DINAMO Networks, Inc.

DINAMO CD, XP, and ST Hardware Security Modules

Hardware Models: DINAMO CD, DINAMO XP, and DINAMO ST
Firmware Version: 5.0.8.0

FIPS 140-2 Non-Proprietary Security Policy

FIPS Security Level: 3
Document Version: 0.10

`

Prepared for:

DINAMO Networks, Inc.
United Nations Avenue, 14401
ED. TARUMA
Sao Paulo

Phone: +55 11 3304 3120
www.dinamonetworks.com

Prepared by:

Corsec Security, Inc.
13921 Park Center Road, Suite 460
Herndon, VA 20171
United States of America

Phone: +1 703 267 6050
www.corsec.com

Table of Contents

List of Tables

List of Figures

1. Introduction

1.1 Purpose

This is a non-proprietary Cryptographic Module Security Policy for the DINAMO CD, XP, and ST Hardware Security Modules (hardware models: DINAMO CD, DINAMO XP, and DINAMO ST; firmware version 5.0.8.0) by DINAMO Networks, Inc. (hereafter referred to as "DINAMO"). This Security Policy describes how the DINAMO CD, XP, and ST Hardware Security Modules meets the security requirements of Federal Information Processing Standards (FIPS) Publication 140-2, which details the U.S.[1] and Canadian government requirements for cryptographic modules. More information about the FIPS 140-2 standard and validation program is available on the Cryptographic Module Validation Program (CMVP) website, which is maintained by the National Institute of Standards and Technology (NIST) and the Canadian Centre for Cyber Security (CCCS).

This document also describes how to run the module in a secure FIPS-Approved mode of operation. This policy was prepared as part of the Level 3 FIPS 140-2 validation of the module. The DINAMO CD, XP, and ST Hardware Security Modules are referred to in this document as the HSMs, module, or modules. The DINAMO CD, XP, and ST Hardware Security Modules are also referred to individually as the DINAMO CD, DINAMO XP, and the DINAMO ST.

1.2 References

This document deals only with operations and capabilities of the module in the technical terms of a FIPS 140-2 cryptographic module security policy. More information is available on the module from the following sources:

- The DINAMO website (https://www.dinamonetworks.com/en/dinamo/) contains information on the full line of products from DINAMO.

- The search page on the CMVP website (https://csrc.nist.gov/Projects/cryptographic-module-validation-program/Validated-Modules/Search) can be used to locate and obtain vendor contact information for technical or sales-related questions about the module.

1.3 Document Organization

The Security Policy document is organized into two primary sections. Section 2 provides an overview of the validated module. This includes a general description of the capabilities and the use of cryptography, as well as a presentation of the validation level achieved in each applicable functional area of the FIPS standard. It also provides high-level descriptions of how the module meets FIPS requirements in each functional area. Section 3 documents the guidance needed for the secure use of the module, including initial setup instructions and management methods and applicable usages policies.

This Security Policy and the other validation submission documentation were produced by Corsec Security, Inc. under contract to DINAMO. With the exception of this Non-Proprietary Security Policy, the FIPS 140-2 Submission Package is proprietary to DINAMO and is releasable only under appropriate non-disclosure agreements. For access to these documents, please contact DINAMO.

[1] U.S. – United States

2. DINAMO CD, XP, and ST HSMs

2.1 Overview

DINAMO has been providing solutions to the Information Security segment for over fifteen years. The family of DINAMO HSMs reduce risk and operation costs by centralizing enterprise cryptographic key management.

DINAMO HSMs are network-attached devices that offer a secure environment for the storage and lifecycle management of cryptographic keys, as well as offering cryptographic services such as encryption, digital signatures, key generation, and authentication.

DINAMO HSMs are offered in three models: DINAMO CD, DINAMO XP, and DINAMO ST shown in Figure 1, Figure 2, and Figure 3 respectively. While differing in processing capability, all three models run the same DINAMO HSM firmware and provide the same overall architecture and cryptographic functionality as well as user key partition separation and protection against tampering. In addition, the DINAMO ST offers a redundant power supply.

Figure 1 – DINAMO CD

Figure 2 – DINAMO XP

Figure 3 – DINAMO ST

The HSMs are 1U[2] rack-mounted appliances with two 10/100/1000 Mbps[3] Ethernet management interfaces and an internal smart card reader. Management of the HSMs is accomplished via the following methods:

[2] U – Rack Unit
[3] Mbps – Megabits per second

- Local management console, which is accessible via direct attachment to the HSM's USB[4] keyboard port. This interface is accessible only to Crypto Officer operators and is used primarily for initial setup and configuration of the module. This requires smart cards and the establishment of a Master Key using split knowledge procedures.

- Remote Console, which is accessible remotely via a cleartext session or TLS[5] v1.2 over Ethernet management ports. Certain services require a TLS v1.2 session (e.g., import/export of keys). These services will be blocked if attempted over a cleartext session. The services that require a TLS v1.2 session are indicated as such in Table 7 and Table 8. The Remote Console is accessible to all operators and is used for appliance management (Crypto Officers) and obtaining key management and cryptographic services (all operators). This interface requires a client software package and uses the HSM's native API[6].

- HTTPS Console, which is accessible remotely via HTTPS over the Ethernet interface and offers the same services as the Remote Console, with TLS v1.2 mandatory. The HTTPS Console is accessible to all operators and is used for appliance management (Crypto Officers) and obtaining key management and cryptographic services (all operators).

Standard APIs, including MS[7] Crypto API, Java JCA[8]/JCE[9], PKCS[10]#11, and Native API are also available for integration with the HSM. Additionally, replication is provided between modules.

The DINAMO CD, XP, and ST Hardware Security Modules are validated at the FIPS 140-2 section levels shown in Table 1.

Table 1 – Security Level per FIPS 140-2 Section

Section	Section Title	Level
1	Cryptographic Module Specification	3
2	Cryptographic Module Ports and Interfaces	3
3	Roles, Services, and Authentication	3
4	Finite State Model	3
5	Physical Security	3
6	Operational Environment	N/A[11]
7	Cryptographic Key Management	3
8	EMI/EMC[12]	3
9	Self-tests	3
10	Design Assurance	3
11	Mitigation of Other Attacks	3

[4] USB – Universal Serial Bus
[5] TLS – Transport Layer Security
[6] API – Application Programming Interface
[7] MS – Microsoft
[8] JCA – Java Cryptography Architecture
[9] JCE – Java Cryptography Extension
[10] PKCS – Public Key Cryptography Standards
[11] N/A – Not Applicable
[12] EMI/EMC – Electromagnetic Interference / Electromagnetic Compatibility

2.2 Module Specification

The HSM is a hardware cryptographic module with a multiple-chip standalone embodiment. The overall security level of the module is 3. The cryptographic boundary is defined by the physical enclosure of the HSM and includes all internal hardware as well as the HSM (Version 5.0.8.0) firmware.

The main hardware components consist of processors, memories, SSD[13], smart card reader, border breach supervisory circuit and associated battery, power supplies, fans, and the enclosure containing all of these components.

The cryptographic boundary for the DINAMO CD, DINAMO XP, and DINAMO ST is depicted in the block diagram in Figure 4.

The following undefined acronyms appear in Figure 4:

- CPU – Central Processing Unit
- LED – Light Emitting Diode
- VGA – Video Graphics Array

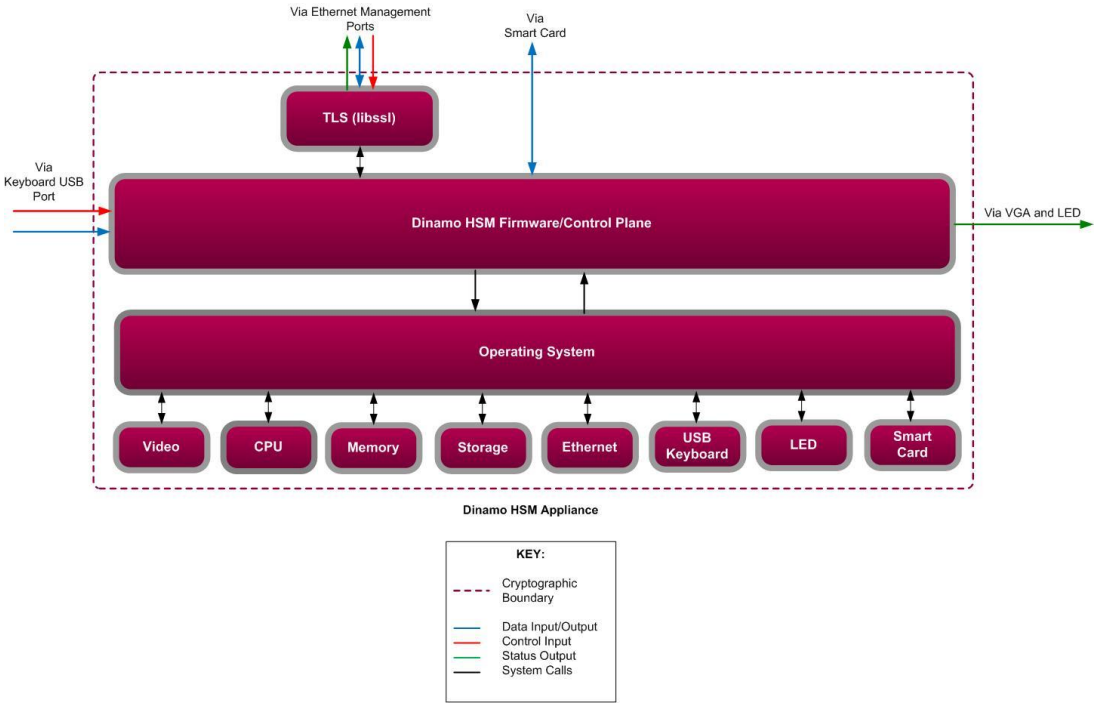

Figure 4 – DINAMO CD, DINAMO XP, and DINAMO ST Block Diagram

The DINAMO CD, DINAMO XP, and DINAMO ST include the cryptographic algorithm providers listed in Table 2.

[13] SSD – Solid State Drive

Table 2 – Cryptographic Algorithm Providers

Certificate Number	Implementation Name	Version	Use
C1902	DINAMO Hardware Security Module Cryptographic Library	1.0	Firmware-based cryptographic primitives (based on OpenSSL 1.1.1a)
C1905	DINAMO Hardware Security Module KBKDF[14] and RSA[15] KeyGen	1.0	NIST SP[16] 800-108 KBKDF implementation and an RSA Key Generation implementation
C1906	DINAMO Hardware Security Module TLS KDF[17]	1.0	TLS v1.2 KDF implementations (based on OpenSSL 1.1.1a)

The module implements the FIPS-Approved algorithms listed in Table 3 below:

Table 3 – FIPS-Approved Algorithm Implementations

Certificate Number	Algorithm	Standard	Mode / Method	Key Lengths / Curves / Moduli	Use
C1902	AES[18]	FIPS PUB[19] 197 NIST SP 800-38A	CBC[20], CTR[21], ECB[22]	128, 192, 256	encryption/decryption
		NIST SP 800-38B	CMAC[23]	128, 192, 256	generation/verification
		NIST SP 800 38D	GCM[24]	128, 192, 256	encryption/decryption
Vendor Affirmed	CKG[25]	NIST SP 800-133rev1	-	-	symmetric key generation *Symmetric keys and generated seeds are produced using unmodified output from the Approved DRBG.*
C1902	CVL	NIST SP 800-135rev1	ANS X9.63-2001	-	key derivation *No part of the ANS X9.63-2001 protocol, other than the KDF, has been tested by the CAVP[26] and CMVP.*

[14] KBKDF – Key-based Key Derivation Function
[15] RSA – Rivest Shamir Adleman
[16] SP – Special Publication
[17] KDF – Key Derivation Function
[18] AES – Advance Encryption Standard
[19] PUB – Publication
[20] CBC – Cipher Block Chaining
[21] CTR – Counter
[22] ECB – Electronic Codebook
[23] CMAC – Cipher-Based Message Authentication Code
[24] GCM – Galois Counter Mode
[25] CKG – Cryptographic Key Generation
[26] CAVP – Cryptographic Algorithm Validation Program

Certificate Number	Algorithm	Standard	Mode / Method	Key Lengths / Curves / Moduli	Use
C1906	CVL	NIST SP 800-135rev1	TLS v1.2	-	key derivation *No part of the TLS protocol, other than the KDF, has been tested by the CAVP[27] and CMVP.*
C1902	DRBG[28]	NIST SP 800-90Arev1	CTR-based	256-bit AES	deterministic random bit generation
C1902	ECDSA[29]	FIPS PUB 186-4	PKG[30]	P-224, P-256, P-384, P-521	key pair generation
			PKV[31]	P-192, P-224, P-256, P-384, P-521	key pair verification
			SigGen	P-224, P-256, P-384, P-521	digital signature generation
			SigVer	P-192, P-224, P-256, P-384, P-521	digital signature verification
C1902	HMAC[32]	FIPS PUB 198-1	SHA2[33]-224, SHA2-256, SHA2-384, SHA2-512, SHA3-224, SHA3-256, SHA3-384, SHA3-512	SHA2-224, SHA2-256, SHA2-384, SHA2-512, SHA3-224, SHA3-256, SHA3-384, SHA3-512	message authentication
Vendor Affirmed	KAS-SSC[34]	NIST SP 800-56Arev3	ECDH[35]	P-224, P-256, P-384, P-521	Key Agreement Scheme – shared secret computation per SP 800-56Arev3 and Key Derivation per SP 800-135rev1 (Certs. #C1902 and #C1906)
C1905	KBKDF	NIST SP 800-108	Counter mode	HMAC SHA2-256, HMAC SHA2-512	key derivation
C1902	KTS[36]	NIST SP 800 38D	AES	128, 192, 256	*This implementation has been tested for its compliance with AES GCM and this mode of AES is used for key wrapping.*
Vendor Affirmed	PBKDF2[37]	NIST SP 800-132	Option 1a with HMAC SHA2-256	-	password-based key derivation
C1905	RSA	FIPS PUB 186-4	-	2048, 3072	key pair generation
C1902	RSA	FIPS PUB 186-4	ANSI X9.31 PKCS[38]1.5 PSS[39]	2048, 3072 (SHA2-224, SHA2-256, SHA2-384, SHA2-512)	digital signature generation
			ANSI X9.31 PKCS 1.5 PSS	2048, 3072 (SHA-1, SHA2-224, SHA2-256, SHA2-384, SHA2-512)	digital signature verification
C1902	SHS[40]	FIPS PUB 180-4	SHA-1, SHA2-224, SHA2-256, SHA2-384, SHA2-512	-	message digest
C1902	SHA3	FIPS PUB 202	SHA3-224, SHA3-256, SHA3-384, SHA3-512	-	message digest
C1902	Triple-DES[41]	NIST SP 800-67rev2	TCBC, TECB	Keying option 1	decryption

While the module includes CAVP-tested implementations of Triple-DES Keying option 1 (CBC, ECB) encryption and Triple-DES CMAC generation/verification (#C1902), these algorithms are not used for any security-relevant functions.

The vendor affirms the following cryptographic security methods:

- Password-based key derivation – The module performs PBKDF2 in compliance with *NIST SP 800-132* using option 1(a) in Section 5.4 to derive the following keys: AES KEK[42], Triple-DES Decryption Key, and Backup Key. The PBKDF2 is used for storage applications only. HMAC SHA-256 is used as the approved PRF[43]. The iteration count is 16384 iterations. The length of the salt is 512 bits, and it is generated by the FIPS-Approved DRBG. Please refer to Section 3.2.3 for Crypto Officer guidance specific to this function.

- Symmetric key generation – Per *NIST SP 800-133*, the module uses the FIPS-Approved CTR-based DRBG specified in *NIST SP 800-90Arev 1* to generate cryptographic keys. The resulting symmetric key or generated seed is an unmodified output from the DRBG. The module's DRBG is seeded via /dev/random, a non-deterministic random number generator (NDRNG) internal to the module.

- Key agreement scheme (shared secret computation) – The module implements an ECC CDH shared secret computation for its ECDH key agreement scheme. The shared secret computation is compliant with section 5.7.1.2 of *NIST SP 800-56Arev3*. This compliance claim follows scenario X1 of section D.8 of the *Implementation Guidance for FIPS PUB 140-2 and the CMVP*. This primitive is used by the Full Unified Model, Ephemeral Unified Model, One-Pass Unified Model, One-Pass Diffie-Hellman, and Static Unified Model schemes found in section 6 of that recommendation.

  Note that vendor affirmation of the KAS-SSC with NIST-recommended elliptic curves is included above in compliance with section A.2 of the Implementation Guidance for FIPS PUB 140-2 and the CMVP to support the allowed use of non-NIST-recommended elliptic curves in the ECDSA signature algorithm and the ECDH key agreement scheme in the approved mode of operation. The non-NIST-recommended curves implemented by the module are referenced in Table 4.

The module implements the non-Approved but allowed algorithms shown in Table 4.

[27] CAVP – Cryptographic Algorithm Validation Program
[28] DBRG – Deterministic Random Bit Generator
[29] ECDSA – Elliptic Curve Digital Signature Algorithm
[30] PKG – Public Key (Q) Generation
[31] PKV – Public Key (Q) Validation
[32] HMAC – (keyed-) Hashed Message Authentication Code
[33] SHA – Secure Hash Algorithm
[34] KAS-SSC – Key Agreement Scheme - Shared Secret Computation
[35] ECDH – Elliptic Curve Diffie-Hellman
[36] KTS – Key Transport
[37] PBKDF2 – Password-based Key Derivation Function 2
[38] PKCS – Public Key Cryptography Standard
[39] PSS – Probabilistic Signature Scheme
[40] SHS – Secure Hash Standard
[41] DES – Data Encryption Standard
[42] KEK – Key Encryption Key
[43] PRF – Pseudo-Random Function

Table 4 – Allowed Algorithm Implementations

Algorithm	Caveat	Use
EC Diffie-Hellman with non-NIST-recommended curves	key establishment methodology provides between 112 and 256 bits of encryption strength as follows: • BrainpoolP224r1 (112-bits) • BrainpoolP256r1 (128 bits) • BrainpoolP320r1 (160 bits) • BrainpoolP384r1 (192 bits) • BrainpoolP512r1 (256 bits)	Key agreement
ECDSA with non-NIST-recommended curves	key establishment methodology provides between 112 and 256 bits of encryption strength as follows: • BrainpoolP224r1 (112-bits) • BrainpoolP256r1 (128 bits) • BrainpoolP320r1 (160 bits) • BrainpoolP384r1 (192 bits) • BrainpoolP512r1 (256 bits)	Key pair generation, digital signature generation, digital signature verification
NDRNG	-	Seeding for the DRBG
RSA	Key establishment methodology provides between 112 and 128 bits of encryption strength	Key encapsulation/establishment - key transport in TLSv1.2 (NIST SP 800-56Brev1, section 9.2.3) Key transport (PKCS#1 v2.2 RSAES_OAEP)
SHA-1	Legacy-use	ECDSA and RSA signature verification
2-key Triple-DES	Legacy-use	Decryption

2.3 Module Ports and Interfaces

The module's design separates the physical ports and interfaces into four logically distinct and isolated categories. They are:

- Data Input Interface
- Data Output Interface
- Control Input Interface
- Status Output Interface

The DINAMO CD contains the physical ports and interfaces shown in Figure 5 and Figure 6.

Figure 5 – DINAMO CD Ports and Interfaces (Front)

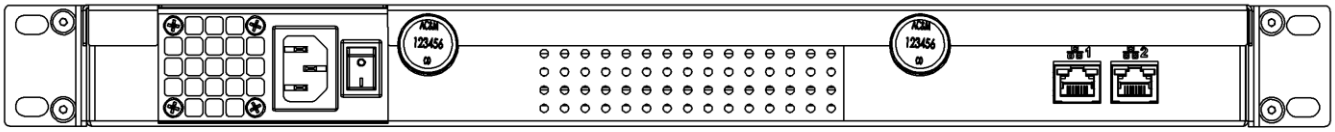

Figure 6 – DINAMO CD Ports and Interfaces (Rear)

The DINAMO XP contains the physical ports and interfaces shown in Figure 7 and Figure 8 below.

FIGURE 7 – DINAMO XP Ports and Interfaces (FRONT)

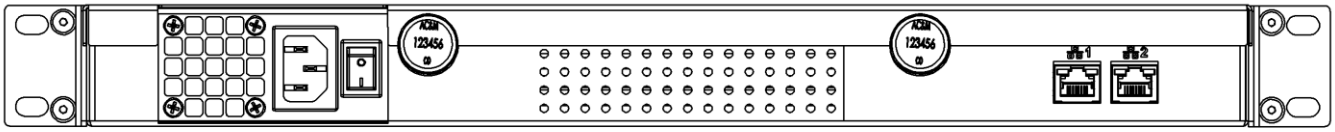

FIGURE 8 – DINAMO XP Ports and Interfaces (REAR)

The DINAMO ST contains the physical ports and interfaces shown in and Figure 9 and Figure 10 below.

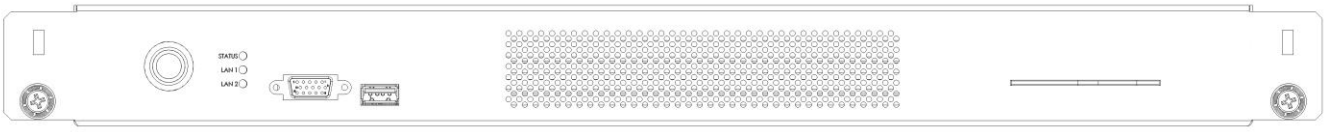

FIGURE 9 – DINAMO ST ports and Interfaces (FRONT)

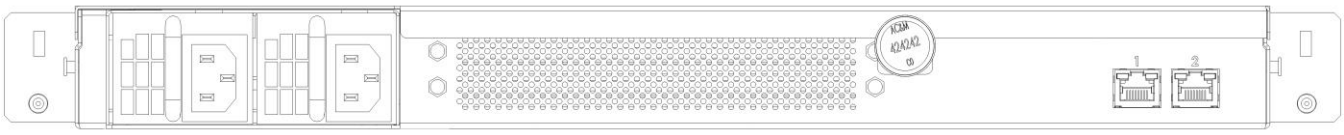

FIGURE 10 – DINAMO ST Ports and Interfaces (REAR)

Table 5 provides the mapping from the physical interfaces to logical interfaces as defined by FIPS 140-2 for the DINAMO CD and DINAMO XP.

Table 5 – FIPS 140-2 Logical Interface Mappings for the DINAMO CD and DINAMO XP

Physical Port/Interface	Quantity	Description	FIPS 140-2 Logical Interface
Front Panel			
Power Button with Power LED	1	Power status indicator: • Solid blue = System on • Off = No power present	• Control Input • Status Output
Network Port LED - LAN[44] 1	1	Network Port LAN 1 status indicator: • Solid green = Link signal present • Flashing green = Link signal present and network port activity • Off = No link signal on port	• Status Output
Network Port LED - LAN 2	1	Network Port LAN 2 status indicator: • Solid green = Link signal present • Flashing green = Link signal present and network port activity • Off = No link signal on port	• Status Output
Smart Card Reader Port	1	Smart card slot	• Data Input • Data output
USB Keyboard Port	1	USB Keyboard interface	• Data Input • Control Input
VGA[45] Connector Port	1	Analog video output port (DE-15)	• Status Output
Rear Panel			
RJ-45 Ethernet 10/100/1000 Mbps LAN connector	2	Interface to Remote Console and HTTPS Console for cryptographic services	• Data Input • Data Output • Control Input • Status Output
Power connector	1	Power connector	• Power Input
Network Port LED - LAN 1	1	Network Port LAN 1 status indicator: • Solid green = Link signal present • Flashing green = Link signal present and network port activity ○ Off = No link signal on port	• Status Output
Network Port LED - LAN 2	1	Network Port LAN 2 status indicator: • Solid green = Link signal present • Flashing green = Link signal present and network port activity ○ Off = No link signal on port	• Status Output

[44] LAN – Local Area Network
[45] VGA – Video Graphics Array

Table 6 provides the mapping from the physical interfaces to logical interfaces as defined by FIPS 140-2 for the DINAMO ST.

TABLE 6 – FIPS 140-2 Logical Interface Mappings for the DINAMO ST

Physical Port/Interface	Quantity	Description	FIPS 140-2 Logical Interface
Front Panel			
Power Button with Power LED	1	Power status indicator: • Solid blue = System on • Off = No power present	• Control Input • Status Output
Power Status LED	1	Power status indicator: • Off = Both source modules are powered on and operating • Flashing green = only one of the source modules is operating	• Status Output
Network Port LED - LAN 1	1	Network Port LAN 1 status indicator: • Solid green = Link signal present • Flashing green = Link signal present and network port activity • Off = No link signal on port	• Status Output
Network Port LED - LAN 2	1	Network Port LAN 2 status indicator: • Solid green = Link signal present • Flashing green = Link signal present and network port activity • Off = No link signal on port	• Status Output
Smart Card Reader Port	1	Smart card slot	• Data Input • Data Output
USB Keyboard Port	1	USB Keyboard interface	• Data Input • Control Input
VGA Connector Port	1	Analog video output port	• Status Output
Rear Panel			
RJ-45 Ethernet 10/100/1000 Mbps LAN connector	2	Interface to Remote Console and HTTPS Console for cryptographic services	• Data Input • Data Output • Control Input • Status Output
Power connector	2	Power connector	• Power Input

Physical Port/Interface	Quantity	Description	FIPS 140-2 Logical Interface
Network Port LED - LAN 1	1	Network Port LAN 1 status indicator: • Solid green = Link signal present • Flashing green = Link signal present and network port activity ○ Off = No link signal on port	• Status Output
Network Port LED - LAN 2	1	Network Port LAN 2 status indicator: • Solid green = Link signal present • Flashing green = Link signal present and network port activity ○ Off = No link signal on port	• Status Output

2.4 Roles, Services, and Authentication

The sections below describe the module's roles and services and define any authentication methods employed.

2.4.1 Authorized Roles

The module supports two roles that operators may assume:

- Crypto Officer (CO) role – The CO is responsible for initializing the module for first use. The CO has all permissions over the module and access to all services provided over both the local management console and Remote Console. The CO has its own cryptographic key partition in which to store keys. The CO also can give Users specific system permissions that allow them to perform limited management functionality (including creating and removing users, listing users, accessing log records, and creating and restoring backups). This is done by enabling these system permissions in the User's account using the Remote Console **Create** or **Attributes** menu. A minimum of two COs, each with a smart card and PIN, are required to initialize the module.

- User role – The User creates, removes, imports, exports, performs cryptographic services with, and grants permissions to keys in its own user partition. The User does not manage the module unless given specific system permissions by the CO as described above. The User accesses the module only via the Remote Console.

The module implements two types of authentication:

- Local management console authentication - At the local management console, the module uses identity-based two-factor authentication to authenticate operators. Each operator must possess a smart card and have knowledge of the associated smart card PIN. Only COs authenticate to the local management console. A minimum of two COs, each with their own smart card and PIN must successfully authenticate to the module before services are provided from the local management console.

- Remote Console and HTTPS Console authentication - At the Remote Console and HTTPS Console, the module implements identity-based authentication using username and password to individually identify

each operator and explicitly select the role assigned to that operator. The Remote Console is enabled only after smart card operator authentication at the local management console, after services are enabled.

A crypto officer over the Remote Console and HTTPS Console might not necessarily have smart card access.

2.4.2 Strength of Authentication Mechanisms

The strength of the authentication mechanism is such that for each attempt to use the authentication mechanism, the probability shall be less than one in 1,000,000 that a random attempt will succeed or a false acceptance will occur. Details are provided below for both the local management console and Remote Console authentication:

Local management console authentication:
The smart card PIN has a length of eight (8) digits; thus, the probability that a random PIN is correct is 1 in 10^8 = 1: 100, 000,000.

The smart card allows six wrong PIN attempts, after which the protection circuit is triggered and the card is permanently locked, preventing any further use. If the correct PIN is entered before the card is locked, the failed retry count is reset. In case of multiple attempts, the process will be interrupted on the seventh attempt. The probability of one of these six attempts succeeding is 6 out of 100,000,000 or about 1 out of 16,666,666. This is less than one in 100,000, as required by FIPS 140-2.

Remote Console and HTTPS Console authentication:
Operators authenticate to the Remote Console and HTTPS Console of the module with a username and password. Each password is a minimum of 8 characters, which is enforced by the module. Each password can contain any combination of upper- and lower-case letters [A-z, a-z] and numbers [0-9]. Each character of the 8-character password could be 1 of 62 printable ASCII[46] characters, providing for a password strength of (1/62^8 =) 1 in 218,340,105,584,896. This meets the 1 in 1,000,000 requirement.

The module allows for seven consecutive failed authentication attempts at the Remote Console or HTTPS Console before an operator (CO or User) is blocked and can no longer authenticate until the operator is unblocked by a CO via the Remote Console. Hence at most seven password attempts can be made in a one-minute period. Therefore, the probability that a random attempt will succeed or a false acceptance will occur in one minute is:
1: (62^8 possible passwords / 7 passwords per minute)
1: 31,191,443,654,985

This is less than one in 100,000, as required by FIPS 140-2.

2.4.3 Operator Services

Descriptions of the services available to the CO role and User role are provided in Table 7 and Table 8 below. Please note that the keys and Critical Security Parameters (CSPs) listed in Table 7 and Table 8 indicate the type of access required using the following notation:

- R – Read: The CSP is read.
- W – Write: The CSP is established, generated, modified, or zeroized.

[46] ASCII – American Standard Code for Information Interchange

- X – Execute: The CSP is used within an Approved or Allowed security function or authentication mechanism.

Table 7 – Operator Services via the Local Management Console

Service	Operator		Description	Input	Output	CSP and Type of Access
	CO	User				
Initialize module	✓		Perform module Initialization (at first boot from factory the Master Key is created within the module and its components exported to smart cards)	Command and parameters	Command response; status output	CO PINs – R/W/X Smart card PINs – R/W/X Master Key components – R/W/X Master Key – R/W/X Replication TLS-PSK Key – W Data Protection Key – W AES GCM IV[47] – W/X DRBG Seed – R/W/X Entropy Input String – R/X DRBG 'V' Value – R/W/X DRBG Key Value – R/W/X
Start service or Stop service	✓		Enable or disable module services available through the Remote Console and HTTPS Console	Command	Status output	CO PINs – R/X Smart card PINs – R/X
Shutdown	✓		Shutdown module	Command	Status output	All ephemeral keys/CSPs – W CO PINs – R/X Smart card PINs – R/X
Reboot	✓		Reboot module	Command	Command response; status output	All ephemeral keys/CSPs – W CO PINs – R/X Smart card PINs – R/X
Configure network parameters	✓		Configure network parameters	Command and parameters	Command response; status output	CO PINs – R/X Smart card PINs – R/X
Perform self-tests on demand	✓		Perform on-demand self-tests	Command	Status output	CO PINs – R/X Smart card PINs – R/X
Zeroize keys	✓		Zeroize keys and CSPs via Reboot, Shutdown, or Reset HSM Database commands	Command	Command response; Status output	All ephemeral keys/CSPs – W
Reset HSM Database	✓		Return module to factory state	Command	Command response; status output	Smart card PINs – R/X CO PINs – R/X All ephemeral and persistent keys/CSPs – W

47 IV – Initialization Vector

Table 8 – Operator Services via the Remote Console and HTTPS Console

Service	Operator		Description	Input	Output	CSP and Type of Access
	CO	User				
Show status	✓		Display the current mode of the module	Command	Status output	None
Manage users	✓	✓*	List users; create or remove a user (removing a user deletes all keys and CSPs in the user's partition) Creating a user requires TLS v1.2 session to Remote Console	Command and parameters	Command response; status output	CO Password – R/W User Password – R/W All persistent keys and CSPs in partition of removed user – W
View logs	✓	✓*	View module log data	Command	Command response; status output	None
Generate AES key	✓	✓	Generate and return an AES key Requires TLS v1.2 session to Remote Console	Command and parameters	AES key, status output	AES Key – W AES GCM IV – W/X Data Protection Key – R/X
Generate asymmetric key pair	✓	✓	Generate and return the specified type of asymmetric key pair (RSA or ECDSA) Requires TLS v1.2 session to Remote Console	Command and parameters	Key, status output	RSA Public Key – W RSA Private Key – W ECDSA Public Key – W ECDSA Private Key – W Data Protection Key – R/X
Destroy key	✓	✓	Deletes a cryptographic key from a user or CO partition	Key id	Status output	Key associated with Key id – R/W Data Protection Key – R/X
Perform symmetric encryption	✓	✓	Encrypt plaintext data using specified key id Requires TLS v1.2 session to Remote Console	Command, parameters, and plaintext	Ciphertext, status output	AES Key – R/X Data Protection Key – R/X
Perform symmetric decryption	✓	✓	Decrypt ciphertext using specified key id	Command, parameters, and ciphertext	Plaintext, status output	AES Key – R/X Data Protection Key – R/X

Service	Operator		Description	Input	Output	CSP and Type of Access
	CO	User				
Generate Signature	✓	✓	Generate and return a digital signature for supplied message using specified key id	Command, parameters, and message	Digital signature, status output	RSA Private Key – R/X ECDSA Private Key – R/X Data Protection Key – R/X
Verify Signature	✓	✓	Verify a digital signature on supplied message using specified key id	Command, parameters, and message	Command response; status output	RSA Public Key – R/X ECDSA Public Key – R/X Data Protection Key – R/X
Generate Hash	✓	✓	Generate and return hash using specified hash type	Command, parameters, and message	Hash, status output	None
Generate keyed hash (HMAC)	✓	✓	Generate and return message authentication code using specified HMAC type	Command, parameters, and message	Hash, status output	HMAC Key – R/X Data Protection Key – R/X
Import key	✓	✓	Import certificates and keys using specified KEK or RSA key pair and import method Requires TLS v1.2 session to Remote Console	Command, parameters, and key material	Status output	AES KEK – R/W/X AES GCM KEK – R/W/X AES GCM IV – W/X RSA Public Key – R/W RSA Private Key – R/W PBKDF Import/Export Password – R/X Triple-DES Decryption Key – R/W/X Data Protection Key – R/X
Export key	✓	✓	Export certificates and keys using specified KEK or RSA key pair and export method Requires TLS v1.2 session to Remote Console	Command and parameters	AES Key; RSA Public/Private Key (PKCS#7, PKCS#8, PKCS#12); ECDSA Public/Private Key; status output	AES KEK – R/W/X AES GCM KEK – R/W/X AES GCM IV – W/X RSA public key – R/W RSA private key – R/W PBKDF2 Import/export password – R/X Data Protection Key – R/X
List keys	✓	✓	List the keys in a partition	Command	Status output	None
Change permissions	✓	✓	Change permissions on keys in partition	Command and parameters	Status output	None
Change one's own password	✓	✓	Modify existing login passwords	Command and parameters	Status output	CO Password – R/W User Password – R/W

Service	Operator		Description	Input	Output	CSP and Type of Access
	CO	User				
Establish TLS session	✓	✓	Establish Remote Console session using TLS protocol	Command	Command response/ Status output	TLS Public Key – W/X TLS Private Key – W/X TLS Bundle Public Key – W/X TLS Bundle Private Key – W/X ECDH Private Component – X ECDH Public Component – R/X TLS Pre-Master Secret – W/X TLS Master Secret – W/X TLS Session Key – R/W/X TLS Authentication Key – W/X AES GCM IV – W/X DRBG Seed – R/W/X Entropy Input String – R/X DRBG 'V' Value – R/W/X DRBG Key Value – R/W/X
Set TLS bundle (HTTPS Console only)	✓		Import a TLS bundle (certificate and private key)	Command/Data	Command response/Status output	TLS Bundle Public Key – W/X TLS Bundle Private Key – W/X
Perform global backup	✓	✓*	Backup HSM database Requires TLS v1.2 session to Remote Console	Command and parameters	HSM global encrypted backup; status output	Data Protection Key – R/X PBKDF2 Backup Password – R/X Backup Key – W/X
Perform global restore	✓	✓*	Restore HSM database Requires TLS v1.2 session to Remote Console	Command and parameters, local backup file to read	Status output	Data Protection Key – R/X PBKDF2 Backup Password – R/X Backup Key – W/X

✓*: these services are only available if the CO has enabled permission on the User's account, as described in Section 2.4.1.

2.4.4 Additional Services

The module provides a limited number of services for which the operator is not required to assume an authorized role. Table 9 lists the services for which the operator is not required to assume an authorized role. None of these services disclose or substitute cryptographic keys and CSPs or otherwise affect the security of the module.

Table 9 – Additional Services

Service	Description	Input	Output	CSP and Type of Access
Zeroize	Zeroize ephemeral keys and CSPs	Power cycle	Status output	All ephemeral keys/CSPs – W
Perform on-demand self-tests	Perform self-tests on demand	Power cycle	Status output	All ephemeral keys/CSPs – W

Service	Description	Input	Output	CSP and Type of Access
Authenticate to local management console	Authenticate COs to local management console	Command and parameters	Status output	CO PINs – R/X Smart card PINs – R/X
Authenticate to Remote Console or HTTPS Console	Authenticate operators to Remote Console or HTTPS Console	Command and parameters	Status output	Crypto Officer Password – X User Password – X
Tamper Response	Zeroize all keys and CSPs	Trigger of border breach supervisory circuit	Status output	All keys/CSPs – W
About (HTTPS Console Only)	Displays some system aspects	Command	Status Output	N/A

2.5 Physical Security

The following physical security mechanisms are implemented by the module:

- module enclosure – the module enclosure consists of a hard, opaque metal case. It has a top cover that is only meant to be removed for maintenance by the manufacturer.
- tamper-evident seals – the modules employ tamper evident seals consisting of thin gauged vinyl to cover the area adjoining the top cover to the rest of the enclosure, as shown in Figure 11, Figure 12, Figure 13, and Figure 14.
- metal seals – metal screw covers protect the screws (DINAMO CD and XP have two screws; DINAMO ST has one screw) to the rear of the enclosure, preventing access to the screw heads. Any attempt to remove the covers will damage them preventing reuse and providing tamper evidence. These covers are shown in Figure 15.
- probing protection – all physical ports have additional protection to avoid probing, observing, or directly manipulating internal components of the module. This protection consists of steel plates that are attached to the front and rear panel of the module enclosure.
- ventilation panel holes and deflectors – the ventilation panel holes are smaller than 1/16th of an inch. The ventilation panels have deflectors with a specific geometric pattern and positioning to prevent probing, observing, or directly manipulating the internal components of the module.
- protection for removable power supplies (only DINAMO ST has removable power supplies) – no access is provided through the removable power supplies.
- border breach supervisory circuit – the active element of physical security that contains tamper-response and zeroization circuitry that monitors the top cover. This circuit is connected to two pairs of sensors located on each side of the module and detect if any of the screws attaching the top cover to the base of the cabinet structure are attempted to be removed. The circuitry records any violation and the module firmware zeroizes all plaintext secret and private keys and unprotected CSPs, halts all HSM services, and shuts down the module.

FIGURE 11 – Tamper-Evident Seal

FIGURE 12 – Example of Tamper-Evident Seals Adjoining Top Cover to Base of Enclosure (DINAMO XP)

FIGURE 13 – Example of Tamper-Evident Seals Adjoining Top Cover to Base of Enclosure (DINAMO CD)

FIGURE 14 – Example of Tamper-Evident Seals Adjoining Top Cover to Base of Enclosure (DINAMO ST)

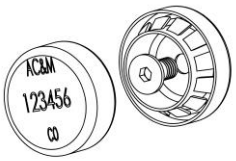

FIGURE 15 – Metal Covers for Screws

2.6 Operational Environment

The operational environment of the module does not provide a general-purpose OS to module operators.

The module employs a non-modifiable operating environment. The HSM firmware is executed by the module's processors running CentOS 7.4 as indicated below:

- DINAMO CD (one Intel i3 6100 3.7 GHz[48] two-core processor)
- DINAMO ST (two Intel Xeon Silver 4210 2.2 GHz ten-core processors)
- DINAMO XP (one Intel i7 7700 3.60 GHz four-core processor)

The module provides no mechanisms for operators to update the firmware. This must be performed by the vendor.

[48] GHz – Gigahertz

2.7 Cryptographic Key Management

The module supports the CSPs listed below in Table 10.

Table 10 – Cryptographic Keys, Cryptographic Key Components, and CSPs

CSP	CSP Type	Generation / Input	Output	Storage	Zeroization	Use
Replication TLS-PSK Key	128-bit AES-CBC key	Derived from the Master Key via KBKDF per SP 800-108	Never exits the module	Plaintext in volatile RAM	At end of TLS session, power cycle, shutdown, reboot, HSM database reset, violation attempt	Encryption/decryption of TLS sessions used for replication between modules
AES GCM IV	96-bit value	Generated internally via FIPS-Approved DRBG with RBG construction per Section 8.2.2 of NIST SP 800-38D	Never exits the module	Plaintext in volatile RAM	Power cycle, shutdown, reboot, HSM database reset, violation attempt	IV for AES GCM function
AES GCM KEK	128, 192, 256-bit AES-GCM key	Internally generated via Approved DRBG	Never exits the module	Plaintext in volatile RAM	Power cycle, shutdown, reboot, HSM database reset, violation attempt	Key transport
AES CMAC key	128, 192, 256-bit AES-CMAC key	Internally generated via Approved DRBG	Never exits the module	Plaintext in volatile RAM	Power cycle, shutdown, reboot, HSM database reset, violation attempt	MAC generation and verification
Master Key components	24-byte components of Master Key	Generated internally during module initialization by splitting Master Key into multiple key components (minimum of two) using Shamir Sharing scheme	Output to smart cards using split-knowledge procedures during module initialization	Smart cards	N/A	Reconstructing Master Key

CSP	CSP Type	Generation / Input	Output	Storage	Zeroization	Use
Master Key	192-bit symmetric key	Generated internally via FIPS-Approved DRBG per NIST SP 800-133 CKG during module initialization Reconstructed using split knowledge procedures from Master Key components input from smart cards (for module activation after restart)	Never exits the module	Plaintext in volatile RAM	Power cycle, shutdown, reboot, HSM database reset, violation attempt	Derivation of Data Protection Key
Data Protection Key	256-bit AES-GCM key	Derived from the Master Key via KBKDF per SP 800-108	Never exits the module	Plaintext in volatile RAM	Power cycle, shutdown, reboot, HSM database reset, violation attempt	Encryption/decryption of all data in persistent storage
ECDH Private Component	Private component of ECDH: P-256 BrainpoolP224r1, BrainpoolP256r1, BrainpoolP320r1, BrainpoolP384r1, BrainpoolP512r1	Generated internally using FIPS-Approved DRBG	Never exits the module	Plaintext in volatile RAM	At end of TLS session, power cycle, shutdown, reboot, HSM database reset, violation attempt	Generation of TLS shared secrets
ECDH Public Component	Public component of ECDH: P-256 BrainpoolP224r1, BrainpoolP256r1, BrainpoolP320r1, BrainpoolP384r1, BrainpoolP512r1	Generated internally using FIPS-Approved DRBG	Exits in plaintext form	Plaintext in volatile RAM	At end of TLS session, power cycle, shutdown, reboot, HSM database reset, violation attempt	Generation of TLS shared secrets
TLS Private Key	2048 or 3072-bit RSA private key P-256 ECDSA private key	Generated internally via FIPS-Approved DRBG	Never exits the module	Plaintext in volatile RAM	At end of TLS session, power cycle, shutdown, reboot, HSM database reset	TLS authentication

CSP	CSP Type	Generation / Input	Output	Storage	Zeroization	Use
TLS Bundle Private Key	2048 or 3072-bit RSA private key P-256 ECDSA private key	Generated externally and imported in encrypted form via HTTPS Console using Set TLS bundle command	Never exits the module	Encrypted (via Data Protection Key) on SSD	N/A[49]	TLS authentication
TLS Public Key	2048 or 3072-bit RSA public key P-256 ECDSA public key	Generated internally via FIPS-Approved DRBG	Exits the module in plaintext form	Plaintext in volatile RAM	N/A	TLS authentication
TLS Bundle Public Key	2048 or 3072-bit RSA public key P-256 ECDSA public key	Generated externally and imported via HTTPS Console	Exits the module in plaintext form	Encrypted (via Data Protection Key) on SSD	N/A	TLS authentication
TLS Pre-Master Secret	[for RSA cipher suites] 384-bit random value [for ECDH cipher suites] ECDH shared secret	[for RSA cipher suites] Generated externally and imported in encrypted form via RSA key transport [for ECDH cipher suites] Derived internally via ECDH shared secret computation	Never exits the module	Plaintext in volatile RAM	Upon completion of TLS Master Secret computation, power cycle, shutdown, reboot, HSM database reset, violation attempt	Derivation of the TLS Master Secret
TLS Master Secret	256 or 384-bit shared secret	Derived internally using the TLS Pre-Master Secret via TLS KDF	Never exits the module	Plaintext in volatile RAM	At end of TLS session, power cycle, shutdown, reboot, HSM database reset, violation attempt	Derivation of the TLS Session Key and TLS Authentication Key

[49] N/A – Not Applicable

CSP	CSP Type	Generation / Input	Output	Storage	Zeroization	Use
TLS Session Key	128 or 256-bit AES key 128 or 256-bit AES GCM key	Derived internally using the TLS Master Secret via TLS KDF	Never exits the module	Plaintext in volatile RAM	At end of TLS session, power cycle, shutdown, reboot, HSM database reset, violation attempt	Encryption and decryption of TLS session packets
TLS Authentication Key	160, 256, or 384-bit HMAC key	Derived internally using the TLS Master Secret via the TLS KDF	Never exits the module	Plaintext in volatile RAM	At end of TLS session, power cycle, shutdown, reboot, HSM database reset, violation attempt	Authentication of TLS session packets
DRBG Seed	384-bit value	Generated internally using entropy input string	Never exits the module	Plaintext in volatile RAM	Power cycle, shutdown, reboot, reset HSM database, violation attempt	Seeding material for DRBGs
Entropy Input String	256-bit value	Generated internally	Never exits the module	Plaintext in volatile RAM	End of DRBG function, power cycle, shutdown, reboot, HSM database reset, violation attempt	Entropy material for SP 800-90A DRBG
DRBG Key Value	Internal DRBG state value 256 bits	Generated internally	Never exits the module	Plaintext in volatile RAM	Power cycle, shutdown, reboot, HSM database reset, violation attempt	Random number generation
DRBG ‘V’ Value	Internal DRBG state value 128 bits	Generated internally	Never exits the module	Plaintext in volatile RAM	Power cycle, shutdown, reboot, HSM database reset, violation attempt	Random number generation
CO Password	Alphanumeric string Minimum of eight (8) characters	Input electronically in encrypted form via Remote Console or HTTPS Console (over TLS session)	Never exits the module	Hashed and encrypted (via Data Protection Key) on SSD	N/A	Authentication to the module via Remote Console or HTTPS Console
Smart Card PIN	Eight digits	Read from smart card	Never exits the module	Plaintext in volatile RAM	Power cycle, shutdown, reboot, HSM database reset, violation attempt	CO authentication to the module via local management console

CSP	CSP Type	Generation / Input	Output	Storage	Zeroization	Use
CO PIN	Eight digits	Input manually in plaintext via local management console (over USB keyboard port)	Never exits the module	Plaintext in volatile RAM	Power cycle, shutdown, reboot, HSM database reset, violation attempt	CO authentication to the module via local management console
User Password	Alphanumeric string Minimum of eight (8) characters	Input electronically in encrypted form via Remote Console or HTTPS Console (over TLS session)	Never exits the module	Hashed and encrypted (via Data Protection Key) on SSD	N/A	User authentication to the module via Remote Console or HTTPS Console
RSA Public Key	1024, 2048 or 3072-bit RSA public key	Imported in encrypted form (1024, 2048, 3072) or Generated internally via FIPS-Approved DRBG (2048, 3072)	Exported in encrypted form	Encrypted (via Data Protection Key) in User/CO partitions on SSD	N/A	Verifying digital signatures and encrypting symmetric key envelopes 1024 Verification only
RSA Private Key	2048 or 3072-bit RSA private key	Imported in encrypted form or Generated internally via FIPS-Approved DRBG	Exported in encrypted form (if export attribute of “exportable” is assigned to key during key generation)	Encrypted (via Data Protection Key) in User/CO partitions on SSD	N/A	Generating digital signatures and decrypting symmetric key envelopes
ECDSA Private Key	ECDSA private key: P-224, P-256, P-384, P-521 BrainpoolP224r1, BrainpoolP256r1, BrainpoolP320r1, BrainpoolP384r1, BrainpoolP512r1	Generated internally using FIPS-Approved DRBG or Imported in encrypted form	Exported in encrypted form (if export attribute of “exportable” is assigned to key during key generation)	Encrypted (via Data Protection Key) in User/CO partitions on SSD	N/A	Digital signature generation

CSP	CSP Type	Generation / Input	Output	Storage	Zeroization	Use
ECDSA Public Key	ECDSA public key: P-192, P-224 P-256, P-384, P-521 BrainpoolP224r1, BrainpoolP256r1, BrainpoolP320r1, BrainpoolP384r1, BrainpoolP512r1	Generated internally using FIPS-Approved DRBG or Imported in encrypted form	Exported in encrypted form	Encrypted (via Data Protection Key) in User/CO partitions on SSD	N/A	Digital signature verification
Triple-DES Decryption Key	112 or 168-bit Triple-DES key	Derived internally using PBKDF2 Import/Export Password per NIST SP 800-132	Never output from module	Plaintext in volatile RAM	Power cycle, shutdown, reboot, HSM database reset, violation attempt	Decryption of PKCS#8/12 imports
AES Key	128, 192, and 256-bit AES key (ECB, CBC, CTR, GCM)	Imported in encrypted form or Generated internally via FIPS-Approved DRBG	Exported in encrypted form (if export attribute of "exportable" is assigned to key during key generation)	Encrypted (via Data Protection Key) in User/CO partitions on SSD	N/A	Encryption/decryption
PBKDF2 Import/Export Password	16-character value	Input electronically in encrypted form via Remote Console or HTTPS Console (over TLS session)	Never output from module	Plaintext in volatile RAM	Power cycle, shutdown, reboot, HSM database reset, violation attempt	Used to derive AES KEK for PKCS#8/#12 import/export Used to derive Triple-DES Decryption Key for PKCS#8/#12 import (decrypt only)
HMAC Key	Variable-bit HMAC key	Internally generated via FIPS-Approved DRBG	Exported in encrypted form (if export attribute of "exportable" is assigned to key during key generation)	Encrypted (via Data Protection Key) in User/CO partitions on SSD	N/A	Message authentication with SHS/SHA3

CSP	CSP Type	Generation / Input	Output	Storage	Zeroization	Use
AES KEK	256-bit AES-CBC key	Derived internally using PBKDF2 Import/Export Password per NIST SP 800-132	Never output from module	Plaintext in volatile RAM	Power cycle, shutdown, reboot, HSM database reset, violation attempt	Encrypting/decrypting RSA private keys in PKCS#8/12 envelopes during import/export
PBKDF2 Backup Password	Minimum eight-character value	Input electronically in encrypted form via Remote Console or HTTPS Console (over TLS session)	Never output from module	Plaintext in volatile RAM	Power cycle, shutdown, reboot, HSM database reset, violation attempt	Deriving Backup Key
Backup Key	128-bit AES- CBC Key	Derived internally using PBKDF2 Backup Password per NIST SP 800-132	Never output from module	Plaintext in volatile RAM	Power cycle, shutdown, reboot, HSM database reset, violation attempt	Encrypting backups

***Keys derived from the PBKDF2 function shall only be used for storage applications.*

The AES GCM IV is used for generating the Data Protection Key, operator AES GCM keys, AES GCM KEKs for key wrap/unwrap, and AES GCM keys used in the TLS protocol. The AES GCM IV is internally generated via RBG-based construction in compliance with Section 8.2.2 of NIST SP 800-38D using the Approved DRBG within the module's physical boundary and is 96 bits in length.

2.8 EMI / EMC

The module was tested and found to be conformant 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).

2.9 Self-Tests

The module performs power-up self-tests, conditional self-tests, and critical function tests. These tests are described in the sections that follow.

2.9.1 Power-Up Self-Tests

The HSM performs the following self-tests at power-up to verify the integrity of the firmware images and the correct operation of the FIPS-Approved algorithm implementations:

- Firmware Integrity Test on DINAMO HSM firmware components and crypto library using HMAC SHA-256
- Cryptographic algorithm tests:
  - AES ECB encrypt KAT[50]
  - AES ECB decrypt KAT
  - AES CTR encrypt KAT
  - AES CTR decrypt KAT
  - AES GCM encrypt KAT
  - AES GCM decrypt KAT
  - AES CBC encrypt KAT
  - AES CBC decrypt KAT
  - AES CMAC KAT
  - Triple-DES 3-key encrypt KAT (CBC, ECB)
  - Triple-DES 3-key decrypt KAT (CBC, ECB)
  - Triple-DES 2-key decrypt KAT (CBC, ECB)
  - Triple-DES CMAC KAT (2-key and 3-key)
  - HMAC SHA-224, HMAC SHA-256, HMAC SHA-384, and HMAC SHA-512 KAT
  - HMAC SHA3-224, HMAC SHA3-256, HMAC SHA3-384, and HMAC SHA3-512 KAT
  - SHA-1, SHA-224, SHA-256, SHA-384, SHA-512 KAT
  - SHA3-224, SHA3-256, SHA3-384, SHA3-512 KAT
  - CTR DRBG KAT
  - Critical Functions Tests for DRBG (Instantiate, Generate, Reseed, Uninstantiate)
  - RSA signature generation KAT
  - RSA signature verification KAT
  - ECDSA signature generation KAT
  - ECDSA signature verification KAT
  - Primitive “Z” Computation KAT
  - KBKDF KAT

[50] KAT – Known Answer Test

2.9.2 Conditional Self-Tests

The HSM performs the following conditional self-tests:

- CRNGT for the NDRNG entropy source
- RSA Pairwise Consistency Test
- ECDSA Pairwise Consistency Test

2.9.3 Self-Test Failure Handling

If the module fails a power-up self-test, the module enters a “Critical” error state and reports this error to a Crypto Officer via the VGA video port and logs the error. Once in a Critical error state, the module remains there until the Crypto Officer acknowledges the error (via the local management console), at which point the module shuts down.

If an error occurs during the power-up self-tests, the module is in a state in which it cannot be activated for operation, so authentication is not possible and network ports cannot be enabled for Remote Console access. Consequently, all access to the cryptographic functionality and CSPs is disabled. All data outputs via data output interfaces are inhibited and the management interfaces will not respond to any commands, other than the self-test error acknowledgement (shutdown).

There is no action the operator can take to repair a critical error state and the module should be returned to the vendor for servicing. The only option for the operator is to acknowledge the error (which shuts down the module).

If an error occurs during conditional self-tests, the module transitions to a soft error state. The module logs the error, clears the error state, and then resumes normal operation.

2.10 Mitigation of Other Attacks

Fault-based attacks on a system such as high temperatures or voltage manipulation may be used to induce errors or corrupt messages. Offline analysis of these errors can be used to reverse engineer the cryptographic module, potentially extracting the private key from the cryptographic routines it executes.

The module protects against fault-based attacks that are aimed at creating erroneous RSA and ECDSA digital signatures, by affecting the result of the modular exponentiation algorithm. The protection mechanism involves validating the correctness of every RSA and ECDSA digital signature created by the module using the associated public key. In case of errors, the operation is marked as invalid, and the module returns only TAC ERR OPERATION FAILED. This protection mechanism is always active.

3. Secure Operation

The sections below describe how to place and keep the module in the FIPS-approved mode of operation. **Any operation of the module without following the guidance provided below will result in non-compliant use and is outside the scope of this Security Policy.**

3.1 Installation and Setup

The CO shall be responsible for receiving, installing, initializing, and maintaining the HSM module. To operate the module in the Approved mode, the CO shall configure the module via the local keyboard USB port with VGA output as directed by this Security Policy. The following sections provide the CO with important instructions and guidance for the secure installation and configuration of the HSM.

3.1.1 Initial Setup

Upon receiving the HSM hardware, the CO shall check that the system is not damaged and that all required parts and instructions are included. The CO shall refer to the *Physical Installation* section of the administration guide here for initial setup instructions: https://docs.dinamonetworks.com/.

After the CO has finished installation of the module, the local management console can be used to configure the module in the FIPS-Approved mode of operation, which is outlined in section 3.1.2 below.

3.1.2 FIPS-Approved Mode Configuration and Status

The CO shall configure the module for FIPS mode. This ensures that the system will use only FIPS-Approved cryptographic algorithms and key strengths. To set the module into its FIPS mode of operation, the CO may use the local management console and follow the setup procedure below. These instructions start from the module is in its factory state of non-restricted mode, which is how it ships to the customer.

Setup procedure:

1. Power up the module, and after the self-tests run to completion, a message will appear on the local management console stating “this is a fresh/first time HSM boot. A valid Server Master Key must be generated now. Do you want to load smart card manager?”
2. Select “Yes” and the **Main** menu appears
3. Select **Create Server Master Key**
4. Select “Yes”, then choose values for M and N of the “M of N scheme”:
    - N: the number of cards that will be generated and distributed (between 2 and 250)
    - M: the number of cards, among the N generated, that will be requested for the activation of the HSM. This number must be between 2 and the number defined for N.
5. Select Ok.
6. The module’s FIPS-Approved DRBG generates a Master Key.

7. Each CO must follow the instructions to insert a smart card and enter the PIN (exactly 8 digits) to generate one of the N Master Key components on each smart card.
    - The next screen says " A valid SVMK/SHADOW is already present. Do you want to overwrite it? Click Yes
    - The next screen says "You can provide a card label (optional). Enter label and select OK or select Skip.
    - "Master Key Shadow #1 created." will be reported after creation of each smart card.
    - Server Master Key successfully created with Scheme "2 of 2". Select OK
    - Highlight on arrow and press enter. Each CO must enter smart card and PIN.
8. After all the smart cards have been created, navigate to **Configuration→ Operation Mode**, press enter, and change the operating mode to RM2 (equivalent to FIPS-Approved mode) and select Change.
9. A message displays that HSM is operating in NRM. Do you want to change to RM2? WARNING: HSM database will be reset. All keys and data will be lost. It is highly recommended that you make a backup before changing operation mode. Select Yes.
10. Each CO must authenticate using their smart card and CO PIN to confirm the operating mode change.
11. An HSM database reset is automatically performed (all keys in volatile memory, including the Master Key, derived Data Protection Key, and all other keys in persistent memory are destroyed). This triggers a reboot.
12. Self-tests are automatically performed.
13. The module is now in RM2 (FIPS-Approved mode) A screen shows with "Operation mode: RM2" to indicate FIPS-Approved mode.
14. Repeat Steps 1-6 to generate a new Master Key in FIPS-Approved mode (with new Master Key components on each smart card)

    Note: After successful authentication, remove the smart cards from the reader. As the Master Key is created using an M of N scheme, the HSM automatically detects and requests as many (M) cards as necessary until the key is reconstructed.

15. Choose the *Start service* command from the **Main** menu of the local management console – this opens network ports and allows for Remote Console authentication for all operators.
16. Message with "Service started" appears. Select OK.
17. COs must change the default PIN for their smart cards using the *Change Pin* command from the **Configuration → Smart Card → Change PIN** menu of the local management console.
18. Enter a PIN consisting eight digits and Select **OK**.
19. Lock the local management console using the *Lock console* command from the **Main** menu – after this point, smart cards and PINs must be re-entered by M number of COs to unlock the local management console and perform services (e.g., shutdown, reboot).

Once the local management console is locked, the customer must install the software for the Remote Console. Use the following link to download the software: docs.dinamonetworks.com. Navigate to Software Clients → Downloads or Downloads line from the top of the screen. Choose Windows: msi64-bit and download the executable.

Next, start the Remote Console installer by double-clicking on the remote console executable and install it as follows:

1. Select Avencoir (next)
2. Select Completa (Complete)
3. Select Instalar (Install)
4. Select Concluir (Conclude)

After the software finishes the install, type hsmcon <IP address of HSM> master and select Enter at the command prompt to start the Remote Console. Then follow these steps to complete the setup procedure:

1. Login to the Remote Console by entering default username “master” and default password provided by the vendor.
2. Change the default “master” password to a password with at least 8 characters in length, consisting of upper-case and lower-case letters and numbers or special characters.
3. Create user accounts for the Remote Console and HTTPS Console using the *Create* command from the **Main** menu.
    - Choose 1 for User or 2 for Operator (CO), then type in User ID and Password and confirm password. Two factor authentication is optional.

When configured by following the setup procedure above, the module only operates in a FIPS-Approved mode. Thus, the current status of the module when operational is always in the FIPS-Approved mode.

The appliance’s operational status is indicated with the **About** option on the main menu of the local management console and the **Info** option on the main menu of the Remote Console or HTTPS Console.

3.2 Crypto Officer Guidance

The Crypto Officer is responsible for initialization and security-relevant configuration and management of the module. The operator profile has all possible permissions and is equivalent to the official Security Officer (Crypto Officer). The system allows some permissions to be enabled for certain User profile accounts by creating a user profile intermediate between User and Operator profiles, to facilitate HSM management. Operator profile, being a superset of the User profile, also has its particular domain of cryptographic keys.

3.2.1 Management

Once installed and configured, the CO is responsible for maintaining and monitoring the status of the module to ensure that it is running in its FIPS-Approved mode. Please refer to Section 3.1.2 for guidance that the CO must follow for the module to be considered running in a FIPS-Approved mode of operation.

COs should ensure that physical security of the module is maintained via periodic inspection of tamper-evident seals and checks for border breach supervisory circuit alerts. After the CO has acknowledged a border breach violation flag, the CO may continue operating the module. The status record (“TAMPERED”) will be kept in the logs and can be verified by the CO at the local management console. Only the equipment manufacturer can remove this registry.

3.2.2 On-Demand Self-Tests

The power-up self-tests are automatically performed at power-up. The CO may initiate the power-up self-tests through the following methods:

- issuing the *reboot* command at the **Main** menu of the local management console
- power-cycling the module (issuing the *shutdown* command at the **Main** menu of the local management console and powering up the module)

- issuing the *HSM self-test* or *Reset HSM database* command from the **Configuration** menu of the local management console

3.2.3 PBKDF2 Passwords

The CO can save an encrypted database backup file. The generation of the key used for the encryption of this file is performed by an SP 800-132 PBKDF2. When the CO is prompted to enter a new password, the CO shall enter a password no less than 8 characters in length. The password shall consist of upper-case and lower-case letters and numbers. The probability of guessing the password will be equal to $1:62^8$, or $1:2.18x10^{11}$. The key derived by the PBKDF2 is used solely for storage purposes. Likewise, a PBKDF2 may be used by operators to derive the AES Key and Triple-DES Decryption Key used during import/export of RSA keys (PKCS#8/12 digital envelopes). Operators must enter a password no less than 16 characters in length. The password shall consist of upper-case and lower-case letters and numbers. The probability of guessing the password will be equal to $1:62^{16}$, or $1:4.77x10^{28}$.

3.2.4 Zeroization

Please refer to Table 10 for the key zeroization techniques and the applicable keys. In addition, the border breach supervisory circuitry records any tamper attempt and the module firmware immediately zeroizes all plaintext secret and private keys and unprotected CSPs, halts all HSM services, and shuts down the module.

3.3 User Guidance

The User does not have the ability to configure sensitive information on the module, except for their password. The User must be diligent to pick strong passwords and must not reveal their password to anyone. Additionally, the User should be careful to protect any secret or private keys in their possession.

3.4 Additional Guidance and Usage Policies

This section notes additional policies below that must be followed by module operators:

- If the module fails a power-up self-test, the module is considered to be compromised or malfunctioned and should be sent back to DINAMO for repair or replacement.
- In the event that the module's power is lost and then restored, a new key for use with the AES GCM encryption shall be established.

- The module does not allow for the loading of new firmware.

3.5 Common Vulnerabilities and Exposures

The module is not subject to any high severity CVEs.

3.6 Non-Approved Mode of Operation

When initialized and configured according to the guidance in this Security Policy, the module does not support a non-Approved mode of operation.

4. Acronyms

Table 11 provides definitions for the acronyms used in this document.

Table 11 – Acronyms

Acronym	Definition
AES	Advanced Encryption Standard
ANSI	American National Standards institute
API	Application Programming Interface
CA	Certificate Authority
CAVP	Cryptographic Algorithm Validation Program
CBC	Cipher Block Chaining
CCCS	Canadian Centre for Cyber Security
CKG	Cryptographic Key Generation
CLI	Command Line Interface
CMAC	Cipher-Based Message Authentication Code
CMVP	Cryptographic Module Validation Program
CO	Crypto Officer
CPU	Central Processing Unit
CRNGT	Continuous Random Number Generator Test
CSP	Critical Security Parameter
CSR	Certificate Signing Request
CTR	Counter
CVL	Component Validation List
DES	Data Encryption Standard
DH	Diffie-Hellman
DRBG	Deterministic Random Bit Generator
ECB	Electronic Codebook
ECC	Elliptic Curve Cryptography
ECC CDH	Elliptic Curve Cryptography Cofactor Diffie-Hellman
ECDH	Elliptic Curve Diffie-Hellman
ECDSA	Elliptic Curve Digital Signature Algorithm
EMI/EMC	Electromagnetic Interference/Electromagnetic Compatibility
FIPS	Federal Information Processing Standard
GCM	Galois/Counter Mode
GHz	Gigahertz

Acronym	Definition
HMAC	(keyed-) Hash Message Authentication Code
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IV	Initialization Vector
JCA	Java Cryptography Architecture
JCE	Java Cryptography Extension
KAS	Key Agreement Scheme
KAS-SSC	Key Agreement Scheme - Shared Secret Computation
KAT	Known Answer Test
KBKDF	Key Based Key Derivation Function
KDF	Key Derivation Function
KEK	Key Encryption Key
KPG	Key Pair Generation
LAN	Local Area Network
Mbps	Megabits per second
MS	Microsoft
N/A	Not Applicable
NDRNG	Non-Deterministic Random Number Generator
NIST	National Institute of Standards and Technology
OS	Operating System
PBKDF2	Password-based Key Derivation Function 2
PCT	Pairwise Consistency Test
PKCS	Public Key Cryptography Standard
PKG	Public Key (Q) Generation
PKV	Public Key (Q) Validation
PRF	Pseudo-Random Function
PSK	Pre-shared Key
PSS	Probabilistic Signature Scheme
PUB	Publication
RAM	Random Access Memory
RSA	Rivest Shamir Adleman
RU	Rack Unit
SHA	Secure Hash Algorithm
SHS	Secure Hash Standard
SP	Special Publication
SSD	Solid State Drive

Acronym	Definition
SSL	Secure Socket Layer
TLS	Transport Layer Security
U.S.	United States
USB	Universal Serial Bus
VGA	Video Graphics Array

Prepared by:

Corsec Security, Inc.

13921 Park Center Road, Suite 460
Herndon, VA 20171
United States of America

Phone: +1 703 267 6050
Email: info@corsec.com
http://www.corsec.com