STS Secure for Linux
Security Policy
Document Version 1.4

Inter-4
A Division of Sierra Nevada Corporation

March 20, 2008
# TABLE OF CONTENTS

1. MODULE OVERVIEW .............................................................................................................3

2. SECURITY LEVEL......................................................................................................................4

3. MODES OF OPERATION.........................................................................................................4

4. PORTS AND INTERFACES ....................................................................................................5

5. IDENTIFICATION AND AUTHENTICATION POLICY .........................................................5

6. ACCESS CONTROL POLICY ..............................................................................................5
   - ROLES AND SERVICES ..................................................................................................5
   - DEFINITION OF CRITICAL SECURITY PARAMETERS (CSPs) ...........................................6
   - DEFINITION OF CSPs MODES OF ACCESS .................................................................6

7. OPERATIONAL ENVIRONMENT .........................................................................................7

8. SECURITY RULES ...............................................................................................................7

9. PHYSICAL SECURITY POLICY ........................................................................................8
   - PHYSICAL SECURITY MECHANISMS ...........................................................................8

10. MITIGATION OF OTHER ATTACKS POLICY .................................................................9

11. REFERENCES .....................................................................................................................9

12. DEFINITIONS AND ACRONYMS ..................................................................................10
1. Module Overview

The Inter-4 STS Secure for Linux (Software Version 1.1) is a multi-chip standalone software module, comprised of the Security Manager Application Service (SMA) and the Netfilter driver, that runs on a general purpose computer. The primary purpose for the STS Secure software module is to provide data security for network wireless and/or wired traffic. The physical boundary is defined as being the outer perimeter of the general purpose computer on which the software module is installed. The logical boundary is defined as being the Security Manager Application service executable file (SMA.exe) and the NetFilter Driver file.

The STS Secure for Linux shall be referred to as the “module” or “STS Secure” throughout this document.

**Figure 1 – Image of the Cryptographic Module**
2. Security Level

The cryptographic module meets the overall requirements applicable to Level 1 security of FIPS 140-2.

<table>
<thead>
<tr>
<th>Security Requirements Section</th>
<th>Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cryptographic Module Specification</td>
<td>1</td>
</tr>
<tr>
<td>Module Ports and Interfaces</td>
<td>1</td>
</tr>
<tr>
<td>Roles, Services and Authentication</td>
<td>1</td>
</tr>
<tr>
<td>Finite State Model</td>
<td>1</td>
</tr>
<tr>
<td>Physical Security</td>
<td>N/A</td>
</tr>
<tr>
<td>Operational Environment</td>
<td>1</td>
</tr>
<tr>
<td>Cryptographic Key Management</td>
<td>1</td>
</tr>
<tr>
<td>EMI/EMC</td>
<td>1</td>
</tr>
<tr>
<td>Self-Tests</td>
<td>1</td>
</tr>
<tr>
<td>Design Assurance</td>
<td>1</td>
</tr>
<tr>
<td>Mitigation of Other Attacks</td>
<td>N/A</td>
</tr>
</tbody>
</table>

3. Modes of Operation

Approved mode of operation

The module only supports a FIPS mode of operation. The following FIPS Approved algorithms are supported:

- DSA with 1024 bit keys for digital signature verification (Cert. #157)
- AES 256 bit encryption/decryption (Cert. #350)
- SHA-1 for hashing (Cert. #425)

The module also implements a non-FIPS Approved NDRNG for the purpose of IV generation.
4. Ports and Interfaces
The physical ports of the module are provided by the general purpose computer on which the module is installed. The module supports the following logical interfaces: data input, data output, control input, and status output interface.

5. Identification and Authentication Policy

Assumption of roles
STS Secure shall support two distinct operator roles: User and Site Security Officer (SSO), who acts as the FIPS 140-2 Cryptographic-Officer. The module does not provide any identification or authentication means of its own. The SSO and the User are procedurally allocated specific services.

Table 2 - Roles and Required Identification and Authentication

<table>
<thead>
<tr>
<th>Role</th>
<th>Type of Authentication</th>
<th>Authentication Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>User</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>SSO</td>
<td>N/A</td>
<td>N/A</td>
</tr>
</tbody>
</table>

Table 3 – Strengths of Authentication Mechanisms

<table>
<thead>
<tr>
<th>Authentication Mechanism</th>
<th>Strength of Mechanism</th>
</tr>
</thead>
<tbody>
<tr>
<td>N/A</td>
<td>N/A</td>
</tr>
</tbody>
</table>

6. Access Control Policy

Roles and Services

Table 4 – Services Authorized for Roles

<table>
<thead>
<tr>
<th>Role</th>
<th>Authorized Services</th>
</tr>
</thead>
<tbody>
<tr>
<td>User:</td>
<td>• Firewall Processing: The module accepts encrypted packets by default, all other plaintext data packages received from unknown IP addresses will be rejected, except for DHCP, ARP, and RARP</td>
</tr>
</tbody>
</table>
packages.

<table>
<thead>
<tr>
<th>Site Security Officer:</th>
<th>Site Security Officer:</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Import AES Encryption Key: Imports the AES Encryption Key into the module for use with data encryption.</td>
<td>Site Security Officer:</td>
</tr>
<tr>
<td>• Zeroize: Actively destroys all CSPs contained within the module. Invoking this service causes the module to transition into a Zeroized state where no traffic is supported.</td>
<td></td>
</tr>
</tbody>
</table>

Other Services:
The cryptographic module supports the following services that do not require an operator to assume an authorized role:

- Show status: This service provides the current status of the cryptographic module.
- Self-tests: This service executes the suite of self-tests required by FIPS 140-2 and is invoked by reloading the library.

**Definition of Critical Security Parameters (CSPs)**
The following is a description of the CSPs contained in the module:

- **AES Encryption Key**: This is an AES key used to encrypt/decrypt network messages.

**Definition of Public Keys:**
The following is a description of the public key contained in the module:

- **STS Secure Software Verification Public Key**: This is the public part of the cryptographic module’s DSA Public/Private key pair used to verify DSA signatures over the SMA and NetFilter Driver software image.

**Definition of CSPs Modes of Access**
Table 5 defines the relationship between access to CSPs and the different module services. The modes of access shown in the table are defined as follows:

- **Load**: This operation imports the AES Encryption Key into the software module.
- **Use**: This operation accesses the AES Encryption Key for network encryption/decryption.
- **Destroy**: This operation actively erases the AES Encryption Key that was used for encryption.

**Table 5 – CSP Access Rights within Roles & Services**
### 7. Operational Environment

STS Secure is a software module that runs on an underlying modifiable operational environment and is installed on a general purpose computer. STS Secure is composed of two components: the Security Manager Application (SMA) and the NetFilter driver. The SMA component runs as a service and interacts with the NetFilter driver to provide data security for network wireless and/or wired traffic.

The Inter-4 STS Secure has been tested on Linux 2.6.

### 8. Security Rules

The STS Secure design corresponds to the 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 1 module.

1. The cryptographic module shall provide two distinct operator roles: User and Site Security Officer.
2. The cryptographic module shall not provide authentication.
3. The cryptographic module shall encrypt wired and/or wireless message traffic using the AES 256 bit algorithm.
4. The cryptographic module shall perform the following tests:
   A. Power up Self-Tests:
      1. Cryptographic Algorithm Tests:
         a. AES Known Answer Test
         b. SHA-1 Known Answer Test
         c. DSA Signature Verification Known Answer Test
2. Software Integrity Test: DSA signature verification
3. Critical Functions Tests: N/A

B. Conditional Self-Tests:
   1. Continuous NDRNG Test

5. Data output shall be inhibited during self-tests, zeroization, and error states.
6. Status information shall not contain CSPs or sensitive data that if misused could lead to a compromise of the module.
7. The module shall not support concurrent operators.
8. All components and applications within the module shall not support maintenance mode, key generation, or manual key entry.
9. The module shall support a single operator mode of operation.

9. Physical Security Policy

Physical Security Mechanisms
The STS Secure module is a software module intended for use with Linux 2.6; therefore, the physical security requirements of FIPS 140-2 are not applicable.

Table 7 – Inspection/Testing of Physical Security Mechanisms

<table>
<thead>
<tr>
<th>Physical Security Mechanisms</th>
<th>Recommended Frequency of Inspection/Test</th>
<th>Inspection/Test Guidance Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
</tbody>
</table>
10. Mitigation of Other Attacks Policy

The module has not been designed to mitigate specific attacks beyond the scope of FIPS 140-2 requirements.

<table>
<thead>
<tr>
<th>Other Attacks</th>
<th>Mitigation Mechanism</th>
<th>Specific Limitations</th>
</tr>
</thead>
<tbody>
<tr>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
</tbody>
</table>

11. References


12. Definitions and Acronyms

AES – Advanced Encryption Standard

CO – Cryptographic Officer

CSP – Critical Security Parameter

DSA – Digital Signature Algorithm

IV – Initialization Vector

NDRNG – Non-Deterministic Random Number Generator

SHA – Secure Hash Algorithm

SSO – Site Security Officer

STS – Secure Tactical Software