# LEVEL 3 SECURITY POLICY for

# SafeNet Luna EFT

| | |
|---|---|
| **DOCUMENT NUMBER:** | CR-2786 |
| **AUTHOR(S):** | Brian Franklin / Terry Fletcher / Iain Holness |
| **DEPARTMENT:** | Engineering |
| **LOCATION OF ISSUE:** | Ottawa |
| **DATE ORIGINATED:** | January 15, 2008 |
| **REVISION LEVEL:** | 9 |
| **REVISION DATE:** | September 2, 2011 |
| **SUPERSESSION DATA:** | 8 |
| **SECURITY LEVEL:** | |

*SafeNet, Inc. reserves the right to make changes in the product or its specifications mentioned in this publication without notice. Accordingly, the reader is cautioned to verify that information in this publication is current before placing orders. The information furnished by SafeNet, Inc. in this document is believed to be accurate and reliable. However, no responsibility is assumed by SafeNet, Inc. for its use, or for any infringements of patents or other rights of third parties resulting from its use.*

## TABLE OF CONTENTS

## LIST OF TABLES

## LIST OF FIGURES

# 1. INTRODUCTION

## 1.1. Purpose

This document describes the security policy enforced by the SafeNet Luna EFT.

This document applies to:

- Firmware Version MAL000000E and Hardware Version GRK-09-0100
- Firmware Version MAL000001E and Hardware Version GRK-15-0100.

## 1.2. Scope

The security policy described in this document applies to the SafeNet Luna EFT only and does not apply to any application firmware that may be loaded on the SafeNet Luna EFT (hereafter referred to as “appliance” or “module”).

## 1.3. Intended Audience

The intended audience for this document is the SafeNet HSM Engineering and Product Management Team, external agencies for validation or endorsement of the SafeNet Luna EFT module and selected industry partners and prospective customers.

## 1.4. References

| Document Number | Title |
|---|---|
| N/A | Integrated Circuit Card Application Specification For Debit and Credit on Chip, Version 2.0, MasterCard International. |
| N/A | EMV ’96 Version 3.1.1, May 31, 1998 Integrated Circuit Card Application Specification for Payment Systems |
| N/A | EMV ’96 Version 3.1.1, May 31, 1998 Integrated Circuit Card Specification for Payment Systems Part IV – Security Aspects; Annexes E and F. |
| N/A | EMV Draft version 0.5 October 31, 2000 Issuer Security Guidelines |
| N/A | EMV2000 Version 4.0 December 2000 Integrated Circuit Card Specification for Payment Systems Book 2 – Security and Key Management |
| N/A | Europay Int'l Version 2.1 October 1999 Integrated Circuit Card (ICC) Application Specification for Pay Now (Debit) and Pay Later (Credit) cards |
| N/A | MasterCard Int'l Version 2.1 November 1999 MasterCard Chip— Recommended Specifications for Debit and Credit |
| N/A | Visa Int'l Version 1.4.0 October 2001 Visa Integrated Circuit Card Application Overview |
| N/A | Visa Int'l Version 1.4.0 October 2001 Visa Integrated Circuit Card (ICC) Specification |
| N/A | Common Electronic Purse Specifications – Technical Specification Version 2.3 March 2001 |
| N/A | Joint Specification for Common Electronic Purse Cards Version 2.1.3 February, 2001 |
| N/A | Joint Card Interface Specification for Issuers of Common Electronic Purse Cards –Volume 1 – Load, Currency Exchange and POS Transaction Processing Version 1.0 April 2000 |
| N/A | Visa Cash Electronic Purse Specifications – Technical Specification – Volume 1 Version 4.1 September 2000 |

| Document Number | Title |
|---|---|
| N/A | Visa Cash Electronic Purse Specifications – Technical Specification – Volume 2 Version 4.1 January 2001 |
| N/A | Visa International CEPS PSAM Creator Version 1.0 |
| N/A | PSAM DES Key Card Version 1.10 April 5, 2002 |
| N/A | Diebold, Certificate Management, Rev. 1.4, 24 Jun 02 |
| N/A | Diebold, Remote Key Management, Rev. 1.4, 24 Jun 02 |
| N/A | Diebold, Triple DES Requirements, FIRST Key – 91x Message Formats, Rev. 1.5, 26 Jun 02 |
| N/A | NCR, Modifications to NDC+ to support: EPP, RSA Initial Key loading, ISO PIN Block formats, 17 Jul 01 |
| N/A | RSA Laboratories, PKCS#1: RSA Cryptography Standard, v2.0, 01 Oct 98 |
| N/A | RSA Laboratories, PKCS#10: Certification Request Syntax Standard, v1.7, 26 May 00 |
| N/A | RSA Laboratories, PKCS#7: Cryptographic Message Syntax Standard, v1.5, 01 Nov 93 |
| N/A | X9.24 Part II, Symmetric Key Management, using asymmetric techniques for the distribution of symmetric keys, V1.0., ..03 |
| N/A | ANSI X9, TR-31 2004: Interoperable Secure Key Exchange Key Block Specification for Symmetric Algorithms, Draft, 7 Nov 03 |
| N/A | Vendor Group (ACI WorldWide, HP Atalla, Diebold, Thales e-Security, Verifone Inc.), Global Interoperable Secure Key Exchange key Block, V2.3, 6 Dec 02 |
| N/A | Verifone, Global Interoperable Secure Key Exchange (GISKE) Key Block Specification, VPN 22986 Rev C, data unknown |
| N/A | ISO 9564-1-2002 Banking - Personal Identification Number - PIN - management and security - Part 1- Basic principles and requirements for online PIN handling in ATM and POS systems. |
| N/A | ISO 9564-3-2003 Banking - Personal Identification Number management and security - Part 3- Requirements for offline PIN handling in ATM and POS systems. |
| N/A | ANS X9.24-1 Retail Financial Services Symmetric Key Management Part 1 :Using Symmetric Techniques: 2004 |
| N/A | MasterCard SecureCode Chip Authentication Program: Functional Architecture: Sept, 2004. |
| N/A | Common Personalization Specification,Visa International, Version 1.5, January 2002. |
| N/A | Global Platform Card Specification, Global Platform, Version 2.1, June 2001. |
| N/A | Schnittstellen Spezifikation für die ZKA-Chipkarte: Secure Chip Card Operating System (SECCOS), Version 5.0, June 2001. |
| N/A | EMV Integrated Circuit Card Specification for Payment Systems: Book 2 – Security and Key Management, Version 4.1, May 2004. |
| 004494-002 | SafeNet Luna EFT Programmer's Guide |
| 007427-001 | SafeNet Luna EFT Communications Guide |
| 007428-001 | SafeNet Luna EFT Console User's Guide |

# 2. SECURITY POLICY

## 2.1. Functional Overview

The appliance is a physically and logically secured appliance platform used as the host for the SafeNet Luna EFT product line. The appliance's primary security service is to verify the digital signature of the Luna EFT application firmware before allowing it to load. The appliance is a multi-chip standalone module that meets all FIPS 140-2 Level 3 requirements.

The appliance's loader firmware, which is installed during device manufacture, is included in the scope of the appliance validation. The loader firmware will only allow an application to be loaded if the application has been signed by a private key that corresponds to the public key embedded in the loader application. Loaded firmware must be separately validated in order for a product comprising the appliance plus application firmware to be considered FIPS validated.

The loader firmware is implemented as a 32-bit protected mode Intel executable and runs as the only application on a specially cut-down Fedora Core 3 (FC3) Operating System (O/S). The FC3 system launches the loader firmware and provides disk and memory management services and communication services to the loader firmware.

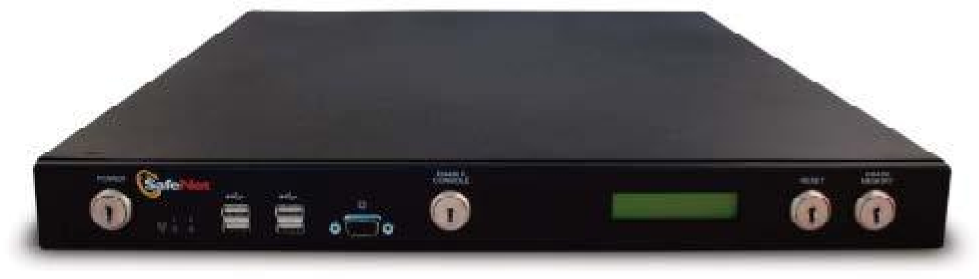

Figure 2.1.1. SafeNet Luna EFT

## 2.2. FIPS-Approved Mode of Operation

The module implements the following FIPS-approved algorithms:

| Algorithm | MAL00000E / GRK-09-0100 | MAL000001E / GRK-15-0100 |
|---|---|---|
| RSA (FIPS 186-2) | Cert. 723 | Cert. 889 |
| SHA-256 (FIPS 180-2) for signature verification | Cert. 1335 | Cert. 1560 |
| TDES (FIPS 46-3) CBC with key lengths: 112 bits, 168 bits | Cert. 994 | Cert. 994 |
| RNG (FIPS 186-2 compliant ANSI X9.31 TDES-2Key) | Cert. 806 | Cert. 806 |

The appliance is in a FIPS-approved mode of operation when no application firmware has been loaded, otherwise it is in non-FIPS mode. The current mode is indicated by reviewing the console output.

It should be noted that the physical security of the appliance and the operation of the Random Number Generator are dependant on internal hardware features and not the firmware being loaded.

### 2.2.1. Non FIPS-Approved Algorithms

The module implements the following non FIPS-approved algorithm: MD5

## 2.3. Cryptographic Module Ports and Interfaces

### 2.3.1. Front Panel Physical Interfaces

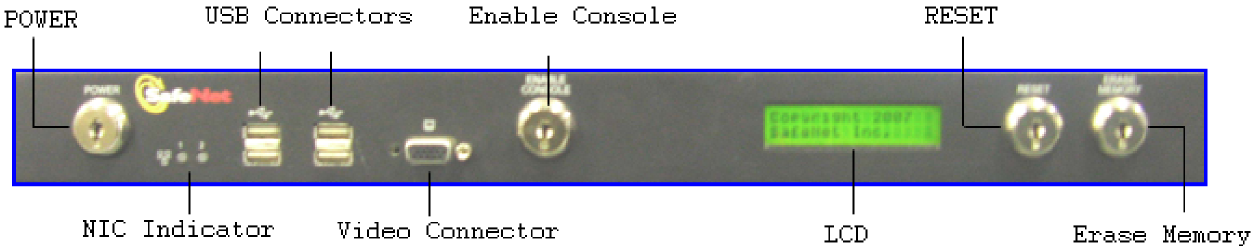

Figure 2.3.1. Front View – SafeNet Luna EFT

The module has the following physical interfaces on the front panel:

- Four USB connectors
- One VGA output
- An LCD display on the front panel that displays system status information
- There are several physical key-activated switches on the front panel:

a. A “POWER” on/off switch to control the device power.

b. A “RESET” switch to command a device reset.

c. A switch labelled “Enable Console” that enables the VGA output and USB connectors.

d. A switch labelled “Erase Memory”. The Erase Memory Key activates the tamper response circuit, which asserts the signal that erases the plaintext master key in the Real Time Clock (RTC) memory of the internal PCI card and also signals the ATX power supply to go to standby mode, removing main power from the motherboard and destroying DRAM contents. When the key switch is released (i.e., the tamper source is removed), the signal to the internal crypto card and the ATX is removed and the device is free to boot up again without any Critical Security Parameters (CSPs) being set.

### 2.3.2. Back Panel Physical Interfaces

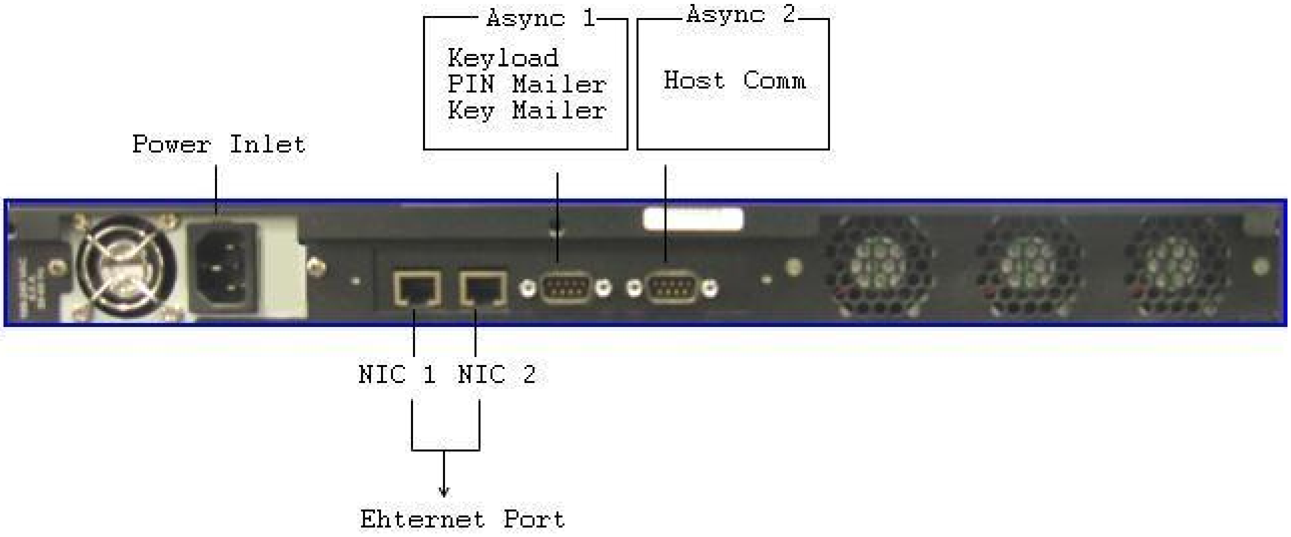

Figure 2.3.2 Back View – SafeNet Luna EFT

The module has the following physical interfaces on the back panel:

- Main power socket (110 or 220 volt 50-60Hz)
- Two RS232 serial ports. These are referred to as the Keyload and Host Comm ports, but with the application loader firmware installed they have no security-related uses.
- Two RJ-45 10BaseT/100BaseTX/1000BaseTX Ethernet connections. One connection is used to receive application firmware updates and the other is reserved for future use.

### 2.3.3. Logical Interfaces

The module's physical interfaces are separated into logical interfaces, defined by FIPS 140-2, and described in Table 2.3.1:

| FIPS 140-2 Logical Interfaces | Device Physical Interfaces |
|---|---|
| Data Input Interface | Ethernet port, USB ports |
| Data Output Interface | VGA port |
| Control Input Interface | Reset SW, Power SW, Erase Memory SW, Console Enable SW, USB ports |
| Status Output Interface | Ethernet port, LCD, VGA port |
| Power Interface | Main power socket |

Table 2.3.1. FIPS 140-2 Logical Interfaces

# 3. ROLES AND SERVICES

## 3.1. Module Roles

The module supports two roles:

- Administrator – an authenticated operator performing administrative duties, the administrator is also authorised to load a signed application firmware package.
- Crypto Officer – an authenticated operator who performs some manufacturing duties

The Administrator role performs the verification of the signature on the application firmware to be loaded into the appliance.

Unauthenticated users may access non-cryptographic services provided by the module.

The services accessible from the module are described in section 3.2.

### 3.1.1. Authentication

The appliance implements identity-based operator authentication and assigns the Crypto Officer or Administrator role based on the type of authentication used.

The identity associated with the module's Crypto Officer is the manufacturer. The manufacturer first initializes the appliance by installing the loader firmware and the public key into the module.

The authentication data required of the manufacturer in the Crypto Officer role is password-based.

In the Administrator role, the manufacturer or authorized agent uses the Console interface to load the signed application, which in turn invokes the signature verification service. The Administrator is authenticated by a password entered through the Console interface. The authentication verification data is a copy of the password entered previously by the Administrator and stored inside the module protected with TDES CBC encryption.

### 3.1.2. Strength of Authentication Mechanisms

Since the size of the search space required to recover a private key for 2048-bit RSA is $2^{112}$, the probability that a random attempt to use the authentication mechanism will succeed or that a false acceptance will occur is significantly less than one in 1,000,000. There is a practical maximum of 15 verification attempts possible in a minute (selecting and verifying signed binaries) versus a total space of $2^{112}$ or (reducing by $10^{20}$) 51,922,968,585,348 possible signed binaries, which becomes a 1/3,461,531,239,023 chance of succeeding in a minute. Since authentication depends on signature verification as a part of the application loading process, the probability that multiple attempts to use the authentication mechanism during a one-minute period will succeed or that a false acceptance will occur is significantly less than one in 100,000.

The Administrator and Crypto Officer passwords are alpha-numeric strings from 6 to 10 characters long. Both uppercase and lowercase alphabetical characters are allowed as well as punctuation marks and the space character. There are at least 88 different characters possible for each character in the password. With a minimum of 6 characters, this means that there are at least $88^6$ or $4.6 \times 10^{11}$ possible passwords[1]. The probability that a random attempt to use the authentication mechanism will succeed or that a false acceptance will occur is significantly less than one in 1,000,000. There is a practical maximum of 30 authentication attempts possible in a minute versus a total space of possible combinations of 88^6 or 464,404,086,784 different signatures. This becomes a 30/464,404,086,784 or 1/15,480,136,226 chance of succeeding in a minute. Since the authentication process must be performed by an operator via the console interface (i.e., cannot be automated) the probability that multiple attempts to use the authentication mechanism during a one-minute period will succeed or that a false acceptance will occur is therefore significantly less than one in 100,000.

[1] The actual space is 4,644,040,867,864 possible passwords.

## 3.2. Module Services

The only two cryptographic (or supporting) services provided by the module are operator authentication (Administrator) and the verification of the digital signature on application firmware to be loaded into the device. The Administrator automatically invokes the signature verification service with an attempt to load an application.

The Administrator also has these management services available:

- Change the Administrator password
- Selectively enable and disable TCP/IP Host port functions
- Set TCP/IP network parameters
- Run self tests and view device status statistics
- View the upgrade public key fingerprint
- Reboot the device (resets the module without losing CSPs)
- Verify and install application firmware package obtained from a mass storage device on an USB port, or previously loaded by host port function

The Crypto Officer has these management services available:

- View the status on the Console
- View device status statistics
- initial installation and configuration of firmware at manufacturing time
- Change the Crypto Officer password

The following non-cryptographic services are also available to unauthenticated operators in physical proximity to the device:

- Reboot unit (resets the module without losing CSPs)
- Erase memory (using front panel keyed switch)
- Disable Console (force Administrator to log off using front panel keyed switch)
- View the status on the LCD display

The following non-cryptographic services are also available to unauthenticated operators accessing the TCP/IP host port:

- Low level network services ICMP (Ping) ARP
- Status Query functions (HSM_STATUS, HSM_ERRORLOG_STATUS, HSM_GET_ERRORLOG, GET_VERSION, HSM_SOFTWARE_STATUS)
- Self-test functions (TEST_PORT, TEST_CRYPTO, GEN_RNG_RSA)
- The LOAD_HSM_SOFTWARE function provides one of several methods to present the application firmware package to the Administrator. This function does not cause the firmware to be verified or installed.

## 4. SELF-TESTS

The power-on self-tests performed by the module are an Error Detection Code (EDC) test for validating the loader application, and Known Answer Tests (KATs) on the RSA signature verification, SHA-256, TDES and RNG algorithms.

If the EDC test or any one of the KAT tests fails, an error message is logged and the module Halts.

Conditional self-tests are applied to the RNG output.

## 5. ACCESS CONTROL POLICY

The Crypto Officer is authorized to install the application loader firmware, which includes the SafeNet public key, into the module at the manufacturing facility. The application loader firmware will prevent itself from being overwritten by anything other than a validly signed application once it is installed. This is to prevent a potentially malicious version of the firmware, with a forged certificate representing a rogue signing key, from being installed before the application is loaded.

The Administrator is authorized to perform signature verification as part of the application-loading service provided by the module.

An operator may also perform other services provided by the module (see Section 3.2).

## 6. CRITICAL SECURITY PARAMETERS

The only cryptographic key directly employed by the module is the public key component of the SafeNet application firmware verification key pair. This is stored on the internal hard disk in plaintext form and is protected by the physical and logical security mechanisms associated with the appliance. The public key remains with the module throughout its operational life. Although disclosure of the public key does not constitute a security risk, replacement of the public key would enable an attacker to sign malicious applications using a rogue private key and thereby potentially cause damage to a customer's application system.

There is one password stored on the device that is used to authenticate the Administrator. The password is stored in an encrypted form (TDES CBC) on the appliance hard disk. The encrypting key is held in tamper responding memory within the internal crypto card.

Private keys are not stored or used by the module.

The PRNG Seed Value and PRNG Key Value are automatically zeroized when the module is powered off.

### 6.1. Access Control

The following table shows each key or CSP along with the type of access for each role.

**R -** The item is **read** or referenced.

**W -** The item is **written** or updated.

**X -** The item is **executed**. (The item is used as part of a cryptographic function.)

**D -** The item is **deleted**.

| Service / Role | Key or CSP | Access Control |
|---|---|---|
| Verify signed image / Administrator / Crypto Officer | RSA Public Key | R<br>R |
| Change password / Administrator / Crypto Officer | User Password | W<br>W |

| Service / Role | Key or CSP | Access Control |
|---|---|---|
| Run self test / Administrator | PRNG Seed Value<br>PRNG Key Value | R,X<br>R,X |
| View Upgrade Public Key Certificate / Administrator | RSA Public Key | R |
| Erase memory / Administrator / Crypto Officer | PRNG Seed Value<br>PRNG Key Value<br>Module Master Key | D<br>D<br>D |
| Initialize appliance / Administrator | Module Master Key | W |

Table 6.1.1 - Access Control for CSPs

## 7. OPERATIONAL ENVIRONMENT

The FIPS 140-2 Operational Environment requirements are not applicable, because the appliance's cryptographic module does not contain a modifiable operational environment. The module only supports the loading of application firmware that is properly signed by the SafeNet application signing authority. In order for the appliance to continue in a FIPS-approved mode of operation after loading an application, the application itself must have been separately validated.

## 8. PHYSICAL SECURITY

The appliance is a tamper-resistant multiple-chip standalone cryptographic module consisting of production grade components intended to meet FIPS 140-2 Level 3. It does not support a maintenance role and therefore security concerns arising from such a role are not relevant.

The appliance is contained in a hard metal enclosure with double louvers and baffles to prevent probing. The enclosure is sealed using break-away screws and tamper-evident seals to prevent easy removal of the enclosure's lid and to provide tamper evidence in the event the lid is forced off in some way.

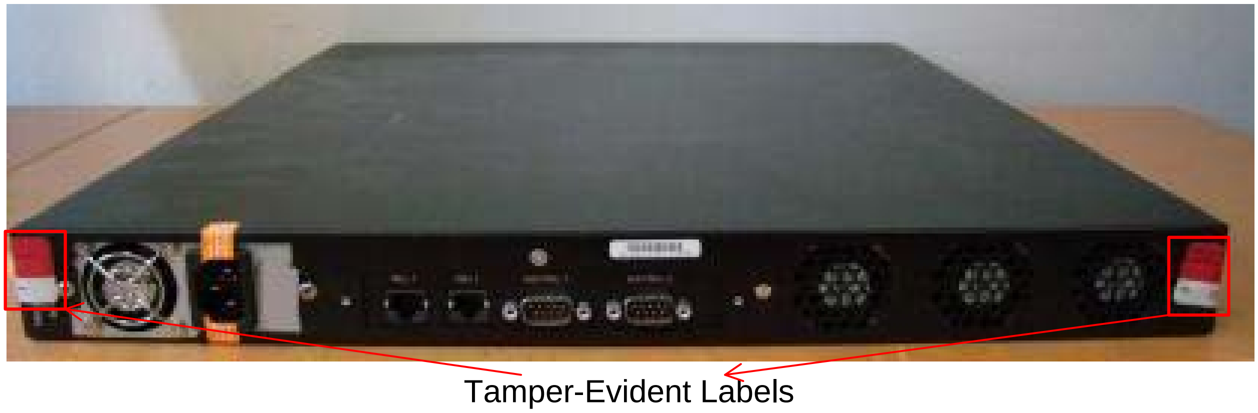

Figure 6.1.1 – Serialized Tamper-Evident Seals (at rear corner of each side of appliance)

The module should be periodically inspected for evidence of tamper (note that only the corner red and white labels shown in Figure 6.1.1 provide tamper evidence). The physical security mechanism described previously uses passive techniques and therefore no testing of the mechanism is required.

The appliance also contains tamper switches that are triggered in the event the lid is removed. If any of the switches are triggered, the module will immediately clear any sensitive application data, power down and prevent access to the loader firmware.

# 9. GLOSSARY OF TERMS, ACRONYMS AND ABBREVIATIONS

| **Terms** | **Definitions** |
|---|---|
| 10BaseT/100BaseTX | Ethernet over twisted pair (10 Mbit/s and 100Mbit/s) |
| ARP | Address Resolution Protocol |
| ATX | Advanced Technology Extended |
| CBC | Cipher Block Chaining |
| CSP | Critical Security Parameter |
| DRAM | Dynamic Random Access Memory |
| EDC | Error Detection Code |
| FC3 | Fedora Core 3 |
| FIPS | Federal Information Processing Standard |
| ICMP | Internet Control Message Protocol |
| KAT | Known Answer Test |
| LCD | Liquid Crystal Display |
| NIC | Network Interface Controller |
| O/S | Operating System |
| PCI | Peripheral Component Interconnect |
| RJ-45 | 8 position 8 contact (8P8C) modular communications connection |
| RNG | Random Number Generator |
| RS-232 | Recommended Standard 232 for serial binary data signals connecting between a Data Terminal Equipment (DTE) and a Data Circuit-terminating Equipment (DCE) |
| RSA | Rivest, Shamir, Adelman |
| SHA | Secure Hashing Algorithm |
| TDES | Triple-DES |
| TCP/IP | Transport Control Protocol / Internet Protocol |
| USB | Universal Serial Bus |
| VGA | Video Graphics Array |