National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

Validation Report

for

CellCrypt Server Version v5.0

Report Number: CCEVS-VR-VID11597-2025
Dated: 1 December 2025
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

Acknowledgements

Validation Team

Swapna Katikaneni
Seada Mohammad
Aerospace Corporation

Common Criteria Testing Laboratory

Anthony Apted
Kofi Owusu
Pascal Patin
Leidos Inc.
Columbia, MD

Table of Contents

List of Tables

1 Executive Summary

This Validation Report (VR) documents the National Information Assurance Partnership (NIAP) assessment of the evaluation of CellCrypt Server v5.0 (the Target of Evaluation, or TOE). It presents the evaluation results, their justifications, and the conformance results. This VR is not an endorsement of the TOE by any agency of the U.S. Government and no warranty of the TOE is either expressed or implied.

This VR is intended to assist the end-user of this product and any security certification agent for that end-user in determining the suitability of this Information Technology (IT) product in their environment. End-users should review the Security Target (ST), which is where specific security claims are made, in conjunction with this VR, which describes how those security claims were evaluated and tested and any restrictions on the evaluated configuration. This VR applies only to the specific version and configuration of the product as evaluated and as documented in the ST. Prospective users should carefully read the Assumptions and Clarification of Scope in Section 5 and the Validator Comments in Section 10, where any restrictions on the evaluated configuration are highlighted.

The evaluation was performed by Leidos Common Criteria Testing Laboratory (CCTL) in Columbia, Maryland, USA, and was completed in December 2025. The information in this report is largely derived from the Evaluation Technical Report (ETR [10]) and associated test report, all written by Leidos. The evaluation determined that the TOE is:

- Common Criteria Part 2 Extended and Common Criteria Part 3 Extended

and demonstrates exact conformance to:

- *Collaborative Protection Profile for Network Devices*, Version 3.0E, 14 December 2023 ([5])
- *Functional Package for SSH,* Version 1.0, 13 May 2021 ([6])
- *PP-Module for Enterprise Session Controller (ESC), Version 1.0, 20 November 2020* ([7])

as clarified by all applicable Technical Decisions.

The TOE is CellCrypt Server v5.0, running on an HPE ProLiant DX380 Gen 10 server appliance.

The TOE identified in this VR has been evaluated at a NIAP approved CCTL using the Common Methodology for IT Security Evaluation (Version 3.1, Rev. 5) for conformance to the Common Criteria for IT Security Evaluation (Version 3.1, Rev. 5). The evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme (CCEVS) and the conclusions of the testing laboratory in the ETR are consistent with the evidence provided.

The validation team monitored the activities of the evaluation team, provided guidance on technical issues and evaluation processes, and reviewed the individual work units documented in the ETR and the Assurance Activities Report (AAR [11]). The validation team found that the evaluation showed that the product satisfies all of the functional requirements and assurance requirements stated in the ST. The conclusions of the testing laboratory in the ETR are consistent with the evidence produced. Therefore, the validation team concludes that the testing laboratory's findings are accurate, the conclusions justified, and the conformance results are correct.

The Leidos evaluation team determined that the TOE is conformant to the claimed Protection Profile (PP) and, when installed, configured and operated as specified in the evaluated guidance documentation CCECG ([9]), satisfies all the security functional requirements stated in the ST ([8]).

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, commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs) use the Common Criteria (CC) and Common Methodology for IT Security Evaluation (CEM) to conduct security evaluations, in accordance with National Voluntary Laboratory Assessment Program (NVLAP) accreditation.

The NIAP Validation Body assigns Validators to monitor the CCTLs to ensure quality and consistency across evaluations. Developers of IT products desiring a security evaluation contract with a CCTL and pay a fee for their product's evaluation. Upon successful completion of the evaluation, the product is added to NIAP's Product Compliant List (PCL).

Table 1 provides information needed to completely identify the product, including:

- The TOE—the fully qualified identifier of the product as evaluated
- The ST—the unique identification of the document describing the security features, claims, and assurances of the product
- The conformance result of the evaluation
- The PP/PP-Modules to which the product is conformant
- The organizations and individuals participating in the evaluation.

Table 1: Evaluation Identifiers

Item	Identifier
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
TOE	CellCrypt Server v5.0
Security Target	Security Target CellCrypt Server, Version 0.5.1, October 2, 2025([8])
Sponsor & Developer	Cellcrypt 361 Southwest Drive Jonesboro, AR 72401
Completion Date	December 2025
CC Version	Common Criteria for Information Technology Security Evaluation, Version 3.1, Release 5, April 2017
CEM Version	Common Methodology for Information Technology Security Evaluation: Version 3.1, Release 5, April 2017
PP	Collaborative Protection Profile for Network Devices, Version 3.0E, 14 December 2023 Functional Package for SSH, Version 1.0, 13 May 2021 PP-Module for Enterprise Session Controller (ESC), Version 1.0, 20 November 2020
Conformance Result	PP Compliant, CC Part 2 extended, CC Part 3 extended

Item	Identifier
CCTL	Leidos Common Criteria Testing Laboratory 6841 Benjamin Franklin Drive Columbia, MD 21046
Evaluation Personnel	Anthony Apted Kofi Owusu Pascal Patin
Validation Personnel	Swapna Katikaneni Seada Mohammad

3 TOE Architecture

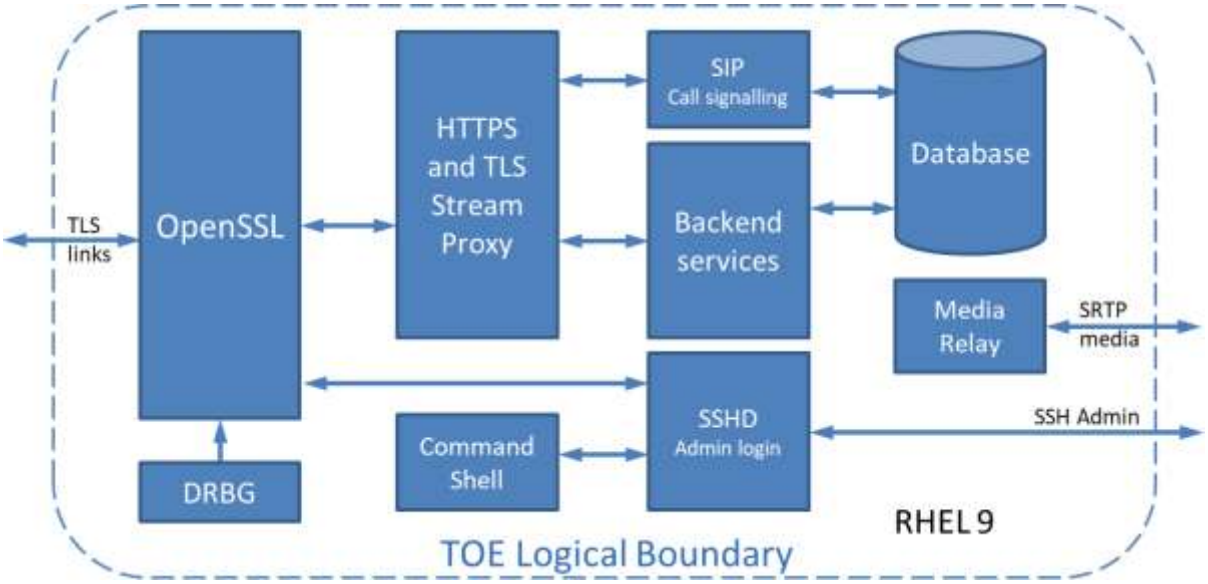
Note: The following architectural description is based on the description presented in the ST[8].

Cellcrypt Server is a secure networking device providing a core set of services for the Cellcrypt communications network. The Cellcrypt network enables end-to-end encrypted multimedia communications between users of mobile and desktop computers. Secure multimedia services include:

- Voice and video (Realtime)
- Text messaging and voice notes (store-and-forward)
- File sharing (store-and-forward)

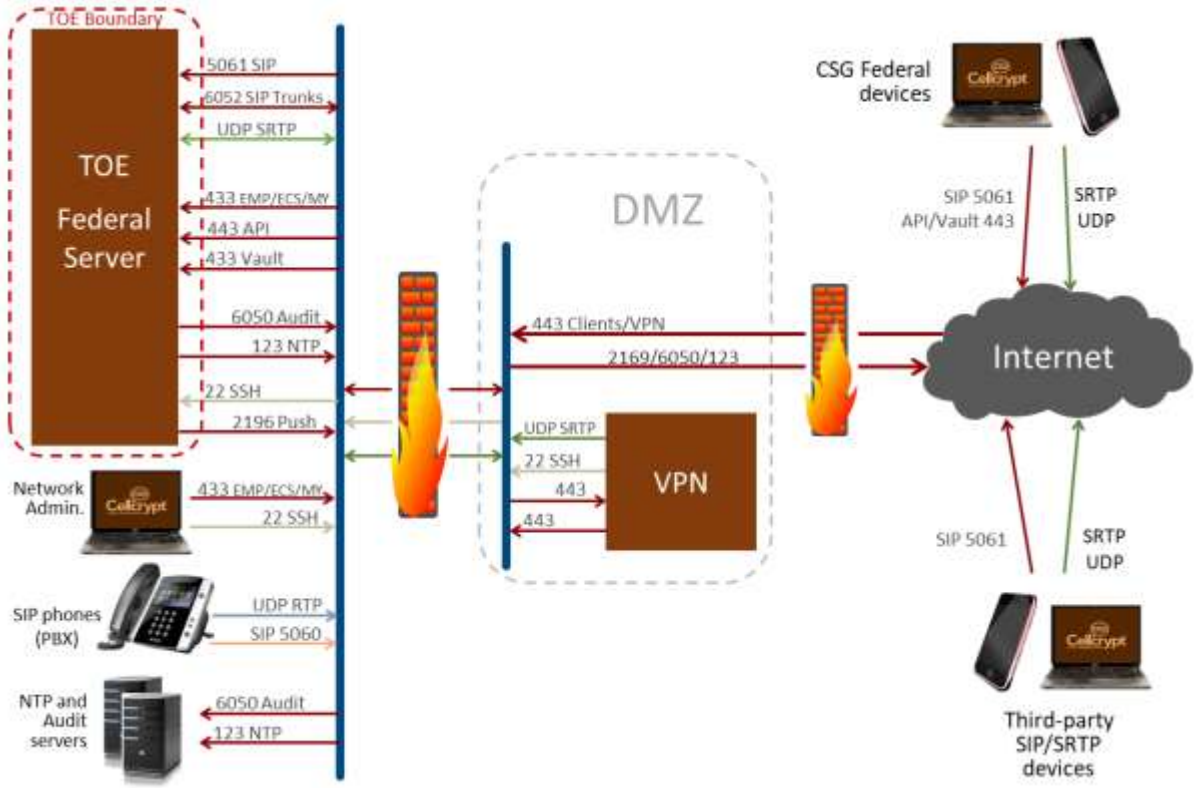
All network communications are encrypted and interoperability with third-party networks using standards-based Realtime and store-and-forward protocols (SIP/SRTP). Cellcrypt Server consists of several services for the management of users, devices and multimedia networks. These services are integrated in a way that takes advantage of common proxying and network security interfaces to better facilitate security analysis.

The TOE software architecture, indicating the TOE logical boundary, is shown in the figure below. Note that the TOE boundary encapsulates the entire Cellcrypt Server and includes the operating system Red Hat Enterprise Linux 9 (64-bit) OS (RHEL 9).



The figure below illustrates a typical TOE deployment network layout showing interoperable access of client devices. The TOE boundary is clearly identified as including the entire Cellcrypt Server. Both Cellcrypt and other Third-party devices make use of the standards based Realtime services (SIP- RFC 3261 and SRTP – RFC 3711). Cellcrypt devices use a proprietary protocol for messaging and attachments via the API and Vault services.

Although not strictly necessary, a VPN server can be set up in a Demilitarized Zone (DMZ) to further protect the internal TOE network.


TOE Boundary
TOE
Federal
Server
5061 SIP
6052 SIP Trunks
UDP SRTP
433 EMP/ECS/MY
443 API
433 Vault
6050 Audit
123 NTP
22 SSH
2196 Push
Network
Admin.
433 EMP/ECS/MY
22 SSH
SIP phones
(PBX)
UDP RTP
SIP 5060
NTP and
Audit
servers
6050 Audit
123 NTP
DMZ
443 Clients/VPN
2169/6050/123
UDP SRTP
22 SSH
443
443
VPN
CSG Federal
devices
SIP 5061
API/Vault 443
SRTP
UDP
Internet
SIP 5061
SRTP
UDP
Third-party
SIP/SRTP
devices

4 Security Policy

The TOE enforces the following security policies as described in the ST.

Note: Much of the description of the security policy has been derived from the ST([8]) and the Final ETR([10]).

4.1.1 Security Audit

The TOE generates audit records of the activities performed on it as well as activities related to trusted channel establishment and operations. This includes call detail records (CDR) of VVoIP calls as well as well as real-time system diagnostic information. The TOE securely stores audit records locally and has the ability to transmit stored audit records to a remote audit server using a trusted channel.

4.1.2 Cryptographic Support

The TOE implements cryptography to protect data in transit. The TOE implements SSH as a server and mutually-authenticated TLS 1.3 as both a client and server. It also implements HTTPS as a server for remote administration and NTP for secure network time synchronization. Cryptographic operations are performed using NIST validated algorithm implementations via OpenSSL. Key destruction is performed when keys are no longer in use. The TOE's DRBG is seeded using entropy from the processor RDSEED instruction set.

4.1.3 Identification and Authentication

The TOE supports administrator authentication using SSH password, SSH public key, local password, and web GUI-based password. It enforces authentication before use of the TSF, both for administrators and for connected VVoIP devices. For password-based authentication, it enforces password composition requirements and lockout in the event of excessive failed authentication attempts. For connections that require validation of X.509 certificates, the TOE enforces validity checking on certificates, including the use of CRL or OCSP for revocation checking. The TOE also has a mechanism to generate a certificate signing request to obtain a certificate that it can present to external entities.

4.1.4 Security Management

The TOE includes management interfaces to configure its own security functionality as well as the functionality that governs the behavior of connected client devices in the TOE's operational environment. Management is performed using a local or remote interface, and security relevant functions are restricted to authorized administrators.

4.1.5 Protection of the TSF

The TOE protects keys and credential data at rest. It also enforces self-protection through performing power-on self-tests and enters a fail-secure state if any of the self-tests fail. It also enforces trusted updates by ensuring that only signed updates will be installed. It includes an NTP server connection to provide accurate time data, which supports auditing, cryptographic, and authentication functions.

4.1.6 TOE Access

The TOE terminates idle administrative sessions and provides a means for administrators to actively terminate their own sessions. It also displays a pre-authentication warning banner governing acceptable use of the TSF.

4.1.7 Trusted Path/Channels

The TOE encrypts sensitive data in transit between itself and its operational environment using TLS and TLS/HTTPS for communication with VVoIP endpoints and remote audit servers and between remote administrators and the TOE using SSH and TLS/HTTPS.

5 Assumptions and Clarification of Scope

5.1 Assumptions

The ST references the PP and the Functional Package to which it claims conformance for assumptions about the use of the TOE. Those assumptions, drawn from the claimed PP, are as follows:

- The TOE is assumed to be physically protected in its operational environment and not subject to attacks that require physical access to the TOE hardware or logical access to a TOE interface that can only be invoked locally.
- The TOE is assumed to provide limited computing functionality outside of its intended purpose and is not used as a general-purpose computer.
- The TOE does not provide protection of traffic that traverses it, beyond ensuring that the channels used for this traffic are established in a secure manner.
- The administrator of the TOE is not careless, willfully negligent or hostile, and administers the software in compliance with the applied enterprise security policy.
- The TOE is updated on a regular basis by an administrator as updates are made available by the TOE developer
- Administrator credentials are protected within the TOE and are not stored in an insecure manner outside of it.
- It is assumed that there is no unauthorized access to the TOE when the TOE is discarded or removed from its operational environment.

5.2 Clarification of Scope

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

- As with any evaluation, this evaluation only shows that the evaluated configuration meets the security claims made, with a certain level of assurance (the evaluation activities specified in *collaborative Protection Profile for Network Devices*, Version 3.0E, 14 December 2023 ([5]), *Functional Package for SSH,* Version 1.0, 13 May 2021 ([6]), and *PP-Module for Enterprise Session Controller (ESC), Version 1.0, 20 November 2020* ([7]) was performed by the evaluation team).
- This evaluation covers only the specific software distribution and version identified in this document, and not any earlier or later versions released or in process.
- The evaluation of security functionality of the product was limited to the functionality specified in Security Target Cellcrypt Server, Version 0.5.1, October 2, 2025 ([8]).
- The TOE consists solely of software and relies on its operational environment for supporting security functionality, as identified in the ST[8].
- 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.
- The TOE must be installed, configured and managed as described in the documentation referenced in Section 6 of this VR.

- Other functionalities excluded from this evaluation are secure messaging, file sharing, or group communications.
-

6 Documentation

The vendor offers guidance documents describing the installation process for the TOE as well as guidance for subsequent administration and use of the applicable security features. The guidance documentation examined during the evaluation and delivered with the TOE is as follows:

- *Common Criteria Administrator Guide Cellcrypt Server, Version 0.7.3, September 15, 2025([9])*

To use the product in the evaluated configuration, the product must be configured as specified in this documentation.

Any additional customer documentation provided with the product, or that which may be available online, was not included in the scope of the evaluation and therefore should not be relied upon to configure or operate the TOE as evaluated. Consumers are encouraged to download the evaluated administrative guidance documentation from the NIAP website.

7 IT Product Testing

This section describes the testing efforts of the evaluation team. It is derived from information contained in the following proprietary document:

- *CellCrypt Server v5.0 Common Criteria Test Report and Procedures,* Version 1.0, September 15, 2025 ([12])

A non-proprietary description of the tests performed, and their results is provided in the following document:

- *Assurance Activities Report for CellCrypt Server v5.0*, Version 1.0, November 26, 2025 ([11])

The purpose of the testing activity was to confirm the TOE behaves in accordance with the TOE security functional requirements as specified in the ST for a product that claims conformance to *Collaborative Protection Profile for Network Devices*, Version 3.0E, 14 December 2023 ([5]), *Functional Package for SSH,* Version 1.0, 13 May 2021 ([6]), and *PP-Module for Enterprise Session Controller (ESC), Version 1.0, 20 November 2020 ([7])*.

The evaluation team devised a Test Plan based on the test evaluation activities in the materials referenced above. The Test Plan described how each test activity was to be instantiated within the TOE test environment. The evaluation team executed the tests specified in the Test Plan and documented the results in the team test report listed above.

Independent testing took place at Leidos CCTL facilities in Columbia, Maryland, from March 2025 to September 2025.

The evaluators received the TOE in the form that customers would receive it, installed and configured the TOE in accordance with the provided guidance, and exercised the Team Test Plan on equipment configured in the testing laboratory.

Given the complete set of test results from the test procedures exercised by the evaluators, the testing requirements for *collaborative Protection Profile for Network Devices, Functional Package for SSH, and PP-Module for Enterprise Session Controller (ESC)* were fulfilled.

7.1 Test Configuration

The evaluation team established a test configuration consisting of the TOE (Cellcrypt Server) appliance deployed in an environment with the following dependencies:

- Android phones running Cellcrypt Client: used to establish VVoIP communications that are brokered by the TOE
- Cellcrypt ESC Server: used to demonstrate inter-TSF trusted communications with a second server located in the TOE's operational environment (to demonstrate call forwarding).
- TLS Test Server: used for TLS client/server testing and port scanning
- Revocation Test Server: used to test X.509 revocation
- NTP Server: used to test NTP time synchronization

8 Evaluated Configuration

The TOE consists of the Cellcrypt Server version 5 firmware running on an HPE ProLiant DX380 Gen10 server appliance.

9 Results of the Evaluation

The results of the evaluation of the TOE against its target assurance requirements are generally described in this section and are presented in detail in the Evaluation Technical Report for Cellcrypt Server5 ([10]). The reader of this VR can assume that all assurance activities and work units received passing verdicts.

A verdict for an assurance component is determined by the resulting verdicts assigned to the corresponding evaluator action elements. The evaluation was conducted based upon CC version 3.1, revision 5 ([1], [2], [3]) and CEM version 3.1, revision 5 ([4]), and the specific evaluation activities specified in *collaborative Protection Profile for Network Devices, Version 3.0E, 14 December 2023* ([5])*, Functional Package for SSH, Version 1.0, 13 May 2021* ([6])*, and PP-Module for Enterprise Session Controller (ESC), Version 1.0, 20 November 2020* ([7]). The evaluation determined the TOE satisfies the conformance claims made in the Cellcrypt Server Security Target([8]), of Part 2 extended and Part 3 extended. The TOE satisfies the requirements specified in:

- *Collaborative Protection Profile for Network Devices*, Version 3.0E, 14 December 2023 ([5])
- *Functional Package for SSH,* Version 1.0, 13 May 2021 ([6])
- *PP-Module for Enterprise Session Controller (ESC), Version 1.0, 20 November 2020 ([7])*

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

9.1 Evaluation of the Security Target (ST) (ASE)

The evaluation team performed each TSS assurance activity and ASE CEM work unit. The ST evaluation ensured the ST contains an ST introduction, TOE overview, TOE description(also referred as the TOE Architecture), security problem definition in terms of threats, policies and assumptions, description of security objectives for the operational environment, a statement of security requirements claimed to be met by the product that are consistent with the claimed Protection Profile, and security function descriptions that satisfy the requirements.

The Validation team reviewed the work of the Evaluation team and found that sufficient evidence and justification was provided by the Evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the Evaluation team was justified.

9.2 Evaluation of the Development (ADV)

The evaluation team performed each ADV assurance activity and applied each ADV_FSP.1 CEM work unit. The evaluation team assessed the evaluation evidence and found it adequate to meet the requirements specified in the claimed Protection Profile for design evidence. The ADV evidence consists of the TSS descriptions provided in the ST and product guidance documentation providing descriptions of the TOE external interfaces.

The Validation team reviewed the work of the Evaluation team and found that sufficient evidence and justification was provided by the Evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the Evaluation team was justified.

9.3 Evaluation of the Guidance Documents (AGD)

The evaluation team performed each guidance assurance activity and applied each AGD work unit. The evaluation team determined the adequacy of the operational user guidance in describing how to operate the TOE in accordance with the descriptions in the ST. The evaluation team followed the guidance in the TOE preparative procedures to test the installation and configuration procedures to ensure the procedures result in the evaluated configuration. The guidance documentation was assessed during the design and testing phases of the evaluation to ensure it was complete.

The Validation team reviewed the work of the Evaluation team and found that sufficient evidence and justification was provided by the Evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the Evaluation team was justified.

9.4 Evaluation of the Life Cycle Support Activities (ALC)

The evaluation team performed each ALC assurance activity and applied each ALC_CMC.1 and ALC_CMS.1 CEM work unit, to the extent possible given the evaluation evidence required by the claimed Protection Profile. The evaluation team ensured the TOE is labeled with a unique identifier consistent with the TOE identification in the evaluation evidence, and that the ST describes how timely security updates are made to the TOE.

The Validation team reviewed the work of the Evaluation team and found that sufficient evidence and justification was provided by the Evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the Evaluation team was justified.

9.5 Evaluation of the Test Documentation and the Test Activity (ATE)

The evaluation team performed each test activity and applied each ATE_FUN.1 CEM work unit. The evaluation team ran the set of tests specified by the claimed PP and recorded the results in the Test Report, summarized in the AAR.

The Validation team reviewed the work of the Evaluation team and found that sufficient evidence and justification was provided by the Evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the Evaluation team was justified.

9.6 Vulnerability Assessment Activity (AVA)

The evaluation team performed a search of the following online sources:

- National Vulnerability Database (https://nvd.nist.gov/)
- US-Cert (https://www.kb.cert.org/vuls/html/search)
- Tipping Point Zero Day Initiative (https://www.zerodayinitiative.com/advisories/published/)
- Palo Alto Networks Security Advisories (https://security.paloaltonetworks.com/).

The searches were performed several times, most recently November 10, 2025 using the following search terms:

- Cellcrypt
- Redhat 9.5

- HPE ProLiant
- Intel Xeon Gold
- 2nd Generation Intel Xeon
- SATA hot-plug
- RDSEED
- SRTP
- SIP RFC 3261
- Enterprise Communications Service
- Enterprise Communications System
- Enterprise Management Portal
- Auxiliary service

The results of these searches did not identify any vulnerabilities that are applicable to the TOE. The conclusion drawn from the vulnerability analysis is that no residual vulnerabilities exist that are exploitable by attackers with Basic Attack Potential as defined by the Certification Body in accordance with the guidance in the CEM.

The evaluation team's assessment of the evaluation evidence demonstrates that the claims in the ST are met, sufficient to satisfy the assurance activities specified in the claimed PP. Additionally, the evaluation team's testing also demonstrated the accuracy of the claims in the ST.

The validation team's assessment of the evidence provided by the evaluation team is that it demonstrates that the evaluation team followed the procedures defined in the CEM, and correctly verified that the product meets the claims in the ST.

9.7 Summary of Evaluation Results

The evaluation team's assessment of the evaluation evidence demonstrates that the claims in the ST are met, sufficient to satisfy the assurance activities specified in the claimed Protection Profile. Additionally, the evaluation team's testing also demonstrated the accuracy of the claims in the ST.

The validation team's assessment of the evidence provided by the evaluation team is that it demonstrates that the evaluation team followed the procedures defined in the CEM, and correctly verified that the product meets the claims in the ST.

10 Validator Comments/Recommendations

The validation team notes that the evaluated configuration is dependent upon the TOE being configured per the evaluated configuration instructions in the Common Criteria Administrator Guide Cellcrypt Server, Version 0.7.3, September 15, 2025.

No versions of the TOE and software, either earlier or later are covered by the scope of this evaluation. The scope of this evaluation was limited to the functionality and assurances covered in the collaborative Protection Profile for Network Devices, Version 3.0E, 14 December 2023, Functional Package for SSH, Version 1.0, 13 May 2021, and PP-Module for Enterprise Session Controller (ESC), Version 1.0, 20 November 2020 as described for this TOE in the Security Target.

Other functionalities like secure messaging, file sharing, or group communications (included in the product) were not assessed as part of this evaluation because no NIAP Protection Profile exists for these functionalities and Exact Conformance requires only the functionality specified by Protection Profiles to be included within the evaluation scope. All other functionality provided by the devices needs to be assessed separately, and no further conclusions can be drawn about their effectiveness. All other items and scope issues have been sufficiently addressed elsewhere in this document.

11 Security Target

The ST for this product's evaluation is *CellCrypt Server Security Target, Version 0.5.1, October 2, 2025 [8].*

12 Abbreviations and Acronyms

This section identifies abbreviations and acronyms used in this document.

API	Application Programming Interface
CC	Common Criteria for Information Technology Security Evaluation
CCTL	Common Criteria Testing Laboratory
CEM	Common Evaluation Methodology
ETR	Evaluation Technical Report
IT	Information Technology
PCL	Product Compliant List
PII	Personally Identifiable Information
SAR	Security Assurance Requirement
SFR	Security Functional Requirement
ST	Security Target
TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	TOE Security Functions
TSS	TOE Summary Specification
VR	Validation Report

13 Bibliography

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

[1] Common Criteria Project Sponsoring Organisations. Common Criteria for Information Technology Security Evaluation: Part 1: Introduction and general model, Version 3.1, Revision 5, April 2017.

[2] Common Criteria Project Sponsoring Organisations. Common Criteria for Information Technology Security Evaluation: Part 2: Security functional components, Version 3.1, Revision 5, April 2017.

[3] Common Criteria Project Sponsoring Organisations. Common Criteria for Information Technology Security Evaluation: Part 3: Security assurance requirements, Version 3.1, Revision 5, April 2017.

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

[5] collaborative Protection Profile for Network Devices, Version 3.0E, 14 December 2023

[6] Functional Package for SSH, Version 1.0, 13 May 2021

[7] PP-Module for Enterprise Session Controller (ESC), 20 November 2020

[8] Security Target CellCrypt Server, Version 0.5.1, October 2, 2025

[9] Common Criteria Administrator Guide Cellcrypt Server, Version 0.7.3, September 15, 2025

[10] Evaluation Technical Report for CellCrypt Server v5.0 (Proprietary), Version 1.0, November 26, 2025

[11] Assurance Activities Report for CellCrypt Server v5.0, Version 1.0, November 26, 2025

[12] CellCrypt Server v5.0 Common Criteria Test Report and Procedures, Version 1.0, September 15, 2025

[13] CellCrypt Server v5.0 Vulnerability Analysis, Version 1.0, November 10, 2025