Excrypt Cryptographic Module

Security Policy

Document Version 1.8

April 2007

TABLE OF CONTENTS

1. Module Overview

The Excrypt Cryptographic Module (HW P/N 9750-0235-R, Version 1.1; FW Version 2.4.1) is a multi-chip embedded cryptographic module encased in a hard opaque potted enclosure. Within the potted enclosure, all cryptographic operations and secure information is protected using a tamper wire sensor and response circuitry that will cease operation and erase secure information upon detection of penetration. The primary purpose for this device is to provide data security and encryption processes for the business and financial communities. The device provides status output via an LCD and IP network/serial interface. The device provides a network interface for data input/output and control input. The picture below depicts the cryptographic module and provides a visual indication of the black epoxy that defines the cryptographic boundary.

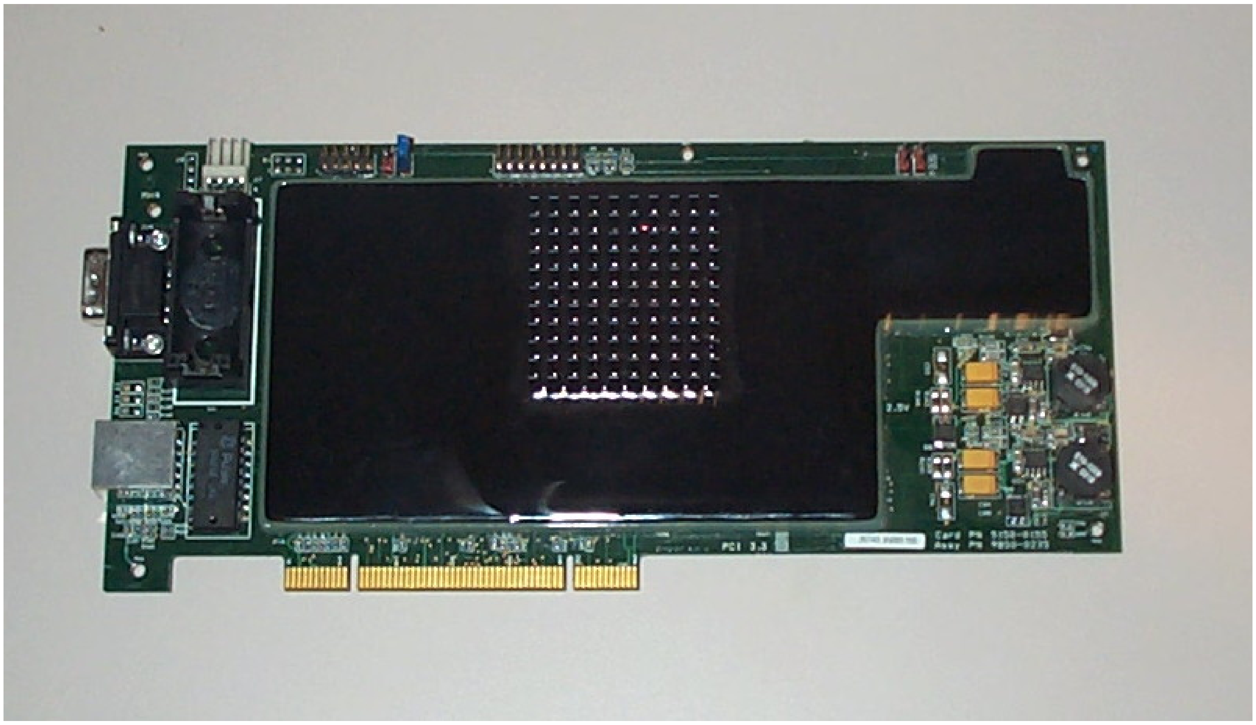

Figure 1 - Excrypt Cryptographic Module

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

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

- RSA with 1024 bit keys for key transport, digital signature generation and verification
- RSA with 2048 bit keys for key transport, digital signature generation and verification
- Triple-DES (three key) for encryption and decryption
- Triple-DES (two key) for encryption and decryption
- Single-DES (single key) for encryption and decryption [for legacy systems only; transitional phase only – valid until May 19, 2007]
- SHA-1 for hashing
- RNG (X9.31) for deterministic random number generation
- HMAC-SHA-1 for keyed message authentication

The cryptographic module supports the commercially available TLS protocol for key establishment. Although MD5 is not a FIPS approved algorithm, MD5 is used in the approved mode of operation only as specified and required by the TLS Version 1.0 protocol.

Data input to and data output from the cryptographic module utilizes an established TLS session. A TLS session uses the approved RSA implementation for key transport, digital signature generation and verification via TLS session certificates containing 2048 bit key components. The TLS session operates with the compliant Triple-DES implementation for all data encryption and decryption through the cryptographic module.

The cryptographic module relies on the implemented pseudo random number generator (PRNG) that is compliant with ANSI X9.31 and constructed from two-key Triple-DES for generation of cryptographic keys. Intermediate key values are not outputted from the module. Each call to the PRNG produces a 64-bit block of pseudo random data. PRNG seed and seed key inputs are generated from an independent hardware-based PRNG that must pass the 64-bit continuous random number generator test.

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 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.

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

4. Ports and Interfaces

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

- Ethernet port: 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.
- Serial port 1 (Factory Init): data input, data output
    - This serial port shall be used for factory initialization of the cryptographic module.
    - This serial port shall be disabled during the approved mode of operation.
- Serial port 2 (Factory Init): control input, data input, data output
    - This serial port shall be used for factory initialization of the cryptographic module.
    - This serial port shall be disabled during the approved mode of operation.
- I^2C port (LCD): status output
    - The I^2C port provides status output only.
- Main power port (over PCI bus):
    - This port is the primary power interface for the module and is supplied via the PCI bus.

- Battery power port:
  - Allows the module to be supplied power for maintaining configuration settings and operating the physical security circuitry while main power is removed.

5. Identification and Authentication Policy

5.1. Assumption of roles

The cryptographic module shall support two distinct operator roles (User and Crypto-Officer). An operator may communicate with the cryptographic module through a TLS session with valid TLS session certificates. Multiple concurrent operators shall be supported and shall be distinguished by independent TLS sessions. The cryptographic module shall enforce the separation of roles using identity-based operator authentication. An operator must have a valid TLS session certificate to communicate with the module via the Ethernet port. A Crypto-Officer must enter a username and password to log in. The username is an alphanumeric string of one to fifteen characters. The password is an alphanumeric string of four to nineteen characters randomly chosen from the 90 printable and human-readable characters. When entering a password, the characters are either not echoed back to the operator or echoed as stars. An operator that provides a valid username and password is a Crypto-Officer. At the end of a session, the operator may logout. After a period of inactivity, an operator's TLS session shall timeout. In order to re-establish communication after a timeout, an operator must re-authenticate.

Role	Type of Authentication	Authentication Data
User	TLS session	TLS session certificate
Crypto-Officer (via Ethernet port)	TLS session and Identity-based authentication	TLS session certificate with Username and Password

Table 2 - Roles and Required Identification and Authentication

Authentication Mechanism	Strength of Mechanism
Username and Password	The probability that a random attempt will succeed or a false acceptance will occur is 1/65,610,000 (90^4), which is less than 1/1,000,000. The probability of successfully authenticating to the module within one minute is 1/109,350, which is less than 1/100,000.
TLS session	The probability that a random attempt will succeed or a false acceptance will occur is 1/3.741e50 (2^{168}), 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.

TLS session with Username and Password	The probability that a random attempt will succeed or a false acceptance will occur is 1/2.455e58 (2^{168}×90^4), which is less than 1/1,000,000. The probability of successfully authenticating to the module within one minute is 1/4.091e55, 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 LCD or Ethernet port.
- Self-tests: This service will enable an operator to initiate the suite of self-tests required by FIPS 140-2.

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 using a Triple-DES session key. • 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 using a Triple-DES session key. • 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

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. For more information on the storage of CSPs refer to Section 6.6 on Key Management. Operators will not be allowed to directly access CSPs within the device. The following are CSPs contained in the module:

CSP	Type	Description
Master Certificate Key (MCK)	The private part of a RSA key pair	Used for signing Server Certificates and User Certificates. Server and User Certificates contain both the private and public key components.
Server Certificate Key (SCK)	The private part of a RSA key pair	The private key component is used to decrypt data sent to the device from an operator during the creation of a TLS session. The public key component is used to encrypt data sent to the device from an operator during the creation of a TLS session.
User Certificate Key (UCK)	The private part of a RSA key pair	The private key component is used to decrypt data sent to an operator from the device during the creation of a TLS session. The public key component is used to encrypt data sent to an operator from the device during the creation of a TLS session.
Session Encryption Key (SEK)	Triple-DES key	Encrypts / Decrypts data passed between an operator and the device during an established TLS session. This key is generated by the device and encrypted under the UC.
Session Hash Key (SHK)	Triple-DES key	Used for hashing data passed between an operator and the device during an established TLS session. This key is generated by the device and encrypted under the UC.
User Password	Pass-phrase	Used for obfuscating the UCK and UC when being exported by a Crypto-Officer. The use of this password to obfuscate the UCK and UC does not provide any additionally security. The security of the exported UCK and UC is contingent on the prior establishment of a valid TLS session. This pass-phrase is not stored within the module.
Crypto-Officer Password	Pass-phrase	Used to authenticate the identity of a Crypto-Officer.

Table 6 - Critical Security Parameters

6.4. Definition of Public Keys

The following are the public keys contained in the module:

- Master Certificate Public Key: The public key component of the MCK. This public key accompanies the private key component of the MCK and is also included in the Master Certificate.

- Server Certificate Public Key: The public key component of the SCK. This public key accompanies the private key component of the SCK and is also included in the Server Certificate.
- User Certificate Public Key: The public key component of the UCK. This public key accompanies the private key component of the UCK and is also included in the User Certificate. This key is Triple-DES encrypted under an operator provided pass-phrase and may be checked for unauthorized modification by verifying the User Certificate's signature.
- Futurex Public Key: This public key is used for signature verification of the firmware and firmware updates in order to protect against unauthorized modification.

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**
MCK	×				×
MC	×				×
SCK	×				×
SC	×				×
UCK	×		×	×	
UC	×		×	×	
SEK	×		×	×	×
SHK	×		×	×	×
User Password		×	×	×	
Crypto-Officer Password		×	×	×	×

Table 7 - Supported Access Operations

Role		**Service**	**Cryptographic Keys and CSPs Access Operation**
User	**Crypto-Officer**		
×	×	Create Session	Generate SEK, Generate SHK Wrap SEK, Un-wrap SEK Wrap SHK, Un-wrap SHK
×	×	Process Transactions	Wrap MCK, Wrap SCK
×	×	Logout	Destroy SEK, Generate SHK
×	×	Status	
	×	Initialization	Generate MCK, Generate MC Generate SCK, Generate SC Generate UCK, Generate UC Wrap MC, Wrap SC Wrap UCK, Wrap UC Destroy CO Password
	×	Zeroize	Destroy MCK, Destroy MC Destroy SCK, Destroy SC Destroy CO Password
×	×	Self-Tests	
	×	User Administration	Wrap UC, Wrap UCK Un-wrap UC, Un-wrap UCK Load User/CO Password Wrap User/CO Password Un-wrap User/CO Password Destroy CO Password
	×	Update Firmware	Destroy MCK, Destroy MC Destroy SCK, Destroy SC Destroy CO Password

Table 8 - CSP Access Rights within Roles & Services

6.6. Key Management

The following table provides an overview of the lifecycle for secret, private, and public keys:

CSP / Key	Location	Created by	Destroyed by
MCK	SRAM	Module, TLS Init State	Zeroize Service
MC	RAM	Module, TLS Init State	Zeroize Service
SCK	SRAM	Module, TLS Init State	Zeroize Service
SC	RAM	Module, TLS Init State	Zeroize Service
UCK	Not stored	Module, at request of Crypto-Officer	
UC	Not stored	Module, at request of Crypto-Officer	
SEK	RAM	Module, Create Session Service	Module at end of TLS Session
SHK	RAM	Module, Create Session Service	Module, at end of TLS Session
User Password	Not stored	Crypto-Officer, Manual entry	
Crypto-Officer Password	SRAM	Default set by manufacturer, or manually set by Crypto-Officer	Initialization Service, Zeroize Service, Update Firmware
Master Certificate Public Key	RAM	Module, TLS Init State	Zeroize Service
Server Certificate Public Key	RAM	Module, TLS Init State	Zeroize Service
Futurex Public Key	Flash	Manufacturer	

Table 9 - Key Management

6.7. First-Time Authentication

After receiving the module from the manufacturer, first-time authentication takes place when a Crypto-Officer attempts to access the module's configuration for the first time. To access the module's configuration settings, two Crypto-Officers must use a TLS Session with the Futurex supplied certificate to authenticate through the Ethernet port. Crypto-Officers are required to provide valid username/password combinations in order to access the module's configuration.

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 the Triple-DES algorithm.
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 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. Presently, the module will support a maximum of 20 individual users.
15. 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.
16. The cryptographic module shall perform a checksum (CRC32) on SRAM upon power-up.

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:
    - DES CBC mode (encrypt/decrypt)
    - Triple-DES CBC, ECB modes (encrypt/decrypt)
    - PRNG
    - SHA-1
    - RSA (encrypt/decrypt and sign/verify)
    - HMAC-SHA-1
- Pair-wise Consistency Test for RSA key generation and signature generation/verification
- Firmware Integrity Test (32-bit CRC)

8.1.2. Conditional Self-Tests

The device will perform the following conditional self-tests:

- Continuous Random Number Generator Test (64-bit blocks)
- 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:

- Tamper response and zeroization circuitry.
- Hard potting material encapsulation of multiple chip circuitry enclosure with removal/penetration attempts causing serious damage and tamper response.

9.2. Operator Required Actions

The operator is 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	If applicable, inspect hard potting for removal/penetration attempts. If applicable, inspect enclosure for entry attempts.

Table 10 - 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, 2005 May 19.
3. Annex B: Approved Protection Profiles for FIPS PUB 140-2, *Security Requirements for Cryptographic Modules*, Draft, National Institute of Standards and Technology, 2004 November 04.

4. Annex C: Approved Random Number Generators for FIPS PUB 140-2, *Security Requirements for Cryptographic Modules*, Draft, National Institute of Standards and Technology, 2005 January 31.
5. Annex D: Approved Key Establishment Techniques for FIPS PUB 140-2, *Security Requirements for Cryptographic Modules*, Draft, National Institute of Standards and Technology, 2005 September 12.
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, 2005 December 01.
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 March 01.
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

ANSI	American National Standards Institute
CA	Certificate Authority
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^{2}C	Inter-Integrated Circuit
IP	Internet Protocol
LCD	Liquid Crystal Display
MD5	Message Digest 5
NIST	National Institute of Standards and Technology
PRNG	Pseudo Random Number Generator
RNG	Random Number Generator
RSA	Rivest-Shamir-Adelman public key algorithm
SHA	Secure Hash Algorithm
SHS	Secure Hash Standard