FIPS 140-2 Security Policy
EXP9000 Hardware Security Module

Document Version 1.1

July 2011

Futurex
864 Old Boerne Rd.
Bulverde, TX 78163
USA

Telephone: 830-980-9782
Toll-Free: 1-800-251-5112
Fax: 830-438-8782

TABLE OF CONTENTS

1. Module Overview 3
2. Security Level 4
3. Modes of Operation 5
3.1. Approved mode of operation 5
3.2. Non-FIPS mode of operation 6
4. Ports and Interfaces 7
5. Identification and Authentication Policy 8
5.1. Assumption of roles 8
6. Access Control Policy 9
6.1. Unauthenticated Services 9
6.2. Authenticated Services 9
6.3. Definition of Critical Security Parameters (CSPs) 11
6.4. Definition of Public Keys 12
6.5. Modes of Access for CSPs 13
7. Operational Environment 15
8. Security Rules 15
8.1. Self-Tests 16
8.1.1. At Power-Up 16
8.1.2. Conditional Self-Tests 16
9. Physical Security Policy 17
9.1. Physical Security Mechanisms 17
9.2. Operator Recommended Actions 17
10. Mitigation of Other Attacks 18
11. Design Assurance 18
11.1. Configuration Management 18
11.2. Guidance Documents 18
12. References 18
13. Glossary 19

1. Module Overview

The EXP9000 Hardware Security Module (HW P/N 9750-2075, Revision B FW Version 4.0.0) is a multi-chip embedded cryptographic module that provides data security and encryption processes for business and financial communities. The module is physically protected by a tamper resistant and evident casing where all cryptographic operations are performed. Additionally, operations are protected with a tamper response that will erase critical security parameters upon detection of intrusion. The module is assembled from production quality components and provides gigabit Ethernet and PCIe interfaces for control input, data input, data output, status output and includes a USB interface for status output. The image below depicts the cryptographic module and provides a visual indication of the black epoxy that defines the cryptographic boundary.

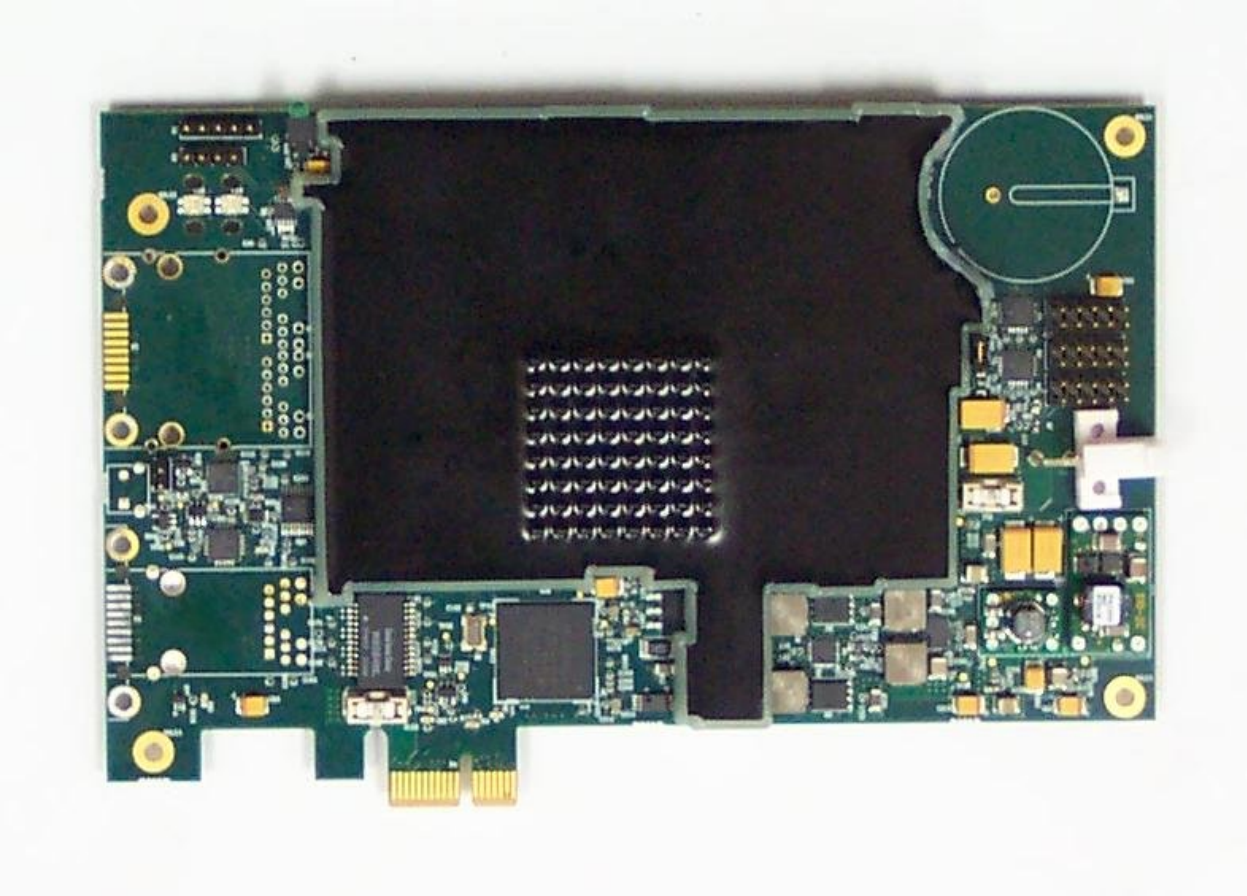

Figure 1 – EXP9000 Cryptographic Module

2. Security Level

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

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	N/A

Table 1 - Module Security Level Specification

3. Modes of Operation

3.1. Approved mode of operation

Approved Functions

In FIPS mode, the cryptographic module supports the FIPS approved algorithms:

- RSA with 1024 bit keys for key generation, digital signature generation and verification (cert #810)
- RSA with 2048 bit keys for key generation, digital signature generation and verification (cert #810)
- AES with 128, 192 and 256 bit keys for encryption and decryption (cert #1636)
- Triple-DES (two key) for encryption and decryption (cert #1072)

  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.
- Triple-DES (three key) for encryption and decryption (cert #1072)
- SHA-1 for hashing (cert #1441)
- SHA-256 for hashing(cert #1441)
- HMAC-SHA-1 for keyed message authentication (cert #962)
- RNG (ANSI X9.31) for random number generation (cert #877)

Allowed but not Approved Functions

- RSA 2048 Encrypt/Decrypt for key transport (key wrapping; key establishment methodology provides 112 bits of encryption strength)
- MD5 with TLS 1.0
- NDRNG used for RNG seed data

Non Approved functions:

- DES: No security is claimed. Provided for legacy use.
- TR-31: No security is claimed. Key Block Specification

The cryptographic module may be configured for FIPS mode by initiating the module's Initialization service. To perform the Initialization service while in non-FIPS mode, an operator must access the module's web interface and update the device configuration accordingly on the *Initial Setup* tab. As part of the Initialization service, the module will zeroize all CSPs and transition to the FIPS mode of operation. The user can determine if the cryptographic module is running in FIPS vs. non-FIPS mode via the "Status" service.

Data input to and data output from the cryptographic module are entered over an established TLS encryption session or in encrypted form. The module negotiates a session using a 2048 bit certificate and operates with a TLS compliant cipher suite for key transport. Cryptographic keys are generated from the approved RNG and seeded from a system RNG device.

3.2. Non-FIPS mode of operation

In non-FIPS mode, the cryptographic module provides all FIPS Approved algorithms as well as the following non-FIPS Approved algorithms:

- MD5 for hashing
- DES for encrypt/decrypt
- RSA 512

4. Ports and Interfaces

The cryptographic module provides the following physical ports and logical interfaces:

- Ethernet port (x2): control input, data input, data output, status output
  - This Ethernet port will allow dual authenticated, encrypted communication sessions to be established using the TLS protocol.
  - This Ethernet port will allow encrypted communication sessions for control input, data input, data output, and status output through a TLS session.
- PCI Express: Control input, data input, data output, status output
  - This PCI Express port will allow dual authenticated, encrypted communication sessions to be established using the TLS protocol.
  - This PCI Express port will allow encrypted communication sessions for control input, data input, data output, and status output through a TLS session.
- USB Host Interface: Control input, data input, data output, status output
- USB Device Interface: Disabled
- Serial port 1 (Factory Init): Disabled
  - This serial port shall be used for factory initialization of the cryptographic module.
  - This serial port shall be disabled via software during the approved mode of operation.
- Serial port 2: Disabled
- Serial port 3: Disabled
- Serial port 4 (Setup Init): Disabled
  - This serial port shall be used for setup initialization of the cryptographic module.
  - This serial port shall be disabled via software during the approved mode of operation.
- I^2C port: Status output
- LEDs (x8): Status output
- Main power port (over PCIe bus): power interface
- External Power Interface: power interface
- Reset port: Control input
- Battery power port: power interface

5. Identification and Authentication Policy

5.1. Assumption of roles

The cryptographic module shall support two distinct operator roles (User and Crypto-Officer). In the Approved mode, an 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. An operator must enter an initial username and password to log in. The username is an alphanumeric string of one to fifteen characters and default passwords must be updated upon initial login. The password is an alphanumeric string of five to nineteen characters chosen from the 90 printable and human-readable characters. When entering a password, the characters are echoed back to the operator as stars. An operator that provides a valid username and password will be identified as a User or Crypto Officer and must re-authenticate to change identity or role. At the end of a session, the operator may logout. Operator authentication is cleared at power down and a session shall timeout after 300 seconds. In order to re-establish communication after an operator logout or timeout, an operator must re-authenticate.

5.2. Roles and Required Identification and Authentication

Role	Type of Authentication	Authentication Data
User	Identity-based	User name and password TLS RSA 2048 bit Certificate
Crypto-Officer	Identity-based	User name and password TLS RSA 2048 bit Certificate

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 1/5,904,900,000 (90^5), which is less than 1/1,000,000. The probability of successfully authenticating to the module within one minute is less than 1/100,000. The module allows for 3 failed attempts and then times out for 30 seconds before retry. A max number of 6 tries in one minute is possible.
TLS session	The probability that a random attempt will succeed or a false acceptance will occur is 1/3.403e38 (2^{128}), which is less than 1/1,000,000. The probability of successfully authenticating to the module within one minute is 1/6.236e47, which is less than 1/100,000.

Table 3 - Strengths 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. (Zero all CSPs, set passwords back to default)

6.2. Authenticated Services

Role	Authorized Service
User: This role shall provide all of the services necessary for the secure transport of data over an insecure network.	• Create Session: This service will enable the operator to establish an encrypted TLS session. • Process Transactions: This service will enable the operator to communicate with the cryptographic module once a TLS session is established. • Logout: This service will enable the operator to log off from the device and close the encrypted TLS session link.
Cryptographic-Officer: This role shall provide services necessary for configuration of the cryptographic module.	• Create Session: This service will enable the operator to establish an encrypted TLS session. • Initialization: This service shall enable a Crypto-Officer to initialize the cryptographic module. This service shall reboot the module and utilize the Zeroize and Self-test services. If the module is already in FIPS mode, it will remain in FIPS mode. If the module is not in FIPS mode, it will transition into FIPS mode. Once initialized, this service is not required on power up to remain in FIPS mode. Transitioning out of FIPS mode shall call the Zeroize service and then reboot the module. In order to transition back into FIPS mode, the Initialization service must be called. • Zeroize: This service actively destroys all critical security parameters. • Process Transactions: This service will enable the operator to communicate with the cryptographic module once a TLS session is established.

	• Update Firmware: This service shall enable the operator to update the cryptographic module's firmware through an established TLS session to either of the module's Ethernet ports. Firmware authenticity is verified using an RSA signature. This service shall utilize the Zeroize service and reboot the module. • User Administration: This service will allow an operator to create new user certificates. • Logout: This service will enable the operator to log off from the device and close the encrypted TLS session link

Table 4 - Authorized Services by Role

Service	Control Input	Data Input	Data Output	Status Output
Create Session	Header Info	Signed Plaintext Data	Encrypted Data	
Process Transactions	Header Info	Encrypted Data	Encrypted Data	Plaintext Status Data
Logout	Header Info			
Status				Plaintext Status Data
Initialization	Header Info	Encrypted Data	Encrypted Data	Success / Fail
Zeroize	Header Info			Success / Fail
Self-Tests				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 service	Header Info			Success

Table 5 - Specification of Service Inputs & Outputs

6.3. Definition of Critical Security Parameters (CSPs)

CSPs are stored in either RAM or SRAM, which is secured within the cryptographic boundary, as unencrypted plaintext or binary data. Operators will not be allowed to directly access CSPs within the device. The following are CSPs contained in the module:

CSP	Type	Description
Server Private Key	RSA 2048	Decrypt data sent to the device from an operator during the creation of a TLS session.
Session Hash Key	HMAC-SHA-1	Used for hashing data passed between an operator and the device during an established TLS session
Session Encryption Key	AES-256	Encrypts / Decrypts data passed between an operator and the device during an established TLS session
Crypto-Officer Password	Pass-phrase	Used to authenticate the identity of a Crypto-Officer.
User Password	Pass-phrase	Used to authenticate the identity of a User.
Seed Key	NDRNG Value	Seed Key for RNG
Seed Value	NDRNG Value	Seed for RNG
Master File Key	TDES 112 or 168	Master File Key for encrypting CSPs
Key Exchange Key	TDES 112 or 168	Key Exchange Key
Backup Key	TDES 112 or 168	Backup Key
Pending Master File Key	TDES 112 or 168	Pending Master File Key
Smart Card Encryption Key	TDES 112 or 168	Smart Card Encryption Key
User Keys	TDES 112 or 168, RSA 512*, 1024, 2048	Data encryption, key exchange keys, MAC keys used by user

*** No security is being claimed by the use of RSA 512. RSA 512 is only supported in non-FIPS mode.**

Table 6 - Critical Security Parameters

6.4. Definition of Public Keys

The following are the public keys contained in the module:

- Server Public Key: The public key component of the server certificate.
- Firmware Public Key: This public key is used for signature verification of the firmware and firmware updates in order to protect against unauthorized modification.
- Feature Public Key: This public key is used to decrypt feature/configuration options.
- User Public Keys: These public keys are always used by the user.

6.5. Modes of Access for CSPs

Table 7 provides a list of supported access operations by the cryptographic module. Access rights for the supported modes of access are shown in table 8 below. Supported Access operations are defined as follows:

- Generate Functions: These operations generate a particular CSP within the cryptographic module.
- Load Functions: These operations allow for a particular CSP to be loaded into the cryptographic module.
- Wrap Functions: These operations encrypt a particular CSP.
- Un-wrap Functions: These operations decrypt a particular CSP.
- Destroy: These operations erase the CSP from the cryptographic module.

CSP	Operation				
	Generate	**Load**	**Wrap**	**Un-wrap**	**Destroy**
Server Private Key	×				×
Session Encryption Key	×		×	×	×
Session Hash Key	×		×	×	×
Crypto-Officer Password		×			×
User Password		×			x
Master File Key			×	×	x
Key Exchange Key			x	x	x
Backup Key			x	x	x
Pending Master File Key			x	x	x
Smart Card Encryption Key			x	x	x
User Keys			×	×	x
Seed Key	x				x
Seed	x				x

Table 7 - Supported Access Operations

User Role	CO Role	U/A*	Service	Cryptographic Keys and CSPs Access Operation
×	×		Create Session	Generate Session Encryption and Hash keys
×	×		Process Transactions	Wrap and un-wrap with Session Encryption and Hash keys
×	×		Logout	Destroy Session Encryption and Hash keys
		×	Status	
	×		Zeroize	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
	×		Initialization	Zeroize and generate Server Private and Public Key
		×	Self-Tests	
	×		User Administration	Load CO/User Names and Passwords Destroy CO/User Names and Passwords
	×		Update Firmware	Verify with Firmware Public Key
		×	Factory Reset	Zeroize CSPs and restore factory defaults

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

Table 8 - CSP Access Rights within Roles & Services

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 two distinct operator roles. These are the User role, and the Cryptographic-Officer 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 traffic using an approved TLS cipher suite.
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. At 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 internal RNG and NDRNG 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. The module shall not provide access to revenue related data structures while plaintext CSPs are present.
14. 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 an error state.

8.1.1. At Power-Up

The following tests shall be performed at power-up:

- Known Answer Tests for:
  - AES
  - Triple-DES
  - RNG
  - SHA
  - RSA
  - HMAC
- Firmware Integrity Test (RSA signature)

8.1.2. Conditional Self-Tests

The device will perform the following conditional self-tests:

- Continuous Random Number Generator Tests for NDRNG and Approved RNG
- Pair-wise Consistency Test for RSA key generation
- Firmware Load Test (RSA 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 module and removal or intrusion attempts will result in serious damage, which will cause the module to stop functioning.
- The module includes tamper response and CSP zeroization; however, the potting material alone provides the required FIPS 140-2 Level 3 physical security protections. Tamper response and CSP zeroization were not tested as part of the validation and provide no FIPS related security or functionality.

Note: Module hardness testing was only performed at ambient temperature. No assurance is provided for Level 3 hardness conformance at any other temperature.

9.2. 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

10. Mitigation of Other Attacks

The module has not been designed to mitigate against specific attacks as described in FIPS 140-2 Area 11.

11. Design Assurance

11.1. Configuration Management

Documentation for the cryptographic module, which includes hardware specifications, software components, firmware source code, guidance documents, and FIPS documents, is maintained using a Subversion repository. All configuration management items are uniquely identified by a path and filename within the Subversion repository. All configuration management items have a uniquely identifiable version based on the item's Subversion revision number.

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

12. 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.

13. Glossary

Term	Definition
ANSI	American National Standards Institute
CA	Certificate Authority
CO	Cryptographic Officer

Term	Definition
CRC	Cyclic Redundancy Check
CSP	Critical Security Parameter
DES	Data Encryption Standard
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