National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

TM

Validation Report

PP-Configuration for Application Software and Voice/Video over IP (VVoIP) Endpoints

Version 1.1

31 May 2022

Report Number: CCEVS-VR-PP-0083
Dated: January 27, 2023
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 Meade, MD 20755-6982

ACKNOWLEDGMENTS

Common Criteria Testing Laboratory
Base and Additional Requirements
Gossamer Security Solutions
Columbia, MD

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 PP-Configuration for Application Software and Voice/Video over IP (VVoIP) Endpoints (CFG_APP-VVoIP_V1.1). This PP-Configuration defines how to evaluate a TOE that claims conformance to the Protection Profile for Application Software, Version 1.4 (PP_APP_V1.4) Base-PP, and the PP-Module for Voice/Video over IP (VVoIP) Endpoints, Version 1.0 (MOD_VVoIP_V1.0). It presents a summary of the CFG_APP-VVoIP_V1.1 and the evaluation results.

Gossamer Security Solutions, located in Columbia, Maryland, performed the evaluation of the PP_APP_V1.4 and MOD_VVoIP_V1.0, contained within the PP-Configuration, concurrent with the first product evaluation against the PP-Configuration's requirements. The evaluated product was SecuSUITE v5.0 and SteelBox v5.0 (SecuSUITE and SteelBox).

This evaluation addressed the base security functional requirements of PP_APP_V1.4 and MOD_VVoIP_V1.0 as part of CFG_APP-VVoIP_V1.1. The Validation Report (VR) author independently performed an additional review of the PP-Configuration, Base-PP, and PP-Module as part of the completion of this VR, to confirm they meet the claimed APE and ACE requirements.

The evaluation determined the CFG_APP-VVoIP_V1.1 is both Common Criteria Part 2 extended and Part 3 extended. An accredited Information Technology Security Evaluation Facility (ITSEF) evaluated the PP-Configuration and PP-Module identified in this VR using the Common Methodology for IT Security Evaluation (Version 3.1, Revision 5) for conformance to the Common Criteria for IT Security Evaluation (Version 3.1, Revision 5). The Security Target (ST) includes material from the PP_APP_V1.4 and MOD_VVoIP_V1.0; completion of the ASE workunits satisfied the APE workunits for this PP and ACE workunits for this PP-Module, but only for the materials defined in this PP-Module, and only when the PP-Module is in the defined PP-Configuration.

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 Common Criteria Testing Laboratories (CCTLs). CCTLs evaluate products against Protection Profiles (PPs) and PP-Modules that have Evaluation Activities, which are interpretations of the Common Methodology for Information Technology Security Evaluation (CEM) v3.1 workunits specific to the technology described by the PP or PP-Modules. Products may only be evaluated against PP-Modules when a PP-Configuration is defined to include the PP-Modules with at least one corresponding Base-PP.

To promote thoroughness and efficiency, the evaluation of the CFG_APP-VVoIP_V1.1, PP_APP_V1.4, and MOD_VVoIP_V1.0, was performed concurrent with the first product evaluation to claim conformance to the PP-Configuration. In this case, the Target of Evaluation (TOE) was SecuSUITE and SteelBox, performed by Gossamer Security Solutions in Columbia, MD.

This evaluation addressed the base security functional requirements of PP_APP_V1.4, and MOD_VVoIP_V1.0 as part of CFG_APP-VVoIP_V1.1. The PP-Module defines additional requirements, some of which the SecuSUITE and SteelBox device evaluation claimed.

PP_APP_V1.4 and MOD_VVoIP_V1.0 contain a set of base requirements that all conformant STs must include, and additionally contain optional, selection-based, and objective requirements. Selection-based requirements are those that must be included based on the selections made in other requirements and the abilities of the TOE. Optional requirements may be claimed or omitted at the product vendor's discretion. Objective requirements are not currently prescribed but are expected to be included in future versions. Vendors planning to have evaluations performed against future products are encouraged to plan for these objective requirements to be met. MOD_VVoIP_V1.0 also defines implementation-dependent requirements, which must be claimed if the TOE implements some functionality that is not mandatory for the product type.

The VR authors evaluated all discretionary requirements not claimed in the initial TOE evaluation as part of the evaluation of the APE_REQ workunits performed against the Base-PP and the ACE_REQ workunits performed against the PP-Module. 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 CFG_APP-VVoIP_V1.1 were evaluated.

The following identifies the Base-PP and the PP-Module in the PP-Configuration evaluated by this VR. It also includes supporting information from the initial product evaluation performed against these PP-Modules.

PP-Configuration	PP-Configuration for Application Software and Voice/Video over IP (VVoIP) Endpoints, Version 1.1, 31 May 2022 (CFG_APP-VVoIP_V1.1)
Base-PP	Protection Profile for Application Software, Version 1.4, 07 October 2021 (PP_APP_V1.4)
Module in PP-Configuration	PP-Module for Voice/Video over IP (VVoIP) Endpoints, Version 1.0, 28 October 2020 (MOD_VVoIP_V1.0)
ST (Base)	SecuSUITE v5.0 and SteelBox v5.0 Security Target, Version 0.6, 08 December 2022

Assurance Activity Report (Base)	Assurance Activity Report for SecuSUITE v5.0 and SteelBox v5.0, Version 0.4, 08 December 2022
CC Version	Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 5
Conformance Result	CC Part 2 Extended, CC Part 3 Extended
CCTL	Gossamer Security Solutions Columbia, MD

3 CFG_APP-VVoIP_V1.1 Description

CFG_APP-VVoIP_V1.1 is a PP-Configuration that combines the following.

- Protection Profile for Application Software, Version 1.4, (PP_APP_V1.4)
- PP-Module for Voice/Video over IP (VVoIP) Endpoints, Version 1.0 (MOD_VVoIP_V1.0)

MOD_VVoIP_V1.0 defines two possible embodiments of a VVoIP product: a standalone VVoIP-capable device (i.e., a dedicated hardware phone) and a software application that runs on a general-purpose device such as a smartphone, tablet, or PC. Regardless of whether the TOE is a hardware appliance or a client application on an operating system, it will be deployed in the same environment and implement the same functionality. This PP-Configuration is for the software application use case.

4 Security Problem Description and Objectives

4.1 Assumptions

Table 1 shows the assumptions defined in the individual components of CFG_APP-VVoIP_V1.1.

Table 1: Assumptions

Assumption Name	Assumption Definition
From PP_APP_V1.4	
A.PLATFORM	The TOE relies upon a trustworthy computing platform with a reliable time clock for its execution. This includes the underlying platform and whatever runtime environment it provides to the TOE.
A.PROPER_ADMIN	The administrator of the application software is not careless, willfully negligent or hostile, and administers the software in compliance with the applied enterprise security policy.
A.PROPER_USER	The user of the application software is not willfully negligent or hostile, and uses the software in compliance with the applied enterprise security policy.
From MOD_VVoIP_V1.0	
A.UPDATE_SOURCE	It is assumed that TOE software/firmware updates will be made available on either the call control server that the TOE connects to or a separate file server managed by the organization.

4.2 Threats

Table 2 shows the threats defined in the individual components of CFG_APP-VVoIP_V1.1.

Table 2: Threats

Threat Name	Threat Definition
From PP_APP_V1.4	
T.LOCAL_ATTACK	An attacker can act through unprivileged software on the same computing platform on which the application executes. Attackers may provide maliciously formatted input to the application in the form of files or other local communications.
T.NETWORK_ATTACK	An attacker is positioned on a communications channel or elsewhere on the network infrastructure. Attackers may engage in communications with the application software or alter communications between the application software and other endpoints in order to compromise it.
T.NETWORK_EAVESDROP	An attacker is positioned on a communications channel or elsewhere on the network infrastructure. Attackers may monitor and gain access to data exchanged between the application and other endpoints.
T.PHYSICAL_ACCESS	An attacker may try to access sensitive data at rest.
From MOD_VVoIP_V1.0	
T.MEDIA_DISCLOSURE	An attacker can use the encrypted variable rate vocoder frames to their advantage to decode transmitted data.

Threat Name	Threat Definition
T.UNDETECTED_TRANSMISSION	An attacker may cause the TOE to exfiltrate audio or video media over a remote channel while in a state where the user has a reasonable expectation that no media is being transmitted.

4.3 Organizational Security Policies

Table 3 shows the organizational security policies defined in the individual components of CFG_APP-VVoIP_V1.1.

Table 3: Organizational Security Policies

OSP Name	OSP Definition
From PP_APP_V1.4	
No OSPs defined in PP_APP_V1.4.	
From MOD_VVoIP_V1.0	
No OSPs defined in MOD_VVoIP_V1.0.	

4.4 Security Objectives

Table 4 shows the security objectives for the TOE defined in the individual components of CFG_APP-VVoIP_V1.1.

Table 4: Security Objectives for the TOE

TOE Security Objective	TOE Security Objective Definition
From PP_APP_V1.4	
O.INTEGRITY	Conformant TOEs ensure the integrity of their installation and update packages, and also leverage execution environment-based mitigations. Software is seldom, if ever, shipped without errors. The ability to deploy patches and updates to fielded software with integrity is critical to enterprise network security. Processor manufacturers, compiler developers, execution environment vendors, and operating system vendors have developed execution environment-based mitigations that increase the cost to attackers by adding complexity to the task of compromising systems. Application software can often take advantage of these mechanisms by using APIs provided by the runtime environment or by enabling the mechanism through compiler or linker options.
O.MANAGEMENT	To facilitate management by users and the enterprise, conformant TOEs provide consistent and supported interfaces for their security-relevant configuration and maintenance. This includes the deployment of applications and application updates through the use of platform-supported deployment mechanisms and formats, as well as providing mechanisms for configuration. This also includes providing control to the user regarding disclosure of any PII.
O.PROTECTED_COMMS	To address both passive (eavesdropping) and active (packet modification) network attack threats, conformant TOEs will use a trusted channel for sensitive data. Sensitive data includes cryptographic keys, passwords, and any other data specific to the application that should not be exposed outside of the application.

TOE Security Objective	TOE Security Objective Definition
O.PROTECTED_STORAGE	To address the issue of loss of confidentiality of user data in the event of loss of physical control of the storage medium, conformant TOEs will use data-at-rest protection. This involves encrypting data and keys stored by the TOE in order to prevent unauthorized access to this data. This also includes unnecessary network communications whose consequence may be the loss of data.
O.QUALITY	To ensure quality of implementation, conformant TOEs leverage services and APIs provided by the runtime environment rather than implementing their own versions of these services and APIs. This is especially important for cryptographic services and other complex operations such as file and media parsing. Leveraging this platform behavior relies upon using only documented and supported APIs.
From MOD_VVoIP_V1.0	
O.ENCRYPTION	To prevent data disclosure from decryption, conformant TOEs will transmit and store sensitive data using mechanisms that provide adequate protections.
O.NO_UNATTENDED_TRANSMISSION	To prevent undetected transmissions, conformant TOEs will not transmit unattended voice or video data when streaming media is not in use.
O.TOE_ADMINISTRATION	To support the enforcement of other security functionality, a conformant TOE will provide a management capability that allows for configuration of the TSF.

Table 5 shows the security objectives for the operational environment defined in the individual components of CFG_APP-VVoIP_V1.1.

Table 5: Security Objectives for the Operational Environment

Environmental Security Objective	Environmental Security Objective Definition
From PP_APP_V1.4	
OE.PLATFORM	The TOE relies on a trustworthy computing platform for its execution. This includes the underlying operating system and any discrete execution environment provided to the TOE.
OE.PROPER_ADMIN	The administrator of the application software is not careless, willfully negligent, or hostile, and administers the software within compliance of the applied enterprise security policy.
OE.PROPER_USER	The user of the application software is not willfully negligent or hostile and uses the software within compliance of the applied enterprise security policy.
From MOD_VVoIP_V1.0	
OE.UPDATE_SOURCE	The operational environment will have TOE software or firmware made available on either the call control server that the TOE connects to or a separate file server managed by the organization.

5 Functional Requirements

As indicated above, CFG_APP-VVoIP_V1.1 includes the PP_APP_V1.4 and MOD_VVoIP_V1.0.

Requirements in the PP_APP_V1.4 and MOD_VVoIP_V1.0 are comprised of the "base" requirements, additional requirements that are optional, selection-based, implementation-dependent, or objective, and in the case of the PP-Module, additional requirements that are dependent on the Base-PP that the PP-Module is used with. Table 6 contains the "base" requirements that were validated as part of the evaluation activities referenced above as well as any additional requirements that depend on the Base-PP that is claimed.

Table 6: Base-PP Security Functional Requirements

Requirement Class	Requirement Component	Verified By
Modified when PP_APP_V1.4 is the Base-PP		
FPT: Protection of the TSF	FPT_TUD_EXT.1: Trusted Update	SecuSUITE and SteelBox
FTP: Trusted Path/Channels	FTP_DIT_EXT.1: Protection of Data in Transit	SecuSUITE and SteelBox
Additional when PP_APP_V1.4 is the Base-PP		
There are no additional SFRs in the MOD_VVoIP_V1.0		

Table 7 contains the "base" requirements specific to the TOE.

Table 7: TOE Security Functional Requirements

Requirement Class	Requirement Component	Verified By
From PP_APP_V1.4		
FCS: Cryptographic Support	FCS_CKM.1: Cryptographic Key Generation Services	SecuSUITE and SteelBox
	FCS_RBG_EXT.1: Random Bit Generation Services	SecuSUITE and SteelBox
	FCS_STO_EXT.1: Storage of Credentials	SecuSUITE and SteelBox
FDP: User Data Protection	FDP_DAR_EXT.1: Encryption of Sensitive Application Data	SecuSUITE and SteelBox
	FDP_DEC_EXT.1: Access to Platform Resources	SecuSUITE and SteelBox
	FDP_NET_EXT.1: Network Communications	SecuSUITE and SteelBox
FMT: Security Management	FMT_CFG_EXT.1: Secure by Default Configuration	SecuSUITE and SteelBox
	FMT_MEC_EXT.1: Supported Configuration Mechanism	SecuSUITE and SteelBox
	FMT_SMF.1: Specification of Management Functions	SecuSUITE and SteelBox

Requirement Class	Requirement Component	Verified By
FPR: Privacy	FPR_ANO_EXT.1: User Consent for Transmission of Personally Identifiable Information	SecuSUITE and SteelBox
FPT: Protection of the TSF	FPT_AEX_EXT.1: Anti-Exploitation Capabilities	SecuSUITE and SteelBox
	FPT_API_EXT.1: Use of Supported Services and APIs	SecuSUITE and SteelBox
	FPT_IDV_EXT.1: Software Identification and Versions	SecuSUITE and SteelBox
	FPT_LIB_EXT.1: Use of Third Party Libraries	SecuSUITE and SteelBox
	FPT_TUD_EXT.1: Integrity for Installation and Update	SecuSUITE and SteelBox
FTP: Trusted Path/Channels	FTP_DIT_EXT.1: Protection of Data in Transit	SecuSUITE and SteelBox
From MOD_VVoIP_V1.0		
FCO: Communications	FCO_VOC_EXT.1: Fixed-Rate Vocoder	SecuSUITE and SteelBox
FDP: User Data Protection	FDP_IFC.1: Subset Information Flow Control	SecuSUITE and SteelBox
	FDP_IFF.1: Simple Security Attributes	SecuSUITE and SteelBox
FMT: Security Management	FMT_SMF.1/VVoIP: Specification of Management Functions (VVoIP Communications)	SecuSUITE and SteelBox
FTA: TOE Access	FTA_SSL.3/Media: TSF-Initiated Termination (Media Channel)	SecuSUITE and SteelBox
FTP: Trusted Path/Channels	FTP_ITC.1/Control: Inter-TSF Trusted Channel (Signaling Channel)	SecuSUITE and SteelBox
	FTP_ITC.1/Media: Inter-TSF Trusted Channel (Media Channel)	SecuSUITE and SteelBox

Table 8 contains the "**Optional**" requirements contained in Appendix A.1 of the Base-PP and PP-Module, and an indication of how those requirements were evaluated (from the list in the *Identification* section above). If no completed evaluations have claimed a given optional requirement, the VR author has evaluated it through the completion of the relevant APE and ACE workunits and has indicated its verification through "PP Evaluation" or "Module Evaluation."

Table 8: Optional Requirements

Requirement Class	Requirement Component	Verified By
From PP_APP_V1.4		
FCS: Cryptographic Support	FCS_CKM.1/SK: Cryptographic Symmetric Key Generation	PP Evaluation

Requirement Class	Requirement Component	Verified By
From MOD_VVoIP_V1.0		
FAU: Security Audit	FAU_GEN.1/CS-Admin: Audit Data Generation (Client-Server Admin Events)	Module Evaluation
	FAU_GEN.1/CS-VVoIP: Audit Data Generation (Client-Server VVoIP Events)	Module Evaluation

Table 9 contains the "**Implementation-Dependent**" requirements contained in Appendix A.3 of the PP-Module, and an indication of how those requirements were evaluated (from the list in the *Identification* section above). If no completed evaluations have claimed a given implementation-dependent requirement, the VR author has evaluated it through the completion of the relevant APE and ACE workunits and has indicated its verification through "PP Evaluation" or "Module Evaluation."

Table 9: Implementation-Dependent Requirements

Requirement Class	Requirement Component	Verified By
From PP_APP_V1.4		
There are no implementation-dependent requirements in PP_APP_V1.4.		
From MOD_VVoIP_V1.0		
FAU: Security Audit	FAU_STG_EXT.1: Protected Audit Event Storage	Module Evaluation

Table 10 contains the "**Selection-Based**" requirements contained in Appendix B of the Base-PP and PP-Module, and an indication of how those requirements were evaluated (from the list in the *Identification* section above). If no completed evaluations have claimed a given selection-based requirement, the VR author has evaluated it through the completion of the relevant APE and ACE workunits and has indicated its verification through "PP Evaluation" or "Module Evaluation."

Table 10: Selection-Based Requirements

Requirement Class	Requirement Component	Verified By
From PP_APP_V1.4		
FCS: Cryptographic Support	FCS_CKM.1/AK: Cryptographic Asymmetric Key Generation	SecuSUITE and SteelBox
	FCS_CKM.1/PBKDF: Password Conditioning	PP Evaluation
	FCS_CKM.2: Cryptographic Key Establishment	SecuSUITE and SteelBox
	FCS_COP.1/SKC Cryptographic Operation – Encryption/Decryption	SecuSUITE and SteelBox
	FCS_COP.1/Hash: Cryptographic Operation – Hashing	SecuSUITE and SteelBox
	FCS_COP.1/KeyedHash: Cryptographic Operation – Keyed-Hash Message Authentication	SecuSUITE and SteelBox

Requirement Class	Requirement Component	Verified By
	FCS_COP.1/Sig: Cryptographic Operation – Signing	SecuSUITE and SteelBox
	FCS_HTTPS_EXT.1/Client: HTTPS Protocol	SecuSUITE and SteelBox
	FCS_HTTPS_EXT.1/Server: HTTPS Protocol	PP Evaluation
	FCS_HTTPS_EXT.2: HTTPS Protocol with Mutual Authentication	PP Evaluation
	FCS_RBG_EXT.2: Random Bit Generation from Application	SecuSUITE and SteelBox
FIA: Identification and Authentication	FIA_X509_EXT.1: X.509 Certificate Validation	SecuSUITE and SteelBox
	FIA_X509_EXT.2: X.509 Certificate Authentication	SecuSUITE and SteelBox
FPT: Protection of the TSF	FPT_TUD_EXT.2: Integrity for Installation and Update	SecuSUITE and SteelBox
From MOD_VVoIP_V1.0		
FAU: Security Audit	FAU_GEN.1/P2P-Admin: Audit Data Generation (Peer-to-Peer Admin Events)	Module Evaluation
	FAU_GEN.1/P2P-VVoIP: Audit Data Generation (Peer-to-Peer VVoIP Events)	Module Evaluation
FCS: Cryptographic Support	FCS_COP.1/SRTP: Cryptographic Operation (Encryption/Decryption for SRTP)	SecuSUITE and SteelBox
	FCS_SRTP_EXT.1: Secure Real-Time Transport Protocol	SecuSUITE and SteelBox
FDP: User Data Protection	FDP_IFC.1/CallControl: Subset Information Flow Control (for Call Control)	Module Evaluation
	FDP_IFF.1/CallControl: Simple Security Attributes (for Call Control)	Module Evaluation
FPT: Protection of the TSF	FPT_STM_EXT.1/VVoIP: Reliable Time Stamps (VVoIP Communications)	Module Evaluation

Table 11 contains the "**Objective**" requirements contained in Appendix A.2 of the Base-PP and an indication of how those requirements were evaluated (from the list in the *Identification* section above). If no completed evaluations have claimed a given objective requirement, the VR author has evaluated it through the completion of the relevant APE and ACE workunits and has indicated its verification through "PP Evaluation" or "Module Evaluation."

Table 11: Objective Requirements

Requirement Class	Requirement Component	Verified By
From PP_APP_V1.4		
FPT: Protection of the TSF	FPT_API_EXT.2: Use of Supported Services and APIs	PP Evaluation

Requirement Class	Requirement Component	Verified By
From MOD_VVoIP_V1.0		
The MOD_VVoIP_V1.0 does not define any additional objective requirements.		

6 Assurance Requirements

The PP-Configuration defines its security assurance requirements as those required by PP_APP_V1.4. The SARs defined in that PP are applicable to MOD_VVoIP_V1.0, as well as CFG_APP-VVoIP_V1.1 as a whole.

7 Results of the Evaluation

Note that for APE and ACE elements and workunits identical to ASE elements and workunits, the lab performed the ACE workunits concurrent to the ASE workunits.

Table 12: Evaluation Results: PP_APP_V1.4

APE Requirement	Evaluation Verdict	Verified By
APE_INT.1	Pass	PP Evaluation
APE_CCL.1	Pass	PP Evaluation
APE_SPD.1	Pass	PP Evaluation
APE_OBJ.2	Pass	PP Evaluation
APE_ECD.1	Pass	PP Evaluation
APE_REQ.2	Pass	PP Evaluation

Table 13: Evaluation Results: MOD_VVoIP_V1.0

ACE Requirement	Evaluation Verdict	Verified By
ACE_INT.1	Pass	Module Evaluation
ACE_CCL.1	Pass	Module Evaluation
ACE_SPD.1	Pass	Module Evaluation
ACE_OBJ.1	Pass	Module Evaluation
ACE_ECD.1	Pass	Module Evaluation
ACE_REQ.1	Pass	Module Evaluation

Table 14: Evaluation Results: CFG_APP-VVoIP_V1.1

ACE Requirement	Evaluation Verdict	Verified By
ACE_MCO.1	Pass	PP-Config Evaluation
ACE_CCO.1	Pass	PP-Config Evaluation

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 PP_APP_V1.4 and MOD_VVoIP_V1.0 Evaluation 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 5, dated: April 2017.

[2] Common Criteria Project Sponsoring Organizations. *Common Criteria for Information Technology Security Evaluation: Part 2: Security Functional Requirements*, Version 3.1, Revision 5, dated: April 2017.

[3] Common Criteria Project Sponsoring Organizations. *Common Criteria for Information Technology Security Evaluation: Part 3: Security Assurance Requirements*, Version 3.1, Revision 5, dated: April 2017.

[4] Common Criteria Project Sponsoring Organizations. *Common Evaluation Methodology for Information Technology Security*, Version 3.1, Revision 5, dated: April 2017.

[5] CC and CEM addenda – Exact Conformance, Selection-Based SFRs, Optional SFRs, Version 0.5, dated: May 2017.

[6] Protection Profile for Application Software, Version 1.4, 07 October 2021.

[7] PP-Module for Voice/Video over IP (VVoIP) Endpoints, Version 1.0, 28 October 2020.

[8] PP-Configuration for Application Software and Voice/Video over IP (VVoIP) Endpoints, Version 1.1, 31 May 2022.

[9] SecuSUITE v5.0 and SteelBox v5.0 Security Target, Version 0.6, 08 December 2022.

[10] Assurance Activities Report for SecuSUITE v5.0 and SteelBox v5.0, Version 0.4, 08 December 2022.