NETWORK DEVICE COLLABORATIVE PROTECTION PROFILE V2.7 SECURITY TARGET

13 October 2017

Evertz Microsystems Ltd
5292 John Lucas Dr. Burlington, Ontario, Canada

Table of Contents

Table of Figures

Table of Tables

Document Revision History

Version	Date	Revision Description	Author
0.1	9/1/16	Parsed IPX version from previous IPX-Magnum v0r4.	J Bilheimer
0.2	9/15/16	Updated architecture discussions and drawings. Copy edits.	J Bilheimer
0.3	9/16/16	Updated SFRs to match NDcPP vice NDPP. Updated part numbers.	J Bilheimer
0.5	9/30/16	Updated SFR responses.	J Bilheimer
0.6	1/30/17	Housekeeping	J Bilheimer
1.0	3/22/17	Add sec. 8.2 & other updates & fixes	B. Mathews
1.1	5/3/17	Partial rewrite	B. Mathews
1.2	5/7/17	Finished rewrite pending input from IPX Team	B. Mathews
1.3	5/11/17	Partial input from IPX Team (Section 8)	B. Mathews
2.0	5/12/17	Rewrite Based on NDcPP, include Technical Decisions	B. Mathews
2.1	5/18/17	Add sec. 2.2, 2.3, and numerous tweaks	B. Mathews
2.2	5/19/17	CAPV Certification issue – for now they are TBD	B. Mathews
2.3	6/27/17	Fix errors uncovered during testing	B. Mathews
2.4	8/2/17	Update per TD0223-8 & add CAVP Cert. #s	B. Mathews
2.5	9/25/17	Add clarifications per evaluators	B. Mathews
2.6	10/11/17	Add clarifications per evaluators	B. Mathews
2.7	10/13/17	Add clarifications per evaluations	B. Mathews

1 Introduction

This document demonstrates the compliance of a suite of functionally similar products of Evertz Microsystems, Ltd. with the Network Device Collaborative Protection Profile, version 1.0. The devices are the MMA10G-IPX-16, MMA10G-IPX-32 and MMA10G-IPX-64 (hereinafter referred to as “IPX”), which are Ethernet switches optimized for video content.

1.1 Security Target (ST) and Target of Evaluation (TOE) Reference

ST Title	**Evertz IPX NDcPP v2.7 Security Target**		
ST Document Number	**2.7**		
ST Version	**2.7**		
ST Issue Date	**10/13/2017**		
TOE Identification			
Component Type	**Part ID**	**Hardware Version**	**Firmware Version**
Card	MMA10G-IPX-16	1.0	2v0_b1
	MMA10G-IPX-32	1.0	2v0_b1
	MMA10G-IPX-64	1.0	2v0_b1
SFP	SFP-10G-TR13	1.0	1.0
	SFP-10G-TR15S	1.0	1.0
	SFP-10G-TR15H	1.0	1.0
	SFP-10G-TRC*xx*H[1]	1.0	1.0
	SFP-10G-TRD*xxx*H[2]	1.0	1.0
	SFP-1G-TR13	1.0	1.0
	SFP-1G-TR15S	1.0	1.0
	SFP-1G-TR15H	1.0	1.0
	SFPTR-RJ45-SGM-GI	1.0	1.0
Frame	EMX1-FR	1.2	n/a
	EMX3-FR	1.2	n/a
	EMX6-FR	1.1	n/a
Frame Controller	EMX-FC	1.1	Rev. 1, Build 14372.1
Power Supply	EMX1-PS	1.0	n/a
	EMX3-PS	1.3	n/a
	EMX6-PS	1.0	n/a
	[1] *xx* serves as a placeholder for varying CWDM wavelengths.		
	[2] *xxx* serves as a placeholder for varying DWDM wavelengths.		

Table 1. ST and TOE Reference

2 Target of Evaluation (TOE) Overview

2.1 Physical Scope of the TOE

The Internet Protocol Crosspoint (IPX) switch is a 10 Gigabit (Gb) Internet Protocol (IP) switch optimized for video-over-IP traffic (compressed or uncompressed). The IPX features (16), (32) or (64) 10 Gigabit per second (Gbps) IP ports (depending on the capacity of the IPX card). Each port accepts one (1) optical 10 Gbps Small Form-Factor Pluggable (SFP) transceiver. Individual 1000 Megabit per second (Mbps) SFPs (either electrical or optical) may be substituted on a port-by-port basis. 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 EMX frames come in three sizes (1 RU, 2 slots; 3RU, 5 slots; 6RU, 15 slots). All IPX-compatible cards may be inserted into any IPX frame configuration provided there are sufficient contiguous free slots available.

The IPX builds on the capabilities of the existing Evertz line of video routing switches. Video routers receive video signals in various formats, such as Serial Digital Interface (SDI), Serial Data Transport Interface (SDTI), or Asynchronous Serial Interface (ASI), and switch dedicated physical input ports to dedicated physical output ports based on external commands. Video routing networks utilize dedicated physical plant and are highly efficient, sustainable, and secure. The IPX provides the same capability within the context of packet-based networks using shared network infrastructure.

Traditional packet-based networks do not support the extremely high standards for signal integrity and fault tolerance required for broadcast video. Evertz's solution to this problem has been to develop a packet-based switching fabric from a video perspective, rather than rely on traditional packet-based network architecture. Since video by nature has a unidirectional flow, and also since it is normal for multiple copies of a single incoming video stream to be sent to multiple output destinations, the IPX exclusively uses multicast IP addressing. Unicast is not feasible for streaming video in an enterprise production environment and is not supported by the IPX platform.

Multicast switching can be challenging, especially for non-automated systems. Momentary delays and signal loss are common in these networks but are unacceptable in broadcast environments. To address this issue, a typical IPX installation will also include a standard video routing switch software platform (such as Evertz Magnum) to route data seamlessly between program streams in a manner sufficient to meet broadcast video standards for signal availability and integrity. 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.

2.2 Logical Scope of the TOE (Overview)

The NDcPP-compliant TOE is comprised of several security features.   Each of the security features identified above consists of several security functionalities, as identified below.

1. Security audit
2. Cryptographic support
3. Identification and authentication
4. Secure Management
5. Protection of the TSF
6. TOE access
7. Trusted path/channels

These features are described in more detail in the subsections below.

2.2.1 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
- Any update attempt
- Result of the update attempt
- Management of TSF data
- Changes to Time

The TOE can store the generated audit data on itself and it can be configured to send syslog 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 logs can be viewed 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.

2.2.2 Cryptographic Support

The TOE provides cryptography support for secure communications and protection of information. The cryptographic services provided by the TOE include: symmetric encryption and decryption using AES; asymmetric key generation; cryptographic key establishment using RSA-based key establishment schemes and DH key establishment; digital signature using RSA; cryptographic hashing using SHA-256; random bit generation using DRBG and keyed-hash message authentication using HMAC-SHA (SHA-1 and SHA-256). The TOE implements the secure protocols TLS/HTTPS on the server side and TLS on the client side. The algorithm certificate references are listed in the table below.

Algorithm	Description	Mode Supported	CAVP Cert. #
AES	Used for symmetric encryption/decryption FCS_TLSC_EXT.1 FCS_TLSS_EXT.2 FCS_HTTPS_EXT.1 FCS_COP.1(1)	CBC (128 and 256 bits)	4652
SHS (SHA-256)	Cryptographic hashing services FCS_TLSC_EXT.1 FCS_TLSS_EXT.2 FCS_HTTPS_EXT.1 FCS_COP.1(1) FCS_COP.1(3)	Byte Oriented	3811
HMAC (HMAC-SHA-1, HMAC-SHA-256)	Keyed hashing services and software integrity test FCS_TLSC_EXT.1 FCS_TLSS_EXT.2 FCS_HTTPS_EXT.1 FCS_COP.1(1) FCS_COP.1(4)	Byte Oriented	3080
DRBG	Deterministic random bit generation services in accordance with ISO/IEC 18031:2011 FCS_TLSC_EXT.1 FCS_TLSS_EXT.2 FCS_HTTPS_EXT.1 FCS_RBG_EXT.1	CTR_DRBG (AES 256)	1570
RSA	Signature Verification and key transport FCS_TLSC_EXT.1 FCS_TLSS_EXT.2 FCS_HTTPS_EXT.1 FCS_CKM.1 FCS_CKM.2 FCS_COP.1(2)	FIPS PUB 186-4 Key Generation (2048-bit key)	2538

Table 2. CAVP Certificate References

2.2.3 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.) Once an Administrator attempts to access the management functionality of the TOE, the TOE prompts the Administrator for a user name 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 functionalitirmwy 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.

2.2.4 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
- fConfigure the cryptographic services
- 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.

2.2.5 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.

2.2.6 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.

2.2.7 Trusted Paths/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 syslog data to a syslog server using TLS and other external authentication stores using TLS-protected communications.

2.3 Excluded Functionality

Excluded Functionality	**Exclusion Rationale**
Multicast IP Stream (switching IP Video streams, which is the purpose of the IPX)	Encryption (if required) is handled at the transmit & receive locations, not the switch.
SNMP Traps (Alarms)	This only sends alarm information to an alarm monitoring system (such as Evertz VistaLINK). This function does not map to the NDcPP requirements.

Table 3. Excluded Functionality

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). The whole purpose of the IPX is to switch IP video streams. 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 there is no point in adding cryptology functions to the switch function itself. Indeed, adding de-encryption and re-encryption of the IP video streams at the IPX would add vulnerability (creating a midpoint where all the encrypted video is unencrypted). This is why the actual IP video switching is considered outside the scope of the TOE. The exclusion of this functionality does not alter compliance to the collaborative Protection Profile for Network Devices Version 1.0.

3 TOE Description

3.1 IPX Component Description

The IPX cards, associated SFPs, their mounting frames and the frames' controllers and power supplies make up an IPX installation.

IPX Card	Contiguous Slots	SFP Ports	EMX1-FR	EMX3-FR	EMX6-FR
MMA10G-IPX-16-CC	2	16	✓	✓	✓
MMA10G-IPX-32-CC	2	32	✓	✓	✓
MMA10G-IPX-64-CC	4	64		✓	✓

Table 4. IPX Card Types

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 5. 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 serve as a passthrough proxy to distribute Ethernet-based control connections to the individual IPX cards within the EMX frame chassis. The controllers also provide limited Simple Network Management Protocol (SNMP) alarm information, such as the card type, slot location, and the status of power supplies and fans.) Details are in the "Notify" section of the IPX Manual.

The SFP ports are unencrypted. Sites requiring enclave-based data security will deploy physical security controls to isolate the video network enclave. Where operational mission requires that video needs to cross a logical enclave boundary, Evertz stipulates a network architecture deploying third-party software or hardware encryption at the video transmitting and video receiving endpoints.

3.2 IPX Module Description

COMPONENT	PART NUMBER	DESCRIPTION
IPX CARDS	**MMA10G-IPX-16-CC**	16-Port IPX Switch Card, 2 EMX Slots
	MMA10G-IPX-32-CC	32-Port IPX Switch Card, 2 EMX Slots
	MMA10G-IPX-64-CC	64-Port IPX Switch Card, 4 EMX Slots
IPX SFP PLUGGABLE MODULES	**SFP10G-TR13**	SFP+ Optical Transceiver, 10Gbs, 1310nm, SMF, 10km
	SFP10G-TR15S	SFP+ Optical Transceiver, 10Gbs, 1550nm DFB, SMF, 40km max
	SFP10G-TR15H	SFP+ Optical Transceiver, 10Gbs, 1550nm DFB, SMF, 80km max
	SFP10G-TRCxxH*	SFP+ Optical Transceiver, 10Gbs, CWDM (1470-1610nm) DFB, SMF, 80km max (70km for 1590-1610nm)
	SFP10G-TRDxxxH	SFP+ Optical Transceiver, 10Gbs, DWDM (ch 20-60) DFB, SMF, 80km max
	SFPTR-RJ45-SGM-GI	10/100/1000 RJ45 Electrical SFP module
	SFP1G-TR13	SFP Optical Transceiver, 1.25Gbs, 1310nm, SMF, 20km
	SFP1G-TR15S	SFP Optical Transceiver, 1.25Gbs, 1550nm, SMF, 40km
IPX FRAMES & FRAME COMMON CARDS	**EMX1-FR**	2-Slot Frame, 1 RU, AC Power (Redundant Power Supply Optional), Accepts One Frame Controller
	EMX1-PS	Power Supply for EMX1-FR Frame
	EMX1-FR+PS	EMX-1 Frame with (2) (Redundant) Power Supplies
	EMX3-FR	5-Slot Frame, 3 RU, AC Power (Redundant Power Supply Optional), Accepts One or Two (Redundant) Frame Controllers
	EMX3-PS	Power Supply for EMX3-FR Frame
	EMX3-FR+3PS	EMX-3 Frame with Two (Redundant) Power Supplies
	EMX6-FR	15-Slot Frame, 6 RU, AC Power (Redundant Power Supply Optional), Accepts (1) or (2) (Redundant) Frame Controllers
	EMX6-PS	Power Supply for EMX6-FR Frame
	EMX6-FR+6PS	EMX-6 Frame with (2) (Redundant) Power Supplies
	EMX-FC	Frame Controller for EMX Frames

See CWDM & DWDM SFP details in* **Table 7. CWDM SFP Details *and* **Table 8.** DWDM Specific Details
.

Table 6. TOE Product Reference Numbers

CWDM SFP	Wavelength	CWDM SFP	Wavelength
SFP10G-TRC27H	1270 nm	SFP10G-TRC47H	1470 nm
SFP10G-TRC29H	1290 nm	SFP10G-TRC49H	1490 nm
SFP10G-TRC31H	1310 nm	SFP10G-TRC51H	1510 nm
SFP10G-TRC33H	1330 nm	SFP10G-TRC53H	1530 nm
SFP10G-TRC35H	1350 nm	SFP10G-TRC55H	1550 nm
SFP10G-TRC37H	1370 nm	SFP10G-TRC57H	1570 nm
SFP10G-TRC43H	1430 nm	SFP10G-TRC59H	1590 nm
SFP10G-TRC45H	1450 nm	SFP10G-TRC61H	1610 nm

Table 7. CWDM SFP Details

DWDM SFP	ITU Channel	DWDM SFP	ITU Channel	DWDM SFP	ITU Channel
SFP10G-TRD200H	20	SFP10G-TRD340H	34	SFP10G-TRD480H	48
SFP10G-TRD210H	21	SFP10G-TRD350H	35	SFP10G-TRD490H	49
SFP10G-TRD220H	22	SFP10G-TRD360H	36	SFP10G-TRD500H	50
SFP10G-TRD230H	23	SFP10G-TRD370H	37	SFP10G-TRD510H	51
SFP10G-TRD240H	24	SFP10G-TRD380H	38	SFP10G-TRD520H	52
SFP10G-TRD250H	25	SFP10G-TRD390H	39	SFP10G-TRD530H	53
SFP10G-TRD260H	26	SFP10G-TRD400H	40	SFP10G-TRD540H	54
SFP10G-TRD270H	27	SFP10G-TRD410H	41	SFP10G-TRD550H	55
SFP10G-TRD280H	28	SFP10G-TRD420H	42	SFP10G-TRD560H	56
SFP10G-TRD290H	29	SFP10G-TRD430H	43	SFP10G-TRD570H	57
SFP10G-TRD300H	30	SFP10G-TRD440H	44	SFP10G-TRD580H	58
SFP10G-TRD310H	31	SFP10G-TRD450H	45	SFP10G-TRD590H	59
SFP10G-TRD320H	32	SFP10G-TRD460H	46	SFP10G-TRD600H	60
SFP10G-TRD330H	33	SFP10G-TRD470H	47		

Table 8. DWDM Specific Details

3.3 Component Interconnectivity

The TOE consists of one or more IPX cards located within a given EMX frame. 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). In each case the second port provides optional redundancy.

3.4 Non-Scope Elements

The nature of the physical network connection is considered outside the scope of the TOE, as the available network elements (IP switches, IP routers, etc.) which may be used in establishing that link are site-specific. Evertz stipulates that any connection must meet organizationally-specific security requirements for the location(s) where the equipment is deployed.

3.5 TOE Component Reference Images

3.5.1 EMX Frame Reference Images

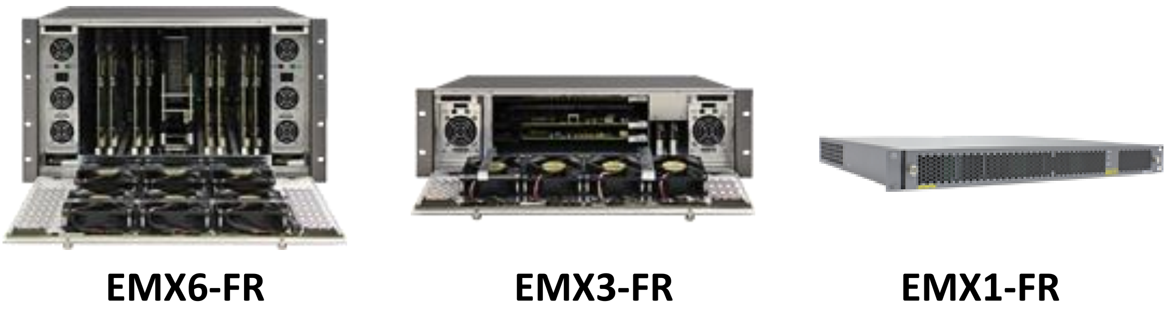

Figure 1. EMX Frame Options for the IPX Family

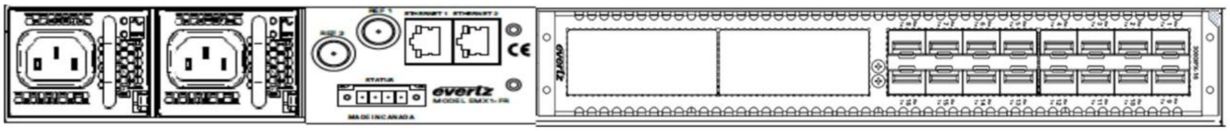

Figure 2. EMX1-FR Rear View (Equipped with (1) MMA10G-IPX-1-CC6)

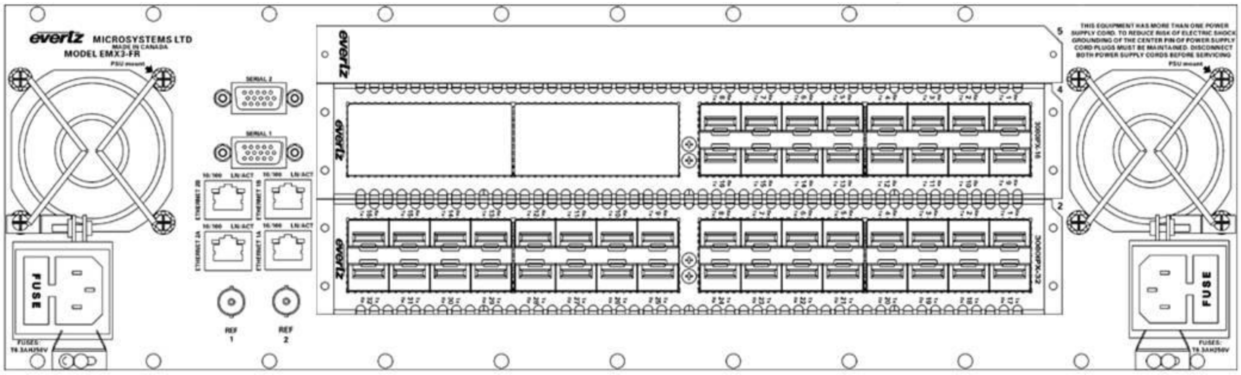

Figure 3. EMX3-FR Rear View (Equipped with one MMA10G-IPX-32-CC & one MMA10G-IPX-16-CC)

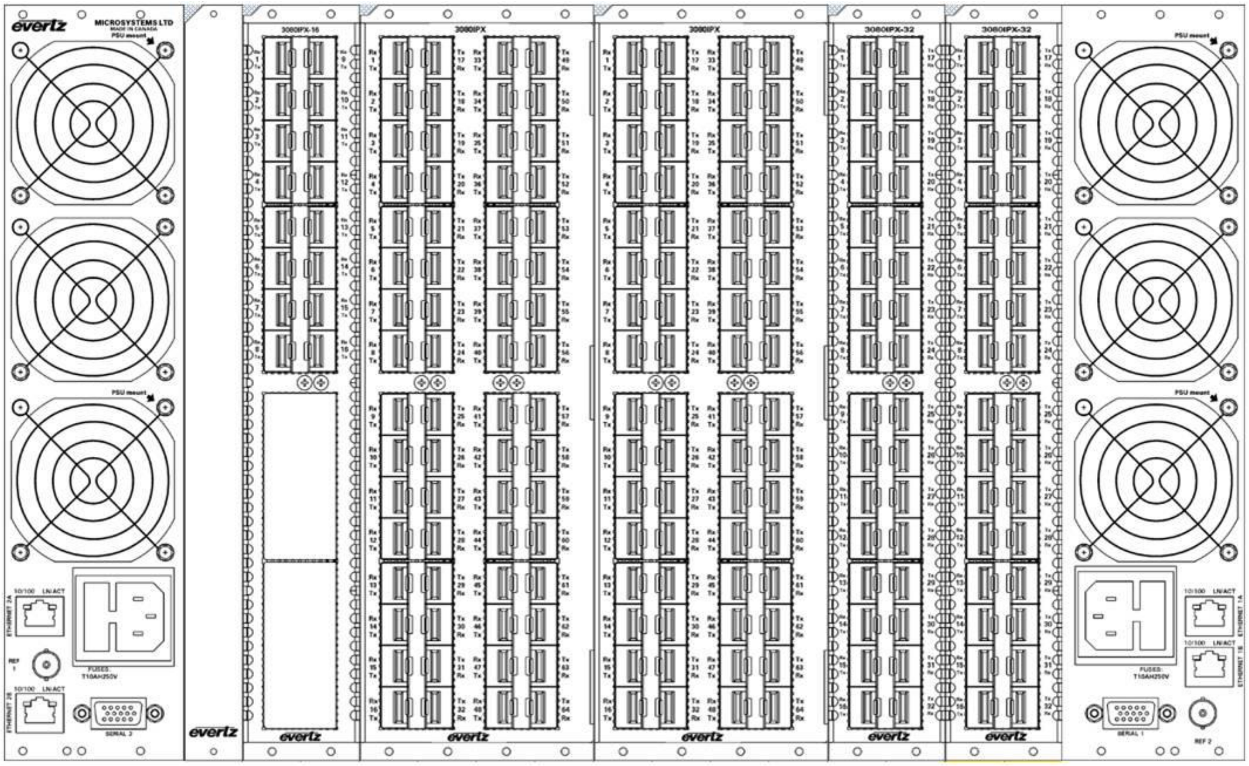

Figure 4. EMX6-FR Rear View (Equipped with (2) MMA10G-IPX-3-CC2, (2) MMA10G-IPX-6-CC4, and (1) MMA10G-IPX-16-CC)

3.5.2 IPX Card Reference Images

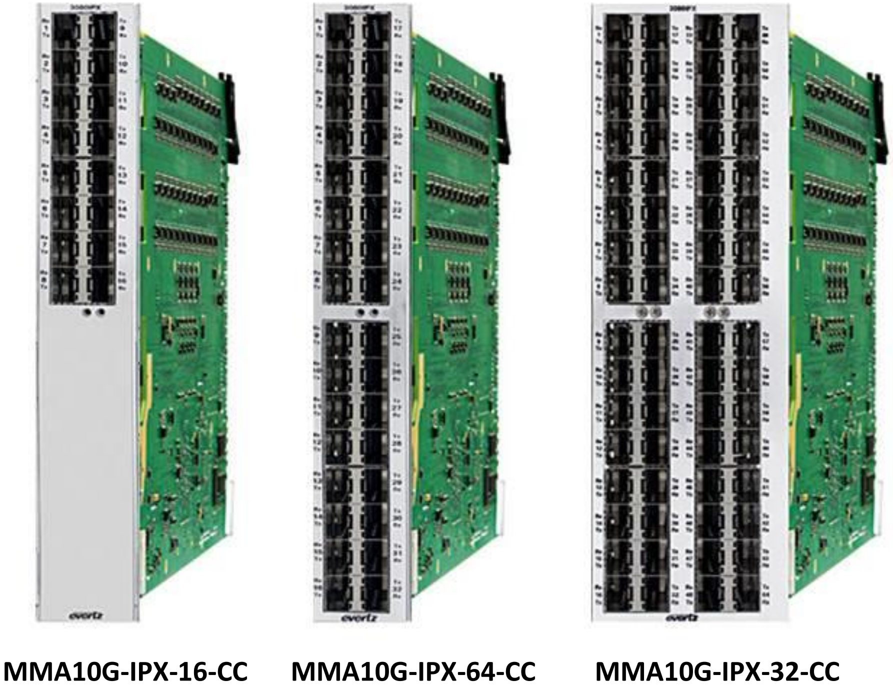
MMA10G-IPX-16-CC **MMA10G-IPX-64-CC** **MMA10G-IPX-32-CC**

Figure 5. 10Gb Interface Cards for the IPX Family

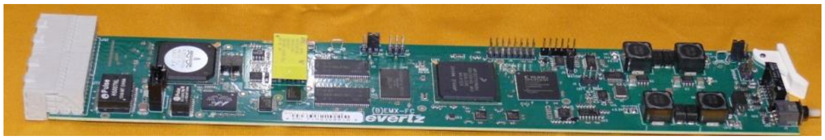

Figure 6. Frame Controller for the IPX Family

3.6 Physical Scope of the TOE

3.6.1 IPX Routing Switcher

3.6.1.1 IPX Chassis

IPX supports three (3) available chasses (frames). Each chassis includes a single standard power supply, and each can support dual redundant power supplies. Each chassis has front panels with fans, and there are also fans on the power supplies.

- ***EMX1-FR*** is a 1 RU frame with two (2) horizontal card slots housing one (1) frame controller. The front panel is removable. There is no serial port; serial connections to IPX cards for configuring the IP address are via a special ribbon cable that connects directly to the Frame Controller card (only for initial set-up).
- ***EMX3-FR*** is a 3 RU frame with five (5) horizontal card slots housing up to two (2) frame controllers. Two (2) serial ports are available for configuring the IP addresses of each Frame Controller card (only for initial set-up).
- ***EMX6-FR*** is a 6 RU frame with (15) vertical card slots housing up to two (2) frame controllers. Two (2) serial ports are available for configuring the IP addresses of each Frame Controller card (only for initial set-up).

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

3.6.1.2 IPX Chassis I/O Interface

The IPX Chassis features the following physical I/O Interfaces:

3.6.1.2.1 EMX Frame 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.

3.6.1.2.2 EMX 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. If the IPX is in an EMX6-FR or an EMX3-FR frame, the administrator connects via a site-provided workstation and a local serial cable with DB9 connectors. If the IPX is in an EMX1-FR fame, an Evertz-supplied four-pin ribbon cable adapter is used. (This may optionally be used in an EMX6-FR or EMX3-FR frame, but is not required.) The serial connection has no functionality except setting up the IP address and related information.

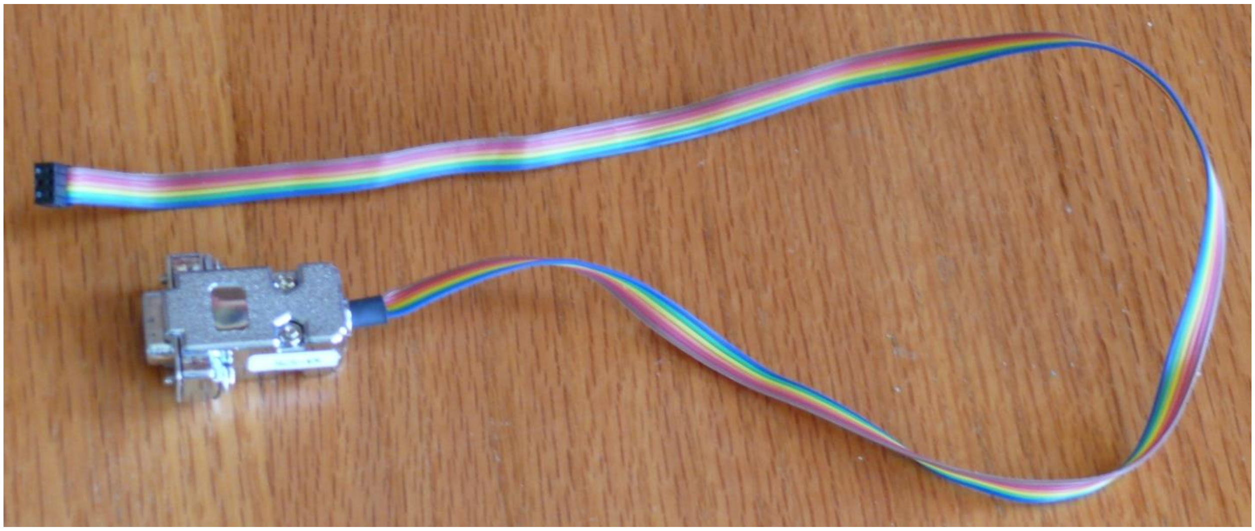

Figure 7. Serial Cable Adapter

Administrators establish the serial connection using a site-provided terminal client. The serial connection is password-protected.

3.6.1.3 IPX Routing Cards

IPX routing and distribution cards are functionally identical except for the number of ports (16, 32, or 64). Each physical port consists of an SFP cage. The default mode is for 10 Gbps SFPs; 1.25 Gbps optical or 1 Gbps electrical (1000BaseT) SFPs may optionally be used. Optical SFPs come with a variety of optical options (power, sensitivity, wavelength). All 63 unique configurations of SFPs may be freely mixed and matched in any physical SFP port.

3.6.1.3.1 IPX Routing Card I/O Interfaces

Each IPX routing card features the following I/O 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)

3.6.2 TOE Interconnectivity

The IPX components in a given installation communicate with each other and with external systems over standard Layer 2 Ethernet. The IPX manual specifies that deployment of the secure version of these products will include the use of secure IP connection(s) for control purposes.

3.6.3 TOE Operational Environment

There are three deployment options for the IPX in secure applications:

3.6.3.1 Physically Isolated Data Enclaves

The most common scenario features the IPX deployed within a physically isolated enclave. In such an application the video signals on the SFP ports do not require encryption (although they certainly may be encrypted by the end user based on site policy or preference), as confidentiality is maintained via physical access controls implemented by the user. Video equipment that provides such encryption is widely available and is outside the scope of this TOE.

3.6.3.2 Encrypted Remote Endpoints

“Remote” is defined here as any location outside the secured area (room, building, campus, etc.), and as such may encompass LAN and/or WAN architecture. In this scenario, video signals must be encrypted. The most efficient place to perform such encryption is at the source and terminal point of the video signal itself. As a result, in the Evertz operational environment, encryption and decryption are performed by the originating and terminating video equipment.[1] The IPX passes through the signals as received (whether encrypted or unencrypted) and does not perform any port scanning or traffic analysis on received signals.

[1] As stated elsewhere in this document, originating and terminating video equipment is not included in the TOE.

3.6.3.3 Unencrypted Remote Endpoints

A third situation could arise if video signals originate and/or terminate at a remote location and are transmitted in the clear (unencrypted). In this case a VPN or similar secured communications would provide logical isolation of the video streams.

3.6.3.4 System Control

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 may be securely downloaded to a Syslog server via TLS.

3.6.4 TOE Applications

Typical applications of IPX applications include:

- Security Cameras
- Multiviewer Displays
- Teleconferencing
- Video Production
- Video Storage
- Video Distribution

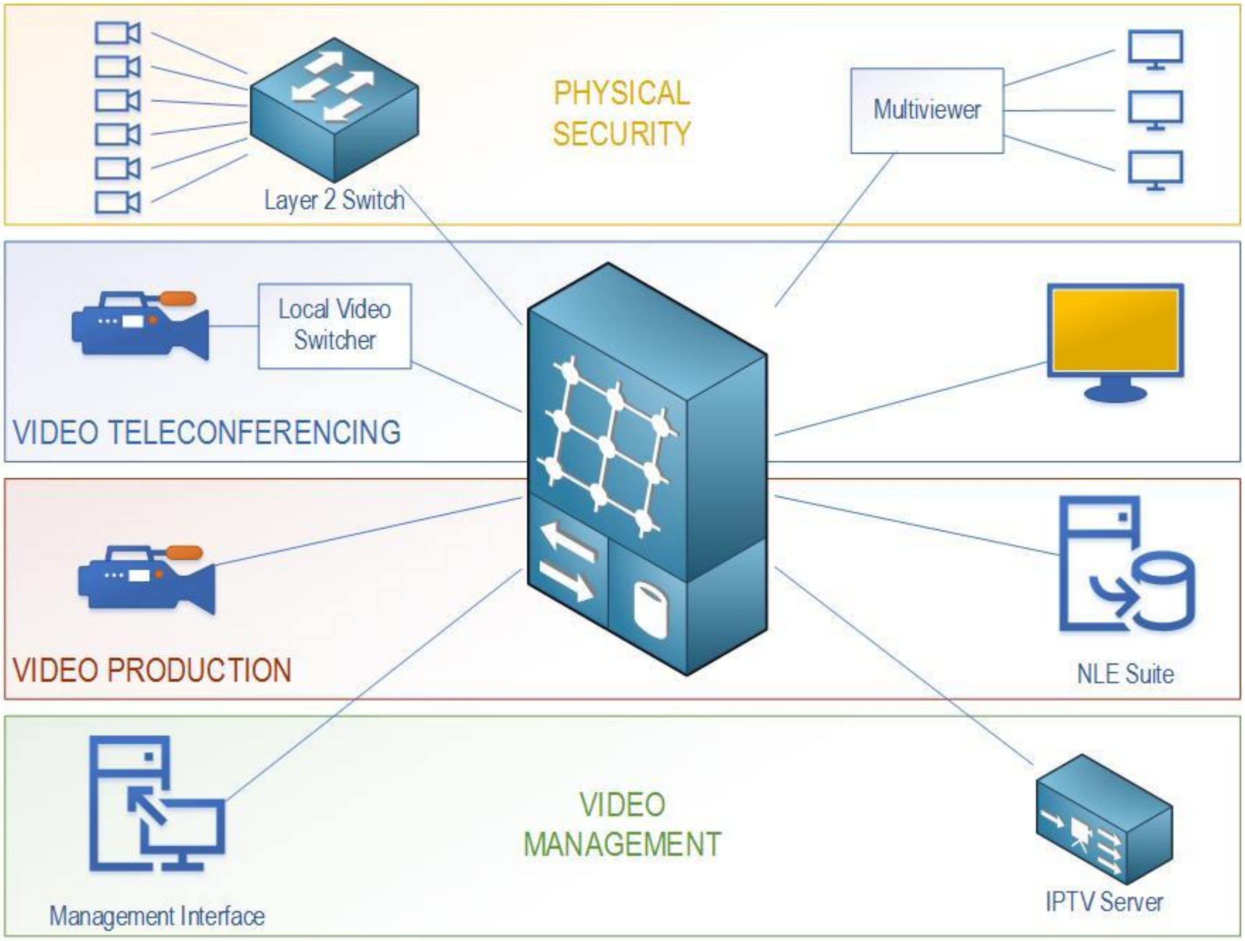

Figure 8. Examples of Typical IPX / Magnum Uses

3.6.5 TOE Management Overview

System operators deploy Evertz's proprietary Magnum software for device control and media stream routing. IPX administration requires use of Evertz's proprietary WebEasy browser interface and VistaLINK Pro management software.

3.6.5.1 Magnum Control Software

Evertz's proprietary Magnum software provides users with the ability to route and configure all enterprise video signals within the Evertz ecosystem. Specific to this TOE, Magnum allows users to setup, modify, and teardown multicast IP video cross-connect points for each IPX card within the EMX frame(s). Magnum's Intelligent Signal Path engine provides the ability to automate multiple-hop signal path management, including:

- Core routing, including through the IPX backplane
- System interlinking
- Multi-view display operation
- Facility Master Control
- Signal transport optimization
- Tally management
- Dynamic signal formatting

3.6.5.2 VistaLINK® Pro

VistaLINK® PRO is the Network Management System (NMS) for the Evertz ecosystem. While VistaLINK® PRO is a full-service NMS, some functionality is limited in the configuration required for proper operation of the TOE. In Secure Mode, VistaLINK® PRO provides the required out-of-band management (OOBM) functionality for this ST, including:

- Fault management
- Alarm/event notification
- Report and log management
- Intelligent correlation and root cause analysis

Site administrators must configure a Simple Network Management Protocol (SNMP) trap host or NMS and a syslog server or network database for site-specific fault, alarm, and log management. Sites may configure an SNMP management tool to automate IPX and peripheral management as desired.

3.6.5.3 WebEasy Browser Interface

The proprietary WebEasy interface 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

3.6.6 Role Based Access Control

The TOE provides functional module authorization to administrative users through two defined roles:

- **User:** Provides rights to create, change and remove logical cross connections within the IPX. The “User” only has access to the system through the Magnum interface. Specific users may have access to all or only some of the ports under the control of the CO / Administrator.
- **Cryptography Officer (CO) / Administrator:** Provides all access rights and sets up secure communications.

Non-administrative Users may only control the IPX via the Magnum interface and have no direct access to the IPX. As a result, there is no need for the IPX to differentiate between roles, since only Security Administrators communicate directly with the device. There is no external role database, as all TOE authentication is local to the respective components. The table below describes role-based access to functional modules for the IPX:

	FUNCTIONAL MODULE	USER	CO/ADMIN
OPERATIONAL MODULES	Switch Operation	✓	✓
	Port Configuration		✓
	Port Naming	✓	✓
	Establish Sub-Users	✓	✓
	Administer Sub-Users	✓	✓
SECURITY MODULES	Network		✓
	Services		✓
	Administer All Accounts		✓
	Cryptographic Support		✓
	Serial I/O		✓
	Self-Test		✓
	Security Audit		✓
	Firmware Upgrades		✓

Table 9. Rate-Based Access to TOE Functional Module Settings

3.6.7 IPX Functional Modules (All)

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 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.

3.7 Logical Scope of the TOE

The figure below depicts the logical scope of the TOE.

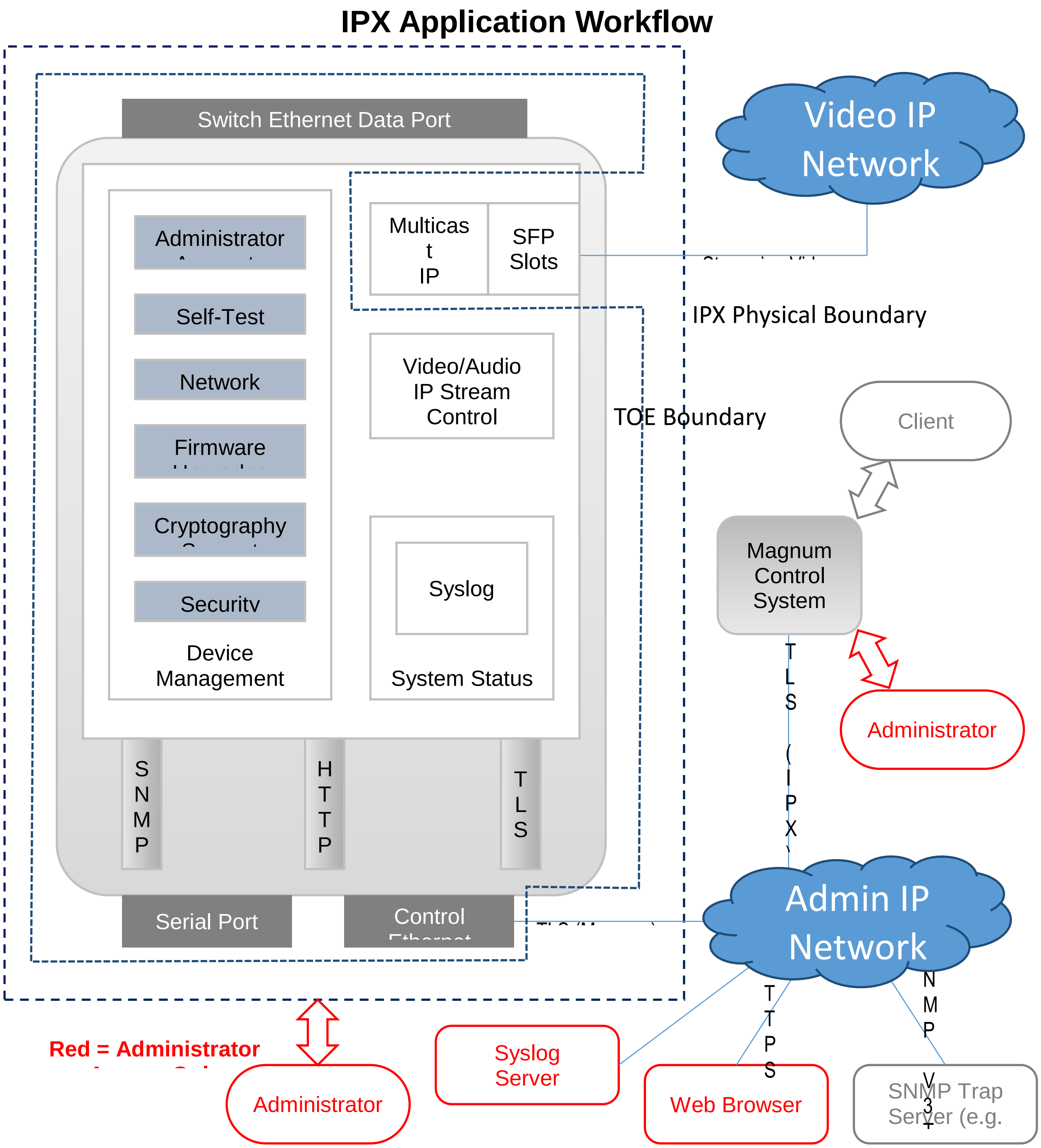

Figure 9. TOE Logical Scope and Workflow

3.7.1 TOE Functional Modules (TOE Only)

The IPX has thirteen functional modules, two of which are not part of the Target Security Function (TSF).

3.8 Usage and Major Security Features of the TOE

3.8.1 System Architecture / IT Environment

The IPX deploys a Layer 2 switching fabric optimized for streaming compressed and uncompressed video over IP. As a Layer 2 technology, the IPX architecture requires a dedicated physically or logically isolated (“closed”) network which must support IPv4 multicast addressing. Sources and destinations (the nature and format of which are independent of the IPX switching system) interface with the switch fabric via Ethernet, either via direct packetized streams or via media gateways. The IPX performs no signal processing and is format-neutral, allowing support for any IP-compliant broadcast video streaming product.

The IPX frame controller assigns each source to a dedicated multicast address using Evertz’s proprietary Synergy routing protocol.[2] Media gateway destinations join and leave each source group based on API commands received from the frame controller. Neither individual gateways nor destination endpoints have the ability to issue a join request.

3.8.1.1 Security Architecture

3.8.1.1.1 Auditing

Audit data are stored internally and distributed over TLS to an external syslog server via a trusted path. The TOE supports role-based access control (RBAC) for authentication and authorization to management and security functions. To maintain the closed TOE network configuration, site administrators deploy at least one (1) syslog server and one (1) Simple Network Management Protocol (SNMP) trap host within the network boundary as trusted path connections. Sites may deploy as many such external trusted path hosts as desired, including aggregators and portals, as long as these do not violate the network boundary.

3.8.1.1.2 Authentication

Due to the closed nature of the deployed network, the TOE does not support the ability to use external authentication servers for user authentication. The IPX authenticates administrative users directly to local onboard databases.

[2] In non-secure mode, the IPX also supports unicast stream addressing for third-party API control distribution. This option is disabled in secure mode.

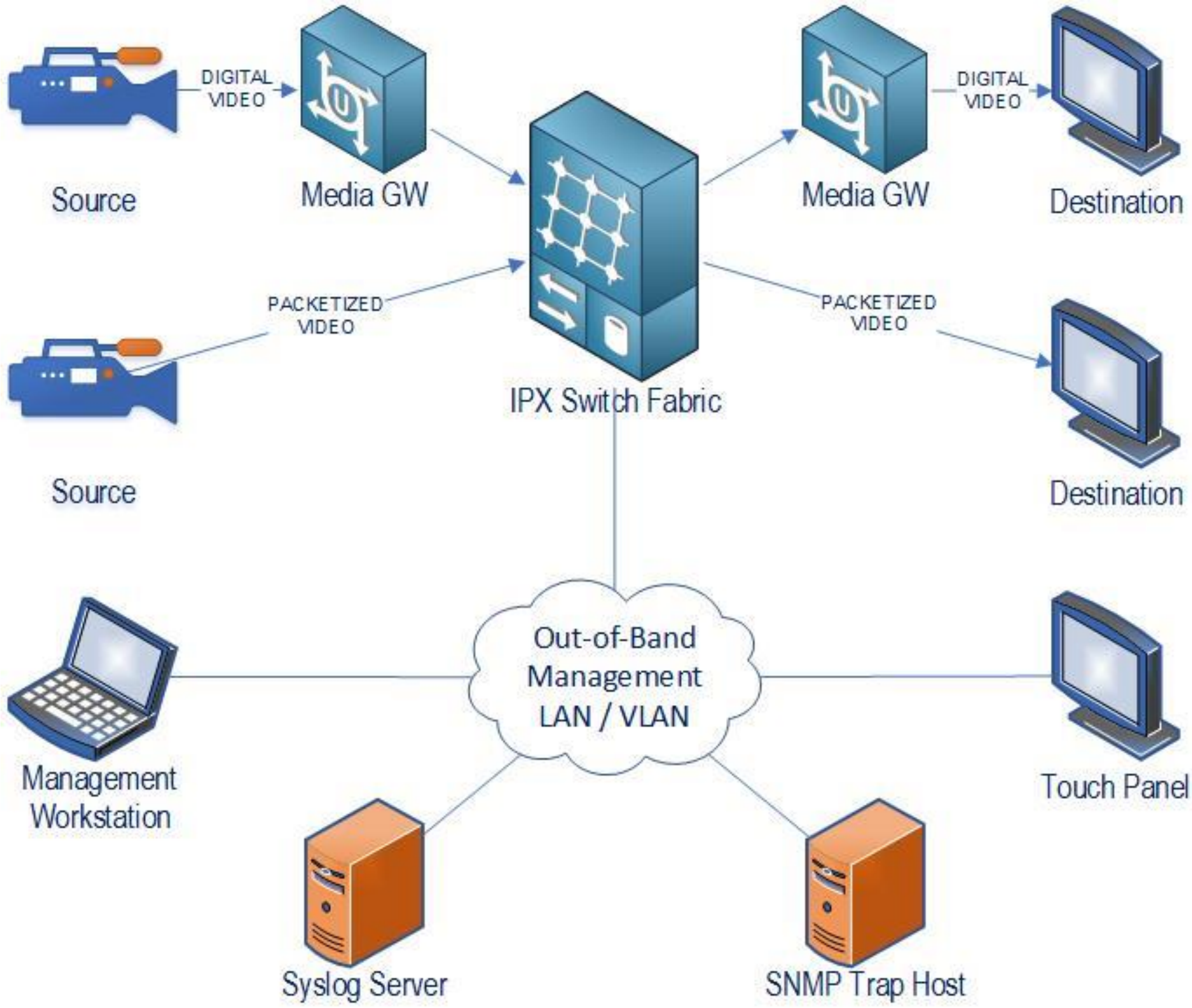

Figure 10. TOE System Architecture

3.8.2 Physical Design

The IPX cards mount in EMX frames. The frames are used to distribute Ethernet connectivity to the IPX cards. The Frame Controllers also provide OOBM data via SNMPv3 traps using VistaLINK® PRO software.

An IPX card contains the following computational elements:

- SoC CPU: MPC8377E with single core, 400MHz frequency
- DRAM Memory: 512MB
- NOR Flash memory: 64MB
- FRAM memory: 1MB
- BroadCom 56841/56843/56845 Switch Chip;

The IPX switch ports consist of SFP sockets. A wide variety of industry-standard SFPs may be used in these sockets, varying by interface (optical or 1000BaseT), speed (1, 1.25 or 10 Gb/sec), and optical characteristics (laser power, laser wavelength and receive sensitivity). Any SFP may be used in any port.

3.8.3 System Design

3.8.3.1 Operational Control

The IPX communicates with the dedicated Magnum application controller (either a dedicated touch panel interface or an external site-provided workstation) via Ethernet; this connection is authenticated and encrypted. Please see the respective component technical specification documentation for further information.

The IPX does not encrypt or process IP-based streaming media traffic. The IPX serves merely as a media distribution switch, directing inbound media streams to their respective multicast groups. There is neither physical nor virtual internal connectivity between the encrypted management ports and the unencrypted IPX switch ports. Sites are responsible for deploying operational, physical, and transport security policies to ensure adequate confidentiality and integrity for switched IP streams. The IPX manual guidelines address this operational requirement.

3.8.3.2 System Management

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.

COMMUNICATION PURPOSE	IPX
IPX	n/a
Magnum	TLS
Set IP Address	RS-232
Syslog Server	TLS
Synergy Server	TLS
SNMP Trap Host	SNMPv3
SSH Client	n/a
Web Browser Client	HTTPS

Table 10. Secure IP Protocols Between TOE Components

3.8.4 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.

CATEGORY	PRODUCT	MANUAL
LAYER 2 DISTRIBUTION CARDS	MMA10G-IPX-16-CC	MMA10G-IPX Series-CC High Bandwidth 10GE Switch Fabric User Manual,” Version 1.0, January 2017
	MMA10G-IPX-32-CC	
	MMA10G-IPX-64-CC	
SIGNAL TRANSCEIVERS	SFP10G-TR13	
	SFP10G-TR15S	
	SFP10G-TR15H	
	SFP10G-TRCxxH*	
	SFP10G-TRDxxxH*	
	SFPTR-RJ45-SGM-GI	
	SFP1G-TR13	
	SFP1G-TR15S	
CONTROL FRAMES	EMX1-FR	EMX Series Multiframe User Manual, Version 1.3, August 2014
	EMX1-FR+PS	
	EMX3-FR	
	EMX3-FR+3PS	
	EMX6-FR	
	EMX6-FR+6PS	
CONTROL FRAME MANAGEMENT CARDS	EMX1-PS	
	EMX3-PS	
	EMX6-PS	
	EMX-FC	
MANAGEMENT SOFTWARE	MAGNUM-SC-CC	Magnum User Manual, Version 1.3, April 2016 MAGNUM – SDVN Management and Control of Evertz IP Switch Fabrics and Gateways User Manual, Version 0.1, November 2014 MAGNUM-SDVN Security Administration Manual, Revision 12, March 22, 2017

Table 11. List of Evertz Operating Mnuals

3.9 Conformance Claims (ASE_CCL)

3.9.1 Common Criteria Claims

The following conformance claims are made for the TOE and ST:

- **CC v3.1, Rev. 3 Conformant**
  The ST and TOE are conformant to Common Criteria version 3.1, Revision 4.

- **Part 2 Extended**
  The ST is Common Criteria Part 2 extended.

- **Part 3 Conformant**
  The ST is Common Criteria Part 3 Conformant.

- **PP Conformant**
  The ST complies to the NDcPP (Collaborative Protection Profile "Security Requirements for Network Devices"), Version 1.0, with additional requirements drawn from Appendix C of the NDcPP.

3.9.2 NIAP Technical Decisions

IPX conforms to the requirements of the following NIAP Technical Decisions:

- 0235 NIT Technical Decision adding DH group 14 to the selection in FCS_CKM.2
  FCS_CKM.2 – Adds optional cybersuites that IPX does not use.

- 0228 NIT Technical Decision for CA certificates - basicConstraints validation
  FIA_X509_EXT.1.2 Test change only; no change to the Security Target.

- 0227 NIT Technical Decision for TOE acting as a TLS Client and RSA key generation
  FCS_CKM.1 - Makes a client-side requirement optional; IPX already does this.

- 0226 NIT Technical Decision for TLS Encryption Algorithms
  FCS_TLSC_EXT.2.1 & FCS_TLSS_EXT.2.1 One ciphersuite no longer mandatory; slight wording change only.

- 0225 NIT Technical Decision for Make CBC cipher suites optional in IPsec
  IPX does not use IPSec, so this does not apply.

- 0224 NIT Technical Decision Making DH Group 14 optional in FCS_IPSEC_EXT.1.11
  IPX does not use IPSec, so this does not apply.

- 0223 NIT Technical Decision for "Expected" vs "unexpected" DNs for IPsec Communications
  IPX does not use IPSec, so this does not apply.

- 0201 – NIT Technical Decision for Use of intermediate CA certificates and certificate hierarchy depth
  FCS_TLSS_EXT.1.1 Removed the mandatory selection – only a slight wording change to IPX.

- 0200 – NIT Technical Decision for Password authentication for SSH clients
  IPX does not use SSH, so this does not apply.

- 0199 – NIT Technical Decision for Elliptic Curves for Signatures
  FCS_COP.1.1(2) Changed wording considerably, but actual changes apply to Elliptic Curves, which IPX does not use.

- 0195 – NIT Technical Decision making DH Group 14 optional in FCS_IPSEC_EXT.1.11
  IPX does not use IPSec, so this does not apply.

- 0191 – NIT Technical Decision for Using secp521r1 for TLS communication
  FCS_TLSS_EXT.2.3 Wording change for some options; did not change our wording.

- 0189 – NIT Technical Decision for SSH Server Encryption Algorithms
  IPX does not use SSH, so this does not apply.

- 0188 – NIT Technical Decision for Optional use of X.509 certificates for digital signatures
  FPT_TUD_EXT.1 Made optional what IPX already does. so no change.

- 0187 – NIT Technical Decision for Clarifying FIA_X509_EXT.1 test 1
  FIA_X509_EXT.1.1 Test change only; no change to the Security Target.

- 0186 – NIT Technical Decision for Applicability of X.509 certificate testing to IPSec
  IPX does not use IPSec, so this does not apply.

- 0185 – NIT Technical Decision for Channel for Secure Update.
  FTP_ITC.1 Expanded TSS description to explicitly state how updates are secured.

- 0184 – NIT Technical Decision for Mandatory use of X.509 certificates
  FIA_X509_EXT.[1,2 & 3] X.509 is Mandatory; IPX already uses X.509 certificates.

- 0183 – NIT Technical Decision for Use of the Supporting Document
  No specific SFRs – This clarifies that evaluators do not have to evaluate SFRs that are n/a to the TOE. Applies to testing, not the Security Target.

- 0182 – NIT Technical Decision for Handling of X.509 certificates fellated to SSH-RSA and remote comms
  IPX does not use SSH, so this does not apply.

- 0181 – NIT Technical Decision for Self-testing of integrity of firmware and software.
  FPT_TST_EXT.1 This simply says testing must abide by the SFR. Applies to testing, not the Security Target.

- 0170 - NIT Technical Decision for SNMPv3 Support
  FTP_TRP.1 Disallows the use of SNMPv3 except for "read-only" monitoring, which is how IPX uses it (for alarms).

- 0169 – NIT Technical Decision for Compliance to RFC5759 and RFC5280 for using CRLs
  FIA_X509_EXT.1.1 Wording change to some optional selections; IPX's selection did not change.

- 0168 – NIT Technical Decision for Mandatory requirement for CSR generation
FIA_X509_EXT.3 There was no change.

- 0167 – NIT Technical Decision for Testing SSH 2^28 packets
IPX does not use SSH, so this does not apply.

- 0165 – NIT Technical Decision for Sending the ServerKeyExchange message when using RSA
FCS_TLSC_EXT.1.1 Test change only; no change to the Security Target.

- 0164 – NIT Technical Decision for Negative testing for additional ciphers for SSH
IPX does not use SSH, so this does not apply.

- 0160 – NIT Technical Decision for Transport mode and tunnel mode in IPSEC communications
IPX does not use IPSec, so this does not apply.

- 0156 – NIT Technical Decision for SSL/TLS Version Testing in the NDcPP v1.0 and FW cPP v1.0
FCS_TLSS_EXT.2.2 Slight wording change only.

- 0156 – NIT Technical Decision for SSL/TLS Version Testing in the NDcPP v1.0 and FW cPP v1.0
FCS_TLSS_EXT.2.2 Removed an optional selection that did not affect IPX.

- 0155 – NIT Technical Decision for TLSS tests using ECDHE in the NDcPP v1.0.
FCS_TLSS_EXT.2.3 Testing change for ECDHE, which is not used by IPX.

- 0154 – NIT Technical Decision for Versions of TOE Software in the NDcPP v1.0 and FW cPP v1.0
FPT_TUD_EXT.1.1: Added a selection option that does not apply to IPX.

- 0153 – NIT Technical Decision for Auditing of NTP Time Changes in the NDcPP v1.0 and FW cPP v1.0
FAU_GEN.1: Added clarification that IPX audits NTP time discontinuities.

- 0152 – NIT Technical Decision for Reference identifiers for TLS in the NDcPP v1.0 and FW cPP v1.0
FCS_TLSC_EXT.2 IPX already does this.

- 0151 – NIT Technical Decision for FCS_TLSS_EXT Testing - Issue 1 in NDcPP v1.0.
FCS_TLSS_EXT.1 Test change only; no change to the Security Target.

- 0150 – NIT Technical Decision for Removal of SSH re-key audit events in the NDcPP v1.0 and FW cPP v1.0
IPX does not use SSH, so this does not apply.

- 0143 – NIT Technical Decision for Failure testing for TLS session establishment in NDcPP and FWcPP
FCS_TLSS_EXT.1 Test change only; no change to the Security Target.

- 0130 – NIT Technical Decision for Requirements for Destruction of Cryptographic Keys
FCS_CKM.4.1 Considerable text change; IPX was already compliant.

- 0126 – NIT Technical Decision for TLS Mutual Authentication
FTP_ITC.1 & FCS_TLSC_EXT.1 Application notes change that does not affect IPX.

- 0125 – NIT Technical Decision for Checking validity of peer certificates for HTTPS servers
FCS_HTTPS_EXT.1.3 Wording change; IPX is already compliant.

- 0117 – NIT Technical Decision for FIA_X509_EXT.1.1 Requirement in NDcPP
FIA_X509_EXT.1.1 Added clarification in TSS that IPX's X.509 certificate validation includes revocation checking.

- 0116 – NIT Technical Decision for a Typo in reference to RSASSA-PKCS1v1_5 in NDcPP and FWcPP
FCS_COP.1.1(2) Typo correction.

- 0115 – NIT Technical Decision for Transport mode and tunnel mode in IPsec communication in NDcPP and FWcPP
IPX does not use IPSec, so this does not apply.

- 0114 – NIT Technical Decision for Re-Use of FIPS test results in NDcPP and FWcPP
FCS_COP.1 IPX has not been evaluated for FIPS per se, so this is n/a.

- 0113 – NIT Technical Decision for testing and trusted updates in the NDcPP v1.0 and FW cPP v1.0
FPT_TUD_EXT.1 IPX updates are performed manually, so this is n/a.

- 0112 – NIT Technical Decision for TLS testing in the NDcPP v1.0 and FW cPP v1.0.
(General) Test clarificcation only; no change to the Security Target.

- 0111 – NIT Technical Decision for third party libraries and FCS_CKM.1 in NDcPP and FWcPP
FCS_CKM.1 IPX complies with FIPS 186-4, so this is n/a.

- 0096 – NIT Technical Interpretation regarding Virtualization
(General) – IPX is a physical device, so this is n/a.

- 0095 – NIT Technical Interpretations regarding audit, random bit generation, and entropy in NDcPP
FAU_STG_EXT.1, FCS_COP.1 & FCS_RBG_EXT.1.1 IPX is already compliant.

- 0094 – NIT Technical Decision for validating a published hash in NDcPP
FPT_TUD_EXT & FMT_MOF Application note clarifications; IPX is already compliant.

- 0093 – NIT Technical Decision for FIA_X509_EXT.1.1 Requirement in NDcPP
FIA_X509_EXT, FPT_TST_EXT, FPT_TUD_EXT Addition to Application Notes and test procedures; IPX is already complaint. No Security Target change.

- 0090 – NIT Technical Decision for FMT_SMF.1.1 Requirement in NDcPP
  FMT_SMF.1.1 Adds Hash option; IPX uses a Hash within a Digital Signature; the Security Target was updated accordingly.

These are all the Technical Decisions related to the "collaborative Protection Profile for Network Devices Version 1.0" per the NIAP web site as of 9/25/2017.

4 Definition of the Security Problem

This section identifies the following:

- Significant assumptions about the TOE's operational environment.
- IT related threats to the organization countered by the TOE.
- Environmental threats requiring controls to provide sufficient protection.
- Organizational security policies for the TOE as appropriate.

This document identifies assumptions as A.assumption with "assumption" specifying a unique name. Threats are identified as T.threat with "threat" specifying a unique name. Organizational Security Policies (OSPs) are identified as P.osp with "osp" specifying a unique name.

The security problem & the associated assumptions, threats, etc are taken directly from the NDcPP v. 1.0.

4.1 Assumptions

The following assumptions about the operational environment are made regarding its ability to provide security functionality. If the TOE is placed in an operational environment that does not meet these assumptions, the TOE may not be able to provide all of its security functionality.

Assumption	Assumption Definition
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 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.**
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.**

Table 12. Operational Environment Assumptions

4.1.1 Threat Model

The table below shows the threats that are to be countered by the TOE, its operational environment, or a combination of the two.

Threat Name	Threat Definition
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., 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 themselvesinto 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 include 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	**A component of the network device may fail during start-up or during operations causing a compromise or failure in the security functionality of the network device, leaving the device susceptible to attackers.**

Table 13. Threat Model

4.2 Organizational Security Policies (OSP)

An organizational security policy is a set of rules, practices and procedures imposed by an organization to address its security needs. The table below shows the OSPs that are to be enforced by the TOE, its operational environment or a combination of the two.

Threat Name	Threat Definition
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 14. Organizational Security policies

5 Security Objectives (ASE_OBJ)

This section identifies the security objectives of the TOE and the IT Environment. The security objectives identify the responsibilities of the TOE and the TOE's IT environment in meeting the security needs.

5.1 Security Objectives for the TOE

The collaborative Protection Profile for Network Devices v1.0 does not define any security objectives for the TOE

5.2 Security Objectives for the Operational Environment (OE)

All of the assumptions stated in Section 3.1 are considered to be security objectives for the environment. The following are the Protection Profile non-TOE security objectives, which, in addition to those assumptions, are to be satisfied without imposing technical requirements on the TOE. That is, they will not require the implementation of functions in the TOE hardware and/or software. Thus, they will be satisfied largely through application of procedural or administrative measures.

Those objectives are described in the table below:

Environment Security Objective	IT Environment Security Objective Definition
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 Administrators are trusted to follow and apply all administrator guidance in a trusted manner.
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

Table 15. Security Objectives for the Environment

6 Security Requirements

This section specifies the requirements for the TOE. The security functional requirements correspond to the security functions implemented by the TOE, as required by the PP.

6.1 TOE Security Functional Requirements (SFR)

This sub-section specifies the SFRs for the TOE. It organizes the SFRs by CC classes as per the table below.

CC Functional		Security Functional Requirements	
Class	**Description**	**TOE SFR**	**Description**
FAU	Security Audit	FAU_GEN.1	Audit Data Generation
		FAU_GEN.2	User Identity Association
		FAU_STG_EXT.1	External Audit Trail Storage
FCS	Cryptographic Support	FCS_CKM.1	Cryptographic Key Generation
		FCS_CKM.2	Cryptographic Key Establishment
		FCS_CKM.4	Cryptographic Key Destruction
		FCS_COP.1(1)	Cryptographic Operation (AES Data Encryption/Decryption)
		FCS_COP.1(2)	**Cryptographic Operation (Signature Generation and Verification)**
		FCS_COP.1(3)	Cryptographic Operation (Hash Algorithm)
		FCS_COP.1(4)	Cryptographic Operation (Keyed-Hash Algorithm)
		FCS_RBG_EXT.1	Random Bit Generation
		FCS_TLSC_EXT.1	Explicit: TLS (Client)
		FCS_TLSS_EXT.2	Explicit: TLS (Server)
		FCS_HTTPS_EXT.1	Explicit: HTTPS
FIA	Identification and Authentication	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	X.509 Certificate Validation
		FIA_X509_EXT.2	X.509 Certificate Authentication
		FIA_X509_EXT.3	X.509 Certificate Requests
FMT	Security Management	FMT_MOF.1(1) / Trusted Update	Management of security functions behavior
		FMT_MTD.1	Management of TSF Data
		FMT_SMF.1	Specification of Management Functions
		FMT_SMR.2	Restrictions on Security Roles
FPT	Protection of the TSF	FPT_SKP_EXT.1	Protection of TSF Data (for Reading of All Symmetric Keys)
		FPT_APW_EXT.1	Protection of Administrator Passwords
		FPT_TST_EXT.1	TSF Testing
		FPT_TUD_EXT.1	Trusted Update
		FPT_STM.1	Reliable Time Stamps
FTA	TOE Access	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 Banners
FTP	Trusted Path/Channels	FTP_ITC.1	Inter-TSF Trusted Channel
		FTP_TRP.1	Trusted Path

Table 16. TOE Security Functional Requirements

6.1.1 Security Audit (FAU)

6.1.1.1 FAU.GEN.1 – Audit Data Generation

FAU_GEN1.1 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).*
- *Security related 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).*
- *Starting and stopping services (if applicable)*
- No other actions

d) [Specifically defined auditable events listed in **Table 17.** *TOE Security Functional Requirements and Auditable Events*
e)].

SFR	Auditable Events	Additional Audit Record Contents
FAU_GEN.1	None	
FAU_GEN.2	None	
FAU_STG_EXT.1	None	
FCS_CKM.1	None	
FCS_COP.1(1)	None	
FCS_COP.1(2)	None	
FCS_COP.1(3)	None	
FCS_COP.1(4)	None	
FCS_RBG-EXT.1	None	
FDP_RIP.2	None	
FCS_PMG_EXT.1	None	
FCS_TLSC_EXT.1	Failure to Establish a TLS Session (Client).	Non-TOE Endpoint (IP Address)
		Reason for Failure
	Establishment of a TLS Session (Client)	Non-TOE Endpoint (IP Address)
	Termination of a TLS Session (Client)	Non-TOE Endpoint (IP Address)
FCS_TLSS_EXT.1	Failure to Establish a TLS Session (Server).	Non-TOE Endpoint (IP Address)
		Reason for Failure
	Establishment of a TLS Session	Non-TOE Endpoint (IP Address)

SFR	Auditable Events	Additional Audit Record Contents
	(Server)	
	Termination of a TLS Session (Server)	Non-TOE Endpoint (IP Address)
FCS_HTTPS_EXT.1	Failure to Establish an HTTPS Session.	Non-TOE Endpoint (IP Address)
		Reason for Failure
	Establishment of an HTTPS Session	Non-TOE Endpoint (IP Address)
	Termination of an HTTPS Session	Non-TOE Endpoint (IP Address)
FIA_UIA_EXT.1	All Use of the Identification and Authentication Mechanism	Provided User Identity
		Origin of Attempt (IP Address, etc.)
FIA_UAU_EXT.2	All Use of the Identification and Authentication Mechanism	Origin of Attempt (IP Address, etc.)
FIA_UAU.7	None	
FIA_X509.EXT.1	Unsuccessful attempt to validate a certificate	Reason for failure
FIA_X509.EXT.2	None	None
FIA_X509.EXT.3	None	None
FMT_MOF.1(1) / Trusted Update	Any attempt to initiate a manual update.	None.
FMT_MTD.1	All management activities of TSF data.	None
FMT_SMF.1	None	None
FMT_SMR.2	None	None
FPT_SKP_EXT.1	None	None
FPT_APW_EXT.1	None	None
FPT_TST_EXT.1	None	None
FPT_TUD_EXT.1	Initiation of Update; result of the update attempt	No additional information.
FPT_STM.1	Changes to Time	Old Time Value
		New Time Value
		Origin of Attempt (IP Address, etc.)
FTA_SSL_EXT.1	Any Attempts at Unlocking an Interactive Session	None
FTA_SSL.3	Termination of a Remote Session by the Session Locking Mechanism	None
FTA_SSL.4	Termination of an Interactive Session	None
FTA_TAB.1	None	None
FTP_ITC.1	Initiation of a Trusted Channel	Identification of the Initiator
		Identification of the Target
	Termination of a Trusted Channel	Identification of the Initiator
		Identification of the Target
	Failure of Trusted Channel Functions	Identification of the Initiator

SFR	Auditable Events	Additional Audit Record Contents
		Identification of the Target
FTP_TRP.1	Initiation of a Trusted Path	Identification of Claimed User Identity
	Termination of a Trusted Path	Identification of Claimed User Identity
	Failure of Trusted Path Functions	Identification of Claimed User Identity

Table 17. TOE Security Functional Requirements and Auditable Events

The Evertz administrative guide lists all of these auditable events with associated formats.

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

- Date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event; and
- For each audit type, based on the auditable event definitions of the functional components listed in the PP/ST, *information specified in column three of Table 17.* TOE Security Functional Requirements and Auditable Events
- *above*.

Auditable Event	Audit Record Contents*	Associated SFRs
Webeasy login/logout event,	User Name + (IP address) + <action description>	FCS_HTTPS_EXT.1 FTA_SSL.3 FTA_SSL.4 FTP_TRP.1
All device control/management (i.e., SET) action	Ctrl Name: <control name> + Type: SET + Idx: [*], + from <user name>	FMT_MOF.1(1) / Trusted Update FMT_MTD.1 FPT_TUD_EXT.1
Date change event,	Date change description	FPT_STM.1 FTA_SSL_EXT.1
Login event from serial port,	Event description + user name	FIA_UIA_EXT.1 FIA_UAU_EXT.2 FIA_X509.EXT.1
Syslog client app start/restart event,	Server IP and Port Info	FCS_TLSC_EXT.1 FTP_ITC.1
Data port link status up/down event,	ENS_SW: Port # + Link <UP|Down>	FCS_TLSC_EXT.1 FCS_TLSS_EXT.1 FCS_HTTPS_EXT.1 FTP_ITC.1 FTP_TRP.1
Command from Switch Control System (typically Evertz Magnum)	SYNERGY [client IP] : + <Msg_ID> + <Control description>	FMT_MTD.1
TLS connection with Switch Control System (typically Evertz Magnum)	SYNERGY: + <Msg description> + [Client IP]	FCS_TLSC_EXT.1 FCS_TLSS_EXT.1 FIA_UIA_EXT.1 FIA_UAU_EXT.2 FIA_X509.EXT.1 FTP_ITC.1
TLS connection close with Switch Control System (typically Evertz Magnum)	SYNERGY: + Connection description + Client IP	FCS_TLSC_EXT.1 FCS_TLSS_EXT.1 FTP_ITC.1

*In addition to Timestamp + App Name, which is common to all entries.

Table 18. TOE Auditable Events and Data Fields

6.1.1.2 FAU_GEN.2 – User Identity Association

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

6.1.1.3 FAU_STG_EXT.1 – External Audit Trail Storage

FAU_STG_EXT.1.1 The TSF shall be able to transmit generated audit data to an external IT entity using a trusted channel according to **FTP_ITC.1 – Inter-TSF Trusted Channel**.

NOTE: For the purposes of this ST, the external IT entity is an organizationally-provided syslog server.

FAU_STG_EXT.1.2 The TSF shall be able to store generated audit data on the TOE itself.

FAU_STG_EXT.1.3 The TSF shall overwrite previous audit records according to the following rule: *on a circular (FIFO) basis* when the local storage space for audit data is full.

6.1.2 Cryptographic Support (FCS)

6.1.2.1 FCS_CKM.1 – Cryptographic Key Generation (Refined)

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***

6.1.2.2 FCS_CKM.2 – Cryptographic Key Establishment (Refined)

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 meets the following: NIST Special Publication 800-56B, "Recommendation for Pair-Wise Key Establishment Schemes Using Integer Factorization Cryptography"***

6.1.2.3 FCS_CKM.4 – Cryptographic Key Zeroization

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method:

- *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*.

6.1.2.4 FCS_COP.1(1) – Cryptographic Operation (AES Data Encryption/Decryption)

FCS_COP.1.1(1) The TSF shall perform *encryption/decryption* in accordance with a specified cryptographic algorithm *AES used in* CBC *modes* and cryptographic key sizes 128-bits and 256-bits that meet the following: *AES as specified in ISO 18033-3,* CDC as specified in ISO 10116*.*

6.1.2.5 FCS_COP.1(2) – Cryptographic Operation (Signature Generation and Verification)

FCS_COP.1.1(2) 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.*

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

6.1.2.6 FCS_COP.1(3) – Cryptographic Operation (Hash Algorithm)

FCS_COP.1.1(3) The TSF shall perform *cryptographic hashing services* in accordance with a specified cryptographic algorithm **(**SHA-1**,** SHA-256**)** that meet the following: *ISO/IEC 10118-3:2004*.

6.1.2.7 FCS_COP.1(4) – Cryptographic Operation (Keyed Hash Algorithm)

FCS_COP.1.1(4) The TSF shall perform *keyed-hash message authentication* in accordance with a specified cryptographic algorithm HMAC-SHA-256 and cryptographic key sizes 256 bits and message digest size 256 bits, that meet the following: ISO/IEC 9797-2:2011, Section 7 “MAC Algorithm 2”.

6.1.2.8 FCS_RGB_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_CRBG (AES).

FCS_RBG_EXT.1.2 The deterministic RBG shall be seeded by at least one entropy source that accumulates entropy from *one* software-based noise source with a minimum of 256 bits of entropy at least equal to the greatest security strength, according ISO/IEC 18031:2011 Table C.1 “Security Strength Table for Hash Functions,” of keys and hashes that it will generate.

6.1.3 Identification and Authorization (FIA)

6.1.3.1 FIA_PMG_EXT.1 – Password Management

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

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

6.1.3.2 FIA_UIA_EXT.1 – User Identification and Authorization

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

- Display the warning banner in accordance with FTA_TAB.1;
- ICMP echo

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

6.1.3.3 FIA_UAU_EXT.2 – Extended: Password-Based Authentication Mechanism

FIA_UAU_EXT.2.1 The TSF shall provide a local password-based authentication mechanism to perform administrative user authentication.

6.1.3.4 FIA_UAU.7 – Protected Authentication Feedback

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

6.1.4 Security Management (FMT)

6.1.4.1 FMT_MOF.1(1)/TrustedUpdate – Management of Security Functions Behavior

FMT_MOF.1.1(1)/TrustedUpdate The TSF shall restrict the ability to enable the functions *to perform manual update* to *Security Administrators*.

6.1.4.2 FMT_MTD.1 – Management of TSF Data (for General TSF Data)

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

6.1.4.3 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*
- ***No other capabilities.***

6.1.4.4 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.

6.1.5 Protection of the TSF (FPT)

6.1.5.1 FPT_SKP_EXT.1 – Extended: Protection of TSF Data (for reading of all symmetric keys

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

6.1.5.2 FPT_APW_EXT.1 – Extended: Protection of Security 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 reading of plaintext passwords.

6.1.5.3 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;*
- *from the previous successful upgrade, or in the case of first time upgrade, the one-time user-generated hash value;*
- *Presence of certificate and public key files.*

6.1.5.4 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 the most recently installed version of the TOE/firmware/software.

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 a means to authenticate firmware/software updates to the TOE using a digital signature mechanism, published hash prior to installing those updates.

6.1.5.5 FPT_STM.1 – Reliable Time Stamps

FPT_STM.1.1 The TSF shall be able to provide reliable time stamps.

6.1.6 TOE Access (FTA)

6.1.6.1 FTA_SSL_EXT.1 – TSF-Initiated Session Locking

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

- *lock the session – disable any activity of the user's data access/display devices other than unlocking the session, and requiring that the administrator re-authenticate to the TSF prior to unlocking the session*

after a Security Administrator –specified time period of inactivity.

6.1.7 FTA_SSL.3 – TSF-Initiated Termination

FTA_SSL.3.1 **Refinement:** The TSF shall terminate a **remote** interactive session after *a Security Administrator –configurable time interval of session inactivity*.

6.1.7.1 FTA_SSL.4 – User-Initiated Termination

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

6.1.7.2 FTA_TAB.1 – Default TOE Access Banners

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

6.1.8 Trusted Path/Channels (FTP)

6.1.8.1 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:**

- **Video Switch Control System (such as Evertz' Magnum)**
- **Audit Server**

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 Refinement: 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 system logging.*

6.1.8.2 FTP_TRP.1 – Trusted Path

FTP_TRP.1.1 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 communications 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 Refinement: The TSF shall permit **remote administrators** to initiate communication via the trusted path.

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

6.2 Selection-Based Requirements (Annex B)

IPX performs TLS server-side tasks when communicating with external control interfaces (web browser, dedicated touch panel). When communicating via the web, HTTPS is required. Therefore, FCS_HTTPS and FCS_TLSS applies for these functions.

IPX serves as the client for TLS-based syslog communication. Therefore, FCS_TLSC applies for this function.

6.2.1 Cryptographic Support (FCS)

6.2.1.1 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 The TSF shall establish the connection only if the peer presents a valid certificate during handshake, or the peer initiates handshake.

6.2.1.2 FCS_TLSC_EXT.1– TLS Client Protocol

FCS_TLSC_EXT.1.1 The TSF shall implement TLS1.2 (RFC 5246) supporting 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

FCS_TLSC_EXT.1.2 The TSF shall verify that the presented identifier matches the reference identifier according to RFC 6125.

FCS_TLSC_EXT.1.3 The TSF shall only establish a trusted channel if the peer certificate is valid.

FCS_TLSC_EXT.1.4 The TSF shall present the Supported Elliptic Curves Extension in the Client Hello with the following NIST curves: none and no other curves.

6.2.1.3 FCS_TLSS_EXT.2 – TLS Server Protocol with mutual authentication

FCS_TLSS_EXT.2.1 The TSF shall implement TLS1.2 (RFC 5246) supporting 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

FCS_TLSS_EXT.2.2 The TSF shall deny connections from clients requesting SSL 2.0, SSL 3.0, TLS 1.0 and TLS 1.1.

FCS_TLSS_EXT.2.3 The TSF shall generate key establishment parameters using RSA with key size 2048 bits and no other size and no other**.**

FCS_TLSS_EXT.2.4 The TSF shall support mutual authentication of TLS clients using X.509v3 certificates.

FCS_TLSS_EXT.2.5 The TSF shall not establish a trusted channel is the peer certificate is invalid.

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 peer.

6.2.1.4 FIA_X509_EXT.1 – X.509 Certificate Validation

FIA_X509_EXT.1.1 The TSF shall validate certificates in accordance with the following rules:

- RFC 5280 certificate validation and certificate path validation
- The certificate path must terminate with a trusted CA certificate.
- The TSF shall validate a certificate path by ensuring the presence of the basicConstraints extension and that the CA flag is set to TRUE for all CA certificates.
- 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 The TSF shall use X.509v3 certificates as defined by RFC 5280 to support authentication for TLS, HTTPS, and no additional uses.

6.2.1.5 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 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: allow the administrator to choose whether to accept the certificate in the case of HTTPS; not accept the certificate in the case of TLS.

6.2.1.6 FIA_X509_EXT.3 – X.509 Certificate Requests

FIA_X509_EXT.3.1 The TSF shall generate a Certificate Request Message as specified by RFC 2986 and be able to provide the following information in the request: public key and Common Name, Organization, Organizational Unit, and Country**.**

FIA_X509_EXT.3.2 The TSF shall validate the chain of certificates from the Root CA upon receiving the CA Certificate Response.

7 TOE Security Assurance Requirements

The TOE meets the security assurance requirements of NDPP v1.1. The following table is the summary of those requirements:

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

Table 19. TOE Security Assurance Requirements

8 TOE Summary Specification (TSS)

8.1 Target Security Function (TSF) Overview

The table below summarizes the security functions provided by the TOE.

SECURITY FUNCTION	TOE SCOPE DESCRIPTION
Security Audit (FAU)	IPX generates audit logs that consist of various auditable events or actions. This includes logins, use of trusted channel/path and cryptographic operations. Each audit event contains an associated date/time stamp, a label for the type of event, a user ID (if applicable) and a description of the event. 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 assuming one is connected and configured (the Syslog server is beyond the scope of the TOE). The IPX manual explains how to do this.
Cryptographic Support (FCS)	The cryptographic module protects the management interfaces (TLS/HTTPS). It uses the following cryptographic algorithms: AES128 & 256 (Symmetric Cipher), RSA with 2048 bit keys (Asymmetric Cipher), SHA256 (Hashed MAC), RSA with 2048 bit keys (Digital Signatures), X509 (Certificate Encoding) and DRBG-AES-256-CTR Mode (Random number generation). In addition SNMPv3 is used exclusively for alarms. SNMPv3 uses HMAC-SHA-SHA1 (Authentication Protocol) and CFB-AES-128 (Encryption).
Identification and Authentication (FIA)	The only accounts that the IPX will establish are Security Administrator accounts; Users only control the IPX indirectly via Magnum. CO/Administrative users are identified and authenticated via user name and password prior to performing any operations. The IPX CO/Administrators user accounts module maintains Security Administrator credentials. Since the only role that accesses the IPX directly is that od Security Administrator there is no assignment of roles required. Passwords of 15 characters or more are supported.
I Security Management (FMT)	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. No administrative functionality is available prior to login.

SECURITY FUNCTION	TOE SCOPE DESCRIPTION
Protection of the TSF (FPT)	IPX prevents the unauthorized modification of TSF data. This protection includes self-tests to ensure the correct operation of cryptographic functions. Firmware upgrades (only performed by a Security Administrator) are impossible unless the new firmware first passes two separate authentication tests.The IPX relies on trusted channels to protect communications between itself and other trusted services, such as syslog. Communications between the IPX and a remote administrative user are protected via a trusted path.
TOE Access (FTA)	Security Administrators can configure a maximum allowable period of inactivity for a Security Administrator session. If there is no user interaction with the IPX for the specified amount of time, the session is terminated. The initial, default session timeout is 15 minutes. The IPX also provides for a login banner message to be displayed by the management interfaces (WebEasy or Magnum), to advise Security Administrators regarding the appropriate use of the IPX, and the penalty for its misuse.
Trusted Path/Channels (FTP)	IPX only communicates with Administrative Users via Trusted Paths (using HTTPS). IPX only communicates with other devices via Trusted Channels (using TLS). "Regular" (non-administrative) users only communicate with IPX via a switch control system (such as Evertz' Magnum). From an IPX standpoint this is communicating with another device (and hence uses Trusted Channels).

Table 20. TSF Overview

8.2 TSS Items Requiring Further Specification

8.2.1 Security Audit (FAU)

8.2.1.1 FAU_GEN.1 – Audit Data Generation

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.

8.2.1.2 FAU_GEN.2 – User Identity Association

Each audit event is associated with the user/application that has triggered that event. This user/application is identified by the username used for login or by the application name. For access log events, IP address/hostname may also be included.

8.2.1.3 FAU_STG_EXT.1 – External Audit Trail Storage

Audit data is sent to external syslog server through secured TLS sessions. For this to happen, an external syslog server should be configured (IP address/TCP Port number). A trusted certificate chain that is used to sign syslog server's certificate must be also uploaded to IPX.

IPX stores all audit data locally in a secure location; it is accessible to administrators using the "Syslog" tab on the web interface; this is explained in the manual.

Two files are used, each with a maximum capacity of 900 KB. Initially both files are empty and entries are added to file1. Once file 1 is full, newer entries will be added to file 2 until it becomes full, at which time content of file 1 will be cleared and entries added to file 1 again. Basically the strategy is always switching to the other file when one becomes full.

8.2.2 Cryptographic Support (FCS)

8.2.2.1 FCS_CKM.1 – Cryptographic Key Generation

The TOE supports 2048-bit RSA keys. Key generation is invoked from the platform by first securely wiping any existing key (according to FIPS requirements), then calling "openssl genrsa -out $key_path 2048" (with openssl in FIPS mode).

IPX uses the following OpenSSL module:

- IPX OpenSSL Cryptographic Module, Version 2v0_b1

8.2.2.2 FCS_CKM.2 – Cryptographic Key Establishment

The TOE acts as both sender and recipient for RSA-based key establishment schemes. The underlying platform provides key confirmation services.

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.

8.2.2.3 FCS_CKM.4 – Cryptographic Key Destruction

Cryptographic keys are destroyed by first overwriting the key file content with all 0s. This will be done three times. Then a read-verification will be performed to ensure that the entire content has really been changed to zeros and not any other values. If this steps fails, then the file will be over-written again 3 times with 0s until the read-verify step succeeds.

The following keys are stored:

- the trust CA certificate, which is used for certificate verification;
- the server certificate, which is used for HTTP web service and Magnum TLS connection;
- the private key matching the server certificate, which is used for de-encryption;
- encrypted credential file, which is used for web service login;
- CRL (certificate revocation list) file, which is used for certificate verification;

All of these cryptographic keys are stored in plaintext on nonvolatile NOR flash storage. No direct interface/access is provided to view or modify the contents of these files.

8.2.2.4 FCS_COP.1(1) – Cryptographic Operation(AES Data Encryption/Decryption)

The secure version of the IPX application software forming this TOE is not configurable WRT cryptographic operation. In other words, the system defaults to the selected cryptographic modes and is not alterable when the system is placed into High Security mode.

8.2.2.5 FCS_COP.1(2) – Cryptographic Operation (Signature Generation and Verification)

The TOE implements hashing in byte-oriented mode. HMACs are used for verification of the firmware image and encrypted password files during bootup. The Linux and Web passwords are saved in a partition of the NOR flash memory separate from the firmware image and all executable files. The TOE uses hashing for the following security functions:

- Linux Passwords
- Web Passwords

8.2.2.6 FCS_COP.1(3) – Cryptographic Operation (Hash Algorithm)

SHA-1/SHA256 algorithms are used for TLS. SHA256 is used for firmware integrity check during power-on-self-test and upgrade.

8.2.2.7 FCS_COP.1(4) – Cryptographic Operation (Keyed-Hash Algorithm)

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.

HMAC-SHA-256 is the only keyed-hash message authentication function used by IPX.

8.2.2.8 FCS_RBG_EXT.1 – Random Bit Generation

As determined in *Evertz Microsystems IPX Entropy Assessment Report*, 10 JAN 2017, the Linux kernel on which the IPX application is built uses */dev/random* as the entropy source for all random numbers. The functions which obtain random numbers from the RBG are:

- Haveged
- Linux Kernel Entropy

Please see the *Evertz Microsystems Entropy Assessment Report* for IPX for further information, such as seeding parameters.

8.2.2.9 FCS_TLSC_EXT.1 – Explicit: TLS (Client)

IPX specifies only a restricted set of cipher suites that it supports during the negotiation phase with its peer. If no match of cipher suites can be found with peer, TLS session will not be started. 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

Protocols that do not conform to TLS1.2 are explicitly excluded in IPX's cipher suites

IPX only supports cipher suites that use RSA keys for key exchange and authentication. These keys are generated with OpenSSL's RSA command line utility

This is done by the OpenSSL implementation internally.

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 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/SAN field. The verification against DN/SAN peer certificate is implemented within OpenSSL.

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 the wildcard 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.

8.2.2.10 FCS_TLSS_EXT.2 – Explicit: TLS (Server)

(With IPX the server-side TLS works the same way as the Client side, except that on the server side mutual authentication is supported; see above.)

8.2.2.11 FCS_HTTPS_EXT.1 – Explicit: HTTPS

IPX uses Apache web server's HTTPS implementation to provide a secure interactive webpage interface for remote administrative functions, and to support secure exchange of user authentication parameters during login. HTTPS uses TLS to securely establish the encrypted session. The sessions are not established if peer's certificates can't be validated.

HTTPS is basically HTTP running on top of TLS sessions.

Certificates (IPX's own certificate, trusted CA certificate) can be uploaded on IPX prior to establishing connection with peers. These certificates are used in the TLS handshaking process and is taken care of by TLS protocol implementation.

8.2.3 Identification and Authorization (FIA)

8.2.3.1 FIA_PMG_EXT.1 – Password Management

IPX enforces that passwords must meet minimum requirements (length, mix of number of lower/upper case letters, numbers as well as special characters, no common dictionary words. etc).

Valid passwords are stored as hashed values in /etc/shadow

8.2.3.2 FIA_UIA_EXT.1 – User identification and Authentication

Warning banner is displayed before login prompt becomes ready to accept login credentials from user. Users must acknowledge the warning banner before they can login to the system

Authentication of administrator is based on username/password. Prior to successful login, no interface is exposed to allow unauthorized access.

8.2.3.3 FIA_UAU_EXT.2– Password-Based Authentication Mechanism

Out of the factory, IPX is configured to use a default password. Any user is then required to update their passwords when they login for the first time.

IPX enforces that passwords must meet minimum requirements (length, mix of number of lower/upper case letters, numbers as well as special characters, no common dictionary words. etc).

Valid passwords are stored as hashed values in /etc/shadow.

8.2.3.4 FIA_UAU.7 – Protected Authentication Feedback

On the webpage, solid dots are used when entering a password. On serial port access, no feedback of any sort is used.

8.2.3.5 FIA_X509_EXT.1 – X.509 Certificate Validation

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. They 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. Certificates presented by remote TLS servers or by clients using mutual authentication are 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.

8.2.3.6 FIA_X509_EXT.2 – X.509 Certificate Authentication

Instructions about generating/downloading CSR and loading certificate can be found on IPX manual. The Administrator can only upload one certificate and one 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 mutual authentication. 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.

8.2.3.7 FIA_X509_EXT.3 – X.509 Certificate Requests

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.

8.2.4 Security Management (FMT)

8.2.4.1 FMT_MOF.1(1) / Trusted Update – Management of Security Functions Behavior

IPX implements a role-based access policy. Only users with administrative privilege is allowed to perform image updates.

8.2.4.2 FMT_MTD.1 – Management of TSF Data

IPX implements a role-based access policy. Only users with administrative privilege is allowed to modify configurations.

The (non-administrative) User has no direct access or control over IPX; a (non-administrative) User may only access an IPX card through Magnum. No administrative functionality is available prior to login.

8.2.4.3 FMT_SMF.1 – Specification of Management Functions

The *MMA10G-IPX Series CC (Common Criteria) User Manual* describes the management functions required by this PP. The following management capabilities are described in the manual:

- Login to local console;
- Configure IPX date and time;
- Control port IP configuration;
- Edit login banner;
- Change Linux password for console account "customer";
- Create certificate signing request CSR, download CSR;
- Reset certificate;
- SNMP v3 user create for SNMP TRAP;
- Import certificate;
- Import Trusted CA certificate;
- Zeroize all Critical Security Parameters (CSP);
- Console menu system timeout configuration;

8.2.4.4 FMT_SMR.2 – Restrictions on Security Roles

By default, administrator role is configured to have full access/privilege to manage IPX. Unlike other role types, the set of privileges associated with administrator is fixed .

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.

8.3 Protection of the TSF (FPT)

8.3.1.1 FPT_SKP_EXT.1– Protection of TSF Data (for Reading of All Symmetric Keys)

Cryptographic keys are stored in a directory in flash memory. As there is no command line access, users cannot gain any direct access to these files.

8.3.1.2 FPT_APW_EXT.1 – Protection of Administrator Passwords

No passwords are stored in plaintext. Their hashed values are stored instead 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.

8.3.1.3 FPT_TST_EXT.1 – TSF Testing

Upon enabling FIPS mode (or on power-up with FIPS mode set "on") the algorithm self-tests required by FIPS are performed. After loading the image, a hash value is computed from the memory partition containing the image. This hash values is compared with a pre-stored hash value at another location on flash. The two hash values must match for the boot process to succeed.

8.3.1.4 FPT_TUD_EXT.1 – Trusted Update

The site administrators do not have access to install any application. The IPX embedded system can only be updated with the valid firmware release from Evertz. Operators may verify the current version with Web GUI.

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 local stored public key. There's no way to change the local stored public key by administrators. When HMAC verification passes, IPX will verify the firmware binary header with Evertz-defined proprietary format. If there's no mismatch, the new firmware code will overwrite the current one.

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.

8.3.1.5 FPT_STM.1 – Reliable Time Stamps

Timestamps found in auditable log events use system clock on IPX. Administrators can set the system time clock through serial port console menu after each card reboot.

Timestamps found in auditable log events come from system time on IPX. The system time of IPX can only be set through serial port console menu by administrator. 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.

8.4 TOE Access (FTA)

8.4.1.1 FTA_SSL_EXT.1– TSF-Initiated Session Locking

Current session will be terminated. Unsaved changes will be discarded. Administrators need to re-login before attempting more configuration changes.

8.4.1.2 FTA_SSL.3 – TSF-Initiated Termination

The same thing happens as above, except it is initiated from the web interface.

8.4.1.3 FTA_SSL.4 – User-Initiated Termination

An Administrator may terminate his own session (web page) by clicking on “Logout” at the upper right of the screen, or (serial console) typing “x” to exit.

8.4.1.4 FTA_TAB.1 – Default TOE Access Banner

An Administrator may 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 type / overtype the “Agree” text and/or the “Disagree” text. (The “Disagree” text shows up when a user “disagrees” with the Security Banner text. A user who does this is not logged into the system.)

8.5 Trusted Path/Channels (FTP)

8.5.1.1 FTP_ITC.1– Inter-TSF Trusted Channel

IPX sets up trusted channels with Magnum and syslog servers through the TLS protocol. Specifically, the handshaking process must occur and succeed before application level communication could occur.

Furthermore, once session is established, TLS ensures the confidentiality, integrity and authenticity of the communication data.

8.5.1.2 FTP_TRP.1 – Trusted Path

IPX sets up trusted path with administrators over secure HTTPS session, which again uses TLS as the underlying security protocol to protect communications. Like with trust channels,

TLS handshake needs to be performed prior to HTTPS session establishment, which ensures communications only happen with trusted parties. TLS also ensures the confidentiality, integrity and authenticity of the communication data

Appendix A. Glossary of Terms

TERM	DEFINITION
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
ECDSA	Elliptic Curve Digital Signature Algorithm
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)
NTP	Network Time Protocol
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