3e Technologies International

3e-636 Series Network Security Device

Security Target

45040-007-01

Revision J

March 12, 2015

Version 1.0

3e Technologies International 636 Series Network Security Device Security Target

This document, as well as the software described in it, is furnished under license and may be used or copied only in accordance with the terms of such license. The content of this document is furnished for informational use only, is subject to change without notice, and should not be construed as a commitment by 3eTI. 3eTI assumes no responsibility or liability for any errors or inaccuracies that may appear in this document.

Document ID Number: 45040-007-01 Revision J

Contact:

3e Technologies International, Inc.
9715 Key West Avenue
5th Floor
Rockville, MD 20850 USA

Telephone: +1 (301) 670-6779
Fax: +1 (301) 670-6989

Website: http://www.3eti.com/
Email: mailto:info@3eti.com

Table of Contents

List of Tables and Figures

1 Security Target Introduction

This section presents security target (ST) identification information and an overview of the ST. The structure and content of this ST comply with the requirements specified in the Common Criteria (CC), Part 1, Annex A.

1.1 Security Target References

ST Title: 3eTI 3e-636 Series Network Security Device Security Target

ST Version: Version 1.0, Revision J

Vendor: 3e Technology International, Inc.

ST Publication Date: March 12, 2015

Keywords: Encryption, VLAN, VPN, IPSec, access control, data packet inspection, traffic filter, 802.1X

1.1.1 Document References

The following documents were used to develop the Security Target.

Table 1-1: US Government and Standards Document References

Reference	Document
[CC_PART1]	Common Criteria for Information Technology Security Evaluation-Part 1: Introduction and general model, July 2009, version 3.1R3, CCMB-2009-07-001
[CC_PART2]	Common Criteria for Information Technology Security Evaluation-Part 2: Security functional components, July 2009, version 3.1R3, CCMB-2009-07-002
[CC_PART3]	Common Criteria for Information Technology Security Evaluation-Part 2: Security assurance components, July 2009, version 3.1R3, CCMB-2009-07-03
[CEM]	Common Methodology for Information Technology Security Evaluation, Evaluation methodology, July 2009, version 3.1R3, CCMB-2009-07-004
[NDPP V1.1]	US Government, Protection Profile for Network Devices, June 08, 2012
[PKE PP]	US Government Family of Protection Profiles: Public Key-Enabled Applications for Basic Robustness Environments, May 1 2007, Version 2.8
[FIPS PUB 140-2]	National Institute of Standards and Technology, FIPS PUB 140-2 Security Requirements for Cryptographic Modules, December 2002.
[FIPS PUB 186-3]	Digital Signature Standard (DSS), June 2009
[NIST SP 800-56A]	NIST Special Publication 800-56A, “Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography”
[NIST SP 800-57]	NIST Special Publication 800-57, “Recommendation for Key Management”
[NIST SP 800-120]	NIST Special Publication 800-120, Recommendation for EAP Methods Used in Wireless Network Access Authentication, September 2009.
[IEEE 802.1X]	IEEE 802.1X-2004, “Standard for Local and metropolitan area networks, Port-Based Network Access Control, 2004
RFC 4301	Security Architecture for the Internet Protocol
RFC 4303	IP Encapsulating Security Payload (ESP)
RFC 4106	The Use of Galois/Counter Mode (GCM) in IPsec Encapsulating Security Payload (ESP)

Table 1-2: 3eTI Document References

Reference	Document

Reference	Document
636 UG	3e Technologies International Inc., 636-series User's Guide

1.2 TOE References

TOE Identification: 3eTI 3e-636 Series Network Security Devices

The TOE consists of the following 636 Series product:

- 3e-636L3 Network Security Device; Hardware Version 1.0, Firmware Version 5.1 build 73
- 3e-636L2 High Speed Encryption Network Security Device, Hardware Version 1.0, Firmware Version 5.1 build 62

1.3 TOE Overview

1.3.1 Type of TOE

The Target of Evaluation [TOE] is a Network Device as defined by the protection profile: "*A network device is a device composed of hardware and software that is connected to the network and has an infrastructure role in the overall enterprise".*

1.3.2 TOE Usage

3eTI's 636 Network Security Devices offer the multiple capabilities necessary for protecting embedded devices and safety-critical industrial control systems (ICS) against attacks from internal and external attacks.

The 3e-636 Series Network Security Devices share the identical hardware platform. Both devices provide the same functionalities of access control, traffic filter and data packet inspection for network data traffic between the private networks. GUI Management interfaces over TLS/HTTPS share many similarities with minor differences in the encryption configuration options.

1.3.3 Hardware, Firmware, and Software Required by the TOE

The TOE consists on the hardware, firmware and software residing on the Network Security Device as listed in Section 1.2 above.

The evaluated configuration of the TOE requires the following Operational Environment support which is not included in the TOE's physical boundary.

- **Administrator Workstations:** Trusted administrators access the TOE through the TLS/HTTPS protocol.
- **Audit Servers:** The TOE relies upon the audit server for storage of audit records. The TOE itself stores limited amount of the audit records in its internal persistence storage. Those audit records are accessible and exportable through the Web GUI interface.
- **NTP Servers (Optional):** The TOE relies upon an NTP server to provide reliable time**.** If the time is configured locally, the TOE will use its own reliable hardware clock to maintain time as well.

1.3.4 TOE Security Functionality

The following security functionality is within scope of this NDPP evaluation.

- Security Audit
  - Generate audit logs for security-relevant events
  - Supports secure communications to remote syslog servers
- Cryptography
  - Validated cryptographic algorithms
  - Data zeroization
- User Data Protection
  - Residual information clearing
- Identification and Authentication
  - Password and user access policies
- Security Management
  - Local and remote administration
- Protection of the security functionality
  - Self-test on power-up
  - Trusted update
- TOE Access
  - Role-based access control
  - Session timeout and lockout
- Trusted Path/Channels
  - Trusted path for remote administrators

.

Evaluation Clarification: The TOE provides additional security features, such as IPSec to provide transport layer security as VPN Client, which may be briefly described in this ST to help the reader understand what the product does. However, as this evaluation is strict compliance to the Network Device Protection Profile these additional features are considered out of scope.

1.4 TOE Description

1.4.1 Acronyms

The following acronyms and abbreviations are used in this Security Target:

Table 1-3: Acronyms

Acronym	Definition
AES	Advanced Encryption Standard
AS	Authentication Server
CA	Certificate Authority
CAVP	Cryptographic Algorithm Validation Program
CBC	Cipher Block Chaining (AES mode)
CC	Common Criteria for Information Technology Security Evaluation
CCM	Counter with Cipher Block Chaining-Message Authentication Code (AES mode)
CCTL	Common Criteria Testing Laboratory
CEM	Common Evaluation Methodology for Information Technology Security
CM	Configuration Management
CMVP	Cryptographic Module Validation Program
COTS	Commercial Off-The-Shelf
CPD	Certificate Path Development
CPU	Central Processing Unit
CPV	Certificate Path Validation
CRL	Certificate Revocation List
CSP	Critical Security Parameter
DN	Distinguished Name
DSA	Digital Signature Algorithm
DSS	Digital Signature Standard
EAL	Evaluation Assurance Level
ECCCDH	Elliptic Curve Cryptography Cofactor Diffie-Hellman
ECDSA	Elliptic Curve Digital Signature Algorithm
ECB	Electronic Codebook (AES Mode)
EE PROM	Electrically Erasable Programmable Read-Only Memory
FIPS	Federal Information Processing Standard
GUI	Graphic User Interface
HLD	High Level Design
HMAC	Hashed Message Authentication Code
HTTPS	Secure Hypertext Transfer Protocol
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IP	Internet Protocol
IT	Information Technology
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
MAC	Media Access Control
Mbps	Megabits per second
NIAP	National Information Assurance Partnership
NIC	Network Interface Card
NIST	National Institute of Standards and Technology
OCSP	Online Certificate Status Protocol

Acronym	Definition
OS	Operating System
PKI	Public Key Infrastructure
PP	Protection Profile
PSK	Pre-shared key
PSP	Public Security Parameter
RADIUS	Remote Authentication Dial-In User Service
RFC	Request for Comments
RSA	Rivest, Shamir, and Adleman
SAR	Security Assurance Requirement
SDRAM	Synchronous Dynamic Random Access Memory
SFP	Security Function Policy
SFR	Security Functional Requirement
SHA-1	US Secure Hash Algorithm 1
SNMP	Simple Network Management Protocol
SOF	Strength of Function
SP	Security Parameter
ST	Security Target
TCP	Transmission Control Protocol
TK	Temporal Key
TLS	Transport Layer Security
TOE	Target of Evaluation
TOI	Time of Interest (used in certificate processing)
TSF	TOE Security Function
TSP	TOE Security Policy
UDP	User Datagram Protocol
VLAN	Virtual Local Area Network
WAN	Wide Area Network

1.4.2 Terminology

The following terminology is used in the Security Target:

Table 1-4: Terms

Term	Definition
802.1X	The IEEE 802.1X standard provides a framework for many authentication types at the link layer.
IPsec	Internet Protocol Security (IPsec) is a protocol suite for securing Internet Protocol (IP) communications by authenticating and encrypting each IP packet of a communication session. IPsec includes protocols for establishing mutual authentication between agents at the beginning of the session and negotiation of cryptographic keys to be used during the session.
Cryptographic Module	The set of hardware, software, firmware, or some combination thereof that implements cryptographic logic or processes, including cryptographic algorithms, and is contained within the cryptographic boundary of the module.

1.4.3 TOE Description

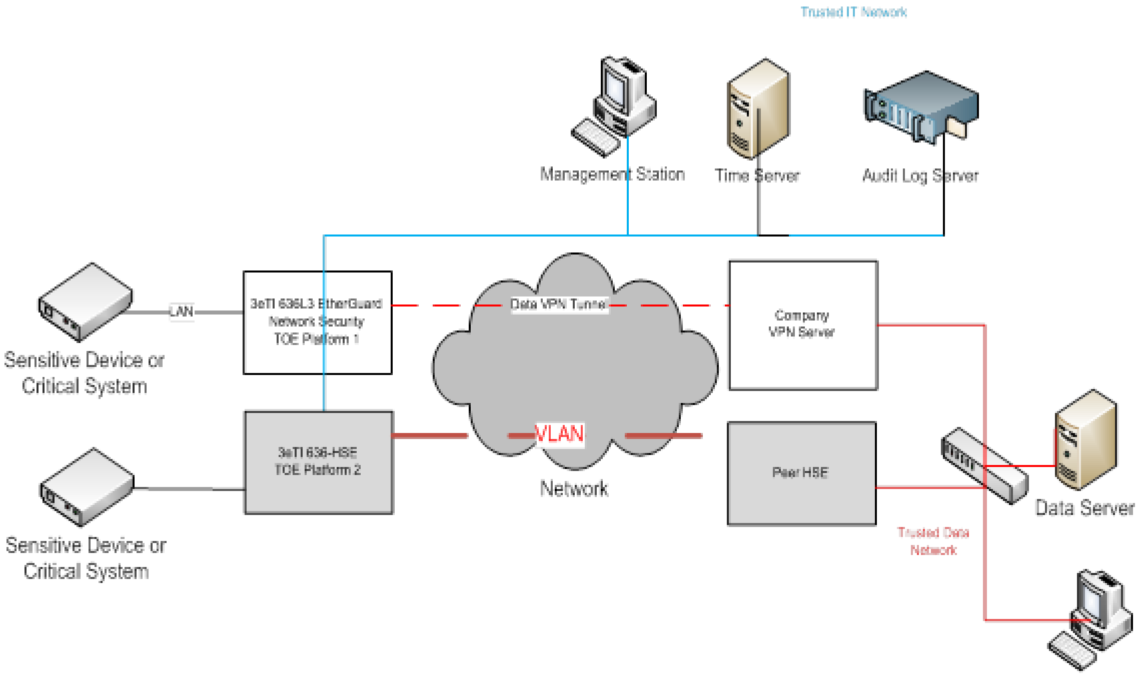
The Target of Evaluation (TOE) is network devices that provide high speed information assurance that combines a number of different capabilities to create a tailored cyber defense.

Acting as an IPsec client, the 3e-636L3 authenticates the IPsec Gateway during IKEv2 negotiation. It provides further data integrity and confidentiality using the ESP mode of the IPsec. AES with 128/256 bits key is used for network data encryption while SHS, CCM or GCM is used for data integrity.

The 3e-636L2 provides high speed IEEE802.3 MAC layer encryption. All 3e-636-HSE devices can communicate securely on the same VLAN using the symmetric encryption key. Data integrity is offered through HMAC-SHS or CCM mode of encryption.

Figure 1-1 depicts a normal operational scenario with the TOE. The 3e-636L3 uses IPSec tunnel while 3e-636L2 operates with symmetric encryption on the VLAN. The TOE relies upon an NTP Server and an Audit Server in its Operational Environment.   The TOE may also be configured to communicate with DHCP and SNMP Management Servers in the Operational Environment, but does not depend upon them to support its security functionality.

Figure 1-1: 3e-636L3/3e-636L2TOE Operational Configuration


Trusted IT Network
Management Station
Time Server
Audit Log Server
Sensitive Device or Critical System
LAN
3eTI 636L3 EtherGuard Network Security TOE Platform 1
Data VPN Tunnel
Company VPN Server
3eTI 636-HSE TOE Platform 2
VLAN
Network
Peer HSE
Data Server
Trusted Data Network
Sensitive Device or Critical System

Evaluation Clarification: The TOE components use IPSec to provide transport layer security as VPN Client. While the TOE meets (vendor assertion) the FCS_IPSEC_EXT.1 SFR, the NDPP states "The intent of the above requirement is to use a cryptographic protocol to protect external communications with authorized IT entities that the TOE interacts with to perform its functions. This is not, however, to be used to specify VPN Gateway functionality; a separate VPN Protection Profile should be used in these instances." Therefore, the VPN IPSec feature is not evaluated.

Similarly, the TOE uses encrypted VLAN payload to offer data link layer security, the VLAN feature is not evaluated under the NDPP either.

1.4.4 Physical Scope of the TOE

The TOE physical boundary defines all hardware and firmware that is required to support the TOE's logical boundary and the TOE's security functions. The TOE hardware platform uses FreeScale MPC8378E CPU and the TOE's firmware contains embedded Linux Kernel customized by 3eTI based on kernel version 2.6. In short, the TOE's physical boundary is the physical device/appliance for both models.

Figure 1-1 in Section 1.4.3 depicts the evaluated TOE configurations and the Operational Environment. The table below describes the ports and interfaces implemented by the TOE

Port/Interfaces	Management/Control I/O	Data Input	Data Output	Status Output	Same on 3e-636L3 and 3e-636L2
Local Management Ethernet port (1)	X				Yes
Plain text Ethernet port (1)	X	X	X		Yes
Cipher text Ethernet port (1)	X	X	X		Yes
Auxiliary Ethernet port (1)	N/A	N/A	N/A		Disabled on both devices
Power					Yes
LED				X	Yes
Reset Pin	X				Yes

The Operational Environment components relied upon by the TOE and not included in the physical boundary are described in Section 1.3.3

1.4.5 Logical Scope of the TOE

The Logical Scope of the TOE includes Audit, Cryptographic Services, User Data Protection, Identification and Authentication, Management, Protection of the TSF, TOE Access security functionality and Trusted Path/Channels.

1.4.5.1 Audit

The TOE generates auditable events for actions on the TOE with the capability of selective audit record generation. The records of these events can be viewed within the TOE Management Interface or they can be exported to audit systems in the Operational Environment. The TOE generates records for its own actions, containing information about the user/process associated with the event, the success or failure of the event, and the time that the event occurred. Additionally, all administrator actions relating to the management of TSF data and configuration data are logged by the TOE's audit generation functionality.

1.4.5.2 Cryptographic Services

The TOE uses a random number generator and secures communication channels with the following cryptographic algorithms: AES, RSA, ECDSA, SHA, HMAC. The TOE is designed to zeroize Critical Security Parameters (CSPs) to mitigate the possibility of disclosure or modification.

1.4.5.3 User Data Protection

The TSF ensures that network packets sent from the TOE do not include data "left over" from processing the previous network information.

1.4.5.4 Identification and Authentication

The TOE provides Identification and Authentication security functionality to ensure that all users are properly identified and authenticated before accessing TOE functionality The TOE enforces a local password-based authentication mechanism to perform administrative user authentication. Passwords are obscured when being displayed during any attempted login.

1.4.5.5 Management

The Web Management Application of the TOE provides the capabilities for configuration and administration. The Web Management Application can be accessed via the dedicated local Ethernet port configured for "out-of-band" management. There is no local access such as a serial console port. Therefore, the local and remote management is considered the same for this evaluation.

An authorized administrator has the ability to modify, edit, and delete security parameters such as audit data, configuration data, and user authentication data. The Web Management Application also offers an authorized administrator the capability to manage how security functions behave. For example an administrator can enable/disable certain audit functions query and set encryption/decryption algorithms used for network packets.

1.4.5.6 Protection of the TSF

Internal testing of the TOE hardware, software, and software updates against tampering ensures that all security functions are running and available before the TOE accepting any communications. The TSF prevents reading of pre-shared keys, symmetric keys, and private keys, and passwords. The TOE uses electronic signature verification before any firmware/software updates are installed.

1.4.5.7 TOE Access

The TOE provides the following TOE Access functionality:

- TSF-initiated session termination when a connection (remote or local) is idle for a configurable time period
- Administrative termination of own session
- TOE Access Banners

1.4.5.8 Trusted Path/Channels

The TOE protects interactive communication with administrators using TLS/HTTPS, both integrity and disclosure protection is ensured.

The TOE protects communication with network entities, such as a log server, using TLS connection and optionally using a dedicated physical port to prevent unintended disclosure or modification of logs and management information.

1.4.5.9 Logical Dependencies on the Operational Environment

The TOE relies upon the Operational Environment for the following security functionality:

- Audit storage
- Reliable time stamps from a Network Time Protocol (NTP) server

2 Conformance Claims

2.1 Common Criteria Conformance

This ST claims conformance to Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 3, July 2009. International Standard – ISO/IEC 15408.

The requirements in this Security Target are Part 2 extended, and Part 3 conformant.

2.2 Protection Profile Claim

This ST claims Strict Compliance to the ***US Government Protection Profile for Network Devices, Version 1.1, 8 June 2012*** with Errata 3

2.3 Conformance Rationale

This security target claims strict conformance to only one Protection Profile [PP] – NDPP.

The security problem definition of this ST is consistent with the statement of the security problem definition in the PP, as the ST claims *exact* conformance to the PP and no other threats, organizational security policies, or assumptions are added.

The security objectives of this ST are consistent with the statement of the security objectives in the PP as the ST claims *exact* conformance to the PP and no other security objectives are added.

The security requirements of this ST are consistent with the statement of the security requirements in the PP as the ST claims *exact* conformance to the PP.

3 Security Problem Definition

The Security Problem Definition defines:

a) Communications with the TOE

b) Malicious “Updates”

c) Undetected System Activity

d) Accessing the TOE

e) User Data Disclosure

f) TSF Failure

This document identifies threats are identified as T.threat with “threat” specifying a unique name. Policies are identified as P.policy with “policy” specifying a unique name. Assumptions are identified as A.assumption with “assumption” specifying a unique name.

3.1 Threats to Security

Table 3-1 below lists the threats to security.

Table 3-1: Threats to Security

#	Threat Name	Threat Definition
1	T.UNAUTHORIZED_ACCESS	A user may gain unauthorized access to the TOE data and TOE executable code. A malicious user, process, or external IT entity may masquerade as an authorized entity in order to gain unauthorized access to data or TOE resources. A malicious user, process, or external IT entity may misrepresent itself as the TOE to obtain identification and authentication data.
2	T.UNAUTHORIZED_UPDATE	A malicious party attempts to supply the end user with an update to the product that may compromise the security features of the TOE.
3	T.ADMIN_ERROR	An administrator may unintentionally install or configure the TOE incorrectly, resulting in ineffective security mechanisms.
4	T.UNDETECTED_ACTIONS	Malicious remote users or external IT entities may take actions that adversely affect the security of the TOE. These actions may remain undetected and thus their effects cannot be effectively mitigated.
5	T.USER_DATA_REUSE	User data may be inadvertently sent to a destination not intended by the original sender.
6	T.TSF_FAILURE	Security mechanisms of the TOE may fail, leading to a compromise of the TSF.

3.2 Organization Security Policies

An organizational security policy is a set of rules, practices, and procedures imposed by an organization to address its security needs. Table 3-2 below lists the Organizational Security Policies enforced by the TOE.

Table 3-2: Organizational Security Policies

#	Policy Name	Policy Definition
7	P.ACCESS_BANNER	The TOE shall display an initial banner describing restrictions of use, legal agreements, or any other appropriate information to which users consent by accessing the TOE.

3.3 Secure Usage Assumptions

Table 3-3 below lists the secure usage assumptions.

Table 3-3: Secure Usage Assumptions

#	Assumption Name	Assumption Definition
1	A.NO_GENERAL_PURPOSE	It is assumed that there are no general-purpose computing capabilities (e.g., compilers or user applications) available on the TOE, other than those services necessary for the operation, administration and support of the TOE.
2	A.PHYSICAL	Physical security, commensurate with the value of the TOE and the data it contains, is assumed to be provided by the environment.
3	A.TRUSTED_ADMIN	TOE Administrators are trusted to follow and apply all administrator guidance in a trusted manner.

4 Security Objectives

This section defines TOE security objectives and objectives for the Operational Environment.

4.1 Security Objectives for the TOE

Table 4-1 below lists the Security Objectives for the TOE.

Table 4-1: Security Objectives

#	TOE Security Objective	TOE Security Objective Definition
1	O.PROTECTED_COMMUNICATIONS	The TOE will provide protected communication channels for administrators, other parts of a distributed TOE, and authorized IT entities.
2	O.DISPLAY_BANNER	The TOE will display an advisory warning regarding use of the TOE.
3	O.SESSION_LOCK	The TOE shall provide mechanisms that mitigate the risk of unattended sessions being hijacked.
4	O.RESIDUAL_INFORMATION_CLEARING	The TOE will ensure that any data contained in a protected resource is not available when the resource is reallocated.
5	O.TOE_ADMINISTRATION	The TOE will provide mechanisms to ensure that only administrators are able to log in and configure the TOE, and provide protections for logged-in administrators.
6	O.TSF_SELF_TEST	The TOE will provide the capability to test some subset of its security functionality to ensure it is operating properly.
7	O.VERIFIABLE_UPDATES	The TOE will provide the capability to help ensure that any updates to the TOE can be verified by the administrator to be unaltered and (optionally) from a trusted source.
8	O.SYSTEM_MONITORING	The TOE will provide the capability to generate audit data and send those data to an external IT entity.

4.2 Security Objectives for the Operational Environment

Table 4-2 below lists the Security Objectives for the Operational Environment.

Table 4-2: Security Objectives for the Operational Environment

#	TOE Security Objective	TOE Security Objective Definition
1	OE.NO_GENERAL_PURPOSE	There are no general-purpose computing capabilities (e.g., compilers or user applications) available on the TOE, other than those services necessary for the operation, administration and support of the TOE.
2	OE.PHYSICAL	Physical security, commensurate with the value of the TOE and the data it contains, is provided by the environment.
3	OE.TRUSTED_ADMIN	TOE Administrators are trusted to follow and apply all administrator guidance in a trusted manner.

5 Extended Security Requirements Definition

All of the extended requirements in this ST have been drawn from the NDPP. The NDPP defines the following extended SFRs and since they are not redefined in this ST, the NDPP should be consulted for more information in regard to those CC extensions.

5.1 Network Device Protection Profile Extended Security Requirements Definition

- FAU_STG_EXT.1 Extended: External Audit Trail Storage
- FCS_CKM_EXT.4 Extended: Cryptographic Key Zeroization
- FCS_RBG_EXT.1 Extended: Cryptographic Operation (Random Bit Generation)
- FCS_TLS_EXT.1 Extended: TLS
- FCS_HTTPS_EXT.1 Extended: HTTPS
- FIA_PMG_EXT.1 Extended: Password Management
- FIA_UAU_EXT.2 Extended: Password-based Authentication Mechanism
- FIA_UIA_EXT.1 Extended: User Identification and Authentication
- FPT_APW_EXT.1 Extended: Protection of Administrator Passwords
- FPT_SKP_EXT.1 Extended: Protection of TSF Data (for reading of all symmetric keys)
- FPT_TST_EXT.1 Extended: TSF Testing
- FPT_TUD_EXT.1 Extended: Trusted Update
- FTA_SSL_EXT.1 Extended: TSF-initiated Session Locking

***NOTE**: The PP authors were not consistent in following their own conventions. Several of the Extended SFR naming conventions had the "Extended: "missing from its title. The ST author fixed this error to be consistent within this ST. The fixes are shown in red and are only shown in this section.*

The FCS_TLS_EXT.1 used the word "Explicitly" instead of "Extended". This has been fixed to be consistent within this ST.

The FCS_HTTPS_EXT.1 used the word "Explicitly" instead of "Extended". This has been fixed to be consistent within this ST.

6 Security Requirements

The following conventions have been applied in this document:

- **Security Functional Requirements:** Part 2 of the CC defines the approved set of operations that may be applied to functional requirements: iteration, assignment, selection, and refinement.
- **Extended Security Functional Requirements**: Extended requirements were written by the PP author when Part 2 of the CC did not offer suitable requirements to meet the authors' needs. Extended requirements will be indicated with the "_EXT" inserted within the component name (e.g., FAU_STG_EXT.1)
- **Iteration**: allows a component to be used more than once with varying operations. In the ST, iteration is indicated by a reference in parenthesis placed at the end of the component. For example FCS_COP.1 (1) and FCS_COP.1 (2) indicate that the ST includes two iterations of the FCS_COP.1 requirement, (1) and (2).
- **ST Author Assignment**: allows the specification of an identified parameter. Assignments made by the ST author are indicated using italic+bold text and are surrounded by brackets (e.g., [***assignment***]).
- **ST Author Selection**: allows the specification of one or more elements from a list. Selections made by the ST author are indicated using bold text and are surrounded by brackets (e.g., [**selection**]).
- **ST Author Refinement**: The refinement operation is used to add detail to a requirement, and thus further restricts a requirement. Refinement of security requirements made by the ST author is denoted by the word "Refinement" in bold text after the element number and the additional text in the requirement in bold text.
- **PP Author Selections, Assignments, & Refinements:** PP author selections and assignments are shown in normal text. Refinements made by the PP authors will not be identified as refinements in this ST. The "Refinement" identifier is reserved for identifying any refinements made by the ST author.

6.1 TOE Security Functional Requirements

The following table describes the SFRs that are satisfied by 3eTI's 636 series Network Device.

Table 6-1: 636 Security Functional Requirements

Functional Class	Functional Components		#
Security Audit (FAU)	FAU_GEN.1	Audit Data Generation	1
	FAU_GEN.2	User Identity Association	2
	FAU_STG_EXT.1	Extended: External Audit Trail Storage	3
Cryptographic Support (FCS)	FCS_CKM.1	Cryptographic Key Generation (for asymmetric keys)	4
	FCS_CKM_EXT.4	Extended: Cryptographic Key Zeroization	5
	FCS_COP.1 (1)	Cryptographic Operation (for data encryption/decryption)	6
	FCS_COP.1 (2)	Cryptographic Operation (for cryptographic signature)	7

Functional Class	Functional Components		#
	FCS_COP.1 (3)	Cryptographic Operation (for cryptographic hashing)	8
	FCS_COP.1 (4)	Cryptographic Operation (for keyed-hash message authentication)	9
	FCS_TLS_EXT.1	Extended: TLS	10
	FCS_HTTPS_EXT.1	Extended: HTTPS	11
	FCS_RBG_EXT.1	Extended: Cryptographic Operation (Random Bit Generation)	12
User Data Protection (FDP)	FDP_RIP.2	Full Residual Information Protection	13
Identification and Authentication (FIA)	FIA_PMG_EXT.1	Extended: Password Management	14
	FIA_UIA_EXT.1	Extended: User Identification and Authentication	15
	FIA_UAU.7	Protected Authentication Feedback	16
	FIA_UAU_EXT.2	Extended: Password-based Authentication Mechanism	17
Security Management (FMT)	FMT_MTD.1	Management of TSF Data (for general TSF data)	18
	FMT_SMF.1	Specification of Management Functions	19
	FMT_SMR.2	Restrictions on Security Roles	20
Protection of TSF (FPT)	FPT_SKP_EXT.1	Extended: Protection of TSF Data (for reading of all symmetric keys)	21
	FPT_APW_EXT.1	Extended: Protection of Administrator Passwords	22
	FPT_STM.1	Reliable Time Stamps	23
	FPT_TUD_EXT.1	Extended: Trusted Update	24
	FPT_TST_EXT.1	Extended: TSF Testing	25
TOE Access (FTA)	FTA_SSL.3	TSF-initiated Termination	26
	FTA_SSL.4	User-initiated Termination	27
	FTA_SSL_EXT.1	Extended: TSF-initiated Session Locking	28
	FTA_TAB.1	Default TOE Access Banners	29
Trusted Path/Channels (FTP)	FTP_ITC.1	Inter-TSF trusted channel	30
	FTP_TRP.1	Trusted Path	31

6.1.1 Security Audit (FAU) Requirements

6.1.1.1 FAU_GEN.1 Audit Data Generation

FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events:

a) Start-up and shut-down of the audit functions;

b) All auditable events for the not specified level of audit; and

c) All administrative actions;

d) Specifically defined auditable events listed in Table 6-2.

Table 6-2: Auditable Events

#	Requirement	Auditable Events	Additional Audit Record Contents
1	FAU_GEN.1	None	N/A
2	FAU_GEN.2	None	N/A
3	FAU_STG_EXT.1	None	N/A
4	FCS_CKM.1	None	N/A
5	FCS_CKM_EXT.4	None	N/A
6	FCS_COP.1 (1)	None	N/A
7	FCS_COP.1 (2)	None	N/A
8	FCS_COP.1 (3)	None	N/A
9	FCS_COP.1 (4)	None	N/A
10	FCS_RBG_EXT.1	None	N/A
11	FCS_TLS_EXT.1	Failure to establish a TLS Session Establishment/Termination of a TLS session	Reason for failure. Non-TOE endpoint of connection (IP address)
12	FCS_HTTPS_EXT.1	Failure to establish a TLS Session Establishment/Termination of a TLS session	Reason for failure. Non-TOE endpoint of connection (IP address)
13	FDP_RIP.2	None	N/A
14	FIA_PMG_EXT.1	None	N/A
15	FIA_UIA_EXT.1	All use of the identification and authentication mechanism	Provided user identity, origin of the attempt (e.g., IP address)
16	FIA_UAU_EXT.2	All use of the authentication mechanism	Origin of the attempt (e.g., IP address)
17	FIA_UAU.7	None	N/A
18	FMT_MTD.1	None	N/A
19	FMT_SMF.1	None	N/A
20	FMT_SMR.2	None	N/A
21	FPT_SKP_EXT.1	None	N/A
22	FPT_APW_EXT.1	None	N/A
23	FPT_STM.1	Changes to the time	The old and new values for the time. Origin of the attempt (e.g., IP address).
24	FPT_TUD_EXT.1	Initiation of the update. Any failure to verify the integrity of the update.	No additional information
25	FPT_TST_EXT.1	None	N/A
26	FTA_SSL_EXT.1	Any attempts at unlocking of an interactive session.	No additional information
27	FTA_SSL.3	The termination of a remote session by the session locking mechanism	No additional information
28	FTA_SSL.4	The termination of an interactive session	No additional information
29	FTA_TAB.1	None	N/A

#	Requirement	Auditable Events	Additional Audit Record Contents
30	FTP_TRP.1	Initiation of a trusted channel. Termination of the trusted channel. Failure of the trusted channel functions	Identification of the claimed user identity
31	FTP_ITC.1	Initiation of the trusted channel. Termination of the trusted channel. Failure of the trusted channel functions.	Identification of the initiator and target of failed trusted channels establishment attempt

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:

a) Date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event; and

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, information specified in column three of Table 6-2.

6.1.1.2 FAU_GEN.2 User Identity Association

FAU_GEN.2.1 For audit events resulting from actions of identified users, the TSF shall be able to associate each auditable event with the identity of the user that caused the event.

6.1.1.3 FAU_STG_EXT.1 Extended: External Audit Trail Storage

FAU_STG_EXT.1.1 The TSF shall be able to [**transmit the generated audit data to an external IT entity**] using a trusted channel implementing the [**TLS**] protocol.

6.1.2 Cryptographic Support (FCS) Requirements

6.1.2.1 FCS_CKM.1 Cryptographic Key Generation (for asymmetric keys)

FCS_CKM.1.1 The TSF shall generate asymmetric cryptographic keys used for key establishment in accordance with [

- **NIST Special Publication 800-56A, "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography" for elliptic curve-based key establishment schemes and implementing "NIST curves" P-256, P-384 and** [**P-521**] **(as defined in FIPS PUB 186-3, "Digital Signature Standard")**
- **NIST Special Publication 800-56B, "Recommendation for Pair-Wise Key Establishment Schemes Using Integer Factorization Cryptography" for RSA-based key establishment schemes**

]

and specified cryptographic key sizes equivalent to, or greater than, a symmetric key strength of 112 bits.

6.1.2.2 FCS_CKM_EXT.4 Extended: Cryptographic Key Zeroization

FCS_CKM_EXT.4.1 The TOE shall zeroize all plaintext secret and private cryptographic keys and CSPs when no longer required.

6.1.2.3 FCS_COP.1 (1) Cryptographic Operation (for data encryption/decryption)

FCS_COP.1.1 (1) The TSF shall perform encryption and decryption in accordance with a specified cryptographic algorithm AES operating in [**CBC,** [***and ECB mode***]] and cryptographic key sizes 128-bits and 256-bits that meets the following:

- FIPS PUB 197, “Advanced Encryption Standard (AES)”
- [**NIST SP 800-38A**].

6.1.2.4 FCS_COP.1 (2) Cryptographic Operation (for cryptographic signature)

FCS_COP.1.1 (2) The TSF shall perform cryptographic signature services in accordance with a

[

- **RSA Digital Signature Algorithm (rDSA) with a key size (modulus) of 2048 bits or greater**
- **Elliptic Curve Digital Signature Algorithm (ECDSA) with a key size of 256 bits or greater**

]

that meets the following:

Case: **RSA Digital Signature Algorithm**

- FIPS PUB 186-2 or FIPS PUB 186-3, “Digital Signature Standard”.

Case: Elliptic Curve Digital Signature Algorithm

- FIPS PUB 186-3, “Digital Signature Standard”
- The TSF shall implement “NIST curves” P-256, P-384 and [**P-521**] (as defined in FIPS PUB 186-3, “Digital Signature Standard”).

6.1.2.5 FCS_COP.1 (3) Cryptographic Operation (for cryptographic hashing)

FCS_COP.1.1 (3) **Refinement:** The TSF shall perform cryptographic hashing services in accordance with a specified cryptographic algorithm [**SHA-1, SHA-224, SHA-256, SHA-384, SHA-512**] and message digest sizes [**160, 224, 256, 384, 512**] bits that meet the following: FIPS PUB 180-**4**, “Secure Hash Standard”.

Application Note: *The PP calls out for FIPS PUB 180-3. Since the time of the approved PP FIPS PUB 180-4 has been approved and supersedes 180-3. Therefore, the vendor is claiming the latest standard.*

6.1.2.6 FCS_COP.1 (4) Cryptographic Operation (for keyed-hash message authentication)

FCS_COP.1.1 (4) **Refinement:** The TSF shall perform keyed-hash message authentication in accordance with a specified cryptographic algorithm HMAC- [**SHA-1, SHA-224, SHA-256, SHA-384, SHA-512**], key size [***160 bits***], and message digest sizes [**160, 224, 256, 384, 512**] bits that meet the following: FIPS PUB 198-1, "The Keyed-Hash Message Authentication Code", and FIPS PUB 180-**4**, "Secure Hash Standard".

Application Note: *The PP calls out for FIPS PUB 180-3. Since the time of the approved PP FIPS PUB 180-4 has been approved and supersedes 180-3. Therefore, the vendor is claiming the latest standard.*

6.1.2.7 FCS_RBG_EXT.1 Extended: Cryptographic Operation (Random Bit Generation)

FCS_RBG_EXT.1.1 The TSF shall perform all random bit generation (RBG) services in accordance with [**FIPS PUB 140-2 Annex C: X9.31 Appendix 2.4 using AES**] seeded by an entropy source that accumulated entropy from [**a TSF-hardware-based noise source**].

FCS_RBG_EXT.1.2 The deterministic RBG shall be seeded with a minimum of [**128 bits**] of entropy at least equal to the greatest security strength of the keys and hashes that it will generate.

6.1.2.8 FCS_TLS_EXT.1 Extended: TLS

FCS_TLS_EXT.1.1 The TSF shall implement one or more of the following protocols [**TLS 1.0 (RFC 2246), TLS 1.1 (RFC 4346), TLS 1.2 (RFC 5246)**] supporting the following ciphersuites:

Mandatory Ciphersuites:
TLS_RSA_WITH_AES_128_CBC_SHA

Optional Ciphersuites:
[
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA
TLS_DHE_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA256
TLS_RSA_WITH_AES_256_CBC_SHA256
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
].

6.1.2.9 FCS_HTTPS_EXT.1 Extended: HTTPS

FCS_HTTPS_EXT.1.1 The TSF shall implement the HTTPS protocol that complies with RFC 2818.

FCS_HTTPS_EXT.1.2 The TSF shall implement HTTPS using TLS as specified in FCS_TLS_EXT.1.

6.1.3 User Data Protection (FDP) Requirements

6.1.3.1 FDP_RIP.2 Full Residual Information Protection

FDP_RIP.2.1 The TSF shall ensure that any previous information content of a resource is made unavailable upon the [**allocation of the resource to**] all objects.

6.1.4 Identification and Authentication (FIA) Requirements

6.1.4.1 FIA_PMG_EXT.1 Extended: Password Management

FIA_PMG_EXT.1.1 The TSF shall provide the following password management capabilities for administrative passwords:

1. Passwords shall be able to be composed of any combination of upper and lower case letters, numbers, and the following special characters: **[“!”, “@”, “#”, “$”, “%”, “^”, “&”, “*”, “(“, “)”**, [***“+”, “-“, “_”***]];
2. Minimum password length shall settable by the Security Administrator, and support passwords of 15 characters or greater;

6.1.4.2 FIA_UIA_EXT.1 Extended: User Identification and Authentication

FIA_UIA_EXT.1.1 The TSF shall allow the following actions prior to requiring the non-TOE entity to initiate the identification and authentication process:

- Display the warning banner in accordance with FTA_TAB.1;
- [[***no other actions***]]

FIA_UIA_EXT.1.2 The TSF shall require each administrative user to be successfully identified and authenticated before allowing any other TSF-mediated actions on behalf of that administrative user.

6.1.4.3 FIA_UAU_EXT.2 Extended: Password-based Authentication Mechanism

FIA_UAU_EXT.2.1 The TSF shall provide a local password-based authentication mechanism, [**none**] to perform administrative user authentication.

6.1.4.4 FIA_UAU.7 Protected Authentication Feedback

FIA_UAU.7.1 The TSF shall provide only obscured feedback to the administrative user while the authentication is in progress at the local console.

6.1.5 Security Management (FMT) Requirements

6.1.5.1 FMT_MTD.1 Management of TSF Data (for general TSF data)

FMT_MTD.1.1 The TSF shall restrict the ability to manage the TSF data to the Security Administrators.

6.1.5.2 FMT_SMF.1 Specification of Management Functions

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions:

- Ability to administer the TOE locally and remotely;
- Ability to update the TOE, and to verify the updates using [**digital signature**] capability prior to installing those updates;
- **[Ability to configure the list of TOE-provided services available before an entity is identified and authenticated, as specified in FIA_UIA_EXT.1;**
- **Ability to configure the cryptographic functionality**]

6.1.5.3 FMT_SMR.2 Restrictions on Security Roles

FMT_SMR.2.1 The TSF shall maintain the roles:

- Authorized Administrator.

FMT_SMR.2.2 The TSF shall be able to associate users with roles.

FMT_SMR.2.3 The TSF shall ensure that the conditions:

- Authorized Administrator role shall be able to administer the TOE locally;
- Authorized Administrator role shall be able to administer the TOE remotely;

are satisfied.

6.1.6 Protection of TSF (FPT) Requirements

6.1.6.1 FPT_SKP_EXT.1 Extended: Protection of TSF Data (for reading of all symmetric keys)

FPT_SKP_EXT.1.1 The TSF shall prevent reading of all pre-shared keys, symmetric keys, and private keys.

6.1.6.2 FPT_APW_EXT.1 Extended: Protection of Administrator Passwords

FPT_APW_EXT.1.1 The TSF shall store passwords in non-plaintext form.

FPT_APW_EXT.1.2 The TSF shall prevent the reading of plaintext passwords.

6.1.6.3 FPT_STM.1 Reliable Time Stamps

FPT_STM.1.1 The TSF shall be able to provide reliable time stamps for its own use.

6.1.6.4 FPT_TUD_EXT.1 Extended: Trusted Update

FPT_TUD_EXT.1.1 The TSF shall provide security administrators the ability to query the current version of the TOE firmware/software.

FPT_TUD_EXT.1.2 The TSF shall provide security administrators the ability to initiate updates to TOE firmware/software.

FPT_TUD_EXT.1.3 The TSF shall provide a means to verify firmware/software updates to the TOE using a [**digital signature mechanism**] prior to installing those updates.

6.1.6.5 FPT_TST_EXT.1 Extended: TSF Testing

FPT_TST_EXT.1.1 The TSF shall run a suite of self-tests during initial start-up (on power on) to demonstrate the correct operation of the TSF.

6.1.7 TOE Access (FTA) Requirements

6.1.7.1 FTA_SSL_EXT.1 Extended: TSF-initiated Session Locking

FTA_SSL_EXT.1.1 The TSF shall, for local interactive sessions, [

- **terminate the session**

]

after a Security Administrator-specified time period of inactivity.

6.1.7.2 FTA_SSL.3 TSF-initiated Termination

FTA_SSL.3.1 The TSF shall terminate a remote interactive session after a Security Administrator-configurable time interval of session inactivity.

6.1.7.3 FTA_SSL.4 User-initiated Termination

FTA_SSL.4.1 The TSF shall allow Administrator-initiated termination of the Administrator's own interactive session.

6.1.7.4 FTA_TAB.1 Default TOE Access Banners

FTA_TAB.1.1 Before establishing an administrative user session the TSF shall display a Security Administrator-specified advisory notice and consent warning message regarding use of the TOE.

6.1.8 Trusted Path/Channels (FTP) Requirements

6.1.8.1 FTP_ITC.1 Inter-TSF Trusted Channel

FTP_ITC1.1 The TSF shall use [**TLS**] to provide a trusted communication channel between itself and authorized IT entities supporting the following capabilities: audit server, [***no other***] that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from disclosure and detection of modification of the channel data.

FTP_ITC.1.2 The TSF shall permit the TSF, or the authorized IT entities to initiate communication via the trusted channel.

FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for [***remote logging***]**.**

6.1.8.2 FTP_TRP.1 Trusted Path

FTP_TRP.1.1 The TSF shall use [**TLS/HTTPS**] provide a trusted communication path between itself and remote administrators that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from disclosure and detection of modification of the communicated data.
.

FTP_TRP.1.2 The TSF shall permit remote administrators to initiate communication via the trusted path.

FTP_TRP.1.3 The TSF shall require the use of the trusted path for initial administrator authentication and all remote administration actions.

6.2 TOE Security Assurance Requirements

The security assurance requirements for the TOE are the EAL 1 components as specified in Part 3 of the Common Criteria (with the exception of some name changes in accordance with the NDPP). Table 6-3 lists the assurance components.

Table 6-3: TOE Security Assurance Requirements

Assurance Class	Assurance Components
Development (ADV)	ADV_FSP.1 Basic Functional Specification
Guidance Documents (AGD)	AGD_OPE.1 Operational User Guidance
	AGD_PRE.1 Preparative Procedures
Life-cycle Support (ALC)	ALC_CMS.1 TOE CM coverage
	ALC_CMC.1 Labeling of the TOE
Tests (ATE)	ATE_IND.1 Independent testing – conformance
Vulnerability Assessment (AVA)	AVA_VAN.1 Vulnerability Survey

6.2.1 Development (ADV)

6.2.1.1 Basic Functional Specification (ADV_FSP.1)

ADV_FSP.1.1d The developer shall provide a functional specification.

ADV_FSP.1.2d The developer shall provide a tracing from the functional specification to the SFRs.

ADV_FSP.1.1c The functional specification shall describe the purpose and method of use for each SFR-enforcing and SFR-supporting TSFI.

ADV_FSP.1.2c The functional specification shall identify all parameters associated with each SFR-enforcing and SFR-supporting TSFI.

ADV_FSP.1.3c The functional specification shall provide rationale for the implicit categorization of interfaces as SFR-non-interfering.

ADV_FSP.1.4c The tracing shall demonstrate that the SFRs trace to TSFIs in the functional specification.

ADV_FSP.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADV_FSP.1.2e The evaluator shall determine that the functional specification is an accurate and complete instantiation of the SFRs.

6.2.2 Guidance documents (AGD)

6.2.2.1 Operational User Guidance (AGD_OPE.1)

AGD_OPE.1.1d The developer shall provide operational user guidance.

AGD_OPE.1.1c The operational user guidance shall describe, for each user role, the user-accessible functions and privileges that should be controlled in a secure processing environment, including appropriate warnings.

AGD_OPE.1.2c The operational user guidance shall describe, for each user role, how to use the available interfaces provided by the TOE in a secure manner.

AGD_OPE.1.3c The operational user guidance shall describe, for each user role, the available functions and interfaces, in particular all security parameters under the control of the user, indicating secure values as appropriate.

AGD_OPE.1.4c The operational user guidance shall, for each user role, clearly present each type of security-relevant event relative to the user-accessible functions that need to be performed, including changing the security characteristics of entities under the control of the TSF.

AGD_OPE.1.5c The operational user guidance shall identify all possible modes of operation of the TOE (including operation following failure or operational error), their consequences and implications for maintaining secure operation.

AGD_OPE.1.6c The operational user guidance shall, for each user role, describe the security measures to be followed in order to fulfill the security objectives for the operational environment as described in the ST.

AGD_OPE.1.7c The operational user guidance shall be clear and reasonable.

AGD_OPE.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

6.2.2.2 Preparative Procedures (AGD_PRE.1)

AGD_PRE.1.1d The developer shall provide the TOE including its preparative procedures.

AGD_PRE.1.1c The preparative procedures shall describe all the steps necessary for secure acceptance of the delivered TOE in accordance with the developer's delivery procedures.

AGD_PRE.1.2c The preparative procedures shall describe all the steps necessary for secure installation of the TOE and for the secure preparation of the operational environment in accordance with the security objectives for the operational environment as described in the ST.

AGD_PRE.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AGD_PRE.1.2e The evaluator shall apply the preparative procedures to confirm that the TOE can be prepared securely for operation.

6.2.3 Life-cycle Support (ALC)

6.2.3.1 Labeling of the TOE (ALC_CMC.1)

ALC_CMC.1.1d The developer shall provide the TOE and a reference for the TOE.

ALC_CMC.1.1c The TOE shall be labeled with its unique reference.

ALC_CMC.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

6.2.3.2 TOE CM coverage (ALC_CMS.1)

ALC_CMS.1.1d The developer shall provide a configuration list for the TOE.

ALC_CMS.1.1c The configuration list shall include the following: the TOE itself; and the evaluation evidence required by the SARs.

ALC_CMS.1.2c The configuration list shall uniquely identify the configuration items.

ALC_CMS.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

6.2.4 Tests (ATE)

6.2.4.1 Independent testing - conformance (ATE_IND.1)

ATE_IND.1.1d The developer shall provide the TOE for testing.

ATE_IND.1.1c The TOE shall be suitable for testing

ATE_IND.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ATE_IND.1.2e The evaluator shall test a subset of the TSF to confirm that the TSF operates as specified.

6.2.5 Vulnerability Assessment (AVA)

6.2.5.1 Vulnerability Survey (AVA_VAN.1)

AVA_VAN.1.1d The developer shall provide the TOE for testing..

AVA_VAN.1.1c The TOE shall be suitable for testing.

AVA_VAN.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AVA_VAN.1.2e The evaluator shall perform a search of public domain sources to identify potential vulnerabilities in the TOE.

AVA_VAN.1.3e The evaluator shall conduct penetration testing, based on the identified potential vulnerabilities, to determine that the TOE is resistant to attacks performed by an attacker possessing Basic attack potential.

NOTE*: There were inconsistencies in the assurance naming convention used in the PP. The Table 6-3 has been and section titles have been corrected to be consistent within this ST.*

7 TOE Summary Specification

This chapter identifies and describes the security functions implemented by the TOE. The Security Functions are summarized in Table 6-1.

7.1.1 Audit Functions

7.1.1.1 Audit Generation

FAU_GEN.1

The TOE is designed to be able to generate log records for a wide range of security relevant and other events as they occur. The events that can cause an audit record to be logged include starting and stopping the audit function, Security Administrator's configuration of CSPs and security functions as well as all of the events identified in Table 6-2: Auditable Events. The TOE generates records for several separate classes of events: authentication/access to the system, actions taken directly on the system by network clients, and management of security functions by authorized administrators.

All audit records include the date/time of the event, the identity associated with the event (such as the service, computer or user), the success/failure of the event and a definition of the event (by code or explanation).

7.1.1.2 Audit Identity Association

FAU_GEN.2

All actions performed by the TOE are associated with a unique identifier, this information is maintained in the audit record, allowing the events stored there to be traced directly to the user or system for which they were performed.

7.1.1.3 External Audit Trail Storage

FAU_STG_EXT.1, FCS_TLS_EXT.1

The TOE stores audit logs locally with up to a fixed size of 256K bytes. The Security Administrator can configure the TOE to send email alert upon the audit logs reaching a configurable percentage of the fixed size.

Local password based authentication and authorization limits the access to the local audit log records. Only the Security Administrator can gain access to the local audit log records and those records are delivered confidentially over TLS encryption.

When the TOE is configured to export audit logs to an external SYSLOG server, it simultaneously sends the message to the server and local store. The TOE requires the external audit server and itself to be connected via a TLS session. The User's Guide provides details about the "Export Audit Logs" configuration.

The TOE exports audit data over TLS using AES128/256 bit encryption.

NOTE: If the TLS connection terminates unexpectedly the syslog audit will fail to update and the TOE will default to local storage. The TOE does not implement an automatic synchronization mechanism between the local and remote audit storage.

7.1.2 Cryptographic Support Functions

There are two cryptographic engines within the device, thus within the TOE. First is the 3eTI's own OpenSSL library. 3eTI's OpenSSL Library serves as the sole user application level cryptographic library. It provides the FCS_COP functions listed below. All user level applications, such as HTTPS/TLS Web UI, use this library.

3eTI's OpenSSL provides the following cryptographic algorithms in FIPS mode:

- AES
- RSA
- HMAC
- SHS
- ECDSA
- RNG

Table 7-1: 636L3 FIPS-140 Tested Algorithms

Algorithm	Cert No.	SFR Mapping
3eTI OpenSSL		
AES (ECB, CBC, 128, 256 bits key)	2060	FCS_COP.1(1)
ECDSA, sign/verify with P256, P384 and P512	303,415	FCS_COP.1(2)
SHS (SHA-1, SHA-224, SHA-256, SHA-384 and SHA-512)	1801	FCS_COP.1(3)
HMAC	1253	FCS_COP.1(4)
RSA	1072,1278,1491	FCS_COP.1(2) FCS_CKM.1
RNG ANSI X9.31 with one independent hardware based noise source of 128 bits of non-deterministic	1076	FCS_RBG_EXT.1

Secondly, the TOE also contains NIST CMVP validate cryptographic module. For 3e-636L3, it contains 3e-636M CyberFence Cryptographic Module with NIST CMVP validation number 2210. For 3e-636L2, it contains 3e-636M-HSE CyberFence Cryptographic Module with NIST CMVP validation number 2336. These two modules are identical in hardware and software cryptographic functionalities. The differences between the two modules resides in the module software's network functionality with 3e-636M handling IPsec VPN security while the 3e-636M-HSE providing Ethernet MAC encryption. 3e-636L3 and L2 devices use this core for IPsec ESP data and Ethernet MAC data encryption/decryption and secured hashing operations correspondingly. This functionality is outside the scope of the NDPP evaluation.

Compliance to the CC NDPP evaluated configuration for cryptography is provided out of the box. There is no means to modify/disable/enable the cryptography used.

7.1.2.1 Cryptographic Key Generation (for asymmetric keys)

FCS_CKM.1

The TOE support both RSA and ECDSA for authentication. TOE enforces the RSA key size to be 2048 bits or greater. All keys are generated with the Approved RBG then internally verified with 3eTI OpenSSL public key verification function (PKV)

The TOE generally fulfills all of the NIST SP 800-56A requirements without extensions; the following table specifically identifies the "should", "should not", and "shall not" conditions from the publication along with an indication of whether the TOE conforms to those conditions with deviations rationalized.

Table 7-2: NIST SP800-56A Implementation

NIST SP800-56A Section Reference	"should", "should not", or "shall not"	Implemented accordingly?	Rationale for deviation
5.4	Should	yes	
5.5	Should(first occurrence)	yes	
5.5	Should (second occurrence)	yes	
5.6.2	Should	yes	
5.6.2.1	Should	yes	
5.6.2.2	Should	yes	
5.6.2.3	Should	yes	
5.6.3.1	Should(first occurrence)	yes	
5.6.3.1	Should (second occurrence)	yes	
5.6.3.2	Should	yes	
5.6.4.2	Should	yes	
5.6.4.3	Should (first occurrence)	yes	
5.6.4.3	Should(second occurrence)	yes	
5.6	Shall not (first occurrence)	yes	
5.6	Shall not (second occurrence)	yes	
5.8	Shall not (first occurrence)	no	Not needed for TOE operation, therefore not implemented.
5.8	Shall not (second occurrence)	no	Not needed for TOE operation, therefore not implemented.
6	Should (first occurrence)	yes	
6	Should (second occurrence)	yes	
7	Shall not (first occurrence)	no	Not needed for TOE operation, therefore not implemented.
7	Shall not (second occurrence)	no	Not needed for TOE operation, therefore not implemented.
9	Shall not	no	Not needed for TOE operation, therefore not implemented.

The TOE generally fulfills all of the NIST SP 800-56B requirements without extensions; the following table specifically identifies the "should", "should not", and "shall not" conditions from the publication along with an indication of whether the TOE conforms to those conditions with deviations rationalized.

Table 7-3: NIST SP800-56B Implementation

NIST SP800-56B Section Reference	"should", "should not", or "shall not"	Implemented accordingly?	Rationale for deviation
5.6	Should	Yes	
5.8	Shall Not	No	RSA OAEP is not supported. The TOE supports RSA PKCS1 Padding
5.9	Shall Not (1st instance)	Yes	
5.9	Shall Not (2nd instance)	Yes	
6.1	Should Not	Yes	
6.1	Should (1st instance)	Yes	
6.1	Should (2nd instance)	Yes	
6.1	Should (3rd instance)	Yes	
6.1	Should (4th instance)	Yes	
6.1	Shall Not (1st instance)	Yes	
6.1	Shall Not (2nd instance)	Yes	
6.2.3	Should	Yes	
6.5.1	Should	Yes	
6.5.2	Should	Yes	
6.5.2.1	Should	Yes	
6.6	Shall Not	Yes	
7.1.2	Should	Yes	
7.2.1.3	Should	Yes	
7.2.1.3	Should Not	Yes	
7.2.2.3	Shall Not	No	RSA OAEP is not supported. The TOE supports RSA PKCS1 Padding
7.2.2.3	Should (1st instance)	No	RSA OAEP is not supported. The TOE supports RSA PKCS1 Padding
7.2.2.3	Should (2nd instance)	No	RSA OAEP is not supported. The TOE supports RSA PKCS1 Padding

NIST SP800-56B Section Reference	"should", "should not", or "shall not"	Implemented accordingly?	Rationale for deviation
7.2.2.3	Should (3rd instance)	No	RSA OAEP is not supported. The TOE supports RSA PKCS1 Padding
7.2.2.3	Should (4th instance)	No	RSA OAEP is not supported. The TOE supports RSA PKCS1 Padding
7.2.2.3	Should Not	No	RSA OAEP is not supported. The TOE supports RSA PKCS1 Padding
7.2.3.3	Should (1st instance)	No	RSA-KEM-KSW is not supported
7.2.3.3	Should (2nd instance)	No	RSA-KEM-KSW is not supported
7.2.3.3	Should (3rd instance)	No	RSA-KEM-KSW is not supported
7.2.3.3	Should (4th instance)	No	RSA-KEM-KSW is not supported
7.2.3.3	Should (5th instance)	No	RSA-KEM-KSW is not supported
7.2.3.3	Should Not	No	RSA-KEM-KSW is not supported
8	Should	Yes	
8.3.2	Should Not	Yes	

When the TOE is operated in FIPS-mode, all cryptographic operations performed by the TOE are FIPS-compliant, using only FIPS-approved algorithms. The corresponding FIPS 140-2 approved algorithms are all CAVP validated by 3eTI as listed in Table 7-1.

7.1.2.2 Cryptographic Key Zeroization

FCS_CKM_EXT.4

Table 7-4 below lists all the keys and CSPs used and managed by the TOE.

Table 7-4: TOE CSPs Use and Management

Non-Protocol Keys/CSPs

Key/CSP	Type	Generation/ Input	Output	Storage	Zeroization	Use
Operator passwords	ASCII string	Input encrypted (using TLS session key)	Not output	PKCS5 hash in flash	Zeroized when reset to factory settings.	Used to authenticate CO and Admin role operators
Firmware verification key	ECDSA public key	Embedded in firmware at compile time. Firmware upgrade is through encrypted (using TLS session key)	Not output	Plaintext in flash	Zeroized when firmware is upgraded.	Used for firmware digital signature verification
RNG Keys/CSPs						
Key/CSP	**Type**	**Generation/ Input**	**Output**	**Storage**	**Zeroization**	**Use**
FIPS ANSI X9.31RNG Seed Key	16-byte value	512 bytes from hardware noise, then hashed by HMAC-SHA256	Not output	Plaintext in RAM	Zeroized every time a new random number is generated using the FIPS PRNG after it is used.	Used to initialize FIPS RNG
RNG Seed	16-byte value	512 bytes from hardware noise, then hashed by HMAC-SHA256	Not output	Plaintext in RAM	Zeroized every time a new random number is generated using the FIPS PRNG after it is used.	Used as seed for FIPS RNG.
RFC 2818 HTTPS Keys/CSPs						
Key/CSP	**Type**	**Generation/ Input**	**Output**	**Storage**	**Zeroization**	**Use**
RSA private key	RSA (2048) (key wrapping; key establishment methodology provides 112-bits of encryption strength)	Not input (installed at factory)	Not output	Plaintext in flash	Zeroized when new private key is uploaded	Used to support CO and Admin TLS/HTTPS interfaces.

TLS session key for encryption	Triple-DES (192) AES (128/256)	Not input, derived using TLS protocol	Not output	Plaintext in RAM	Zeroized when a page of the web GUI is served after it is used.	Used to protect TLS/HTTPS session.
Public Security Parameter						
HTTPS Public certificate	RSA (2048)	Input encrypted (using TLS session key)	During TLS session setup			Used to setup TLS session for TLS/HTTPS
HTTPS root certificate	RSA (2048)	Input encrypted (using TLS session key)	Not output			Used to setup TLS session for TLS/HTTPS

The zeroization technique is to write all 0xa5, then 0x5a, 0xff and finally all zeros to the memory location where the key is stored. The same zeroization technique is applied to flash and RAM with maximum time delay of approximately 100 ns. Therefore there is not sufficient time to read keys and CSPs before they are zeroized, ie from the zeroization determination time to the zeroization effective time.

7.1.2.3 Cryptographic Operation (Data encryption/decryption)

FCS_COP.1 (1)

The 3eTI's OpenSSL Library provides AES services for application level data encryption and decryption. The management interface uses this library to provide Transport Layer Security (TLS/HTTPS)..

Table 7-1 lists the AES mode and key sizes, all AES algorithm implementations are NIST CAVP validated.

7.1.2.4 Cryptographic Operation (for cryptographic signature)

FCS_COP.1 (2)

The 3eTI OpenSSL Library provides the RSA Digital Signature Algorithm (rDSA) to the TLS/HTTPS Daemon for the TLS session. The TLS/HTTPS Daemon enforces a 2048 bit RSA key length for use with the RSA. Table 7-1 lists RSA and ECDSA CAVP validation certificate numbers.

7.1.2.5 Cryptographic Operation (Hashing)

FCS_COP.1 (3)

The TSF supports SHA-1, SHA-224, SHA-256, SHA-384, or SHA-512 for secure hashing. See Table 7-1 for details.

7.1.2.6 Cryptographic Operation (for keyed-hash message authentication)

FCS_COP.1 (4)

The TOE's OpenSSL Library implements an HMAC algorithm in FIPS-approved mode. See Table 7-1 for details.

7.1.2.7 Cryptographic Operation (Random Bit Generation)

FCS_RBG_EXT.1

The TOE implement RBG as defined in X9.31 Appendix 2.4 using AES. The entropy source is hardware based noise generator.

7.1.3 User Data Protection Functions

7.1.3.1 Full Residual Information Protection

FDP_RIP.2

Message buffers are zeroized before reallocation to ensure that the TOE does not allow data from a previously transmitted packet to be inserted into unused areas or passed in the current packet. Newly allocated memory buffers are also zeroized prior to its usage.

Message buffers are store in a pool. Each message buffers is zeroized by writing a zero to each memory location in the buffer before the buffer is added to the pool. Buffers get used by removing them from the pool, used, then returned to the pool. The buffer is zeroized by writing a zero to each memory location before it is returned to the pool.

7.1.4 User Identification and Authentication

7.1.4.1 User Identification and Authentication

FIA_PMG_EXT.1, FIA_UIA_EXT.1, FIA_UAU_EXT.2, FIA_UAU.7, FCS_TLS_EXT.1, FCS_HTTPS_EXT.1

The Security Administrator must logon to the TOE over HTTP/TLS. The TOE supports TLS version 1.0/1.1/1.2 with AES-CBC-128 and AES-CBC-256 as the supported cipher. The TOE's TLS/HTTPS server uses RSA 2048 bits certificate for TLS authentication. After the TLS session's successful setup, the security administrator logs into the TOE via user name and passwords. If the failure count reaches the configured threshold, the TLS/HTTPS session will be terminated by the TLS/HTTPS server.

The TOE supports the password policy defined in FIA_PMG_EXT.1. Additionally, the TOE supports password lengths up to 32 characters long. NOTE: The TOE will truncate passwords that are longer than 32 characters when creating a user or changing passwords for an existing user.

A successful login is constituted by the completion of a successful TLS handshake followed by the client providing a valid user name and password over that TLS session.

7.1.5 Security Management Functions

The Web Management Application over HTTP/TLS provides capabilities for the authorized administrator to manage cryptographic, audit, and authentication functions and data. This Web Management Application can be accessed via the dedicated local Ethernet configured for "out-of-band" management. There is no local access such as a serial console port. Therefore, the local and remote management is considered the same for this evaluation.

Management of TSF Data

FMT_MTD.1, FMT_SMF.1, FMT_SMR.2

The TOE provides three roles: Security Administrator, Non-security Administrator, and user (Peer Device). Security Administrator and Administrator can only access the TOE through Web Application through TLS/HTTPS.

Upon successful authentication with the TOE, the Security Administrator can manage TSF data as shown in the table below.

Table 7-5: Management of TSF Data

Service and Purpose	Details	Security Administrator (referred to as Crypto officer in guidance)	Security Administrator (referred to as Crypto officer in guidance)
Input of Keys	IKE v2 digital certificate private key, 802.1X supplicant private key, device HTTPS private keys, authentication key with RADIUS Server.	X	
Create and manage users	Support up to 10 administrator users and 5 crypto officer users.	X	
Change password	Administrator changes his own password only.	X	X
Show system status	View traffic status and systems log excluding security audit log.	X	X
Manage audit logging	Select audit events to be logged. Configure remote audit logging. View audit event records.	X	
Key zeroization via reboot		X	X
Factory default	Delete all configurations and set device back to factory default state.	X	
Perform Self-Test	Run algorithm KAT through reboot.	X	X
Load New Firmware	Upload 3eTI digitally signed firmware.	X	
SNMP Management	Manage all SNMP settings including SNMPv3 encryption key.	X	X
HTTPS Management	Load HTTPS server certificate and private key.	X	

Key Generation	Create asymmetric key pairs and X509v3 Certificate Signing Request.	X	X

No GUI interfaces are accessible to user prior to authentication. The TOE enforces authentication then enables the TSF data configuration interfaces. The Non-security administrators have no access to those TSF data configuration interfaces.

7.1.6 Protection of the TSF Functions

7.1.6.1 Reliable Time Stamps

FPT_STM.1

The TOE has a running NTP daemon to synchronize the local time with an external NTP server. The NTP server is located in trusted IT environment and connected to the TOE via dedicated physical port. In the absence of an NTP server in the Operational Environment, the authorized security administrator has the capability to set the time locally.

The local time is used for the following security functions identified in this ST:

- Time stamping each audit record.
- Verifying the validity of the Web Server X509v3 Certificate.
- Verifying the validity of the Firmware X509v3 Certificate during the firmware upload process.
- Enforcing user lockout periods for “Bad Password” login attempts.
- Timing out login sessions due to inactivity.

7.1.6.2 TSF Testing

FPT_TST_EXT.1

The TSF performs a firmware integrity check and a configuration file integrity check on system start up. Algorithm Known Answer Tests are run at startup time as shown below:

Power-on self-tests:

Software Integrity Test

- Bootloader Integrity Test
- Firmware Integrity Test

FreeScale PowerQUICC Crypto Engine Power-on self-tests:

• AES ECB	encrypt/decrypt KAT
• AES_CCM	encrypt/decrypt KAT
• AES_GCM	encrypt/decrypt KAT
• AES_CMAC	
• SHA-1, SHA224, SHA256, SHA384, SHA512	KAT
• HMAC SHA-1, SHA224, SHA256, SHA384, SHA512	KAT

3eTI OpenSSL library Power-on self-tests:

AES ECB –	encrypt/decrypt KAT
Triple-DES CBC –	encrypt/decrypt KAT
HMAC SHA-1, SHA224, SHA256, SHA384, SHA512	KAT
SHA-1, SHA224, SHA256, SHA384, SHA512	KAT
ANSI X.31 RNG	KAT
RSA sign/verify	KAT
ECDSA sign/verify	KAT

Vectors for each known answer test (KAT) are compiled into the Firmware. The known inputs are provided to the cryptographic function and the output of that function is compared to the known output. The firmware is halted if any of the known answer tests fail.

After device is powered on, the first thing done by bootloader is to check its own integrity. If the integrity is broken, firmware won’t boot. Firmware integrity is performed at firmware boot up. Both firmware and bootloader are digitally signed with ECDSA.

Conditional self-tests:

- Continuous Random Number Generator Test (CRNGT) on Approved RNG
- Continuous Number Generator Test (CRNGT) on NDRNG
- DH pair-wise consistency test at key generation time
- Firmware load test

The Continuous Random Number test consists of a Repetitive Count test and an Adaptive Proportion test. Each random sample is compared to previous samples. The Repetitive Count test ensures the new sample is not repeated sequentially above a threshold. The Adaptive Proportion test ensures the new sample is not repeated beyond a threshold within a window of previous samples.

7.1.6.3 Protection of TSF Data

FPT_SKP_EXT.1, FPT_APW_EXT.1

The authentication passwords are stored in PKCS5 format in the TOE. All other CSPs are stored in encrypted format in the TOE on non-volatile memory. The file system that holds the hashed password and encrypted CSPs are made read-only during runtime to avoid data corruption. None of the files or CSPs is available through any external interfaces to users/administrators. The Web Application Interface allows security administrator to input keys/passwords to the TOE with no output capabilities.

7.1.6.4 Trusted Update

FPT_TUD_EXT.1

The Security Administrator can update the TOE's firmware. The firmware is digitally signed with ECDSA. The TOE uses the public key to verify the digital signature. Upon successful verification, the TOE will load the new update upon reboot. The update will be rejected if the verification fails.

The TOE's firmware contains a self signed X509v3 certificate compiled into the firmware. This certificate is used to verify future firmware updates. The certificate contains an ECDSA public key using prime256v1 curve. Firmware updates must be signed using the corresponding private key held in confidence by 3eTI. The certificate is built with validity dates between the years 1970 and 2038. The certificate is manually updated when a new firmware image is loaded into the device.

7.1.7 TOE Access (FTA)

7.1.7.1 TSF-Initiated Termination

FTA_SSL_EXT.1, FTA_SSL.3, FTA_SSL.4

The Web Management Application terminates the remote or local session if it detects inactivity longer than the configured time period. The default time period is 10 minutes. The remote session will be closed by the Web Management Application together with the HTTPS session. The Security Administrator is required to re-authenticate with the TOE and setup a new session. The time intervals are configurable by the security administrator.

7.1.7.2 TOE Access Banners

FTA_TAB.1

The Management GUI displays a customizable TOE access banner to the remote administrative user before the user can log into the system.

7.1.8 Trusted Path/Channels Functions

7.1.8.1 Inter-TSF Trusted Channel /Trust Path

FTP_ITC.1, FTP_TRP.1, FCS_TLS_EXT.1, FCS_HTTPS_EXT.1

The TOE connects with a trusted Audit Log server via TLS session. Time server is optional with the TOE's time-keeping operation; it's connected to the TOE via dedicated physical port in the trusted IT network.

The management interface with remote administration station is always TLS/HTTPS. The HTTPS implementation is fully compliant with RFC 2818. The TOE acts as HTTPS server and waits for client connection on TCP port 443. The TOE's HTTPS server permits an HTTP client to close the connection at any time, and the HTTPS server will recover gracefully. In particular, the HTTPS server is prepared to receive an incomplete close from the client, and is willing to resume TLS sessions closed in this fashion.

The TOE's HTTPS server supports TLS version 1.0/1.1/1.2 with AES-CBC-128, and AES-CBC-256 as the supported cipher. The TOE's TLS/HTTPS server uses RSA 2048 bits certificate for

TLS authentication. After the TLS session’s successful setup, the security administrator logs into the TOE via user name and passwords. If the failure count reaches the configured threshold, the TLS/HTTPS session will be terminated by the TLS/HTTPS server.