Entrust® CygnaCom™

PROFESSIONAL SERVICES

ENTRUST CYGNACOM IPSEC CRYPTOGRAPHIC MODULE

Security Policy, Version 3.4

Date: **October 25, 2002**

Table of Contents

1. APPLICABLE DOCUMENTS

[ANSI X9.52] Triple Data Encryption Algorithm Modes of Operation, ANSI,

[FIPS 46-3] Data Encryption Standard (DES), NIST, October 25, 1999.

[FIPS 81] DES Modes of Operation, NIST, December 2, 1980.

[FIPS 113] Computer Data Authentication, NIST, May 30, 1985.

[FIPS 140-1] Security Requirements for Cryptographic Modules, NIST, January 11, 1994.

[FIPS 180-1] Secure Hash Standard (SHS), NIST, April 17, 1995.

[FIPS 186-2] Digital Signature Standard (DSS), Digital Signature Standard, NIST, January 27, 2000.

Derived Test Requirements for FIPS 140-1, Security Requirements for cryptographic Modules, NIST, March 1995.

[SSH IPSEC] SSH IPSEC Express Toolkit 3.0.1 Library and API Reference

2. SCOPE OF DOCUMENT

This document defines the Security Policy for the Entrust CygnaCom IPSec Cryptographic Module. It provides a description of how the module meets the requirements for Security Level 1 of Federal Information Processing Standards Publication 140-1 (FIPS PUB 140-1), *Security Requirements for Cryptographic Modules*. The U.S. National Institute of Standards and Technology (NIST) and the Canadian Communications Security Establishment (CSE) have validated that the Entrust CygnaCom IPSec Cryptographic Module conforms to FIPS 140-1. This document may be printed, posted, replicated, and freely distributed without modification.

3. OVERVIEW

The Entrust CygnaCom IPSec Cryptographic Module is a software cryptographic module intended to provide secure IPSEC communications between client workstations/laptops and servers. The communications are secured by the use of Triple DES (TDES) running in the Triple Cipher Block Chaining (TCBC) mode of operation to encrypt the data portion of TCP/IP packets using either the IPSEC ESP-tunneled mode or ESP-transport mode. Further details may be found in the *SSH IPSEC Express Toolkit: White Paper, Version 4.1, June 2001*.

The system complies with FIPS 140-1 Level 1 security requirements overall.

4. CRYPTOGRAPHIC MODULE (LEVEL 1)

The cryptographic module consists of the Entrust CygnaCom IPSec Cryptographic Module software running on a client platform. The platform runs the SCO CMW+[1] 3.0.1 operating system with all current service packs, ITSEC supplements, and machine-specific software drivers. SCO CMW+ 3.0.1 is a multi-

[1] CMW+ is a trademark of the Hewlett-Packard Corporation.

user operating system intended to be used on a standalone workstation or on multiple workstations networked together as peers. It is derived from SCO's Open Desktop/Open Server operating system, an X Window System-based Graphical User Interface and HP's Compartmented Mode Workstation, and MaxSix trusted networking software. It is intended for use as a secure operating system that allows organizations, users, and their applications to share data in a controlled and accountable manner through Mandatory Access Controls and Discretionary Access Controls. It provides a user interface and offers applications programming and network interfaces. For the purposes of this module, the operating system is pre-configured for single user operation (see Section 13). Although the operating system has been validated as providing E3 protection in accordance with the Information Technology Security Evaluation Criteria, the module was not tested on the same computer systems as used in the E3 validation. Therefore, from a FIPS 140-1 viewpoint, a trusted operating system is not claimed. The module boundary is defined by the platform enclosure.

The system is intended to run on a Pentium based computer with PCI networking.

5. SECURITY RULES

The module supports the following security rules.

1. The module shall encrypt and decrypt TCP/IP packets with validated TDES running in the TCBC mode of operation.
2. The module shall run on client systems.
3. The platform shall be a production grade system.
4. The module shall comply with FIPS 140-1.
5. The module shall provide identity-based authentication of the cryptographic officers and users for access to the cryptographic services of the module.
6. The module provides for session key establishment using the Diffie-Hellman IKE protocol.
7. The Diffie-Hellman modulus shall be 1024-bits.
8. Pre-shared keys will be used for authentication of the communicating entities.
9. The hash function used by the IKE protocol shall be a validated SHA-1 hash algorithm.
10. The module shall use a FIPS approved pseudo-random number generator to generate Diffie-Hellman private keys.
11. A cryptographic officer may perform both cryptographic officer and user functions.

6. MODULE INTERFACES (LEVEL 1)

The module has four logical interfaces.

Data Input Interface: All data input to the module other than control information enters by the data input interface. This data includes plaintext data to be encrypted, received ciphertext data to be decrypted, key establishment information, and authentication data. IPSEC communications are input through the RJ45 connector. Data may also be input to the module via the keyboard connector, the RS232 connectors, or one of the disk drives.

Data Output Interface: All data output from the module other than status information exits via the data output interface. This data includes plaintext data after decryption, ciphertext data after encryption, and key establishment information. Only the data portion of the packet is encrypted. IPSEC communications are output via the RJ45 connector. Data may also be output from the module via the CRT connector, the RS232 connectors, or one of the floppy disk drives.

Control Input Interface: The cryptographic officer may enter control information via the module keyboard or via control switches on the platform itself.

Status Output Interface: The platform outputs control information via the CRT connector or control indicators on the platform itself. The control information includes a status indicator that indicates to the operator any error condition that may occur. Status information pertaining to commands and conditional tests is placed in the sshipm.log file and status pertaining to power-up self-tests is placed in the fips.log file.

Power Interface: The module platforms have an external power interface that supplies power to the module's processor. The client laptops have an internal power source that can provide power to the module for a limited time period.

Maintenance Access Interface: The module does not have a maintenance access interface.

7. ROLES (LEVEL 1)

The module supports two roles, the cryptographic officer role and the user role.

Cryptographic Officer Role: The cryptographic officer is responsible for initializing the module, initializing users, inserting user passwords, establishing user profiles (if applicable), and monitoring the overall use of the module. All control input is provided by the cryptographic officer.

User Role: The user makes use of the cryptographic services provided by the module. Thus, the user may submit data to be encrypted and transmitted to other modules and the user may receive and decrypt data from users of other modules.

8. SERVICES (LEVEL 1)

The module provides the following services. The cryptographic officer may obtain all user services plus the services restricted to the cryptographic officer.

Initialize: Initializes the module (Cryptographic officer only). May be called by the cryptographic officer from the policy manager daemon.

Control Input: Inputs control information to the module (Cryptographic officer only). Performed by the cryptographic officer by modifying the sshipsec.spd file, and route.dat file.

Show status: Outputs the current status of the module to the CRT or a status indicator.

Log-on: Logs on and authenticates operator to module.

Self-tests: Initiates and runs the self-tests. This service is automatically provided whenever the system is rebooted.

Establish connection: Establishes a secure or bypass connection to another module. Whether the connection is secure or bypass is determined by the cryptographic officer at initialization time.

Close connection: Closes the connection and terminates the session.

Send data: Sends data to another module. Data is encrypted before transmission.

Receive data: Receives and decrypts data from another module.

Log-off: Logs off operator from module.

9. OPERATOR AUTHENTICAT ION (LEVEL 1)

The module provides for identity-based authentication of users and cryptographic officers at Level 1.[2] This authentication is provided by means of username and password. Operators are logged off the module whenever the system is powered down. Therefore, operators must be authenticated after each power up.

10. FINITE STATE MACHINE MODEL (LEVEL 1)

The finite state machine model is provided in a separate document [18].

11. PHYSICAL SECURITY (LEVEL 1)

The module platform is a multi-chip standalone module. The platform consists of production–grade multi-chip electronics with standard passivation completely contained in production-grade metal or hard plastic enclosures. Thus, it complies with Level 1 physical security requirements.

12. SOFTWARE SECURITY (LEVEL 1)

The design of the cryptographic software is documented in reference [2]. Reference [3] explains the correspondence between the design of the software and the security policy. Reference [4] provides a complete source code listing for all cryptographic software contained in the module. For each software module, function and procedure, the source code listing is annotated with comments that clearly depict the relationship of the software entities to the design of the software.

13. OPERATING SYSTEM SECURITY (LEVEL 1)

?? The cryptographic software is installed only as executable code and libraries.

?? A TDES data authentication code is computed on the cryptographic software within the module.

?? Only a single user is capable of using the module at a given time. The SCO CMW+ 3.0.1 operating system will only allow a single user session through direct logon to the module. In addition, the operating system is pre-configured to a single user mode at the vendor facility to prevent remote logon by disabling system features that would otherwise permit remote logon .

[2] Technically no authentication is required for Level 1 systems and only role-based authentication is required for Level 2 systems. However, the operating system provides for identity-based authentication, which is used by the module.

?? Use of the module is dedicated to the cryptographic process during the time the cryptographic process is in use.

14. CRYPTOGRAPHIC KEY MANAGEMENT (LEVEL 1)

Key types:

?? A *pre-shared secret (symmetric) key* is generated within the module by the cryptographic officer and can be updated by the cryptographic officer using the ipsecadmin utility. This key is used to authenticate the communicating party. It can only be imported into the module and exported from the module by the cryptographic officer in plaintext form.

?? A new *Diffie-Hellman public/private key pair* is generated for each secure session. This key pair is generated within the module using a FIPS approved random number generator. The private component of the key pair is never imported to or exported from the module.

?? A *Triple DES session key* is derived from the shared secret that is established using the Diffie-Hellman key pair. This key is used to encrypt the protocol data units that are transmitted in the IPSEC connection. Session keys are never imported to, or exported from, the module. The initialization vectors that are used during a session are generated using the module's FIPS approved pseudorandom number generator.

?? An *AH (symmetric) authentication key* is derived from the Internet Key Exchange negotiation (IKE)[3]. Inputs include random bit vectors from both initiator and responder and "SKEYID_d" field. This key is used with the HMAC SHA-1 (the first 96 bits) algorithm to generate an authentication code on message headers and protocol data units that are transmitted in the IPSEC connection. AH authentication keys are never imported to or exported from the module.

?? A *Triple DES MAC key* is fixed into the code at the factory under controlled conditions. It is used to perform a TCBC DAC as an integrity test on the cryptographic software. This key is never exported from the module.

Key generation:

?? The Diffie-Hellman domain parameter, *p*, is generated using a FIPS approved random number generator.

?? The Diffie-Hellman private key, *x*, is generated as specified in Appendix 3.1 of FIPS 186-2 with the function *G* constructed using the SHA-1 algorithm as specified in Appendix 3.3 of FIPS 186-2.

?? The PRNG has a Known Answer Test that is executed at power-up.

Key Distribution:

?? TDES session keys are established using the IKE protocol and the Diffie-Hellman key establishment method.

?? The IKE protocol also makes use of the SHA-1 algorithm.

[3] Further details may be found at http://www.ssh.com/tech/whitepapers/SSH_IPSEC_Express.pdf, that is, the *SSH IPSEC Express Toolkit: White Paper, Version 4.1, June 2001*.

?? A 1024-bit Diffie-Hellman scheme is used to establish a shared secret.

?? The two communicating modules derive the TDES session key from the shared secret.

Key Entry and Output:

?? Pre-shared secret keys are manually distributed and electronically entered to each module in plaintext form. The two communicating modules use these pre-shared keys for authentication purposes.

?? Diffie-Hellman public keys may be output from the module. Pre-shared secret keys can only be output from the module by the cryptographic officer. No private keys are output from the module.

?? TDES session keys are established by means of the Diffie-Hellman key agreement scheme.

Key Storage:

?? All keys within the module are in plaintext form with their access protected by the SCO CMW+ operating system.

Key Destruction:

?? All keys and other critical security parameters are zeroized by reformatting the computer disk drive.

?? The TDES, Diffie-Hellman, and AH authentication session keys are cleared immediately after the session is completed.

Key Archiving: The module does not archive keys.

15. CRYPTOGRAPHIC ALGORITHMS (LEVEL 1)

The module employs the following FIPS approved cryptographic algorithms.

?? TDES as referenced in FIPS 46-3 and specified in ANSI X9.52.

?? SHA-1 as specified in FIPS 180-1.

?? HMAC as specified in FIPS PUB 198 The Keyed-Hash Message Authentication Code (HMAC)

?? PRNG as specified in FIPS 186-2 Appendix 3.1 with the exception that SHA as specified in FIPS 180-1 is used instead of the modified SHA specified in FIPS 186-2.

16. ELECTROMAGNETIC INTERFERENCE/ELECTROMAGNETIC COMPATIBILITY (EMI/EMC) (LEVEL 1)

The module conforms to the EMI/EMC requirements specified by FCC Part 15, Subpart J, Class A (i.e., for business use).

17. SELF-TESTS (LEVEL 1)

When the module fails a self-test, the module enters an error state and outputs an error indicator via the status output interface. The module does not perform any cryptographic operations while in the error state and no data is output via the data output interface while the error condition exists. Each error condition and actions necessary to clear the error is documented in reference [4].

Power-Up Tests:

The following power-up tests are implemented.

?? PRNG Known Answer Test (KAT)

?? TDES Known Answer Test (KAT)

?? HMAC SHA-1 KAT

?? SHA-1 KAT

?? Software/firmware test: A TDES MAC is applied to all cryptographic software in the module and the MAC is stored in the module. This MAC is verified when the power-up tests are run.

Conditional Tests:

The following conditional tests are implemented.

?? Pair-wise consistency test: Whenever a Diffie-Hellman public-private key pair (x, g^x) is generated, and a third value t is also generated. The equation $(g^x)^t ? (g^t)^x \bmod p$ is then verified. It is also verified that x does not equal g^x.

?? Continuous random number generator test: The first random number generated by the PRNG after power-up is not used, but is saved for comparison with the next random number generated. Upon each subsequent generation, the newly generated number is compared with the previously generated random number. The test fails if the two compared blocks are equal.

?? Bypass test:The protection to be provided to a channel (encrypted or bypass) is redundantly encoded so that a single garble of the control table would be detected as an error and communications of improperly protected data would not be permitted. In addition, the first plaintext packet of each message to be encrypted is compared to the corresponding ciphertext packet. If the two packets are equal, control is transferred to the error state

18. REFERENCES

1. Entrust CygnaCom IPSec Cryptographic Module Finite State Machine Model
2. Entrust CygnaCom IPSec Cryptographic Module Software Architecture Document
3. Entrust CygnaCom IPSec Cryptographic Module Design Correspondence Document
4. Entrust CygnaCom IPSec Cryptographic Module Source Code Listing Document
5. UK ITSEC Scheme Certification Report No. P131, SCO CMW+ Release 3.0.1, Issue 1.0, September 1999.
6. The SSH IPSEC Express Toolkit: White Paper, Version 4.1, June 2001