



# **FUTUREX**

## **FIPS 140-2 Non-Proprietary Security Policy**

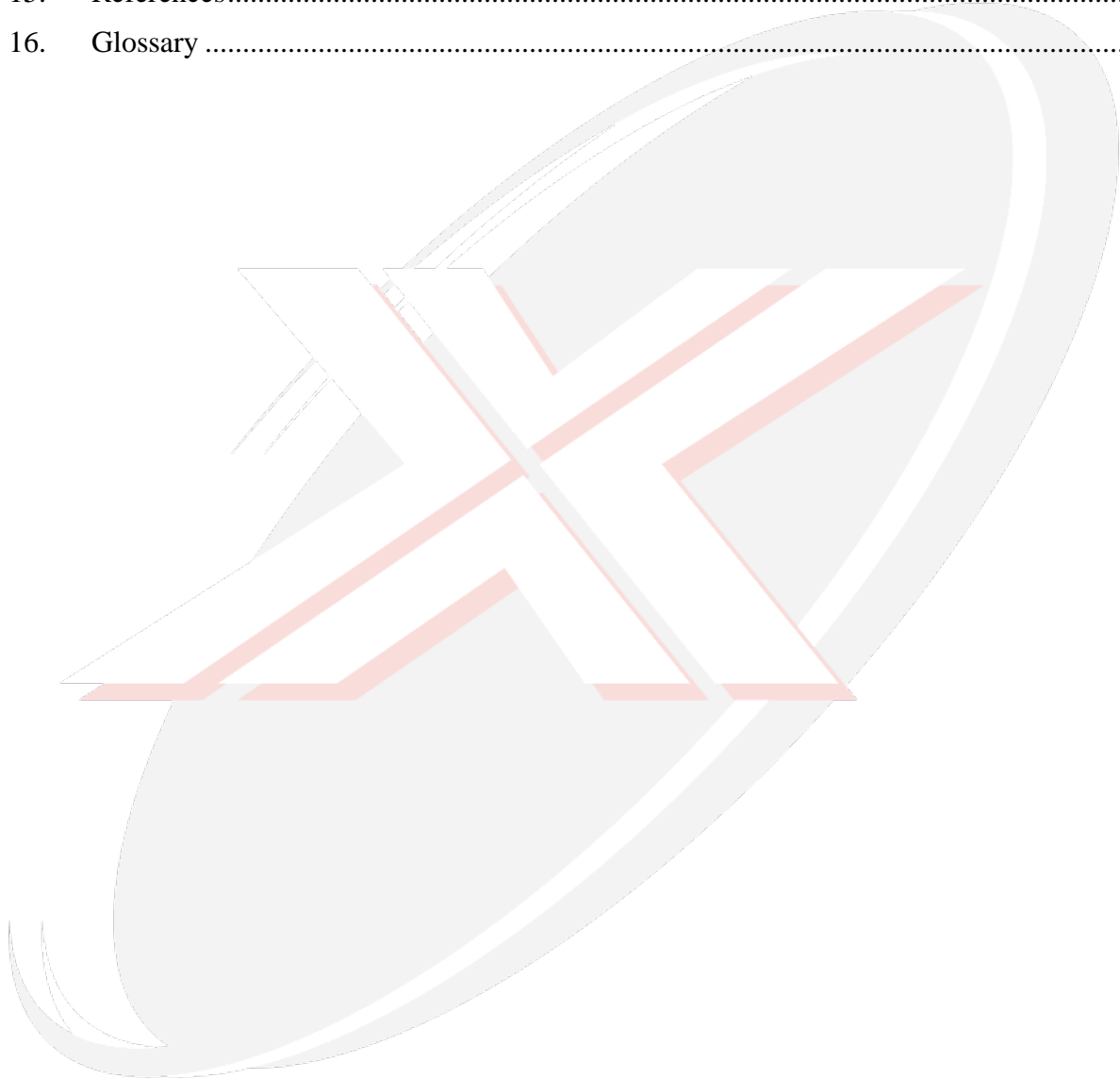
GSP3000 Hardware Security Module

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

# Table of Contents

|  |    |
|--|----|
| 1. Module Overview .....   | 4  |
| 2. Security Level .....  | 5  |
| 3. Modes of Operation .....  | 6  |
| 3.1. FIPS Approved Mode of Operation .....                                       | 6  |
| 3.2. PCI HSM Mode of Operation (non-Approved) .....                              | 7  |
| 3.3. General Non-Approved Mode of Operation .....                                | 8  |
| 4. Ports and Interfaces .....  | 10 |
| 5. Identification and Authentication Policy .....                                | 11 |
| 5.1. Assumption of Roles .....   | 11 |
| 5.2. Roles and Required Identification and Authentication .....                  | 11 |
| 5.3. Strengths of Authentication Mechanisms .....                                | 12 |
| 6. Access Control Policy .....   | 12 |
| 6.1. Unauthenticated Services .....  | 12 |
| 6.2. Authenticated Services .....  | 13 |
| 6.3. Definition of Critical Security Parameters (CSPs) .....                     | 17 |
| 6.4. Definition of Public Keys .....   | 19 |
| 6.5. Modes of Access for CSPs .....  | 21 |
| 7. Operational Environment .....   | 26 |
| 8. Security Rules .....  | 26 |
| 8.1. Self-Tests .....  | 27 |
| 9. Physical Security Policy .....  | 28 |
| 9.1. Physical Security Mechanisms .....  | 28 |
| 9.2. Environmental Conditions and Partial Environmental Failure Protection ..... | 28 |
| 9.3. Operator Recommended Actions .....  | 28 |
| 10. Mitigation of Other Attacks .....  | 30 |
| 11. Design Assurance .....   | 30 |
| 11.1. Configuration Management .....   | 30 |
| 11.2. Guidance Documents .....   | 30 |
| 11.3. System Identification and Authentication .....                             | 30 |
| 11.4. Audit Logs and Inspection Frequency .....                                  | 30 |
| 12. Key Loading .....  | 31 |

- 12.1. Key Loading (FIPS/PCI-HSM Modes) ..... 31
- 13. Version Scheme ..... 31
  - 13.1. Major.Audit.Non-Security Related Changes..... 31
- 14. TLS Protocols ..... 31
  - 14.1. TLS Protocols Supported ..... 31
- 15. References..... 32
- 16. Glossary ..... 33



## 1. Module Overview

The GSP3000 (HW P/N 9800-2079 Rev7, FW Version 6.2.0.0) 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.

| <b>Security Requirements Section</b> | <b>Level</b> |
|--------------------------------------|--------------|
| 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)
- AES KWP (NIST SP800-38F) with 128, 192, and 256 bit keys for key wrapping and key unwrapping (AES Cert. #4118)
- AES CBC for key wrap and unwrap (SP800-38F §3.1) using AES+HMAC (see TLS cipher suite for details) (AES Certs. #4117; HMAC Cert. #2689)
- 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)
- 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 (SHA 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)
- Triple-DES (3-key) TCBC for key wrap and unwrap (SP800-38F §3.1) using Triple-DES+HMAC (Triple-DES Cert. #2248; HMAC Cert. #2689)
- 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

- NDRNG used for DRBG seed data
- Triple-DES (3-key) TECB for wrap and unwrap (key establishment methodology provides 112 bits of encryption strength)
- RSA Key Transport (2048) (key wrapping; key establishment methodology provides 112 bits of encryption strength)
- DH Key Agreement (2048) (key establishment methodology provides 112 bits of encryption strength)
- ECDH Key Agreement (P-521) (key establishment methodology provides 256 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 |       |       |       |         |         |
|--------|-------------|-------------|-------|-------|-------|---------|---------|
|        |             | ISO 0       | ISO 1 | ISO 2 | ISO 3 | IBM3624 | PIN Pad |
| Source | 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      |
|        | IBM36<br>24 | Yes         | Yes   | Yes   | Yes   | Yes     | Yes     |
|        | PIN<br>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  $2048 + n \cdot 8$  [ $n = 0$  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:

- RSA with additional, non-compliant key sizes (full selection is  $512 + n \cdot 8$  [ $n = 0$  to 256] up to 4096 bits) for key generation, digital signature generation, and verification
- ECC with 192 bit keys for key generation, digital signature generation and verification (non-compliant)
- DES for encryption and decryption
- Triple-DES (2-key) for all usages without restriction (non-compliant)
- MD5, RIPEMD-160 for hashing
- HMAC MD5, HMAC RIPEMD-160 for keyed message authentication
- 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 |       |       |       |         |         |
|--------|---------|-------------|-------|-------|-------|---------|---------|
|        |         | ISO 0       | ISO 1 | ISO 2 | ISO 3 | IBM3624 | PIN Pad |
| Source | 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  $512 + n \cdot 8$  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 takes 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         | <p>The probability that a random attempt will succeed or a false acceptance will occur is <math>1/531,441,000,000</math> (<math>1/90^6</math>).</p> <p>The module allows for 3 failed attempts and then times out for 20 seconds before retry. The probability of successfully authenticating to the module within one minute is <math>1/59,049,000,000</math>.</p>  |
| AES-KWP                       | <p>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 <math>1/18,446,744,073,709,551,616</math> (<math>1/2^{64}</math>).</p> <p>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 <math>1/122,978,293,824,730,344</math>.</p> |
| Key Parity (3-key Triple-DES) | <p>3-key Triple-DES has 24 parity bits. Thus, the probability that a random attempt will succeed or a false acceptance will occur is <math>1/16,777,216</math> (<math>1/2^{24}</math>).</p> <p>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 <math>1/111,848</math>.</p>  |

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:            | <ul style="list-style-type: none"> <li>• <u>Create Session</u>: This service allows an operator to create a secure session to the HSM.</li> <li>• <u>Authenticate</u>: 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.</li> <li>• <u>Destroy Session</u>: This service allows an operator to end the session.</li> <li>• <u>Logout</u>: This service allows an operator to end authentication.</li> <li>• <u>View Configuration</u>: 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.</li> <li>• <u>Configuration</u>: Allows operator to change IP address, syslog level, Operations user passwords, and reboot device.</li> </ul> |
| Cryptographic-Officer: | <ul style="list-style-type: none"> <li>• <u>Create Session</u>: This service allows an operator to create a secure session to the HSM.</li> <li>• <u>Authenticate</u>: 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.</li> <li>• <u>Destroy Session</u>: This service allows a Crypto-Officer to end the session.</li> <li>• <u>Initialization</u>: 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.</li> <li>• <u>Zeroize</u>: This service shall enable a Crypto-Officer to destroy critical security parameters by zeroization.</li> </ul>      |

|                        |  |
|------------------------|--|
|                        | <ul style="list-style-type: none"> <li>• <u>Key Loading</u>: This service allows a Crypto-Officer to load keys into the module.</li> <li>• <u>Update Firmware</u>: 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.<br/><br/><b>Note:</b> 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.</li> <li>• <u>General Configuration</u>: This service allows a Crypto-Officer to change all configuration options for the module.</li> <li>• <u>View Configuration</u>: 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.</li> <li>• <u>User Administration</u>: This service will allow the Crypto-Officer to create, manage, and delete users.</li> <li>• <u>Logout</u>: This service will enable the Crypto-Officer to end authentication.</li> <li>• <u>Load Encrypted Key</u>: 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 MFK.</li> <li>• <u>Process Transactions</u>: 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.</li> </ul> |
| Transaction Processing | <ul style="list-style-type: none"> <li>• <u>Create Session</u>: This service allows a user to create a secure session to the HSM.</li> <li>• <u>Destroy Session</u>: This service allows a user to end the session.</li> <li>• <u>Authenticate</u>: This service allows a user to send credentials to be authenticated by the cryptographic module.</li> <li>• <u>Logout</u>: This service will enable the Crypto-Officer to end authentication.</li> <li>• <u>Load Encrypted Key</u>: This service allows a user to send in Encrypted keys and have the keys translated and stored in</li> </ul>  |

|  |   |
|--|---|
|  | <p>the key table or returned as a cryptogram encrypted under the MFK.</p> <ul style="list-style-type: none"> <li>• <u>Process Transactions</u>: 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.</li> </ul> |
|--|---|

**Table 3 - Authorized Services by Role**

| <b>Service</b>       | <b>Control Input</b> | <b>Data Input</b>     | <b>Data Output</b> | <b>Status Output</b>  |
|----------------------|----------------------|-----------------------|--------------------|-----------------------|
| 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 4 - 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<br>RSA 2048                        | Sign or Decrypt data sent to the device from an operator during the creation of a TLS session.<br><br>Used during creation of a TLS session. |
| Session Encryption Key   | AES-128<br>AES-256<br>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<br>HMAC-SHA-256<br>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<br>DH 2048                         | Used for DH TLS exchange   |
| Ephemeral Asymmetric Key | RSA 2048 or<br>ECC 521                     | Used to transfer Ephemeral Key between HSM's for component transfer  |

|                           |   |   |
|---------------------------|---|---|
| Ephemeral Symmetric Key   | 3-key Triple-DES or 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.  |
| Master File Key           | 3-key Triple-DES  | "Master Key" for symmetric cipher operations, e.g. loading of User Keys (key transport)<br>(Typically specific to one instance of the module)           |
| 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          | 3-key Triple-DES<br>AES 256   | Used to load User Keys as part of Transaction Processing (key transport)  |
| Backup Key                | 3-key Triple-DES or AES 256   | Encrypts the User Keys for backup (key transport)   |
| Pending Master File Key   | Triple-DES 192 bits   | "Pre" Master File Key; can be "rotated in" to become the Master File Key.   |
| Smart Card Encryption Key | 3-key Triple-DES or AES 256   | Wraps smart card fragments (keys and other sensitive data) for storage on smart card.   |
| User Keys                 | 2-key Triple-DES**;<br>3-key Triple-DES;<br>RSA 1024*,<br>2048, 3072; | Data encryption, key exchange, CMAC, and HMAC keys used by user<br><br>These keys are available to the Crypto Officer and Transaction Processing roles. |

|                         |   |   |
|-------------------------|---|---|
|                         | AES 128, 192, 256; ECC 192***, 224, 256, 384, 521; HMAC |   |
| Seed Value              | NDRNG value   | Seed for CTR DRBG.<br>(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 5 - 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.

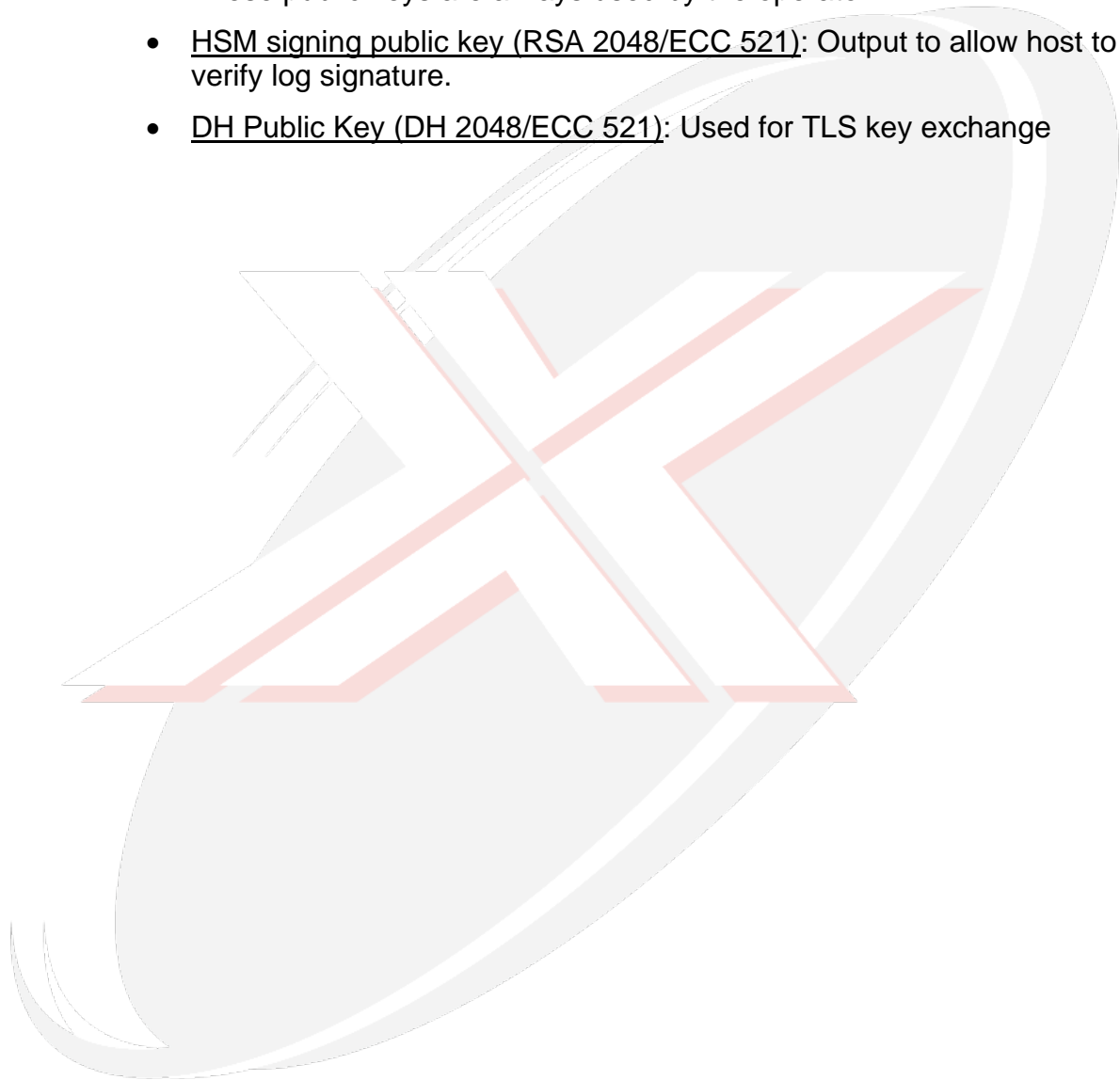
#### 6.4. Definition of Public Keys

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      | x         |      |      |         | x       |
| Session Encryption Key   | x         |      | x    | x       | x       |
| Session Hash Key         | x         |      | x    | x       | x       |
| 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  |           | x    |      |         | x       |
| Operations Password      |           | x    |      |         | x       |
| Master File Key          |           | x    | x    | x       | 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 |
| Pending Master File 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 6 - 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, Master File Key, Key Exchange Key, Backup Key, Pending Master File 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<br>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 MFK, PMK, FTK, KEK, Backup Key, Pending MFK, SCEK, User Keys | Key Loading           |   | X |   |   |
| Loading of Encrypted User Keys  | Load Encrypted Key    |   | X | X |   |

Table 7 - CSP Access Rights within Roles &amp; 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:

- Known answer tests 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
- Firmware integrity and authenticity test (ECC signature)

### Conditional Self-Tests

The device will perform the following conditional self-tests:

- 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 8 - 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 on a daily basis, 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. Version Scheme

### 13.1. Major.Audit.Non-Security Related Changes

- 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.
- Non-Security Related Changes

## 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.

## 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 (SHA VS), 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 <sup>2</sup> C | 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          |
| MFK  | Master File Key           |
| PMK  | Platform Master Key       |
| SCEK | Smart Card Encryption Key |

A large, semi-transparent watermark of the Futurex.com logo is centered on the page. The logo features the text "FUTUREX.COM" in a bold, italicized, sans-serif font. Below the text is a stylized graphic consisting of several overlapping, curved lines in shades of gray and red, forming a shape reminiscent of a stylized 'X' or a dynamic swoosh. The watermark is positioned behind the table and other text elements.

**FUTUREX.COM**

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

**FUTUREX ENGINEERING CAMPUS**