3SGX

3S Group Cryptographic Module

Non-Proprietary Security Policy

DOCUMENT NUMBER	VERSION	DATE
3SG-FIPS-001	1. 5	May 22, 2013

3S Group Incorporated
125 Church Street, NE Suite 204
Vienna, VA 22180

Distribution Statement:

The information contained in this document, including all concepts, inventions and know how derived from it, are 3S Group Incorporated Proprietary Information and are protected by the U.S. Trade Secrets Act at 18 U.S.C. § 1905. Disclosure, reproduction, distribution, or use in whole or in part, for any other purpose by any other means, including electronically, without written authorization from 3S Group Incorporated, is strictly prohibited.

This document may be reproduced and distributed only whole and intact, including this copyright notice.

TABLE OF CONTENTS

TABLE OF FIGURES

TABLE OF TABLES

Table 1 Record of Changes

VER NUM	DATE	BRIEF DESCRIPTION
1.0	07/12/2012	Baseline
1.1	02/07/2013	Updated with CMVP comments.
1.2	04/02/2013	Updated with CMVP comments.
1.3	04/05/2013	Updated with CMVP comments.
1.4	05/01/2013	Updated with CMVP comments.
1.5	05/22/2013	Updated with CMVP comments.

1 SCOPE

The purpose of this document is to define the security policy of the 3S Group cryptographic module, namely 3SGX. This security policy is presented in accordance with the documentation requirements of National Institute of Standards and Technology (NIST) Federal Information Processing Standard (FIPS) 140-2, Security Requirements for Cryptographic Modules. This policy document describes how the 3SGX satisfies the level 3 requirements of FIPS140-2 to protect sensitive information in U.S. Government as well as non-Government information systems.

2 APPLICABLE DOCUMENTS

The algorithms and modes of operation of the 3SGX conform to the following documents:

1. FIPS PUB 46-3, Data Encryption Standard (DES), NIST, 25 October 1999.
2. FIPS PUB 180-3, Secure Hash Standard, NIST, October 2008.
3. FIPS PUB 185 Escrow Encryption Standard, NIST, February 1994.
4. FIPS PUB 186-2 Digital Signature Standard (DSS), NIST, January 2007.
5. FIPS PUB 186-3, Digital Signature Standard (DSS), NIST, June 2009.
6. FIPS PUB 197, Advanced Encryption Standard, NIST, November 2001.
7. FIPS PUB 140-2, Security Requirements for Cryptographic Modules, NIST, 25 May 2001.
8. Skipjack and KEA Algorithm Specifications, NIST, 29 May 1998.
9. Clarification to the Skipjack Algorithm Specification, NIST, 9 May 2002.
10. Derived Test Requirements for FIPS 140-2, Security Requirements for Cryptographic Modules, NIST, 24 March 2004.
11. FORTEZZA Application Implementers Guide, NIST, Document # MD4002101-1.52, 15 July, 2011.
12. Interface Control Document for the FORTEZZA Crypto Card (Production Version) (DRAFT), Revision P1.5, National Security Agency (NSA) X21, December 2 1994.
13. Special Publication 800-38A Recommendation for Block Cipher Modes of Operation, NIST, 2001.
14. Special Publication 800-56A, Recommendation for Pair-wise Key Establishment Schemes Using Discrete Logarithm Cryptography (Revised), NIST, March 2007.
15. Special Publication 800-56B, Recommendation for Pair-wise Key Establishment Schemes Using Integer Factorization Cryptography, NIST, August 2009.
16. Special Publication 800-57 Recommendation for Key Management Part 1: General, NIST, May 2006.
17. Special Publication 800-89 Recommendation for Obtaining Assurances for Digital Signature Applications, NIST, November 2006.
18. Special Publication 800-90 Recommendation for Random Number Generation Using Deterministic Random Bit Generators (Revised), NIST, March 2007.
19. Special Publication 800-131A Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths, NIST, January 2011.
20. Special Publication 800-135, Recommendation for Existing Application-Specific Key Derivation Functions, December 2011.
21. Request for Review of Key Wrap Algorithms, American Standards Committee X9 (X9F1), November 2004.
22. AES Key Wrap Specification, NIST, 16 November 2001.
23. PKCS #1 v2.1: RSA Cryptography Standard, RSA Laboratories, June 2002.

3 CRYPTOGRAPHIC MODULE

The 3S Group Cryptographic Module (3SGX) is a multi-chip embedded hardware cryptographic module that provides trusted, high-throughput cryptographic support to server applications that have demanding security assurance and performance requirements. The operational environment for the 3SGX is non-modifiable. The 3SGX resides in a secure server required to handle multiple requests for security services from multiple users. Figure 1 3S Group 3SGX – Enclosure and Figure 2 3S Group 3SGX - Epoxy Coated show pictures of the module with different physical embodiments.

This security policy applies to the following board version(s):

Hardware: 1.0

Firmware: 1.0

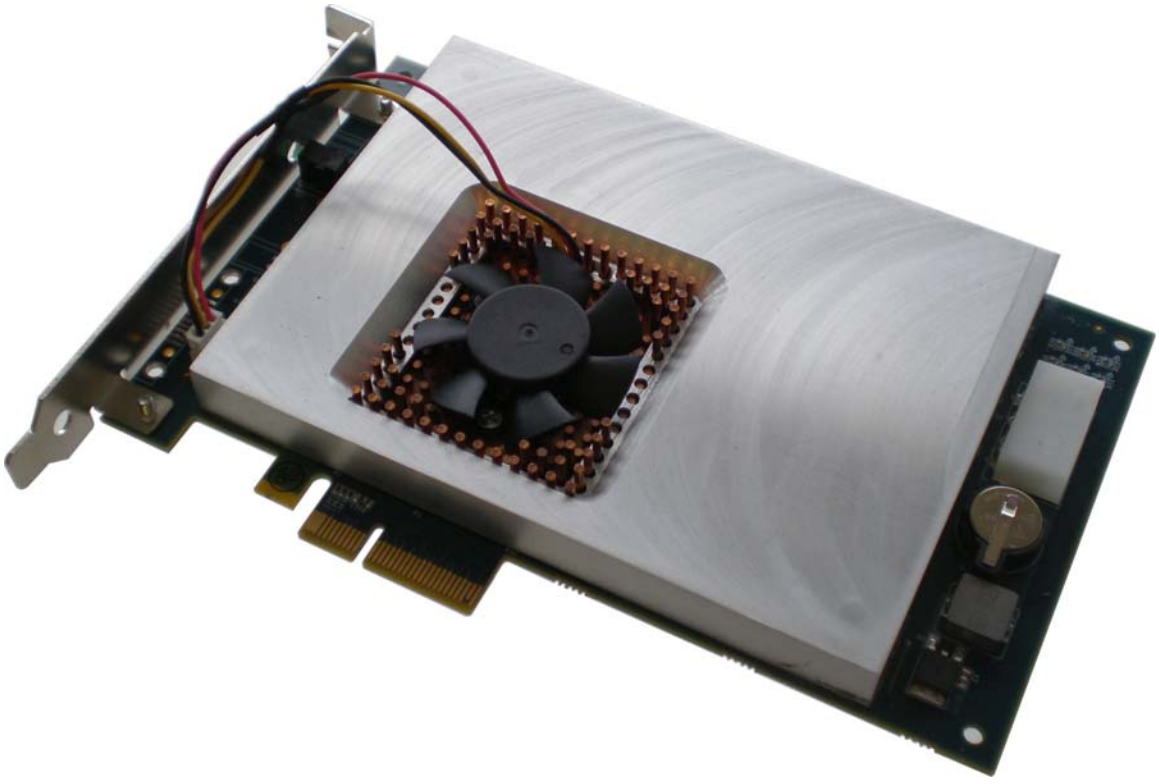

Figure 1 3S Group 3SGX – Enclosure

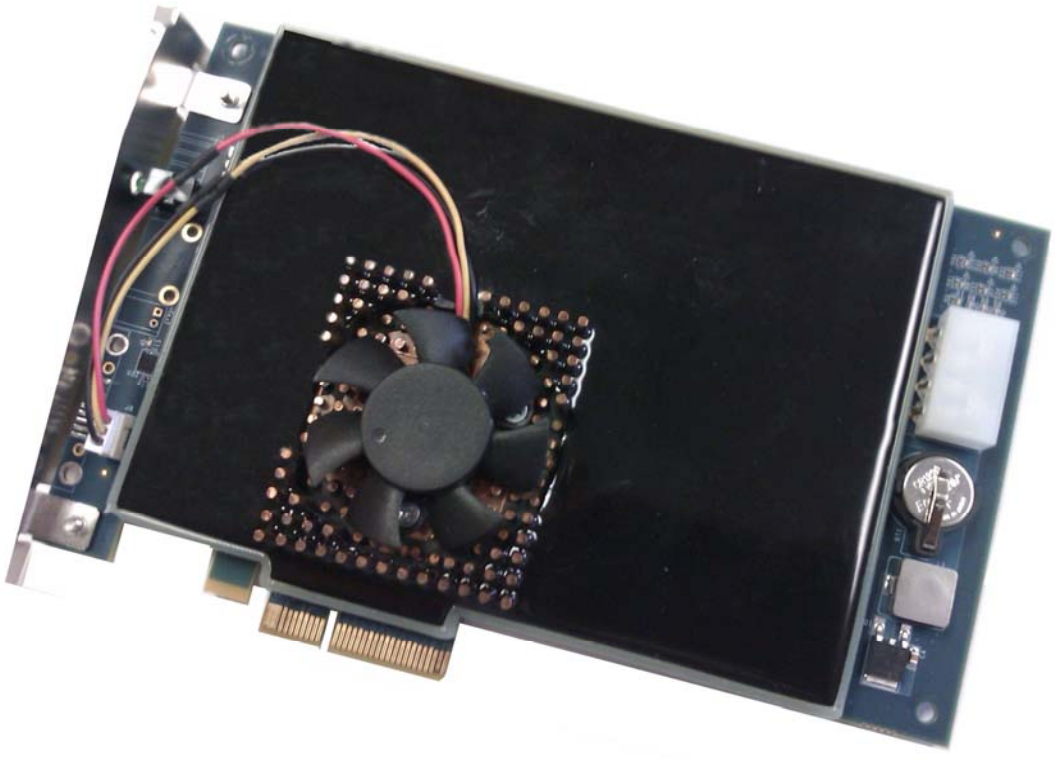

Figure 2 3S Group 3SGX - Epoxy Coated

A 3SGX system contains two major components; a multi-chip hardware board with PCI Express (PCIe) interface and a suite of host software that performs data transfer, management, administrative and maintenance support functions.

3.1 Cryptographic Module Overview

The 3SGX cryptographic module contains multiple processing cores, along with dedicated hardware units for data transfer, random number generation and cryptographic processing. Cryptographic services are based on the concept of tokens. A 3SGX token contains cryptographic material such as keys, certificates and user information necessary to authenticate users and control access to the cryptographic material.
The 3SGX supports the following two types of tokens:

a) A single Board Token which is always resident in board's nonvolatile memory. It is never offloaded from the 3SGX board. It is intended to control access to the 3SGX system, protect a 'database key' ("Kd") and to fulfill other administrative purposes. Certain operators defined in Section 5 later can access 3SGX.
b) Several Virtual Tokens (VTs) belonging to users/applications are loaded on the board stored wrapped in Kd. VTs are unwrapped on the board prior to use. The owner of a VT is the only one who can access its nonvolatile keys and certificates. From an operational standpoint, the VT owner can view this process as a temporary “leasing” of the cryptoprocessor hardware.

Users and applications can request security services, defined later, using these tokens and their contents after successfully logging into one's token.

3.1.1 Cryptographic Boundary

The 3SGX cryptographic boundary is the area inside the security embodiment on the 3SGX board.

3.1.2 Excluded Components

The following components are excluded from FIPS validation:

1. Battery
2. Unpopulated component pads
3. FIPS Mode LED
4. PCIe Connector
5. Input Power Connector
6. Flash loader
7. Boot loader

3.1.3 Ports and Interfaces

The PCIe bus is the only physical interface used by applications connecting to the module. The four logical interfaces (command input, data input, data output and status output) all use this single physical interface. A single LED is also part of the status output interface. The LED is located on the PCIe bracket of the board. It is activated when the board has completed all its boot-time initialization tasks and has transitioned into the FIPS operating mode.

The Power port consists of a 4-pin power connector. 3SGX does not draw power from the PCIe connector.

3.2 Security Level

The 3SGX meets the overall security level 3 requirements defined in FIPS 140-2. Table 2 shows the security levels for the eleven categories listed in FIPS 140-2.

Table 2 Security Level List

Security Requirements	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	N/A
Cryptographic Security Policy	3
Overall	3

4 SECURITY FEATURES

4.1 Security Services

The 3SGX provides security services such as data confidentiality, data integrity, key management, digital signatures, time stamping, and random number generation. Security mechanisms for authentication, access control and certificate management are implemented.

4.2 Functions, Algorithms and Algorithm Modes

The 3SGX system implements Government and commercial cryptographic algorithms in hardware, making it capable of satisfying the requirements of both Government and non-Government information systems. This section presents approved as well as non-approved but allowed functions, algorithms and algorithm modes.

4.2.1 Approved Functions, Algorithms and Algorithm Modes

In the 3SGX, the following approved functions, algorithms and algorithm modes are implemented.

1. 128-bit, 192-bit and 256-bit AES encryption and decryption: ECB, CBC, OFB128, CFB128, CFB64, CFB32, CFB16, CFB8 chaining modes
2. 2-key (112-bit) and 3-key (168-bit) triple-DES encryption and decryption: ECB, CBC, OFB64, CFB64, CFB32, CFB16, CFB8 chaining modes
3. 80-bit Skipjack: ECB, CBC, OFB64, CFB64, CFB32, CFB16, CFB8 chaining modes
4. Hashing using SHA-1, SHA-224, SHA-256, SHA-384 or SHA-512
5. Key Agreement Scheme (KAS) using Diffie-Hellman (DH) and Elliptic Curve Diffie-Hellman (ECDH). The following are compliant with NIST Special Publication 800-56A except item c(ii) below.
    a. Finite-field DH and ECDH algorithms
        i. 160-bit private keys and 1024-bit moduli
        ii. 224-bit private keys and 2048-bit moduli
        iii. All NIST prime elliptic curves (P192, P224, P256, P384, P521)
    b. Key agreement modes
        i. All combinations of shared secret derived from static and ephemeral DH or ECDH keys
        ii. Support for initiator and responder versions of all schemes
        iii. Tag computation using one of HMAC-SHA1, HMAC-SHA224, HMAC-SHA256, HMAC-SHA384, or HMAC-SHA512
    c. Key Derivation
        i. NIST concatenation KDF
        ii. KDF described in ANSI X9.63 using DH or ECDH

    The security strength of the key agreement scheme must equal or exceed that of the resulting key. This strength comparison is strictly enforced by the module. This enforcement obviates the need to specify caveats to the security strength of the key agreement methodology in the module's validation certificate.
6. RSA Key transport in accordance with NIST Special Publication 800-56B (vendor affirmed).
    a. 32-bit public exponent and 1024-bit or 2048-bit modulus

   b. OAEP padding
   c. OAEP can use any hash algorithm whose security level is greater than or equal to the security level of the RSA key

   The security strength of the key transport scheme must equal or exceed that of the key to be transported. This strength comparison is strictly enforced by the module. This enforcement obviates the need to specify caveats to the security strength of the key transport methodology in the module's validation certificate.
7. Digital Signature compliant with FIPS 186-2 and 186-3
   a. Finite-field and elliptic curve DSA
      i. 160-bit private keys and 1024-bit moduli
      ii. 224-bit private keys and 2048-bit moduli
      iii. All NIST prime curves (P192, P224, P256, P384, P521)
   b. RSA signature
      i. 32-bit public exponent and 1024-, 2048- or 3072-bit modulus
      ii. PKCS #1-v1.5 padding
8. Random number generation
   a. Compliant with NIST Special Publication 800-90
   b. Implements HASH-DRBG with mandatory prediction resistance, using SHA-384
   c. Reseeding uses 24 bytes of entropy input
   d. Uses the processor's nondeterministic random number generator as an entropy source

See Section 7 for the list of algorithm certificates granted for the 3SGX by the NIST Cryptographic Algorithm Validation Program (CAVP).

4.2.2 Non-Approved Functions, Algorithms and Algorithm Modes

The following non-approved functions, algorithms and algorithm modes are implemented in the 3SGX.

1. RSA Key transport
   a. 32-bit public exponent and 1024-bit, 2048-bit or 3072-bit modulus
   b. Supports PKCS #1-v1.5

   The security strength of the key transport scheme must equal or exceed that of the key to be transported. This strength comparison is strictly enforced by the module. This enforcement obviates the need to specify caveats to the security strength of the key transport methodology in the module's validation certificate.
2. Wrapping of symmetric and asymmetric keys
   a. Symmetric key wrapping algorithm using Skipjack
   b. Asymmetric key wrapping algorithm for 160-bit finite-field key agreement or digital signature using Skipjack
   c. All other wrapping operations using the method of ANSI X9.102
      i. AES key wrap (128, 192, or 256 bits security strength)
      ii. Triple-DES key wrap (80 or112 bits security strength)
3. Trusted timestamping and timekeeping

4. Key Exchange Algorithm (KEA) uses Diffie Hellman (DH) to establish Skipjack keys. KEA provides no security protection except for its use of the allowed Diffie-Hellman scheme.

For all cryptographic algorithms, refer to NIST Special Publication 800-131A, Tables 1 through 10, as applicable, regarding transitioning the use of cryptographic algorithms and key lengths. During module validation, Skipjack encryption is treated as plaintext.

4.2.3 Mode of Operation

3SGX has a single mode of operation, the FIPS-Approved mode. It enters the FIPS mode once all boot-time initialization tasks, including self-tests are completed. Then, as stated in Section 3.1.3, the FIPS mode LED is lit.

4.3 Board Token

The Board Token contains keys and certificates that support the security services and algorithms listed above. It controls the board's transition to an operational state. It is used to authenticate authorized users, protect the database key Kd and perform management and administrative functions permitted for these users. These authorized users are addressed later in this document.

4.4 Virtual Tokens (VT)

Virtual tokens contain keys and certificates supporting the services and algorithms listed above. The database key Kd cryptographically protects each VT when stored in the VT database. This database key never leaves the hardware in unencrypted form and is generated using the board's pseudo-random number generator.

4.5 Self Tests

The 3SGX design includes automatic cryptographic self-tests, performed at system startup and run conditionally at any time. Tests are repeated for all processing cores in the 3SGX. They include:

1. Known answer tests for all symmetric algorithms and chaining modes
    a. 128-bit, 192-bit and 256-bit AES encryption and decryption: ECB, CBC, OFB128, CFB128, CFB64, CFB32, CFB16, CFB8 chaining modes.
    b. 2-key (112-bit) and 3-key (168-bit) triple-DES encryption and decryption: ECB, CBC, OFB64, CFB64, CFB32, CFB16, CFB8 chaining modes.
    c. 80-bit Skipjack decryption: ECB, CBC, OFB64, CFB64, CFB32, CFB16, CFB8 chaining modes.
2. Known answer tests for all hash algorithms: SHA-1, SHA-224, SHA-256, SHA-384, and SHA-512.
3. Pairwise consistency tests for finite-field DSA (1024-bit and 2048-bit) and elliptic curve DSA (all NIST prime curves). The same consistency tests are performed at power up and conditionally.
4. Known answer tests for RSA digital signature generation and verification, using all supported key sizes (1024, 2048 and 3072-bit moduli).
5. Known answer tests for Key Agreement Schemes (KAS) compliant with SP800-56A, using finite-field (1024-bit and 2048-bit) and elliptic curve (all NIST prime curves)

key agreement and tag computation, with all supported key sizes, shared secret computation modes and key derivation functions; also includes known answer tests for the HMAC tag computation used in the key agreement operation.

6. Known answer tests for KEA.
7. Known answer and pairwise consistency tests for RSA Key Transport Scheme (KTS) with OAEP padding and 1024-bit or 2048-bit keys, compliant with SP800-56B.
8. Known answer and pairwise consistency tests for RSA Key Transport Scheme (KTS) with PKCS#1v1.5 padding.
9. Tests of the random number generator
    a. Known answer tests for initialization and output.
    b. Continuous tests for repeated generator output.
    c. Continuous tests for repeated entropy seeding.
10. Firmware boot-up integrity test validating the hash of the firmware image in flash using a FIPS approved algorithm.
11. Firmware load test (conditional only) validating the digital signature of the loaded image using a FIPS approved algorithm.

4.6 Random Number Generation

Each processing core maintains the state for a deterministic random bit generator (DRBG) conforming to the HASH_DRBG specification in NIST Special Publication 800-90. All such instantiated DRBGs use the nondeterministic noise source present in the 3SGX for entropy input. Each generator is reseeded whenever random bits are requested, and both the generator and the noise source are subjected to a continuous test for repeated output.

4.7 Physical Security Policy

The 3SGX is permanently enclosed in a strong enclosure or coated with epoxy that provide tamper evidence. Compliance with FIPS physical security requirements was tested at room temperature. Removal of the enclosure or epoxy coat will render the 3SGX inoperable. Attempted tampering of the enclosure or epoxy coating that will lead to compromise is detectable by visual inspection. Either physical embodiment is opaque to visual inspection. Periodic visual inspection of the module is recommended in order to detect any evidence of tamper. The module hardness testing was only performed at a single temperature of 70° F and no assurance is provided for Level 3 hardness conformance at any other temperature.

Table 3 Inspection/Testing of Physical Security Mechanism

Physical Security Mechanism	Recommended Frequency of Inspection/Test	Inspection/Test Guidance Details
Enclosure or epoxy coating	6 months	Inspect 3SGX enclosure or epoxy coat on both sides to detect any evidence of tamper.

4.8 Mitigation of Other Attacks

The 3SGX includes a sensor that detects visible light. The presence of visible light as a result of tampering with the enclosure or epoxy coating will trigger an immediate zeroization of plaintext key material that is resident on the board. Temperature sensor informs the system management software of elevated temperature conditions in the module. This notification causes appropriate action, including shutdown, to be taken.

4.9 Key Management

The 3SGX supports the following functions performed on keys:

1. Generation,
2. Distribution,
3. Entry and output,
4. Storage,
5. Destruction,
6. Archival.

Keys, to include symmetric and asymmetric keys, are handled for the various algorithms enumerated above. Symmetric cryptographic keys are generated using the on-chip random number generator or loaded from external source. Asymmetric key pairs are generated in the 3SGX according to the relevant FIPS standard or loaded from an external source.

All keys are input and output only electronically from the module. The module does not allow plaintext keys to be input or output. All keys entering the 3SGX, regardless of key type, are encrypted using a FIPS approved algorithm.

Cryptographic keys are stored in wrapped form even when resident in board's memory and unwrapped when cryptographic operations are performed. Should the board transitions to the Alarm state, plaintext key material is zeroized.

The 3SGX system provides storage and retrieval of certificates issued by Government as well as commercial PKIs.

5 ROLES AND IDENTITIES

The 3SGX defines two types of roles for authorized access, supporting identity-based authentication conforming to FIPS level 3 requirements. It also supports a third role permitting authorized access to a non-authenticated user. These roles and identities for each token type are presented in Table 4 Roles, Identities, and Tokens. The strength of the authentication mechanism is shown in Table 5 Strengths of Authentication Mechanisms.

Table 4 Roles, Identities, and Tokens

Token Type	Identity	FIPS Role	Type of Authentication	Authentication Data
Board Token	1. Board Site Security Officer (SSO)	Crypto-Officer	Identity-based	PIN
	2. Board Operator (Administrator)	User	Identity-based	PIN
	3. Non-Authenticated User	Non-Authenticated Role	None	NA
Virtual Token	4. VT SSO	Crypto-Officer	Identity based	PIN
	5. VT Operator	User	Identity-based	PIN
	6. Non-Authenticated User	Non-Authenticated Role	None	NA

Table 5 Strengths of Authentication Mechanisms

Authentication Mechanism	Strength of Mechanism
PIN set independently for each identity of each token. Alphanumeric and special characters. Default size is 6. Can be as long as 12.	The probability that a PIN made up of random characters will succeed is 1 in 1.4×10^{11} (or 72^6) to 1 in 2×10^{22} (or 72^{12}). 3SGX only allows 10 failed attempts prior to requiring re-initializing the token offline.

PINs used for authentication by the 3SGX may contain arbitrary characters. The maximum size of a PIN is 12 characters. Assuming that a PIN is composed from a 72-character alphabet set, and a token allows a maximum of 10 unsuccessful login attempts, then a 4-character random PIN is sufficient to limit the probability of a successful 'false positive' authentication attempt to a probability of 10^{-6}. Tokens enforce a default minimum PIN size of 6 characters.

PIN submission is performed via electronic means and may be performed up to 20 times per second. The lower limit on PIN size described above is sufficient to lock a user token due to failed login attempts with a 10^{-5} probability of false-positive authentication within a 1-minute timeframe.

An individual may assume more than one of these identities at different times.

Each operator identity requiring authentication must present a unique, valid PIN to be authenticated successfully.

5.1 Board SSO Identity

The Board SSO identity is responsible for initialization and management of the Board Token. Services include setting of PIN phrases (SSO or User); archiving private keys on the Board Token; setting the Real-Time Clock (RTC) on the board; loading cryptographic keys, security parameters and trusted certificates; and, updating board firmware image.

5.2 Board Administrator Identity

The Board Administrator identity is responsible for managing the day-to-day operation of the 3SGX system and the contents of the VT database. The Board Administrator is responsible to transition the 3SGX from power-up state to an operational state, load VTs, monitor and reset the board, select audit levels, and archive or restore the VT database and database key. The Board Administrator can also update the board firmware image.

The Board Administrator uses the Board Token to perform these functions. The next two identities (VT Operator and VT SSO) cannot request security services from the 3SGX board until the Board Administrator has transitioned it to operational state.

5.3 VT SSO Identity

Each User VT supports its own SSO operator. The VT SSO identity provides initialization services similar to those of the Board SSO identity, except that the scope of these services is limited strictly to the VT. This identity loads cryptographic keys, security parameters and trusted certificates into a User VT in the same way that the Board SSO identity loads the Board Token.

5.4 VT Operator Identity

Each Virtual Token supports an identity that can request cryptographic services from the 3SGX board; this is the VT Operator identity. All security services and algorithms listed previously in Section 4.2 are available to the VT Operator. User/application that require 3SGX services must be authenticated as VT Operator in order to activate its VT and gain access to the services.

5.5 Non-Authenticated Identity

For both token types, a non-authenticated user has authorized access to non-security-relevant information without requiring identity-based authentication.

5.6 Crypto-Officer Guidance

The token Crypto-Officer (SSO for board or VT) is responsible for initializing the token. Without this operation, the token cannot be used. The CO is authenticated prior to accepting any initialization commands. Once programmed, a user can access the 3SGX security services. Refer to Table 7 for a detailed list of services available to the Crypto-

Officer. Refer to Section 6.2 for guidance on zeroizing plaintext keys and CSPs which may be especially helpful in the event the 3SGX is removed from service.

5.7 User Guidance

The Board User (Administrator) must authenticate his/her identity to the board prior to a VT Crypto-Officer or VT User has access to the 3SGX services. The VT User (Operator) is allowed access to services only after the VT Crypto-Officer has initialized a VT.

6 SERVICES AND RULES

The services provided by the 3SGX system can be broken down into two broad categories, Cryptographic Services and Management/Administrative Services

6.1 3SGX Cryptographic Services

Cryptographic services involve operations on security-relevant data. The 3SGX security design will ensure that only authorized users and applications access 3SGX services and that only they have access to the specific services corresponding to the roles. The data items affected by these operations are listed in Table 6 below.

Table 6 Security Relevant Data Items (SRDI)

SRDI	Description
Database Key (Kd)	The Key that is used to protect the VT database
Manufacturer Default PIN	The PIN phrase that must be entered to log in to an uninitialized Virtual Token
Message Encryption Key (MEK)	A symmetric bulk encryption key
VT SSO PIN	The PIN phrase that must be input to assume the VT SSO identity
Board SSO PIN	The PIN phrase that must be input to assume the Board SSO identity
Token Encryption Key (TEK)	A symmetric key used to wrap other symmetric or asymmetric keys
Board Administrator PIN	The PIN phrase that must be input to assume the Board Administrator identity
VT Operator PIN	The PIN phrase that must be input to assume the VT Operator identity
Storage Key Variable (Ks)	A symmetric key stored permanently in its own token key register; used for encrypting asymmetric keys generated by or loaded into the token. Also functions as a TEK
Key File Encryption Key (KFEK)	A symmetric key derived from the PIN of one of the four 3SGX Identities, and used to encrypt the Ks of the Board Token (Board SSO or Board User Identity) or Virtual Token (for VT User or VT SSO Identity).
Key Entry Key (KEK)	A symmetric key used to encrypt plaintext keys prior to entry into the module
Firmware Load Public Key	An asymmetric public key resident in firmware, used to verify the signature on firmware images that are conditionally loaded
Board Token Zeroize Default PIN	The Board SSO PIN phrase that must be entered to log on to the Board Token once it has been zeroized.
User VT Zeroize Default PIN	The VT SSO PIN phrase that must be entered to log

SRDI	Description
	onto a Virtual Token once it has been zeroized.
RNG state	The V component of the random number generator state, defined by NIST SP800-90 (888 bits)
RNG seed	The output from the on-chip noise source, corresponding to the entropy_input value defined by NIST SP800-90 (192 bits)
Signature Key Pair	An asymmetric key used for digital signature. The private key is wrapped in Ks until used
Global Signature Key Pair	A key pair that can be used by all VTs for digital signatures.
Key Agreement or Key Transport Key Pair	An asymmetric key used for key agreement or key transport. The private key is wrapped in Ks until used

Table 7 below lists all 3SGX Cryptographic Services available by role. Unless indicated otherwise, successful authentication by a particular identity performing a particular role is required before being allowed to access the services listed in Table 7. See Section 5 for an explanation of the identities supported by the 3SGX.

Table 7 Services and Rules for Cryptographic Operations

Board Operator	VT Operator	Board SSO	VT SSO	Non-Auth Role	Service	CSPs and Keys
		Create / Write	Create / Write		Generate/Load Storage Key (Ks)	Ks
Create / Delete	Create / Delete				Generate/Load/Delete MEK	MEK
Create / Delete	Create / Delete				Generate/Delete TEK	Use key agreement key pair to create TEK
Create	Create	Create	Create		Generate/Load Signature key pairs	Signature key pair
Create	Create	Create	Create		Generate/Load Key Agreement or Key Transport key pairs	Key agreement or key transport key pair
Write					Load Global Signature Keys	Global signature key pair
Write	Write	Write	Write	Write	Load Global Application Signature Public Keys	Global signature public key[1]

[1] Loaded as part of factory installation.

Board Operator	VT Operator	Board SSO	VT SSO	Non-Auth Role	Service	CSPs and Keys
		Write	Write		Load Trusted Certificate	NA
Write	Write	Write	Write		Load All other Certificates	NA
Delete	Delete	Delete	Delete		Delete Certificates	NA
Read	Read	Read	Read		Retrieve Certificates	NA
Use	Use				Encrypt	MEK
Use	Use				Decrypt	MEK
Use	Use				Hash	NA
Use	Use				Generate / Verify Digital Signature	Signature key pair
Use	Use				Generate / Verify Timestamp	Signature key pair
		Export	Export		Extract Private Keys (export service)	Use key agreement key pair to generate TEK and export an asymmetric private key (signature, key transport or key agreement)
Import	Import	Import	Import		Relay/Install Private Keys (import service)	Use key agreement key pair to generate TEK and import an asymmetric private key (signature, key transport or key agreement)
Export	Export				Encrypt Symmetric Keys	Wrap MEK with TEK or with Key Transport key pair
Export / Import	Export / Import				Save/Restore Crypto State	NA
Read	Read	Read	Read	Read	View Time	NA
		Write			Set Time	NA
		Write			Update Firmware	NA
Read	Read	Read	Read	Read	View Status/ Configuration	NA
Read	Read	Read	Read	Read	Generate Random Numbers	RNG state
Delete	Delete	Delete	Delete	Delete	Zeroize Token	All token CSPs
Execute	Execute	Execute		Execute	Self-Tests	NA

Board Operator	VT Operator	Board SSO	VT SSO	Non-Auth Role	Service	CSPs and Keys
Use	Use	Use	Use		Authenticate with PIN Note: VT Operator/Board Administrator locked out after a number of unsuccessful PIN check attempts; for VT SSO and Board SSO, token is zeroized after a number of unsuccessful PIN check attempts	PIN, KFEK
Create	Create	Create	Create		Change Pin	PIN, KFEK

6.2 Zeroization

Cryptographic keys and CSPs are stored in wrapped form even when resident in board DRAM or NVRAM, and unwrapped into private per-core memory when cryptographic operations are performed. Thus, when the board transitions to the Alarm state and plaintext cryptographic keys and CSPs must be erased, only these private memory regions and the cryptographic hardware blocks in each core are affected. A secure erase firmware routine zeroizes plaintext cryptographic keys and CSPs on the board.

6.3 3SGX Management/Administration Services

Table 8 below lists all the 3SGX Management/Administrative Services available on the 3SGX board to the operators. These services are not available to the VT Operator or VT SSO identities.

Table 8 3SGX Management Services

Service	Board Administrator Identity	Board SSO Identity
Board Token Initialization		✓
Update Board Firmware	✓	✓

Service	Board Administrator Identity	Board SSO Identity
Management of Virtual Tokens	✓	
Management of Database Key	✓	
System Monitoring	✓	

Brief details on the 3SGX Management/Administration Services follow.

6.3.1 Board Token Initialization

Initializing the Board Token is primarily the responsibility of the Board SSO identity. This identity sets PIN phrases and loads Ks, asymmetric keys, and certificates.

6.3.2 Update Board Firmware

The Board SSO and Administrator are responsible for updating the firmware on the board.

6.3.3 Management of User VTs

A user/application can only use 3SGX once the board has been transitioned to an operational state; only then can the VT Operator access his/her token. The 3SGX Administrator must log in to the Board Token with the Board Administrator PIN to transition the board(s) from an initialized to an operational state.

The steps required to initialize a User VT match those of initializing the Board Token with the exception that the VT SSO (not the Board SSO) performs the initialization process. The 3SGX host software and board firmware implement measures to securely import an encrypted User VT image into the 3SGX. Only the Board Administrator can perform this initialization service following a successful Board Token login.

6.3.4 Management of Database Key

Only the 3SGX Administrator has means to manage the VT database and to create, save and restore the board key that encrypts the database. The Board Administrator also has the means to re-encrypt, archive and restore a VT database. The 3SGX Administrator can perform this service following a successful Board Token login.

6.3.5 System Monitoring

The 3SGX Administrator, through host software, can view 3SGX system information such as system status, board status, etc. The 3SGX Administrator can also view the audit information generated by the 3SGX system.

7 ALGORITHM CERTIFICATES

Algorithm	CAVP Certificate Number
AES	2038
Triple-DES	1315
DSA	646
RSA	1058
ECDSA	297
SHS	1784
DRBG	200
HMAC	1237
KAS	35
Skipjack	19
CVL	25

8 ACRONYMS AND ABBREVIATIONS

Term	Definition
3SGX	3S Group Cryptographic Module
CA	Certificate Authority
DRBG	Deterministic Random Bit Generator
ECC	Elliptic Curve Cryptography
FIPS	Federal Information Processing Standard
Ks	Storage Key
Kd	Database Key
KDF	Key Derivation Function
MEK	Message Encryption Key
NIST	National Institute of Standards and Technology
PCIe	Peripheral Component Interconnect (PCI) Express
PIN	Personal Identification Number
PKI	Public Key Infrastructure
RNG	Random Number Generator
TEK	Token Encryption Key
SSO	Site Security Officer
VT	Virtual Token