems
Module Logical Boundary
DRBG, SHS, HMAC, AES, Triple-DES, ECC CDH, RSA, ECDSA, DSA, SP800-108 KDF, SP800-132 PBKDF2, SP800-38G FF1
Programming API

Figure 1 – Block diagram of the Module

The Module was tested on the general-purpose operating systems and operating environments listed as follows:

- CPU Intel(R) Core(TM) i7-3770 with AES-NI w/ CentOS Linux release 7.0.1406
- CPU Intel(R) Core(TM) i7-3770 w/o AES-NI w/ CentOS Linux release 7.0.1406
- CPU Intel Itanium 9300, model NB54000c w/ HP NonStop TNS/E J06.19.00 – OSS
- CPU Intel Xeon E5-2600 v2 with AES-NI, model NS7 X1 w/ HP NonStop TNS/X L15.08.00 – OSS
- CPU Intel Itanium 9300, model NB54000c w/ HP NonStop TNS/E J06.19.00 – Guardian
- CPU Intel Xeon E5-2600 v2 with AES-NI, model NS7 X1 w/ HP NonStop TNS/X L15.08.00 – Guardian
- CPU Intel Xeon E5-2600 v2 w/o AES-NI, model NS7 X1 w/ HP NonStop TNS/X L15.08.00 – OSS
- CPU Intel Xeon E5-2600 v2 w/o AES-NI, model NS7 X1 w/ HP NonStop TNS/X L15.08.00 – Guardian
- CPU Intel(R) Core(TM) i7-2600 with AES-NI w/ Windows Server 2012 R2
- CPU Intel(R) Core(TM) i7-2600 w/o AES-NI w/ Windows Server 2012 R2

2. Security Level

The Module meets the overall requirements applicable to Level 1 security of FIPS 140-2.

Table 1: Module Security Level Specification

Security Requirements	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	N/A

3. Modes of Operation

The Module supports two modes of operation: FIPS Approved mode and non-Approved mode.

3.1 Approved mode of operation

The initialization happens when the calling application invokes FIPS_mode_set() , which returns a “1” for success and “0” for failure. The fips_mode_set() function verifies the integrity of the runtime executable using a HMAC-SHA1 digest computed at build time. If the digest matches, the power-up self-tests are performed automatically. If the power-up self-tests are successful, FIPS_mode_set() sets the FIPS_mode flag to TRUE and the module is in a FIPS Approved mode of operation.

The Module conforms to the IG 9.10 requirements by providing a Default Entry Point (DEP). The DEP is automatically executed, without requiring operator intervention (calling application).

In FIPS Approved mode, the Module supports the Approved algorithms listed in Table 2:

Table 2: Approved Algorithms and Modes of Operation

Algorithm	Modes of Operation	Certificate #
ECDSA (FIPS 186-4)	SigGen: P-224, 256, 384, 521 SigVer: P-192, 224, 256, 384, 521	803, 806, 829, 845, 846
DSA (FIPS 186-4)	Sign/Verify	1042, 1044, 1050, 1059, 1060
Two-key Triple-DES	Decrypt for TECB, TCBC, TCFB1, TCFB8, TCFB64, TOFB	1915, 1916, 1917, 1918, 2091, 2117, 2137, 2138
Three-Key Triple-DES	Encrypt/Decrypt for TECB, TCBC, TCFB1, TCFB8, TCFB64, TOFB	2169, 2208, 2209
SHA-1, SHA-224, SHA-256, SHA-384, SHA-512	Byte Oriented	2791, 2792, 2793, 2794, 3131, 3166, 3210, 3211
AES – 128-, 192- and 256-bit keys are supported	ECB, CBC, OFB, CFB1	3372, 3373, 3374, 3375, 3761, 3843, 3894, 3895
AES – 128-, 192- and 256-bit keys are supported	GCM	3410, 3411, 3412, 3413, 3761, 3843, 3894, 3895
AES – 128-, 192- and 256-bit keys are supported	CMAC Generation/Verification	3918, 4033, 4034
SP800-38G FPE – 128, 192 and 256-bit keys are supported (vendor affirmed)	Encrypt/decrypt for AES-FF1 (vendor affirmed: SP800-38G)	Prerequisite: 3372, 3373, 3374, 3375, 3761, 3843, 3894, 3895

Algorithm	Modes of Operation	Certificate #
		(AES-FF1, vendor affirmed: SP800-38G)
SP800-132 PBKDF2 (vendor affirmed)	Password based key derivation for storage applications (vendor affirmed: SP800-132)	Prerequisite: 2791, 2792, 2793, 2794, 3131, 3166, 3210, 3211 (PBKDF2, vendor affirmed: SP800-132)
HMAC-SHA1, HMAC-SHA256. HMAC-SHA512	Byte Oriented	2455, 2461, 2493, 2528, 2529
RSA	Sign/Verify	1730, 1731, 1732, 1733, 1935, 1963, 1984, 1985
SP800-90A DRBG	Hash-DRBG	796, 797, 798, 799, 1033, 1088, 1114, 1115
SP800-108 KBKDF	CTR	63, 67, 68, 69, 76, 83, 87, 88
CVL	Section 5.7.1.2: ECC CDH Primitive (P-224, P-256, P-384, P-521)	509, 510, 511, 512, 709, 732, 754, 755

Operators should reference the transition tables that will be available at the CMVP Web site (http://csrc.nist.gov/groups/STM/cmvp/). The data in the tables will inform users of the risks associated with using a particular algorithm and a given key length.

In FIPS Approved mode, the Module also supports non-Approved algorithms in limited uses as follows:

Table 3: Non-Approved Algorithms Available in FIPS Approved mode.

Algorithm	Limitations to Use
RSA key wrap	*RSA (key wrapping; key establishment methodology provides 112 bits of encryption strength)*
EC Diffie-Hellman	*EC Diffie-Hellman (key agreement; key establishment methodology provides between 112 and 256 bits of encryption strength)*

In FIPS Approved mode, the Module supports the following vendor affirmed algorithms:

- SP800-132 PBKDF2: shall only be used in storage applications.
- SP800-38G AES-FF1: the Module supports the following parameter lengths:
  - 128-, 192- and 256-bit keys
    - the underlying AES block cipher has a block size of 128-bits
  - *maxTlen* $\leq 2^{32} - 1$

  - *maxTlen* is the maximum length of the tweak *T*, where the tweak *T* is the input parameter to the encryption and decryption functions whose confidentiality is not necessarily protected by the mode
- $0 \leq t \leq \mathit{maxTlen}$
  - *t* is the byte length of the tweak *T*
- $\mathit{radix} \in [2 \,..\, 2^{16}]$
  - the number of characters in a given alphabet is the base, denoted by *radix*, thus $\mathit{radix} \geq 2$
- $2 \leq \mathit{minlen} \leq \mathit{maxlen} < 2^{32}$
  - range of supported message lengths, [*minlen* … *maxlen*]
- $\mathit{radix}^{\mathit{minlen}} \geq 100$
  - the parameters *radix* and *minlen* shall meet this requirement

3.2 Non-Approved mode of operation

The following table lists services implemented by the module that shall not be used when operating in the FIPS Approved mode of operation. If any of these services are used, the module is no longer considered to be in the FIPS Approved mode of operation. In the event that the Crypto Officer or User violates or attempts to violate such restrictions, the module is in strict violation of this Security Policy and is deemed fully non-compliant and unfit for service to protect sensitive unclassified data with cryptography. Both the Crypto Officer role and the User role have access to the non-Approved services listed in table below.

Table 4: Non-Approved Algorithms Disallowed in FIPS Approved mode

Roles	Function	Algorithm	Options
Crypto Officer, User	Random Number Generation; Symmetric Key Generation	ANSI X9.31 RNG	AES 128, 192 and 256-bit
		[SP800-90A] DRBG (non-compliant)	Dual EC DRBG
Crypto Officer, User	Encryption, Decryption and CMAC	[SP800-67] Three-Key Triple-DES (non-compliant)	CMAC generation and verification
		[SP800-67] Two-Key Triple-DES	Encrypt for TECB, TCBC, TCFB1, TCFB8, TCFB64, TOFB; CMAC generation and verification
		[FIPS 197] AES (non-compliant)	128, 192, 256-bit in CFB8, CFB128, CTR, XTS; CCM
		[SP800-38C] CCM (non-compliant) [SP800-38E] XTS (non-compliant)	
Crypto Officer, User	Keyed Hash	[FIPS 198] HMAC (non-compliant)	SHA-224, SHA-384
Crypto Officer, User	Digital Signature and Asymmetric Key Generation	[FIPS 186-2] RSA (non-compliant)	GenKey9.31, SigGen9.31, SigGenPSS, SigVer9.31, SigVerPSS (2048, 3072, 4096-bit with all SHA-2 sizes) GenKey9.31, SigGen9.31, SigGenPKCS1.5, SigGenPSS (1024/1536 with all SHA sizes, 2048/3072/4096 with SHA-1)
		[FIPS 186-2] DSA (non-compliant)	PQG Gen, Key Pair Gen, Sig Gen (1024 with all SHA sizes, 2048/3072 with SHA-1)
		[FIPS 186-4] DSA (non-compliant)	PQG Gen, PQG Ver, Key Pair Gen, Sig Gen (3072-bit with all SHA-2 sizes), Sig Ver (3072-bit with all SHA-2 sizes)

			PQG Gen, Key Pair Gen, Sig Gen (1024 with all SHA sizes, 2048/3072 with SHA-1)
		[FIPS 186-2] ECDSA (non-compliant)	PKG: CURVES(P-192 P-224 P-384 P-521 K-163 K-233 K-283 K-409 K-571 B-163 B-233 B-283 B-409 B-571) PKV: CURVES(P-192 P-224 P-256 P-384 P-521 K-163 K-233 K-283 K-409 K-571 B-163 B-233 B-283 B-409 B-571) PQG Gen, Key Pair Gen, Sig Gen (1024 with all SHA sizes, 2048/3072 with SHA-1)
		[FIPS 186-4] ECDSA (non-compliant)	PKG: CURVES(P-192 P-224 P-256 P-384 P-521 K-163 K-224 K-256 K-384 K-521 B-163 B-224 B-256 B-384 B-521 ExtraRandomBits TestingCandidates) PKV: CURVES(ALL-P ALL-K ALL-B) SigGen: CURVES(P-192: (SHA-1, 224, 256, 384, 512) P-224:(SHA-1) P-256:(SHA-1) P-384:(SHA-1) P-521:(SHA-1) K-163: (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) K-571: (SHA-1, 224, 256, 384, 512) B-163: (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)) SigVer: CURVES(K-163: (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) K-571: (SHA-1, 224, 256, 384, 512) B-163: (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))
Crypto Officer, User	ECC CDH (KAS)	[SP800-56A] (§5.7.1.2) (non-compliant)	All curves excluding CVL with P-224, P-256, P-384, P-521

4. Ports and Interfaces

The Module restricts all access to its Critical Security Parameters (CSPs) through the API calls listed in the "Roles and Services" section of this document. This API acts as the logical interface to the Module.

The physical ports of the general-purpose computer on which the Module runs, such as keyboards, hard disks, displays, etc., provide a means to access the Module, but the logical interface to the Module is just via the API itself. **Table 5** lists the logical interfaces to the Module.

Table 5: Module Logical Ports

Port	Description
Data Input	Parameters passed to the Module through API calls.
Data Output	Data returned by the Module through API calls.
Control Input	Control Input – API function calls.
Status Output	Error and status codes returned by API calls.

The Module does not support a cryptographic bypass mode.

All Data Output is inhibited during an error state. Data Output is also inhibited during the self-test and zeroization processes.

The following is the mapping of the physical ports/interfaces to the logical ports/interfaces available to the module:

1. Power supply unit: Provides power to the cryptographic module: Power Input
2. Video connector: Connects a monitor to the general purpose computing platform: Data Output, Status Output.
3. Serial connector: connects peripheral general purpose I/O devices such as mouse, keyboard, and monitor: Data Input, Data Output, Control Input, and Status Output
4. USB connectors: Connects peripheral general purpose I/O devices such as mouse, keyboard, and monitor: Data Input, Data Output, Control Input, and Status Output.
5. Ethernet connectors: provides network connectivity: Data Input, Data Output, Control Input, and Status Output.

5. Identification and Authentication Policy

This section describes the identification and authentication policy of the Module.
The Module supports two distinct operator roles (User and Crypto Officer). See section 6.1 Roles and Services

The Module does not support a Maintenance role.
The role of the operator of the Module is identified implicitly from the API function being called, as shown in **Table 8**. The Module is designed to meet the requirements specified for a Level 1 software-only module as per FIPS 140-2 and therefore does not support operator authentication, as shown in Table 7.

Table 6: Roles and Required Identification and Authentication

Role	Type of Authentication	Authentication Data
User	N/A	N/A
Crypto Officer	N/A	N/A

Table 7: Strengths of Authentication Mechanisms

Authentication Mechanism	Strength of Mechanism
N/A	N/A

6. Access Control Policy

This section describes the access control policy of the Module.

6.1 Roles and Services

The Module operator is any software application that is linked to the Module shared library.

The Module supports two roles: User and Crypto Officer. An operator accesses both roles while using the Module and the means of access is the same for both roles. A role is implicitly assumed based on the services that are accessed. These roles are defined as the following:

- User: allowed to perform all services provided by the Module.
- Crypto Officer: allowed to perform all services provided by the Module and also responsible for the installation of the module.

The Crypto Officer is any entity that can install the module library onto a general purpose computer system, configure the operating system and validate the compliance of the module. This role is implicitly selected when the Module is installed or the operating system is configured.

The Crypto Officer must have permission to write the library comprising the Module into an operating system directory. This typically requires administrator access to the operating system.

The *run self-tests* service is ran automatically when the Module is loaded.

6.2 Service Inputs and Outputs

The following table summarizes which CSPs are accessed by each service and how the CSP is accessed on behalf of the operator when the service is performed in FIPS mode of operation. All services are available to both the Crypto Officer and User roles.

Table 8: Summary of Service Inputs & Outputs

Service	Role	CSP	Create	Destroy	Read	Write
Installation of the module	Crypto Officer	None				
Initialization of the module	Crypto Officer, User	None				
Encrypt/decrypt data with symmetric key	Crypto Officer, User	AES Secret Key (128-, 192- and 256-bit) Two-Key Triple-DES Secret Key (112-bit) (decrypt only) Three-Key Triple-DES Secret Key (168-bit)	✓	✓	✓	✓

Signature generation and verification	Crypto Officer, User	RSA Private Signature Key (2048-bit) RSA Public Signature Key (2048-bit) RSA Private Key for Key Transport (2048-bit) RSA Public Key for Key Transport (2048-bit) DSA Private Key (2048-bit) DSA Public Key (1024- or 2048-bit) ECDSA Private Signature Key (P-224, P-256, P-384, P-521) ECDSA Public Signature Key (P-224, P-256, P-384, P-521) DRBG V Value DRBG C Value	✓	✓	✓	✓
Calculate message digest	Crypto Officer, User	None				
Compute HMAC on data	Crypto Officer, User	HMAC Secret Key (112-, 192- and 256-bit)	✓	✓	✓	✓
Compute CMAC on data	Crypto Officer, User	AES CMAC Key (128-, 192- and 256-bit)	✓	✓	✓	✓
Derive symmetric key	Crypto Officer, User	SP800-108 KBKDF Key Derivation Key (256-bit) SP800-108 KBKDF Internal State (256-bit) SP800-132 PBKDF2 Master Key (256-bit)	✓			

		SP800-132 PBKDF2 Internal State (256-bit) Password (64-bit)				
ECDH key pair establishment	Crypto Officer, User	ECC CDH Private Key (P-224, P-256, P-384, P-521) ECC CDH Shared Secret (P-224, P-256, P-384, P-521) ECC CDH Public Key (P-224, P-256, P-384, P-521)	✓	✓	✓	✓
Storage management	Crypto Officer, User	None				
Show status	Crypto Officer, User	None				
Run self-tests	Crypto Officer, User	None				
Random number generation	Crypto Officer, User	DRBG V Value DRBG C Value	✓	✓	✓	✓
Zeroize	Crypto Officer, User	AES Secret Key (128-, 192- and 256-bit) Two-key Triple-DES Secret Key (112-bit) DSA Private Key (2048-bit) RSA Private Signature Key (2048-bit) RSA Private Key for Key Transport (2048-bit) ECDSA Private Signature Key (P-224, P-256, P-384, P-521)		✓		

		SP800-108 KBKDF Key Derivation Key (256-bit) SP800-108 KBKDF Internal State (256-bit) ECC CDH Private Key (P-224, P-256, P-384, P-521) ECC CDH Shared Secret (P-224, P-256, P-384, P-521) DRBG V Value DRBG C Value HMAC Secret Key (112-, 192- and 256-bit) SP800-132 PBKDF2 Master Key (256-bit) SP800-132 PBKDF2 Internal State (256-bit) Password (64-bit) AES CMAC Key (128-, 192- and 256-bit) Three-Key Triple-DES Secret Key (168-bit) DSA Public Key (1024- or 2048-bit) RSA Public Signature Key (2048-bit) RSA Public Key for Key Transport (2048-bit) ECDSA Public Signature Key (P-224, P-256, P-384, P-521) ECC CDH Public Key (P-224, P-256, P-384, P-521)				

Table 8**: Summary of Service Inputs & Outputs** describes how the services performed by each role access each CSP. A checkmark is placed when a service can create, destroy, read or write a CSP.

6.3 Definition of Critical Security Parameters (CSPs)

The following list enumerates the secret keys, private keys, and CSPs contained in the Module:

- AES Secret Key (128-, 192- and 256-bit)
- Two-key Triple-DES Secret Key (112-bit)
- DSA Private Key (2048-bit)
- RSA Private Signature Key (2048-bit)
- RSA Private Key for Key Transport (2048-bit)
- ECDSA Private Signature Key (P-224, P-256, P-384, P-521)
- SP800-108 KBKDF Key Derivation Key (256-bit)
- SP800-108 KBKDF Internal State (256-bit)
- ECC CDH Private Key (P-224, P-256, P-384, P-521)
- ECC CDH Shared Secret (P-224, P-256, P-384, P-521)
- DRBG V Value
- DRBG C Value
- HMAC Secret key (112-, 192- and 256-bit)
- SP800-132 PBKDF2 Master Key (256-bit)
- SP800-132 PBKDF2 Internal State (256-bit)
- Password (64-bit)
- AES CMAC Key (128-, 192- and 256-bit)
- Three-Key Triple-DES Secret Key (168-bit)

The following list enumerates the public keys contained in the Module:

- DSA Public Key (1024- or 2048-bit)
- RSA Public Signature Key (2048-bit)
- RSA Public Key for Key Transport (2048-bit)
- ECDSA Public Signature Key (P-224, P-256, P-384, P-521)
- ECC CDH Public Key (P-224, P-256, P-384, P-521)

6.4 Definition of CSPs Modes of Access

Table 9 defines the relationship between access to CSPs and the different Module services. The modes of access shown in the table are defined as follows:

Table 9: CSP Access Rights within Roles & Services

Access	**Description**
Create	An object is created
Destroy	An object is destroyed and memory that it used is released
Read	Data stored by an object is accessed for use
Write	An object is modified

7. Operational Environment

The operational environment for the Module is a “modifiable operational environment”.

The FIPS 140-2 Operational Environment requirements for Security Level 1 are satisfied in the following ways:

When the Module is operated in FIPS approved mode, the environment is restricted to a single operator mode of operation (i.e., concurrent operators are explicitly excluded). The tested operating systems separate user processes into separate address spaces, where each space is logically separated from any other address space by the operating systems and the hardware on which it runs. The Module runs entirely within the address space of the calling application so it implicitly satisfies the requirement for a single user mode of operation.

Processes that are spawned by the Module are owned by the Module and are not owned by external processes/operators. Non-cryptographic processes shall not interrupt the Module during execution.

The Module software is installed in a form that protects the software and executable code from unauthorized disclosure and modification.

Cryptographic algorithm integrity tests are performed using Power-Up Self-Tests, Software Integrity Tests and Conditional Self Tests. (See Section 8. Security Rules - Security Rules)

8. Security Rules

The following rules must be followed when operating the Module in Approved mode.

1. The Module must be used as described in this document.
2. Installation of the Module is the responsibility of the Crypto Officer.
3. Before the Module can be used in Approved mode, it must be initialized as described in the "Approved Mode of Operation" section of this document.
4. Only Approved cryptographic algorithms as enumerated in the "Approved Mode of Operation" section of this document may be used.
5. The Module does not perform key generation.
6. The Module inhibits Data Output during self-tests and error states. The Data Output interface is logically disconnected from the processes performing self-tests and zeroization.
7. The zeroization process must be implemented using the appropriate API function
8. The Module is designed to satisfy the requirements of FIPS 140-2 Level 1, therefore the Module does not provide authentication mechanisms.
9. The Module conforms to the EMI/EMC requirements specified by 47 Code of Federal Regulations, Part 15, Subpart B, Unintentional Radiators, Digital Devices, Class B (i.e., for Home use) which vacuously satisfies Class A.
10. The cryptographic module fully implements the SP800-90A Section 11.3 requirements, and therefore meets the requirements of SP800-90A Section 11.3.
11. The Module conforms to requirements of IG A.5. The GCM IV is constructed internally according to Section 8.2.1 of SP800-38D. The IV fixed field has a minimum size of 32 bits which allows for at least 2^32 different names. The IV invocation field has a minimum size of 64 bits. The Module implements a counter that increments the invocation field by 1. If the Module power is lost and restored, then the calling function can set the IV to the last value used.
12. Power-up self-tests do not require any operator intervention.
13. Status information does not contain CSPs or sensitive data that if misused could lead to a compromise of the Module.
14. The Module does not support a maintenance interface or role.
15. The Module does not support manual key entry.
16. The Module does not support bypass mode.
17. The Module does not enter or output plaintext CSPs.
18. The Module does not output intermediate key values.
19. The Module enforces logical separation of all data inputs, data outputs, control inputs, and status outputs.
20. The general purpose-computing platform includes a power port.
21. Roles are implicitly assumed based upon the service requested.
22. The Module performs the following self-tests:
    - a Power up Self-Tests:
        - i Cryptographic Known Answer Tests (KAT):

1 DRBG KAT

2 SHA-1 KAT (Hashing)

3 HMAC-SHA1 KAT (Hashing)

4 HMAC-SHA256 KAT (Hashing)

5 HMAC-SHA512 KAT (Hashing)

6 AES (256-bit) KAT (encrypt) in GCM

7 AES (256-bit) KAT (decrypt) in GCM

8 AES (128-bit) KAT (encrypt) in ECB

9 AES (128-bit) KAT (decrypt) in ECB

10 AES (128-, 192-, 256-bit) KAT (generation) in CMAC

11 AES (128-, 192-, 256-bit) KAT (verification) in CMAC

12 Three-key Triple-DES KAT (encrypt) in ECB mode

13 Three-key Triple-DES KAT (decrypt) in ECB mode

14 RSA 2048-bit with SHA-256 KAT (signature generation)

15 RSA 2048-bit with SHA-256 KAT (signature verification)

16 ECDSA P-224 with SHA-512 Pairwise Consistency Test (sign/verify)

17 DSA 2048-bit with SHA-384 Pairwise Consistency Test (sign/verify)

18 SP800-108 KBKDF with HMAC-SHA256 KAT in CTR mode

19 SP800-132 PBKDF2 with HMAC-SHA256 KAT

ii Software Integrity Test: HMAC-SHA1

b Conditional Self Tests:

i Continuous Random Number Generator Tests: RNG and DRBG Tests

ii Manual Key Entry Test: N/A

iii Bypass Test: N/A

iv Pairwise Consistency Test: N/A

9. Physical Security Policy

The Module is a software module and the physical security requirements are not applicable.

Table 10: Inspection/Testing of Physical Security Mechanisms

Physical Security Mechanisms	Recommended Frequency of Inspection/Test	Inspection/Test Guidance Details
N/A	N/A	N/A

10. Mitigation of Other Attacks Policy

The Module is not designed to mitigate any other attacks.

Table 11: Mitigation of Other Attacks

Other Attacks	Mitigation Mechanism	Specific Limitations
N/A	N/A	N/A

11. Definitions and Acronyms

The following paragraphs define the acronyms used in this document.

AES. Advanced Encryption Standard secret key algorithm. See [FIPS-197].
API. Application Programming Interface
CBC. Cipher Block Chaining mode
CFB. Cipher Feedback mode
CSP. Critical Security Parameters
DES. Data Encryption Standard. See [FIPS-46-3].
DRBG. Deterministic Random Bit Generator.
DSS. Digital Signature Standard. See [FIPS-186-4]
ECB. Electronic Codebook mode
EMI. Electromagnetic Interference
EMC. Electromagnetic Compatibility
FIPS. Federal Information Processing Standards of NIST.
IV. Initialization Vector
KDF. Key Derivation Function See [SP800-108, SP800-132]
NIST. National Institute of Standards and Technologies.
OFB. Output Feedback mode
SHA-1. Secure Hash Algorithm revision 1. See [FIPS-180-4].

Appendix A: Critical Security Parameters and Public Keys

A.1 Private Keys

The module supports the following secret keys, private keys, and CSPs:

1. AES Secret Key (128-, 192- and 256-bit)
- Description: 128-, 192- and 256-bit AES secret keys are used in ECB, CBC, OFB, GCM, CFB1, CMAC and FF1 mode for encrypt/decrypt services
- Generation: N/A
- Establishment: N/A
- Storage: In RAM as plaintext
- Entry: N/A - the key is entered by the calling application; as per FIPS 140-2 IG 7.7 the calling application entering the key is considered as not applicable.
- Output: N/A - the key is output to the calling application; as per FIPS 140-2 IG 7.7 the module outputting the key to the calling application is considered as not applicable.
- Entity: Process
- Zeroization: Power off or actively overwritten by calling program

2. Two-key Triple-DES Secret Key (112-bit)
- Description: 112-bit Triple-DES secret keys are used in TECB, TCBC, TCFB1, TCFB8, TCFB64, and TOFB mode for decrypt services
- Generation: N/A
- Establishment: N/A
- Storage: In RAM as plaintext
- Entry: N/A - the key is entered by the calling application; as per FIPS 140-2 IG 7.7 the calling application entering the key is considered as not applicable.
- Output: N/A - the key is output to the calling application; as per FIPS 140-2 IG 7.7 the module outputting the key to the calling application is considered as not applicable.
- Entity: Process
- Zeroization: Power off or actively overwritten by calling program

3. DSA Private Key (2048-bit)
- Description: 2048-bit DSA private key used for digital signature generation
- Generation: N/A
- Establishment: N/A
- Storage: In RAM as plaintext
- Entry: N/A - the key is entered by the calling application; as per FIPS 140-2 IG 7.7 the calling application entering the key is considered as not applicable.
- Output: N/A - the key is output to the calling application; as per FIPS 140-2 IG 7.7 the module outputting the key to the calling application is considered as not applicable.
- Entity: Process
- Zeroization: Power off or actively overwritten by calling program

4. RSA Private Signature Key (2048-bit)
- Description: 2048-bit RSA private key used for digital signature generation
- Generation: N/A
- Establishment: N/A
- Storage: In RAM as plaintext
- Entry: N/A - the key is entered by the calling application; as per FIPS 140-2 IG 7.7 the calling application entering the key is considered as not applicable.
- Output: N/A - the key is output to the calling application; as per FIPS 140-2 IG 7.7 the module outputting the key to the calling application is considered as not applicable.

- Entity: Process
- Zeroization: Power off or actively overwritten by calling program

5. RSA Private Key for Key Transport (2048-bit)
- Description: 2048-bit RSA private key used for key transport
- Generation: N/A
- Establishment: N/A
- Storage: In RAM as plaintext
- Entry: N/A - the key is entered by the calling application; as per FIPS 140-2 IG 7.7 the calling application entering the key is considered as not applicable.
- Output: N/A - the key is output to the calling application; as per FIPS 140-2 IG 7.7 the module outputting the key to the calling application is considered as not applicable.
- Entity: Process
- Zeroization: Power off or actively overwritten by calling program

6. ECDSA Private Signature Key (P-224, P-256, P-384, P-521)
- Description: ECDSA (P-224, P-256, P-384, P-521) key used for digital signature generation
- Generation: N/A
- Establishment: N/A
- Storage: In RAM as plaintext
- Entry: N/A - the key is entered by the calling application; as per FIPS 140-2 IG 7.7 the calling application entering the key is considered as not applicable.
- Output: N/A - the key is output to the calling application; as per FIPS 140-2 IG 7.7 the module outputting the key to the calling application is considered as not applicable.
- Entity: Process
- Zeroization: Power off or actively overwritten by calling program

7. SP800-108 KBKDF Key Derivation Key (256-bit)
- Description: 256-bit SP800-108 KBKDF key used in CTR mode for deriving keys
- Generation: N/A
- Establishment: N/A
- Storage: In RAM as plaintext
- Entry: N/A - the key is entered by the calling application; as per FIPS 140-2 IG 7.7 the calling application entering the key is considered as not applicable.
- Output: N/A - the key is output to the calling application; as per FIPS 140-2 IG 7.7 the module outputting the key to the calling application is considered as not applicable.
- Entity: Process
- Zeroization: Power off or actively overwritten by calling program

8. SP800-108 KBKDF Internal State (256-bit)
- Description: Internal State of the SP800-108 KBKDF
- Generation: N/A
- Establishment: N/A
- Storage: In RAM as plaintext
- Entry: N/A - the key is entered by the calling application; as per FIPS 140-2 IG 7.7 the calling application entering the key is considered as not applicable.
- Output: N/A - the key is output to the calling application; as per FIPS 140-2 IG 7.7 the module outputting the key to the calling application is considered as not applicable.
- Entity: Process
- Zeroization: Power off or actively overwritten by calling program

9. ECC CDH Private Key (P-224, P-256, P-384, P-521)
- Description: ECC CDH (P-224, P-256, P-384, P-521) private key
- Generation: N/A
- Establishment: N/A
- Storage: In RAM as plaintext
- Entry: N/A - the key is entered by the calling application; as per FIPS 140-2 IG 7.7 the calling application entering the key is considered as not applicable.
- Output: N/A - the key is output to the calling application; as per FIPS 140-2 IG 7.7 the module outputting the key to the calling application is considered as not applicable.
- Entity: Process
- Zeroization: Power off or actively overwritten by calling program

10. ECC CDH Shared Secret (P-224, P-256, P-384, P-521)
- Description: ECC CDH (P-224, P-256, P-384, P-521) shared secret for the ECC CDH private key
- Generation: N/A
- Establishment: N/A
- Storage: In RAM as plaintext
- Entry: N/A - the key is entered by the calling application; as per FIPS 140-2 IG 7.7 the calling application entering the key is considered as not applicable.
- Output: N/A - the key is output to the calling application; as per FIPS 140-2 IG 7.7 the module outputting the key to the calling application is considered as not applicable.
- Entity: Process
- Zeroization: Power off or actively overwritten by calling program

11. DRBG V Value
- Description: Internal state of the DRBG: 440 bits (for SHA-256 construction) or 888 bits (for SHA-512 construction)
- Generation: N/A
- Establishment: N/A
- Storage: In RAM as plaintext
- Entry: N/A - the key is entered by the calling application; as per FIPS 140-2 IG 7.7 the calling application entering the key is considered as not applicable.
- Output: N/A
- Entity: Process
- Zeroization: Power off or actively overwritten by calling program

12. DRBG C Value
- Description: Internal state of the DRBG: 440 bits (for SHA-256 construction) or 888 bits (for SHA-512 construction)
- Generation: N/A
- Establishment: N/A
- Storage: In RAM as plaintext
- Entry: N/A - the key is entered by the calling application; as per FIPS 140-2 IG 7.7 the calling application entering the key is considered as not applicable.
- Output: N/A
- Entity: Process
- Zeroization: Power off or actively overwritten by calling program

13. HMAC Secret key (112-, 192- and 256-bit)
- Description: 112-, 192- and 256-bit HMAC secret keys are used for message authentication services
- Generation: N/A
- Establishment: N/A
- Storage: In RAM as plaintext
- Entry: N/A - the key is entered by the calling application; as per FIPS 140-2 IG 7.7 the calling application entering the key is considered as not applicable.
- Output: N/A - the key is output to the calling application; as per FIPS 140-2 IG 7.7 the module outputting the key to the calling application is considered as not applicable.
- Entity: Process
- Zeroization: Power off or actively overwritten by calling program

14. SP800-132 PBKDF2 Master Key (256-bit)
- Description: 256-bit SP800-132 PBKDF2 key using HMAC-SHA-256 for deriving keys; for use by Storage Based Applications only
- Generation: N/A
- Establishment: N/A
- Storage: In RAM as plaintext
- Entry: N/A - the key is entered by the calling application; as per FIPS 140-2 IG 7.7 the calling application entering the key is considered as not applicable.
- Output: N/A - the key is output to the calling application; as per FIPS 140-2 IG 7.7 the module outputting the key to the calling application is considered as not applicable.
- Entity: Process
- Zeroization: Power off or actively overwritten by calling program

15. SP800-132 PBKDF2 Internal State (256-bit)
- Description: Internal State of the SP800-132 PBKDF2; for use by Storage Based Applications only
- Generation: N/A
- Establishment: N/A
- Storage: In RAM as plaintext
- Entry: N/A - the key is entered by the calling application; as per FIPS 140-2 IG 7.7 the calling application entering the key is considered as not applicable.
- Output: N/A - the key is output to the calling application; as per FIPS 140-2 IG 7.7 the module outputting the key to the calling application is considered as not applicable.
- Entity: Process
- Zeroization: Power off or actively overwritten by calling program

16. Password (64-bit)
- Description: 64-bit Password used to derive keying material for SP800-132 PBKDF2; for use by Storage Based Applications only
- Generation: N/A
- Establishment: N/A
- Storage: In RAM as plaintext
- Entry: N/A - the key is entered by the calling application; as per FIPS 140-2 IG 7.7 the calling application entering the key is considered as not applicable.
- Output: N/A - the key is output to the calling application; as per FIPS 140-2 IG 7.7 the module outputting the key to the calling application is considered as not applicable.
- Entity: Process
- Zeroization: Power off or actively overwritten by calling program

17. AES CMAC Key (128-, 192- and 256-bit)
- Description: 128-, 192- and 256-bit AES secret keys are used in CMAC mode for generation/verification services
- Generation: N/A
- Establishment: N/A
- Storage: In RAM as plaintext
- Entry: N/A - the key is entered by the calling application; as per FIPS 140-2 IG 7.7 the calling application entering the key is considered as not applicable.
- Output: N/A - the key is output to the calling application; as per FIPS 140-2 IG 7.7 the module outputting the key to the calling application is considered as not applicable.
- Entity: Process
- Zeroization: Power off or actively overwritten by calling program

18. Three-key Triple-DES Secret Key (168-bit)
- Description: 168-bit Triple-DES secret keys are used in TECB, TCBC, TOFB, TCFB1, TCFB8, TCFB64, and TOFB mode for encrypt and decrypt services
- Generation: N/A
- Establishment: N/A
- Storage: In RAM as plaintext
- Entry: N/A - the key is entered by the calling application; as per FIPS 140-2 IG 7.7 the calling application entering the key is considered as not applicable.
- Output: N/A - the key is output to the calling application; as per FIPS 140-2 IG 7.7 the module outputting the key to the calling application is considered as not applicable.
- Entity: Process
- Zeroization: Power off or actively overwritten by calling program

A.2 Public Keys

The module supports the following public keys:

1. DSA Public Key (1024- or 2048-bit)
- Description: 1024- or 2048-bit DSA public key used for digital signature verification
- Generation: N/A
- Establishment: N/A
- Storage: In RAM as plaintext
- Entry: N/A - the key is entered by the calling application; as per FIPS 140-2 IG 7.7 the calling application entering the key is considered as not applicable.
- Output: N/A - the key is output to the calling application; as per FIPS 140-2 IG 7.7 the module outputting the key to the calling application is considered as not applicable.
- Entity: Process

2. RSA Public Signature Key (2048-bit)
- Description: 2048-bit RSA public key used for digital signature verification
- Generation: N/A
- Establishment: N/A
- Storage: In RAM as plaintext
- Entry: N/A - the key is entered by the calling application; as per FIPS 140-2 IG 7.7 the calling application entering the key is considered as not applicable.
- Output: N/A - the key is output to the calling application; as per FIPS 140-2 IG 7.7 the module outputting the key to the calling application is considered as not applicable.
- Entity: Process

3. RSA Public Key for Key Transport (2048-bit)
- Description/Usage: 2048-bit RSA public key used for key transport
- Generation: N/A
- Establishment: N/A
- Storage: In RAM as plaintext
- Entry: N/A - the key is entered by the calling application; as per FIPS 140-2 IG 7.7 the calling application entering the key is considered as not applicable.
- Output: N/A - the key is output to the calling application; as per FIPS 140-2 IG 7.7 the module outputting the key to the calling application is considered as not applicable.
- Entity: Process

4. ECDSA Public Signature Key (P-224, P-256, P-384, P-521)
- Description: ECDSA (P-224, P-256, P-384, P-521) public key used for digital signature verification
- Generation: N/A
- Establishment: N/A
- Storage: In RAM as plaintext
- Entry: N/A - the key is entered by the calling application; as per FIPS 140-2 IG 7.7 the calling application entering the key is considered as not applicable.
- Output: N/A - the key is output to the calling application; as per FIPS 140-2 IG 7.7 the module outputting the key to the calling application is considered as not applicable.
- Entity: Process

5. ECC CDH Public Key (P-224, P-256, P-384, P-521)
- Description: ECC CDH (P-224, P-256, P-384, P-521) public key
- Generation: N/A
- Establishment: N/A
- Storage: In RAM as plaintext
- Entry: N/A - the key is entered by the calling application; as per FIPS 140-2 IG 7.7 the calling application entering the key is considered as not applicable.
- Output: N/A - the key is output to the calling application; as per FIPS 140-2 IG 7.7 the module outputting the key to the calling application is considered as not applicable.
- Entity: Process