FUTUREX

EXP1000 Hardware Security Module

FIPS 140-2 Non-Proprietary Security Policy

This document may be reproduced only in its original entirety [without revision].

# Table of Contents

1. MODULE OVERVIEW

The EXP1000 (HW P/Ns: 9850-0365 Rev10, 9800-2082 Rev 10[1], 9800-2082 Rev 10A[2], 9800-2082 Rev 10B, 9800-2082 Rev 10C, 9800-2082 Rev 10D, 9800-2082 Rev 10E, 9800-2082 Rev 11 and 9800-2082 Rev 11A; and FW Version 7.0.0.3) Hardware Security Module (HSM) is a multi-chip embedded cryptographic module that provides secure data storage and processing functionality. All sensitive components of the module are physically protected by a tamper resistant, responsive, and evident casing where all cryptographic operations are performed. Upon tamper detection, normal operations are halted and critical security parameters are erased. The module is assembled from production quality components and provides high speed interfaces for control and data input, status, and data output. The image below depicts the cryptographic module and provides a visual indication of the potting layer that outlines the cryptographic boundary.
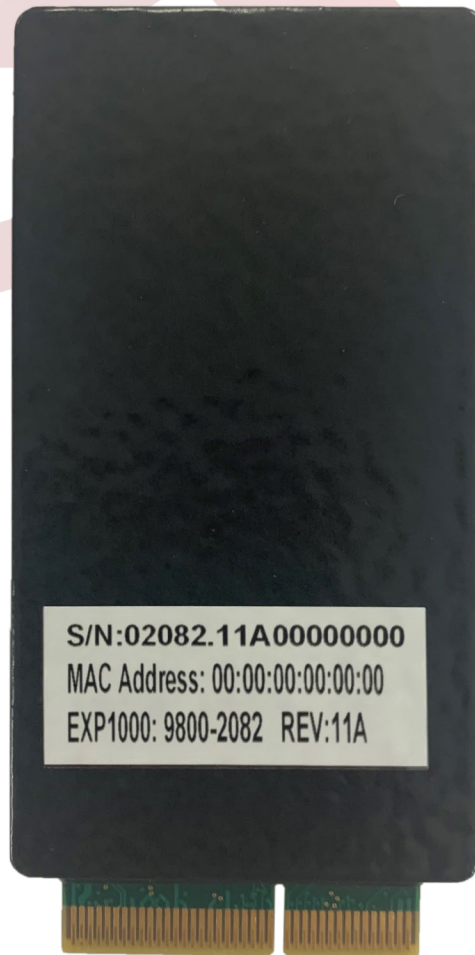
Figure 1 – EXP1000 Hardware Security Module

---

[1] There was a change in Futurex's Configuration Management Policy during the evaluation period that necessitated the use of a new part number for the EXP1000. An initial batch of the hardware product was shipped to customers with the original part number prior to the policy change. All new shipments make use of P/N: 9800-2082. Both part numbers are included in the Security Policy to ensure existing product, once updated with the FIPS approved firmware, will be compliant.

[2] For the versions of P/N: 9800-2082, there are no security relevant differences. The main changes are resistors and BOM part number changes.

2. SECURITY LEVEL

The cryptographic module meets the FIPS 140-2 overall security requirements applicable to Level 3.

Security Requirements Section	Level
Cryptographic Module Specification	3
Module Ports and Interfaces	3
Roles, Services and Authentication	3
Finite State Model	3
Physical Security	3
Operational Environment	N/A
Cryptographic Key Management	3
EMI/EMC	3
Self-Tests	3
Design Assurance	3
Mitigation of Other Attacks	3

Table 1 - Module Security Level Specification

3. MODES OF OPERATION

The cryptographic module may be configured for FIPS Approved mode, PCI-HSM (Non-Approved for FIPS 140) Mode of Operation, or General (Non-Approved) Mode of Operation by accessing the *System* tab on the module's web interface. A drop-down menu is shown for FIPS mode ("On" or "Off") and another for PCI HSM mode. The System tab will then show FIPS mode enabled.

When used in the Excrypt Plus parent device, the mode of operation is also displayed on its LCD screen. When transitioning between modes, the module will zeroize CSPs before entering the selected mode of operation and restart. The user can determine which mode the cryptographic module is in by accessing the *Status* tab on the module's web interface.

3.1. FIPS APPROVED MODE OF OPERATION

In FIPS Approved mode, the module supports the following algorithms:

Approved Functions

CAVP Cert	Algorithm	Standard	Mode/Method	Key Lengths/Curves/Moduli	Use
C1991	AES	NIST SP 800-38A	CTR	128 and 256-bit	Encryption
		NIST SP 800-38A	ECB, CBC, CFB1, CFB8, CFB128, OFB	128, 192, and 256-bits	Encryption and Decryption
		NIST SP 800-38B	CMAC	128, 192, and 256-bits	MAC Generation and Verification
		NIST SP 800-38D	GCM	128, 192, and 256-bits	Encryption and Decryption
C1992		NIST SP800-38F	AES KWP	128, 192, and 256-bits	Key Wrap
Vendor Affirmed	CKG[3]	SP 800-133 rev2	N/A	N/A	Symmetric Key Generation
C1991	CVL	NIST SP 800-135	TLS v1.0, v1.1 and v1.2 KDF	N/A	Key Derivation
C1991	DRBG	NIST SP 800-90A	CTR Mode: AES-256 Derivation Function Enabled: Yes Additional Input: 0-256 Entropy Input: 256 Nonce: 128	AES-256	Random Number Generation
C1991	ECDSA	FIPS 186-4	ECDSA KeyGen (184-4)	P-224, P-256, P-384 and P-521	Key generation
			ECDSA SigGen (186-4)	P-224, P-256, P-384 and P-521	Digital signature generation
			ECDSA SigVer (186-4)	P-192, P-224, P-256, P-384 and P-521	Digital signature verification

[3]***NOTE:*** *In accordance with FIPS 140-2 IG D.12, the cryptographic module performs Cryptographic Key Generation as per scenario 1 of section 4 in SP800-133 rev2. The resulting generated symmetric key and the seed used in the asymmetric key generation are the unmodified output from SP800-90A DRBG.*

C1991	HMAC	FIPS 198-1	SHA-1, SHA2-224, SHA2-256, SHA2-384 and SHA2-512	Key sizes: minimum 128-bits, maximum 256-bits.	Keyed Message Authentication
Vendor Affirmed	KAS-SSC	SP 800-56A rev3	ECC Ephemeral Unified Scheme	Key Establishment methodology provides between 112 and 256-bits of encryption strength	EC Diffie-Hellman Shared Secret Computation
			ECC One-Pass Diffie-Hellman scheme	All NIST Defined ECC Curves except 192 (P-224, P-256, P-384, and P-521)	
			FFC dhEphem scheme	2048, 3072, 4096 Safe Primes as defined by SP800-56A Rev3 Appendix D and RFC7919	Diffie-Hellman Shared Secret Computation
			FCC dhOneFlow scheme	Key Establishment methodology provides between 112 and 150-bits of encryption strength	
C1992	KBKDF	SP 800-108	Counter Mode, using AES-CMAC as PRF	128, 192, and 256-bits	Key Based KDF
Vendor Affirmed	KDA	SP800-56C Rev2	ECC Ephemeral Unified Scheme	RFC 8446 (TLS 1.3) and SP800-56C rev2 Section 5 HKDF Implementation	Key Derivation
				Two-Step Key Derivation using implementation dependent Auxilary PRF based KDF Option A. Used for TLS 1.0-1.2 (Cert#C1991)	
			ECC One-Pass Diffie Hellman	RFC 8446 (TLS 1.3) and SP800-56C rev2 Section 5 HKDF Implementation	
			FFC dhEphem Scheme	Cert #C1991 Two-Step Key Derivation using implementation-dependent Auxiliary PRF-based KDF Option A	
			FFC dhOneFlow Scheme	One-Step Key Derivation Option 1 (Hash (SHS FIPS 180-4)	
C1992	KTS	NIST SP 800-38F	AES KWP	Key establishment methodology provides between 128 and 256 bits of encryption strength	Encryption and Decryption
			AES CBC / AES CMAC		Encryption and Authentication
C1991			AES CBC / HMAC		Encryption and Authentication (See TLS Cipher Suite Listing)

C1991	RSA	FIPS 186-4	RSA KeyGen (186-4)	Modulo 2048 and 3072	Key Generation Mode B.3.3 and B.3.6
			RSA SigGen (186-4)	Modulo 2048, 3072 and 4096*	ANSI X9.31, PKCS 1.5 and PKCSPSS, Signature Generation
			RSA SigVer (186-4)	Modulo 1024, 2048, and 3072	ANSI X9.31, PKCS 1.5 and PKCSPSS, Signature
C1991	SHS	FIPS 180-4	SHA-1, SHA-224, SHA-256, SHA-384 and SHA-512	-	Message Digest Note: SHA-1 is not available for digital signature creation.

Table 2 – FIPS 140-2 Approved Functions

* Note: 186-4 RSA 4096 SigGen was not available for CAVP testing; however, per IG G.18, it is approved for use because 186-2 RSA 4096 SigGen was tested.

Allowed Non-Approved Functions

Algorithm	Caveat/Use
MD5	Message digest used in TLS 1.0/1.1 ONLY
NDRNG	Entropy input of 256-bits provided to the DRBG for Seed Data.
RSA	Key wrapping: key establishment methodology which provides 112-bits of encryption strength. RSA algorithm may be used for encryption or decryption of keys. No claim is made for SP 800-56B compliance, and no CSPs are established into or exported out of the module using these services.
Shamir Secret Sharing	Split Knowledge Procedures: Polynomial method used only for secret-sharing. *Note: As per NISTIR 8214, Section 6.2, implementation of Shamir Secret Sharing is used to satisfy section 4.7.4 of the FIPS 140-2 standard which defines security requirements for split-knowledge procedures.*

Table 3 – Allowed Non-Approved Functions

3.1.1.   AES GCM Considerations

AES GCM encryption and decryption are used in the context of the *TLS protocol version 1.2* (compliant to Scenario 1 path (i) in FIPS 140-2 A.5). The module is compliant with NIST SP 800-52 rev2 and the mechanism for IV generation is compliant with RFC 5288. The module ensures that it is strictly increasing and thus cannot repeat. When the IV exhausts the maximum number of possible values for a given session key, the first party, client or server, to encounter this condition may either trigger a handshake to establish a new encryption key in accordance with RFC 5246, or fail. In either case, the module prevents IV duplication and thus enforces the security property.

AES GCM encryption and decryption are used in the context of the *TLS protocol version 1.3* (compliant to Scenario 5 in FIPS 140-2 IG A.5). The module is compliant with NIST SP 800-52 rev2 and the mechanism for IV generation is compliant with RFC 8446. The module ensures that it is strictly increasing and thus cannot repeat. When the IV exhausts the maximum number of possible values for a given session key, the first party, client or server, to encounter this condition may either trigger a handshake to establish a new encryption key in accordance with RFC 8446, or fail. In either case, the module prevents IV duplication and thus enforces the security property.

The module requires there to be a fixed field of 32-bits and defaults a value based on the HSM's unique serial number.

In approved mode, the module **shall not** allow the user to utilize GCM with an externally generated IV; a fresh key is always used. The module supports internal IV generation by the module's Approved DRBG. The DRBG seed is generated inside the module's physical boundary. The minimum IV length is 96-bits per NIST SP 800-38D. On module power on, the next IV available is calculated by taking the previously stored invocation value and adding an additional 8,000,000 to ensure the IV field is not reused, even after power cycling. This is following the guidance of SP800-38D section 9.1 which recommends that after a power loss the stored IV is always one or more values ahead of the operational invocation value.

3.2.   PCI HSM MODE OF OPERATION (NON-APPROVED)

In PCI HSM Mode of Operation, the module supports the following algorithms in addition to the FIPS Approved Mode algorithms:

- AKB/TR-31: key bundling techniques

- DUKPT: key management technique

- PIN generation: random and derived

- RSA with additional, non-compliant key sizes (full selection is 2048 + n*8 [n = 0 to 256], up to 4096 bits) for key generation, digital signature generation, and verification

- RSA with additional, non-compliant key sizes (full selection is 2048 + n*8 [n = 0 to 256] up to 4096 bits), encrypt/decrypt for key transport

- Triple-DES (keying option 2) for decryption, including key wrapping (non-compliant)

- Triple-DES (keying option 1) for encryption and decryption, including key wrapping (non-compliant)

   Note: The use of two-key Triple-DES for encryption is restricted. The total number of blocks of data encrypted with the same cryptographic key shall not be greater than 2^20.

- When configured for operation in an issuer environment*

   o   Clear PIN processing

   o   *The HSM cannot be configured for both PIN processing and clear PIN operations in this mode of operation.*

- When configured for PIN processing, the following pin block format translation will be allowed or disallowed.

		Destination						
		ISO Format 0	ISO Format 1	ISO Format 2	ISO Format 3	ISO Format 4	IBM3624	PIN Pad
Source	ISO Format 0	Yes	No	No	Yes	Yes	No	No
	ISO Format 1	Yes	Yes	Yes	Yes	Yes	No	No
	ISO Format 2	No	No	Yes	No	No	No	No
	ISO Format 3	Yes	No	No	Yes	Yes	No	No
	ISO Format 4	Yes	No	No	Yes	Yes	No	No
	IBM3624	Yes	Yes	Yes	Yes	Yes	Yes	Yes
	PIN Pad	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Table 4 - PIN Block Translation in PCI Mode of Operation

3.3.   GENERAL (NON-APPROVED) MODE OF OPERATION

In General (non-approved) Mode of Operation, the module supports the following algorithms in addition to the FIPS Approved Mode and PCI-HSM Mode algorithms:

- DES for encryption and decryption

- ECC with 192-bit keys for key generation, digital signature generation and verification (non-compliant)

- HMAC MD5, HMAC RIPEMD-160 for keyed message authentication

- MD5, RIPEMD-160 for hashing

- RSA with additional, non-compliant key sizes (full selection is 512 + n*8 [n = 0 to 256] up to 4096 bits) for key generation, digital signature generation, and verification

- RSA with additional, non-compliant key sizes (full selection is 512 + n*8 up to 4096 bits), encrypt/decrypt for key transport

- Triple-DES (2-key) for all usages without restriction (non-compliant)

- When configured for operation in an issuer environment*

    o Clear PIN processing

    o ***The HSM cannot be configured for both PIN processing and clear PIN operations in this mode of operation**

- When configured for PIN processing, the following pin block format translation will be allowed.

		Destination						
		ISO Format 0	ISO Format 1	ISO Format 2	ISO Format 3	ISO Format 4	IBM3624	PIN Pad
Source	ISO Format 0	Yes	Yes	Yes	Yes	Yes	Yes	Yes
	ISO Format 1	Yes	Yes	Yes	Yes	Yes	Yes	Yes
	ISO Format 2	Yes	Yes	Yes	Yes	Yes	Yes	Yes
	ISO Format 3	Yes	Yes	Yes	Yes	Yes	Yes	Yes
	ISO Format 4	Yes	Yes	Yes	Yes	Yes	Yes	Yes
	IBM3624	Yes	Yes	Yes	Yes	Yes	Yes	Yes
	PIN Pad	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Table 5 - PIN Block Translation in Non-Approved Mode of Operation

4. INSTALLATION

Each Futurex GSP3000 secure cryptographic device (SCD) contains a processor and system memory. The SCD stores keys and performs cryptographic processing tasks. GSP3000 units are FIPS 140-2 Level 3 validated under certificate number 3373.

Each SCD arrives with certificates loaded at the point of manufacture. These certificates are unique CAs specific to the customer, allowing the device to incorporate into that customer's architecture.

For security, the SCD comes encased in a hard, opaque epoxy barrier and sensor wires that protect the SCD from a physical attack. If the SCD is physically tampered with, the unit will enter a tampered state.

INSTALL PREPARATION

To facilitate installation, Futurex recommends that all shipment materials and at least two Administrators/Key Officers be present to maintain dual control.

EXCRYPT MANAGER APPLICATION INSTALLATION

Note This setup process is not required if the Excrypt Touch will be used to connect to the HSM.

This application is needed to load the Master File Key (MFK) and configure the HSM.

1. Power on the setup computer and insert the Excrypt Manager Application CD and run the Excrypt Manager installer. Follow the instructions given by the Excrypt Manager Setup Wizard.

2. Once the Excrypt Manager Application is running on the setup computer, power on the HSM.

3. Locate the power switch on the back of the device and turn it on.

4. Connect the USB setup cable after the HSM has completed the initial power-on process.

5. ENABLING FIPS AND PCI HSM MODES

The primary manner to configure the HSM is through the secure web interface. All configuration changes to the device are made through this TLS-secured interface.

FIPS and PCI HSM modes disable the non-secure management of the HSM and require that all configuration activity, including firmware updates, are completed using the Excrypt Manager.

Note: Port 443 or the HSM IP must be used to connect to the HSM while in PCI mode.

5.1. ENABLING THROUGH THE WEB INTERFACE

     1. Connect the HSM to the network and log in the two Crypto Officers.
     2. Change either FIPS Mode or PCI HSM Mode to Enabled.
     3. Click Update Mode. The HSM will reset, clear all keys, and resetting users to factory defaults. Once the device has rebooted, it is in the selected mode.

Note When switching between modes of operation, all sensitive information will be cleared, including all keys, critical security parameters (CSP), and user credentials.

Once PCI HSM mode has been activated, connection to the HSM may only be made via the Securus or through a web browser-based SSL/TLS (https) connection. Anonymous connections are disabled when in FIPS or PCI HSM mode.

Settings for these connections may be modified through the SSL/TLS tab in the Web Configuration Panel.

5.2.   COM SETUP

Once FIPS or PCI Mode of Operations has been activated, all serial ports will be disabled and the HSM must be connected to via a TLS-secured web connection. The COM Setup tab on the Dashboard will automatically have the normal contents removed in this situation.

FIGURE 4: WEB INTERFACE - COM SETUP PANEL

5.3.   ENABLING THROUGH EXCRYPT MANAGER

1. Log into Excrypt Manager using two Crypto-Officer identities for dual control.
1. Go to the Maintenance tab.
2. Under the Tools heading, use the drop-down menus next to the FIPS Mode and PCI-HSM Mode lines to choose between Off and On.
3. Click the Update Modes button.
4. A warning window will open to warn the user that enabling these modes will clear all keys and critical security parameters, remove all users, reset to factory defaults, and restart the HSM. To continue, click OK.
5. After enabling PCI or FIPS mode, the HSM will display a visual indicator in the bottom-right corner of the Excrypt Manager application.

6. RESET TO FACTORY DEFAULT

Futurex HSMs have two recessed switches, located on either side of the device's front plate. These switches allow users to reset the cryptographic module inside of the device, restore the unit to factory defaults, or to completely decommission the unit.

6.1.   RESET CRYPTOGRAPHIC MODULE

To reset the cryptographic module located inside the HSM:

1. Ensure the device is powered on.
2. Locate the switch inside the left-hand lock port.
3. Push the switch downwards and hold for one second and then release the switch.
4. After approximately five minutes and multiple automatic restarts, the cryptographic module will be reset.

Note During the reset process, the device will stop processing all API calls, including performing cryptographic operations.

6.2.   RESTORE DEVICE TO FACTORY DEFAULTS – HARDWARE METHOD

To restore the device to its factory default settings:

1. Ensure the device is powered on.
2. Locate the switch inside the left-hand lock port.
3. Push the switch downwards and hold for one second and then push the switch upwards and hold for 60 seconds.

4. After approximately five minutes and multiple automatic restarts, the HSM will reset to the original firmware and factory default settings.

7. PORTS AND INTERFACES

The cryptographic module provides one physical edge card connector (data in, data out, control in, status out, power) that allows for the following interfaces; the standard physical connectors (e.g., RJ45) are provided outside the boundary:

- RGMII/MDI(x2): control input, data input, data output, status output

    - Ethernet ports provide encrypted communication sessions established with the TLS protocol for control input, data input, data output, and status output.

- USB Host port (x1): Control input, data input, data output, status output

    - USB ports support encrypted data input/output, control input, and status output.

- USB Client port (x1): Control input, data input, data output, status output

    - USB ports support encrypted data input/output, control input, and status output. These ports are disabled in FIPS/PCI-HSM modes.

- Power status LED (x1): Status output

- Tamper status LED (x1): Status output

- Host ID Signal (x4): Control input

- Client ID Signal (x4): Status output

- USB enable port (x1): Status Output

- Client present port: Control input

- Primary Power port (x1): Power interface

- USB Power port (x1): Power interface

- Reset port: Control input

- Reset default port: Control input

- Battery detect port: Control input

- Battery power port: Power interface

- Ground port (x12): Power interface

8. IDENTIFICATION AND AUTHENTICATION POLICY

8.1. ASSUMPTION OF ROLES

The cryptographic module shall support Crypto-Officer and Crypto-User Identities. In FIPS or PCI HSM mode, a Crypto-Officer or Crypto-User identity may communicate with the cryptographic module via an established TLS session. The cryptographic module shall enforce the separation of roles using identity-based authentication for all roles.

For Crypto-Officer and Crypto-Users, an operator must enter their username and password to log in. The username is an alphanumeric string of 4 to 16 characters, and the password is an alphanumeric string of 8 to 64 characters chosen from the 95 printable and human-readable ASCII characters (0x20 to 0x7E) excluding the following: '[ ]<>;' (thus, 90 characters are possible). Default passwords are only used for the default identities and must be updated upon initial login. An identity that provides a valid username and password will be identified as an Crypto-Officer or Crypto-User and must re-authenticate to change identity or role. The operator may end the session by logging out or power cycling the module, or the session shall automatically timeout after a fixed duration or transaction limit. To re-establish communication, an operator must re-authenticate.

All cryptograms used while processing transactions contain authentication data for the Transaction Processing role, which take the form of key parity bits for KWP for AES. In either case, the symmetric key (AES) which is used to encrypt the cryptogram corresponds to the operator's identity. For AES-wrapped keys, the key is auth-decrypted according to SP800-38F (KWP); if this operation fails, the command is rejected.

8.2. ROLES AND REQUIRED IDENTIFICATION AND AUTHENTICATION

Role	Type of Authentication	Authentication Mechanism
Crypto-Officer	Identity-based	Username and password
		ID of wrapping key and wrapped key (KWP/Key Parity)
Crypto-User	Identity-based	Username and password
		ID of wrapping key and wrapped key (KWP/Key Parity)
Customizable User Identity	Identity-based	Username and password
		ID of wrapping key and wrapped key (KWP/Key Parity)

Table 6 - Roles and Required Identification and Authentication

8.3.   STRENGTHS OF AUTHENTICATION MECHANISMS

Authentication Mechanism	Strength of Mechanism
Username and Password	The probability that a random attempt will succeed or a false acceptance will occur is 1/4,304,672,100,000,000 (1/90^8). The module allows for three (3) failed attempts and then times out for 20 seconds before retry. The worst-case scenario is that there are 150 attempts in a one-minute period. The probability of successful authenticating to the module within one minute is 1/478,296,900,000,000 (9/90^8).
AES-KWP	AES-KWP (SP800-38F) provides 64 bits of authentication strength to a wrapped key. Thus, the probability that a random attempt will succeed or a false acceptance will occur is 1/18,446,744,073,709,551,616 (1/2^{64}). The module allows for 50 failed attempts over 24 hours and then times out for 20 seconds before retry. The worst-case scenario is that there are 150 attempts in a one-minute period. The probability of successfully authenticating to the module within one minute is 1/122,978,293,824,730,344 (150/2^{64}).
Key Parity (3-key Triple-DES)	3-key Triple-DES has 24 parity bits. Thus, the probability that a random attempt will succeed, or a false acceptance will occur is 1/16,777,216 (1/2^{24}) The module allows for 50 failed attempts over 24 hours and then times out for 20 seconds before retrying. The worst-case scenario is that there are 150 attempts in a one-minute period. The probability of successfully authenticating to the module within one minute is 1/111,848 (150/2^{24}). **Note: TDES operations are not permitted in FIPS Mode of Operation, likewise Key Parity with 3-key Triple DES is not permitted in FIPS Mode of Operation.*

Table 7 – Strength of Authentication Mechanisms

9. ACCESS CONTROL POLICY

9.1.   UNAUTHENTICATED SERVICES

The cryptographic module supports the following unauthenticated services:

- Status: This service provides the current status of the cryptographic module via the USB or Ethernet port.

- Self-Tests: This service will enable an operator to initiate the suite of self-tests via power cycling the module.

- Factory Reset: This service resets the module back to factory default. (Zeroize CSPs. Passwords are zeroized and set back to default. Firmware is also restored to version shipped with HSM.)

- Tamper: There are pins on the HSM that will allow the user to force a tamper event by shorting them. This will zeroize all CSPs to include default TLS pairs.

9.2.   AUTHENTICATED SERVICES

Identity	Authorized Service
Crypto-Officer:	• Create Session: This allows an operator to create a secure session to the HSM. • Authenticate: This service allows an operator to send credentials to be authenticated by the cryptographic module. Sessions will timeout after one minutes of inactivity, fifteen minutes of use, or 7,500 transactions. • Destroy Session: This service allows a Crypto-Officer to transition the cryptographic module into or out of an Approved mode. This service shall zeroize the module and restart. If the module is already in an Approved mode, it will remain in that Approved mode. • Initialization: This service zeroizes and generates Server Private and Public Key • Zeroize: This service shall enable a Crypto-Officer to destroy critical security parameters by zeroization. • Key Loading: This service allows a Crypto-Officer to load keys into the module. • *Update Firmware: This service shall enable the Crypto-Officer to update the cryptographic module's firmware. Firmware authenticity is verified using an ECC signature. If the authenticity of the firmware is not confirmed, the cryptographic module will reject and delete the update. • General Configuration: This service allows a Crypto-Officer to change all configuration options for the module. • View Configuration: Gives operator the ability to view configuration status to include IP, COM, SSL, Time, Features, Users, IP tools, and Logs. This does not allow configuration changes of these items. • Configuration: Allows operator to change IP address, syslog level, and reboot the device. • User Administration: This service will allow the Crypto-Officer to create, manage, and delete users. • Logout: This service will enable the Crypto-Officer to end authentication. • Load Encrypted Key: This service allows a user to send in Encrypted Keys and have the keys translated and stored in the key table or returned as a cryptogram encrypted under the master key. • Process Transactions: This service allows a user to use any of the commands listed in the Futurex TRM. These commands must be unblocked by the Crypto-Officer for Use. ***Note:** *New firmware versions within the scope of this validation must be validated through the FIPS 140-2 CMVP. Any other firmware loaded into this module is out of scope of this validation and require a separate FIPS 140-2 validation.*
Crypto-User	• Create Session: This service allows a user to create a secure session to the HSM. • Destroy Session: This allows a user to end the session. • Authenticate: This service allows a user to send credentials to be authenticated by the cryptographic module. • View Configuration: Gives operator the ability to view configuration status to include IP, COM, SSL, Time, Features, Users, IP tools, and Logs. This does not allow configuration changes of these items. • Configuration: Allows operator to change IP address, syslog level, and reboot the device. • Logout: This service will enable the Crypto-Operator to end authentication.

	• Load Encrypted Key: This service allows a user to send in Encrypted Keys and have the keys translated and stored in the key table or returned as a cryptogram encrypted under the master key. • Process Transactions: This service allows a user to use any of the commands listed in Futurex TRM. These commands must be unblocked by the Crypto-Officer for use.

Customizable User Identity	• Configurable Services based on permissions that make up the identities.
	• This Customizable Identity will always be able to perform the following services:
	    o Create Session: This service allows a user to create a secure session to the HSM.
	    o Destroy Session: This allows a user to end the session.
	    o Authenticate: This service allows a user to send credentials to be authenticated by the cryptographic module.
	    o Logout: This service will enable the Crypto-Officer to end authentication.
	• These Crypto-User services may be given to the Customizable User Identity by authenticated Crypto-Officers under dual-control.
	    o Load Encrypted Key: This service allows a user to send in Encrypted Keys and have the keys translated and stored in the key table or returned as a cryptogram encrypted under the master key (Commands must be unblocked by Crypto-Officer).
	    o Process Transactions: This service allows a user to use any of the commands listed in Futurex TRM. These commands must be unblocked by the Crypto-Officer for use (Commands must be unblocked by Crypto-Officer. By default, GHSH command for approved SHA security functions available).
	• If any of the following services are present the Customizable User Identity *assumes the responsibility of Crypto Officer*: Requiring dual-control, identity-based, authentication. These services may only be given to the Customizable User Identity by authenticated Crypto-Officers under dual-control.
	    o Zeroize: This service shall enable a Crypto-Officer to destroy critical security parameters by zeroization.
	    o Key Loading: This service allows a Crypto-Officer to load keys into the module.
	    o *****Update Firmware: This service shall enable the Crypto-Officer to update the cryptographic module's firmware. Firmware authenticity is verified using an ECC signature. If the authenticity of the firmware is not confirmed, the cryptographic module will reject and delete the update.
	    o General Configuration: This service allows a Crypto-Officer to change all configuration options for the module.
	    o User Administration: This service will allow the Crypto-Officer to create, manage, and delete users.
	    o Configuration: Allows operator to change IP address, syslog level, and reboot the device
	*Note: *New firmware versions within the scope of this validation must be validated through the FIPS 140-2 CMVP. Any other firmware loaded into this module is out of scope of this validation and require a separate FIPS 140-2 validation.*

Table 8 - Authorized Services by Role

9.2.1.   Specification of Service Inputs and Outputs

Service	Control Input	Data Input	Data Output	Status Output
Create Session	Header Info	Signed Plaintext Data	Encrypted Data	N/A
Authenticate	Header Info	Username & Password	N/A	Success / Fail
Destroy Session	Header Info	N/A	N/A	N/A
Process Transactions	Header Info	Encrypted Data	Encrypted Data	Plaintext Status Data
Logout	Header Info	N/A	N/A	N/A
Status	N/A	N/A	N/A	Plaintext Status Data
Initialization	Header Info	Encrypted Data	Encrypted Data	Success / Fail
Zeroize	Header Info	N/A	N/A	Success / Fail
Self-Tests	N/A	N/A	N/A	Success / Fail
User Administration	Header Info	Encrypted Data	Encrypted Data	Plaintext Status Data
Update Firmware	Header Info	Encrypted Data	Encrypted Data	Plaintext Status Data
Factory Reset	Header Info	N/A	N/A	Success
View Configuration	Header Info	N/A	N/A	Plaintext Status Data
Configuration	Header Info	N/A	N/A	Success/Fail
General Configuration	Header Info and Configuration Options	N/A	N/A	Success/Fail
Tamper	Tamper Signal	N/A	N/A	Tamper
Key Loading	Header Info	Encrypted Data	Encrypted Data	Plaintext Status Data
Load Encrypted Key	Header Info	Encrypted Data	Encrypted Data	Plaintext Status Data

Table 9 - Specification of Service Inputs & Outputs

9.3.   DEFINITION OF CRITICAL SECURITY PARAMETERS (CSPS)

CSPs are secured within the cryptographic boundary. Operators do not have direct access to CSPs within the device. The following are CSPs contained in the module:

CSP	Type	Description
Unique Device Keys	AES-256	Encryption and Decryption of TLS Private Keys
Virtual UDKs	AES-256	Encryption and Decryption of TLS Private Keys
Global Derivation Key	AES-256	Used to derive Master Key Encryption Key and Virtual Firmware Key
Virtual Global Derivation Key	AES-256	Derivation key
Master Key Encryption Key (MKEK)	AES-256	Encryption and Decryption of master keys
Server Private Keys[4]	ECC-521 RSA-2048	Sign or Decrypt data sent to the device from an operator during the creation of a TLS session. Used during creation of a TLS session.
Session Encryption Key	AES-128 AES-256	Encrypts / Decrypts data passed between an operator and the device during an established TLS session
Session Hash Key	HMAC-SHA-1 HMAC-SHA-256 HMAC-SHA-384 HMAC-SHA-512	Key size minimum of 128-bits and maximum of 256-bits enforced in secure modes of operation. Used for hashing data passed between an operator and the device during an established TLS session.
Pre-Master Secret	Keying Material	Used to create the TLS session keys
Maser Secret	AES-256	Used for TLS, destroyed at the end of each TLS Session
DH/ECDHE Private Key	ECC-521 DH-2048	Used for DH/ECDHE TLS exchange
Ephemeral Asymmetric Key	RSA 2048 or ECC 521	Used to transfer Ephemeral Key between HSM's for component transfer

---

[4] Server Private Keys in the CSP table represents a combination of Customer Admin, Customer Admin App, Customer Prod App, Customer Prod Excrypt, and Customer Prod International Private Keys in one line item to conserve space/paper.

Ephemeral Symmetric Key	AES 256	Used to encrypt key components
Crypto-Officer Password	Passphrase	Used to authenticate the identity of a Crypto-Officer.
Crypto-User Password	Passphrase	Used to authenticate the identity of a Crypto-Operator.
Customizable User Identity Password	Passphrase	Used to authenticate the identity of a Customizable User Identity
Platform Master Key	AES 256	Used to encrypt User Keys and Ephemeral Asymmetric keys
Pending Master File Key	AES-256	Used for rotation of master keys. Not used to encrypt/decrypt any data until it is ready to replace master keys.
FTK Key	AES 256	Used to encrypt AES keys for PKCS #11
Key Exchange Key	AES 256	Used to load User Keys as part of Transaction Processing (key transport)
Backup Key	AES 256	Encrypts the User Keys for backup (key transport)
Smart Card Encryption Key	AES 256	Wraps smart card fragments (keys and other sensitive data) for storage on smart card.
User Keys	RSA 1024*, 2048, 3072 AES 128, 192, 256 ECC 192***, 224, 256, 384, 521 HMAC	Data encryption, key exchange, CMAC, and HMAC keys used by user. These keys are available to Crypto Officer and Crypto-Operator roles.
Seed Value	NDRNG value	Seed for CTR DRBG.
Seed Key (DRBG State)	Internal RNG state	"V" and "Key" internal values for CTR DRBG.
HSM Signing Private Key	RSA 2048	Used to sign the logs when output
Virtual Firmware Key	AES-256	Unique Virtual HSM Firmware Key used to encrypt and decrypt the UDK and GDK of individual virtual HSMs

Table 10 - Critical Security Parameters

NOTE: *RSA 1024 can only be used for verification.*

***NOTE:* *ECC 192 can only be used for verification.*

9.4.   DEFINITION OF PUBLIC KEYS

The following are the public keys contained in the module:

- Firmware Public Keys (ECC 521): These public keys are used for signature verification of the firmware and firmware updates to protect against unauthorized modification.

- Customer Admin Public Keys (RSA 2048/ECC 521): The public keys components of the Administration certificates used for verifying signatures. This corresponds to one of the server private keys.

- Customer Production Excrypt Public Keys (RSA 2048/ECC 521): The public keys components of the Production Excrypt certificates used for verifying signatures. This corresponds to one of the server private keys.

- Customer Production International Public Keys (RSA 2048/ECC 521): The public keys components of the Production International certificates used for verifying signatures. This corresponds to one of the server private keys.

- Customer Production Web Public Keys (RSA 2048/ECC 521): The public keys components of the Production Web certificates used for verifying signatures. This corresponds to one of the server private keys.

- Customer App Administration Public Keys (RSA 2048/ECC 521): The public keys components of the Application Administration certificates used for verifying signatures. This corresponds to one of the server private keys.

- Customer App Production Public Keys (RSA 2048/ECC 521): The public keys component of the Application Production certificates used for verifying signatures. This corresponds to one of the server private keys.

- User Public Keys (RSA 2048-4096, ECC 192/224/256/384/521): These public keys are always used by the operator.

- HSM Signing Public Key (RSA 2048): Output to allow host to verify log signature.

- DH Public Key (DH 2048/ECC 521): Used for TLS key exchange

9.5.   MODES OF ACCESS FOR CSPS

Table 11 provides a list of supported access operations by the cryptographic module. Access rights for the supported modes of access are shown in Table 12 below. Supported Access operations are defined as follows:

- Generate functions: These operations generate a particular CSP within the cryptographic module.

- Load functions: These operations allow for a particular CSP to be loaded into the cryptographic module.

- Wrap functions: These operations encrypt a particular CSP.

- Un-wrap functions: These operations decrypt a particular CSP.

- Destroy functions: These operations erase the CSP from the cryptographic module.

CSP	Operation				
	Generate	**Load**	**Wrap**	**Un-wrap**	**Destroy**
Unique Device Keys	X		X	X	X
Virtual UDKs	X		X	X	X
Global Derivation Key	X				X
Virtual Global Derivation Key	X				X
Master Key Encryption Key	X		X	X	X
Server Private Keys	X				X
Session Encryption Key	X		X	X	X
Session Hash Key	X		X	X	X
Pre-Master Secret	X				X
Master Secret	X				X
DHE/ECDHE Private Key	X				X
Ephemeral Asymmetric Key	X		X	X	X

Ephemeral Symmetric Key	**x**		**x**	**x**	**x**
Crypto-Officer Password		**x**			**x**
Crypto-User Password		**x**			**x**
Customizable User Identity Password		**x**			**x**
Platform Master Key (PMK)		**x**	**x**	**x**	**x**
FTK Key		**x**	**x**	**x**	**x**
Key Exchange Key (KEK)		**x**	**x**	**x**	**x**
Backup Key		**x**	**x**	**x**	**x**
Smart Card Encryption Key (SCEK)		**x**	**x**	**x**	**x**
User Keys		**x**	**x**	**x**	**x**
Seed Value	**x**				**x**
Seed Key (DRBG State)	**x**				**x**
HSM Signing Private Key	**x**				**x**
Virtual Firmware Key	**x**		**x**	**x**	**x**

Table 11 - Supported Operations

Note: Unique Device Key is generated at time of manufacture or re-generated during tamper recovery and is not associated with any user roles.

Cryptographic Keys and CSPs Access Operation	Service	Crypto-Officer	Crypto-User	U/A*
Generate Session Encryption and Hash keys *(Session Encryption Key, Session Hash Key, Pre-Master Secret, Server Private Keys, DHE/ECDHE Private Keys)*	Create Session	**x**	**x**	

Wrap and un-wrap with Session Encryption and Hash keys *(Session Encryption Key, Session Hash Key, Pre-Master Secret, Master Secret)*	Process Transactions	X	X	
Destroy Session Encryption and Hash keys *(Session Encryption Key, Session Hash Key, Pre-Master Secret, Master Secret)*	Destroy Session	X	X	
(No CSP access)	Status			X
Generate Ephemeral Keys; Wrap and un-wrap with Ephemeral Keys *(Ephemeral Symmetric, Ephemeral Asymmetric)*	Key Loading	X		
Destroy Ephemeral Keys *(Ephemeral Symmetric, Ephemeral Asymmetric)*	Key Loading (upon completion)	X		
Destroy Keys *(Global Derivation Key, Virtual Global Derivation Key, Master Key Encryption Key, Server Private Keys, DHE/ECDHE Private Keys, Crypto-Officer Password, Crypto-User Password, Customizable User Identity Password, PMK, FTK, KEK, Backup Key, SCEK, User Keys, HSM Signing Private Key, Virtual Firmware Key)*	Zeroize	X		
Zeroize and generate Server Private and Public Key *(Unique Device Key, Virtual UDK, Global Derivation Key, Virtual Global Derivation Key, Master Key Encryption Key, Server Private Keys, DHE/ECDHE Private Keys, Seed Value, Seed Key, HSM Signing Private Key)*	Initialization	X		
Zeroize all CSPs *(All CSPs listed in table 11 are cleared and actively zeroized upon detection of a tamper event)*	Tamper			X
(No CSP access)	Self-Tests			X
Load or Destroy Usernames/Passwords *(Crypto-Officer Password, Crypto-User Password, Customizable User Identity Password)*	User Administration	X		
Verify with Firmware Public Key	Update Firmware	X		

Zeroize CSPs and restore factory defaults** *(Global Derivation Key, Virtual Global Derivation Key, Master Key Encryption Key, Server Private Keys, DHE/ECDHE Private Keys, Crypto-Officer Password, Crypto-User Password, Customizable User Identity Password, PMK, FTK, KEK, Backup Key, SCEK, User Keys, HSM Signing Private Key, Virtual Firmware Key)*	Factory Reset			**X**
Send in authentication credentials *(Crypto-Officer Password, Crypto-User Password, Customizable User Identity Password)*	Authenticate	**X**	**X**	
No CSP access	Logout	**X**	**X**	
No CSP access	General Configuration	**X**		
No CSP access	Configuration	**X**		
No CSP access	View Configuration	**X**	**X**	
Loading of PMK, FTK, KEK, Backup Key, SCEK, User Keys *(Global Derivation Key, Virtual Global Derivation Key, Master Key Encryption Key, Crypto-Officer Password, Customizable User Identity Password, PMK, FTK, KEK, Backup Key, SCEK, User Keys)*	Key Loading	**X**		
Loading of Encrypted User Keys *(Global Derivation Key, Virtual Global Derivation Key, Master Key Encryption Key, Crypto-Officer Password, Crypto-User Password, Customizable User Identity Password, User Keys)*	Load Encrypted Key	**X**	**X**	

Table 12 - CSP Access Rights within Roles & Services

*NOTE 1: *U/A = Unauthenticated services typically available with physical access (e.g. power cycle, view LCD)*

**NOTE 2: *The Factory Reset service does not zeroize the UDK (only a Tamper does that). If the UDK has been previously zeroized by a tamper event, the Factory Reset service generates a new UDK.*

10.   OPERATIONAL ENVIRONMENT

The FIPS 140-2 Area 6 Operational Environment requirements are not applicable because the cryptographic module supports a non-modifiable operational environment.

11.   SECURITY RULES

The cryptographic module's design corresponds to the cryptographic module's security rules. This section documents the security rules enforced by the cryptographic module to implement the security requirements of this FIPS 140-2 Level 3 module.

1. The cryptographic module **shall** provide two distinct operator roles. These are the Crypto-Officer role, and the Crypto-User role.

    i.   Customizable rolls **shall** assume classification of one of the two roles mentioned above and in section 6.2

2. The cryptographic module **shall** provide identity-based authentication.

3. When the module has not been placed in a valid role, the operator **shall not** have access to any cryptographic services.

4. The cryptographic module **shall** encrypt message data using an approved TLS cipher suite when TLS is used.

5. The cryptographic module **shall** perform the Power-Up and Conditional self-tests as specified in section 8.1 below.

6. The cryptographic module **shall** clear previous authentications on power off/cycle.

7. Any time the cryptographic module is in an idle state, the operator **shall** be capable of commanding the module to perform the Power-Up self-test.

8. Prior to each use, the DRBG **shall** be tested using the conditional test specified in FIPS 140-2 §4.9.2.

9. Data output **shall** be logically inhibited during key generation, self-tests, zeroization, and error states using separate system processes.

10. Zeroization **shall** clear all CSPs in at most one-tenth of a second.

11. Status information **shall not** contain CSPs or sensitive data that if misused could lead to a compromise of the module.

12. The module **shall not** support the update of the logical serial number or vendor ID.

13. If the cryptographic module remains inactive in any valid role for a maximum period of five minutes, the module **shall** automatically log-out the operator.

11.1. SELF-TESTS

In all Modes of Operation, the cryptographic module will perform power-up self-tests without operator intervention. Self-tests may also be executed at the request of an operator by power cycling the module. When power cycling the module, no operator intervention is required before self-tests are performed. If a self-test fails, the device will transition to the Fatal Error state and report an error which is observed on the LCD screen of the parent device. If all tests pass, the module powers up normally and reports All Self-Tests Passed on the LCD screen of the parent device.

Power-Up and Periodic Self Tests

The following tests shall be performed at power-up:

- Firmware integrity and authenticity tests (ECDSA P-521 signature) are performed in all modes of operation.

- Known answer tests are executed in FIPS and PCI modes of operation for:

  o AES-KWP (NIST AES-KWP Cert.#C1992)

    ▪ AES key sizes 128, 192, and 256-bits used for KWP self-tests

  o AES Encrypt and Decrypt (NIST AES Cert. #C1991)

    ▪ AES key size of 256-bits used for AES self-tests

      • Modes Tested: CBC, CFB1, CFB128, CFB8, ECB, OFB

    ▪ AES key size of 128-bits is used for the AES self-test

      • Modes Tested: CTR

  o AES-CMAC Generate and Verify (NIST AES-CMAC Cert. #C1991)

    ▪ AES key size of 128, 192, and 256-bits used for AES-CMAC self-tests

  o AES-GCM Encrypt and Decrypt (NIST AES-GCM Cert. #C1991)

    ▪ AES key size 256-bits used for AES-GCM self-tests

  o DRBG Known Answer (NIST Counter DRBG Cert. #C1991)

    ▪ DRBG KAT performed with 256-bit output.

  o ECC Sign and Verify (NIST ECDSA Cert. #C1991)

    ▪ ECC key sizes of 224, 256, 384, and 521-bits used for ECC sign/verify self-tests

  o HMAC SHA1/SHA224/SHA256/SHA384/SHA512 (NIST HMAC Cert. #C1991)

  o KDF Counter Mode using CMAC (NIST KDF Cert. #C1992)

    ▪ AES key sizes of 128, 192, 256-bits used for KDF using CMAC self-tests

  o RSA Sign and Verify (NIST RSA Cert. #C1991)

    ▪ RSA Modulus of 2048-bits used for self-test

  o SHA1/SHA224/SHA256/SHA384/SHA512 (NIST SHS Cert. #C1991)

      o   Triple-DES CMAC Generate and Verify[5]

      o   Triple-DES Keying Option 1 and 2 Encrypt and Decrypt (NIST TDES Cert. #C1991)

Conditional Self-Tests

The device will perform the following conditional self-tests:

- Firmware load test (ECC signature verification) is performed in all modes of operation.
- The following conditional self-tests are executed in FIPS and PCI modes of operation

  - Continuous random number generator tests for NDRNG and DRBG.

  - DRBG Health Checks (SP800-90A §11.3)

  - Pairwise consistency test for RSA, ECC key generation

  - Firmware load test (ECDSA signature verification)

12. PHYSICAL SECURITY POLICY

12.1. PHYSICAL SECURITY MECHANISMS

The multi-chip embedded cryptographic module includes the following physical security mechanisms:

- Hard, opaque potting material encapsulates the body of the module, and intrusion attempts will result in serious damage which will cause the module to stop functioning. (More gentle attempts will scratch the potting, leaving evidence of a tamper attempt.)

- The module is protected by a tamper sensing envelope, which responds to physical tampering with CSP zeroization.

- Environmental monitoring sensors will trigger a tamper response and CSP zeroization to prevent the module from being compromised from altering certain environmental or operational conditions.

12.2. ENVIRONMENTAL CONDITIONS AND ENVIRONMENTAL FAILURE PROTECTION

The following environmental conditions should be maintained for the module:

- Operating environment temperature: -40 to 60°C
- Storage temperature: -40 to 85°C

Environmental Failure Protection will trigger a shutdown or tamper response should the module detect environmental conditions outside of these specifications:

- Temperature: -40 to 85°C
- Voltage: 5.77 VDC at Primary and USB Power port
- Voltage: 2.41 to 3.58 VDC at Battery Power port.

12.3. OPERATOR RECOMMENDED ACTIONS

The operator may be required to periodically inspect the unit for forced entry.

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

---

[5] Triple-DES algorithms are only performed in FIPS Mode of Operation when executing a power-up, on-demand, or daily self-tests.

Tamper Evident Potting	Monthly, and prior to module Initialization	Inspect hard potting for removal/penetration attempts.

Table 13 - Inspection / Testing of Physical Security Mechanisms

The figures below show the module with its tamper evident potting intact, and a sample of the potting after a tamper attempt has been made.

Figure 2 – EXP1000 with its Tamper Potting Intact
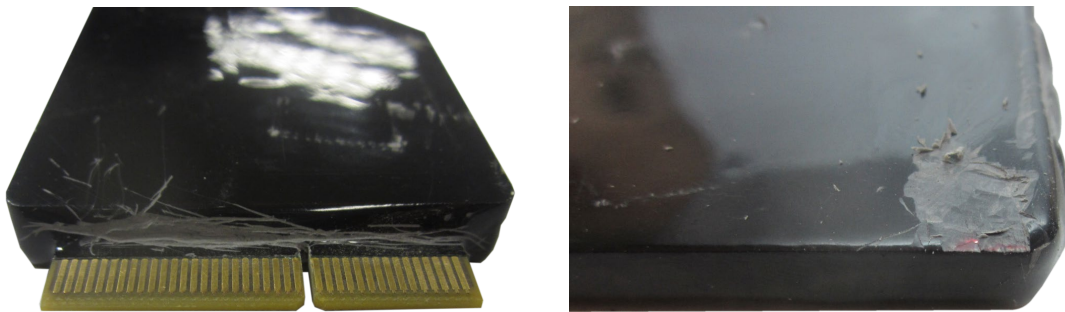
Figure 3 – Examples of Tamper Attempts on the EXP1000 Potting

13. MITIGATION OF OTHER ATTACKS

The module mitigates the Simple Power Analysis (SPA) and Differential Power Analysis (DPA) attacks by emitting compromising emanations through suppression and containment of side channel signals. The module's physical enclosure functions as a Faraday cage to attenuate such signals.

The module also provides Partial Environmental Failure Protection, as described in Section 9.

14. DESIGN ASSURANCE

14.1. CONFIGURATION MANAGEMENT

Documentation for the cryptographic module, which includes hardware specifications, firmware source code, guidance documents, and FIPS documents, is maintained using a version control repository. All configuration management items are uniquely identified by a path and filename within the repository. All configuration management items within the version control repository are uniquely identifiable.

14.2. GUIDANCE DOCUMENTS

Provided with the cryptographic module are all Crypto-Officer and user guidance documents that specify the following:

- Administrative functions, physical ports, and interfaces
- Procedures describing how to securely administer the cryptographic module
- Approved security functions
- User responsibilities for securely operating the cryptographic module

14.3. SYSTEM IDENTIFICATION AND AUTHENTICATION

Procedures for system identification and authentication of the module are detailed in the Futurex PCI HSM User Guide Addendum.

14.4. AUDIT LOGS AND INSPECTION FREQUENCY

Understanding of the operation and initialization of the module is requisite to configure logging. Procedures to configure audit logging are detailed in the Futurex PCI HSM User Guide Addendum.

- The module supports secure logging of transactions, data, and events to enable auditing
- Operator restrictions for accessing, archiving, or deleting logs are configured by settings and policies established by system administrators
- Logs should be audited on a daily basis, and an appropriate notification tree should be established for escalating and investigating any suspicious log activity
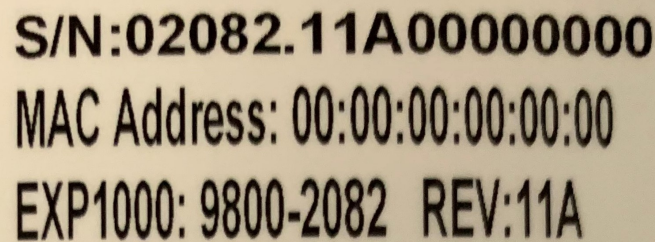
15. KEY LOADING

15.1. KEY LOADING (FIPS/PCI-HSM MODES)

When operating in FIPS or PCI-HSM Modes, all key loading traffic to HSM must be encrypted. This is accomplished by using a Futurex Excrypt Touch. The Excrypt Touch is a fully functional TRSM that will encrypt all data between it and the HSM using TLS.

16. PRODUCT IDENTIFICATION

16.1. HARDWARE IDENTIFICATION

To identify an EXP1000, refer to the product identification label. Refer to Figure 1 for the location of the product identification lable. Figure 4 shows the product identification label. Note that the EXP1000 may be identified by the part number 9800-2082 or 9850-0365.
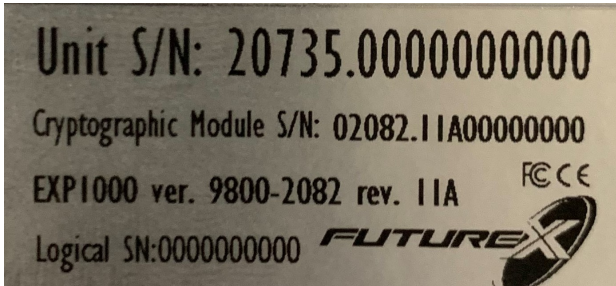
Figure 4 – EXP1000 Product Identification Label

The EXP1000 is typically sold as an embedded component inside of other Futurex devices and its product identification label is not visible without opening the chassis. Internal inspection is not possible without specialized tools only available to authorized service technicians. As such, Futurex places product identification labels on the exterior of all chassis that support the EXP1000. Figure 5 shows an example of a chassis label that references the existence of an embedded EXP1000.

Figure 5 – Chassis Label

Figure 6 through Figure 8 show typical placements of chassis labels.

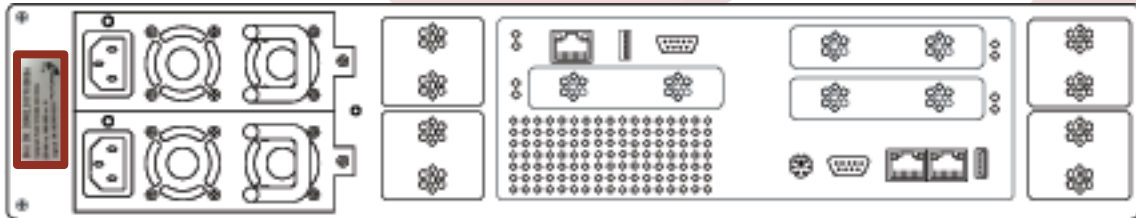*Figure 6 – 1U Chassis Label Location*
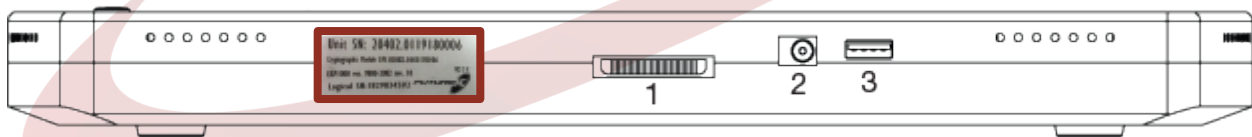

Figure 7 – 2U Chassis Label Location

Figure 8 – Securus 2 Label Location

16.2. FIRMWARE VERSIONING SCHEME AND IDENTIFICATION

The firmware version is made of four components concatenated with periods in the form of *Major.Audit.Branch.Release* where:

- Major - The major number shall only be incremented when large scale changes have been made to the release in question. Its value will be updated when Futurex believes the scope of the changes warrants an update.

- Audit - The audit number shall only be incremented when changes have been made that require an additional PCI security audit or when the firmware is submitted for audit to an independent lab.

- Branch - This is incremented when a new branch is created. These changes are non-security related.

- Release - This is incremented when a new release happens off a branch. These changes are non-security related.

The firmware version can be found on the LCD screen, web portal, or in Excrypt Manager. Please refer to the images below for reference. Also, provided in this view is the enabled feature identifier that may be concatenated to the end of the firmware version and indicated by one or more of the following characters: 'i' International Restriction Crypto, 'c' Clear PIN Support, or 'k' RSA Support.

Figure 9 - Firmware Version through Web Portal

Figure 10 - Firmware Version through Excrypt Manager

17.   TLS PROTOCOLS

17.1.   TLS PROTOCOLS SUPPORTED

The list below contains all the TLS Protocols supported.

- TLS_AES_128_GCM_SHA256

- TLS_AES_256_GCM_SHA384

- TLS_DHE_RSA_WITH_AES_128_CBC_SHA

- TLS_DHE_RSA_WITH_AES_256_CBC_SHA

- TLS_DHE_RSA_WITH_AES_128_CBC_SHA256

- TLS_DHE_RSA_WITH_AES_256_CBC_SHA256

- TLS_DHE_RSA_WITH_AES_128_GMC_SHA256

- TLS_DHE_RSA_WITH_AES_256_GMC_SHA256

- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA

- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384

- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384

Note: The TLS protocol, other than the KDF, have not been tested by the CMVP or CAVP as per FIPS 140-2 Implementation Guidance D.11

Note: TLS ciphers that utilize FFC key agreement use the following Safe Prime Groups: ffdhe2048 (ID = 256), ffdhe3072 (ID = 257), ffdhe4096 (ID = 258) as specified in SP800-56A rev3 Appendix D and RFC 7919

18. REFERENCES

1. FIPS PUB 140-2, *Security Requirements for Cryptographic Modules,* National Institute of Standards and Technology, 2001 May 25.
2. Annex A: Approved Security Functions for FIPS PUB 140-2, *Security Requirements for Cryptographic Modules,* Draft, National Institute of Standards and Technology, 2019 June 10.
3. Annex B: Approved Protection Profiles for FIPS PUB 140-2, *Security Requirements for Cryptographic Modules,* Draft, National Institute of Standards and Technology, 2019 June 10.
4. Annex C: Approved Random Number Generators for FIPS PUB 140-2, *Security Requirements for Cryptographic Modules,* Draft, National Institute of Standards and Technology, 2019 June 10.
5. Annex D: Approved Key Establishment Techniques for FIPS PUB 140-2, *Security Requirements for Cryptographic Modules,* Draft, National Institute of Standards and Technology, 2020 August 10.
6. Derived Test Requirements for FIPS PUB 140-2, *Security Requirements for Cryptographic Modules,* Draft, National Institute of Standards and Technology, 2004 March 24.
7. Implementation Guidance for FIPS PUB 140-2 and the Cryptographic Module Validation Program, National Institute of Standards and Technology, 2020 August 28
8. NIST Special Publication 800-38D, *Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC,* National Institute of Standards and Technology, November 2007
9. NIST Special Publication 800-38F, *Recommendation for Block Cipher Modes of Operation: Methods for Key Wrapping,* National Institute of Standards and Technology, December 2012
10. NIST Special Publication 800-52 Rev2, *Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations,* National Institute of Standards and Technology, August 2019
11. NIST Special Publication 800-56A Rev3, *Recommendation for Pair-Wise Key-Establishment Using Integer Factorization Cryptography,* National Institute of Standards and Technology, April 2018
12. NIST Special Publication 800-56C Rev2, *Recommendation for Pair-Wise Key-Establishment Using Integer Factorization Cryptography,* National Institute of Standards and Technology, April 2018
13. NIST Special Publication 800-90A Rev.1, *Recommendation for Random Number Generation Using Deterministic Random Bit Generators,* National Institute of Standards and Technology, June 2016
14. ANSI X9.31-1998, *Digital Signature using Reversible Public Key Cryptography for the Financial Services Industry (rDSA),* Accredited Standards Committee X9, Inc., 1998.
15. The RSA Validation System (RSAVS), National Institute of Standards and Technology, 2004 November 09.
16. FIPS PUB 180-2 with Change Notice 1, *Secure Hash Standard (SHS),* National Institute of Standards and Technology, 2004 February 25.
17. The Secure Hash Algorithm Validation System (SHAVS), National Institute of Standards and Technology, 2004 July 22.
18. FIPS PUB 198-1, *The Keyed-Hash Message Authentication Code (HMAC),* National Institute of Standards and Technology, 2002 March 06.
19. The Keyed-Hash Message Authentication Code Validation System (HMACVS), National Institute of Standards and Technology, 2004 December 03.

19. GLOSSARY

Term	Definition
ANSI	American National Standards Institute
CA	Certificate Authority
CO	Cryptographic Officer
CRC	Cyclic Redundancy Check
CSP	Critical Security Parameter
DES	Data Encryption Standard
DRBG	Deterministic Random Bit Generator
ECC	Elliptic Curve Cryptography (i.e. ECDH, ECDSA)
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
FIPS	Federal Information Processing Standard
FIPS PUB	Federal Information Processing Standards Publication
GCM	Galois/Counter Mode
HMAC-SHA-1	Keyed-Hash Message Authentication Code using SHA-1
I²C	Inter-Integrated Circuit
IP	Internet Protocol
LCD	Liquid Crystal Display
MD5	Message Digest 5
NDRNG	Non-Deterministic Random Number Generator
NIST	National Institute of Standards and Technology
RNG	Random Number Generator
RSA	Rivest-Shamir-Adelman public key algorithm
SHA	Secure Hash Algorithm
SHS	Secure Hash Standard

Table 14 - Glossary

20. CSP ABBREVIATIONS

Term	Definition
KEK	Key Exchange Key
PMK	Platform Master Key
MKEK	Master Key Encryption Key
GDK	Global Derivation Key
BEK	Backup Encryption Key
SCEK	Smart Card Encryption Key

Table 15 - Abbreviations

FUTUREX ENGINEERING CAMPUS

OFFICE: +1 830 - 980 - 9782 TOLL FREE: 800 - 251 - 5112
864 OLD BOERNE ROAD, BULVERDE, TEXAS, USA 78163