National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

Validation Report

PP-Configuration for Network Device and Enterprise Session Controller (ESC)

Version 1.0

19 November 2020

Report Number: **CCEVS-VR-PP-0077**
Dated: **27 October 2022**
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
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 PP-Configuration for Network Device and Enterprise Session Controller (ESC), Version 1.0 (CFG_NDcPP-ESC_V1.0). This PP-Configuration defines how to evaluate a TOE that claims conformance to the collaborative Protection Profile for Network Devices (CPP_ND_V2.2E) Base-PP and the PP-Module for Enterprise Session Controller (ESC), Version 1.0 (MOD_ESC_V1.0). It presents a summary of the CFG_NDcPP-ESC_V1.0 and the evaluation results.

Acumen Security, located in Rockville, Maryland, performed the evaluation of the CFG_NDcPP-ESC_V1.0 and MOD_ESC_V1.0 contained within the PP-Configuration, concurrent with the first product evaluation against the PP-Configuration's requirements. The evaluated product was Cellcrypt Server (Cellcrypt).

This evaluation addressed the base security functional requirements of MOD_ESC_V1.0 as part of CFG_NDcPP-ESC_V1.0. The Module defines additional requirements but the Cellcrypt evaluation did not claim any of these.

The Validation Report (VR) author independently performed an additional review of the PP-Configuration and Module as part of the completion of this VR, to confirm they met the claimed ACE requirements.

The evaluation determined the CFG_NDcPP-ESC_V1.0 is both Common Criteria Part 2 extended and Part 3 conformant. A NIAP approved Common Criteria Testing Laboratory (CCTL) evaluated the PP-Configuration and 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 CPP_ND_V2.2E and MOD_ESC_V1.0; completion of the ASE workunits satisfied the ACE workunits for this Module, but only for the materials defined in this Module, and only when this 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 CCTLs. CCTLs evaluate products against Protection Profiles (PPs) and 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 Modules. Products may only be evaluated against Modules when a PP-Configuration is defined to include the Module with at least one corresponding Base-PP.

To promote thoroughness and efficiency, the evaluation of the CFG_NDcPP-ESC_V1.0 and MOD_ESC_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 Cellcrypt, performed by Acumen Security in Rockville, Maryland, United States.

This evaluation addressed the base security functional requirements of MOD_ESC_V1.0 as part of CFG_NDcPP-ESC_V1.0. The Module defines additional requirements but the Cellcrypt evaluation did not claim any of these.

MOD_ESC_V1.0 contains a set of base requirements that all conformant STs must include, and additionally contains optional and selection-based requirements. Optional requirements may or may not be included within the scope of the evaluation, depending on whether the vendor provides that functionality within the tested product and chooses to include it inside the TOE boundary. Selection-based requirements are those that must be included based upon the selections made in other requirements and the capabilities of the TOE.

The VR authors evaluated all discretionary requirements not claimed in the initial TOE evaluation as part of the evaluation of the ACE_REQ workunits performed against the 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_NDcPP-ESC_V1.0 were evaluated.

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

PP-Configuration	PP-Configuration for Network Device and Enterprise Session Controller (ESC, Version 1.0, 19 November 2020
Modules in PP-Configuration	PP-Module for Enterprise Session Controller (ESC), Version 1.0, 19 November 2020
ST (Base)	Cellcrypt Server Security Target, Version 1.0.0, 10 June 2022
Assurance Activity Report (Base)	Assurance Activity Report for Cellcrypt Server, Version 0.3, 14 June 2022
CC Version	Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 5
Conformance Result	CC Part 2 Extended, CC Part 3 Conformant
CCTL	Acumen Security Rockville, Maryland 20850

3 CFG_NDcPP-ESC_V1.0 Description

CFG_NDcPP-ESC_V1.0 is a PP-Configuration that combines the following:

- collaborative Protection Profile for Network Devices, Version 2.2E (CPP_ND_V2.2E)
- Protection Profile Module for Enterprise Session Controller (ESC), Version 1.0, (MOD_ESC_V1.0)

The PP-Configuration defines a baseline set of security functional requirements (SFRs) for network devices (defined in CPP_ND_V2.2E) that are bundled with agent applications to enforce configured policies on ESCs (defined in MOD_ESC_V1.0).

ESCs are privately-owned telecommunication switches that are used primarily to set up, process, and terminate voice and video calls over an enterprise-wide Internet Protocol (IP) network.

ESCs execute switchboard operations automatically while providing simultaneous connectivity to hundreds of callers virtually instantaneously. Most ESCs support auxiliary services such as VVoIP conferencing, voicemail, chat, telepresence, encrypted communications, and protocol translation for end-to-end connectivity of diverse endpoints.

A TOE that conforms to CFG_NDcPP-ESC_V1.0 is a network device that has ESC abilities. A conformant TOE is therefore able to facilitate connectivity between two or more VVoIP endpoints.

4 Security Problem Description and Objectives

4.1 Assumptions

Table 1 shows the assumptions defined in the individual components of CFG_NDcPP-ESC_V1.0.

Table 1: Assumptions

Assumption Name	**Assumption Definition**
From CPP_ND_V2.2E	
A.ADMIN_CREDENTIALS_SECURE	The Administrator’s credentials (private key) used to access the Network Device are protected by the platform on which they reside.
A.LIMITED_FUNCTIONALITY	The device is assumed to provide networking functionality as its core function and not provide functionality/services that could be deemed as general purpose computing. For example, the device should not provide a computing platform for general purpose applications (unrelated to networking functionality). In the case of vNDs, the VS is considered part of the TOE with only one vND instance for each physical hardware platform. The exception being where components of the distributed TOE run inside more than one virtual machine (VM) on a single VS. There are no other guest VMs on the physical platform providing non-Network Device 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 and PP-Modules for particular types of Network Devices (e.g., firewall).
A.PHYSICAL_PROTECTION	The Network Device is assumed to be physically protected in its operational environment and not subject to physical attacks that compromise the security or interfere with the device’s physical interconnections and correct operation. This protection is assumed to be sufficient to protect the device and the data it contains. As a result, the cPP does not include any requirements on physical tamper protection or other physical attack mitigations. The cPP does not expect the product to defend against physical access to the device that allows unauthorized entities to extract data, bypass other controls, or otherwise manipulate the device. For vNDs, this assumption applies to the physical platform on which the VM runs.
A.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.RESIDUAL_INFORMATION	The Administrator must ensure that there is no unauthorized access possible for sensitive residual information (e.g. cryptographic keys, keying material, PINs, passwords etc.) on networking equipment when the equipment is discarded or removed from its operational environment.

Assumption Name	**Assumption Definition**
A.TRUSTED_ADMINISTRATOR	The Security Administrator(s) for the Network Device are assumed to be trusted and to act in the best interest of security for the organization. This includes appropriately trained, following policy, and adhering to guidance documentation. Administrators are trusted to ensure passwords/credentials have sufficient strength and entropy and to lack malicious intent when administering the device. The Network Device is not expected to be capable of defending against a malicious Administrator that actively works to bypass or compromise the security of the device. For TOEs supporting X.509v3 certificate-based authentication, the Security Administrator(s) are expected to fully validate (e.g. offline verification) any CA certificate (root CA certificate or intermediate CA certificate) loaded into the TOE’s trust store (aka 'root store', ' trusted CA Key Store', or similar) as a trust anchor prior to use (e.g. offline verification).
From MOD_ESC_V1.0	
All assumptions for the operational environment of the Base-PP also apply to this PP-Module. A.NO_THRU_TRAFFIC_PROTECTION is still operative, but only for the interfaces in the TOE that are defined by the Base-PP and not the PP-Module.	

4.2 Threats

Table 2 shows the threats defined in the individual components of CFG_NDcPP-ESC_V1.0.

Table 2: Threats

Threat Name	**Threat Definition**
From CPP_ND_V2.2E	
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_COMPROMISE	Threat agents may compromise credentials and device data enabling continued access to the Network Device and its critical data. The compromise of credentials includes replacing existing credentials with an attacker’s credentials, modifying existing credentials, or obtaining the Administrator or device credentials for use by the attacker.
T.SECURITY_FUNCTIONALITY_FAILURE	An external, unauthorized entity could make use of failed or compromised security functionality and might therefore subsequently use or abuse security functions without prior authentication to access, change or modify device data, critical network traffic or security functionality of the device.
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 attacks, which would provide access to the administrative session, or sessions between Network Devices. Successfully gaining Administrator access allows

Threat Name	Threat Definition
	malicious actions that compromise the security functionality of the device and the network on which it resides.
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.UNTRUSTED_COMMUNICATION_ CHANNELS	Threat agents may attempt to target Network Devices that do not use standardized secure tunnelling 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.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.WEAK_AUTHENTICATION_ENDPOINTS	Threat agents may take advantage of secure protocols that use weak methods to authenticate the endpoints, e.g. a 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.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.
From MOD_ESC_V1.0	
T.MALICIOUS_TRAFFIC	A malformed packet is a protocol packet containing modified data not recognizable by the receiving device (e.g. TOE), or contains modified protocol packets intended to crash or cause the TOE to act in ways unintended. An attacker may attempt to use a VVoIP endpoint to send these malformed packets or malicious traffic towards the TOE in an attempt to control or crash the call control system and connected network devices. To mitigate VVoIP endpoint devices from being used to successfully launch malicious traffic, the TOE must provide encryption remedies to prevent modification of protocol packets. The TOE must also provide authentication mechanisms to prevent unauthorized VVoIP endpoints from improperly registering to the ESC for the purpose of launching malicious attacks.

Threat Name	Threat Definition
T.NETWORK_DISCLOSURE	An attacker may attempt to “map” IP addresses of VVoIP endpoint/devices and other telecommunications equipment for the purpose of determining the organizational structure of the enterprise, providing reconnaissance for future targeted attacks.
T.UNAUTHORIZED_CLIENT	An attacker may attempt to register an unauthorized VVoIP endpoint to the TOE for the purpose of impersonating a legitimate end user device in order to gain unauthorized connectivity to other clients or active calls.

4.3 Organizational Security Policies

Table 3 shows the organizational security policies defined in the individual components of CFG_NDcPP-ESC_V1.0.

Table 3: Organizational Security Policies

OSP Name	OSP Definition
From CPP_ND_V2.2E	
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.
From MOD_ESC_V1.0	
P.SECURED_PLATFORM	Administrators in the organization ensure that general purpose computers use secure operating systems and are configured in accordance with applicable security standards.

4.4 Security Objectives

Table 4 shows the security objectives for the TOE defined in the individual components of CFG_NDcPP-ESC_V1.0.

Table 4: Security Objectives for the TOE

TOE Security Objective	TOE Security Objective Definition
From CPP_ND_V2.2E	
No security objectives for the TOE defined in CPP_ND_V2.2E.	
From MOD_ESC_V1.0	
O.AUTHORIZED_ADMINISTRATION	All network devices are expected to provide services that allow the security functionality of the device to be managed. The ESC, as a specific type of network device, has a refined set of management functions to address its specialized behavior.
O.MEDIA_RECORDING	The ESC has the ability to capture and store metadata for the communications it facilitates in the form of call detail records. It also may optionally capture and store audio/video recordings of these communications. This data can be used to create a record of potential unauthorized or malicious activity that is occurring on the network in which the ESC is deployed.

TOE Security Objective	TOE Security Objective Definition
O.SECURE_VVOIP	The ESC has the ability to securely broker VVoIP communications between endpoint devices as well as external telecommunications equipment. This involves authentication and encryption of VVoIP communications as well as the enforcement of policies that route valid traffic to its intended destination while discarding unauthorized traffic flows. The ESC optionally has the ability to function as an update server for VVoIP software/firmware to ensure that endpoint devices are securely configured.
O.SELF_PROTECTION	The ESC has the ability to capture diagnostic data about its own functionality in real-time so that anomalous behavior or failures can be diagnosed. The ESC also has the ability to respond securely if a failure state is detected so that a crash of the TOE cannot be used to facilitate malicious activity. The ESC also enforces purging of residual data so that security-relevant information cannot be obtained from a decommissioned or refurbished device.
O.SYSTEM_MONITORING	In order to ensure that potentially malicious activity is detected, the NDcPP requires security-relevant events to be audited. The ESC also provides security functions to support system monitoring for the functionality that it adds to the NDcPP. This includes the generation of audit records and system log data, the secure storage and ability to review stored data with authorization, and optionally the ability to suppress the generation of certain audit records to reduce log volume as a means to decrease the likelihood that a critical event is overlooked.

Table 5 shows the security objectives for the Operational Environment defined in the individual components of CFG_NDcPP-ESC_V1.0.

Table 5: Security Objectives for the Operational Environment

Environmental Security Objective	Environmental Security Objective Definition
From CPP_ND_V2.2E	
OE.ADMIN_CREDENTIALS_SECURE	The Administrator’s credentials (private key) used to access the TOE must be protected on any other platform on which they reside.
OE.NO_GENERAL_PURPOSE	There are no general-purpose computing capabilities (e.g., compilers or user applications) available on the TOE, other than those services necessary for the operation, administration and support of the TOE. Note: For vNDs the TOE includes only the contents of the its own VM, and does not include other VMs or the VS.
OE.NO_THRU_TRAFFIC_PROTECTION	The TOE does not provide any protection of traffic that traverses it. It is assumed that protection of this traffic will be covered by other security and assurance measures in the operational environment.
OE.PHYSICAL	Physical security, commensurate with the value of the TOE and the data it contains, is provided by the environment.
OE.RESIDUAL_INFORMATION	The Security Administrator ensures that there is no unauthorized access possible for sensitive residual information (e.g. cryptographic keys, keying material, PINs, passwords etc.) on networking equipment when the equipment is discarded or removed from its operational

Environmental Security Objective	Environmental Security Objective Definition
	environment. For vNDs, this applies when the physical platform on which the VM runs is removed from its operational environment.
OE.TRUSTED_ADMIN	Security Administrators are trusted to follow and apply all guidance documentation in a trusted manner. For vNDs, this includes the VS Administrator responsible for configuring the VMs that implement ND functionality. For TOEs supporting X.509v3 certificate-based authentication, the Security Administrator(s) are assumed to monitor the revocation status of all certificates in the TOE's trust store and to remove any certificate from the TOE's trust store in case such certificate can no longer be trusted.
OE.UPDATES	The TOE firmware and software is updated by an Administrator on a regular basis in response to the release of product updates due to known vulnerabilities.
From MOD_ESC_V1.0	
OE.SECURED_PLATFORM	The operating system of the network device does not provide an interface or other capability that can be used to adversely affect the TOE or its own functionality.
All objectives for the operational environment of the Base-PP also apply to this PP-Module. OE.NO_THRU_TRAFFIC_PROTECTION is still operative, but only for the interfaces in the TOE that are defined by the Base-PP and not the PP-Module.	

5 Functional Requirements

As indicated above, CFG_NDcPP-ESC_V1.0 includes CPP_ND_V2.2E and MOD_ESC_V1.0. The functional requirements from CPP_ND_V2.2E were evaluated separately so this section applies only to the requirements of MOD_ESC_V1.0.

As indicated above, requirements in the MOD_ESC_V1.0 are comprised of modified Base-PP, "base" requirements and additional requirements that are objective. Table 6 contains the modified "base" requirements that were validated as part of the Acumen Security evaluation activities referenced above.

Table 6: Base-PP Modified Security Functional Requirements

Requirement Class	Requirement Component	Verified By
FAU: Security Audit	FAU_GEN.1: Audit Data Generation (Audit Log)	Cellcrypt Server
	FAU_STG.1: Protected Audit Trail Storage	Cellcrypt Server
FCS: Cryptographic Support	FCS_DTLSS_EXT.1 DTLS Server Protocol without Mutual Authentication	Module Evaluation
	FCS_DTLSS_EXT.2 DTLS Server Support for Mutual Authentication	Module Evaluation
	FCS_NTP_EXT.1 NTP Protocol	Cellcrypt Server
	FCS_TLSC_EXT.1 TLS Client Protocol without Mutual Authentication	Cellcrypt Server
	FCS_TLSC_EXT.2 TLS Client Support for Mutual Authentication	Cellcrypt Server
	FCS_TLSS_EXT.1 TLS Server Protocol without Mutual Authentication	Cellcrypt Server
	FCS_TLSS_EXT.2 TLS Server Support for Mutual Authentication	Cellcrypt Server
FIA: Identification and Authentication	FIA_X509_EXT.1/Rev: X.509 Certificate Validation	Cellcrypt Server
	FIA_X509_EXT.2: X.509 Certificate Authentication	Cellcrypt Server
	FIA_X509_EXT.3: X.509 Certificate Requests	Cellcrypt Server
FPT: Protection of the TSF	FPT_STM_EXT.1: Reliable Time Stamps	Cellcrypt Server

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

Table 7: TOE Security Functional Requirements

Requirement Class	Requirement Component	Verified By
FAU: Security Audit	FAU_GEN.1/CDR: Audit Data Generation (Call Detail Record)	Cellcrypt Server

Requirement Class	Requirement Component	Verified By
	FAU_GEN.1/Log: Audit Data Generation (System Log)	Cellcrypt Server
	FAU_SAR.1/Log Audit Review (System Log)	Cellcrypt Server
	FAU_STG.1/CDR Protected Audit Trail Storage (Call Detail Record)	Cellcrypt Server
	FAU_VVR_EXT.1 Recording Voice and Video Call Data	Cellcrypt Server
FDP: User Data Protection	FDP_IFC.1 Subset Information Flow Control	Cellcrypt Server
	FDP_IFF.1 Simple Security Attributes	Cellcrypt Server
	FDP_RIP.1 Subset Residual Information Protection	Cellcrypt Server
FIA: Identification and Authentication	FIA_UAU.2/TC User Authentication before Any Action (Telecommunications Devices)	Cellcrypt Server
	FIA_UAU.2/VVoIP User Authentication before Any Action (VVoIP Endpoints)	Cellcrypt Server
FMT: Security Management	FMT_CFG_EXT.1 Secure by Default Configuration	Cellcrypt Server
	FMT_SMF.1/ESC: Specification of Management Functions (ESC)	Cellcrypt Server
FPT: Protection of the TSF	FPT_FLS.1: Fail with Preservation of a Secure State	Cellcrypt Server
FTP: Trusted Path/Channels	FTP_ITC.1/ESC: Inter-TSF Trusted Channel (ESC Communications)	Cellcrypt Server

Table 8 contains the "**Optional**" (Implementation-Dependent) requirement contained in Appendix A, 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 ACE workunits and has indicated its verification through "Module Evaluation."

Table 8: Optional Requirement (Implementation-Dependent)

Requirement Class	Requirement Component	Verified By
FPT: Protection of the TSF	FPT_TUD_EXT.1/VVoIP Trusted Update (VVoIP Endpoints)	Module Evaluation

Table 9 contains the "**Selection-Based**" requirements contained in Appendix B, and an indication of what evaluation those requirements were verified in (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 ACE workunits and has indicated its verification through "Module Evaluation."

Table 9: Selection-Based Requirements

Requirement Class	Requirement Component	Verified By
FAU: Security Audit	FAU_SEL.1 Selective Audit	Module Evaluation
	FAU_STG.1/VVR Protected Audit Trail Storage (Voice/Video Recording)	Module Evaluation
	FAU_VVR_EXT.2 Generation of Voice and Video Recordings	Module Evaluation

Table 10 contains the "**Objective**" requirements contained in Appendix A, and an indication of what evaluation those requirements were verified in (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 ACE workunits and has indicated its verification through "Module Evaluation."

Table 10: Objective Requirements

Requirement Class	Requirement Component	Verified By
No additional objective requirements.		

6 Assurance Requirements

The PP-Configuration defines its security assurance requirements as those required by CPP_ND_V2.2E. The SARs defined in that PP are applicable to MOD_ESC_V1.0, as well as CFG_NDcPP-ESC_V1.0 as a whole.

7 Results of the Evaluation

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

Table 11: Evaluation Results

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
ACE_MCO.1	Pass	Module evaluation
ACE_CCO.1	Pass	Module 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 MOD_ESC_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] 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] PP-Module for Enterprise Session Controller (ESC), Version 1.0, 19 November 2020.

[7] collaborative Protection Profile for Network Devices, Version 2.2E, 23 March 2020.

[8] PP-Configuration for Network Device and Enterprise Session Controller (ESC), Version 1.0, 19 November 2020

[9] Cellcrypt Server Security Target, Version 0.9.12, 07 April 2022

[10] Assurance Activity Report for Cellcrypt Server, Version 0.2, 11 April 2022