National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

TM

Validation Report

for the

MMA10G-IPX Series, Version 1.0

Report Number:	**CCEVS-VR-VID11009-2019**
Dated:	**December 17, 2019**
Version:	**0.1**

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

National Security Agency
Information Assurance Directorate
9800 Savage Road STE 6740
Fort George G. Meade, MD 20755-6740

ACKNOWLEDGEMENTS

Validation Team

Paul Bicknell: Senior Validator
Jenn Dotson: ECR Team
Randy Heimann: ECR Team
Linda Morrison: Lead Validator

Common Criteria Testing Laboratory

Brad Mitchell

Kathleen Moyer

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-IPX 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 December 2019. The information in this report is largely derived from the 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 Extended and meets the assurance requirements defined in the U.S. Government Protection Profile for Security Requirements for collaborative Protection Profile for Network Devices, Version 2.1 [NDcPP].

The Target of Evaluation (TOE) identified in this Validation Report has been evaluated on-site at the Evertz facility 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 collaborative Protection Profile for Network Devices, Version 2.1. The TOE was located in a physically protected, access controlled, designated test area with no unattended entry/exit ways. The customer facilitated testing, but testing was performed by Acumen employees only at the Evertz facility. This Validation Report 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 evaluation technical report 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 Security Target (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 evaluation technical report are consistent with the evidence produced.

2 Identification

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards 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 Protection Profile containing Assurance Activities, which are interpretation of 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 information technology 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 Compliance 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-IPX Series
Protection Profile	collaborative Protection Profile for Network Devices, Version 2.1, September 24, 2018
Security Target	MMA10G-IPX Series V.7 December 3, 2019
Evaluation Technical Report	Evaluation Technical Report for MMA10G-IPX Series running IPX v3.2, V3.0, December 3, 2019
CC Version	Version 3.1, Revision 5
Conformance Result	CC Part 2 Extended and CC Part 3 Extended
Sponsor	Evertz Microsystems Ltd. 5292 John Lucas Drive Burlington, Ontario CANADA
Developer	Evertz Mircosystems Ltd. 5292 John Lucas Drive Burlington, Ontario CANADA
Common Criteria	Acumen Security

Testing Lab (CCTL)	Rockville, MD
CCEVS Validators	Paul Bicknell, Jenn Dotson, Randy Heimann, Linda Morrison

3 Architectural Information

3.1 TOE Product Type

The TOE is a network-based audio video distribution system and is classified as a network device (a generic infrastructure device that can be connected to a network). The IPX appliances are Ethernet switches optimized for video content.

3.2 TOE Usage

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

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

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

4 Security Policy

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

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

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

4.2 Cryptographic Support

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

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

The TOE provides the capability to set password rules. This is to ensure the use of strong passwords in attempts to protect against brute force attacks.

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

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

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.

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.

4.6 TOE Access

Aside from the automatic Administrator session termination due to inactivity, 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 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.

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.

4.8 TOE Documentation

In addition, the following Common Criteria documentation is included:

- MMA10G-IPX Security Target v0.7, December 3, 2019
- IPX MMA10G-IPX Security Administration Manual Revision 1d, December 5, 2019

Other References

- collaborative Protection Profile for Network Devices, Version 2.1 [NDcPP], September 24, 2018

5 Assumptions, Threats & Clarification of Scope

5.1 Assumptions

The assumptions are drawn directly from the [NDcPP].

5.2 Threats

The threats are drawn directly from the [NDcPP].

5.3 Clarification of Scope

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, with a certain level of assurance. The level of assurance for this evaluation is defined within the collaborative Protection Profile for Network Devices, Version 2.1.
- Consistent with the expectations of the Protection Profile, 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 claimed PPs. 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:

- IPX Security Target v0.7, December 3, 2019
- IPX MMA10G-IPX Security Administration Manual Revision 1d, December 5, 2019

7 TOE Evaluated Configuration

7.1 Evaluated Configuration

The evaluated configuration of the TOE is described in the [ST], and after being configured according to all directives and instructions in the [AGD]. Additionally, the TOE requires the following components of the operational environment to be present and correctly operating:

Component	Required	Usage/Purpose Description for TOE performance
Syslog server	Yes	• Conformant with RFC 5424 (Syslog Protocol) • Supporting Syslog over TLS (RFC 5425) • Acting as a TLSv1.2 server • Supporting Client Certificate authentication • Supporting at least one of the following cipher suites: o TLS_RSA_WITH_AES_128_CBC_SHA o TLS_RSA_WITH_AES_256_CBC_SHA o TLS_RSA_WITH_AES_128_CBC_SHA256 o TLS_RSA_WITH_AES_256_CBC_SHA256 o TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 o TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
Management Workstation with web browser	Yes	• Internet Explorer 11, Google Chrome 50, or Firefox 38 • Supporting TLSv1.2 • Supporting Client Certificate authentication • Supporting at least one of the following ciphersuites: o TLS_RSA_WITH_AES_128_CBC_SHA o TLS_RSA_WITH_AES_256_CBC_SHA o TLS_RSA_WITH_AES_128_CBC_SHA256 o TLS_RSA_WITH_AES_256_CBC_SHA256 o TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 o TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
CRL Server	Yes	• Conformant with RFC 5280
MAGNUM Server	Yes	• Provides remote management of the TOE's routing and switching of video signals • Supporting TLSv1.2 with at least one of the following ciphersuites: o TLS_RSA_WITH_AES_128_CBC_SHA o TLS_RSA_WITH_AES_256_CBC_SHA o TLS_RSA_WITH_AES_128_CBC_SHA256 o TLS_RSA_WITH_AES_256_CBC_SHA256

Component	Required	Usage/Purpose Description for TOE performance
		○ TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ○ TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
Media Gateway	No	• Optional component for converting media streams. Not required for TOE operation.
Video Source devices	No	• Optional component for creating video streams that are sent to the TOE. Not required for TOE operation. • Supporting packetized or digital video
Video Destination devices	No	• Optional component for viewing video streams output by the TOE. Not required for TOE operation. • Supporting packetized or digital video

7.2 Excluded Functionality

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

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

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

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

8 IT Product Testing

This section describes the testing efforts of the developer and the evaluation team. It is derived from information contained in Evaluation Test Report for MMA10G-IPX Series, which is not publicly available. The Assurance Activities Report 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 the vendor-provided guidance documentation and ran the tests specified in the *collaborative Protection Profile for Network Devices, Version 2.1*. The Independent Testing activity is documented in the Assurance Activities Report, 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 Evaluation Technical Report (ETR). The reader of this document can assume that 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 MMA10G-IPX Series to be Part 2 extended, and meets the SARs contained in the PP. Additionally the evaluator performed the Assurance Activities specified in the NDcPP.

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-IPX Series that are consistent with the Common Criteria, and product security function descriptions that support the requirements. Additionally the evaluator performed an assessment of the Assurance Activities specified in the collaborative Protection Profile for Network Devices, Version 2.1.

The validators reviewed the work of the evaluation team and agreed with their practices and findings.

9.2 Evaluation of Development Documentation

The evaluation team applied each EAL 1 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 Security Target's TOE Summary Specification. Additionally, the evaluator performed the Assurance Activities specified in the collaborative Protection Profile for Network Devices, Version 2.1 related to the examination of the information contained in the TOE Summary Specification.

The validators reviewed the work of the evaluation team and agreed with their practices and findings.

9.3 Evaluation of Guidance Documents

The evaluation team applied each EAL 1 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 2.1 related to the examination of the information contained in the operational guidance documents.

The validators reviewed the work of the evaluation team and agreed with their practices and findings.

9.4 Evaluation of Life Cycle Support Activities

The evaluation team applied each EAL 1 ALC CEM work unit. The evaluation team found that the TOE was identified.

The validators reviewed the work of the evaluation team and agreed with their practices and findings.

9.5 Evaluation of Test Documentation and the Test Activity

The evaluation team applied each EAL 1 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 2.1 and recorded the results in a Test Report, summarized in the Evaluation Technical Report and Assurance Activities Report.

The validators reviewed the work of the evaluation team and agreed with their practices and findings.

9.6 Vulnerability Assessment Activity

The evaluation team applied each EAL 1 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 validators reviewed the work of the evaluation team and agreed with their practices and findings.

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 validators reviewed the work of the evaluation team and agreed with their practices and findings.

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. Common Criteria Supplemental User Guide. No versions of the TOE and software, either earlier or later were evaluated.

Please note that the functionality evaluated is scoped exclusively to the security functional requirements specified in the Security Target. Other functionality included in the product was not assessed as part of this evaluation. Other functionality provided by devices in the operational environment, such as the audit server, need to be assessed separately and no further conclusions can be drawn about their effectiveness.

11 Annexes

Not applicable.

12 Security Target

IPX Security Target v0.7, December 3, 2019

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.