National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme Validation Report

Motorola Solutions, Inc.

Motorola Network Devices, S6000 and GGM 8000 with EOS version 16.9

Report Number: CCEVS-VR-VID10738-2017
Dated: March 23, 2017
Version: 1.0

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 6940
Fort George G. Meade, MD 20755-6940

Acknowledgements

Validation Panel

Rob Heald

Jerome Myers

Ken Stutterheim

The Aerospace Corporation

Common Criteria Testing Laboratory

Brad Mitchell, Kenji Yoshino

UL Verification Services Inc.

San Luis Obispo, CA

Table of Contents

1 Executive Summary

This report documents the NIAP validators' assessment of the CCEVS evaluation of the Motorola Network Devices, S6000 and GGM 8000 with EOS version 16.9.0.40

This report is intended to assist the end-user of this product with determining the suitability of this IT product in their environment. End-users should review both the Security Target (ST), which is where specific security claims are made, in conjunction with this Validation Report (VR), which describes how those security claims were evaluated.

The Motorola Network Device models S6000 and GGM 8000 provide a flexible routing solution for integrated data, voice and virtual private network (VPN) applications.

These solutions feature the Motorola Enterprise OS software suite with a choice of two hardware platforms: S6000/GGM 8000 series. Each series provides different throughput and scalability capabilities. The common OS software provides Enterprise networking features including: traffic shaping and Quality of Service (QoS), WAN/LAN connectivity, Voice & Multi-Service and Network Management support.

The Network Device features a comprehensive Administrative-user interface that allows for the setup, configuration, monitoring and management of the device using a Command Line Interface (CLI) over a local console interface or secured over an SSHv2 secured connection.

Cryptographic algorithms implemented by the TOE are NIST validated.

This table identifies components that must be present in the Operational Environment to support the operation of the TOE.

Component	Description
RADIUS	Authentication Server (optional)[1] with IPsec peer capabilities
Syslog Host	Syslog host for offloading of audit records with IPsec peer capabilities
NTP Server	NTP Server with IPsec peer capabilities
SSHv2 client	SSHv2 client to support Administrative tunnels to the TOE
Serial Console	Console to perform local administration of the TOE.
HTTP Server for CRL	CRL Distribution Point

Table 1: Operational Environment Components

[1] If your organization requires authentication failure counters and account lockouts for remote accounts, ensure your RADIUS Server supports these features.

2 Identification of the TOE

Table 2 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 organizations and individuals participating in the evaluation.

Evaluation Scheme	United States Common Criteria Evaluation Validation Scheme
Evaluated Target of Evaluation	Motorola Network Devices, S6000 and GGM 8000 with EOS version 16.9.0.40
Protection Profile	collaborative Protection Profile for Network Devices, v1.0, February 27, 2015
Security Target	Motorola Network Router Security Target, Version 1.1, March 22, 2017
Completion Date	March 22, 2017
Conformance Result	Pass - Exact Conformance
Common Criteria Version	3.1r4
Common Evaluation Methodology (CEM) Version	3.1r4
Evaluation Technical Report (ETR)	16-3324-R-0070 V1.2
Sponsor/Developer	Motorola Solutions, Inc.
Common Criteria Testing Lab (CCTL)	UL Verification Services Inc.
CCTL Evaluators	Brad Mitchell, Kenji Yoshino
CCEVS Validators	Rob Heald, Jerome Myers, Ken Stutterheim

Table 2: Product Identification

3 Interpretations

The Evaluation Team performed an analysis of the international interpretations of the CC and the CEM and determined that none of the International interpretations issued by the Common Criteria Interpretations Management Board (CCIMB) were applicable to this evaluation.

The TOE is also compliant with all international interpretations with effective dates on or before

October 12, 2016.

4 Security Policy

This section contains the product features and denotes which are within the logical boundaries of the TOE. The following Security Functions are supported by the TOE:

4.1 Audit

- The TOE will audit all events and information defined in Table 11 in the Security Target.
- The TOE will also include the identity of the user that caused the event (if applicable), date and time of the event, type of event, and the outcome of the event.
- The TOE protects storage of audit information from unauthorized deletion.
- The TOE prevents unauthorized modifications to the stored audit records.
- The TOE can transmit audit data to an external IT entity using IPsec protocol.

4.2 Cryptographic Operations

The TSF performs the following cryptographic operations:

- SSH with AES-CBC-128 or AES-CBC-256 for protection of remote administrative sessions.
- IPsec with AES-CBC-128 or AES-CBC-256 for protection of communication paths with RADIUS, Syslog, and NTP hosts/servers.
- The TSF zeroizes all plaintext secret and private cryptographic keys and CSPs once they are no longer required.

4.3 Identification and Authentication

- The TSF supports passwords consisting of alphanumeric and special characters. The TSF also allows administrators to set a minimum password length and support passwords with 15 characters or more.
- The TSF requires all administrative-users to authenticate before allowing the user to perform any actions other than:
    - Viewing the warning banner
    - ARP
    - ICMP
    - Routing Services
    - BFD Send
    - DHCP Services
    - SSH
    - IPDV (port UDP/49402)
    - RSVP (port UDP/1698)
    - NTP (port UDP/123)
- The TSF allows for authentication via password or public-key infrastructure (PKI).
- All authentication information is obfuscated.
- The TOE supports the use of X.509 certificates for the purposes of IPsec peer authentication, including support for creating and validating certificates.

4.4 Security Management

- The TOE manages the following TSF data:
  - User account names
  - User passwords
  - Internally generated cryptographic keys
  - Imported SSH public keys
- The only role in the TOE is that of the Administrator.
- All administration is performed over an SSH connection or via direct console session.

4.5 Protection of the TSF

- The TSF prevents the reading of secret and private keys.
- The TOE provides reliable time stamps for itself.
- The TOE runs a suite of self-tests during the initial start-up (upon power on) to demonstrate the correction operation of the TSF.
- The TOE provides a means to verify firmware/software updates to the TOE using a digital signature mechanism prior to installing those updates.

4.6 TOE Access

- The TOE, for local interactive sessions, terminates the administrative session after an Authorized Administrator-specified period of session inactivity.
- The TOE terminates a remote interactive session after an Authorized Administrator-configurable period of session inactivity.
- The TOE allows Administrator-initiated termination of the Administrator's own interactive session.
- Before establishing an administrative user session, the TOE is capable of displaying an Authorized Administrator-specified advisory notice and consent warning message regarding unauthorized use of the TOE.

4.7 Trusted Path/Channels

- The TOE uses IPsec to provide a trusted communication channel between itself and all authorized IT entities 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.
- The TOE permits the TSF, or the authorized IT entities to initiate communication via the trusted channel.
- The TOE permits remote administrators to initiate communication over SSH.
- The TOE requires the use of the trusted path for initial administrator authentication and all remote administration actions.

5 TOE Security Environment

5.1 Secure Usage Assumptions

The following assumptions are made about the usage of the TOE:

Table 3: Assumptions	
Assumption	Description
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.

5.2 Threats Countered by the TOE

The TOE is designed to counter the following threats:

Table 4: Threats	
Threat	Description
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

Table 4: Threats	
Threat	Description
	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 themselves into the network stream and perform a man-in-the-middle attack. The result is the critical network traffic is exposed and there could be a loss of confidentiality and integrity, and potentially the network device itself could be compromised.
T.UPDATE_COMPROMISE	Threat agents may attempt to provide a compromised update of the software or firmware which undermines the security functionality of the device. Non-validated updates or updates validated using non-secure or weak cryptography leave the update firmware vulnerable to surreptitious alteration.
T.UNDETECTED_ACTIVITY	Threat agents may attempt to access, change, and/or modify the security functionality of the network device without administrator awareness. This could result in the attacker finding an avenue (e.g., misconfiguration, flaw in the product) to compromise the device and the administrator would have no knowledge that the device has been compromised.
T.SECURITY_FUNCTIONALITY_COMPROMISE	Threat agents may compromise credentials and device data enabling continued access to the network device and its critical data. The compromise of credentials 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.

5.3 Organizational Security Policies

The TOE enforces the following OSPs:

Table 5: Organizational Security Policies	
OSP	Description
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.

5.4 Clarification of Scope

All evaluations (and all products) have limitations, as well as potential misconceptions that need clarification. This text covers some of the more important limitations and clarifications of this evaluation. Note that:

1. As with any evaluation, this evaluation only shows that the evaluated configuration meets the security claims made, with a certain level of assurance (the assurance activities specified in the claimed PPs and performed by the evaluation team).

2. This evaluation covers only the specific software version identified in this document, and not any earlier or later versions released or in process.

3. The evaluation of security functionality of the product was limited to the functionality specified in the claimed PPs. Any additional security related functional capabilities of the product discussed in supporting documentation were not covered by this evaluation. In particular, the following list of services provided by the models is outside the scope of this evaluation:

- Firewall capabilities
- Routing capabilities
- Gateway capabilities
- Protocol Authentication
- Support for FRF.17 as noted in the Security Target
- VoIP capabilities
- Virtual Port Tunneling
- WAN Concentrator

4. This evaluation did not specifically search for, nor attempt to exploit, 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.

Architectural Information

The TOE is classified as Network Device for Common Criteria purposes. The TOE is made up of the following hardware and software components:

5.5 TOE Hardware

The TOE consists of the following:

5.5.1 GGM 8000

Table 6: GGM 8000 Hardware	
Tanapa Number	Description
CLN1841F Rev AB	GGM 8000 Base Unit
CLN8787A Rev B	FIPS 140-2 Kit
CLN1850A Rev G	AC Power Option[2]
CLN1849C Rev AA	DC Power Option[3]
	Choice of Pluggable Modules for the GGM 8000 from Table 4
	Optional Analog CCGW support

With EOS Software SW/GGM8000-KS, 16.9.0.40 and Firmware BM/GGM8000, 16.9.0.40.

5.5.2 S6000

Table 7: S6000 Hardware	
Tanapa Number	Description
CLN1780L Rev FB	S6000 Base Unit
CLN8261D Rev NA	Encryption Module
	Choice of Pluggable Modules for the S6000 from Table 4
	Optional Analog CCGW support

With EOS Software SW/S6000-GS, 16.9.0.40 and Firmware FW/S6000, 16.9.0.40.

Table 8: Pluggable Module Combinations by Hardware Platform Shaded = N/A Numbers indicate possible configuration options (number of modules supported per chassis). A single hardware platform device of one of the two shown is required.		
Module Type	S6000	GGM 8000
T1/E1 (WAN/Telco), 2 ports per module		0, 1, 2
T1/E1 (UltraWAN), 4 ports per module	0, 1, 2	
T1/E1, 12 ports per module	0, 1, 2	
FlexWAN Serial, 1 port per module		0, 1, 2
FlexWAN Serial, 4 ports per module	0, 1, 2	
V.24, 2 ports per module		0, 1, 2
T3/E3, 2 ports (one T3/E3) per module	0, 1, 2	

[2] Either the AC or DC Power Option must be selected.

[3] Either the AC or DC Power Option must be selected.

Table 9: Hardware Features		
Implementation Characteristics	S6000	GGM 8000
CPU Internal Operating Frequency	1GHz	1GHz
Level-1 Instruction Cache Size / Structure	32KB, 8-Sets (Built-In)	32KB, 8-Way Set Associative
Level-1 Data Cache Size / Structure	32KB, 8-Sets (Built-In)	32KB, 8-Way Set Associative
Level-2 Cache Size	512KB (Built-In)	512KB
Cache Coherency on Shared Memory Accesses	Yes	Yes
Shared Memory Type	SDRAM	DDR2
Shared Memory Size	256 MB (DIMM)	512 MB
Shared Memory Bus Width	64 Bits	64 Bits
Shared Memory Peak Transfer Rate	1,064 MBS (133 MTS)	3,200 MBS
Embedded SW (Flash PROM Memory)	1 MB	32 MB
Flash File System (Flash PROM Memory)	16 MB	64 MB
Built-In LAN Ports	3 - 10/100	4 – 10/100/1000
Built-In WAN Ports	None	2 – T1/E1
Pluggable Module Options4	Slots for two I/O Modules	Slots for two I/O Modules
Analog CCGW option (4 Port E&M Analog module and DSP module)	No	Yes

The guidance documentation that is part of the TOE is listed in Section 6.

5.6 TOE Software

TOE's of model type S6000 operate EOS Software SW/S6000-GS, 16.9.0.40 and Firmware FW/S6000, 16.9.0.40.

TOEs of model type GGM-8000 operate EOS Software SW/GGM8000-KS, 16.9.0.40 and Firmware BM/GGM8000, 16.9.0.40.

6 Documentation

This section details the documentation that is (a) delivered to the customer, and (b) was used as evidence for the evaluation of the Motorola Network Devices, S6000 and GGM 8000 with EOS version 16.9. In these tables, the following conventions are used:

- Documentation that is delivered to the customer is shown with **bold** titles.
- Documentation that was used as evidence but is not delivered is shown in a normal typeface.
- Documentation that is delivered as part of the product but was not used as evaluation is shown with a hashed background.

[4] Table 2 specifies the maximum number of each module type that each base unit supports.

The TOE is shipped via normal channels to the customer. The guidance documents are provided in the box with the hardware, and are available via the vendor website, and apply to the CC Evaluated configuration:

6.1 Design Documentation

Document	Revision	Date
Assurance Documentation	N/A	N/A

6.2 Guidance Documentation

Document	Revision	Date
Network Device S6000 and GGM 8000 with EOS Version 16.9 Common Criteria User Guide	1.2	July 28, 2016
Enterprise OS Software Version 16.9 Reference Guide	N/A	June 28, 2016
Enterprise OS Software Version 16.9 User Guide	N/A	June 28, 2016
GGM 8000 Hardware User Guide	N/A	May 30, 2016
S6000 Hardware User Guide	N/A	May 30, 2016

6.3 Configuration Management and Lifecycle

Document	Revision	Date
Assurance Documentation	N/A	N/A

6.4 Test Documentation

Document	Revision	Date
16-3324-R-0031 V1.0 NDcPP Test Plan-v1 6 1	1.3	March 22, 2017

The test documentation is evaluation sensitive, and was summarized in the evaluation associated Assurance Activity Report.

6.5 Vulnerability Assessment Documentation

Vulnerability assessment was performed as part of ATE, and is documented in Section 8 of the test report cited in Section 6.4, above.

6.6 Security Target

Document	Revision	Date
Motorola Network Router Security Target	1.1	March 22, 2017
Motorola Network Routers Entropy Assessment Report	0.3	April 13, 2016

The Entropy Assessment Report is evaluation sensitive and was provided to NIAP for assessment. It is not publically available.

7 IT Product Testing

This section describes the testing efforts of the Developer and the Evaluation Team.

7.1 Developer Testing

The developer performed all test cases specified in NDcPP, and verified the correct behavior of the TOE.

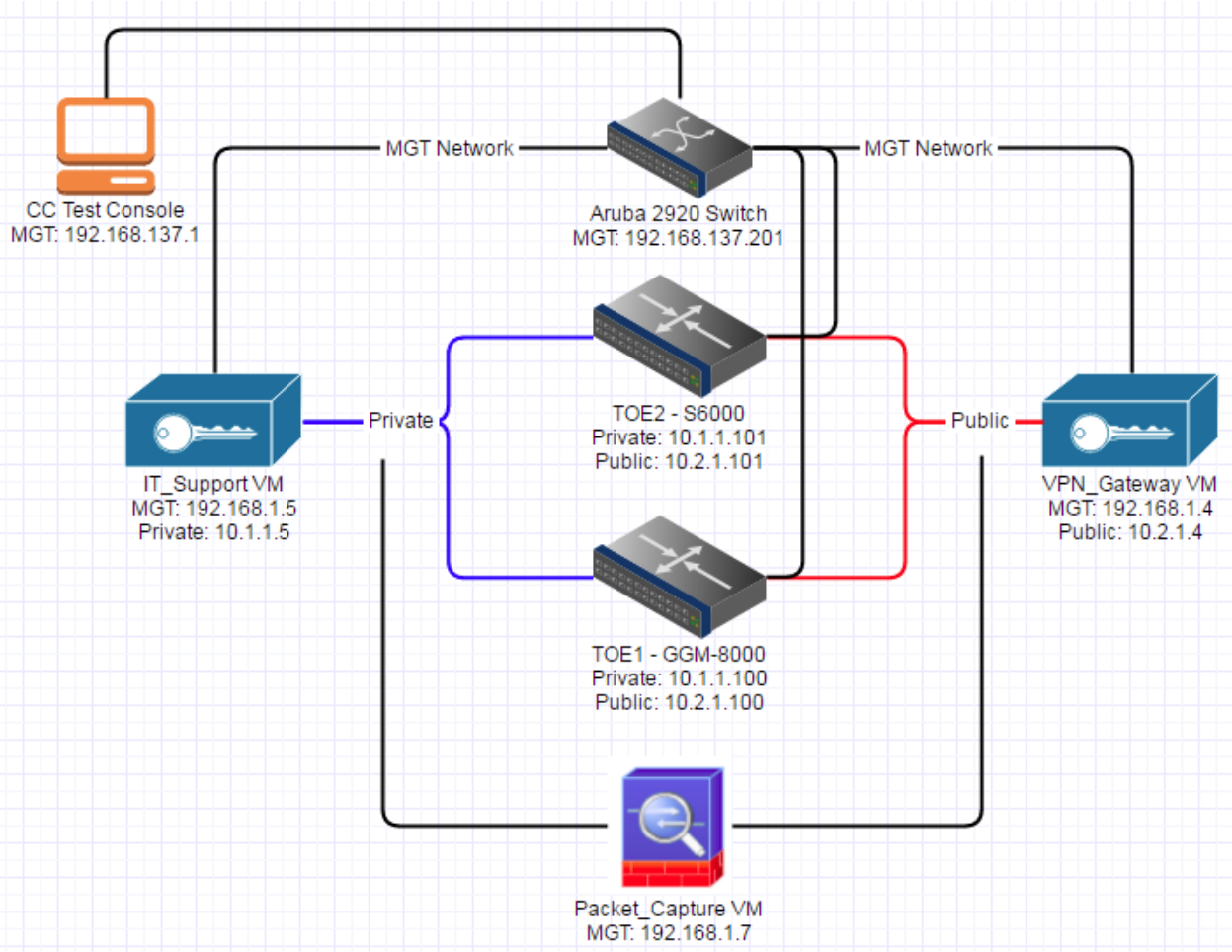
7.2 Evaluation Team Independent Testing

The CCTL (UL Verification Services Inc.) generated the testing plan and designed the testing activities specified in the collaborative Protection Profile for Network Devices v1.0, February 27, 2015 and generated automated and manual tests to execute the designed test plan.

The evaluation team verified the product conformities during the period July 11 - July 30, 2016 at the CCTL according to the Motorola Network Router Security Target, v0.3, July 28, 2016 and ran the tests specified in the collaborative Protection Profile for Network Devices v1.0, February 27, 2015 document. An updated Security Target v1.1 has been generated, addressing the updated wording of certain SFRs based on Technical Decisions. These modifications do not affect the assurance activities in any way, and the evaluation team therefore believes that the test results performed with Security Target v0.3 are applicable to Security Target v1.1.

The test configurations and tools used to evaluate the TOE are described in the Assurance Activity Report (AAR) Section 4, “Testing Environment”.

7.3 Test configuration



The CCTL developed a custom testing environment for NDcPP-based evaluations that uses several virtual machines, isolated networks, and smart switches in order to meet the requirements stated by the testing assurance activities.

7.4 Vulnerability Analysis

All testing assurance activities and vulnerability assessment (AVA_VAN) activities were performed against the TOE by the CCTL.

The evaluation team performed an internet based search using the following search terms:

- Motorola
- Mnr
- GGM-8000
- S6000
- Motorola Network Router

The evaluator only received results for products that were not the TOE (i.e., other Motorola products such as mobile devices or cable modems). The evaluator then received a list of all third-party network-visible libraries in use by the TOE, and searched for relevant vulnerabilities for these modules.

A thorough report of vulnerability assessment activities may be found in the AAR Section 3.5.

8 Results of the Evaluation

The evaluation was carried out in accordance with the Common Criteria Evaluation and Validation Scheme (CCEVS) processes and procedures. The TOE was evaluated against the criteria contained in the Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 4. The evaluation methodology used by the Evaluation Team to conduct the evaluation is the Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 4.

UL has determined that the TOE meets the security criteria in the Security Target, which specifies assurance requirements specified in collaborative Protection Profile for Network Devices, v1.0, February 27, 2015. A team of Validators, on behalf of the CCEVS Validation Body, monitored the evaluation. The evaluation was completed in December 2016.

9 Validator Comments/Recommendations

The products evaluated were evaluated against the Collaborative Protection Profile for Network Devices. Although the products provide extensive functionality, only the security functional requirements associated with the protection profile were evaluated. All other claims of device functionality were not tested and no claims can be made regarding their effectiveness or correct operation.

10 Security Target

Motorola Network Router Security Target, Version 1.1, March 22, 2017.

11 Terms

11.1 Acronyms

CC	Common Criteria
CSP	Critical Security Parameters
DAC	Discretionary Access Control
EAL	Evaluation Assurance Level
FIPS	Federal Information Processing Standards Publication 140-2
IDS	Intrusion Detection System
IPS	Intrusion Prevention System
I/O	Input/Output

MIB	Management Information Base
NIST	National Institute of Standards and Technology
OCSP	Online Certificate Status Protocol
PP	Protection Profile
SF	Security Functions
SFR	Security Functional Requirements
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions

12 Bibliography

[1] Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model, dated September 2012, Version 3.1 Revision 4, CCMB-2012-09-001.

[2] Common Criteria (CC) for Information Technology Security Evaluation – Part 2: Security functional components, September 2012, Version 3.1, Revision 4, CCMB-2012-09-002.

[3] Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance components, September 2012, Version 3.1, Revision 4, CCMB-2012-09-003.

[4] Common Methodology for Information Technology Security Evaluation – Evaluation methodology, September 2012, Version 3.1, Revision 4, CCMB-2012-09-004.

[5] Assurance Activity Report VID 10738, 16-3324-R-0069, V1.2, March 22, 2017, UL Verification Services Inc.

[6] Common Criteria Evaluation Technical Report VID10378, 16-3324-R-0070 Version 1.2, March 22, 2017, UL Verification Services Inc. [Evaluation Sensitive]

[7] Motorola Network Router Security Target, 16-3324-R-0008, Version 1.1, March 22, 2017, UL Verification Services Inc. and Motorola Solutions Inc.

[8] Network Device S6000 and GCM8000 with EOS Version 16.9 Common Criteria User Guide, Common Criteria Supplement Version 1.2, 2016, Motorola Solutions Inc.

[9] Enterprise OS Software Version 16.9 Reference Guide, June 2016, Motorola Solutions Inc.

[10] Enterprise OS Software Version 16.9 User Guide, June 2016, Motorola Solutions Inc.

[11] Motorola GGM 8000 Hardware User Guide, May 2016, Motorola Solutions Inc.

[12] Motorola Network Router (MNR) S6000 Hardware User Guide, May 2016, Motorola Solutions, Inc.