PERMIT/Gate Crypto Module Security Policy
for the
TSCMP30 v2.00

Document Number: FIPSSP00

Version: 1.4

Last Revised: 2000-09-14

TABLE OF CONTENTS

TSCMP30 SECURITY POLICY INTRODUCTION

About this Document

This document provides supplemental security policy information for the TSCMP30 Crypto Module (CM). The TSCMP30 CM is an integrated collection of hardware, firmware and software running on the PERMIT/Gate 1520 (Alcatel 7132), 2520 (Alcatel 7133), 4520, 4620 (Alcatel 7134) and 7520 (Alcatel 7137) designed to do DES encryption in a manner that meets the FIPS 140-1 standard level 2 (level 3 Physical Security for 7520).

Valid PERMIT/Gate Platforms

What follows are the product names for the validation certificates.

TimeStep PERMIT/Gate 2520 and 4520 series 40 and 50 and 1520 series 50, running the software release 3.00.026 or 3.01.026. Alternate names are the Alcatel 7133 for the 2520 and 7132 for the 1520. The 4520 has been replaced by the 4620.

TimeStep PERMIT/Gate 4620 series 40 and 50, running the software release 3.00.026 or 3.01.026. Alternate name is the Alcatel 7134.

TimeStep PERMIT/Gate 7520 series 20 and 30, running the software release 3.00.026 or 3.01.026. Alternate name is the Alcatel 7137.

Software Version Details

The PERMIT/Gate builds 3.00 and 3.01 are the same code with the exception that the former includes the Entrust PKI and the latter includes support for the Netscape PKI. Neither impacts the crypto-module.

The same software source is built into eight different binary executable packages for distribution, all of which use the identical crypto-module code:

- 7520 3.00 – Export-controlled Entrust build for the 7520[1]
- 7520 3.00E – International Entrust build for the 7520

[1] Export Controlled versions restrict cryptographic key length to 56 bits for each of Cast, Blowfish and RC5. In addition, selection of 3DES will default to 56bit DES.

- 7520 3.01 – Export-controlled Netscape PKI build for the 7520[2]
- 7520 3.01E – International Netscape PKI build for the 7520
- xx20 3.00 – Export-controlled Entrust build for the 1520, 2520, 4520 and 4620[2]
- xx20 3.00E – Export-controlled Entrust build for the 1520, 2520, 4520 and 4620[2]
- xx20 3.01 – Export-controlled Netscape PKI build for the 1520, 2520, 4520 and 4620[2]
- xx20 3.01E – International Netscape PKI build for the 1520, 2520, 4520 and 4620

Module Purpose

The CM is used by the IPSec layer to encrypt and decrypt traffic passing though the gate. The CM is part of the standard build of the PERMIT/Gate models listed above and is used whenever the gate is in at least “Minimum” mode of operation. The module is designed to ensure that customers have access to the FIPS 140-1 validated CM for use on these platforms.

How it affects the PERMIT/Gate

The CM is responsible for the ESP DES and ESP 3DES cryptography done on the gateway when the module is enabled. On the 1520, 2520 and 4520 even when the CM is disabled it is still used in a non-validated mode. On the 7520, the CM is only used when in “Secure” or “Minimum” mode and IPComp is not enabled. When IPComp is enabled, the CM is in a valid FIPS mode, however the CM is not used in favor of the performance provided by the HiFn daughter card.

These CM makes use of two “master” keys: the “Master Authentication Key” and the “Master Decryption Key”. These keys are DES keys and are entered into the gateway via the console. They are stored in the zeroizable NVRAM so that in the event of tamper switch release, or activation of the clear button, they will be cleared and the stored key table will be illegible. A 32-bit DES MAC generated with the Master Authentication Key authenticates the key file. Before loading a key file the

[2] Export Controlled versions restrict cryptographic key length to 56 bits for each of Cast, Blowfish and RC5. In addition, selection of 3DES will default to 56bit DES.

module will verify this signature and in the event of failure, it will reject the file and return the module to the un-initialized state.

TSCMP30 FUNCTIONS

Master Key Management

Two master keys will be used to safeguard the key table, as described in the next section. These keys will be kept in the zeroizable RTC NVRAM and in the event of tamper switch release or activation of clear button, this key will be erased. Functions will be provided for loading and clearing these master keys.

In order to change one of the master keys, the crypto-officer must enter the existing authentication master key. If the gate has been zeroized then the master authentication key is 00000000000000.

Key Table Management

All keys to be used for DES encryption and decryption will be stored in a table. This table will be stored in RAM, and each key will be encrypted with ECB DES with the Master Decryption Key.

When the key file is loaded, it will be authenticated by the second master key, the Master Authentication Key. The file’s 32 bit CBC DES MAC will calculated with this key.

Encryption / Decryption

This module will be used to do DES and 3DES encryption of network traffic passing through the gateway. The IPSec module will make calls to this crypto module passing it data to encode or decode. It will also supply all initialization vectors and will specify which key is to be used by the key’s reference number (a form of index into the key table). The module will use the decryption master key to decrypt the specified key from the table so that it can perform the requested operation.

Crypto-officer Interface

The crypto-officer has two interfaces:

- Setting and clearing the master keys (authentication and decryption). To set the master keys, the crypto-officer must enter the existing master authentication key as validation of identity; and

- Loading and clearing the Static Key Table.

TSCMP30 ROLES

Crypto Officer

The Crypto Officer is a user authorized to select the mode of operation of the module, set the master keys, and to load the static key table. Outside the CM, the Crypto Officer is also allowed to set up security associations so that the PERMIT/Gate has a policy for what to do with data passing through (whether to let it pass, to encrypt it, to decrypt it, or to block it).

The Crypto Officer is responsible for the initialization and configuration of the device and for selecting an appropriate mode of operation.

With respect to the CM, the Crypto Officer is allowed to:

- Enable and disable the module’s FIPS 140-1 validated operation.
- Enable and disable the hardware active tamper and zeroization switch.
- Set the master keys (but not read the currently loaded keys).
- Clearing the current master keys.
- Load a new static key table in encrypted form (but not read the currently loaded table).
- Clearing the currently loaded static key table.

User

The user is defined as the IPSec module application process residing on the gate that accesses the CM on behalf of external entities. The IPSec module can request encryption and decryption operations on data with keys from the Key Table. The IPSec module does not have identities, passwords, or keys.

TSCMP30 DETAILED SECURITY POLICY

Crypto-Module Definition

The CM is the integrated hardware, firmware and software component of the PERMIT/Gate, modules 1520, 2520, 4520, 4620 and 7520, that performs the following functions:

- DES and 3DES encryption for data encryption;
- the digital signature checking on loading application software which is needed to verify that the FIPS module software is indeed as shipped by Alcatel;
- random number generation; and
- SHA-1 hashing.

The PERMIT/Gate uses the validated CM to perform the packet data encryption needed for the IPSec Encapsulated Security Payload (ESP) transform whenever the CM is in “secure” or “minimum” mode.

Modes of Operation

The CM has two validated and one non-validated modes of operation. They are as follows:

1. “Secure” mode enables the validated module including the hardware active anti-tamper and zeroization feature. This is a FIPS validated mode of operation providing FIPS level 2 for the 1520, 2520, 4520 and 4620 gates and FIPS level 2 with Physical Security Level 3 for the 7520 gate.
2. “Minimum” mode enables the validated module with the exception of the hardware anti-tamper and zeroization feature. This is a FIPS validated mode of operation providing FIPS level 2 for all gate models.
3. “Disabled” mode does not use the module in a validated mode of operation. On some gates it may provide a higher level of performance by not using the module at all. This is a non-validated mode of operation.

Crypto-Module Services

The CM provides the following services:

1. It verifies that any application software being loaded has not been tampered with or changed since it was shipped from Alcatel. This occurs regardless of the mode of operation of the CM.

2. It allows the CO to enable and disable the module by selecting the mode of operation from “Disabled”, “Minimum” and “Secure”.

3. It provides an interface for the CO to initialize the module by setting master keys which then allow the loading of a signed and encrypted key file generated by the CO outside of the CM. Loaded keys are added to the CM’s key table.

4. It also provides an interface for application software to load keys into the CM while it is running. These keys are then encrypted with the master key and added to the CM’s key table.

5. It encrypts and decrypts data as requested by the application software running on the PERMIT/Gate using either the DES or 3DES algorithms, using the keys previously loaded into the CM. The application software uses a key handle to select the key to use. The master keys are not selectable for data encryption nor decryption.

6. It provides a random byte stream to the application software upon request.

7. It provides SHA-1 hashing services to the application software upon request.

8. It provides a power-on self-test function service on start-up.

Authentication Policy

The CM employs a role based authentication scheme.

The crypto officer role is established by initializing the module with the master authentication keys.

For calls to set master keys or to change the mode, the crypto-officer must correctly enter the first 8 hex digits of the current master authentication key.

The user role (IPSec module) is authenticated by the DSA signature verification of the application during start-up.

If the module is zeroized by the clear button or a tamper switch release, the master authentication key must be reentered and the user is not authenticated to perform this action.

Access Control Policy

Roles: Crypto Officer and User.

Services: Verification of application software load, Setting the mode of operation, Setting the Master Key, Loading the Key Table, performing cryptography on data, providing a random byte stream to the application, SHA-1 hashing service, and power-on self-tests.

Security Relevant Data Items: The Master Authentication Key (plaintext), the Master Decryption Key (plaintext), the Key Table (encrypted) and authentication data.

Modes of Access: Write mode of operation, Write/Delete Master Key, Write/Delete Key Table, Read/Write Data.

Physical Security Policy

1520, 2520, 4520, 4620: The two halves of the enclosure are fastened together using four Phillips screws. A frangible seal covers two of the screws. The frangible seal must be in place at least 48 hours to ensure proper bonding of seal to enclosure. The module enclose has a clear button on the front and a compromise detection switch. Pressing the clear button or releasing the switch will zeroize the two master keys.

7520: The two halves of the metal enclosure are fastened together by six Phillips screws on the sides. A frangible seal covers two of the screws. The frangible seals must be in place at least 48 hours to ensure proper bonding of seal to enclosure. The module enclosure has a clear button on the front and a compromise detection switch. Pressing the clear button or opening the enclosure will zeroize the two master keys.

Crypto Officers note: The frangible seals are applied at manufacturing time. The normal packaging, shipping and delivery process should ensure 48 hour bonding of the frangible seals. To ensure proper bond, Crypto Officers are advised to delay gate installation for 48 hours after receipt of equipment.

Signs of physical security for all platforms would be broken seals and/or missing master keys which would lead to the module ceasing operations and not encrypting nor decrypting data although the RNG and SHA-1 interfaces would still be operational.

Key Security Policy

“Secure” mode: The master keys are stored in the real time clock (RTC) where they are cleared if the PERMIT/Gate detects a tamper switch release or if the clear button is pressed.

“Minimum” mode: The master keys are stored in a Serial EEPROM (SEEP) where they are cleared if the PERMIT/Gate detects the clear button or tamper condition when power is applied. They are not cleared on a tamper switch release or if the clear button is pressed when power is not applied.

At initialization, the master keys are loaded into the module from the RTC or SEEP, the key file is verified with the master authentication key. If the authentication of the key file fails, the key file is rejected and not loaded.

The master encryption key is stored inside of the hardware DES chip after initialization in a register only used for key encryption and decryption.

User keys from the key file and loaded keys are stored in the PERMIT/Gate’s memory in encrypted form and are never stored in memory in clear form.

Crypto Officer

Services that can be performed: Selecting the mode of operation, initializing the module by setting the Master Keys (write only), Loading the Key Table (write only).

User (IPSec Module)

Services that can be performed: verification of authenticity and integrity of application, load keys to the Key Table while CM is running, performing DES or 3DES cryptography on data with keys from the Key Table (read/write), generating a random byte stream, SHA-1 hashing services, and performing Power-on Self-Tests.

Gate Redundancy Feature

The PERMIT/Gate product supports a redundancy feature that archives keys from a master gate to one or more backup gates. In the event that the master gate becomes unavailable, the backup gates hold an election and select a new master.

The redundancy feature relies upon a shared secret between the gates in a cluster to determine who can join the cluster. The shared secret is used to authenticate and encrypt the communications between the master and the backup gates through negotiation of an IPSec Security Association (SA). The following explanation clarifies the operation of the Gate Redundancy feature, providing assurance that this feature does not violate the FIPS validation.

The TSCMP30 crypto module does not generate keys. Under normal operation, plaintext Keys are loaded by the user (IPSec module) on the gate to the CM. These keys are then encrypted by the CM (using the Master Key) for storage and released to memory in encrypted form.

In redundancy mode, prior to passing the keys to the CM for encryption, the plaintext keys are transmitted to the redundant gates within the cluster. Because these keys originate outside the CM, transfer of these keys does not violate the TSCMP30 FIPS validation. The IPSec module, not the CM, is exporting the keys. However, recognizing the danger of transmitting plaintext keys, the design ensures that the keys are encrypted in transit.

When operating in FIPS mode (secure or minimum), the gates communicate using IPSec Security Associations (SA) that use the validated CM DES or 3DES engine to encrypt all traffic between gates. Therefore, when transmitting the plaintext keys, a DES or 3DES SA is established. The plaintext keys are encrypted within the resulting IPSec tunnel. The receiving gate decrypts the keys and plaintext keys arrive at the destination gate IPSec module. The destination gate IPSec module then passes the plaintext keys to the local CM to encrypt (using the local Master Key) and to add to the local Key Table as if it was a set of keys locally generated.

Therefore, the IPSec module transfer of keys is outside the CM, however in FIPS mode the FIPS validated CM is used to encrypt the traffic between gates. There is no change to the loading of Master Keys, since the keys transferred are not Master Keys. There is no change to the loading of Key Tables, since the receiving gate CM encrypts the key provided and adds them to the Key Table the same as it does for all other keys. All roles and authentication mechanisms are as per normal operation. The archival process is initiated outside the CM by configuring the gates to do redundancy (also called clustering). Hence, from the CM perspective, there is no change to its FIPS validated secure operation.