SingleSignOn.Net

Secure Identity Appliance

FIPS 140-1 Non-Proprietary Security Policy

Level 2 Validation

March 2002

Table of Contents

1 INTRODUCTION

1.1 Purpose

This is a non-Proprietary FIPS 140-1 Security Policy for the SingleSignOn.Net Secure Identity Appliance. It describes how the SingleSignOn.Net Secure Identity Appliance meets all FIPS 140-1 Level-2 requirements. The Security Policy was prepared as part of the level 2 FIPS 140-1 certification of the SingleSignOn.Net Secure Identity Appliance.

FIPS 140-1 (Federal Information Processing Standards Publication 140-1) 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 certified by the U.S. national institute of Standards and Technology (NIST) and the Canadian Centre de la Sécurité des Télécommunications (CST).

1.2 References

This FIPS 140-1 Security Policy describes features and design of SingleSignOn.Net Secure Identity Appliance components using the technical terms of FIPS 140-1.

- For more information on the FIPS 140-1 standard and validation program readers are referred to the NIST website at http://csrc.nist.gov/cryptval/.

- For more information on the SingleSignOn.Net product line, please visit the SingleSignOn.Net web site at http://www.SingleSignOn.Net.

1.3 Terminology

In this document the SingleSignOn.Net Secure Identity Appliance is referred to as the module, the Secure Identity Appliance, and the SIA.

1.4 Document Organization

The Security Policy document is one document in complete FIPS 140-1 Submission Package. In addition to this document, the complete Submission Package contains:

- Vendor Evidence document
- Finite State Machine
- Other supporting documentation as additional references

This document provides an overview of the Secure Identity Appliance and explains the secure configuration and operation of the module. This introduction section is followed by Section 2, which details the general features and functionality of the Secure Identity Appliance. Section 3 specifically addresses the required configuration for the FIPS-mode of operation. Section 4 provides a list of the acronyms used in this document.

This Security Policy and other Certification Submission Documentation was produced by Corsec Security, Inc. under contract to SingleSignOn.Net. With the exception of this Non-Proprietary

Security Policy, the FIPS 140-1 Certification Submission Documentation is SingleSignOn.Net-proprietary and is releasable only under appropriate non-disclosure agreements. For access to these documents, please contact SingleSignOn.Net.

2 Secure Identity Appliance

The Secure Identity Appliance (SIA) is an off the shelf system that can be easily plugged into an organizations infrastructure in order to provide Public Key Infrastructure (PKI) that is both practical and secure. The SIA is highly scalable and reliable, built from high-end hardware and running a hardened, stripped down operating system optimized for security and performance.

The Secure Identity Appliance is a PKI and password authentication solution. It allows for the easy deployment of PKI within an organization and provides an ID/Password system that uses the underlying PKI to provide security and robustness. It is able to perform public key-based cryptography, including digital signatures and encryption.

The SIA is accessed over a network, using communications secured with Transport Layer Security (TLS). Users are able to authenticate to the module with passwords, and once authenticated, can access public-key-based crypto-functionality. The SIA is capable of issuing digital certificates to users and allows for the easy addition of PKI into an organization.

Administration of the SIA is simple and easy to learn. SingleSignOn.Net provides graphical utilities to remotely manage the module over a secure session. Using role-based access, administrators authenticate to the module with their passwords and perform tasks as permitted. Taking the approach of least privilege, roles are strictly limited to those abilities required by their tasks.

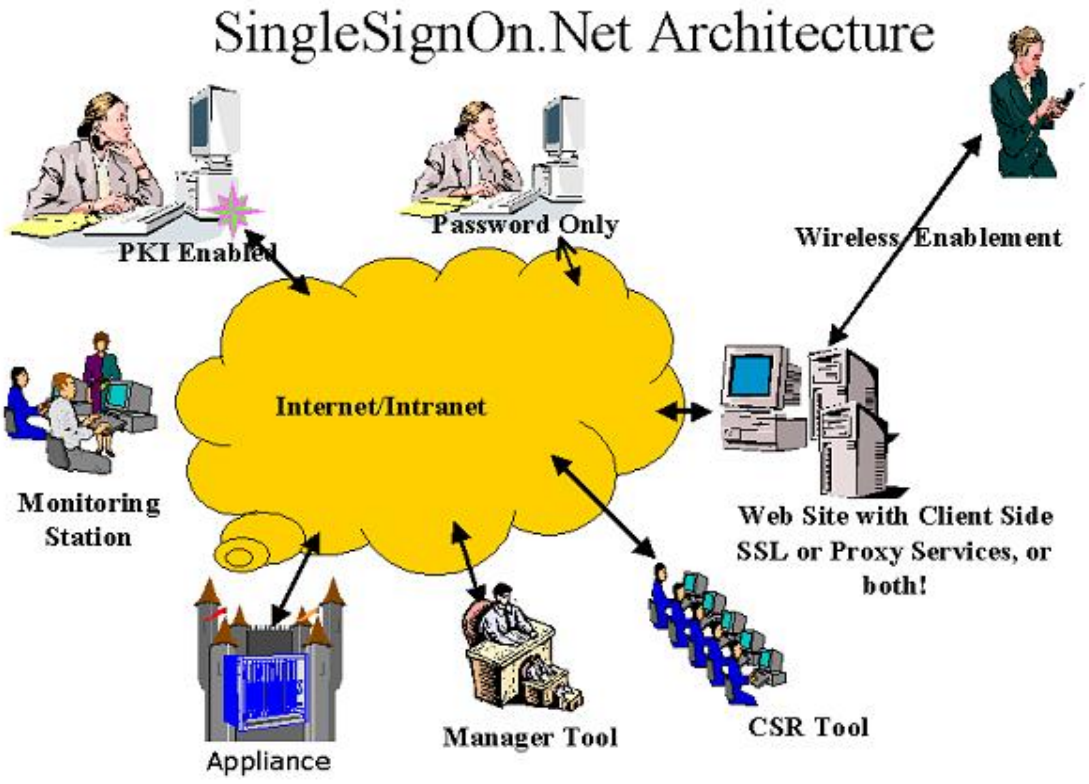

Figure 1 – The Secure Identity Appliance at Work

2.1 Tamper-Evident Hardware with Well-Defined Interfaces

The Secure Identity Appliance is a multi-chip standalone module designed to meet all FIPS 140-1 level 2 requirements. The module is constructed from a high-end rack-mountable computer with tamper-evident labels are affixed to the case in order to provide evidence of any attempts to tamper with the module's hardware (placement of these labels is described in section 3).

The steel case of the Secure Identity Appliance is considered to be the module's cryptographic boundary. Only well-defined interfaces cross the cryptographic boundary, and these interfaces provide the only means of accessing the module. Identity-based authentication is used to ensure only authorized access to the module is granted.

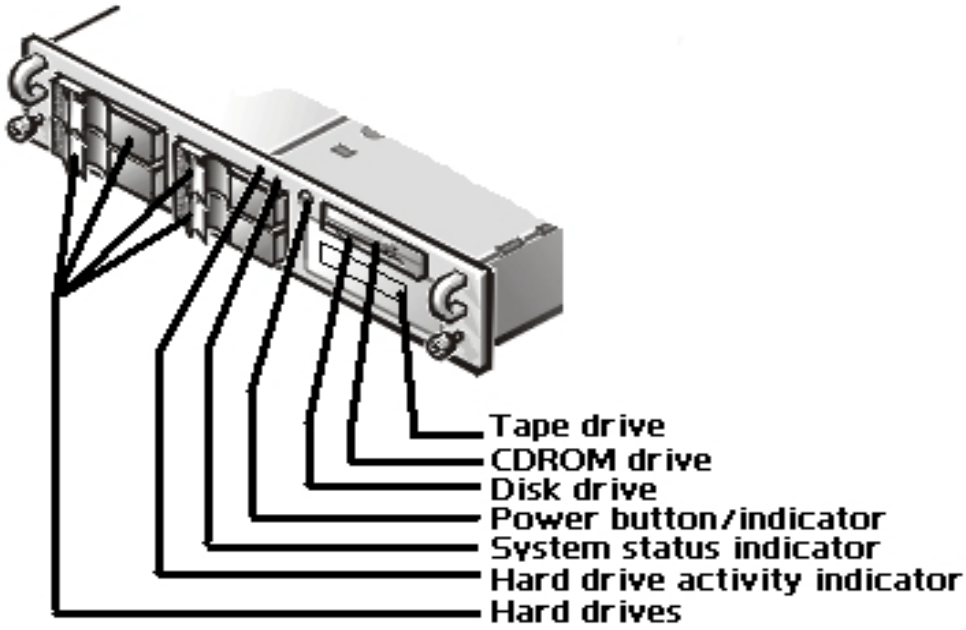

Figure 2 – Front Panel of SIA

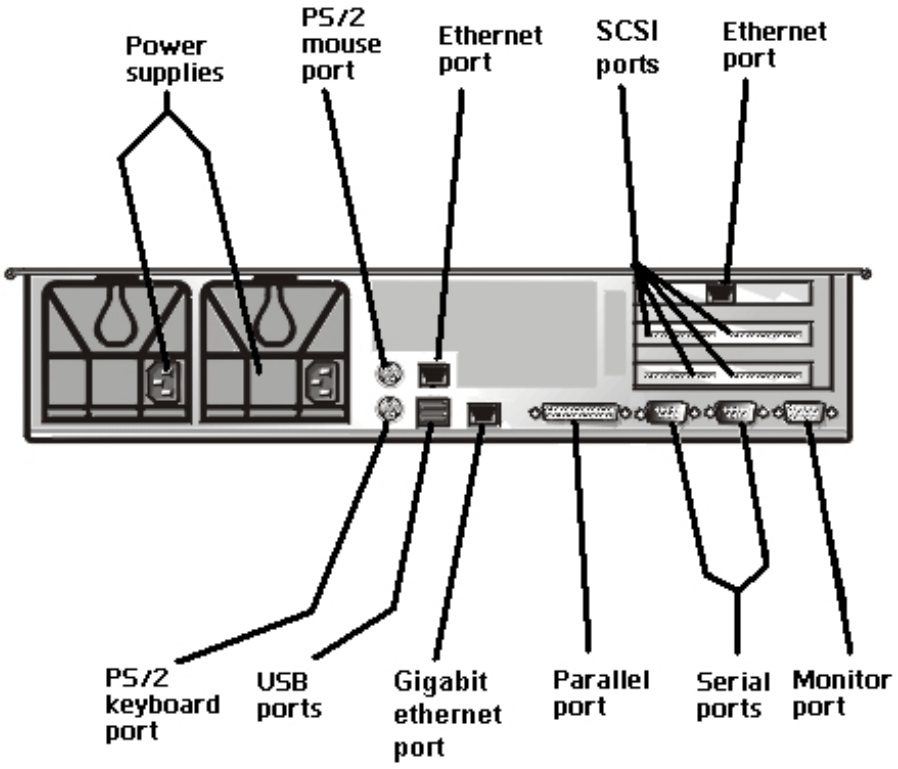

Figure 3 – Rear Panel of SIA

The physical interfaces of the SIA include the power connectors, network ports (Ethernet), power button, indicators (LEDs), and tape drive. All ports use standard PC pin outs with standard protocols. In section 3 of this document, application of tamper-evident labels covering the PS/2 ports, gigabit Ethernet port, SCSI ports, parallel port, serial ports, monitor port, and the disk drive is described and depicted. The remaining physical interfaces map to FIPS 140-1 logical interfaces as follows:

FIPS 140-1 Logical Interface	Physical Interface
Data input interface	Network ports, tape drive
Data output interface	Network ports, tape drive
Control input interface	Network ports
Status output interface	Network ports, indicators, power button
Power interface	Power connectors

Table 1 – Mapping Physical Interfaces to FIPS 140-1 Logical Interfaces

The module's functionality is primarily accessed over its Ethernet ports. Operators log in over the Ethernet ports, accessing the module over an encrypted session. Other than tape backups, all data input/output occurs over the Ethernet ports.

The Secure Identity Appliance's hardware is a Dell PowerEdge 2550 server that has been tested and found to comply with applicable Federal Communication Commission (FCC) Electromagnetic Interference (EMI) and electromagnetic Compatibility (EMC) requirements for home use as defined in Subpart B of FCC part 15.

2.2 Roles and Services

The Secure Identity Appliance uses identity-based authentication to control access to the module. Each role has a password that is used during a challenge-response protocol to authenticate the operator. Once authenticated, an operator implicitly assumes the role to which they are assigned and is able to access the services associated with that role.

The SIA supports two primary roles, User and Crypto-Officer.

2.2.1 Crypto-Officer Role

The Crypto-Officer role is used to configure and maintain the module. By default, this role is divided into six distinct sub-roles, each requiring separate authentication. These six sub-roles are:

1. **Super Manager:** Initialize the module and supervises managerial roles.
2. **System Manager:** Sets system parameters.
3. **Security Manager:** Sets security parameters and Appliance time server.
4. **Super CSR:** Supervises Consumer Service Representative roles.
5. **Create CSR:** Supervises consumer or end-user accounts.
6. **Modify CSR:** Maintains consumer or end-user accounts.

Sections 2.2.1.1 – 2.2.1.6 detail the services available to the Crypto-Officer role, separated according to sub-role. In addition to these services, the Crypto-Office role has the ability to access all services available to the User role.

2.2.1.1 Super Manager

- Create Appliance Keys.
- Modify the Appliance Signed Certificate.
- Change the Record Definition and Field Access.
- Change Role Definitions.
- Define New Roles.

- Change Certificate Profile.
- Set Network Parameters.
- Set Appliance Certificates.
- Create Managerial Accounts.
- Read Managerial Accounts.
- Modify Managerial Accounts.
- Suspend Managerial Accounts.
- Unsuspend Managerial Accounts.
- Revoke Managerial Accounts.
- Reset Managerial Accounts.
- Delete Managerial Accounts.
- Create a certificate for the Super Manager account.
- Zeroize all secret/private keys.

2.2.1.2 System Manager

- Establish Global Parameters.
- Manage Protocol Process Parameters.
- Set Parameters on a ‘Per-Protocol’ basis.
- Perform System Maintenance.
- Perform System Back-up.
- Create a certificate for the System Manager account.

2.2.1.3 Security Manager

- Set the security parameters of the Secure Identity Appliance through a Secure Identity Manager Tool.
- Set the password policy for manager and consumer accounts.
- Control access to the network time protocol server.
- Control access to the external certificate registration authority server (if any).
- Create a certificate for the Security Manager account.

2.2.1.4 Super CSR

- Create CSR accounts (Create-CSR's and Modify-CSR's).
- Modify accounts (Create-CSR's and Modify-CSR's).
- Read accounts (Create-CSR's and Modify-CSR's).
- Suspend accounts (Create-CSR's and Modify-CSR's).
- Unsuspend accounts (Create-CSR's and Modify-CSR's).
- Revoke accounts (Create-CSR's and Modify-CSR's).
- Reset accounts (Create-CSR's and Modify-CSR's).
- Delete accounts (Create-CSR's and Modify-CSR's).
- Create a certificate for the Super CSR account.

2.2.1.5 Create CSR

- Create end-user or customer accounts.
- Modify end-user or customer accounts.
- Read end-user or customer accounts.
- Suspend end-user or customer accounts.
- Unsuspend end-user or customer accounts.
- Revoke end-user or customer accounts.
- Reset end-user or customer accounts.
- Delete end-user or customer accounts.
- Create a certificate for the Create CSR account.

2.2.1.6 Modify CSR

- Modify end-user or customer accounts.
- Read end-user or customer accounts.
- Suspend end-user or customer accounts.
- Unsuspend end-user or customer accounts.
- Revoke end-user or customer accounts.
- Reset end-user or customer accounts.
- Create a certificate for the Modify CSR account.

2.2.2 User Role

The User role accesses the end-user functionality of the module and does not have the ability to use any of the management functionality available to the Crypto-Officer. The services available to the User role include the ability to:

- Perform TLS.
- Get a certificate.
- Activate their new account.
- Activate their account after reset.
- Create a certificate for their account.
- Login.
- Change their user information.
- Change their password or decryption keys.
- Sign documents and verify signatures.
- Decrypt data.
- Log off.
- Revoke their account.
- Status information.

During authentication and the establishment of a connection with the module, session keys are generated to encrypt communications between the module and the client. Depending on the purpose of the session, TLS may also be used to further secure the connection.

2.3 Standards-Based Cryptography

The Secure Identity Appliance implements cryptographic algorithms in compliance with modern cryptographic standards. The module employs many of the strongest, most widely used algorithms today. The following FIPS-approved algorithms are provided by the Secure Identity Appliance:

Data Encryption:

- Triple-DES-CBC (128 and196 bit) – as per NIST PUB FIPS 46-3.

Data Hashing:

- Secure Hash Algorithm (SHA-1) – as per NIST PUB FIPS 180-1.

Digital Signatures:

- RSA (1024 bit) – as per PKCS #1.

Random Number Generation:

- Pseudo Random Number Generator (PRNG) as per Appendix 3.1 of NIST PUB FIPS 186-2.

Besides the above FIPS-approved algorithms, the module supports the following mechanisms that are approved for use in a FIPS mode of operation:

Session Security:

- TLS v1.0 – as per RFC 2246.

Digital Certificates:

- X509 v3 certificates.

Message Authentication Codes:

- Keyed-Hash Message Authentication Code (HMAC) with SHA-1 – as per NIST PUB FIPS 198.

In addition, the module supports the following non-FIPS-approved algorithms:

- MD5.
- RSA for encryption/decryption as per PKCS#1.
- SSL v3 – as per the Transport Layer Security Working Group draft.

2.4 Secure Cryptographic Key Management

The following table summarizes the module's critical security parameters:

Key	Key type	Generation	Storage	Use
Appliance RSA key pair	RSA key pair (1024 bits)	RSA key generation	Stored on disk	Sign Operator RSA public key (in certificate) and during login protocol
TLS RSA key pair	RSA key pair (1024 bits)	RSA key generation (outside of crypto-boundary)	Stored on disk	Public key-based key exchange during TLS handshake
SIA session key	DES/TDES keys (192 bits)	Generated by login protocol (public key-based key agreement)	Stored on disk	Secure SIA session traffic
TLS session key	DES/TDES keys (128 bits)	Generated by TLS handshake (public key-based key agreement)	RAM only	Further secure SIA session traffic
Operator RSA key pair	RSA key pair (1024 bits)	RSA key generation (either by the module or outside of the module's crypto-boundary)	Stored on disk	Generate/verify RSA digital signatures
Backup key	TripleDES (192 bits)	TripleDES key generation	RAM only internally	Encrypt/decrypt backup data
Backup key 2	TripleDES (192 bits)	TripleDES key generation	RAM only internally	Encrypt/decrypt backup key
SSN public key	RSA public key (1024 bits)	RSA key generation (outside of crypto-boundary)	Stored on disk	Verify signatures on software upgrades
(Optional) CA public key	RSA public key (1024 bits)	RSA key generation (outside of crypto-boundary)	If used, stored on disk	Sign the Appliance public key's certificate

(Optional) Mirroring public key	RSA public key (1024 bits)	RSA key generation (outside of crypto-boundary)	If used, stored on disk	Public key-based key exchange during TLS handshake with mirroring modules

Table 2 – Summary of the Module's Critical Security Parameters

The Secure Identity Appliance uses an RSA key pair to sign the certificates containing the public keys of all activated operator's of the module and as part of the login protocol. This key pair is referred to as the appliance key pair.

The module ships with a factory-loaded appliance key pair. This key pair is used during the establishment of the initial management session with the module. In order to initialize the module, a new RSA key pair must be generated to replace the factory-installed key pair. Once initialization is completed, the factory-installed key pair is destroyed and the new appliance key pair is used by the module.

During initialization, the public key of the appliance key pair can be exported to a CA for generation of a certificate. The external CA (not located on the module) generates a certificate for the module's public key. This certificate and the CA's certificate are then loaded onto the module. While not necessary if PKI is not required, these steps are the building blocks of the module's PKI system.

The Secure Identity Appliance is capable of using TLS to secure communications between and client and the appliance. The SIA ships with a default TLS RSA key pair loaded by the manufacturer. As part of the initialization process, the Crypto-Officer can load a new RSA key pair onto the module to be used as the TLS RSA key pair. This new key pair replaces the default key pair and is used during the TLS handshake.

During the login of an operator, the module exchanges random data. This random data is used to derive SIA session keys (with FIPS-approved key generation techniques) to protect the operator's communications with the module. These session keys encrypt/decrypt data as well as provide authentication via TripleDES-MACs. The operator logging out will destroy these session keys.

Along with the SIA session keys, TLS can be used to further secure management and end-user communications with the module. The TLS handshake protocol is used to perform the key exchange, along with a digital certificate for authentication. Ephemeral session keys generated by the TLS protocol are only stored in volatile memory and are destroyed when a session is terminated. Rebooting the module will also destroy all TLS session keys.

The Secure Identity Appliance maintains a key database for all operators of the system. The public key is stored on the module in a certificate signed by the appliance key. The private key is split and part of it is stored on the module. The Crypto-Officer (all six sub-roles) and all operators assuming the User role have RSA key pairs associated with them to be used during authentication and by TLS. Additionally, the RSA key pair associated with an end-user may be

used for digital signatures and encryption/decryption (encryption/decryption is not allowed in the FIPS mode of operation).

The Crypto-Officer has access to functionality that zeroizes all secret and private keys stored on the module. If the Crypto-Officer accesses this functionality, then the module must be returned to manufacturing to be re-initialized.

The module is capable of operating in a pair or triple with other Secure Identity Appliances for redundancy. The two or three modules keep in sync by transferring information, including user accounts and RSA key pairs, between them over a session secured with TLS.

In addition, the module has the ability to perform a system backup. During this process, the key database is backed up to an internal tape drive or to a remote host, TripleDES encrypted for security. The key used to encrypt the database is itself TripleDES encrypted (with another key) and included with the backup.

2.5 Self-Monitoring

The Secure Identity Appliance conducts a series of self-tests to ensure it is functioning properly. Some of the tests are run during startup, while others are executed whenever a particular condition is met. The self-tests include:

- **Hardware Check:** When power is first applied to the module, the hardware performs a series of checks to ensure it is functioning properly.
- **Integrity Test:** The module checks the integrity of the firmware/software at power-up to ensure firmware/software has not been modified.
- **Cryptographic Algorithm KATs:** Known Answer Tests (KATs) are run at power-up for the Triple DES encryption/decryption, RSA digital signature signing/verifying, and SHA-1 hashing.
    - **Triple-DES-CBC KAT**
    - **SHA-1 KAT**
- **Continuous Random Number Generator Test:** This test is run continuously to detect failure of the module's pseudo random number generator.
- **RSA Pairwise Consistency Test:** RSA operations are tested to ensure the correct operation of the RSA key generation and signatures.
- **Firmware Upgrade Test:** All firmware upgrades must be digitally signed by SingleSignOn.Net. Before loading an upgrade, the module will verify the signature on the upgrade to ensure its integrity.

3 FIPS-Compliant Mode of Operation

The Secure Identity Appliance operates in both a FIPS-compliant manner and a non-FIPS-compliant manner. In order to use the module in a FIPS-compliant manner, the following minor steps must be taken.

The SIA uses tamper-evident labels to indicate attempts to physically tamper with the module. These serialized labels are applied to the modules case and must be inspected by the Crypto-Officer to ensure that tampering of the device has not occurred. The following steps detail the application of the sticker:

- Turn off and unplug the SIA before cleaning the chassis and applying labels.
- Clean the chassis of any grease, dirt, or oil before applying the tamper-evident labels. Alcohol-based cleaning pads are recommended for this purpose.
- Apply a label over the lock on the top of the module's case.
- Apply labels as depicted in the figures 4 and 5. If the hard drive locks have no been removed for the bays, then the labels across the hard drives need not be applied (the module ships with these locks in place).
- Record the serial numbers of the labels applied to the system in a security log.

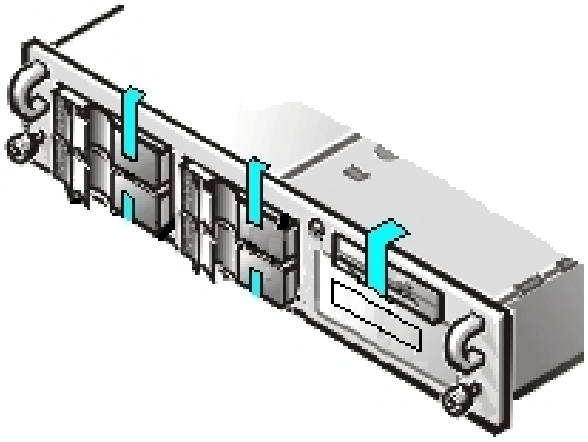

Figure 4 – Tamper-Evident Labels on Front Panel

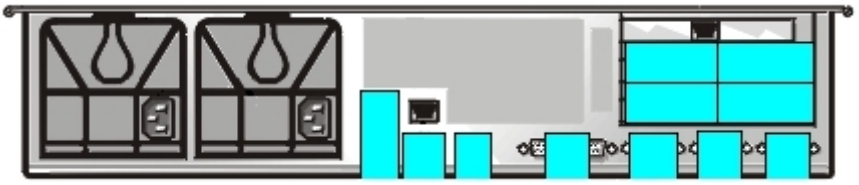

Figure 5 – Tamper-Evident Labels on Rear Panel

The ability to use SSH to access the module must be disabled. This can be accomplished by the following steps:

1. Select *Security Management -> Configuration* and open the **SSH** tab (as depicted in figure 6).
2. Uncheck the **Secure Shell Enabled** checkbox on the **SSH** tab.
3. Click **OK**.

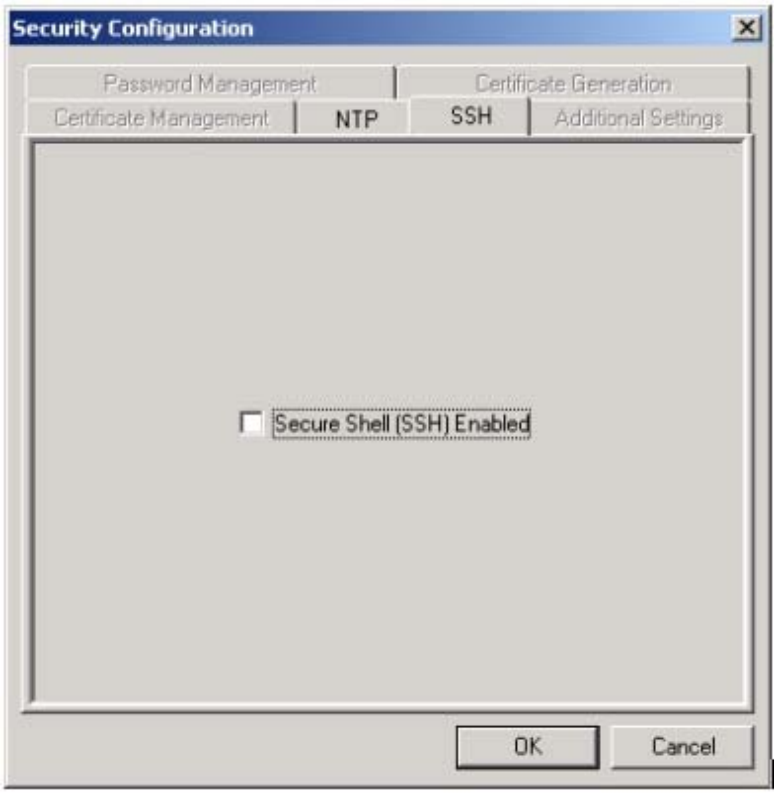

Figure 6 – Disable SSH

Cryptographic services should only use FIPS-approved algorithms. A list of these algorithms can be found in section 2.3.

All operators must be logged off at reboot and only TLS may be used to remotely access the module securely. These options can be configured by the following steps:

1. Select *Security Management -> Configuration* and open the **Additional Settings** tab (as depicted in figure 7).
2. Check the **Logoff all users at reboot** and **Use TLS instead of SSL for all Appliance SSL Communications** checkbox on the **Additional Settings** tab.
3. Click **OK**.

Figure 7 – Select to Use TLS and Logoff Users on Reboot

The login protocol must use TLS to secure its communications. This can be configured as follows:

1. Select *Security Management* → *Parameters* to open the **Security Parameters** dialog (as depicted in Figure 8).
2. Scroll down to "Consumer Login SSL_Enabled."
3. Set **Value** `to 1 in the drop down menu.`
4. Scroll down to "Manager Login SSL_Enabled."
5. Set **Value** `to 1 in the drop down menu.`
6. Click OK.

7. Restart the Appliance processes (*System Management -> Restart/Reboot -> Restart Appliance Processes).*

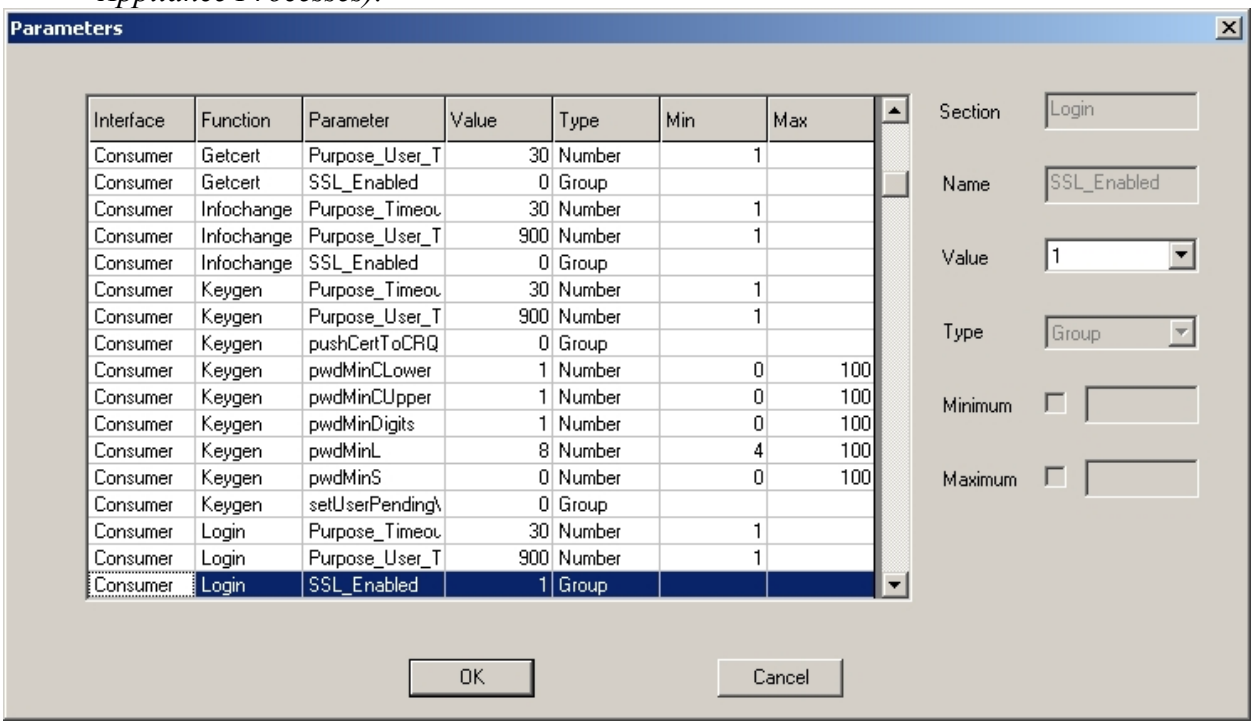

Figure 8 – Use TLS with Login Protocol

4 Acronym List

CBC	Cipher-Block Chaining
CMVP	Cryptographic Module Validation Program
CSE	Communications Security Establishment
CSP	Critical Security Parameters
CO	Crypto Officer
DES	Data Encryption Standard
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
FCC	Federal Communication Commission
FIPS	Federal Information Processing Standard
KAT	Known Answer Test
LED	Light Emitting Diode
MD5	Message Digest Algorithm 5
NIST	National Institute of Standards and Technology
NVLAP	National Voluntary Laboratory Accreditation Program
PKCS	Public Key Cryptography Standards
PKI	Public Key Infrastructure
PRNG	Pseudo Random Number Generator
RNG	Random Number Generator
RSA	Rivest, Shamir, and Adleman
SHA	Secure Hash Algorithm
SIA	Secure Identity Appliance
SSL	Secure Socket Layer
SSN	SingleSignOn.Net
TLS	Transport Layer Security