National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

TM

Validation Report

Network Device Collaborative Protection Profile (NDcPP)/Application Software Protection Profile (App PP) Extended Package Voice/Video over IP (VVoIP) Endpoint, Version 1.0, 28 September 2016

Report Number: CCEVS-VR-EP-0056
Dated: 25 September 2019
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

Common Criteria Testing Laboratory
Base Requirements
Acumen Security Common Criteria Testing Laboratory
Rockville, Maryland

Table of Contents

1 Executive Summary

This report documents the assessment of the National Information Assurance Partnership (NIAP) validation team of the evaluation of the Network Device Collaborative Protection Profile (NDcPP)/Application Software Protection Profile (App PP) Extended Package Voice/Video over IP (VVoIP) Endpoint, Version 1.0, 28 September 2016 (EP_VVOIP_V1.0), which is intended for use with the collaborative Protection Profile for Network Devices (NDcPP), Version 1.0, 27-Feb-2015 Base-PP or the Protection Profile for Application Software, Version (PP_APP) Version 1.2, 2016-04-22 Base PP.

It presents a summary of the EP_VVOIP_v1.0 and the evaluation results.

Acumen Security, located in Rockville, Maryland performed the evaluation of the EP_VVOIP_V1.0 concurrent with the first product evaluation against the Extended Package (EP) requirements. The evaluated product was the Cellcrypt Classified 2. For this evaluation, EP_VVOIP_V1.0 extended the Protection Profile for Application Software Version 1.2, 2016-04-25.

This evaluation addressed the base and selection-based requirements of the EP_VVOIP_V1.0. The EP_VVOIP_V1.0 does not include any objective requirements. Since the TOE claimed conformance to the PP_APP, any EP_VVOIP_V1.0 requirements that only apply when the NDcPP is used as a Base-PP were not applicable to the evaluation.

The Validation Report (VR) author independently performed an additional review of the EP_VVOIP_V1.0 as part of the completion of this VR, to confirm it meets the claimed ACE requirements.

The evaluation determined the EP_VVOIP_V1.0 is both Common Criteria Part 2 extended and Part 3 conformant. A NIAP approved Common Criteria Testing Laboratory (CCTL) evaluated the EP identified in this VR using the Common Methodology for IT Security Evaluation (Version 3.1, Rev 4) for conformance to the Common Criteria for IT Security Evaluation (Version 3.1, Rev 4). The Security Target (ST) includes material from both the PP_APP and the EP_VVOIP_V1.0; completion of the ASE work units satisfied the ACE work units for this EP, but only for the materials defined in this EP.

The evaluation laboratory conducted this evaluation in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme (CCEVS). The conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence given.

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 CCTLs. CCTLs evaluate products against Protection Profiles (PPs) and PP-Modules, and EPs that have assurance activities, which are interpretations of Common Methodology for Information Technology Security Evaluation work units specific to the technology described by the PP, PP-Module or EP.

In order to promote thoroughness and efficiency, the evaluation of the EP_VVOIP_V1.0 was performed concurrent with the first product evaluation against the EP's requirements. In this case the Target of Evaluation (TOE) was Cellcrypt Classified 2, performed by Acumen Security in Rockville, MD, United States of America.

The EP_VVOIP_V1.0 has a set of "base" requirements all conformant STs must include and also has "Additional," "Optional," "Selection-based," and "Objective" requirements. Optional requirements can be included in the ST, but are not mandatory, in order for a TOE to claim conformance to this EP. Selection-based requirements must be included based on the selections made in the base requirements and the capabilities of the TOE. Objective requirements are those the EP sponsor intends to mandate in future versions, and are included as optional requirements that raise industry awareness of expected future requirements. This evaluation did not claim the objective functions these requirements described.

A specific ST may not include these discretionary requirements, so the initial use of the EP addresses (in terms of the EP evaluation) the base requirements and any additional requirements incorporated into the initial ST. The VR authors evaluated all discretionary requirements that were not claimed in the initial TOE evaluation as part of the evaluation of the ACE_REQ work units performed against the EP. When an evaluation laboratory evaluates a TOE against any additional requirements not already referenced in this VR through an existing TOE evaluation, the VR may be amended to include reference to this as additional evidence that the corresponding portions of the EP_VVOIP_V1.0 were evaluated.

The following identifies the EP evaluated by this VR. It also includes supporting information from the initial product evaluation performed against this EP and any subsequent evaluations that address additional optional, selection-based, or objective requirements in the EP.

Protection Profile/Extended Package	Network Device Collaborative Protection Profile (NDcPP)/Application Software Protection Profile (App PP) Extended Package Voice/Video over IP (VVoIP) Endpoint, Version 1.0, 28 September 2016
ST (Base)	Cellcrypt Classified 2 Security Target, Version 1.1 19 April 2019
Assurance Activity Report (Base)	Cellcrypt Classified 2 Common Criteria APP and VVoIP Assurance Activity Report, Version 1.2, April 2019
CC Version	Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 4
Conformance Result	CC Part 2 Extended, CC Part 3 Conformant
CCTL	Acumen Security, Rockville, MD, USA

3 EP_VVOIP_V1.0 Description

The EP_VVOIP_V1.0 specifies information security requirements for a VVoIP endpoint as well as the assumptions, threats, organizational security policies, objectives, and requirements of a compliant TOE.

A VVoIP endpoint is a specific type of network device or software application that carries sensitive data over remote channels and uses protocols that are not implemented by a typical network device or software application. Therefore, additional security requirements are necessary to ensure that sensitive communications are not subject to unauthorized disclosure to unintended recipients.

The Network Device Collaborative Protection Profile (NDcPP)/Application Software Protection Profile (App PP) Extended Package Voice/Video over IP (VVoIP) Endpoint, Version 1.0, 28 September 2016 (EP_VVOIP_V1.0), extends the collaborative Protection Profile for Network Devices (NDcPP), Version 1.0, 27-Feb-2015 Base-PP or the Protection Profile for Application Software, Version (PP_APP) Version 1.2, 2016-04-22 Base PP.

4 Security Problem Description and Objectives

4.1 Assumptions

The specific conditions listed in the following subsections should exist in the TOE's Operational 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.

Table 1: Assumptions

Assumption Name	Assumption Definition
This EP defines no additional assumptions beyond those defined in the supported base PPs.	

4.2 Threats

Table 2 shows applicable threats the EP defines, in addition to those the Base-PPs define.

Table 2: Threats

Threat Name	Threat Definition
T.UNDETECTED_TRANSMISSION	An attacker may cause the TOE to exfiltrate audio and/or video media over a remote channel while in a state where the user has a reasonable expectation that no media is being transmitted.
T.CLOCK_DESYNC	An attacker may cause the TOE to use incorrect clock data, resulting in a denial of service from causing encryption and/or authentication connection failures.
T.MEDIA_DISCLOSURE	An attacker can use the encrypted variable rate vocoder frames to their advantage to decode transmitted data.

4.3 Organizational Security Policies

Table 3 shows applicable organizational security policies the EP defines, in addition to those the Base-PPs define.

Table 3: Organizational Security Policies

OSP Name	OSP Definition
This EP defines no additional organizational security policies beyond those defined in the supported base PPs.	

4.4 Security Objectives

Table 4 shows security objectives for the TOE the EP defines, in addition to those the Base-PPs define.

Table 4: Security Objectives for the TOE

TOE Security Obj.	TOE Security Objective Definition
This EP defines no additional TOE security objectives beyond those specified in the base PPs.	

Table 5 shows security objectives for the Operational Environment, in addition to those the Base-PPs define.

Table 5: Security Objectives for the Operational Environment

Environmental Security Objective	Environmental Security Objective Definition
Because this EP does not define any additional assumptions or organizational security policies, there are no additional security objectives for the Operational Environment to satisfy.	

5 Requirements

As indicated above, the EP_VVOIP_V1.0 requirements include the "base" requirements and additional requirements that are strictly or conditionally optional. Table 6 shows the "base" requirements validated as part of the Cellcrypt Classified 2 evaluation activities referenced above. Those requirements that are listed as being verified by "PP Evaluation" were evaluated separately by the VR author as part of the completion of the ACE evaluation work units against the EP.

Table 6: Mandatory Requirements

Requirement Class	Requirement Component	Verified By
FCO: Communication	FCO_VOC_EXT.1: Fixed-Rate Vocoder	Cellcrypt Classified 2
FDP: Data Protection	FDP_IFC.1: Subset Information Flow Control	Cellcrypt Classified 2
	FDP_IFF.1: Information Flow Control Functions	Cellcrypt Classified 2
	FPT_LIB_EXT.1: Use of Third Party Libraries	Cellcrypt Classified 2
FTA: TOE Access	FTA_SSL.3/Media: TSF-Initiated Termination (Media Channel)	Cellcrypt Classified 2
FTP: Trusted Path/Channels	FTP_ITC.1/Control: Inter-TSF Trusted Channel (Signaling Channel)	Cellcrypt Classified 2
	FTP_ITC.1/Media: Inter-TSF Trusted Channel (Media Channel)	Cellcrypt Classified 2

Table 7 shows the "**Optional**" requirements included in Appendix A of the VVoIP EP, and an indication of what evaluation those requirements were verified in (from the list in the Identification section above). Requirements that do not have an associated evaluation indicator have not yet been evaluated. These requirements are found in an ST if the ST authors claim that the TOE includes one or more of these optional capabilities.

Table 7: Optional Requirements

Requirement Class	Requirement Component	Verified By
Security Audit (FAU)	FAU_GEN.1/VVoIP: Audit Data Generation (VVoIP) **Mandatory SFR was moved to Optional per TD0372**	PP Evaluation

Table 8 shows the "**Selection-Based**" requirements included in Appendix B of the VVoIP EP, and an indication of what evaluation those requirements were verified in (from the list in the Identification section above). Requirements that do not have an associated evaluation indicator have not yet been evaluated. These requirements are found in an ST if the ST authors make associated selections in requirements levied on the TOE by the ST.

Table 8: Selection-Based Requirements

Requirement Class	Requirement Component	Verified By
Security Audit (FAU)	FAU_STG_EXT.1: Protected Audit Event Storage	PP Evaluation

Requirement Class	Requirement Component	Verified By
	Mandatory SFR moved from Optional to Selection-Based per TD0372. This SFR must be claimed if FAU_GEN.1/VVOIP is included in the ST and the TOE claims conformance to the App PP.	
FCS: Cryptographic support	FCS_SRTP_EXT.1: Secure Real-Time Transport Protocol	Cellcrypt Classified 2

Table 9 shows the "**Objective**" requirements included in Appendix C of the VVoIP EP, and an indication of what evaluation those requirements were verified in (from the list in the Identification section above). Requirements that do not have an associated evaluation indicator have not yet been evaluated. These requirements are found in an ST if the ST authors claim that the TOE includes one or more of these optional capabilities.

Table 9: Objective Requirements

Requirement Class	Requirement Component	Verified By
The VVoIP EP does not define any objective requirements.		

6 Assurance Requirements

Table 14 shows the assurance requirements included in the EP_VVOIP_V1.0.

Table 14: Assurance Requirements

Requirement Class	Requirement Component	Verified By
ASE: Security Target	ASE_CCL.1: Conformance Claims	Cellcrypt Classified 2
	ASE_ECD.1: Extended Components Definition	Cellcrypt Classified 2
	ASE_INT.1: ST Introduction	Cellcrypt Classified 2
	ASE_OBJ.1: Security Objectives	Cellcrypt Classified 2
	ASE_REQ.1: Derived Security Requirements	Cellcrypt Classified 2
	ASE_SPD.1: Security Problem Definition	Cellcrypt Classified 2
	ASE_TSS.1: TOE Summary Specification	Cellcrypt Classified 2
ADV: Development	ADV_FSP.1 Basic Functional Specification	Cellcrypt Classified 2
AGD: Guidance Documents	AGD_OPE.1: Operational User Guidance	Cellcrypt Classified 2
	AGD_PRE.1: Preparative Procedures	Cellcrypt Classified 2
ALC: Life-cycle Support	ALC_CMC.1: Labeling of the TOE	Cellcrypt Classified 2
	ALC_CMS.1: TOE CM Coverage	Cellcrypt Classified 2
	ALC_TSU_EXT.1: Timely Security Updates **Note: this SAR is present only when the TOE conforms to the APP PP.**	Cellcrypt Classified 2
ATE: Tests	ATE_IND.1: Independent Testing - Sample	Cellcrypt Classified 2
AVA: Vulnerability Assessment	AVA_VAN.1: Vulnerability Survey	Cellcrypt Classified 2

7 Results of the Evaluation

Note that for ACE elements and work units identical to ASE elements and work units, the lab performed the ACE work units concurrent to the ASE work units.

Table 15: Evaluation Results

ACE Requirement	Evaluation Verdict	Verified By
ACE_INT.1	Pass	Cellcrypt Classified 2
ACE_CCL.1	Pass	Cellcrypt Classified 2
ACE_SPD.1	Pass	Cellcrypt Classified 2
ACE_OBJ.1	Pass	Cellcrypt Classified 2
ACE_ECD.1	Pass	Cellcrypt Classified 2
ACE_REQ.1	Pass	Cellcrypt Classified 2

8 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 unambiguously that a given implementation is correct with respect to the formal model.
- **Evaluation**. An IT product's assessment against the Common Criteria using the Common Criteria Evaluation Methodology as the supplemental guidance, interprets it in the EP_SBC_V1.1 Assurance Activities to determine whether the claims made are justified.
- **Evaluation Evidence**. Any tangible resource (information) required from the sponsor or developer by the evaluator to perform one or more evaluation activities.
- **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 the CCEVS Validation Body uses that leads to the issuance 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.

9 Bibliography

The validation team used the following documents to produce this VR:

[1] Common Criteria Project Sponsoring Organizations. *Common Criteria for Information Technology Security Evaluation: Part 1: Introduction and General Model*, Version 3.1, Revision 4, dated: September 2012.

[2] Common Criteria Project Sponsoring Organizations. *Common Criteria for Information Technology Security Evaluation: Part 2: Security Functional Requirements*, Version 3.1, Revision 4, dated: September 2012.

[3] Common Criteria Project Sponsoring Organizations. *Common Criteria for Information Technology Security Evaluation: Part 3: Security Assurance Requirements*, Version 3.1, Revision 4, dated: September 2012.

[4] Common Criteria Project Sponsoring Organizations. *Common Evaluation Methodology for Information Technology Security*, Version 3.1, Revision 4, dated: September 2012.

[5] Common Criteria, Evaluation and Validation Scheme for Information Technology Security, *Guidance to Validators of IT Security Evaluations*, Scheme Publication #3, Version 3.0, May 2014.

[6] Network Device Collaborative Protection Profile (NDcPP)/Application Software Protection Profile (App PP) Extended Package Voice/Video over IP (VVoIP) Endpoint, Version 1.0, 2016-09-28.

[7] collaborative Protection Profile for Network Devices, Version 1.0, 27-Feb-2015

[8] Security Target Cellcrypt Classified 2, Version 1.1, April 19, 2019

[9] Protection Profile for Application Software, Version: 1.2, 2016-04-22

[10] Cellcrypt Classified 2 Common Criteria APP and VVoIP Assurance Activity Report, Version 1.2, April 2019