MMA10G-IPX Series Security Target

Acumen Security, LLC.

Document Version: 0.7

Prepared For:
Evertz Microsystems, Ltd.
5292 John Lucas Drive
Burlington, Ontario, CANADA

Prepared by:
Acumen Security
2400 Research Blvd
Rockville MD 20850

Table Of Contents

Revision History

Version	Date	Description
0.1	July 8, 2019	Initial Draft
0.2	July 28, 2019	Updates from testing and evaluation
0.3	August 14, 2019	Addressing validator comments
0.4	August 20, 2019	Additional validator comments
0.5	September 19, 2019	Updates for consistency, additional models, and additional TDs
0.6	November 14, 2019	Updated to address validator comments
0.7	December 3, 2019	Updated to address validator comments

1 Security Target Introduction

1.1 Security Target and TOE Reference

This section provides information needed to identify and control this ST and its TOE.

Category	Identifier
ST Title	IPX Security Target
ST Version	0.7
ST Date	December 3, 2019
ST Author	Acumen Security, LLC.
TOE Identifier	MMA10G-IPX Series
TOE Hardware	MMA10G-IPX-16, MMA10G-IPX-32, MMA10G-IPX-64, 3080IPX-16-G3-CC, 3080IPX-32-G3-CC, 3080IPX-64-G6-CC, 3080IPX-16-10G-CC, 3080IPX-32-10G-CC, 3080IPX-64-10G-CC, 3080IPX-16-10G-HW-CC, 3080IPX-32-10G-HW-CC, 3080IPX-64-10G-HW-CC, 3080IPX-16GE-CC, 3080IPX-32GE-CC, 3080IPX-64GE-CC, 3080IPX-16GE-RJ45-CC, 3080IPX-32GE-RJ45-CC, 3080IPX-64GE-RJ45-CC, 9080IPX-16-12RJ45-4SFP10GE-CC, 9080IPX-16GE-12RJ45-4SFP-CC, 9080IPX-32-28RJ45-4SFP10GE-CC, 9080IPX-32-28RJ45-4SFP-CC
TOE Software Version	MMA10G-IPX-16-CC v3.2 MMA10G-IPX-32-CC v3.2 MMA10G-IPX-64-CC v3.2
TOE Developer	Evertz Micorsystems Ltd. 5292 John Lucas Drive Burlington, Ontario CANADA
Key Words	Network Device

Table 1 TOE/ST Identification

1.2 TOE Overview

1.2.1 TOE Product Type

The TOE is a network-based audio video distribution system and is classified as a network device (a generic infrastructure device that can be connected to a network). The TOE hardware devices are the Evertz:

- MMA10G-IPX-16 running MMA10G-IPX-16-CC v3.2,
- MMA10G-IPX-32 running MMA10G-IPX-32-CC v3.2,
- MMA10G-IPX-64 running MMA10G-IPX-64-CC v3.2,
- 3080IPX-16-G3-CC running MMA10G-IPX-16-CC v3.2,
- 3080IPX-32-G3-CC running MMA10G-IPX-32-CC v3.2,
- 3080IPX-64-G6-CC running MMA10G-IPX-64-CC v3.2,
- 3080IPX-16-10G-CC running MMA10G-IPX-16-CC v3.2,
- 3080IPX-32-10G-CC running MMA10G-IPX-32-CC v3.2,
- 3080IPX-64-10G-CC running MMA10G-IPX-64-CC v3.2,
- 3080IPX-16-10G-HW-CC running MMA10G-IPX-16-CC v3.2,
- 3080IPX-32-10G-HW-CC running MMA10G-IPX-32-CC v3.2,
- 3080IPX-64-10G-HW-CC running MMA10G-IPX-64-CC v3.2,
- 3080IPX-16GE-CC running MMA10G-IPX-16-CC v3.2,
- 3080IPX-32GE-CC running MMA10G-IPX-32-CC v3.2,
- 3080IPX-64GE-CC running MMA10G-IPX-64-CC v3.2,

- 3080IPX-16GE-RJ45-CC running MMA10G-IPX-16-CC v3.2,
- 3080IPX-32GE-RJ45-CC running MMA10G-IPX-32-CC v3.2,
- 3080IPX-64GE-RJ45-CC running MMA10G-IPX-64-CC v3.2,
- 9080IPX-16-12RJ45-4SFP10GE-CC running MMA10G-IPX-16-CC v3.2,
- 9080IPX-16GE-12RJ45-4SFP-CC running MMA10G-IPX-16-CC v3.2,
- 9080IPX-32-28RJ45-4SFP10GE-CC running MMA10G-IPX-32-CC v3.2,
- 9080IPX-32-28RJ45-4SFP-CC running MMA10G-IPX-32-CC v3.2

and will be referred to as IPX throughout this document. The IPX appliances are Ethernet switches optimized for video content.

1.2.2 TOE Usage

The Internet Protocol Crosspoint (IPX) switch is a 10 Gigabit (Gb) Internet Protocol (IP) switch optimized for video-over-IP traffic (compressed or uncompressed). For the MMA10G and 3080 models, each IPX card occupies two (2) slots (16- and 32-port IPX cards) or four (4) slots (64-port IPX cards) in an Evertz Modular Crosspoint (EMX) frame. The 9080 models include the IPX cards and frame in a 1RU form factor. All IPX-compatible cards may be inserted into any IPX frame configuration provided there are sufficient contiguous free slots available.

Since video by nature has a unidirectional flow, and multiple copies of a single incoming video stream are often sent to multiple output destinations, the IPX exclusively uses multicast IP addressing.

Equipment to prepare video for IP transport, or to convert it into other video formats, is outside the scope of this TOE. Such equipment includes, but is not limited to, cameras, KVMs, codecs, video servers and video displays. Equipment to perform functions such as embedding audio and/or other information within the video stream is also outside the scope of this TOE.

Figure 1, below shows the TOE with optional video equipment (i.e. sources, media gateway, and destinations) and with the required equipment listed in Table 2.

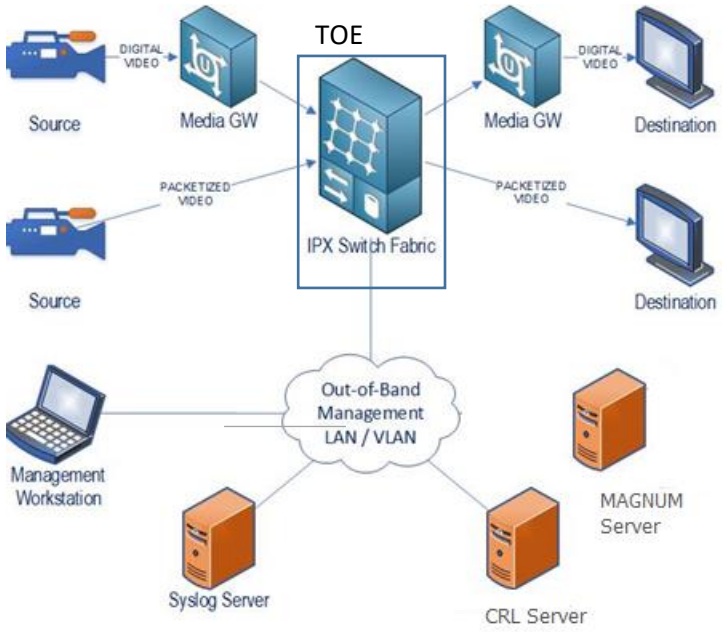

Figure 1 TOE Topology

1.3 TOE IT Environment

The TOE's operational environment must provide the services listed as required to support the secure operation of the TOE. The services not listed as required are optional in the TOE's operational environment.

Component	Required	Usage/Purpose Description for TOE performance
Syslog server	Yes	• Conformant with RFC 5424 (Syslog Protocol) • Supporting Syslog over TLS (RFC 5425) • Acting as a TLSv1.2 server • Supporting Client Certificate authentication • Supporting at least one of the following cipher suites: ○ TLS_RSA_WITH_AES_128_CBC_SHA ○ TLS_RSA_WITH_AES_256_CBC_SHA ○ TLS_RSA_WITH_AES_128_CBC_SHA256 ○ TLS_RSA_WITH_AES_256_CBC_SHA256 ○ TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ○ TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
Management Workstation with web browser	Yes	• Internet Explorer 11, Google Chrome 50, or Firefox 38 • Supporting TLSv1.2 • Supporting Client Certificate authentication • Supporting at least one of the following ciphersuites: ○ TLS_RSA_WITH_AES_128_CBC_SHA ○ TLS_RSA_WITH_AES_256_CBC_SHA ○ TLS_RSA_WITH_AES_128_CBC_SHA256 ○ TLS_RSA_WITH_AES_256_CBC_SHA256 ○ TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256

Component	Required	Usage/Purpose Description for TOE performance
		○ TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
CRL Server	Yes	• Conformant with RFC 5280
MAGNUM Server	Yes	• Provides remote management of the TOE's routing and switching of video signals • Supporting TLSv1.2 with at least one of the following ciphersuites: ○ TLS_RSA_WITH_AES_128_CBC_SHA ○ TLS_RSA_WITH_AES_256_CBC_SHA ○ TLS_RSA_WITH_AES_128_CBC_SHA256 ○ TLS_RSA_WITH_AES_256_CBC_SHA256 ○ TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ○ TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
Media Gateway	No	• Optional component for converting media streams. Not required for TOE operation.
Video Source devices	No	• Optional component for creating video streams that are sent to the TOE. Not required for TOE operation. • Supporting packetized or digital video
Video Destination devices	No	• Optional component for viewing video streams output by the TOE. Not required for TOE operation. • Supporting packetized or digital video

Table 2 IT Environment Components

1.4 TOE Architecture

1.4.1 Physical Boundaries

For the MMA10G and 3080 models, each IPX model includes an EMX chassis, one or more IPX card with TOE software, and SFP module. The 9080 models include IPX cards and chassis. The TOE is shipped with all components, including TOE software pre-installed on the TOE. The TOE software can also be downloaded from the Evertz website. The TOE's user guidance, described in section 1.4.8, is also included with the shipped appliance.

IPX supports four (4) available chassis (frames). Each chassis includes a single standard power supply, and each can support dual redundant power supplies.

- ***EMX1-FR***
- ***EMX3-FR***
- ***EMX6-FR***
- **9080IPX**

These chasses serve only to enclose the IPX cards and provide power distribution. Each EMX chassis must also include an EMX Frame Controller Card.

The IPX cards with MMA10G-IPX firmware, associated SFPs, their mounting frames and the frames' controllers and power supplies make up an IPX installation. The IPX firmware varies for each model, but the differences are only related to the hardware differences and are not security relevant. The firmware is identified as:

- MMA10G-IPX-16-CC v3.2

- MMA10G-IPX-32-CC v3.2
- MMA10G-IPX-64-CC v3.2

With the differences relating only to the different hardware within each model. The functionality provided by the SFP modules and Frame Controller Cards are not security relevant and were not evaluated in this certification effort.

IPX CARD	CONTIGUOUS SLOTS	PORTS	CPU	EMX1-FR	EMX3-FR	EMX6-FR
MMA10G-IPX-16-CC	2	16 SFP	PowerQUICC® II Pro MPC8377E	✓	✓	✓
MMA10G-IPX-32-CC	2	32 SFP	PowerQUICC® II Pro MPC8377E	✓	✓	✓
MMA10G-IPX-64-CC	4	64 SFP	PowerQUICC® II Pro MPC8377E		✓	✓
3080IPX-16-G3-CC	2	16 SFP	PowerQUICC® II Pro MPC8377E	✓	✓	✓
3080IPX-32-G3-CC	2	32 SFP	PowerQUICC® II Pro MPC8377E	✓	✓	✓
3080IPX-64-G6-CC	4	64 SFP	PowerQUICC® II Pro MPC8377E		✓	✓
3080IPX-16-10G-CC	2	16 SFP	PowerQUICC® II Pro MPC8377E	✓	✓	✓
3080IPX-32-10G-CC	2	32 SFP	PowerQUICC® II Pro MPC8377E	✓	✓	✓
3080IPX-64-10G-CC	4	64 SFP	PowerQUICC® II Pro MPC8377E		✓	✓
3080IPX-16-10G-HW- CC	2	16 SFP	PowerQUICC® II Pro MPC8377E	✓	✓	✓
3080IPX-32-10G-HW- CC	2	32 SFP	PowerQUICC® II Pro MPC8377E	✓	✓	✓
3080IPX-64-10G-HW- CC	4	64 SFP	PowerQUICC® II Pro MPC8377E		✓	✓
3080IPX-16GE-CC	2	16 SFP	PowerQUICC® II Pro MPC8377E	✓	✓	✓
3080IPX-32GE-CC	2	32 SFP	PowerQUICC® II Pro MPC8377E	✓	✓	✓
3080IPX-64GE-CC	4	64 SFP	PowerQUICC® II Pro MPC8377E		✓	✓
3080IPX-16GE-RJ45-CC	2	16 RJ45	PowerQUICC® II Pro MPC8377E	✓	✓	✓
3080IPX-32GE-RJ45-CC	2	32 RJ45	PowerQUICC® II Pro MPC8377E	✓	✓	✓
3080IPX-64GE-RJ45-CC	4	64 RJ45	PowerQUICC® II Pro MPC8377E		✓	✓
9080IPX-16-12RJ45-4SFP10GE-CC	2	12 RJ45 4 SFP	PowerQUICC® II Pro MPC8377E	n/a	n/a	n/a
9080IPX-16GE-12RJ45-4SFP-CC	2	12 RJ45 4 SFP	PowerQUICC® II Pro MPC8377E	n/a	n/a	n/a

9080IPX-32-28RJ45-4SFP10GE-CC	2	28 RJ45 4 SFP	PowerQUICC® II Pro MPC8377E	n/a	n/a	n/a
9080IPX-32-28RJ45-4SFP-CC	2	28 RJ45 4 SFP	PowerQUICC® II Pro MPC8377E	n/a	n/a	n/a

Table 3 IPX Card Types

The EMX frames are the chassis in which the MMA10G and 3080 IPX cards are installed.

FRAME	MAIN POWER	REDUNDANT POWER	FRAME CONTROLLER	CONTROLLER SLOTS	EQUIPMENT SLOTS	RUS
EMX1-FR	EMX1-PS	empty slot	EMX-FC	1	2	1
EMX1-FR+PS	EMX1-PS	EMX1-PS	EMX-FC	1	2	1
EMX3-FR	EMX3-PS	empty slot	EMX-FC	2	5	3
EMX3-FR+3PS	EMX3-PS	EMX3-PS	EMX-FC	2	5	3
EMX6-FR	EMX6-PS	empty slot	EMX-FC	2	15	6
EMX6FR-6PS	EMX6-PS	EMX6-PS	EMX-FC	2	15	6

Table 4 EMX Frames

The EMX frames are passive (except for the door-mounted fans, which are the only powered equipment permanently attached to the frame). The frames mount power supplies, frame controllers and IPX cards. The frame controllers provide Ethernet-based connections for control traffic to the individual IPX cards within the EMX frame chassis. These cards do not provide security functionality for the TOE.

1.4.2 IPX Module Description

The IPX features the following physical I/O interfaces.

- Chassis interfaces:
    - **Ethernet Port:** These are 1000BaseT RJ-45 connectors used for IP-based communications over a LAN or WAN. Ethernet ports only support control traffic. Operational traffic (media) is not supported on this channel.
    - **"Ref" (Genlock) Ports:** These are Bayonet Neill-Concelman (BNC) connectors that will accept analog video signals used to establish frame sync for video switching. Genlock is not used for IP video (buffers are used instead), so these ports are not used by the IPX cards that comprise this TOE.
    - **Serial Port:** These are RS-232 ports on DB-9 connectors. They are used to set the IP addresses of the EMX-FC frame controller cards in EMX3-FR and EMX6-FR frames without needing to use the ribbon cable adapters described above.
    - **Alarm Contact Closures:** There are two sets of these (for major and minor alarms) on the EMX1-FR (only). They are pin-type connectors.

- Controller card serial port interface: The serial port interface is used to set the IP address of the EMX-FC card using an RS-232 serial interface. The serial connection has no functionality except setting up the IP address and related information. Administrators establish the serial connection using a site-provided terminal client. The serial connection is password protected.

- IPX routing card interfaces
    - **Serial Port:** The IPX card serial port supports a customized 4-pin connection requiring a special ribbon cable adapter (provided). This interface is only used to set the IP address of the IPX card. While the address may be reset in the field as necessary, this interface is generally only used during initial installation and configuration.
    - **SFP Slot:** Each slot may be equipped with one of the 63 types of SFPs. These interfaces support operational media traffic. SFPs support three transport categories:
        - 10 Gb/sec Optical (60 versions vary in optical power, optical wavelength and optical receive sensitivity)
        - 1.25 Gb/sec Optical (two versions vary in include optical wavelength)
        - 1 Gb/sec Electrical (1000BaseT, DB45 connector)
    - **RJ45 Slot:** only present on models with "RJ45" in the model name. These interfaces support operational media traffic at 1 GbE

1.4.3 Component Interconnectivity

The TOE consists of one or more IPX cards located within a given EMX frame or a 9080 chassis that include the IPX card and frame controller. Each EMX frame supports (2) 1000 Mbps IP ports per EMX frame controller (EMX-FC) card for administration and control (via the EMX-FC frame controller). For all architectures, the control ports on the IPX are fully encrypted. There is no internal logical or physical connection within the IPX hardware between the SFP ports and the control ports. The IPX supports security and operational auditing. Audit data is be securely downloaded to a Syslog server via TLS.

1.4.4 TOE Management Overview

The TOE provides a proprietary WebEasy interface that permits site administrators to configure the IPX for normal operations using a secure TLS session over TCP. This may include:

- Active ports
- Port Capacity
- Port interface
- User configuration

The TOE is configured to only allow the evaluated ciphersuites are these ciphersuites are the only ones offered by the TOE.

1.4.5 Logical Scope of the TOE

The IPX has thirteen functional modules, of which eleven are considered to be part of the Target Security Function (TSF). All modules are described here in order to provide context for the TOE functionality. The following IPX functional modules are part of the TSF:

- **Administrator Accounts:** Used to manage administrator user accounts and assigned roles. The TOE has a default administrative user account with default login credentials, which must be changed at the time of installation.
- **Self-Test:** Used at boot-up time to self-test the security function to ensure no tampering has occurred.
- **Network:** Used to manage the network interface settings for the TOE, including IP address and DNS.

- **Firmware Upgrades:** Used to manage upgrades of the TOE firmware.
- **Cryptography Support:** Used to manage the cryptographic module and keys.
- **Security Audit:** Used to manage the recognition, recording and transmission of information related to security activities.
- **Identification and Authorization:** Used to determine that only authorized users have access.
- **Security Management**: Used to adjust parameters related to security functions.
- **Protection of the TSF**: Used to defend against attacks, malicious or otherwise.
- **TOE Access**: Used to limit access to authorized Administrators.
- **Trusted Path/Channel:** Used to ensure that communications between the IPX and authorized devices and Administrators is secure.

The figure below depicts the logical scope of the TOE.

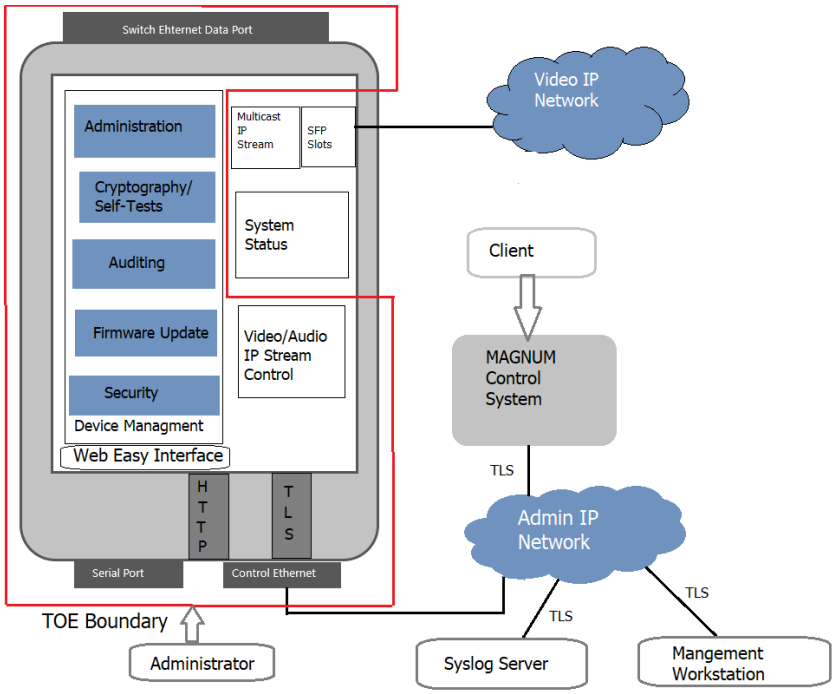

Figure 2 TOE Logical Scope and Workflow

The following functional modules are not part of the TSF:

- **Multicast IP Stream:** Used to manage the settings for the multicast inputs, outputs and virtual cross connection; this is the normal operational function of the IPX.
- **System Status:** Used to record non-security audit information (on the "health" and status of the system) on an external Syslog server. Note: System status and TOE auditing are separate modules.

The TOE supports the following functionality:

- Security Audit
- Cryptographic Support
- Identification and Authentication

- Security Management
- Protection of the TSF
- TOE Access
- Trusted Path/Channels

1.4.6 Security Functions provided by the TOE

The TOE provides the security functionality required by NDcPP v2.1.

1.4.6.1 Security Audit

The TOE's Audit security function supports audit record generation and review. The TOE provides date and time information that is used in audit timestamps. Very broadly, the Audit events generated by the TOE include:

- Establishment of a trusted path or channel session
- Failure to Establish a trusted path or channel session
- Termination of a trusted path or channel session
- Failure of trusted channel functions
- Identification and Authentication
- Unsuccessful attempt to validate a certificate
- Lockouts due to unsuccessful authentication attempts
- Any update attempt
- Result of the update attempt
- Management of TSF data
- Changes to Time
- Session timeouts

The TOE stores generated audit data on itself and sends audit events to a syslog server, using a TLS protected collection method. Logs are classified into various predefined categories. The logging categories help describe the content of the messages that they contain. Access to the logs is restricted to only Security Administrators, who has no access to edit them, only to copy or delete (clear) them. Audit records are protected from unauthorized modifications and deletions.

The TSF provides the capability to view audit data by using the Syslog tab in the web browser. The log records the time, host name, facility, application and "message" (the log details). The previous audit records are overwritten when the allocated space for these records reaches the threshold on a FIFO basis.

1.4.6.2 Cryptographic Support

The TOE includes an OpenSSL library that implements CAVP validated cryptographic algorithms for random bit generation, encryption/decryption, authentication, and integrity protection/verification. These algorithms are used to provide security for the TLS/HTTPs connections for secure management and secure connections to a syslog and authentication servers. TLS and HTTPs are also used to verify firmware updates. The cryptographic services provided by the TOE are described below.

Cryptographic Protocol	Use within the TOE
HTTPS/TLS (client)	Secure connection to syslog FCS_HTTPS_EXT.1, FCS_TLSC_EXT.1

Cryptographic Protocol	Use within the TOE
HTTPS/TLS (server)	Peer connections to a backup MAGNUM and remote management FCS_HTTPS_EXT.1, FCS_TLSS_EXT.2
AES	Provides encryption/decryption in support of the TLS protocol. FCS_TLSC_EXT.1, FCS_TLSS_EXT.2
DRBG	Deterministic random bit generation use to generate keys. FCS_TLSS_EXT.2, FCS_RBG_EXT.1
Secure hash	Used as part of digital signatures and firmware integrity checks. FCS_COP.1/Hash, FCS_TLSC_EXT.1, FCS_TLSS_EXT.2
HMAC	Provides keyed hashing services in support of TLS. FCS_COP.1/KeyedHash, FCS_TLSC_EXT.1, FCS_TLSS_EXT.2
EC-DH	Provides key establishment for TLS. FCS_CKM.2, FCS_TLSC_EXT.1, FCS_TLSS_EXT.2
ECDSA	Provides components for EC-DH key establishment. FCS_CKM.1, FCS_CKM.2, FCS_TLSS_EXT.2
RSA	Provide key establishment, key generation and signature generation and verification (PKCS1_V1.5) in support of TLS. FCS_CKM.1, FCS_COP.1/SigGen, FCS_COP.1/SigVer, FCS_TLSC_EXT.1, FCS_TLSS_EXT.2

Table 5 TOE Cryptographic Protocols

Each of these cryptographic algorithms have been validated for conformance to the requirements specified in their respective standards, as identified below.

Algorithm	Standard	CAVP Certificate #	Processors
AES 128/256-bit CBC, GCM	IOS 19772 (GCM)	C1039	PowerQUICC® II Pro MPC8377E
CTR DRBG using AES 256	ISO/IEC 18031:2011	C1039	PowerQUICC® II Pro MPC8377E
EC-DH	NIST SP 800-56A (key establishment)	C1039	PowerQUICC® II Pro MPC8377E
ECDSA	FIPS PUB 186-4 (key generation)	C1039	PowerQUICC® II Pro MPC8377E
HMAC-SHA-1/256/384	ISO/IEC 9797-2:2011	C1039	PowerQUICC® II Pro MPC8377E
SHA-1/256/384	ISO/IEC 10118-3:2004	C1039	PowerQUICC® II Pro MPC8377E
RSA 2048/3072/4096	FIPS PUB 186-4 (key generation and Digital Signature) ISO/IEC 9796-2 (digital signature)	C1039[1]	PowerQUICC® II Pro MPC8377E

Table 6 CAVP Algorithm Testing References

1.4.6.3 Identification and Authentication

All Administrators wanting to use TOE services are identified and authenticated prior to being allowed access to any of the services other than the display of the warning banner. ("Regular" IPX users do not access IPX directly; they control IP video switching through the IPX using a switch control system, such as Evertz' Magnum. The switching of those IP video transport stream is outside the scope of the TOE.)

[1] Evertz vendor affirms the implementation of RSA 4096 for key generation since no CAVP tests are available for this key size.

Once an Administrator attempts to access the management functionality of the TOE, the TOE prompts the Administrator for a username and password for password-based authentication. The identification and authentication credentials are confirmed against a local user database. Only after the Administrator presents the correct identification and authentication credentials will access to the TOE functionality be granted. The TOE uses X.509v3 certificates as defined by RFC 5280 to support authentication for TLS/HTTPS connections.

The TOE provides the capability to set password minimum length rules. This is to ensure the use of strong passwords in attempts to protect against brute force attacks. The TOE also accepts passwords composed of a variety of characters to support complex password composition. During authentication, no indication is given of the characters composing the password.

Remote administrators are locked out after a configurable number of unsuccessful authentication attempts.

The IPX requires a password-protected serial connection to perform initial configuration of the system IP address(es). Once each address is established, administrators use IP connectivity for all further administrative actions, including configuration, operations, and monitoring.

1.4.6.4 Security Management

The TOE provides secure administrative services for management of general TOE configuration and the security functionality provided by the TOE. All TOE administration occurs either through a secure session or a local console connection. The TOE provides the ability to perform the following actions:

- Administer the TOE locally and remotely
- Configure the access banner
- Configure the cryptographic services
- Configure number of unsuccessful login attempts that trigger a lockout
- Update the TOE and verify the updates using digital signature capability prior to installing those updates
- Specify the time limits of session inactivity

All of these management functions are restricted to an Administrator, which covers all administrator roles. Administrators are individuals who manage specific type of administrative tasks. In IPX only the only admin role exists, since there is no provision for “regular” users to access IPX directly (as described above), and the portion of IPX they access and control are outside the scope of the TOE.

Primary management is done using the Webeasy web-based interface using HTTPS. This provides a network administration console from which one can manage various identity services. These services include authentication, authorization and reporting. All of these services can be managed from the web browser, which uses a menu-driven navigation system.

There is also a very simple serial-based connection (RS-232) that provides a simple menu interface. This is used to configure the IP interface (IP address, etc.). It is password-protected, and is typically only used once, for initial set-up.

1.4.6.5 Protection of the TSF

The TOE will terminate inactive sessions after an Administrator-configurable time period. Once a session has been terminated the TOE requires the user to re-authenticate to establish a new session. The TOE provides protection of TSF data (authentication data and cryptographic keys). In addition, the TOE internally maintains the date and time. This date and time is used as the time stamp that is applied to TOE generated audit records. The TOE also ensures firmware updates are from a reliable source. Finally, the TOE performs testing to verify correct operation.

In order for updates to be installed on the TOE, an administrator initiates the process from the web interface. IPX automatically uses the digital signature mechanism to confirm the integrity of the product before installing the update.

1.4.6.6 TOE Access

Aside from the automatic Administrators session termination due to inactivity describes above, the TOE also allows Administrators to terminate their own interactive session. Once a session has been terminated the TOE requires the user to re-authenticate to establish a new session.

The TOE will display an Administrator-specified banner on the web browser management interface prior to allowing any administrative access to the TOE.

1.4.6.7 Trusted Path/Channels

The TOE allows the establishment of a trusted path between a video control system (such as Evertz' Magnum) and the IPX. The TOE also establishes a secure connection for sending audit data to a syslog server using TLS and other external authentication stores using TLS-protected communications.

The TOE uses HTTPS/TLS to provide a trusted path between itself and remote administrative users. The TOE does not implement any additional methods of remote administration. The remote administrative users are responsible for initiating the trusted path when they wish to communicate with the TOE.

1.4.6.8 Excluded Functionality

The following functionality is not part of the TOE and shall not be enabled or used in in the CC evaluated configuration:

- SNMP Traps (Alarms)
- VistaLINK PRO module
- External Authentication Servers for administrator authentication

These functions are outside the TOE. Alarm monitoring is the sending of SNMP traps to an alarm monitoring system (which is assigned by an Administrator).

In addition, IPX provides IP video stream switching. This IP video switching does not provide security functionality and was therefore not evaluated and is outside the scope of the TOE. The nature of video encryption and decryption is that a video stream is encrypted at the sending end and decrypted at the receiving end; since IPX is a midpoint device and therefore does not perform encryption or decryption functionality. This functionality, while present in the TOE was not evaluated.

1.4.7 TOE Documentation

Evertz Microsystems, Ltd. publishes manuals detailing the installation configuration and operation of the IPX cards, EMX frames and Magnum control software. These are available to customers both on paper and as electronic copies. Electronic copies are available in .pdf format from the Evertz support website with a valid customer login.

CATEGORY	PRODUCT	SOFTWARE	MANUAL
LAYER 2 DISTRIBUTION CARDS	MMA10G IPX Series	MMA10G-IPX-16-CC v3.2	MMA10G-IPX Series-CC High Bandwidth 10GE Switch Fabric User Manual," Version 1.0, January 2017 [IPX UG]
		MMA10G-IPX-32-CC v3.2	
		MMA10G-IPX-64-CC v3.2	
SIGNAL TRANSCEIVERS	SFP10G-TR13	n/a	
	SFP10G-TR15S	n/a	
	SFP10G-TR15H	n/a	
	SFP10G-TRCxxH*	n/a	
	SFP10G-TRDxxxH*	n/a	
	SFPTR-RJ45-SGM-GI	n/a	
	SFP1G-TR13	n/a	
	SFP1G-TR15S	n/a	
CONTROL FRAMES	EMX1-FR	n/a	EMX Series Multiframe User Manual, Version 1.3, August 2014
	EMX1-FR+PS	n/a	
	EMX3-FR	n/a	
	EMX3-FR+3PS	n/a	
	EMX6-FR	n/a	
	EMX6-FR+6PS	n/a	
CONTROL FRAME MANAGEMENT CARDS	EMX-FC	revB v4.11	
	EMX-FC	revB v4.11	
	EMX-FC	revB v4.11	
	EMX-FC	revB v4.11	

Table 7 Evertz Operating Manuals

In addition, the following Common Criteria documentation is included:

- MMA10G-IPX Security Target v0.7, December 3, 2019
- IPX MMA10G-IPX Security Administration Manual Revision 1d, December 3, 2019

1.4.8 Other References

- collaborative Protection Profile for Network Devices, Version 2.1 [NDcPP]

2 Conformance Claims

2.1 CC Conformance

This TOE is conformant to:

- Common Criteria for Information Technology Security Evaluations Part 1, Version 3.1, Revision 5, April 2017
- Common Criteria for Information Technology Security Evaluations Part 2, Version 3.1, Revision 5, April 2017: Part 2 extended
- Common Criteria for Information Technology Security Evaluations Part 2, Version 3.1, Revision 5, April 2017: Part 3 extended

2.2 Protection Profile Conformance

This TOE is conformant to:

- collaborative Protection Profile for Network Devices, Version 2.1 [NDcPP]

2.3 Conformance Rationale

This Security Target provides exact conformance to the collaborative Protection Profile for Network Devices, Version 2.1 [NDcPP]. The security problem definition, security objectives and security requirements in this Security Target are all taken from the Protection Profile performing only operations defined there.

2.3.1 Technical Decisions

All NIAP Technical Decisions (TDs) issued to date that are applicable to [NDcPP] have been addressed. The following table identifies all applicable TD:

Identifier	Applicable	Exclusion Rationale (if applicable)
0453 – NIT Technical Decision for Clarify authentication methods SSH clients can use to authenticate SSH	No	FCS_SSHC_EXT is not claimed.
0452 – NIT Technical Decision for FCS_(d)TLSC_EXT.X.2 IP addresses in reference identifiers	Yes	
0451 – NIT Technical Decision for ITT Comm UUID Reference Identifier	Yes	
0450 – NIT Technical Decision for RSA-based ciphers and the Server Key Exchange message	Yes	
0449 – NIT Technical Decision for Identification of usage of cryptographic schemes	Yes	
0448 – NIT Technical Decision for Documenting Diffie-Hellman 14 groups	No	Diffie-Hellman group 14 is not selected.
0447 – NIT Technical Decision for Using 'diffie'hellman-group-exchange-sha256' in FCS_SSHC/S_EXT.1.7	No	FCS_SSHC/S_EXT is not claimed.
0425 – NIT Technical Decision for Cut-and-paste Error for Guidance AA	Yes	
0424 – NIT Technical Decision for NDcPP v2.1 Clarification – FCS_SSHC/S_EXT.1.5	No	SSH is not included in the evaluation.
0423 – NIT Technical Decision for Clarification about application of RFI#201726rev2	Yes	
0412 – NIT Technical Decision for FCS_SSHS_EXT.1.5 SFR and AA discrepancy	No	FCS_SSHS_EXT is not claimed.
0411 – NIT Technical Decision for FCS_SSHC_EXT.1.5, Test 1 – Server and client side seem to be confused	No	FCS_SSHC_EXT is not claimed.

Identifier	Applicable	Exclusion Rationale (if applicable)
0410 – NIT Technical Decision for Redundant assurance activities associated with FAU_GEN.1	Yes	
0409 – NIT Technical Decision for Applicability of FIA_AFL.1 to key-based SSH authentication	Yes	
0408 – NIT Technical Decision for local vs. remote administrator accounts	Yes	
0407 – NIT Technical Decision for handling Certification of Cloud Deployments	Yes	
0402 – NIT Technical Decision for RSA-based FCS_CKM.2 Selection	Yes	
0401 – NIT Technical Decision for Reliance on external severs to meet SFRs	Yes	
0400 – NIT Technical Decision for FCS_CKM.2 and elliptic curve-based key establishment	Yes	
0399 – NIT Technical Decision for Manual installation of CRL (FIA_X509_EXT.2)	Yes	
0398 – NIT Technical Decision for FCS_SSH*EXT.1.1 RFCs for AES-CTR	No	SSH is not included in the evaluation.
0397 – NIT Technical Decision for Fixing AES-CTR Mode Tests	Yes	
0396 – NIT Technical Decision for FCS_TLSC_EXT.1.1, Test 2	Yes	
0395 – NIT Technical Decision for Different Handling of TLS 1.1 and TLS 1.2	Yes	

Table 8 Technical Decisions

3 Security Problem Definition

The security problem definition has been taken from [NDcPP] and is reproduced here for the convenience of the reader. The security problem is described in terms of the threats that the TOE is expected to address, assumptions about the operational environment, and any organizational security policies that the TOE is expected to enforce.

3.1 Threats

The following threats are drawn directly from the [NDcPP].

ID	Threat
T.UNAUTHORIZED_ADMINISTRATOR_ACCESS	Threat agents may attempt to gain administrator access to the network device by nefarious means such as masquerading as an administrator to the device, masquerading as the device to an administrator, replaying an administrative session (in its entirety, or selected portions), or performing man-in-the-middle attacks, which would provide access to the administrative session, or sessions between network devices. Successfully gaining administrator access allows malicious actions that compromise the security functionality of the device and the network on which it resides.
T.WEAK_CRYPTOGRAPHY	Threat agents may exploit weak cryptographic algorithms or perform a cryptographic exhaust against the key space. Poorly chosen encryption algorithms, modes, and key sizes will allow attackers to compromise the algorithms, or brute force exhaust the key space and give them unauthorized access allowing them to read, manipulate and/or control the traffic with minimal effort.
T.UNTRUSTED_COMMUNICATION_CHANNELS	Threat agents may attempt to target network devices that do not use standardized secure tunneling protocols to protect the critical network traffic. Attackers may take advantage of poorly designed protocols or poor key management to successfully perform man-in-the-middle attacks, replay attacks, etc. Successful attacks will result in loss of confidentiality and integrity of the critical network traffic, and potentially could lead to a compromise of the network device itself.
T.WEAK_AUTHENTICATION_ENDPOINTS	Threat agents may take advantage of secure protocols that use weak methods to authenticate the endpoints – e.g. a shared password that is guessable or transported as plaintext. The consequences are the same as a poorly designed protocol, the attacker could masquerade as the Administrator or another device, and the attacker could insert themselves into the network stream and perform a man-in-the-middle attack. The result is the critical network traffic is exposed and there could be a loss of confidentiality and integrity, and potentially the network device itself could be compromised.
T.UPDATE_COMPROMISE	Threat agents may attempt to provide a compromised update of the software or firmware which undermines the security functionality of the device. Non-validated updates or updates validated using non-secure or weak cryptography leave the update firmware vulnerable to surreptitious alteration.

T.UNDETECTED_ACTIVITY	Threat agents may attempt to access, change, and/or modify the security functionality of the network device without administrator awareness. This could result in the attacker finding an avenue (e.g., misconfiguration, flaw in the product) to compromise the device and the administrator would have no knowledge that the device has been compromised.
T.SECURITY_FUNCTIONALITY_COMPROMISE	Threat agents may compromise credentials and device data enabling continued access to the network device and its critical data. The compromise of credentials includes replacing existing credentials with an attacker's credentials, modifying existing credentials, or obtaining the administrator or device credentials for use by the attacker.
T.PASSWORD_CRACKING	Threat agents may be able to take advantage of weak administrative passwords to gain privileged access to the device. Having privileged access to the device provides the attacker unfettered access to the network traffic, and may allow them to take advantage of any trust relationships with other network devices.
T.SECURITY_FUNCTIONALITY_FAILURE	An external, unauthorized entity could make use of failed or compromised security functionality and might therefore subsequently use or abuse security functions without prior authentication to access, change or modify device data, critical network traffic or security functionality of the device.

Table 9 Threats

3.2 Assumptions

The following assumptions are drawn directly from the [NDcPP].

ID	Assumption
A.PHYSICAL_PROTECTION	The network device is assumed to be physically protected in its operational environment and not subject to physical attacks that compromise the security and/or interfere with the device's physical interconnections and correct operation. This protection is assumed to be sufficient to protect the device and the data it contains. As a result, the cPP will not include any requirements on physical tamper protection or other physical attack mitigations. The cPP will not expect the product to defend against physical access to the device that allows unauthorized entities to extract data, bypass other controls, or otherwise manipulate the device.
A.LIMITED_FUNCTIONALITY	The device is assumed to provide networking functionality as its core function and not provide functionality/services that could be deemed as general purpose computing. For example, the device should not provide computing platform for general purpose applications (unrelated to networking functionality).
A.NO_THRU_TRAFFIC_PROTECTION	A standard/generic network device does not provide any assurance regarding the protection of traffic that traverses it. The intent is for the network device to protect data that originates on or is destined to the device itself, to include administrative data and audit data. Traffic that is traversing the network device, destined for another network entity, is not covered by the ND cPP. It is assumed that this protection will be covered by cPPs and PP-Modules for particular types of network devices (e.g, firewall).

A.TRUSTED_ADMINISTRATOR	The Security Administrator(s) for the network device are assumed to be trusted and to act in the best interest of security for the organization. This includes being appropriately trained, following policy, and adhering to guidance documentation. Administrators are trusted to ensure passwords/credentials have sufficient strength and entropy and to lack malicious intent when administering the device. The network device is not expected to be capable of defending against a malicious administrator that actively works to bypass or compromise the security of the device. For TOEs supporting X.509v3 certificate-based authentication, the Security Administrator(s) are expected to fully validate (e.g. offline verification) any CA certificate (root CA certificate or intermediate CA certificate) loaded into the TOE's trusted source (aka 'root store', 'trusted CA Key Store', or similar) as a trust anchor prior to use (e.g. offline verification).
A.REGULAR_UPDATES	The network device firmware and software is assumed to be updated by an administrator on a regular basis in response to the release of product updates due to known vulnerabilities.
A.ADMIN_CREDENTIALS_SECURE	The administrator's credentials (private key) used to access the network device are protected by the platform on which they reside.
A.COMPONENTS_RUNNING (applies to distributed TOEs only)	For distributed TOEs it is assumed that the availability of all TOE components is checked as appropriate to reduce the risk of an undetected attack on (or failure of) one or more TOE components. It is also assumed that in addition to the availability of all components it is also checked as appropriate that the audit functionality is running properly on all TOE components.
A.RESIDUAL_INFORMATION	The Administrator must ensure that there is no unauthorized access possible for sensitive residual information (e.g. cryptographic keys, keying material, PINs, passwords etc.) on networking equipment when the equipment is discarded or removed from its operational environment.

Table 10 Assumptions

3.3 Organizational Security Policies

The following Organizational Security Policies are drawn directly from the [NDcPP].

ID	OSP
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.

Table 11 OSPs

4 Security Objectives

The security objectives have been taken from [NDcPP] and are reproduced here for the convenience of the reader.

4.1 Security Objectives for the Operational Environment

The following security objectives for the operational environment assist the TOE in correctly providing its security functionality. These track with the assumptions about the environment.

ID	Objective for the Operation Environment
OE.PHYSICAL	Physical security, commensurate with the value of the TOE and the data it contains, is provided by the environment.
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.
OE.NO_THRU_TRAFFIC_PROTECTION	The TOE does not provide any protection of traffic that traverses it. It is assumed that protection of this traffic will be covered by other security and assurance measures in the operational environment.
OE.TRUSTED_ADMIN	TOE Security Administrators are trusted to follow and apply all guidance documentation in a trusted manner. For TOEs supporting X.509v3 certificate-based authentication, the Security Administrator(s) are assumed to monitor the revocation status of all certificates in the TOE's trust store and to remove any certificate from the TOE's trust store in case such certificate can no longer be trusted.
OE.UPDATES	The TOE firmware and software is updated by an administrator on a regular basis in response to the release of product updates due to known vulnerabilities.
OE.ADMIN_CREDENTIALS_SECURE	The administrator's credentials (private key) used to access the TOE must be protected on any other platform on which they reside.
OE.COMPONENTS_RUNNING (applies to distributed TOEs only)	For distributed TOEs the Security Administrator ensures that the availability of every TOE component is checked as appropriate to reduce the risk of an undetected attack on (or failure of) one or more TOE components. The Security Administrator also ensures that it is checked as appropriate for every TOE component that the audit functionality is running properly.
OE.RESIDUAL_INFORMATION	The Security Administrator ensures that there is no unauthorized access possible for sensitive residual information (e.g. cryptographic keys, keying material, PINs, passwords etc.) on networking equipment when the equipment is discarded or removed from its operational environment.

Table 12 Objectives for the Operational Environment

5 Security Requirements

This section identifies the Security Functional Requirements for the TOE. The Security Functional Requirements included in this section are derived from Part 2 of the Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 5, dated: April 2017 and all international interpretations.

Requirement	Description
FAU_GEN.1	Audit data generation
FAU_GEN.2	User identity association
FAU_STG_EXT.1	Protected Audit Event Storage
FCS_CKM.1	Cryptographic Key Generation
FCS_CKM.2	Cryptographic Key Establishment
FCS_CKM.4	Cryptographic Key Destruction
FCS_COP.1/DataEncryption	Cryptographic Operation (AES Data Encryption/Decryption)
FCS_COP.1/SigGen	Cryptographic Operation (Signature Generation and Verification)
FCS_COP.1/Hash	Cryptographic Operation (Hash Algorithm)
FCS_COP.1/KeyedHash	Cryptographic Operation (Keyed Hash Algorithm)
FCS_HTTPS_EXT.1	HTTPS Protocol
FCS_RBG_EXT.1	Random Bit Generation
FCS_TLSC_EXT.1	TLS Client Protocol
FCS_TLSS_EXT.2	TLS Server Protocol with mutual authentication
FIA_AFL.1	Authentication Failure Management
FIA_PMG_EXT.1	Password Management
FIA_UIA_EXT.1	User Identification and Authentication
FIA_UAU_EXT.2	Password-based Authentication Mechanism
FIA_UAU.7	Protected Authentication Feedback
FIA_X509_EXT.1/Rev	X.509 Certificate Validation
FIA_X509_EXT.2	X.509 Certificate Authentication
FIA_X509_EXT.3	X.509 Certificate Requests
FMT_MOF.1/Functions	Management of security functions behavior
FMT_MOF.1/ManualUpdate	Management of security functions behaviour
FMT_MTD.1/CoreData	Management of TSF Data
FMT_MTD.1/CryptoKeys	Management of TSF data
FMT_SMF.1	Specification of Management Functions
FMT_SMR.2	Restrictions on security roles
FPT_SKP_EXT.1	Protection of TSF Data (for reading of all pre-shared, symmetric and private keys)
FPT_APW_EXT.1	Protection of Administrator Passwords
FPT_TST_EXT.1	TSF Testing
FPT_TUD_EXT.1	Trusted Update
FPT_STM_EXT.1	Reliable Time Stamps
FTA_SSL_EXT.1	TSF-initiated Session Locking
FTA_SSL.3	TSF-initiated Termination
FTA_SSL.4	User-initiated Termination
FTA_TAB.1	Default TOE Access Banner
FTP_ITC.1	Inter-TSF trusted channel

FTP_TRP.1/Admin	Trusted Path

Table 13 SFRs

5.1 Conventions

The CC defines operations on Security Functional Requirements: assignments, selections, assignments within selections and refinements. This document follows the conventions used in NDcPP v2.1 in order to comply with exact conformance. Within selections and assignments made in the ST the following font conventions to identify the operations defined by the CC:

- Assignment: Indicated with [*italicized*] text;
- Refinement: Indicated with **bold** text;
- Selection: Indicated with [underlined] text;
- Selection within a selection: Indicated by an additional set of [brackets];
- Iteration: Indicated by appending the iteration identifier after a slash, e.g., /SigGen.
- Where operations were completed in the PP itself, the formatting used in the PP has been retained.

Extended SFRs are identified by having a label 'EXT' after the requirement name. Formatting conventions outside of operations matches the formatting specified within the PP.

5.2 Security Functional requirements

5.2.1 Security Audit (FAU)

5.2.1.1 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 comprising:*

- *Administrative login and logout (name of user account shall be logged if individual user accounts are required for Administrators).*
- *Changes to TSF data related to configuration changes (in addition to the information that a change occurred it shall be logged what has been changed).*
- *Generating/import of, changing, or deleting of cryptographic keys (in addition to the action itself a unique key name or key reference shall be logged).*
- *Resetting passwords (name of related user account shall be logged).*
- [[*no other actions*]]*;*

d) *Specifically defined auditable events listed in Table 14*.

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 cPP/ST, *information specified in column three of Table 14*.

Requirement	Auditable Events	Additional Audit Record Contents
FAU_GEN.1	None.	None.
FAU_GEN.2	None.	None.
FAU_STG_EXT.1	None.	None.
FCS_CKM.1	None.	None.
FCS_CKM.2	None.	None.
FCS_CKM.4	None.	None.
FCS_COP.1/DataEncryption	None.	None.
FCS_COP.1/SigGen	None.	None.
FCS_COP.1/Hash	None.	None.
FCS_COP.1/KeyedHash	None.	None.
FCS_HTTPS_EXT.1	Failure to establish a HTTPS Session.	Reason for failure
FCS_RBG_EXT.1	None.	None.
FCS_TLSC_EXT.1	Failure to establish a TLS Session	Reason for failure
FCS_TLSS_EXT.2	Failure to establish a TLS Session	Reason for failure
FIA_AFL.1	Unsuccessful login attempts limit is met or exceeded.	Origin of the attempt (e.g., IP address).
FIA_PMG_EXT.1	None.	None.
FIA_UIA_EXT.1	All use of identification and authentication mechanism.	Origin of the attempt (e.g., IP address).
FIA_UAU_EXT.2	All use of identification and authentication mechanism.	Origin of the attempt (e.g., IP address).
FIA_UAU.7	None.	None.
FIA_X509_EXT.1/Rev	Unsuccessful attempt to validate a certificate Any addition, replacement or removal of trust anchors in the TOE's trust store.	Reason for failure of certificate validation Identification of certificates added, replaced or removed as trust anchor in the TOE's trust store
FIA_X509_EXT.2	None	None
FIA_X509_EXT.3	None.	None.
FMT_MOF.1/Functions	None.	None.
FMT_MOF.1/ManualUpdate	Any attempt to initiate a manual update	None.
FMT_MTD.1/CoreData	None.	None.
FMT_MTD.1/CryptoKeys	Management of cryptographic keys.	None.
FMT_SMF.1	All management activities of TSF data.	None.
FMT_SMR.2	None.	None.
FPT_SKP_EXT.1	None.	None.
FPT_APW_EXT.1	None.	None.
FPT_TST_EXT.1	None.	None.

Requirement	Auditable Events	Additional Audit Record Contents
FPT_TUD_EXT.1	Initiation of update; result of the update attempt (success or failure)	None.
FPT_STM_EXT.1	Discontinuous changes to time - either Administrator actuated or changed via an automated process. (Note that no continuous changes to time need to be logged. See also application note on FPT_STM_EXT.1)	For discontinuous changes to time: The old and new values for the time. Origin of the attempt to change time for success and failure (e.g., IP address).
FTA_SSL_EXT.1 (if "terminate the session" is selected)	The termination of a local session by the session locking mechanism.	None.
FTA_SSL.3	The termination of a remote session by the session locking mechanism.	None.
FTA_SSL.4	The termination of an interactive session.	None.
FTA_TAB.1	None.	None.
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.
FTP_TRP.1/Admin	Initiation of the trusted path. Termination of the trusted path. Failure of the trusted path functions.	None.

Table 14 Security Functional Requirements and Auditable Events

5.2.1.2 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.

5.2.1.3 FAU_STG_EXT.1 Protected Audit Event 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 according to FTP_ITC.1.

FAU_STG_EXT.1.2

The TSF shall be able to store generated audit data on the TOE itself. [

- TOE shall consist of a single standalone component that stores audit data locally.]

FAU_STG_EXT.1.3

The TSF shall [overwrite previous audit records according to the following rule: [*on a circular (FIFO) bases*]] when the local storage space for audit data is full.

5.2.2 Cryptographic Support (FCS)

5.2.2.1 FCS_CKM.1 Cryptographic Key Generation

FCS_CKM.1.1

The TSF shall generate **asymmetric** cryptographic keys in accordance with a specified cryptographic key generation algorithm: [

- RSA schemes using cryptographic key sizes of 2048-bit or greater that meet the following: FIPS PUB 186-4, "Digital Signature Standard (DSS)", Appendix B.3;
- ECC schemes using "NIST curves" [P-256, P-384] that meet the following: FIPS PUB 186-4, "Digital Signature Standard (DSS)", Appendix B.4;

] ~~and specified cryptographic key sizes [assignment: *cryptographic key sizes*] that meet the following: [assignment: *list of standards*]~~.

5.2.2.2 FCS_CKM.2 Cryptographic Key Establishment

FCS_CKM.2.1

The TSF shall **perform** cryptographic **key establishment** in accordance with a specified cryptographic key **establishment** method: [

- RSA-based key establishment schemes that meet the following: RSAES-PKCS1-v1_5 as specified in Section 7.2 of RFC 3447, "Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specification Version 2.1";
- Elliptic curve-based key establishment schemes that meet the following: NIST Special Publication 800-56A Revision 2, "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography";

] ~~that meets the following: [assignment: *list of standards*]~~.

ST Application Note
FCS_CKM.2 was updated based on TD0402.

5.2.2.3 FCS_CKM.4 Cryptographic Key Destruction

FCS_CKM.4.1

The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method

- *For plaintext keys in volatile storage, the destruction shall be executed by a* [single overwrite consisting of [zeroes]]*;*
- *For plaintext keys in non-volatile storage, the destruction shall be executed by the invocation of an interface provided by a part of the TSF that:*[
    - logically addresses the storage location of the key and performs a [single] overwrite consisting of [zeros]]*;*

that meets the following: *No Standard*.

5.2.2.4 FCS_COP.1/DataEncryption Cryptographic Operation (AES Data Encryption/Decryption)

FCS_COP.1.1/DataEncryption

The TSF shall perform *encryption/decryption* in accordance with a specified cryptographic algorithm *AES used in* [CBC, GCM] *mode* and cryptographic key sizes [128 bits, 256 bits] that meet the following: *AES as specified in ISO 18033-3*, [CBC as specified in ISO 10116, GCM as specified in ISO 19772].

5.2.2.5 FCS_COP.1/SigGen Cryptographic Operation (Signature Generation and Verification)

FCS_COP.1.1/SigGen

The TSF shall perform *cryptographic signature services (generation and verification)* in accordance with a specified cryptographic algorithm [

- RSA Digital Signature Algorithm and cryptographic key sizes (modulus) [*2048 bits, 3072 bits*]

]

that meet the following: [

- For RSA schemes: FIPS PUB 186-4, "Digital Signature Standard (DSS)", Section 5.5, using PKCS #1 v2.1 Signature Schemes RSASSA-PSS and/or RSASSA-PKCS1v1_5; ISO/IEC 9796-2, Digital signature scheme 2 or Digital Signature scheme 3,]

5.2.2.6 FCS_COP.1/Hash Cryptographic Operation (Hash Algorithm)

FCS_COP.1.1/Hash

The TSF shall perform *cryptographic hashing services* in accordance with a specified cryptographic algorithm [SHA-1, SHA-256, SHA-384] ~~and cryptographic key sizes [*assignment: cryptographic key sizes*~~] and **message digest sizes [160, 256, 384] bits** that meet the following: *ISO/IEC 10118-3:2004*.

5.2.2.7 FCS_COP.1/KeyedHash Cryptographic Operation (Keyed Hash Algorithm)

FCS_COP.1.1/KeyedHash

The TSF shall perform *keyed-hash message authentication* in accordance with a specified cryptographic algorithm [HMAC-SHA-1,HMAC-SHA-256, HMAC-SHA-384] and cryptographic key sizes [*160 bits, 256 bits, and 384 bits used in HMAC*] **and message digest sizes [160, 256, 384] bits** that meet the following: *ISO/IEC 9797-2:2011, Section 7 "MAC Algorithm 2"*.

5.2.2.8 FCS_HTTPS_EXT.1 HTTPS Protocol

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.

FCS_HTTPS_EXT.1.3

If a peer certificate is presented, the TSF shall [not establish the connection] if the peer certificate is deemed invalid.

5.2.2.9 FCS_RBG_EXT.1 Random Bit Generation

FCS_RBG_EXT.1.1

The TSF shall perform all deterministic random bit generation services in accordance with ISO/IEC 18031:2011 using [CTR_DRBG (AES)].

FCS_RBG_EXT.1.2

The deterministic RBG shall be seeded by at least one entropy source that accumulates entropy from [[*two*] software-based noise source] with a minimum of [256 bits] of entropy at least equal to the greatest security strength, according to ISO/IEC 18031:2011 Table C.1 "Security Strength Table for Hash Functions", of the keys and hashes that it will generate.

5.2.2.10 FCS_TLSC_EXT.1 TLS Client Protocol

FCS_TLSC_EXT.1.1

The TSF shall implement [TLS 1.2 (RFC 5246)] and reject all other TLS and SSL versions. The TLS implementation will support the following ciphersuites: [

- TLS_RSA_WITH_AES_128_CBC_SHA as defined in RFC 3268
- TLS_RSA_WITH_AES_256_CBC_SHA as defined in RFC 3268
- TLS_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5246
- TLS_RSA_WITH_AES_256_CBC_SHA256 as defined in RFC 5246
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289

].

FCS_TLSC_EXT.1.2

The TSF shall verify that the presented identifiers of the following types: [identifiers defined in RFC 6125] are matched to reference identifiers.

ST Application Note
FCS_TLSC_EXT1.2 was updated based on TD0452.

FCS_TLSC_EXT.1.3

When establishing a trusted channel, by default the TSF shall not establish a trusted channel if the server certificate is invalid. The TSF shall also [

- Not implement any administrator override mechanism

].

FCS_TLSC_EXT.1.4

The TSF shall [present the Supported Elliptic Curves Extension with the following NIST curves: [secp256r1, secp384r1] and no other curves] in the Client Hello.

5.2.2.11 FCS_TLSS_EXT.2 TLS Server Protocol with mutual authentication

FCS_TLSS_EXT.2.1

The TSF shall implement [TLS 1.2 (RFC 5246)] and reject all other TLS and SSL versions. The TLS implementation will support the following ciphersuites:[

- TLS_RSA_WITH_AES_128_CBC_SHA as defined in RFC 3268
- TLS_RSA_WITH_AES_256_CBC_SHA as defined in RFC 3268
- TLS_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5246
- TLS_RSA_WITH_AES_256_CBC_SHA256 as defined in RFC 5246
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289

].

FCS_TLSS_EXT.2.2

The TSF shall deny connections from clients requesting SSL 2.0, SSL 3.0, TLS 1.0 and [TLSv1.1].

FCS_TLSS_EXT.2.3

The TSF shall [perform RSA key establishment with key size [2048 bits], generate EC Diffie-Hellman parameters over NIST curves [secp256r1, secpr384r1] and no other curves].

FCS_TLSS_EXT.2.4

The TSF shall support mutual authentication of TLS clients using X.509v3 certificates.

FCS_TLSS_EXT.2.5

When establishing a trusted channel, by default the TSF shall not establish a trusted channel if the client certificate is invalid. The TSF shall also [

- Not implement any administrator override mechanism

].

FCS_TLSS_EXT.2.6

The TSF shall not establish a trusted channel if the distinguished name (DN) or Subject Alternative Name (SAN) contained in a certificate does not match the expected identifier for the client.

5.2.3 Identification and Authentication (FIA)

5.2.3.1 FIA_AFL.1 Authentication Failure Management

FIA_AFL.1.1

The TSF shall detect when an Administrator configurable positive integer within [*3 to 20*] unsuccessful authentication attempts occur related to *Administrators attempting to authenticate remotely using a password*.

FIA_AFL.1.2

When the defined number of unsuccessful authentication attempts has been met, the TSF shall [prevent the offending Administrator from successfully establishing remote session using any authentication method that involves a password until [*unlocking the offending Administrator*] is taken by an Administrator].

ST Application Note
FIA_AFL.1 was updated based on TD0408.

5.2.3.2 FIA_PMG_EXT.1 Password Management

FIA_PMG_EXT.1.1

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

a) Passwords shall be able to be composed of any combination of upper and lower case letters, numbers, and the following special characters: [“!”; “@”; “#”; “$”; “%”; “^”; “&”; “*”; “(“; “)”; [*“~”, “`”, “_”, “-”, “+”, “=”, “{”, “[”, “}”, “]”, “|”, “\”, “:”, “;”, (”), (’), “<”, “,”, “>”, “.”, “?”, “/”, (space)*]];
b) Minimum password length shall be configurable to between [*15*] and [*20*] characters.

5.2.3.3 FIA_UIA_EXT.1 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;
- [*Respond to ICMP Echo messages with an ICMP Echo Reply message*].

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.

5.2.3.4 FIA_UAU_EXT.2 Password-based Authentication Mechanism

FIA_UAU_EXT.2.1

The TSF shall provide a local [password-based] authentication mechanism to perform local administrative user authentication.

ST Application Note
FIA_UAU_EXT.2.1 was updated based on TD0408.

5.2.3.5 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**.

5.2.3.6 FIA_X509_EXT.1/Rev X.509 Certificate Validation

FIA_X509_EXT.1.1/Rev

The TSF shall validate certificates in accordance with the following rules:

- RFC 5280 certificate validation and certificate path validation **supporting a minimum path length of three certificates**.
- The certificate path must terminate with a trusted CA certificate designated as a trust anchor.

- The TSF shall validate a certification path by ensuring that all CA certificates in the certification path contain the basicConstraints extension with the CA flag set to TRUE.
- The TSF shall validate the revocation status of the certificate using [a Certificate Revocation List (CRL) as specified in RFC 5280 Section 6.3].
- The TSF shall validate the extendedKeyUsage field according to the following rules:
    - *Certificates used for trusted updates and executable code integrity verification shall have the Code Signing purpose (id-kp 3 with OID 1.3.6.1.5.5.7.3.3) in the extendedKeyUsage field.*
    - *Server certificates presented for TLS shall have the Server Authentication purpose (id-kp 1 with OID 1.3.6.1.5.5.7.3.1) in the extendedKeyUsage field.*
    - *Client certificates presented for TLS shall have the Client Authentication purpose (id-kp 2 with OID 1.3.6.1.5.5.7.3.2) in the extendedKeyUsage field.*
    - *OCSP certificates presented for OCSP responses shall have the OCSP Signing purpose (id-kp 9 with OID 1.3.6.1.5.5.7.3.9) in the extendedKeyUsage field.*

FIA_X509_EXT.1.2/Rev

The TSF shall only treat a certificate as a CA certificate if the basicConstraints extension is present and the CA flag is set to TRUE.

5.2.3.7 FIA_X509_EXT.2 X.509 Certificate Authentication

FIA_X509_EXT.2.1

The TSF shall use X.509v3 certificates as defined by RFC 5280 to support authentication for [HTTPS, TLS], and [no additional uses].

FIA_X509_EXT.2.2

When the TSF cannot establish a connection to determine the validity of a certificate, the TSF shall [not accept the certificate].

5.2.3.8 FIA_X509_EXT.3 X.509 Certificate Requests

FIA_X509_EXT.3.1

The TSF shall generate a Certificate Request as specified by RFC 2986 and be able to provide the following information in the request: public key and [Common Name, Organization, Organizational Unit, Country].

FIA_X509_EXT.3.2

The TSF shall validate the chain of certificates from the Root CA upon receiving the CA Certificate Response.

5.2.4 Security Management (FMT)

5.2.4.1 FMT_MOF.1/Functions Management of security functions behavior

FMT_MOF.1/Functions

The TSF shall restrict the ability to [modify the behavior of] the functions [transmission of audit data to an external IT entity] to *Security Administrators.*

5.2.4.2 FMT_MOF.1/ManualUpdate Management of security functions behaviour

FMT_MOF.1.1/ManualUpdate

The TSF shall restrict the ability to enable the functions *to perform manual updates* to *Security Administrators*.

5.2.4.3 FMT_MTD.1/CoreData Management of TSF Data

FMT_MTD.1.1/CoreData

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

5.2.4.4 FMT_MTD.1/CryptoKeys Management of TSF Data

FMT_MTD.1.1/CryptoKeys

The TSF shall restrict the ability to *manage* the *cryptographic keys* to *Security Administrators*.

5.2.4.5 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 configure the access banner;*
- *Ability to configure the session inactivity time before session termination or locking;*
- *Ability to update the TOE, and to verify the updates using* [digital signature] *capability prior to installing those updates;*
- *Ability to configure the authentication failure parameters for FIA_AFL.1;*
- [
    - Ability to configure audit behaviour;
    - Ability to manage cryptographic keys;
    - Ability to re-enable an Administrator account;
    - Ability to set the time which is used for time-stamps;
    - Ability to import X.509v3 certificates to the TOE's trust store].

5.2.4.6 FMT_SMR.2 Restrictions on security roles

FMT_SMR.2.1

The TSF shall maintain the roles:

- *Security 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

- *The Security Administrator role shall be able to administer the TOE locally;*

- *The Security Administrator role shall be able to administer the TOE remotely*

are satisfied.

5.2.5 Protection of the TSF (FPT)

5.2.5.1 FPT_SKP_EXT.1 Protection of TSF Data (for reading of all pre-shared, symmetric and private keys)

FPT_SKP_EXT.1.1

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

5.2.5.2 FPT_APW_EXT.1 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.

5.2.5.3 FPT_TST_EXT.1 TSF Testing

FPT_TST_EXT.1.1

The TSF shall run a suite of the following self-tests [during initial start-up (on power on)] to demonstrate the correct operation of the TSF: [

- *firmware integrity check that compares the SHA256 checksum of the loaded firmware with a permanently stored hash value;*
- *Presence of certificate and public key files*
- *Cryptographic library tests:*
    - *SHA-256 KAT*
    - *HMAC-SHA-256 KAT*
    - *AES 128 GCM Encrypt and Decrypt KAT*
    - *AES 128 Encrypt and Decrypt KAT*
    - *RSA 2048 SHA-256 Sign and Verify KAT*
    - *ECDSA key generation Pairwise Consistency Test*
    - *DRBG AES-CTR-256 KAT (invoking the instantiate, reseed, and generate functions)*

].

5.2.5.4 FPT_TUD_EXT.1 Trusted Update

FPT_TUD_EXT.1.1

The TSF shall provide *Security Administrators* the ability to query the currently executing version of the TOE firmware/software and [no other TOE firmware/software version].

FPT_TUD_EXT.1.2

The TSF shall provide *Security Administrators* the ability to manually initiate updates to TOE firmware/software and [no other update mechanism].

FPT_TUD_EXT.1.3

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

5.2.5.5 FPT_STM_EXT.1 Reliable Time Stamps

FPT_STM_EXT.1.1

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

FPT_STM_EXT.1.2

The TSF shall [allow the Security Administrator to set the time].

5.2.6 TOE Access (FTA)

5.2.6.1 FTA_SSL_EXT.1 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.

5.2.6.2 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*.

5.2.6.3 FTA_SSL.4 User-initiated Termination

FTA_SSL.4.1

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

5.2.6.4 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.

5.2.7 Trusted path/channels (FTP)

5.2.7.1 FTP_ITC.1 Inter-TSF trusted channel

FTP_ITC.1.1

The TSF shall **be capable of using [TLS] to** provide a trusted communication channel between itself and **authorized IT entities supporting the following capabilities: audit server, [[*video switch control system (such as Evertz MAGNUM)*]]** 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 [*auditing services and video switch control*].

5.2.7.2 FTP_TRP.1/Admin Trusted Path

FTP_TRP.1.1/Admin

The TSF shall **be capable of using [TLS, HTTPS] to** provide a communication path between itself and **authorized** 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 provides detection of modification of the channel data.**

FTP_TRP.1.2/Admin

The TSF shall permit remote **Administrators** to initiate communication via the trusted path.

FTP_TRP.1.3/Admin

The TSF shall require the use of the trusted path for *initial Administrator authentication and all remote administration actions*.

5.3 TOE SFR Dependencies Rationale for SFRs

[NDcPP] contains all the requirements claimed in this Security Target. As such, the dependencies are not applicable since the PP has been approved.

5.4 Security Assurance Requirements

The TOE assurance requirements for this ST are taken directly from [NDcPP] which are derived from Common Criteria Version 3.1, Revision 5. The assurance requirements are summarized in the table below.

Assurance Class	Components	Components Description
Development	ADV_FSP.1	Basic Functional Specification
Guidance Documents	AGD_OPE.1	Operational User Guidance
	AGD_PRE.1	Preparative User Guidance
Life Cycle Support	ALC_CMC.1	Labeling of the TOE
	ALC_CMS.1	TOE CM Coverage
Tests	ATE_IND.1	Independent Testing – Conformance
Vulnerability Assessment	AVA_VAN.1	Vulnerability Analysis

Table 15 Security Assurance Requirements

5.5 Rationale for Security Assurance Requirements

The functional specification describes the external interfaces of the TOE; such as the means for a user to invoke a service and the corresponding response of those services. The description includes the interface(s) that enforces a security functional requirement, the interface(s) that supports the enforcement of a security functional requirement, and the interface(s) that does not enforce any

security functional requirements. The interfaces are described in terms of their purpose (general goal of the interface), method of use (how the interface is to be used), parameters (explicit inputs to and outputs from an interface that control the behavior of that interface), parameter descriptions (tells what the parameter is in some meaningful way), and error messages (identifies the condition that generated it, what the message is, and the meaning of any error codes). The development evidence also contains a tracing of the interfaces to the SFRs described in this ST.

5.6 Assurance Measures

The TOE satisfies the identified assurance requirements. This section identifies the Assurance Measures applied by Evertz to satisfy the assurance requirements. The table below lists the details.

SAR Component	How the SAR will be met
ADV_FSP.1	The functional specification describes the external interfaces of the TOE; such as the means for a user to invoke a service and the corresponding response of those services. The description includes the interface(s) that enforces a security functional requirement, the interface(s) that supports the enforcement of a security functional requirement, and the interface(s) that does not enforce any security functional requirements. The interfaces are described in terms of their purpose (general goal of the interface), method of use (how the interface is to be used), parameters (explicit inputs to and outputs from an interface that control the behavior of that interface), parameter descriptions (tells what the parameter is in some meaningful way), and error messages (identifies the condition that generated it, what the message is, and the meaning of any error codes).
AGD_OPE.1	The Administrative Guide provides the descriptions of the processes and procedures of how the administrative users of the TOE can securely administer the TOE using the interfaces that provide the features and functions detailed in the guidance.
AGD_PRE.1	The Installation Guide describes the installation, generation, and startup procedures so that the users of the TOE can put the components of the TOE in the evaluated configuration.
ALC_CMC.1 ALC_CMS.1	The Configuration Management (CM) documents describe how the consumer identifies the evaluated TOE. The CM documents identify the configuration items, how those configuration items are uniquely identified, and the adequacy of the procedures that are used to control and track changes that are made to the TOE. This includes details on what changes are tracked and how potential changes are incorporated.
ATE_IND.1	Evertz Microsystems will provide the TOE for testing.
AVA_VAN.1	Evertz Microsystems will provide the TOE for testing. Evertz Microsystems will provide a document identifying the list of software and hardware components.

Table 16 TOE Security Assurance Measures

6 TOE Summary Specification

This chapter identifies and describes how the Security Functional Requirements identified above are met by the TOE.

TOE SFR	Rationale
FAU_GEN.1 FAU_GEN.2	Audit records are created when an auditable event that belongs to a set of predefined events had occurred. The set of auditable events can be sub-categorized into functional events and access events. Audit records are stored in log files in plaintext. Each entry contains a timestamp of when the event had occurred as well as a message body with description of the event. Log entries are sorted based on chronological order. The TSF generates audit records for the following events: • Startup and shutdown of the audit function • Administrative login and logout events • Changes to TSF data related to configuration changes • Generation of a CSR and associated keypair • Installation of a certificate • Resetting passwords • Failure to establish a HTTPS/TLS session • Failure to establish a TLS session • All use of the identification and authentication mechanism (local and remote connections to the TSF) • Unsuccessful attempts to validate a certificate • Initiation of a software update • Result of a software update • Changes to the time • Modification of the behavior of the TSF • Failure of self-tests • Initiation and termination of the trusted channel • Initiation and termination of the trusted path • Attempts to unlock an interactive session • Termination of a session by the session locking mechanism Each audit record includes the date and time, type, subject identity (IP address, hostname, and/or username), the outcome (success or failure), and any additional information specified in column three of Table 14. The TOE only stores one certificate chain to support TLS. No other server certificates are stored. Logs of Administrator actions on keys associated, such as generating or deleting keys, with this certificate will refer to the key as the server private key.
FAU_STG_EXT.1	The TOE is a standalone TOE. IPX stores audit logs internally. The internal logs are stored unencrypted, but they are only accessible (and then read-only) via the web browser, which can only be used by Administrators. Logs information is also sent (using TLS 1.2) to an external Syslog server. The [IPX UG] explains how to configure this connection. Configurations include adding the syslog server IP address/port number and uploading a trusted certificate chain to the TOE. IPX stores all audit data locally in a secure location; it is accessible to administrators using the “Syslog” tab on the web interface. Two files are used, each with a maximum capacity of 900 KB. Initially both files are empty and entries are added to file 1. Once file 1 is full, newer entries will be added to file 2

TOE SFR	Rationale
	until it becomes full, at which time content of file 1 will be cleared and entries added to file 1 again. The TSF implements Syslog over TLS using TLS v1.2. Logs are sent to the Syslog servers in real-time. The trusted channel with the Syslog server is described in greater detail in the FCS_TLSC_EXT.2 description.
FCS_CKM.1	The TSF supports generation of 2048-bit RSA keys for digital signatures in support of TLS sessions (FCS_TLSC_EXT.1 and FCS_TLSS_EXT.2) and the server certificate (FIA_X509_EXT.3). Generation of ECSA keys with NIST curves of P-256 or P-384 are also used to generate EC-DH components for key establishment in TLS sessions (FCS_TLSC_EXT.1 and FCS_TLSS_EXT.2).
FCS_CKM.2	The TOE acts as both sender and recipient for elliptic curve Diffie-Hellman key establishment schemes that meet the following: • NIST Special Publication (SP) 800-56A revision 2, “Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography” – for FCS_TLSC_EXT.1 connections to the audit server and FCS_TLSS_EXT.2 connections to the MAGNUM server. or • RSAES-PKCS1-v1_5 as specified in Section 7.2 of RFC 3447, “Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specification Version 2.1”. The TOE uses RSA-based key establishment for backwards compatibility for FCS_TLSC_EXT.1 connections to audit server and FCS_TLSS_EXT.2 connections to the MAGNUM server. In the case of a decryption error, the TOE response is dependent on the stage of the connection process. If the connection has not been established, the TOE prevents a connection from occurring. If the connection has already been established, the TOE drops the packet(s) in question and logs the error internally. To address the issue of side-channel attacks, the TOE does not reveal the particular error that occurred through other channels, either through message content or timing variations.
FCS_CKM.4	Cryptographic keys are destroyed by first overwriting the key file content with zeros. A read-verification is then performed to ensure that the entire content has really been changed to zeros and not any other values. If these steps fails, then the file will be over-written again with zeros until the read-verify step succeeds. The following keys are stored in plaintext on nonvolatile NOR flash storage: • the trust CA certificate, which is uploaded onto the TOE and used for certificate verification; • the server certificate, which is uploaded onto the TOE and used for HTTP web service and Magnum TLS connection; • the private key matching the server certificate, which is used for de-encryption; No direct interface/access is provided to view or modify the contents of these files. The CLI provides Security Administrators with a menu item to destroy all CSPs, which would initiate key destruction.

TOE SFR	Rationale
	The following keys are stored in plaintext in volatile storage: • TLS session keys No direct interface/access is provided to view or modify the contents of these files. These keys are automatically destroyed when the TLS session ends. The above destruction methods are followed in all configurations and circumstances.
FCS_COP.1/DataEncryption	The TOE provides AES encryption/decryption in CBC or GCM mode with 128- and 256-bit keys.
FCS_COP.1/SigGen	The TOE supports signature generation of RSA 2048-bit and signature verification with RSA (2048- and 3072-, and 4096-bits) with SHA-1/256/384 in accordance with FIPS PUB 186-4. These signatures support TLS authentication and firmware verification. The TOE's server certificate is 2048-bits.
FCS_COP.1/Hash	The TOE implements hashing in byte-oriented mode. The TOE provides cryptographic hashing services in support of TLS for SHA-1, SHA-256 and SHA-384. SHA-256 is used firmware integrity checks during power-on-self-tests and upgrades.
FCS_COP.1/KeyedHash	Keyed-hash message authentication is used as part of TLS protocol as part of the negotiated cipher suites between peers. It is also used for firmware image integrity check where the hashed-value of the images is signed with Evertz's private key and the result file (signature) is included in the firmware package file. During upgrade, the signature file is first decrypted using the public key stored on IPX, then the hashed value is re-calculated from the uploaded image file and then compared with the decrypted hash value. These hashes must match for this validation to succeed. The following keyed-hash message authentication are used by IPX: • HMAC-SHA-1 with 160-bit key, message digest size of 160 bit and 160 bit message block size, • HMAC-SHA-256 with 256-bit keys, message digest sizes of 256 bits, and block size of 512 bits, and • HMAC-SHA-384 with 384-bit keys, message digest sizes of 384 bits, and block size of 1024 bits.
FCS_HTTPS_EXT.1 FCS_TLSS_EXT.2 FCS_TLSC_EXT.1	The TOE acts as a TLS/HTTPS server to provide web access to administrators. The TOE's HTTPS functionality is in accordance with all shall statements in RFC 2818. The TOE acts as a client when connecting to the syslog server and as a server when connecting to a video switch control system. IPX specifies only a restricted set of cipher suites that it supports during the negotiation phase with a client or a server. If no match of cipher suites can be found with peer, TLS session will not be started. These ciphersuites cannot be configured or changed by an Administrator. The following cipher suites are supported: • TLS_RSA_WITH_AES_128_CBC_SHA • TLS_RSA_WITH_AES_256_CBC_SHA • TLS_RSA_WITH_AES_128_CBC_SHA256 • TLS_RSA_WITH_AES_256_CBC_SHA256 • TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 • TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384

TOE SFR	Rationale
	Protocols that do not conform to TLS v1.2 are explicitly excluded in IPX's cipher suites IPX only supports cipher suites that use RSA keys for authentication. These keys are generated with OpenSSL's RSA command line internally to the TSF. Elliptic curve Diffie-Hellman and RSA are supported for key establishment in TLS for both client and server. The RSA key establishment uses 2046bits. EC-DH key establishment uses NIST curves, P-246 and P-384. By default, the TOE presents the supported Elliptic Curve Extensions, secp256r1 and secp384r1 in the Client Hello. The TOE conforms to RFC 5246, section 7.4.3 for key exchange. When validating a client's certificate, IPX uses CRL (certification revocation list) to check for invalid certificates. CRL files which are signed by trusted CA certificated can be imported to IPX. This CRL file will be used by IPX during certificate validation process to check for revocation status of the peer certificates. IPX allows configuration of reference identifier from a peer it expects to connect with before connection is made. The reference identifier can be any string up to 64 bytes that is present in the peer certificate's DN and SAN-DNS field. The verification against peer certificate is implemented within OpenSSL using a bitwise comparison of the DN and SAN-DNS field. IP addresses are not supported as reference identifiers. IPX does not support certificate pinning. IPX supports wildcard in certificates. The wildcard must be in the left-most label of the presented identifier and can only covers one level of subdomains. For the reference identifier without a left-most label as in the certificate, the connection will fail, i.e., awesome.com doesn't match *.awesome.com.
FCS_RBG_EXT.1	The TOE implements a DRBG in accordance with ISO/IEC 18031:2011 using a CTR DRBG with AES. The TSF seed the CTR_DRBG using 384-bits of data that contains at least 256 bits of entropy. The TSF gathers and pools entropy from two software-based noise source: haveged and the Linux Kernel entropy. The entropy sources are discussed in greater detail in the Entropy documentation.
FIA_AFL.1	An administrator can configure the number of unsuccessful attempts a remote administrator can make before a lock-out. The attempts can range between 3 and 20 attempts. The default number of attempts is 10. Each time the user enters an incorrect password a $failedCount variable is incremented. When the $failedCount variable reaches the configured limit, the username becomes locked and any future attempts to authenticate with this username are denied. The username will show the Lockout enabled on the Settings->Users page on the web interface. The user cannot login through any remote interface on the TOE until a different Administrator can log in and unlock the offending Administrator. Non-administrative users do not have a lockout time and can only be unlocked by an Administrator. The TSF also implements an increasing wait time for each unsuccessful login attempt. Lockouts are not enforced on the TOE's console interface. This ensures that authentication failures cannot lead to a situation where no administrator access is available.
FIA_PMG_EXT.1	IPX enforces that passwords must meet minimum length requirements. IPX passwords can be composed of a mix of number, lower/upper case letters, and the following special

TOE SFR	Rationale
	characters *"!"; "@"; "#"; "$"; "%"; "^"; "&"; "*"; "("; ")";"~"; "`"; "_"; "-"; "+"; "="; "{"; "["; "}"; "]"; "|"; "\"; ":"; ";"; ["]; ['];* "<"; ","; ">"; "."; "?"; "/"; *[space]*. At least two characters from each category are required (upper case letter, lower case letter, number special character). Passwords must be at least a minimum length settable by the administrator between 15 and 20 characters.
FIA_UIA_EXT.1 FIA_UAU_EXT.2	The only accounts that the IPX will establish are Security Administrator accounts. Users only control the IPX indirectly via MAGNUM. CO/Administrators are identified and authenticated via username and password prior to performing any operations other than acknowledging the warning banner. The IPX CO/Administrators user accounts module maintains Security Administrator credentials. Since the only role that accesses the IPX directly is that of Security Administrator there is no assignment of roles required. Administrators can logon via the WebEasy interface using HTTPS or locally on the serial port. Both methods use username and password to authenticate the administrator. The Security Administrator is considered authenticated if the username and password match. Prior to successful identification and authentication on all interfaces, the TSF displays the TOE access banner specified in FTA_TAB.1. Responding to ICMP Echo messages with ICMP Echo Reply messages is allowed from the serial interface prior to authentication. Users must acknowledge the warning banner before they can login to the system.
FIA_UAU.7	When the user is entering their password over the local console, the TSF does not echo any characters back.
FIA_X509_EXT.1/Rev	IPX uses OpenSSL for X.509 certificate validation. The certificate path is validated by ensuring that all the CA certificates have the basicConstraints extension and the path must terminate with a trusted CA certificate. The extendedKeyUsage on each certificate is also checked to ensure there is no inappropriate usage. Server certificates must have the Server Authentication purpose, client's certificates must have the Client Authentication purpose. Certificates for code signing and OCSP signing are not used or accepted by the TOE. Each certificate (other than the first certificate) in the certificate chain has the Subject Type=CA flag set. Certificates are not used for any purposes other than establishing TLS sessions. If certificates are uploaded to IPX for its own use those certificates are checked upon upload. When the TOE acts as a server is does not perform verification of it's server certificate. The TOE's client certificate is validated prior to use for authentication as well as upon upload. The certificate presented by remote TLS clients using mutual authentication is validated during the establishment of a TLS connection. For an expired certificate, IPX will deny the connection. IPX also uses CRL to verify whether the certificate or intermediate CA certificate has been revoked. During session establishment with IPX, any byte modification in the certificate will lead to the failure of connection. The TSF verifies the validity of a certificate when: • A TLS client establishes a TLS connection If the Security Administrator loads a certificate with a Subject Type=CA, the TSF does not validate the certificate path.
FIA_X509_EXT.2	Instructions about generating/downloading CSR and loading certificate can be found on IPX manual. The Administrator can only upload one certificate chain, to include a single CA certificate. The same certificate will be used by IPX for both web service and MAGNUM control. The same CA will be used for certificate verification. IPX enforces

TOE SFR	Rationale
	mutual authentication and therefore requires client certificates to establish a connection. If certificate verification fails for any reason (including a failure to establish a connection), the connection attempt fails, and the trusted channel is not established.
FIA_X509_EXT.3	The TSF allows Security Administrators to generate Certificate Signing Requests. The TSF requires the Security Administrator to specify the following values: • Common Name • Organization • Locality • State • Country • Key Length (2048, 3072, 4096) A CSR can be generated from the serial console menu. When validating certificates, each certificate from the chain is sequentially validated, terminating at the root CA. If any invalid certificate is found in this process, the validation fails.
FMT_MOF.1/Functions FMT_MOF.1/ManualUpdate FMT_MTD.1/CoreData FMT_MTD.1/CryptoKeys FMT_SMF.1 FMT_SMR.2	IPX gives the Security Administrator the ability to manage the security functions: auditing operations, administrative user accounts, password and session policies, advisory banners, software updates, as well as cryptographic functions. IPX ensures that only secure values are accepted for security attributes. A Security Administrator can change passwords, and can add, edit and/or delete Security Administrator accounts. The (non-administrative) User has no direct access or control over IPX; a (non-administrative) User may only access an IPX card through MAGNUM. The (non-administrative) User can only view configurations. No administrative functionality is available prior to login. The TSF implements the Security Administrator role to authorized administrators of the TOE. The TSF allows the Security Administrators to administer the TSF via a local CLI and a remote WebEasy interface. The TSF implements role-based access control of these management functions to users that have been identified, authenticated, and authorized with the Security Administrator role. The WebEasy interface and local console allow the Security Administrator to perform the following TSF management functions: • Configure IPX date and time; • Control port IP configuration; • Edit login banner; • Reset certificates; • Import certificates; • Import Trusted CA certificate; • Configure console menu system timeout; • Verify/Install Firmware Updates • View/Edit settings for sending audit data to the Syslog Server • View/Edit authentication failure parameters • Re-enable locked out Administrator accounts The following can only be performed from the local console interfaces: • Login to local console; • Change Linux password for console account “customer”; • Create certificate signing request CSR, download a CSL; • Zeroize all Critical Security Parameters (CSP); The TSF can also be managed from an optional MAGNUM system, which is a trusted IT entity. When a MAGNUM system is used, the system serves as a control interface for the

TOE SFR	Rationale
	TOE's media streaming switch fabric. The MAGNUM device can establish, change, and tear down multicast IP video streams. The TOE maintains a trust store where the TOE's certificate is stored. Only Security Administrators have access to the trust store. Security Administrators can upload a certificate chain. Uploading the certificate chain, replaces the previously installed certificate chain. When a user account is created (by administrator), it must be assigned with a role that specifies the privileges the account will have. The administrator can choose to assign an existing role with pre-defined privileges or create a new role with customized privileges. Administrators can administer IPX locally through serial port connection. A console menu can be used to perform configurations tasks such as setting IP/system time/session timeout/generate certificate request/system reboot, etc. Administrators can administer IPX remotely through its web interface, which runs on HTTPS. The web interface supports a broader set of the configuration settings that include configurations for certificate imports, syslog server, route mapping, etc. The administrative interfaces provided by the TSF do not allow any of these functions to be accessed by unauthenticated or unauthorized users.
FPT_SKP_EXT.1	The TSF stores cryptographic keys in a directory (/etc/shadow) in flash memory. As there is no command line access, users cannot gain any direct access to these files.
FPT_APW_EXT.1	The TSF does not store plaintext password. Passwords are hashed using SHA-256 and stored in a secure location which is not accessible to users. Secure (one-way) hash functions ensure that it's computationally impossible to recover a plaintext from its hashed value.
FPT_TST_EXT.1	The TSF performs the following hardware self-tests at power-on: • firmware integrity check that compares the SHA256 checksum of the loaded firmware with a permanently stored hash value; • Presence of certificate and public key files. The TSF enables FIPS mode on the OpenSSL library by default at start-up. Upon enabling FIPS mode the algorithm self-tests required by FIPS are performed. The OpenSSL library self-tests include: o SHA-256 KAT o HMAC-SHA-256 KAT o AES 128 GCM Encrypt and Decrypt KAT o AES 128 Encrypt and Decrypt KAT o RSA 4096 SHA-256 Sign and Verify KAT o ECDSA Pairwise Consistency Test o DRBG AES-CTR-256 KAT (invoking the instantiate, reseed, and generate functions) After loading the image, a hash value is computed from the memory partition containing the image. This hash value is compared with a pre-stored hash value at another location on flash. The pre-stored hash is not accessible through any interface for modification. The two hash values must match for the boot process to succeed. If any of the other checks fail, the TSF will display a failure message on the serial console and will perform a reboot. Administrators are instructed to contact Evertz service

TOE SFR	Rationale
	department for repair if the failure does not clear on reboot. These self-tests ensure the TOE software is the correct image and that cryptographic functions are performing appropriately. If failures are seen by the Administrator, they should be immediately corrected.
FPT_TUD_EXT.1	The site administrators do not have access to install any applications on the TOE. The IPX embedded system can only be updated with the valid firmware release from Evertz. Operators may verify the current version with WebEasy interface. The current firmware version is displayed on both webpage and in serial console menu. Digital delivery of new IPX firmware may be provided via File Transfer Protocol Secure (FTPS) using signed and hashed code. Firmware updates are done from the IPX webpage interface under “upgrade”. During a firmware upgrade, IPX will first verify the HMAC of new firmware code with a local stored public key. The TSF does not provide an interface to change the local stored public key to administrators. When HMAC verification passes, IPX will verify the firmware binary header with an Evertz-defined proprietary format. If there is no mismatch, the new firmware code will overwrite the current one. A verification of the firmware’s digital signature is performed next. A hashed-value of the images is generated and then signed with Evertz’s private key. The result file (signature) is included in the firmware package together with the actual firmware binary. During upgrade, the signature file is first decrypted using the public key stored on IPX, then the hashed value is re-calculated from the uploaded image binary file and then compared with the decrypted hash value. These hashes must match for this validation to succeed. If the digital signature fails, the upgrade fails and a log event is generated. If the digital signature succeeds, the upgrade proceeds and the updated firmware is installed onto the TOE.
FPT_STM_EXT.1	The TSF provides a reliable timestamp from the hardware clock on the TOE. Timestamps found in auditable log events use the system clock on IPX. Administrators can, as needed, set the system time clock through serial port console menu after each card reboot. The new system time is also used to set the hardware clock, which is a clock that runs independently of any control program running in the CPU and even when IPX is powered off. During IPX system startup, system time is initialized to the time from the hardware clock.
FTA_SSL_EXT.1 FTA_SSL.3 FTA_SSL.4	Security Administrators can configure a maximum allowable period of inactivity for a Security Administrator session on the WebEasy interface or the local console. If there is no user interaction with the IPX for the specified amount of time, the session is terminated. The TSF polls the session timeout every 60 seconds, so the timeout occurs after the set time plus 60 seconds. The initial, default session timeout is 15 minutes. When the session is terminated, any unsaved changes will be discarded. Administrators may terminate their own sessions by clicking “Logout” at the upper right hand of the WebEasy screen or typing “X” to exit the console.

TOE SFR	Rationale
FTA_TAB.1	The TSF enables Security Administrators to alter the warning banner by navigating to the "System" tab on the web browser and scrolling toward the bottom to the "Warning Banner" section. From here the Security Administrator can modify the "Agree" text and/or the "Disagree" text. (The "Disagree" text shows up when a user "disagrees" with the Security Banner text. The banner can provide warnings against unauthorized access to the TOE as well as any other information that the Security Administrator wishes to communicate. Users who select "Disagree" are not permitted access to the TSF. The TSF presents the access banner prior to authentication when a user connects to the remote WebEasy interface or local console CLI described in the FIA_UIA_EXT.1, FIA_UAU_EXT.2 description.
FTP_ITC.1	The TSF communicates with the external syslog server using TLS as described in the descriptions of FAU_STG_EXT.1 and FCS_TLS* above. The TSF initiates the trusted channel with the Syslog server. The TSF communicates with a MAGNUM server through TLS as well as described in the FCS_TLS* above. The MAGNUM server initiates the trusted channel with the TOE and is a trusted IT entity.
FTP_TRP.1/Admin	The TSF provides a trusted path for remote administration using HTTPs/TLS as described in FCS_HTTPS_EXT.1 and FCS_TLSS_EXT.2 descriptions.

Table 17 TOE Summary Specification SFR Description

7 Terms and Definitions

Abbreviations/Acronyms	Description
AES	Advanced Encryption Standard
AV	Audio-Video, Audiovisual
CBC	Cipher Block Chain
CC	Common Criteria
CO	Cryptography Officer
CTR	Counter (mode)
CWDM	Coarse Wave Division Multiplexing
DFB	Distributed Feedback
DHE	Diffie-Hellman Exchange
DNS	Domain Name Service
DRBG	Deterministic Random Bit Generator
DVI	Digital Video Interface
DWDM	Dense Wave Division Multiplexing
ECDHE	Elliptic Curve Diffie-Hellman Exchange
EMX	Evertz Modular Crosspoint
Gb	Gigabit
GCM	Galois/Counter Mode
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IP	Internet Protocol
IPX	Internet Protocol Crosspoint
km	Kilometer(s)
max	Maximum
NDPP	Network Device Protection Profile
nm	Nanometer(s)
OE	Operational Environment
OOBM	Out of Band Management
RBAC	Role Based Access Control
RFC	Request For Comment
RJ-45	Radio Jack (45)
RS-232	Recommended Standard 232
RSA	Rivest-Shamir-Adelman
SDI	Serial Digital Interface
SFP	Small Form-Factor Pluggable
SFR	Security Functional Requirements
SHA	Secure Hash Algorithm
SMF	Single Mode Fiber
SNMP	Simple Network Management Protocol
SSH	Secure Shell
ST	Security Target
TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	Target Security Function
USB	Universal Serial Bus
VGA	Video Graphics Array

Table 18 TOE Abbreviations and Acronyms

Abbreviations/Acronyms	Description
CC	Common Criteria
CCRA	Arrangement on the Recognition of Common Criteria Certificates in the field of IT Security
DOD	Department of Defense
NIAP	National Information Assurance Partnership
OSP	Organizational Security Policy
PP	Protection Profile
SAR	Security Assurance Requirement
SFR	Security Functional Requirement
SFP	Security Function Policy
SPD	Security Policy Database
ST	Security Target
TOE	Target of Evaluation
TRRT	Technical Rapid Response Team
TSF	TOE Security Functionality
TSFI	TSF Interface
TSS	TOE Summary Specification

Table 19 CC Abbreviations and Acronyms