High Assurance 2000 Gateway

Security Policy
(Non-Proprietary)

FIPS140-2 Level-2 Validation
May 2005

Document Version 1.05

Table of Contents

1 INTRODUCTION

1.1 Purpose

This is a non-Proprietary FIPS 140-2 Security Policy for the SafeNet HA2000. The Security Policy describes how the HA2000 meets all FIPS 140-2 Level 2 requirements, and was prepared as part of the HA2000's FIPS 140-2 certification submission package.

FIPS 140-2 (Federal Information Processing Standards Publication 140-2) is a U.S. Government standard entitled "*Security Requirements for Cryptographic Modules*." This standard mandates a set of strict design and documentation requirements that hardware and software cryptographic module must meet in order to be validated by the U.S. National Institute of Standards and Technology (NIST) and the Canadian Communications Security Establishment (CSE).

This document is intended for use by FIPS 140-2 testers, NIST and CSE reviewers, and others interested in how the HA2000 meets all FIPS 140-2 Level 2 requirements.

1.2 References

This FIPS 140-2 Security Policy describes features and designs of the HA2000 using the technical terms of FIPS 140-2.

- For more information on the FIPS 140-2 standard and validation program readers are referred to the NIST web site at http://csrc.nist.gov/cryptval/.

- For more information on the HA2000 product, please visit the SafeNet web site at http://www.safenet-inc.com.

1.3 Terminology

In this document the SafeNet HA2000 is referred to as the module, the HA2000 device, the device, and the HA2000.

1.4 Document Organization

The Security Policy document is part of the complete FIPS 140-2 Submission Package.

This document provides an overview of the HA2000 and explains the secure configuration and operation of the module.

1.5 Version History

Version	Date	Comments	Name
0.01	8/25/2003	Added History revision	Adam Bell
0.02	8/27/03	Removed document listing	Adam Bell
0.03	8/29/03	Update from feedback	Adam Bell
0.04	9/3/03	Moved DES-MAC into non-FIPS compliant list algorithm list	Adam Bell
0.05	9/3/03	Update from feedback	Adam Bell
1.00	9/5/05	Release first rev. of document	Adam Bell
1.01	9/8/03	Final update/review	Adam Bell

1.6 Acronyms and Abbreviations

Acronym/ Abbreviation	Definition
CA	Certificate Authority
CC	Configuration Certificate
CLI	Command Line Interface
CSP	Critical Security Parameter
DSA	Digital Signature Algorithm
FIPS 140-2	Security Requirements for Cryptographic Modules
FIPS 46-3	Data Encryption Standard (DES)
FIPS 81	DES Modes of Operation
FIPS186	Digital Signature Standard (DSS)
HMAC	Keyed-Hash Message Authentication Code
IKE	Internet Key Exchange
IPSec	Internet Protocol Security
KAT	Known Answer Test
MC	Manufacturing Certificate
MD5	Message Digest version 5
MIB	Management Information Base
NC	Network Certificate
NIC	Network Interface Card
NVRAM	Non-Volatile Random Access Memory
PKCS	Public Key Cryptography System
ROM	Read Only Memory
RSA Algorithm	Rivest, Shamir, Adelman Algorithm
SA	Security Association
SHA-1	Secure Hash Algorithm
SNMPv2	Simple Network Management Protocol version 2
SMC	Security Management Center
SRDI	Security Related Data Item
TFTP	Trivial File Transfer Protocol
VPN	Virtual Private Network
VPNG	Virtual Private Network Gateway

2 High Assurance HA2000 Gateway

The SafeNet HA2000 is a high-performance, standards-based hardware Virtual Private Network (VPN) and firewall. Providing a high speed, low cost solution, it features strong security and complete manageability. SafeNet custom designed a state-of-the-art Application Specific Integrated Circuits (ASIC) for the HA2000 that allow high speed encryption with Data Encryption Standard (DES) *and* triple-DES. DES is included for legacy systems.

The HA2000 supports the internationally standardized Internet Protocol Security (IPSec) protocol and Internet Key Exchange (IKE) protocol. Whether securing an enterprise perimeter, a corporate sub-network, or a single host, the HA2000 controls network access and gives administrators a complete toolbox of functionality. The HA2000 includes the following features:

- IPSec support including IKE (using all modes – main, aggressive, and quick)
- X.509 v3 Digital Certificates, Public Key Infrastructure Certificate Management Protocol (PKIX CMP), and pre-shared keys
- Strong cryptography using Triple-DES, SHA-1, and Digital Signature Algorithm (DSA).
- Tamper-resistant/evident case
- Tamper response
- Encryption to enforce policy and provide data privacy
- Centralized, remote management using SNMPv2 and TFTP.
- Secure software upgrades
- Secure rule updates

The HA2000 acts as a perimeter guard. The module allows you to create enterprise-wide Virtual Private Networks and to securely link distributed networks by adding a single device in front of the network.

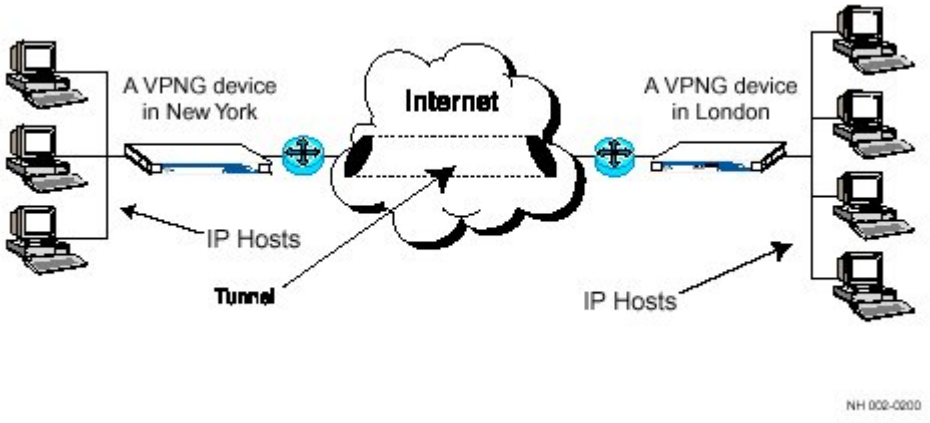

Figure 1 – HA2000 Securely Links Remote Networks

2.1 Secure Remote Management Software

The SafeNet Security Management Console (SMC) is powerful remote management software that can be installed on Windows 2000, Windows XP, or Solaris 8.00 workstation. This software provides a simple, easy-to-use graphical interface to the configurations of the HA2000. It also allows for extensive monitoring of the HA2000, allowing an administrator to remotely keep track of the module's status. All communications between SMC and the HA2000 are through network ports over secure, authenticated IPSec tunnels. The SNMPv2 protocol and TFTP protocol are used to carry out the management services.

3 Security Levels

The HA2000 has been validated as meeting all FIPS 140-2 requirements at level 2 or higher security. Individual security requirements meet the levels indicated in the following table.

Security Requirements Section	**Level**
Cryptographic Module	2
Cryptographic Module Ports and Interfaces	2
Roles, Services, and Authentication	2
Finite State Model	2
Physical Security	2
Operational Environment	n/a
Cryptographic Key Management	2
EMI/EMC	3
Self Tests	2
Design Assurance	2
Mitigation of other attacks	n/a

Table 1. Individual security requirement for HA2000

4 Cryptographic Module Specification

In FIPS terms, the HA2000 is a multi-chip standalone module. The HA2000 features strong physical security with tamper response, its tamper-evident case, extruded sheet metal construction, and a SafeNet iridescent sticker. The entire module is encapsulated by the steel case that forms the cryptographic boundary, and only specified physical interfaces provide access to the module.

The HA2000 Gateway consists of the following parts:

- Hardware Assembly 16406-010-07.
- Hardware Version SE-HA2000.
- System firmware includes the operating system and boot code installed in ROM (flash memory) as part of the manufacturing process. Firmware consists of:
  - Boot Code Version 3.00
  - Wind River pSOS Version 2.17
  - System runtime firmware version 6.21

A crypto officer, an administrator configuring or using the cryptographic module, can examine the product label to confirm the hardware assembly version number. The Boot Code information can be obtained by accessing the menu system which is available to crypto officers.

Figure 2 shows a hardware block diagram of the cryptographic module and indicates the cryptographic boundary.

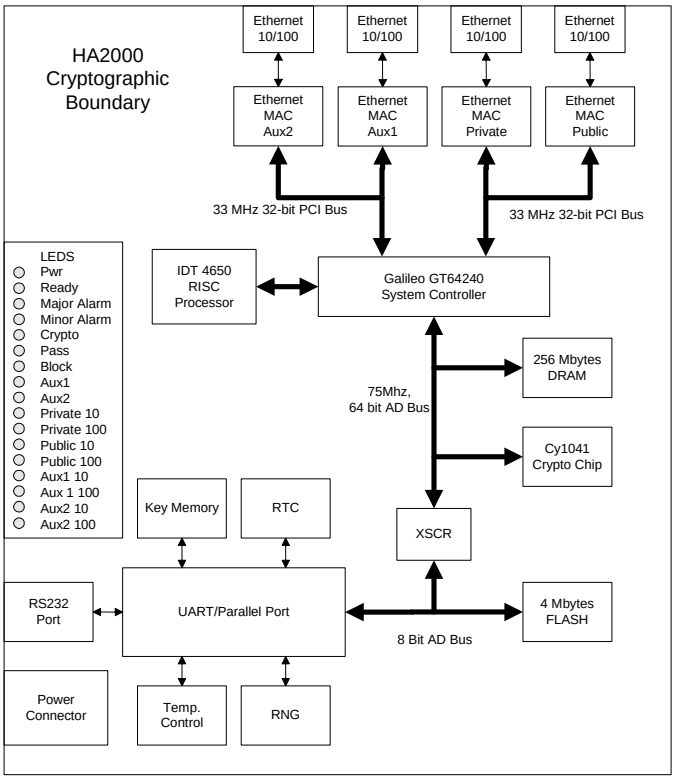

Figure 2. Hardware Block Diagram

4.1 Physical Security Policy

The HA2000 has tamper-evident security tape on the two screws securing the chassis housing that must be removed to access any internal cryptographic module components. A microswitch attached to the chassis senses any attempt to open the module. While the HA2000 is turned on, if an attempt to remove the module cover is detected the system responds to tamper by rebooting, zeroizing any keys or Critical Security Parameters (CSPs) RAM and in flash memory and disabling data traffic. While powered off, if the chassis cover is even partially removed, the module will detect the tamper upon the next boot cycle and will not support any cryptographic processes. Tamper evidence for the HA2000 includes dents and scratches in the metallic case, damage to the security tape, and severe deformation of any panels.

Physical Security Mechanism	Frequency of Inspection/Test	Inspection/Test Guidance Details
Tamper Evidence	Not required to maintain physical security.	1. Determine if the tamper evident seal has been broken or if they have been removed and reapplied
		2. Look for dents and scratches in the metallic case
		3. Determine if there are severely deformed panels on the device.

Table 2. Physical security mechanisms

Figure 3 – The steel-cased HA2000 features tamper response circuitry

4.2 Operational Environment

The cryptographic module has a limited, modifiable operational environment consisting of the pSOS operating system distributed by Wind River Systems. The physical embodiment is a multichip standalone module.

4.3 Module Interfaces

Table 3 shows the mapping of the FIPS140-2 logical interfaces to the module's physical interfaces.

FIPS 140-2 Logical Interfaces	Adapter physical interfaces
Data Input Interface	Private/Public Ethernet ports
Data Output Interface	Private/Public Ethernet ports
Control Input Interface	Private/Public Ethernet ports, Serial port, AC power connector
Status Output Interface	Private/Public Ethernet ports, Serial port, LEDs
Power Interface	AC Power connector

Table 3. Module interfaces mappings to physical interfaces

The HA2000 has status indicators on the front panel and rear panel that allow quick and easy assessment of the working condition of the module. These indicators show severity of errors, operational condition of the module, link state of the Ethernet ports, and if the power is connected. Policy LEDs show when user traffic is passing in the clear, is being blocked, or is being encrypted and decrypted. Figure 4 and 5 depict the front/rear panel of the module. There is also a standard serial port for local configuration.

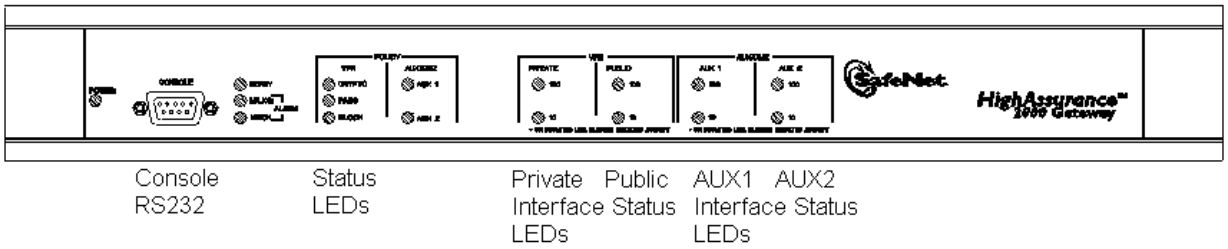

Figure 4 – Indicators show the status of the device

The HA2000 provides 10/100BaseT Ethernet Ports that allow it to connect directly into an existing network.

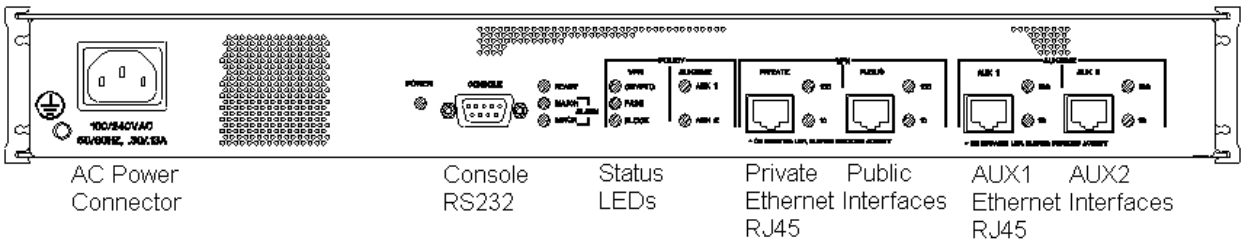

Figure 5 – Standard interfaces connect directly to the network

As shown in Figure 5, the private and public 10/100baseT Ethernet ports are on the rear panel of the HA2000. The Ethernet ports are not crossed over internally and behave like a NIC. The Aux1 and Aux2 ports are non-functional as they are disabled in firmware. These are provided for future expandability. There is also a standard serial port for local configuration. Some local management and monitoring services are available through the Serial port. However, using the secure SMC management station, an administrator can conveniently and remotely access and modify all configurations of the HA2000 through the Ethernet ports. Secured IPSec connections

allow administrators to securely monitor and administer the HA2000 from almost anywhere. The device can be mounted with the Ethernet ports in the back or in the front using the reversible mounting ears provided.

4.4 Supply Voltage and Current

The HA2000 uses an auto-sensing internal power supply. The allowed power values are as follows:

100/240 VAC
0.30/0.13 A
50/60 Hz

4.5 EMI/EMC

The module meets FCC requirements in 47 CFR Part 15 for personal computers and peripherals designated for home use (Class B). The module is labeled in accordance with FCC requirements.

4.6 Roles and Services

The HA2000 employs role-based authentication to provide access to cryptographic module services.

4.6.1 Roles

The HA2000 supports four roles: Local crypto-officer, remote crypto-officer, local user and remote user.

The local crypto-officer is authenticated with a password and is responsible for limited configuration of the module. The password is 8 characters long and meets the strength of authentication requirements. This is shown in a later section of this document. The local crypto-officer interfaces with the HA2000 using the ROM menu and the runtime menu through the serial port. This role has access to all local services provided by the module. This menu is activated only during power up. There is also a runtime menu available for device monitoring and network parameter configuration.

The remote crypto-officer is responsible for the initial configuration and activation of the HA2000. Authentication is performed in the IKE protocol through DSA/RSA signatures. The remote crypto-officer interfaces with the HA2000 using the SMC over an IPSec secured Ethernet port. This role has access to all remote services provided by the module and is able to modify all sensitive settings.

The local user is authenticated with a username and a password and is able to view status information and change certain non-critical settings. The username is a minimum of 4 characters and the password is a minimum of 6 characters long. This combination meets the strength of authentication requirements. This is shown in a later section of this document. The local user interfaces with the module through the serial port in order to change certain configuration parameters, view logs, and view the status of the module. The user can also look at the status indicators located on the front and back of HA2000.

The remote user is able to invoke module services during the establishment of an IPSec tunnel. Authentication is performed in the IKE protocol through DSA/RSA signatures or by way of a pre-shared key. Any one device initiating a valid IKE session is considered a legitimate user of the cryptographic module.

A remote operator using the SMC software initially authenticates to the module using DSA within the IKE protocol. The communication between remote operators and the module is secured: packets are encrypted, protected for data integrity, and both sides are authenticated. Authentication is performed as part of the IPSec SA negotiation, and all module configurations are performed securely (encrypted and authenticated). The device supports DSA and RSA authentication methods.

A local crypto officer using the ROM menu must input a password to access certain sensitive settings. This password is set when changing the ROM menu from an unlocked to locked mode. Only 6 attempts are allowed before all users are locked out of this menu. To recover the ROM menu password, the remote crypto officer must clear the password.

A local crypto officer attempting to access the runtime menu must input a username and password. There is no limit to the number of attempts. However, after 3 failed attempts, a notification in the form of a trap is sent to the SMC station.

4.6.2 Services

The HA2000 uses role-based authentication to distinguish between the services offered to crypto officers and users.

4.6.2.1 Remote crypto-officer services

- Read/write access to all of the module's remote services
- Remotely configure and monitor the module through the Ethernet ports using SMC. Using the SMC, the remote crypto-officer is able to access all configuration settings of the module, including:
    - Creating/modifying security policies
    - Creating/modifying security types
    - Creating/modifying protocol profiles
    - Creating/modifying network objects
    - Creating/modifying VPNs and maintaining them
    - Performing key management for multicast
    - Resetting the module
    - Certifying the module
    - Activating the module's cryptographic services
    - Configuring the module
    - Upgrading the firmware
    - Create user and set privileges.
- RSA or DSS key generation
- RSA or DSS signature generation
- Diffie Hellman key agreement

- DES and TDES encryption and decryption

The above cryptographic services are provided as part of IPSec and IKE protocols.

4.6.2.2 Local crypto-officer services

- Read/write access to all of the module's local services including the local user services
- The ROM menu requires login using a password. The runtime menu requires username and password.
- Full read capability and limited write capability
- Configure and monitor the module through the serial port using the ROM menu. Using the ROM menu, the Local Crypto-Officer is able to:
    - Upgrade the firmware
    - Re-initialize the module's firmware
    - Clear the tamper condition
    - Lock/unlock the ROM menu
    - Set the time
    - View limited logs
    - Run diagnostics

4.6.2.3 Local User service

- Read access to a variety of status information.
- The user is able to access non-critical configuration and monitoring settings of the module, including:
    - Viewing detailed status and log information
    - Setting the time and date
    - LED Status – the front and rear panel LEDs provide the following status indications:

LED	Status indication
Power	Illuminated when power is applied.
Ready	Illuminated when crypto services are available, blinks during boot cycle.
Major Alarm	Illuminated for link down, tamper, over temperature, and active boot code.
Minor Alarm	Illuminated when system alarms of level warning or error are in the system log.
Crypto	Illuminated for 250usec when a packet is encrypted or decrypted.
Pass	Illuminated for 250usec when a packet is passed in the clear per defined rules. Indicates bypass capability is executed.
Block	Illuminated for 250usec when a packet is blocked.
Aux1	The Aux1 interface is disabled by firmware and is non-functional. No packets are received or transmitted on this interface.
Aux2	The Aux2 interface is disabled by firmware and is non-functional. No packets are received or transmitted on this interface.
Link 10	Illuminated when link speed is 10 Mbps. Blinking indicates activity on the interface.

Link 100	Illuminated when link speed is 100 Mbps. Blinking indicates activity on the interface.

- Monitor the module through the serial port using the ROM menu. Using the ROM menu the local user is able to:
  - Start the module
  - Modify VLAN parameters
  - Modify link speed parameters
  - Initialize network parameters prior to certification from SMC

4.6.2.4 Remote User service

- **DH Key Agreement** – This cryptographic module service is used whenever a user initiates an IKE session with the module.
- **Symmetric key (TDES) Generation** – This cryptographic module service is used whenever a user initiates an IKE session with the module. An IKE policy module shared between the cryptographic module and the user dictates which key (DES, TDES) to generate within the Diffie-Hellman key agreement protocol.
- **Encryption and Decryption services using TDES** – This cryptographic module service is used whenever a user communicates via the cryptographic module. An IKE policy module shared between the cryptographic module and the user dictates which encryption algorithm is used.

4.7 Cryptographic Algorithms, Security Functions, and Key Management

Always adhering to the cryptographic standards, HA2000 provides strong cryptography. HA2000 supports IPSec/ESP data encryption, IPSec/ESP data integrity (with the prescribed NULL encryption algorithm), and IPSec/AH for data integrity in Tunnel mode. The "NULL encryption algorithm" is a service in the IPsec Protocol. In ESP, it is acceptable to specify NULL as the encryption algorithm of choice, however this is not allowed in FIPS mode HA2000 implements all IKE modes: main, aggressive, and quick, using IKE/ISAKMP. The HA2000 supports these features with the following algorithms:

Data Encryption

- DES-CBC (56 bits) NIST FIPS PUB 46-3
- Triple DES-CBC (168 bits) NIST FIPS PUB 46-3

Data Packet Integrity

- DES-MAC (64 bits) NIST FIPS PUB 113
- HMAC-MD5 (16 bytes) RFC 2104 (HMAC: Keyed-Hashing for Message Auth).
- HMAC-SHA1 (20 byte) NIST FIPS PUB 198.

Random Number Generation

- Non FIPS approved non-deterministic random number generator (NDRNG) implemented in hardware.

Authentication

- IKE modes Main, aggressive, and quick

- DSA NIST FIPS PUB 186-2
- RSA Vendor affirmed to PKCS#1
- Pre-shared key

The HA2000 implements and uses the following cryptographic keys and CSPs when in FIPS mode. The keys and CSP are generated, stored, used and destroyed in accordance with FIPS 140-2. CSPs are zeroized with a stream of zeros.

Manufacturing private/public key pair	This is a persistent DSA key set that is generated by the cryptographic module during manufacturing certification. The public key is exported to a manufacturing DSA CA; the certificate is imported and stored in the clear text form in flash. The private key is stored in clear text form in flash. This is used to authenticate the first remote crypto-officer management session.
Network private/private key pair	This is a persistent RSA or DSA key set that is generated by the cryptographic module during network certification. The public key is exported to a CA; the certificate is imported and stored in clear text form in flash. The private key is stored in clear text form in flash. This is used to authenticate remote crypto-officer management sessions. The keys and corresponding certificate are erased during tamper response.
IKE Pre-shared keys	The IKE pre-shared keys are stored in a configuration file in clear text form in flash. This is used to authenticate a remote user during IKE. The specific authentication method (pre-shared keys or certificates) to be used by IKE is defined by the remote crypto officer. The pre-shared keys are erased during tamper response.
Diffie-Hellman Public/Private key pairs	Public/private Diffie Hellman key pairs are generated dynamically per security association negotiation and stored in RAM. These are used during the IKE (Internet Key Exchange) phase to establish a shared secret key. When the DH key agreement completes, the DH private key is erased from RAM.
TDES (DES) session keys	These keys are derived from the DH key agreement, stored in RAM, and used for session encryption of payload traffic between endpoints. Each security association has a unique TDES key to maintain confidentiality of the payload traffic from other users in the system. The TDES keys are stored in RAM. When the session completes or on rekey (sessions can be set for automatic re-key after a given time limit, a specific amount of data has been transferred, authenticated request from remote user, or request from the remote crypto officer), the TDES keys are no longer useful and are erased from RAM.
Authentication (MAC) keys	The authentication key is stored in RAM. When the session completes or on rekey (sessions can be set for automatic re-key after a given time limit, a specific amount of data has been transferred, authenticated request from remote user, or request from the remote crypto officer), the authentication keys are no longer useful and are

	erased from RAM. The specific key is decided during IKE and can be used for DES-MAC, HMAC SHA-1, and HMAC MD5.
1 ROM menu password	This is an 8 byte (A-Z, a-z, 0-9) password set by the local crypto or remote crypto officer for local crypto officer access to the ROM menu. The password is stored in clear text form in flash. The password is erased during tamper response.
1 Runtime menu username/ password	This is a 4 byte minimum (A-Z, a-z, 0-9) username and a 6 byte minimum (A-Z, a-z, 0-9) password set by the remote crypto officer for local crypto officer access to the runtime menu. The password is stored in clear text form in flash. The username/password is erased upon tamper detection and is reset to a default value.

Table 4. Cryptographic keys and CSP descriptions

4.7.1 Other Security Functions

Each HA2000 ships with a Manufacturer Certificate (MC) and private key that gives the device a unique ID. The MC is signed using a DSA signature. The SMC uses the MC to initially authenticate the module. Before a HA2000 can be used, it must be certified. The SMC certifies the device by requesting the HA2000 to generate a new public/private key pair and to issue a PKCS#10 request for a new certificate; The Network Certificate (NC). The NC is used to authenticate sessions between the other modules and the SMC. The NC can be signed using DSA or RSA signature. Therefore, the possible authentication interactions are:

1. HA2000 to HA2000
2. SMC to HA2000
3. Generic gateways to HA2000
4. Software client to HA2000

When the first secure connection is established between two devices, the NC exchange and SA exchange use the IKE protocol. The Network Certificate (NC) is used to authenticate secure connections and a session key is used to encrypt the packets. New session keys are negotiated for new connections or when a connection/session key is timed out. Each session uses a different session key. Session keys are negotiated at the beginning of an SA lifetime, and can be set to automatically rekey after a given time limit, a specific amount of data has been transferred, authenticated request from Peer Gateway, or station manager request.

4.8 Self-Tests

The HA2000 monitors firmware operations through a set of self-tests to ensure proper operation in accordance with FIPS 140-2. The module includes the following self-tests described below.

4.8.1 Power-Up Self-Test

The power-up self-test includes the following tests:

Hardware Tests: When power is first applied to the module, the hardware performs a series of checks to ensure it is functioning properly.

Firmware Integrity Test: After the hardware tests, the module performs DSA signature verification to ensure firmware has not been modified. The public key in the manufacturing certificate is used for this verification.

Cryptographic Algorithm KATs: Known Answer Tests (KATs) are run at power-up for the DES and Triple DES encryption/decryption, and Message Authentication Codes.

DES-CBC KAT
Triple-DES-CBC KAT
DES-MAC KAT
HMAC-SHA-1 KAT
DSA KAT
RSA KAT

4.8.2 Conditional Tests

DSA Pair-wise Consistency Test: All DSA operations are tested to ensure the correct operation of the DSA key generation and signatures.

RSA Pair-wise Consistency Test: All RSA operations are tested to ensure the correct operation of the RSA key generation and signatures.

Continuous Random Number Generator Test: This test is constantly run to detect failure of the random number generator in the HA2000.

Management Configuration Files Integrity Test: The module performs SHA-1 check value verification to ensure the configuration files have not been modified.

Firmware Upgrade Test: Module firmware can be remotely upgraded from the management system with proper authentication to the module. However, in order to strictly control the loading of new firmware to the HA2000, the new firmware must be digitally signed by SafeNet using a DSA signature. The public key in the manufacturing certificate is used for this verification.

5 FIPS 140-2 Level 2 Compliant Mode

The HA2000 has the capability of operating in a FIPS 140-2 compliant manner and a non-FIPS 140-2 compliant manner. Therefore, it is necessary to ensure the module's proper configuration for running in a FIPS 140-2 compliant manner.

When operating in a FIPS 140-2 compliant manner, the CLI must be password protected. Therefore a password must be defined. Before the device is certified, the remote crypto officer must authenticate the module using DSA signatures. All remote crypto-officer services must be accessed through secure, authenticated channels. Only the following FIPS-approved cryptographic algorithms may be used:

Data Encryption

- DES-CBC (56 bits) – Certificate #104 (legacy systems only)
- Triple DES-CBC (168 bits) – Certificate #36

Data Packet Integrity

- HMAC-SHA1 (20 byte) – DSA/SHA-1 Cert. #5

Authentication

- DSA – DSA/SHA-1 Cert. #5
- RSA – vendor affirmed to PKCS#1
- Pre-shared Key -- Uses TDES pre-shared key

All traffic employing encryption and/or authentication must be encrypted using DES or Triple-DES and/or authenticated using DSA or RSA signatures or using a pre-shared key.

Message Authentication Codes (MACs) must be generated using HMAC-SHA1. HMAC-MD5 and DES-MAC cannot be used.

The SafeNet tamper-evident stickers should be affixed to the HA2000 under normal operating temperatures, and the surface for application of the stickers should be clean and dry. One tamper-evident sticker is placed along the back edge of the module and wraps around such that the sticker is attached to the cover and the base. The adhesive sets immediately upon application.

Note: RSA is implemented as a "FIPS approved" algorithm that is vendor affirmed as it conforms to PKCS#1.

6 FIPS 140-2 Level 2 Non-Compliant Mode

The remote crypto officer will continue to use FIPS approved algorithms to initially authenticate the module. The remote crypto officer must decide to place the device into a non-FIPS140-2 compliant mode by defining policy in the module that uses the non-compliant algorithms listed below. All remote crypto-officer services are accessed through secure, authenticated channels. The following are all cryptographic algorithms and features available in FIPS non-compliant mode:

Data Packet Integrity

- HMAC-MD5 (20 byte) – per RFC 2104
- DES-MAC (64 bits)

Features

- Secure Multicasting
- Bypass Service during installation (no encryption)

7 SECURITY RULES

7.1 Identification & Authentication Security Rules

The module implements specific methods for identifying and authenticating the different roles. The implementation consists of the binding of a Role-Based Access Control Rule to each service.

7.1.1 Cryptographic Officer Identification and Authentication

For the ROM menu, a local crypto officer must prove possession of the crypto officer password. A valid password causes the module to allow local crypto-officer access to services. There can be only 6 attempts to guess at the password before the local-crypto officer is denied access permanently. The remote crypto-officer can clear the password.

For the runtime menu, a local crypto officer must prove possession of the crypto officer username and password. A valid username and password causes the module to allow local crypto-officer access to services. There is no limit to the number of attempts to guess at the username and password. However, after three failed attempts, a trap is sent to the configured IP addresses that notify the remote-crypto officer of the failed attempts.

A remote crypto officer using SMC through the private or public Ethernet interface must authenticate using DSA or RSA public key authentication. This allows the remote crypto officer access to services.

For the ROM menu, a user has access to minimal services without authentication. A user does not have access to the runtime menu. A user must authenticate when requesting cryptographic services such as setting up a VPN tunnel.

The following table summarizes roles and required authentication.

Role	Type of Authentication	Authentication Data
Remote crypto-officer	Certificate and password	Signature based on 1024 bit key
Local crypto-officer (runtime menu)	Username and password	String of length 4 + String of length 6 Values of a..z, A..Z, 0..9
Local crypto-officer (ROM menu)	password	String of length 8 Values of a..z, A..Z, 0..9
Remote User	Certificate or pre-shared key	Signature based on 1024 bit key
Local User (ROM menu)	password	String of length 8 Values of a..z, A..Z, 0..9

Table 5. Roles and required identification and authentication

7.1.2 Changing Roles

It is not possible to change roles without being authenticated for that specific role. Anytime an operator wishes to change roles, he much log out of the current role and initiate and authenticate in a new role.

7.2 Strength of Authentication

The local crypto officer using a menu must authenticate to the module using a password. The crypto officer using SMC to remotely manage the module must first authenticate using DSA authentication. After issuing a new certificate to the module, the crypto officer must reauthenticate using DSA or RSA authentication. The strength of the each authentication mechanism is explained below.

Authentication Mechanism	Strength of Mechanism	Chance of guessing
ROM Password	$62^8 = 2.18 \times 10^{14}$	3.63×10^{13} (6 attempts max)
Runtime menu username/password	$62^{10} = 8.39 \times 10^{17}$	9.71×10^{12} per 60 seconds
DSA certificate (1024)	2^{1024}	2.99×10^{303}
RSA certificate (1024)	2^{1024}	2.99×10^{303}

Table 6. Strength of each authentication mechanism.

7.2.1 DSA Authentication Strength

Crypto officers and users must first authenticate to the module using a DSA key of 1024 bits. This key space allows 2^{1024} values which require significantly more attempts than one million to guess the correct key.

The IKE process can allow for 1 IKE attempt from a defined peer IP address and Port. At best, an attacker could attempt 10,000 concurrent authentications. The IKE process is no faster than 1 second to complete. The chance of defeating the DSA algorithm in one minute is

$$2^{1024} / 60{,}000 \sim 2.99 \times 10^{303}$$

Therefore the module far exceeds the requirement of 1 in 100,000 for multiple attempts in a 60 second interval.

7.2.2 RSA Authentication Strength

Crypto officers and users can authenticate to the module using a RSA key of 1024 bits. The strength of the 1024 bit RSA authentication is the same as the DSA.

Therefore the module far exceeds the requirement of 1 in 100,000 for multiple attempts in a 60 second interval.

7.2.3 Password Strength

The minimum length of the ROM menu password is 8 bytes. Each byte of the password can be one of the characters a-z, A-Z, 0-9, yielding a 1 in 62^8 = 1 in 2.18 x 10^{14} chance of guessing the password.

The minimum length of the runtime menu username and password is 4+6 bytes. Each byte of the password can be one of the characters a-z, A-Z, 0-9, yielding a 1 in 62^{10} = 1 in 8.39 x 10^{17} chance of guessing the password.

To try an 8-byte password, an attacker must send 8 bytes to the module and get a resulting 2 byte response. There is a single I/O port on the platform and therefore each PIN attempt requires 10 bytes of data to be clocked in or out of the module. The maximum data rate for the module is 115kbps through this single port. If we ignore the processing time required on the module to check the password, we can compute the maximum number of password attempts that could occur within a 60 second interval:

- 10 bytes of I/O * 8bits/byte = 80bits/attempt
- 115,200bits/second * 1 attempt/80bits = 1440 attempt/second
- 60seconds/minute * 1440 attempts/minute = 86400 attempts/minute maximum

The chance of guessing a ROM password is 1/(2.18 x 10^{14}) and you can attempt 86400 times per minute, resulting in 1 in 2,523,148,148 change of achieving the correct password. This exceeds the 1 in 100,000 per minute requirement.

The chance of guessing a runtime menu username and password is 1 in 9,710,648,148,148 chance of the guessing the password in a 60 minute time interval. This exceeds 1 in 100,000 per the requirement.

Feedback of authentication data to an operator is obscured during authentication. Neither the CLI nor the SMC returns a visible display of characters when entering a password.

7.3 Software and Firmware Loading Security Rules

The cryptographic module allows only loading of FIPS validated firmware. The ROM firmware can only be loaded during manufacturing. The runtime firmware can be loaded from the ROM menu or remotely from the SMC. New runtime firmware can also be downloaded from SMC over a secure IPSec tunnel.

The runtime firmware has a DSA signature that ensures integrity and issuer of the firmware. The public key from the manufacturing certificate is used to verify the signature.

7.4 Access Control Security Rules

The remote-crypto officer sends the multicast distribution (non-FIPS mode) and auxiliary keys in encrypted form during policy configuration of the HA2000. The distribution key is a session key used to encrypt messages between gateways. The auxiliary key is used to encrypt the multicast session key before sending it to the multicast receivers. This is only a precautionary step and is not strictly required.

The multicast session keys are created on the multicast sender module and pushed out to the multicast receiver modules.

No other keys are input to the module.

Table 7 describes the type of access operators have with respect to various cryptographic keys and CSPs:

Key or CSP	Local crypto officer	Remote crypto officer	Local User	Remote User
Manufacturing DSA key pair	No access	Execute (once)	No access	No access
Network RSA or DSA key pair	No access	Execute (once)	No access	Execute
IKE Preshared Key	No access	Create, Write	No access	Execute
1 ROM password	No access	Create, Write, Erase	No access	No access
1 runtime menu username/password	No access	Create, Write, Erase	No access	No access
DH key pair	No access	Execute	No access	Execute
TDES (DES) session keys	No access	Execute, Erase	No access	Execute
Authentication (MAC) Keys	No access	Execute, Erase	No access	Execute

Table 7. FIPS Mode Cryptographic Key and CSP Access Control

7.5 Physical Security

The physical security of the cryptographic module meets FIPS 140-2 level 2 requirements. The HA2000 has a tamper-response capability and therefore it meets FIPS 140-2 Level 2 requirements. In addition, the module has security tape for physical protection during transfer and crypto officers are instructed to confirm the module version and the software and firmware version before initializing the module for use. Any attempt to gain physical access to the module will leave evidence of tampering and will also result in tamper response. Crypto officers should examine the module periodically to check for evidence of tampering.

No specific actions are required by users to maintain physical security rules.

7.6 Key Management Security Policy

7.6.1 Cryptographic Key Generation

DH key pair generation is performed as described in PKCS#3.
TDES session key derivation is performed as described in PKCS#3 and FIPS PUB 46-3. (*)

DSS key pair generation is performed as described in FIPS PUB 186-2.
RSA key pair generation is performed as described in FIPS PUB 186-2.

(*) TDES keys used to encrypt and decrypt multicast user data are created locally by the multicast sender module and distributed to the multicast receiver modules.

No intermediate key generation values are output from the cryptographic module upon completion of the key generation process.

7.6.2 Cryptographic Key Entry/Output

The HA2000 supports authentication through an IKE pre-shared key. The remote crypto-officer enters the key into the modules that will authentication using the pre-shared key by way of the SMC. The key is entered in encrypted form through a secure IPsec tunnel.

The HA2000 supports a secure multicast feature. For this feature to work, the SMC must issue a key distribution key and an auxiliary key to the HA2000s that participate in the secure multicast sessions. These keys are always loaded in the encrypted form during policy configuration of the HA2000. The key distribution key is sent to all senders and receivers and is used to establish a shared security association between all endpoints. The auxiliary key is used within the HA2000 at a higher layer than IPSec. Software uses the auxiliary key to encrypt the real TDES session key before sending it over the distribution SA.

Note: The secure multicast feature is not supported in FIPS approved mode.

7.6.3 Cryptographic Key Storage

The RSA and DSA private keys are stored in clear format in flash memory. The flash contents have a SHA-1 hash to ensure data integrity. All other keys are stored in RAM.

The cryptographic module's Roles and Services mechanism correctly associates keys with their correct entity.

7.6.4 Cryptographic Key Destruction

There are several commands from the remote crypto officer that can result in the destruction of cryptographic keys. The commands are

Reset

The remote crypto-officer sends a command for the module to reset. All RAM based CSPs are erased when the module restarts.

Tamper

The remote crypto-officer sends a command for the module to tamper. The resultant behavior is exactly that of a physical tamper.

If the module is opened such that the tamper switch is activated, the module will reset. Once restarted the module will zeroize all of RAM and erase any CSPs stored in ROM, except the manufacturing DSA key pair. All VPN communications are immediately halted. The local

crypto officer must re-initialize the module. The remote crypto officer can then reauthenticate to the module. When the remote crypto officer has reconfigured the module, VPN services are again available.

Clear NVRAM

The remote crypto-officer sends a command for the module to clear NVRAM. The module will erase all device configuration except for the IP addresses parameters, the manufacturing key pair, and public and private keys pair that resulted from the network certification.

The cryptographic module cannot enter FIPS-approved mode until the crypto officer reconfigures the module.

Return to Factory Defaults

The remote crypto-officer sends a command for the module to return to factory defaults. The module will erase all device configuration except for the IP address parameters and the manufacturing public and private key pair.

The cryptographic module cannot enter FIPS-approved mode until the crypto officer reconfigures the module.

7.7 Mitigation of Attacks Security Policy

The HA2000 cryptographic module does not implement a Mitigation of Attacks Security Policy.