STS Secure for Windows CE Security Policy

Document *Version 1.3*

Inter-4
A Division of Sierra Nevada Corporation

March 20, 2008

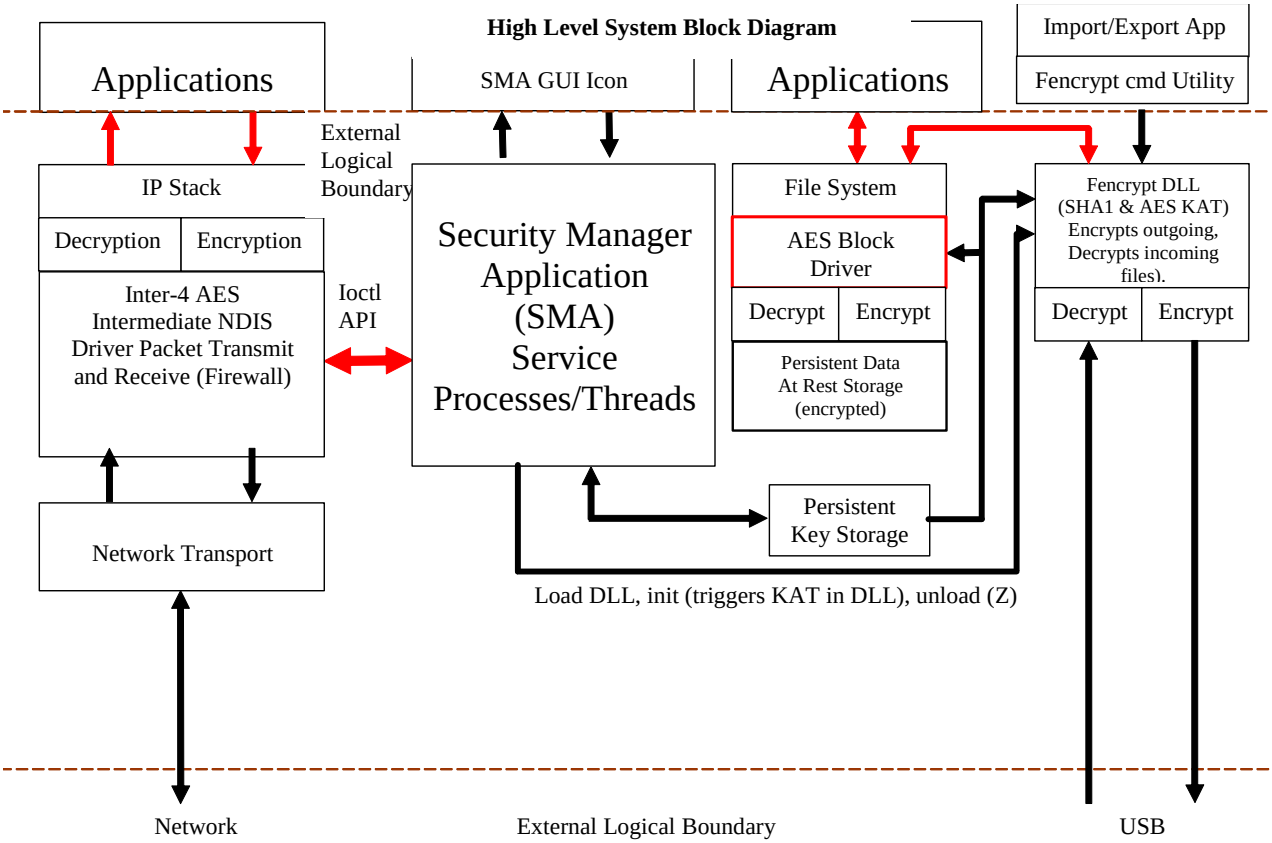
TABLE OF CONTENTS

1. Module Overview

The Inter-4 STS Secure for Windows CE (Software Version 1.1) is a multi-chip standalone software module, comprised of the Security Manager Application Service (SMA), File Encrypt Utility (fencrypt), AES Block Driver, and the AES NDIS Filter 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, as well as data storage. 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), the File Encrypt Utility (fencrypt.dll), the AES Block Driver (extmem.dll) and the AES NDIS Filter Driver (i4aes.dll).

The STS Secure for Windows CE 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 1 - Module Security Level Specification

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

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

Role	Type of Authentication	Authentication Data
User	N/A	N/A
SSO	N/A	N/A

Table 3 – Strengths of Authentication Mechanisms

Authentication Mechanism	Strength of Mechanism
N/A	N/A

6. Access Control Policy

Roles and Services

Table 4 – Services Authorized for Roles

Role	Authorized Services
User:	• 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

	packages. • File Encrypt: Encrypt/decrypt a specified file.
Site Security Officer:	• Import AES Encryption Key: Imports the AES Encryption Key into the module for use with data encryption. • External Software Update: Update the software • 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.

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 traffic, as well as data at-rest.

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 STS Secure 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

Role		Service	Cryptographic Keys and CSPs Access Operation
SSO	**User**		
	X	Firewall Processing	Use AES Encryption Key
	X	File Encrypt	Use AES Encryption Key
X		Import AES Encryption Key	Load AES Encryption Key
X		Zeroize	Destroy AES Encryption Key
X		External Software Update	N/A

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 four components: Security Manager Application (SMA), File Encrypt Utility (fencrypt), AES Block Driver, and the AES NDIS Filter Driver. The SMA component runs as a service and interacts with the AES NDIS Filter Driver to provide data security for network wireless and/or wired traffic. The File Encrypt Utility is a standalone executable that can be used to encrypt/decrypt specified files.

The Inter-4 STS Secure has been tested for use with the Windows CE 4.2 operating system.

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, as well as

data at-rest, 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 Tests
         b. SHA-1 Known Answer Tests
         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
      2. External Software Load Test: DSA Signature Verification

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, manual key entry or key generation.
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 Windows CE; therefore, the physical security requirements of FIPS 140-2 are not applicable.

Table 7 – Inspection/Testing of Physical Security Mechanisms

Physical Security Mechanisms	Recommended Frequency of Inspection/Test	Inspection/Test Guidance Details
N/A	N/A	N/A

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 8 – Mitigation of Other Attacks

Other Attacks	Mitigation Mechanism	Specific Limitations
N/A	N/A	N/A

11. References

[1] *Digital Signature Standard (DSS)*, FIPS Publication 186-2 (+Change Notice), National Institute of Standards and Technology, January 2000.

[2] *Security Requirements for Cryptographic Modules*, FIPS Publication 140-2, National Institute of Standards and Technology, May 2001.

[3] *The Advanced Encryption Standard Algorithm Validation Suite*, FIPS Publication (AESAVS), National Institute of Standards and Technology, November 15, 2002.

[4] *The The Digital Signature Algorithm Validation System*, FIPS Publication (DSAVS), National Institute of Standards and Technology, March 10, 2004.

[5] *The Random Number Generator Validation System*, FIPS Publication (RNGVS), National Institute of Standards and Technology, January 31, 2005.

[6] *The Secure Hash Algorithm Validation System*, FIPS Publication (SHAVS), National Institute of Standards and Technology, March 1, 2004.

[7] *Multiple Examples of DSA*, FIPS Publication (Examples-1024bit), National Institute of Standards and Technology, July 31, 2003.

[8] *Secure Hash Standard*, FIPS Publication 180-2, National Institute of Standards and Technology, August 1, 2002.

[9] *1995 NISPOM*, National Industrial Security Program Operating Manual (DoD 5220.22M), January 1995.

[10] *Digital Signatures Using Reversible Public Key Cryptography for the Financial Services Industry (rDSA)*, X9.31 -1998, American National Standard for Financial Services, 1998.

12. Definitions and Acronyms

AES – Advanced Encryption Standard

CO – Cryptographic Officer

CSP – Critical Security Parameter

DSA – Digital Signature Algorithm

IV – Initialization Vector

NDIS – Network Driver Interface Specification

NDRNG – Non-Deterministic Random Number Generator

RNG - Random Number Generator

SHA – Secure Hash Algorithm

SSO – Site Security Officer

STS – Secure Tactical Software