National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

Validation Report

for the

MMA10G-EXE Series

Report Number: CCEVS-VR-VID11428-2024

Dated: April 5, 2024

Version: 1.0

National Institute of Standards and Technology
Information Technology Laboratory
100 Bureau Drive
Gaithersburg, MD 20899

Department of Defense
ATTN: NIAP, SUITE: 6982
9800 Savage Road
Fort George G. Meade, MD 20755-6982

ACKNOWLEDGEMENTS

Validation Team

Lauren Brandt

Lisa Mitchell

Linda Morrison

Lori Sarem

The MITRE Corporation

Common Criteria Testing Laboratory

Shehan D Dissanayake
Ashish Panchal

Acumen Security, LLC

Table of Contents

1 Executive Summary

This Validation Report (VR) is intended to assist the end user of this product and any security certification Agent for that end user in determining the suitability of this Information Technology (IT) product for their environment. End users should review the Security Target (ST), which is where specific security claims are made, in conjunction with this VR, which describes how those security claims were tested and evaluated and any restrictions on the evaluated configuration. Prospective users should carefully read the Assumptions and Clarification of Scope in Section 5 and the Validator Comments in Section 10, where any restrictions on the evaluated configuration are highlighted.

This report documents the National Information Assurance Partnership (NIAP) assessment of the evaluation of the MMA10G-EXE Series Target of Evaluation (TOE). It presents the evaluation results, their justifications, and the conformance results. This VR is not an endorsement of the TOE by any agency of the U.S. Government and no warranty of the TOE is either expressed or implied. This VR applies only to the specific version and configuration of the product as evaluated and documented in the ST.

The evaluation was completed by Acumen Security in April 2024. The information in this report is largely derived from the evaluation's proprietary Evaluation Technical Report (ETR) and associated test report, all written by Acumen Security. The evaluation determined that the product is both Common Criteria Part 2 Extended and Part 3 Conformant and meets the assurance requirements of the *Collaborative Protection Profile for Network Devices, Version 2.2e, 23 March 2020* (NDcPP22e).

The TOE identified in this VR has been evaluated at a NIAP approved Common Criteria Testing Laboratory (CCTL) using the Common Methodology for IT Security Evaluation (Version 3.1, Rev. 5) for conformance to the Common Criteria for IT Security Evaluation (Version 3.1, Rev. 5), as interpreted by the Assurance Activities contained in the Protection Profile (PP). This VR applies only to the specific version of the TOE as evaluated. The evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme and the conclusions of the testing laboratory in the ETR are consistent with the evidence provided.

The validation team provided guidance on technical issues and evaluation processes, and reviewed the individual work units documented in the ETR and the Assurance Activities Report (AAR). The validation team found that the evaluation showed that the product satisfies all of the functional requirements and assurance requirements stated in the ST. Based on these findings, the validation team concludes that the testing laboratory's findings are accurate, the conclusions justified, and the conformance results are correct. The conclusions of the testing laboratory in the ETR are consistent with the evidence produced.

The technical information included in this report was obtained from the *MMA10G-EXE Series Security Target,* Version 1.4, dated March 19, 2024, and analysis performed by the validation team.

2 Identification

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards and Technology (NIST) effort to establish commercial facilities to perform trusted product evaluations.

Under this program, security evaluations are conducted by commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs). CCTLs evaluate products against PPs containing Assurance Activities, which are interpretations of Common Evaluation Methodology (CEM) work units specific to the technology described by the PP.

The NIAP Validation Body assigns Validators to monitor the CCTLs to ensure quality and consistency across evaluations. Developers of IT products desiring a security evaluation contract with a CCTL and pay a fee for their product's evaluation. Upon successful completion of the evaluation, the product is added to NIAP's Product Compliant List.

Table 1 provides information needed to completely identify the product, including:

- The Target of Evaluation (TOE): the fully qualified identifier of the product as evaluated.
- The Security Target (ST), describing the security features, claims, and assurances of the product.
- The conformance result of the evaluation.
- The Protection Profile(s) to which the product is conformant.
- The organizations and individuals participating in the evaluation.

Table 1: Evaluation Identifiers

Item	Identifier
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
TOE	MMA10G-EXE Series
Protection Profile	*Collaborative Protection Profile for Network Devices,* Version 2.2e*, 23 March 2020*
Security Target	*MMA10G-EXE Series Security Target,* Version 1.4, 19 March 2024
Evaluation Technical Report	*Evaluation Technical Report for MMA10G-EXE Series,* Version 1.3, 28 March 2024
CC Version	Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 5
Conformance Result	CC Part 2 Extended and CC Part 3 Conformant
Sponsor	Evertz Microsystems Ltd.
Developer	Evertz Microsystems Ltd. 5292 John Lucas Drive Burlington, Ontario CANADA
Common Criteria Testing Lab (CCTL)	Acumen Security Rockville, MD
CCEVS Validators	Lauren Brandt, Lisa Mitchell, Linda Morrison, Lori Sarem

3 Architectural Information

Note: The following architectural description is based on the description presented in the Security Target.

The MMA10G-EXE Series switches are Internet Protocol (IP) switches optimized for video-over-IP traffic (compressed or uncompressed). The TOE is classified as a network device (a generic infrastructure device that can be connected to a network). Models of the EXE included in the evaluation provide identical functionality. The only differences between them are the supported speed, the physical size, and the number of physical interfaces supported, and the processor. These differences are detailed at the end of this section.

The EXE 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. The EXE provides the same capability within the context of packet-based networks using shared network infrastructure.

The TOE provides a packet-based switching fabric from a video perspective, rather than relying on traditional packet-based network architecture.

A typical EXE installation will also include a standard video routing switch software platform (such as Evertz Magnum) to route data 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, and non-network based video switching/processing, 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.

The TOE provides secure remote management using an HTTPS/TLS web interface. Administrators only may access EXE via a dedicated management workstation operating over an Out-of-Band Management (OOBM) network. Sites may close this OOBM network or may operate EXE within an existing OOBM as long as the topology is compliant with the security parameters listed below. Users and administrators may also access EXE software via direct connection using a terminal session.

The TOE generates audit logs and transmits the audit logs to a remote syslog server over an authenticated TLS channel. The TOE verifies the authenticity of software updates by verifying the digital signature prior to installing any update.

The summary of the evaluated functionality provided by the TOE includes the following,

- Secure connectivity with remote audit servers and secure retention of audit logs locally
- Identification and authentication of the administrator of the TOE
- Secure remote administration of the TOE via TLS and secure Local administration of the TOE
- Secure access to the management functionality of the TOE

- Secure software updates
- Secure communication with the non-TOE 'video switch control systems' via TLS.

The TOE hardware devices are the Evertz:

Model	AV/ Broadcast	Supported Ports	Form Factor	Chassis Supported	Frame Controller	Processor
MMA10G-EXE16	AV	16 x QSFP28 cages per line card	16	EXE	EXE16-FC-NCS	Intel(R) Xeon(R) E3-1505M v5
MMA10G-EXE26	AV	16 x QSFP28 cages per line card	26	EXE	EXE-FC-NCS	Intel(R) Xeon(R) E3-1505M v5
MMA10G-EXE36	AV	16 x QSFP28 cages per line card	36	EXE	EXE-FC-NCS	Intel(R) Xeon(R) E3-1505M v5
EXE2.0-16-10G-A1	broadcast	16 x QSFP28 cages per line card	16	EXE	EXE16-FC-NCS	Intel(R) Xeon(R) E3-1505M v5
EXE2.0-16-25G-A1	broadcast	16 x QSFP28 cages per line card	16	EXE	EXE16-FC-NCS	Intel(R) Xeon(R) E3-1505M v5
EXE2.0-26-10G-A1	broadcast	16 x QSFP28 cages per line card	26	EXE	EXE-FC-NCS	Intel(R) Xeon(R) E3-1505M v5
EXE2.0-26-25G-A1	broadcast	16 x QSFP28 cages per line card	26	EXE	EXE-FC-NCS	Intel(R) Xeon(R) E3-1505M v5
EXE2.0-36-10G-A1	broadcast	16 x QSFP28 cages per line card	36	EXE	EXE-FC-NCS	Intel(R) Xeon(R) E3-1505M v5
EXE2.0-36-25G-A1	broadcast	16 x QSFP28 cages per line card	36	EXE	EXE-FC-NCS	Intel(R) Xeon(R) E3-1505M v5
EXE2.0-16-10G-A2	broadcast	16 x QSFP28 cages per line card	16	EXE	EXE16-FC-NCS	Intel(R) Xeon(R) E3-1505M v5
EXE2.0-16-25G-A2	broadcast	16 x QSFP28 cages per line card	16	EXE	EXE16-FC-NCS	Intel(R) Xeon(R) E3-1505M v5
EXE2.0-26-10G-A2	broadcast	16 x QSFP28 cages per line card	26	EXE	EXE-FC-NCS	Intel(R) Xeon(R) E3-1505M v5
EXE2.0-26-25G-A2	broadcast	16 x QSFP28 cages per line card	26	EXE	EXE-FC-NCS	Intel(R) Xeon(R) E3-1505M v5
EXE2.0-36-10G-A2	broadcast	16 x QSFP28 cages per line card	36	EXE	EXE-FC-NCS	Intel(R) Xeon(R) E3-1505M v5
EXE2.0-36-25G-A2	broadcast	16 x QSFP28 cages per line card	36	EXE	EXE-FC-NCS	Intel(R) Xeon(R) E3-1505M v5
NATX-8-100G-CC	broadcast	4 x DD QSFP (QSFP200G)	1	DragonFire frame	N/A	Intel(R) Core (TM) i3-4102E C
NATX-16-100G-CC	broadcast	8 x DD QSFP (QSFP200G)	1	DragonFire frame	N/A	Intel(R) Core (TM) i3-4102E C
NATX-32-100G-1-CC	broadcast	16 x DD QSFP (QSFP200G)	1	DragonFire frame	N/A	Intel(R) Core (TM) i3-4102E C
NATX-64-100G-2-CC	broadcast	32 x DD QSFP (QSFP200G)	1	DragonFire frame	N/A	Intel(R) Core (TM) i3-4102E C
MMA10G-NATX-8-CC	AV	4 x DD QSFP (QSFP200G)	1	DragonFire frame	N/A	Intel(R) Core (TM) i3-4102E C

MMA10G-NATX-16-CC	AV	8 x DD QSFP (QSFP200G)	1	DragonFire frame	N/A	Intel(R) Core (TM) i3-4102E C
MMA10G-NATX-32-CC	AV	16 x DD QSFP (QSFP200G)	1	DragonFire frame	N/A	Intel(R) Core (TM) i3-4102E C
MMA10G-NATX-64-CC	AV	32 x DD QSFP (QSFP200G)	1	DragonFire frame	N/A	Intel(R) Core (TM) i3-4102E C
MMA10G-IPX128	AV	32 x QSFP+	3 or 6	EV Frame	ev3-FC or ev6-FC	Intel(R) Core (TM) i3-4102E C
3080IPX-48-25G-CC	AV/broadcast	12 x QSFP+	3 or 6	EV Frame	ev3-FC or ev6-FC	Intel(R) Core (TM) i3-4102E C

The EXE firmware version 1.5 will be referred to as EXE throughout this document.

The EXE appliances are Ethernet switches optimized for video content.

4 Security Policy

The TOE provides the security functions required by the *Collaborative Protection Profile for Network Devices*, Version 2.23, 23 March 2020, hereafter referred to as NDcPP v2.2e or NDcPP.

4.1 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. 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
- Changes to trust anchors in the TOE's trust store
- Any update attempts
- Result of the update attempt
- Management of TSF data
- Changes to Time
- Session termination for inactivity
- Power-on self tests verification
- Changes to audit server configuration
- Users locked out due to failed authentication attempts

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 are authorized to edit them, copy or delete (clear) them. Audit records are protected from unauthorized modifications and deletions.

The TSF provides the capability to view audit data by using the Syslog tab in the local console. 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.

4.2 Cryptographic Support

The TOE includes an OpenSSL library (Version 1.1.1k with Fedora Patches) that implements CAVP validated cryptographic algorithms for random bit generation, encryption/decryption, authentication, and integrity protection/verification. These algorithms are used to provide security for the TLS/HTTPs connections for secure management and secure connections to a syslog and authentication servers. TLS and HTTPs are also used to verify firmware updates. The cryptographic services provided by the TOE are described below:

Table 1 – TOE Cryptographic Protocols

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

Each of these cryptographic algorithms have been validated for conformance to the requirements specified in their respective standards, as identified below and are part of the EXE Cryptographic Module.

Table 2 – CAVP Algorithm Testing References

Algorithm	Standard	CAVP Certificate #	Processors
AES 128/256-bit CBC, GCM	IOS 19772 (GCM)	A2573	Intel(R) Core (TM) i3-4102E C (Haswell)
			Intel(R) Xeon(R) E3-1505M v5 (Skylake)
CTR DRBG using AES 256	ISO/IEC 18031:2011	A2573	Intel(R) Core (TM) i3-4102E C (Haswell)

			Intel(R) Xeon(R) E3-1505M v5 (Skylake)
EC-DH	NIST SP 800-56A (key establishment)	A2573	Intel(R) Core (TM) i3-4102E C (Haswell)
			Intel(R) Xeon(R) E3-1505M v5 (Skylake)
ECDSA	FIPS PUB 186-4 (key generation)	A2573	Intel(R) Core (TM) i3-4102E C (Haswell)
			Intel(R) Xeon(R) E3-1505M v5 (Skylake)
HMAC-SHA-1/256/384	ISO/IEC 9797-2:2011	A2573	Intel(R) Core (TM) i3-4102E C (Haswell)
			Intel(R) Xeon(R) E3-1505M v5 (Skylake)
SHA-1/256/384	ISO/IEC 10118-3:2004	A2573	Intel(R) Core (TM) i3-4102E C (Haswell)
			Intel(R) Xeon(R) E3-1505M v5 (Skylake)
RSA 2048/3072	FIPS PUB 186-4 (key generation and Digital Signature) ISO/IEC 9796-2 (digital signature)	A2573	Intel(R) Core (TM) i3-4102E C (Haswell)
			Intel(R) Xeon(R) E3-1505M v5 (Skylake)

4.3 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” EXE users do not access EXE directly; they control IP video switching through the EXE using a switch control system, such as Evertz’s Magnum. The switching of those IP video transport streams 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 username and password for password-based authentication. The identification and authentication credentials are confirmed against a local user database. Only after the Administrator presents the correct identification and authentication credentials will access to the TOE functionality be granted. If the user fails to provide the correct authentication credentials, the user will be locked out after a configurable threshold until the user is manually unlocked by an Administrator.

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

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

The EXE 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.

The TOE uses X.509v3 certificates as defined by RFC 5280 to support authentication for TLS/HTTPS connections.

4.4 Security Management

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

- Administer the TOE locally and remotely;
- Configure the access banner;
- Configure the session inactivity time before session termination or locking;
- Update the TOE, and to verify the updates using digital signature capability prior to installing those updates;
- Specify the time limits of session inactivity;
- Ability to modify the IP address and the port of the remote syslog server;
- Generate Certificate Signing Requests, import and manage x509 certificates, delete/replace x509 certificates;
- Re-enable an Administrator account;
- Set the time which is used for time-stamps.

All these management functions are restricted to Security Administrators who are authorized to administer the TOE via a local CLI and a remote web interface. Administrators are individuals who manage specific types of administrative tasks. The EXE implements role-based access control of these management functions to users that have been identified, authenticated, and authorized with the Security Administrator role.

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 these services can be managed from the interface, 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.

4.5 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.

An administrator initiates update processes from the web interface for all update installations. EXE automatically uses the RSA digital signature mechanism to confirm the integrity of the product before installing the update.

4.6 TOE Access

Aside from the automatic Administrators session termination due to inactivity described 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.

4.7 Trusted Path/Channels

The TOE allows the establishment of a trusted channel between a video control system (such as Evertz' Magnum) and the EXE. The TOE also establishes a secure connection for sending syslog data to a syslog server using TLS.

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

5 Assumptions and Clarification of Scope

5.1 Assumptions

The specific conditions listed in the following subsections are assumed to exist in the TOE's environment. These assumptions include both practical realities in the development of the TOE security requirements and the essential environmental conditions on the use of the TOE.

The assumptions included in Table 4 are drawn directly from NDcPP.

Table 4 – Assumptions

ID	Assumption
A.PHYSICAL_PROTECTION	The Network Device is assumed to be physically protected in its operational environment and not subject to physical attacks that compromise the security 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 does not include any requirements on physical tamper protection or other physical attack mitigations. The cPP does 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. For vNDs, this assumption applies to the physical platform on which the VM runs.
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 a computing platform for general purpose applications (unrelated to networking functionality). If a virtual TOE evaluated as a pND, following Case 2 vNDs as specified in Section 1.2, the VS is considered part of the TOE with only one vND instance for each physical hardware platform. The exception being where components of a distributed TOE run inside more than one virtual machine (VM) on a single VS. In Case 2 vND, no non-TOE guest VMs are allowed on the platform.
A.NO_THRU_TRAFFIC_PROTECTION	A standard/generic Network Device does not provide any assurance regarding the protection of traffic that traverses it. The intent is for the Network Device to protect data that originates on or is destined to the device itself, to include administrative data and audit data. Traffic that is traversing the Network Device, destined for another network entity, is not covered by the ND cPP. It is assumed that this protection will be covered by cPPs and PP-Modules for particular types of Network Devices (e.g., firewall).

ID	Assumption
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 appropriately trained, following policy, and adhering to guidance documentation. Administrators are trusted to ensure passwords/credentials have sufficient strength and entropy and to lack malicious intent when administering the device. The Network Device is not expected to be capable of defending against a malicious Administrator that actively works to bypass or compromise the security of the device. For TOEs supporting X.509v3 certificate-based authentication, the Security Administrator(s) are expected to fully validate (e.g. offline verification) any CA certificate (root CA certificate or intermediate CA certificate) loaded into the TOE's trust store (aka 'root store', ' trusted CA Key Store', or similar) as a trust anchor prior to use (e.g. offline verification).
A.REGULAR_UPDATES	The Network Device firmware and software is assumed to be updated by an Administrator on a regular basis in response to the release of product updates due to known vulnerabilities.
A.ADMIN_CREDENTIALS_SECURE	The Administrator's credentials (private key) used to access the Network Device are protected by the platform on which they reside.
A.RESIDUAL_INFORMATION	The Administrator must ensure that there is no unauthorized access possible for sensitive residual information (e.g. cryptographic keys, keying material, PINs, passwords etc.) on networking equipment when the equipment is discarded or removed from its operational environment.

5.2 Clarification of Scope

The scope of this evaluation was limited to the functionality and assurances covered in NDcPP22e as described for this TOE in the ST. Other functionality included in the product was not assessed as part of this evaluation. All other functionality provided by the devices needs to be assessed separately, and no further conclusions can be drawn about their effectiveness. All evaluations (and all products) have limitations, as well as potential misconceptions that need clarifying. This text covers some of the more important limitations and clarifications of this evaluation. Note that:

- As with any evaluation, this evaluation only shows that the evaluated configuration meets the security claims made in accordance with the evaluation activities specified in NDcPP22e and performed by the Evaluation team.

- This evaluation covers only the specific software version identified in this document and referenced in the *MMA10G-EXE Series Security Target v1.4*, 19 March 2024 and not any earlier or later versions released or in process.
- Apart from the Admin Guides identified in Section 6, additional customer documentation for the specific software version and platform versions was not included in the scope of the evaluation and, therefore, should not be relied upon when configuring or operating the device as evaluated.
- Consistent with the expectations of the PP, this evaluation did not specifically search for, nor seriously attempt to counter, vulnerabilities that were not "obvious" or vulnerabilities to objectives not claimed in the ST. The CEM defines an "obvious" vulnerability as one that is easily exploited with a minimum of understanding of the TOE, technical sophistication and resources.
- The evaluation of security functionality of the product was limited to the functionality specified in the NDcPP. Any additional security related functional capabilities included in the product were not covered by this evaluation.

6 Documentation

The following documents were provided by the vendor with the TOE for evaluation:

- *MMA10G-EXE Series Security Administrative Guide Addendum for Common Criteria*, Version 1.2, March 19, 2024

Any additional customer documentation provided with the product, or that is available online was not included in the scope of the evaluation and therefore should not be relied upon when configuring or operating the device as evaluated.

To use the product in the evaluated configuration, the product must be installed and configured as specified in *MMA10G-EXE Series Security Administrative Guide Addendum for Common Criteria*, version 1.2, March 19, 2024. Consumers are encouraged to download the configuration guide from the NIAP website to ensure the device is configured as evaluated.

7 TOE Evaluated Configuration

7.1 Evaluated Configuration

Sections 1.2 and 1.3 of the ST provides an overview of the TOE architecture, including physical boundaries, security functions, and relevant TOE documentation and references.

7.1.1 Physical Boundaries and IT Testing Environment Components

The physical boundaries of the TOE are outlined in Section 1.3 of the ST. All physical boundaries are required in the TOE Environment. The IT Testing Environment components used to test the TOE are shown in Table 5 of the ST.

7.1.2 Security Functions Provided by the TOE

The TOE provides the security functions required by the Collaborative Protection Profile for Network Devices, hereafter referred to as NDcPP v2.2e or NDcPP.

7.2 Excluded Functionality

The following product functionality is not included in the CC evaluation:

- SNMP Traps (Alarms)
- SNMP
- VistaLINK PRO module
- Network Time Protocol (NTP) Server
- External Authentication Servers for administrator authentication

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

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

8 IT Product Testing

This Section describes the testing efforts of the developer and the evaluation team. It is derived from information contained in the ETR, which is not publicly available. The AAR provides an overview of testing and the prescribed assurance activities.

8.1 Developer Testing

No evidence of developer testing is required in the Assurance Activities for this product.

8.2 Evaluation Team Independent Testing

The evaluation team verified the product according to the vendor-provided guidance documentation and ran the tests specified in the *Collaborative Protection Profile for Network Devices*, Version 2.2e, 23 March 2020. The Independent Testing activity is documented in the AAR, which is publicly available, and is not duplicated here.

9 Results of the Evaluation

The results of the assurance requirements are generally described in this Section and are presented in detail in the proprietary documents: the Detailed Test Report (DTR) and the ETR. The reader of this document can assume that all activities and work units received a passing verdict.

A verdict for an assurance component is determined by the resulting verdicts assigned to the corresponding evaluator action elements. The evaluation was conducted based upon CC version 3.1 Rev. 5 and CEM version 3.1 Rev. 5. The evaluation determined the TOE Name to be Part 2 extended, and meets the SARs contained in the PP. Additionally, the evaluator performed the Assurance Activities specified in the claimed PP.

9.1 Evaluation of Security Target

The evaluation team applied each ASE CEM work unit. The ST evaluation ensured the ST contains a description of the environment in terms of policies and assumptions, a statement of security requirements claimed to be met by the MMA10G-EXE that are consistent with the Common Criteria, and product security function descriptions that support the requirements. Additionally, the evaluation team performed an assessment of the Assurance Activities specified in the *Collaborative Protection Profile for Network Devices*, Version 2.2e, 23 March 2020.

The validation team reviewed the work of the evaluation team and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.2 Evaluation of Development Documentation

The evaluation team applied each ADV CEM work unit. The evaluation team assessed the design documentation and found it adequate to aid in understanding how the TSF provides the security functions. The design documentation consists of a functional specification contained in the ST's TOE Summary Specification. Additionally, the evaluator performed the Assurance Activities specified in the *Collaborative Protection Profile for Network Devices*, Version 2.2e, 23 March 2020 related to the examination of the information contained in the TOE Summary Specification.

The validation team reviewed the work of the evaluation team and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the Assurance Activities, and that the conclusion reached by the evaluation team was justified.

9.3 Evaluation of Guidance Documents

The evaluation team applied each AGD CEM work unit. The evaluation team ensured the adequacy of the user guidance in describing how to use the operational TOE. Additionally, the evaluation team ensured the adequacy of the administrator guidance in describing how to securely administer the TOE. The guides were assessed during the design and testing phases of the evaluation to ensure they were complete. Additionally, the evaluator performed the Assurance Activities specified in the *Collaborative Protection Profile for Network Devices*, Version 2.2e, 27 March 2020 related to the examination of the

information contained in the operational guidance documents.

The validation team reviewed the work of the evaluation team and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the Assurance Activities, and that the conclusion reached by the evaluation team was justified.

9.4 Evaluation of Life Cycle Support Activities

The evaluation team applied each ALC CEM work unit. The evaluation team found that the TOE was identified.

The validation team reviewed the work of the evaluation team and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.5 Evaluation of Test Documentation and the Test Activity

The evaluation team applied each ATE CEM work unit. The evaluation team ran the set of tests specified by the Assurance Activities in the *Collaborative Protection Profile for Network Devices*, Version 2.2e, 27 March 2020 and recorded the results in a Test Report, summarized in the ETR and AAR.

The validation team reviewed the work of the evaluation team and found that sufficient evidence was provided by the evaluation team to show that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.6 Vulnerability Assessment Activity

The evaluation team applied each AVA CEM work unit. The evaluation team performed a public search for vulnerabilities, performed vulnerability testing and did not discover any issues with the TOE.

The validation team reviewed the work of the evaluation team and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.7 Summary of Evaluation Results

The evaluation team's assessment of the evaluation evidence demonstrates that the claims in the ST are met. Additionally, the evaluation team's test activities also demonstrated the accuracy of the claims in the ST.

The validation team's assessment of the evidence provided by the evaluation team is that it demonstrates that the evaluation team followed the procedures defined in the CEM, and correctly verified that the product meets the claims in the ST.

10 Validator Comments & Recommendations

The validation team notes that the evaluated configuration is dependent upon the TOE being configured per the evaluated configuration instructions in the *MMA10G-EXE Series Security Administrative Guide Addendum for Common Criteria*, Version 1.2, March 19, 2024. As stated in the Clarification of Scope, the evaluated functionality is scoped exclusively to the security functional requirements specified in the ST, and the only evaluated functionality was that which was described by the SFRs claimed in the ST. All other functionality provided by the TOE needs to be assessed separately and no further conclusions can be drawn about its effectiveness.

This TOE has been evaluated and certified by NIAP for use solely in the physical environments described in the Security Target.

11 Annexes

Not applicable.

12 Security Target

The Security Target is identified as: *MMA10G-EXE Series Security Target,* Version 1.4, 19 March 2024.

13 Glossary

The following definitions are used throughout this document:

- **Common Criteria Testing Laboratory (CCTL).** An IT security evaluation facility accredited by the National Voluntary Laboratory Accreditation Program (NVLAP) and approved by the CCEVS Validation Body to conduct Common Criteria-based evaluations.
- **Conformance.** The ability to demonstrate in an unambiguous way that a given implementation is correct with respect to the formal model.
- **Evaluation.** The assessment of an IT product against the Common Criteria using the Common Criteria Evaluation Methodology to determine whether or not the claims made are justified; or the assessment of a protection profile against the Common Criteria using the Common Evaluation Methodology to determine if the Profile is complete, consistent, technically sound and hence suitable for use as a statement of requirements for one or more TOEs that may be evaluated.
- **Evaluation Evidence.** Any tangible resource (information) required from the sponsor or developer by the evaluator to perform one or more evaluation activities.
- **Feature.** Part of a product that is either included with the product or can be ordered separately.
- **Target of Evaluation (TOE).** A group of IT products configured as an IT system, or an IT product, and associated documentation that is the subject of a security evaluation under the CC.
- **Validation.** The process carried out by the CCEVS Validation Body leading to the issue of a Common Criteria certificate.
- **Validation Body.** A governmental organization responsible for carrying out validation and for overseeing the day-to-day operation of the NIAP Common Criteria Evaluation and Validation Scheme.

14 Bibliography

The Validation Team used the following documents to produce this Validation Report:

1. *Common Criteria for Information Technology Security Evaluation - Part 1: Introduction and general model,* Version 3.1 Revision 5.
2. *Common Criteria for Information Technology Security Evaluation - Part 2: Security functional requirements*, Version 3.1 Revision 5.
3. *Common Criteria for Information Technology Security Evaluation - Part 3: Security assurance requirements*, Version 3.1 Revision 5.
4. *Common Evaluation Methodology for Information Technology Security Evaluation*, Version 3.1 Revision 5.
5. *Collaborative Protection Profile for Network Devices,* Version 2.2e, 23 March 2020
6. *Evaluation Technical Report for MMA10G-EXE Series,* Version 1.3, 28 March 2024
7. *MMA10G-EXE Series Security Administrative Guide Addendum for Common Criteria*, Version 1.2, MARCH 19, 2024.
8. *MMA10G-EXE Series Security Target,* Version 1.4, 19 March 2024.
9. *Vulnerability Assessment for Everts MMA10G-EXE*, Version 1.2, 20 March 2024.
10. *Assurance Activity Report for MMA10G-EXE Series*, Version 1.3, March 28, 2024.
11. *Test Report for Evertz MMA10G-EXE Series, Tested TOE Model: EXE2.0-16-25G-A1*, Version 1.2, 20-03-2024.
12. *Test Report for Evertz MMA10G-EXE Series, Tested TOE Model: MMA10G-IPX-128*, Version 1.2, 20-03-2024.
13. *Test Report for Evertz MMA10G-EXE Series, Tested TOE Model: NATX-64-100G*, Version 1.2, March 20, 2024.