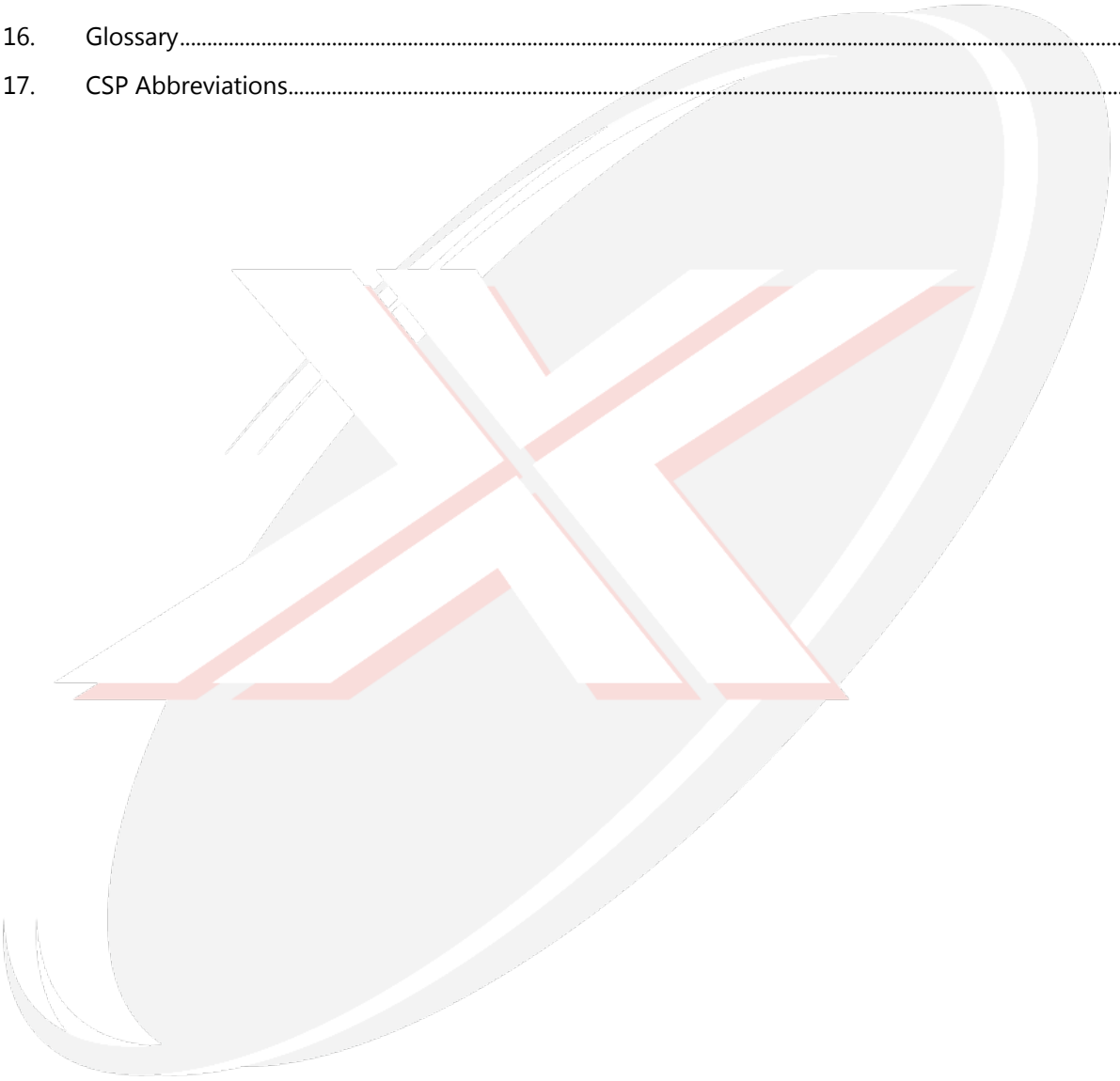
FUTUREX
FIPS 140-2
NON-PROPRIETARY SECURITY POLICY
GSP3000 Hardware Security Module

Table of Contents



1. MODULE OVERVIEW

The GSP3000 (HW P/N 9800-2079 Rev7, Rev8, Rev8C, or Rev8D FW Version 6.2.0.3) 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. The boundary is the entire PCB assembly and protective epoxy, as shown with the red outline. Components not enclosed within the epoxy are non-sensitive and have been excluded from the physical security requirements.

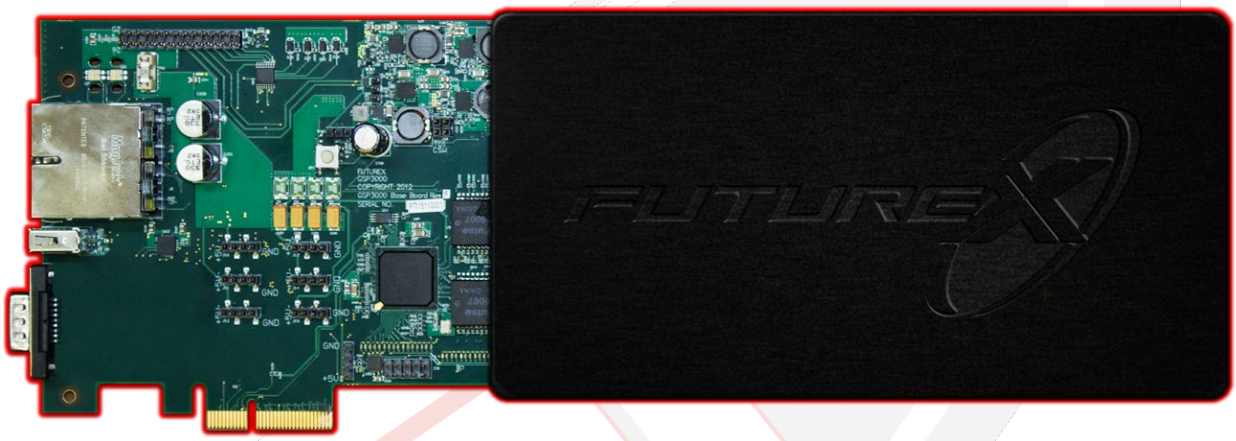


Figure 1 – GSP3000 Hardware Security Module

None of the components outside the epoxy are relevant to the security of the module. They are excluded from the security requirements of FIPS 140-2.

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 mode (non-Approved for FIPS 140), or General non-Approved mode 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. Once a selection is chosen and confirmed, the module automatically reboots into the chosen mode.
When used in the Vectera 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

- AES ECB, CBC, CFB (1, 8, 128), and OFB with 128, 192, and 256 bit keys for encryption and decryption (AES Cert. #4117)
- AES CMAC with 128, 192, 256 bit keys for MAC generation and verification (AES Cert. #4118)
- AES GCM with 256 bit keys for decryption (AES Cert. #4118)
- CKG (vendor affirmed):
    - [SP 800-133]
    - §6: Asymmetric (FIPS 186-4, SP800-56A)
    - §7: Symmetric (Direct output from DRBG)
      Note: The resulting symmetric key or generated seed is an unmodified output from a DRBG.
- CTR DRBG (using AES-256) for random number generation (DRBG Cert. #1240)
- ECC P-192 for digital signature verification (FIPS 186-4; ECDSA Cert. #935)
- ECC P-224, P-256, P-384, and P-521 for key generation, digital signature generation, and verification (FIPS 186-4; ECDSA Cert. #935)
- HMAC SHA-1, SHA-256, SHA-384, SHA-512 for keyed message authentication (HMAC Cert. #2689)
- KDF CMAC Triple-DES (3-key) (KBKDF Cert. #104)
- KDF CMAC AES with 128, 192, 256 bit keys (KBKDF Cert. #104)
- KDF TLS 1.0/1.1, and 1.2 (CVL Cert. #925)
    - Note: No parts of TLS, other than the KDF, have been tested by CAVP or CMVP.
- KTS [SP 800-38F] (symmetric) using:
    - AES KWP (AES Cert #4118) authenticated encryption
    - AES CBC (AES Cert. #4117) encryption and AES CMAC (AES Certs. #4118) authentication

  - AES CBC (AES Cert. #4117) encryption and HMAC (HMAC Cert. #2689) authentication; see TLS cipher suite listing
  - Triple-DES CBC (Triple-DES Cert. #2248) encryption and HMAC-SHA-1 (HMAC Cert. #2689) authentication; key establishment methodology provides 112 bits of encryption strength
- RSA with 1024 bit keys for digital signature verification (RSA Cert. #2226)
- RSA 2048 and 3072 bit keys for key generation, digital signature generation and verification (RSA Cert. #2226)
- SHA-1, SHA-224, SHA-256, SHA-384, SHA-512 for hashing (SHS Cert. #3387)

  Note: SHA-1 is not available for digital signature creation.
- Triple-DES (2-key, 3-key) TECB, TCBC, TCFB (1, 8, 64), and TOFB for decryption (Triple-DES Cert. #2248)
- Triple-DES (3-key) TECB, TCBC, TCFB (1, 8, 64) and TOFB for encryption (Triple-DES Cert. #2248)
- CMAC Triple-DES (2-key, 3-key) for MAC verification (Triple-DES Cert. #2254)
- CMAC Triple-DES (3-key) for MAC generation (Triple-DES Cert. #2254)

Allowed Non-Approved Functions

- Diffie-Hellman Key Agreement (2048) (key establishment methodology provides 112 bits of encryption strength)
- EC Diffie-Hellman Key Agreement (P-521) (key establishment methodology provides 256 bits of encryption strength)
- NDRNG used for DRBG seed data
- RSA Key Transport (2048) (key wrapping; key establishment methodology provides 112 bits of encryption strength)

3.2. PCI HSM Mode of Operation (non-Approved)

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

- 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
- Triple-DES (2-key) for encryption, 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.
- DUKPT: key management technique
- AKB/TR-31: key bundling techniques
- When configured for operation in an issuer environment *
  - Clear PIN processing

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

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

- PIN generation: random and derived

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

- 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

3.3. General Non-Approved Mode of Operation

In General non-Approved mode (not FIPS or PCI HSM), 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
- Triple-DES (2-key) for all usages without restriction (non-compliant)
- When configured for operation in an issuer environment*
  - Clear PIN processing
- When configured for PIN processing, the following pin block format translation will be allowed. *

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

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

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

4. PORTS AND INTERFACES

The cryptographic module provides the following physical ports and logical interfaces. All physical ports are within the boundary, but outside the epoxy material.

- Ethernet ports (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.
  - These ports include connection status LEDs.
- PCIe connector (x1): Control input, data input, data output, status output
  - Provides logical signals for x4 additional Ethernet connections.
- Single-row 4-pin headers (x7): Disabled in FIPS and PCI-HSM modes.
  - Provides USB functionality in the General Non-Approved mode.
- USB Port (x1): Disabled in FIPS and PCI-HSM modes.
  - Provides USB functionality by converting the dual-row 5-pin header to USB in the General Non-Approved mode.
- DB-9 Serial Port (x1): Disabled in FIPS and PCI-HSM modes.
  - Provides serial connection in the General Non-Approved mode.
- Tamper status LED (x1): Status output
  - Reports a module tamper.
- Dual-row 26-pin header (x1): Control input, Power
  - RPM signals
  - Battery sense
  - Main power supply
  - Battery power supply
  - "Power good" signal
- Single-row 3-pin header (x1): Control input
  - Case switch signals
  - Reset signal
  - Reset default port
- Dual-row 5-pin header (x1): Disabled in FIPS and PCI-HSM modes
  - Provides serial connection in the General Non-Approved mode.

5. IDENTIFICATION AND AUTHENTICATION POLICY

5.1. ASSUMPTION OF ROLES

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

For Operations and Crypto-Officer, 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 6 to 64 characters chosen from the 90 printable and human-readable characters. Default passwords are only used for the default Crypto-Officer roles and must be updated upon initial login. An operator that provides a valid username and password will be identified as an Operations or Crypto-Officer 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. In order 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 Triple-DES, or KWP for AES. In either case, the symmetric key (AES or 3-key Triple-DES) which is used to encrypt the cryptogram corresponds to the operator's identity. For Triple-DES-wrapped keys, the loaded key is always Triple-DES as well. The module decrypts the key and checks its parity bits. If any bit is incorrect, the command is rejected. (This prevents an attacker from passing off a random string as a wrapped Triple-DES key.) For AES-wrapped keys, the key is auth-decrypted according to SP800-38F (KWP); if this operation fails, the command is rejected.

5.2. ROLES AND REQUIRED IDENTIFICATION AND AUTHENTICATION

Role	**Type of Authentication**	**Authentication Data**
Operations	Identity-based	User name and password
Crypto-Officer	Identity-based	User name and password
Transaction Processing	Identity-based	ID of wrapping key and wrapped key (KWP/Key Parity)

Table 2 - Roles and Required Identification and Authentication

5.3. 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 1/531,441,000,000 ($1/90^6$). The module allows for 3 failed attempts and then times out for 20 seconds before retry. The probability of successful authenticating to the module within one minute is 1/59,049,000,000.
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 probability of successfully authenticating to the module within one minute is 1/122,978,293,824,730,344.
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 retry. The probability of successfully authenticating to the module within one minute is 1/111,848

Table 3 - Strength of Authentication Mechanisms

6. ACCESS CONTROL POLICY

6.1. 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.

6.2. AUTHENTICATED SERVICES

Role	**Authorized Service**
Operations:	• Create Session: This service 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 minute of inactivity, fifteen minutes of use, or 7,500 transactions. • Destroy Session: This service allows an operator to end the session. • Logout: This service allows an operator to end authentication. • View Configuration: Gives operator the ability to view configuration status to include IP, Com, SSL, Time, Features, Users, IP tools, Logs. This does not allow configuration of these items. • Configuration: Allows operator to change IP address, syslog level, Operations user passwords, and reboot device.
Cryptographic-Officer:	• Create Session: This service 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 minute of inactivity, fifteen minutes of use, or 7,500 transactions. • Destroy Session: This service allows a Crypto-Officer to end the session. • Initialization: This service shall enable 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. • 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.

	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 the scope of this validation and require a separate FIPS 140-2 validation. • 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, Logs. This does not allow configuration of these items. • 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 Futurex TRM. These commands must be unblocked by the Crypto-Officer for use.
Transaction Processing	• Create Session: This service allows a user to create a secure session to the HSM. • Destroy Session: This service allows a user to end the session. • Authenticate: This service allows a user to send credentials to be authenticated by the cryptographic module. • 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 Futurex TRM. These commands must be unblocked by the Crypto-Officer for use.

Table 4 - Authorized Services by Role

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 5 - Specification of Service Inputs & Outputs

6.3. DEFINITION OF CRITICAL SECURITY PARAMETERS (CSPS)

CSPs are secured within the cryptographic boundary as unencrypted plaintext or binary data. 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	Used to Encrypt or Decrypt TLS private keys
Server Private Keys	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 3-key Triple-DES	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	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
DH Private Key	ECC 521 DH 2048	Used for DH TLS exchange
Ephemeral Asymmetric Key	RSA 2048 or ECC 521	Used to transfer Ephemeral Key between HSM's for component transfer
Ephemeral Symmetric Key	AES 256	Used to encrypt key components
Crypto-Officer Password	Pass-phrase	Used to authenticate the identity of a Crypto-Officer.

Operations Password	Pass-phrase	Used to authenticate the identity of an Operations user.
Platform Master Key	AES 256	Used to encrypt AES 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	2-key Triple-DES**; 3-key Triple-DES; 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 the Crypto Officer and Transaction Processing roles.
Seed Value	NDRNG value	Seed for CTR DRBG. (The seed provides at least 384 bits of entropy.)
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

Table 6 - Critical Security Parameters

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

**NOTE: 2-key Triple-DES can only be used for decryption.

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

6.4. 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 in order 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 1024/2048/3072, ECC 192/224/256/384/521): These public keys are always used by the operator.
- HSM signing public key (RSA 2048/ECC 521): Output to allow host to verify log signature.
- DH Public Key (DH 2048/ECC 521): Used for TLS key exchange

6.5. MODES OF ACCESS FOR CSPS

Table 7 provides a list of CSP operations supported by the cryptographic module. Per-service access rights are shown in Table 8. Supported CSP operations are defined as follows:

- Generate: These operations generate a particular CSP within the cryptographic module.
- Load: These operations allow for a particular CSP to be loaded into the cryptographic module.
- Wrap: These operations use a CSP to perform key wrapping.
- Un-wrap: These operations use a CSP to perform key unwrapping.
- Destroy: These operations erase the CSP from the cryptographic module.

CSP	**Operation**				
	Generate	**Load**	**Wrap**	**Un-wrap**	**Destroy**
Unique Device Keys	x		x	x	x
Server Private Keys	×				×
Session Encryption Key	×		×	×	×
Session Hash Key	×		×	×	×
Pre-Master Secret	x				x
DH Private Key	x				x
Ephemeral Asymmetric Key	x		x	x	x
Ephemeral Symmetric Key	x		x	x	x
Crypto-Officer Password		×			×
Operations Password		×			x
Platform Master Key		x	x	x	x
FTK Key		x	x	x	x

Key Exchange Key		x	x	x	x
Backup Key		x	x	x	x
Smart Card Encryption Key		x	x	x	x
User Keys		x	x	x	x
Seed Value	x				x
HSM Signing Private Key	x				x
DRBG State	x				x

Table 7 - Supported CSP Operations

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

Cryptographic Keys and CSPs Access Operation	**Service**	**Operations Role**	**CO Role**	**Transaction Processing**	**U/A***
Generate Session Encryption and Hash keys	Create Session	x	x	x	
Wrap and un-wrap with Session Encryption and Hash keys	Process Transactions		x	x	

Destroy Session Encryption and Hash keys	Destroy Session	x	x	x	
(No CSP access)	Status				x
Generate Ephemeral Keys; Wrap and un-wrap with Ephemeral Keys	Key Loading		x		
Destroy Ephemeral Keys	Key Loading (upon completion)		x		
Destroy Server Private and Public Key, CO/User Names and Passwords, Key Exchange Key, Backup Key, Smart Card Encryption Key	Zeroize		x		
Zeroize and generate Server Private and Public Key	Initialization		x		
Zeroize all CSPs to include default TLS keys	Tamper				x
(No CSP access)	Self-Tests				x

Load CO/User Names and Passwords Destroy CO/User Names and Passwords	User Administration		x		
Verify with Firmware Public Key	Update Firmware		x		
Zeroize CSPs and restore factory defaults**	Factory Reset				x
Send in authentication credentials	Authenticate	x	x	x	
No CSP access	Logout	x	x	x	
No CSP access	General Configuration		x		
No CSP access	Configuration	x	x		
No CSP access	View Configuration	x	x		
Loading of PMK, FTK, KEK, Backup Key, SCEK, User Keys	Key Loading		x		
Loading of Encrypted User Keys	Load Encrypted Key		x	x	

Table 8 - CSP Access Rights within Roles & Services

*NOTE 1: U/A = Unauthenticated (no role required).

**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.

7. OPERATIONAL ENVIRONMENT

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

8. 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 three distinct operator roles. These are the Operations role, the Cryptographic-Officer role, and the Transaction Processing role.
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.

8.1. SELF-TESTS

In FIPS mode, 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 to its parent device. If all tests pass, the module powers up normally and reports success to its parent device.

Power-Up and Periodic Self Tests

The following tests shall be performed at power-up:

- Firmware integrity and authenticity tests (ECDSA signature) are performed in all modes of operation.
- Known answer tests are executed in FIPS and PCI modes of operation for:
  - AES 128/192/256 Encrypt and Decrypt
  - Triple-DES Keying Option 1/2 Encrypt and Decrypt
  - SHA1/SHA224/SHA256/SHA384/SHA512
  - RSA 1024 Verify
  - RSA 2048/3072 Sign and Verify
  - ECC 192/224/256/384/521 Sign and Verify
  - HMAC SHA1/SHA256/SHA384/SHA512
  - DRBG Known Answer
  - Triple-DES CMAC Generate and Verify
  - AES CMAC Generate and Verify
  - KDF Counter Mode using CMAC
  - KWP

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)
  - Pair-wise consistency test for RSA, ECC key generation
  - Firmware load test (ECC signature verification)

9. PHYSICAL SECURITY POLICY

9.1. PHYSICAL SECURITY MECHANISMS

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

- Hard, opaque potting material encapsulates the security relevant portion of the module, and intrusion attempts will result in serious damage which will cause the module to stop functioning.
- 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.

9.2. ENVIRONMENTAL CONDITIONS AND PARTIAL ENVIRONMENTAL FAILURE PROTECTION

The following environmental conditions should be maintained for the module:

- Operating environment temperature: 10 to 35°C
- Storage temperature: -20 to 65°C

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

- Temperature: -20 to 65°C
- Voltage: 2.3 to 4.4 V DC on internal 3V line.

9.3. 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**
Tamper Evident Potting	Monthly, and prior to module Initialization	Inspect hard potting for removal/penetration attempts.

Table 9 - 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 – GSP3000 with its Tamper Potting Intact

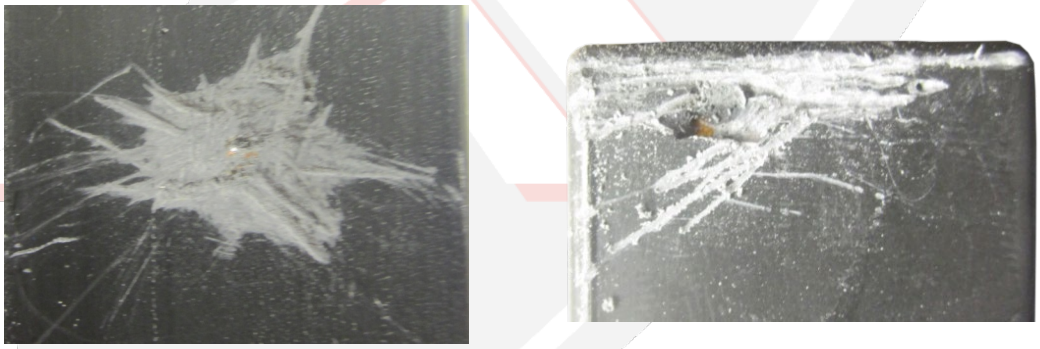


Figure 3 – Examples of Tamper Attempts on the GSP3000 Potting

10. MITIGATION OF OTHER ATTACKS

The module mitigates 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.

11. DESIGN ASSURANCE

11.1. 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.

11.2. 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

11.3. SYSTEM IDENTIFICATION AND AUTHENTICATION

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

11.4. 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 daily, and an appropriate notification tree should be established for escalating and investigating any suspicious log activity

12. KEY LOADING

12.1. 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 Securus. The Securus is a fully functional TRSM that will encrypt all data between it and the HSM using TLS.

13. PRODUCT IDENTIFICATION

13.1. HARDWARE IDENTIFICATION

To identify a GSP3000 refer to the product identification label, as seen in Figure 4

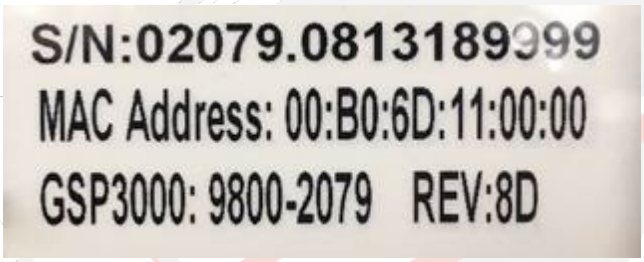


Figure 4 - Product Identification Label

The GSP3000 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 the chassis that supports the GSP3000. Figure 5 shows an example of a chassis label that references the existence of an embedded GSP3000.

Figure 5 - Chassis Label

Figure 6 and Figure 7 show typical placements of chassis labels.

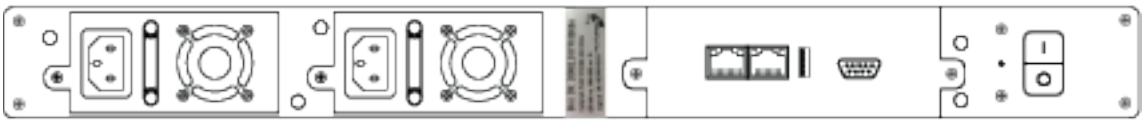


Figure 6 - 1U Chassis Label Location

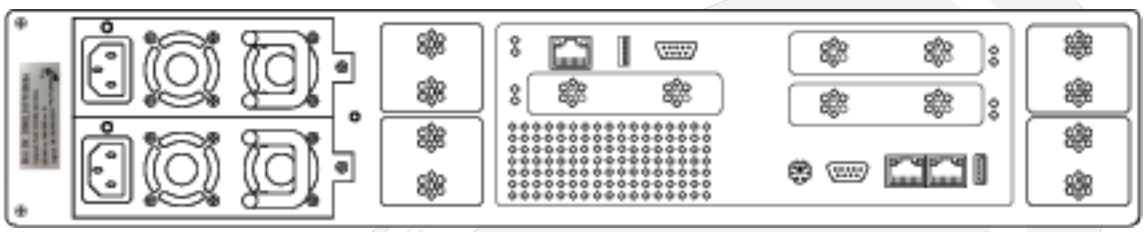


Figure 7 - 2U Chassis Label Location

13.2. 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 a full 3rd party security audit. This would typically be necessary when new security features are added or when branches are merged.
- Branch - This is incremented when a new branch is created. Branches are typically used to distinguish unique packaging of existing security features, introduction of low-impact security changes, or the introduction of new non-security features.
- Release - This is incremented when a new release happens off a branch. Changes to this component represents either bug fixes or refinements to the functionality of existing features. Releases typically represent non-impactful security changes but may have a low-impact.

The firmware version can be found on the LCD screen, web portal, or in Excrypt Manager. Please refer to 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.

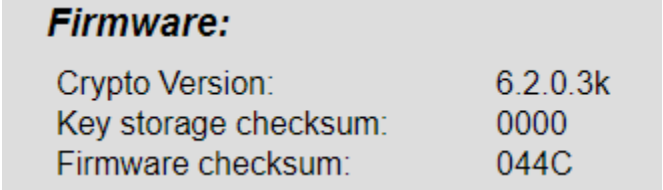


Figure 8 - Firmware Version through Web Portal

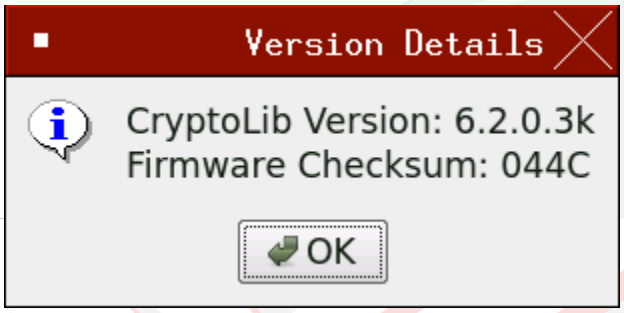


Figure 9 - Firmware Version through Excrypt Manager

14. TLS PROTOCOLS

14.1. TLS PROTOCOLS SUPPORTED

The list below contains all the TLS Protocols supported.

- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_3DES_EDE_CBC_SHA
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA
- TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA

Note: While the component algorithms have been tested by the CAVP, the TLS protocol itself has not been tested by the CAVP or CMVP.

The module limits data block encryptions with the same Triple-DES key to 2^32 operations.

15. REFERENCES

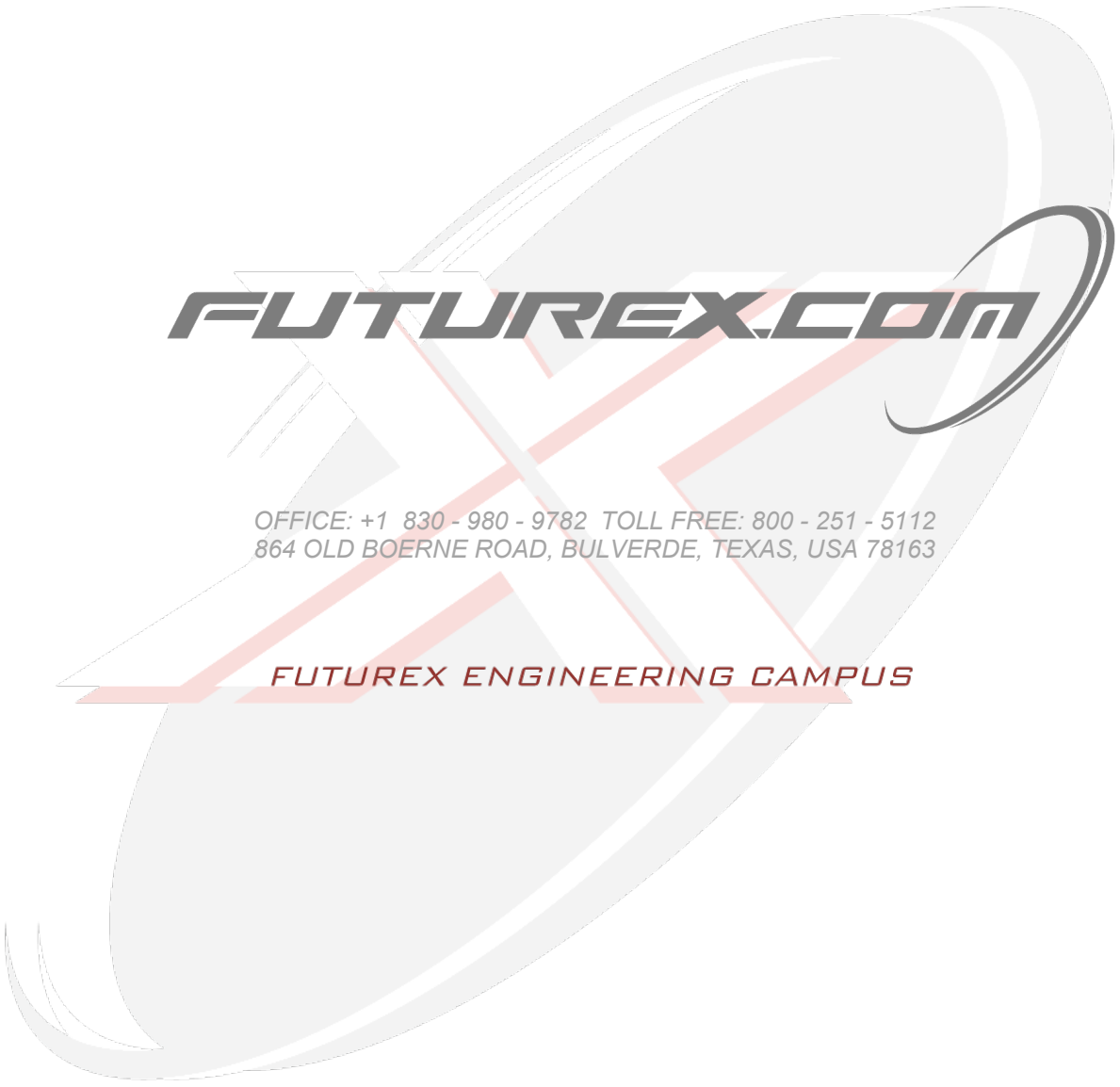
1. FIPS PUB 140-2, *Security Requirements for Cryptographic Modules*, National Institute of Standards and Technology, 2001 May 25.
2. Annex A: Approved Security Functions for FIPS PUB 140-2, *Security Requirements for Cryptographic Modules*, Draft, National Institute of Standards and Technology, 2010 January 27.
3. Annex B: Approved Protection Profiles for FIPS PUB 140-2, *Security Requirements for Cryptographic Modules*, Draft, National Institute of Standards and Technology, 2007 June 14.
4. Annex C: Approved Random Number Generators for FIPS PUB 140-2, *Security Requirements for Cryptographic Modules*, Draft, National Institute of Standards and Technology, 2009 July 21.
5. Annex D: Approved Key Establishment Techniques for FIPS PUB 140-2, *Security Requirements for Cryptographic Modules*, Draft, National Institute of Standards and Technology, 2009 October 08.
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
8. NIST Special Publication 800-17, *Modes of Operation Validation System (MOVS): Requirements and Procedures*, National Institute of Standards and Technology, February 1998.
9. NIST Special Publication 800-20, *Modes of Operation Validation System for the Triple Data Encryption Algorithm (TMOVS): Requirements and Procedures*, National Institute of Standards and Technology, April 2000.
10. ANSI X9.31-1998, *Digital Signature using Reversible Public Key Cryptography for the Financial Services Industry (rDSA),* Accredited Standards Committee X9, Inc., 1998.
11. The RSA Validation System (RSAVS), National Institute of Standards and Technology, 2004 November 09.
12. FIPS PUB 180-2 with Change Notice 1, *Secure Hash Standard (SHS)*, National Institute of Standards and Technology, 2004 February 25.
13. The Secure Hash Algorithm Validation System (SHAVS), National Institute of Standards and Technology, 2004 July 22.
14. The Random Number Generator Validation System (RNGVS), National Institute of Standards and Technology, 2005 January 31.
15. FIPS PUB 198, *The Keyed-Hash Message Authentication Code (HMAC)*, National Institute of Standards and Technology, 2002 March 06.
16. The Keyed-Hash Message Authentication Code Validation System (HMACVS), National Institute of Standards and Technology, 2004 December 03.

16. 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
HMAC-SHA-1	Keyed-Hash Message Authentication Code using SHA-1
I^2C	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
TRM	Technical Reference Manual

17. CSP ABBREVIATIONS

Term	Definition
KEK	Key Exchange Key
PMK	Platform Master Key
SCEK	Smart Card Encryption Key


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