National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

TM

Validation Report

for the

Cellcrypt Server

Report Number: CCEVS-VR-VID11207-2022

Dated: April 25, 2022

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

Jerome Myers, Ph.D.

Patrick Mallett, Ph.D.

DeRon Graves

Seada Mohammed
The Aerospace Corporation

Joyce Baidoo

Richard (Rip) Toren
John Hopkins University APL

Common Criteria Testing Laboratory

Shaunak Shah

Shaina Rae

Swapnil Lad

Rahul Joshi

Acumen Security, LLC

Table of Contents

1 Executive Summary

This Validation Report (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 for 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 tested and evaluated and any restrictions on the evaluated configuration. 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.

This report documents the National Information Assurance Partnership (NIAP) assessment of the evaluation of the Cellcrypt Server Target of Evaluation (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 applies only to the specific version and configuration of the product as evaluated and documented in the ST.

The evaluation was completed by Acumen Security in April 2022. The information in this report is largely derived from the Evaluation Technical Report (ETR) and associated test report, all written by Acumen Security. The evaluation determined that the product is both Common Criteria Part 2 Extended and Part 3 Extended, and meets the assurance requirements of the collaborative Protection Profile for Network Devices, Version 2.2e (cPP_ND_V2.2e) and PP-Module for Enterprise Session Controller (ESC), Version 1.0 (MOD_ESC_V1.0).

The TOE identified in this VR has been evaluated at a NIAP approved Common Criteria Testing Laboratory 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), as interpreted by the Assurance Activities contained in the collaborative Protection Profile for Network Devices, Version 2.2e (cPP_ND_V2.2e) and PP-Module for Enterprise Session Controller (ESC), Version 1.0 (MOD_ESC_V1.0). This VR applies only to the specific version of the TOE as evaluated. The evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme and the conclusions of the testing laboratory in the ETR are consistent with the evidence provided.

The validation 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). The validation team found that the evaluation showed that the product satisfies all of the functional requirements and assurance requirements stated in the ST. Based on these findings, the validation team concludes that the testing laboratory's findings are accurate, the conclusions justified, and the conformance results are correct. The conclusions of the testing laboratory in the ETR are consistent with the evidence produced.

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 PPs containing Assurance Activities, which are interpretations of CEM work units specific to the technology described by the PP.

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.

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

- The Target of Evaluation (TOE): the fully qualified identifier of the product as evaluated.
- The Security Target (ST), describing the security features, claims, and assurances of the product.
- The conformance result of the evaluation.
- The Protection Profile(s) 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 v2.5.0
Protection Profile	collaborative Protection Profile for Network Devices, Version 2.2e (cPP_ND_V2.2e) and PP-Module for Enterprise Session Controller (ESC), Version 1.0 (MOD_ESC_V1.0)
Security Target	Cellcrypt Server Security Target v1.0, dated June 10, 2022
Evaluation Technical Report	Evaluation Technical Report for Cellcrypt Server Version 0.4, dated June 14, 2022
CC Version	Version 3.1, Revision 5
Conformance Result	CC Part 2 Extended and CC Part 3 Conformant
Sponsor	Cellcrypt, Inc.
Developer	Cellcrypt, Inc.
Common Criteria Testing Lab (CCTL)	Acumen Security Rockville, MD
CCEVS Validators	Jerome Myers Patrick Mallett Joyce Baidoo

Item	Identifier
	DeRon Graves Seada Mohammed Richard (Rip) Toren

3 Architectural Information

Product Description:
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/XMPP).

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.

Evaluated Configuration:
The evaluated configuration consists of the hardware and software listed below when configured in accordance with the documentation specified in section 6. The TOE Hardware is implemented as a rack-mounted server.

The TOE hardware consists of a Hewlett-Packard (HP) rack-mounted server with the following specifications:

Table 2: Hardware Details

Feature	Details
Server Model	HP ProLiant DL360p Gen9
Processor	2 x Intel Xeon E5-2680 V4 2.1GHz 8 Core
Chipset family	Broadwell
Memory	96GB DDR4 RAM DIMMs
Disk storage	2 x 300GB 3.5-inch SATA hot-plug disks Smart Array P440ar 12Gbps 2GB Cache RAID Controller
I/O slots	Embedded 4x1GbE Network Adapter; Serial Port Connector (Optional); 3 x PCIe 3.0 Slots; 2 x USB 3.0 Connectors; VGA Video Connector; Dedicated iLO 4 connectors; Flexible LOM bay (Optional)
Ports	Front: 2 USB; Rear: 4 USB, video (1600 x 1200), network; Internal: 1 USB, 1 SD Card
Power Supplies	2 x 800W PSUs
Form Factor	8 Bay SFF 1U Server
Dimensions	19.7 x 19 x 1.75 inches
Weight	40 pounds

The software consist of Cellcrypt Server v2.5.0 distribution package consisting of various Network Services running on Red Hat Enterprise Linux 7.6 64-bit OS (RHEL 7.6).

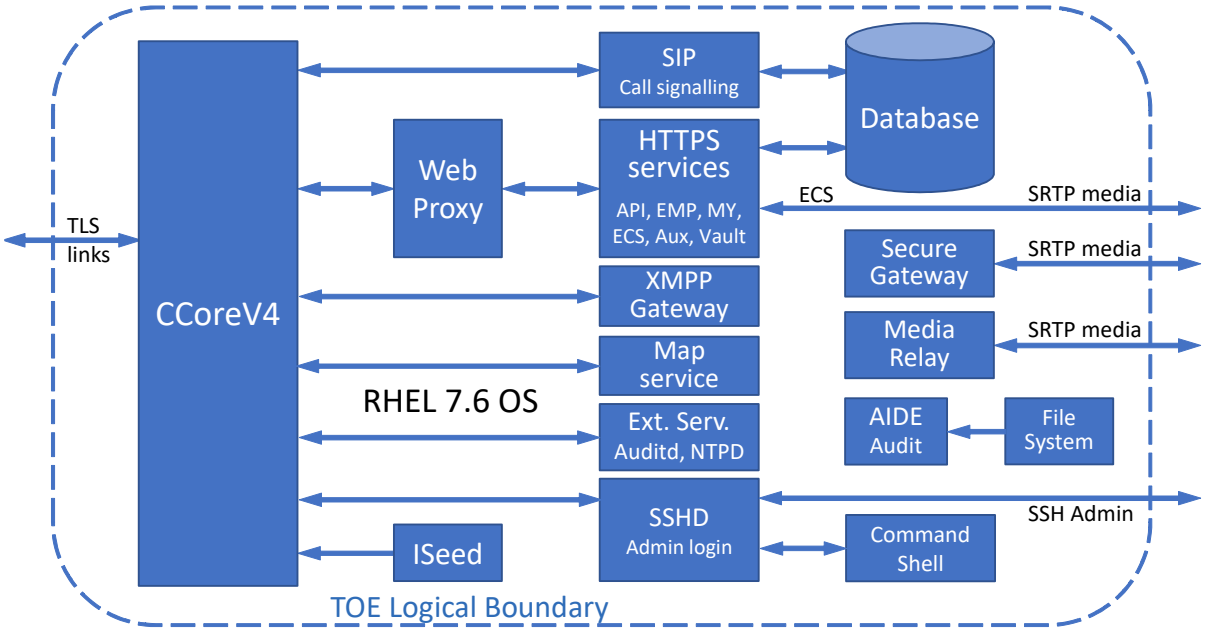

Figure 1 TOE Software Architecture

3.1 Network Services

The network services shown in Figure 1 are described in more detail below. The web proxy (nginx) provides TLS services for the HTTPS virtual hosts using the CCoreV4 module. The other TLS hosts use CCoreV4 directly for TLS services. Command shell access is protected with SSH also using the CCoreV4 crypto algorithms. This provides a consistent secure network interface for the TOE. CCoreV4 is a FIPS 140-2 validated crypto module with its own validated DRBG receiving seeding from the Intel RDSEED instruction. ECS and the Secure Gateway provide media conferencing services protected by SRTP. The media relay is simply a TURN service facilitating SRTP media to traverse NAT routers. The AIDE Intrusion Detection System (IDS) monitors the file system to detect external hacking.

3.1.1 SIP Server

The SIP server provides the main ESC service facilitating all secure voice/video calls by connecting calls and signalling call progress/status using the SIP protocol in accordance with RFC 3261. In addition to normal SIP calling services, SDES key management is handled via the SIP server. The SDES key exchange occurs in the Session Description Protocol (SDP) in accordance with RFC 4566.

3.1.2 Enterprise Management Portal (EMP)

The Enterprise Management Portal provides a secure web application for Enterprise clients to manage their users. Licenses can be purchased, assigned to users and features can be enabled or disabled for users within the Enterprise group. The Enterprise Management Portal provides advanced control of the Cellcrypt user's devices, providing features such as remote wipe, and information about the user's device, such as operating system and version.

3.1.3 MY Server

The MY server is a user-oriented web service, allowing users to manage things like changing passwords, adding devices to the same account, etc. This service may be limited to administrator-only usage.

3.1.4 API Server

The API server is a web service mainly facilitating secure Suite B messaging. All Cellcrypt Suite B messaging clients send and retrieve secure messages via the API server. The API server also provides a general Cellcrypt client API for other housekeeping services.

3.1.5 Vault Server

The Vault service provides its own database (MariaDB) for storing message attachments. All file attachments are encrypted by the clients prior to uploading. The encryption key, together with the Vault attachment URI is distributed to recipients of the attachment via the Cellcrypt secure messaging service (see Cryptography section).

3.1.6 Enterprise Communications Service

Enterprise Communications Service (ECS) allows administrators to set up scheduled voice conferences and add users into groups. The group feature allows, not only administrators, but also users, to create communication groups. Users within groups can communicate with each other just like a Whatsapp group. Group communication features include messaging, attachments, voice notes, and normal voice conferencing.

3.1.7 Auxiliary service

This service provides general purpose information and configuration options for Cellcrypt client devices e.g. The latest version of the Cellcrypt client application software can be queried here.

3.1.8 XMPP Server

The XMPP server provides a gateway service between standard XMPP/Jabber messaging servers and the Cellcrypt Suite B messaging service. The XMPP server interface accepts XMPP/Jabber messages from its own registered clients, or messages forwarded to its domain from specific (configured) external XMPP server. External Jabber usernames can be pre-configured on the server, or automatically added to Cellcrypt contact lists after the first message sent e.g. in the same way that Cellcrypt messaging automatically adds new contacts.

3.1.9 MAP Service

The MAP service provides secure mapping information to facilitate secure navigation and location privacy for field personnel.

3.1.10 Secure Gateway

The Secure Gateway (SG) provides a hub for voice mixing in voice conferences. The SG can bridge calls to a standard PBX as well as standalone SIP phones. Conferences can include a mixture of Cellcrypt users, PBX SIP/analog phones as well as standalone SIP phones.

3.1.11 Secure Shell Host Daemon

This Secure Shell Host Daemon (SSHD) is the standard Linux OpenSSH server which will be used to provide a command terminal for remote server administration. The SSH protocol is secured using the common CCoreV4 instance.

3.1.12 Audit Daemon

The audit daemon (Auditd) is a standard service on Linux providing a user-space central point for sending auditable notifications. All security and other important activities are logged using this service. Auditd is configured to provide remote audit reporting and connects to a remote audit server. The link to the remote audit server is TLS-secured using the STunnel service with CCoreV4.

3.1.13 Network Time Protocol Daemon

The Network Time Protocol Daemon (NTPD) is a Linux service for synchronizing the server's local real-time clock with an online server's real-time clock using the standard NTP protocol [Ref 14]. The link to the remote NTP server is TLS-secured using the STunnel service with CCoreV4.

3.1.14 ISeed Entropy gathering Utility

The ISeed utility gathers entropy using the Intel Processor's RDSEED instruction. The RDSEED instruction provides access to a high-speed NIST SP800-90B & SP 800-90C(draft) compliant entropy source. This will ensure that the CCoreV4 DRBG always has sufficient entropy even under high network usage conditions.

3.1.15 Advanced Intrusion Detection Environment

The Advanced Intrusion Detection Environment (AIDE) detects and logs any changes to the file system. This service is used as a detect-and-alert system to facilitate rapid response to attempts to hack into the Cellcrypt Server. AIDE is only used to support auditing and integrity testing. The intrusion detection and prevention capabilities are excluded from the evaluation.

4 Security Policy

The TOE consists of several security functions that make up the logical scope of the TOE:

- Security audit
- Cryptographic support
- Data protection
- Identification and authentication
- Security management
- Protection of the TSF
- TOE access
- Trusted path/channels

Security Audit

All significant events occurring on the TOE e.g. warnings, errors, and particularly security-related events are logged by the TOE as audit events. The logs also include Call Detail Records (CDR's). All events are uploaded to a remote syslog server protected by a TLS link.

Cryptographic Support

All TOE cryptography is performed by the Cellcrypt CCoreV4 FIPS 140-2 validated crypto module (Certificate #A1999). The TOE cryptographic support includes functions supporting key management, encryption and decryption, random number generation, digital signatures, secure hashing and keyed secure hashing. Cryptographic protocol support includes TLS, SSH, HTTPS.

Table 3: Cryptographic Algorithms

Algorithms	Options	Certificates
DRBG (SP 800-90Ar1)	CTR_DRBG: (AES-256)	CAVP: A1999
AES (FIPS 197)	Modes: CTR, CBC, GCM (SP 800-38D) Key lengths: 128, 256 bits	CAVP: A1999
SHA2 (FIPS 180-4)	Hash lengths: 256, 384, 512	CAVP: A1999
HMAC (FIPS 198)	Hash lengths: 256, 384, 512	CAVP: A1999
RSA (FIPS 186-2)	KeyGen, SigGen, SigVer Key length: 2048 bits	CAVP: A1999
KAS-ECC-SSC (SP 800-56Ar3)	KeyExch Curves: P-256, P-384, P521	CAVP: A1999
ECDSA (FIPS 186-4)	KeyGen, SigGen, SigVer	CAVP: A1999

Data Protection

The TOE enforces the ESC SFP on all VVoIP calls and mediates the data flow between enrolled caller and callee pairs.

Identification and Authentication

The TOE enforces role-based authorization for all administrative access. Administrators must have a user account on the TOE with an assigned administrative role and the TOE authenticates administrators by username and password and validates the administrator's login credentials based on possession of an SSH private key. The TOE also validates X.509v3 certificate access on all TLS ports that make use of client certificates.

Security Management

In addition to command line access, the TOE also provides administrators with HTTPS web portals allowing authorized access to database functionality for administrating user and device profiles. Access to the web portals is based on username and password.

Protection of the TSF

The TOE provides comprehensive protection mechanisms to prevent unauthorized modification of its software. Built-In Self-Tests (BIST) are used to validate the integrity of all files stored on the TOE's persistent storage media and updates to the TOE software are validated using digital signatures. All file modification events are logged locally and remotely based on reliable timestamps due the use of an external NTP time source. Warning banners are used at the start of any interactive session and session inactively timers are used to terminate inactive sessions.

TOE Access

Before any Administrator access to the TOE is established, the TOE displays a security banner with an advisory notice and consent warning message. All inactive Administrator user sessions are automatically terminated after a preconfigured period. Both Administrators and normal users can manually terminate sessions at any time requiring re-authentication to the TOE before establishing a new session.

Trusted Path/Channels

All communication channels on the TOE are cryptographically protected and all administrative interaction is authenticated. ESC SFP is enforced on all user communications based on authorized user subscriptions.

5 Assumptions, Threats & Clarification of Scope

5.1 Assumptions

The specific conditions listed in the following subsections are assumed to exist in the TOE's 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.

Assumptions are drawn from:

- collaborative Protection Profile for Network Devices, Version 2.2e (cPP_ND_V2.2e)
- PP-Module for Enterprise Session Controller (ESC), Version 1.0 (MOD_ESC_V1.0)

5.2 Threats

The following lists the threats addressed by the TOE and the IT Environment. The assumed level of expertise of the attacker for all the threats identified below is Enhanced-Basic.

Threats are drawn from:

- collaborative Protection Profile for Network Devices, Version 2.2e (cPP_ND_V2.2e)
- PP-Module for Enterprise Session Controller (ESC), Version 1.0 (MOD_ESC_V1.0)

5.3 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 level of assurance for this evaluation is defined within the collaborative Protection Profile for Network Devices, Version 2.2e (cPP_ND_V2.2e) and PP-Module for Enterprise Session Controller (ESC), Version 1.0 (MOD_ESC_V1.0). Consistent with the expectations of the PP, this evaluation did not specifically search for, nor seriously attempt to counter, 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 evaluation of security functionality of the product was limited to the functionality specified in the claimed PPs. Any additional security related

functional capabilities included in the product were not covered by this evaluation.

- Please refer to Section 7.2 for any excluded functionality from this evaluation.

6 Documentation

The following documents were provided with the TOE by the vendor for evaluation. Only these documents should be trusted for the installation, administration, and use of the product in the evaluated configuration:

- Cellcrypt Server Common Criteria Administrator Guide v0.8.10, dated March 31, 2022
- Cellcrypt Federal Stack – Installation Manual, dated February 17, 2022
- Cellcrypt Federal Stack – Maintenance Manual, dated February 17, 2022
- Cellcrypt Federal Stack – Auditing and Monitoring dated February 22, 2022
- Cellcrypt Enterprise Management Portal (EMP) User Manual v1.5, dated May 2020
- User Guide for the Enterprise Communications Service v1.0.10, dated March 24, 2016

7 TOE Evaluated Configuration

7.1 Evaluated Configuration

The Cellcrypt Server version 2.5.0 was evaluated on the hardware of a Hewlett-Packard (HP) rack-mounted server. The server model is the HP ProLiant DL360p Gen9 which uses two Intel Xeon E5-2680 V4 2.1 GHz 8 Core (Broadwell) processors.

Please refer to the Cellcrypt Server Common Criteria Administrator Guide in Section 6 to configure the TOE in the evaluated configuration.

7.2 Excluded Functionality

The Advanced Intrusion Detection Environment (AIDE) is only used to support auditing and integrity testing and the intrusion detection and prevention capabilities are excluded from the evaluation.

8 IT Product Testing

This section describes the testing efforts of the developer and the evaluation team. It is derived from information contained in Evaluation Test Report for Cellcrypt Server, which is not publicly available. The Assurance Activities Report (AAR) for Cellcrypt Server Section 4 and Section 6 provides an overview of testing and the prescribed assurance activities. The Test Tools and Test Configurations are identified in Section 4.13 of the AAR.

8.1 Developer Testing

No evidence of developer testing is required in the Assurance Activities for this product.

8.2 Evaluation Team Independent Testing

The evaluation team verified the product according to the vendor-provided guidance documentation and ran the tests specified in the collaborative Protection Profile for Network Devices, Version 2.2e (cPP_ND_V2.2e) and PP-Module for Enterprise Session Controller (ESC), Version 1.0 (MOD_ESC_V1.0). The Independent Testing activity is documented in the Assurance Activities Report for Cellcrypt Server Section 4 and Section 6, which is publicly available, and is not duplicated here.

9 Results of the Evaluation

The results of the assurance requirements are generally described in this section and are presented in detail in the proprietary documents: the Detailed Test Report (DTR) and the Evaluation Technical Report (ETR). The reader of this document can assume that all activities and work units received a passing verdict.

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 rev 5 and CEM version 3.1 rev 5. The evaluation determined the Cellcrypt Server to be Part 2 extended, and meets the SARs contained in the PP. Additionally the evaluator performed the Assurance Activities specified in the collaborative Protection Profile for Network Devices, Version 2.2e (cPP_ND_V2.2e) and PP-Module for Enterprise Session Controller (ESC), Version 1.0 (MOD_ESC_V1.0).

9.1 Evaluation of Security Target

The evaluation team applied each ASE CEM work unit. The ST evaluation ensured the ST contains a description of the environment in terms of policies and assumptions, a statement of security requirements claimed to be met by the Cellcrypt Server that are consistent with the Common Criteria, and product security function descriptions that support the requirements. Additionally the evaluator performed an assessment of the Assurance Activities specified in the collaborative Protection Profile for Network Devices, Version 2.2e (cPP_ND_V2.2e) and PP-Module for Enterprise Session Controller (ESC), Version 1.0 (MOD_ESC_V1.0).

The validator 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 Development Documentation

The evaluation team applied each EAL 1 ADV CEM work unit. The evaluation team assessed the design documentation and found it adequate to aid in understanding how the TSF provides the security functions. The design documentation consists of a functional specification contained in the Security Target's TOE Summary Specification. Additionally the evaluator performed the Assurance Activities specified in the collaborative Protection Profile for Network Devices, Version 2.2e (cPP_ND_V2.2e) and PP-Module for Enterprise Session Controller (ESC), Version 1.0 (MOD_ESC_V1.0) related to the examination of the information contained in the TOE Summary Specification.

The validator 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 Assurance Activities, and that the

conclusion reached by the evaluation team was justified.

9.3 Evaluation of Guidance Documents

The evaluation team applied each EAL 1 AGD CEM work unit. The evaluation team ensured the adequacy of the user guidance in describing how to use the operational TOE. Additionally, the evaluation team ensured the adequacy of the administrator guidance in describing how to securely administer the TOE. The guides were assessed during the design and testing phases of the evaluation to ensure they were complete. Additionally the evaluator performed the Assurance Activities specified in the collaborative Protection Profile for Network Devices, Version 2.2e (cPP_ND_V2.2e) and PP-Module for Enterprise Session Controller (ESC), Version 1.0 (MOD_ESC_V1.0) related to the examination of the information contained in the operational guidance documents.

The validator 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 Assurance Activities, and that the conclusion reached by
the evaluation team was justified.

9.4 Evaluation of Life Cycle Support Activities

The evaluation team applied each EAL 1 ALC CEM work unit. The evaluation team found
that the TOE was identified.

The validator 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 Test Documentation and the Test Activity

The evaluation team applied each EAL 1 ATE CEM work unit. The evaluation team ran the set of tests specified by the Assurance Activities in the collaborative Protection Profile for Network Devices, Version 2.2e (cPP_ND_V2.2e) and PP-Module for Enterprise Session Controller (ESC), Version 1.0 (MOD_ESC_V1.0)and recorded the results in a Test Report, summarized in the Evaluation Technical Report and Assurance Activities Report.

The validator reviewed the work of the evaluation team, and found that sufficient evidence was provided by the evaluation team to show that the evaluation activities addressed the test activities in the collaborative Protection Profile for Network Devices, Version 2.2e (cPP_ND_V2.2e) and PP-Module for Enterprise Session Controller (ESC),

Version 1.0 (MOD_ESC_V1.0), and that the conclusion reached by the evaluation team was justified.

9.6 Vulnerability Assessment Activity

The evaluation team applied each EAL 1 AVA CEM work unit. The evaluation team performed a public search for vulnerabilities, performed vulnerability testing and did not discover any issues with the TOE. The summary of vulnerability assessment and testing can be found in the Assurance Activities Report for Cellcrypt Server Section 7.6.

The validator 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 addressed the vulnerability analysis Assurance Activities in the collaborative Protection Profile for Network Devices, Version 2.2e (cPP_ND_V2.2e) and PP-Module for Enterprise Session Controller (ESC), Version 1.0 (MOD_ESC_V1.0), and that the conclusion reached by the evaluation team was justified.

9.7 Summary of Evaluation Results

The evaluation team's assessment of the evaluation evidence demonstrates that the claims in
the ST are met. Additionally, the evaluation team's test activities 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 performed the Assurance Activities in the collaborative Protection Profile for Network Devices, Version 2.2e (cPP_ND_V2.2e) and PP-Module for Enterprise Session Controller (ESC), Version 1.0 (MOD_ESC_V1.0), 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 guidance documents listed in Section 6. No versions of the TOE and software, either earlier or later were evaluated. Please note that the functionality evaluated is scoped exclusively to the security functional requirements specified in the Security Target. Other functionality included in the product was not assessed as part of this evaluation. Other functionality provided by devices in the operational environment, such as the syslog server, need to be assessed separately and no further conclusions can be drawn about their effectiveness.

11 Annexes

Not applicable.

12 Security Target

Cellcrypt Server Security Target v1.0, 14 June 2022.

13 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 in an unambiguous way that a given implementation is correct with respect to the formal model.
- **Evaluation.** The assessment of an IT product against the Common Criteria using the Common Criteria Evaluation Methodology to determine whether or not the claims made are justified; or the assessment of a protection profile against the Common Criteria using the Common Evaluation Methodology to determine if the Profile is complete, consistent, technically sound and hence suitable for use as a statement of requirements for one or more TOEs that may be evaluated.
- **Evaluation Evidence.** Any tangible resource (information) required from the sponsor or developer by the evaluator to perform one or more evaluation activities.
- **Feature.** Part of a product that is either included with the product or can be ordered separately.
- **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 carried out by the CCEVS Validation Body leading to the issue 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.

14 Bibliography

The Validation Team used the following documents to produce this Validation Report:

1. Common Criteria for Information Technology Security Evaluation - Part 1: Introduction and general model, Version 3.1 Revision 5.
2. Common Criteria for Information Technology Security Evaluation - Part 2: Security functional requirements, Version 3.1 Revision 5.
3. Common Criteria for Information Technology Security Evaluation - Part 3: Security assurance requirements, Version 3.1 Revision 5.
4. Common Evaluation Methodology for Information Technology Security Evaluation, Version 3.1 Revision 5.
5. collaborative Protection Profile for Network Devices, Version 2.2e (cPP_ND_V2.2e)
6. PP-Module for Enterprise Session Controller (ESC), Version 1.0 (MOD_ESC_V1.0)
7. Cellcrypt Server Security Target v1.0, dated June 10, 2022
8. Cellcrypt Server Common Criteria Administrator Guide v0.8.10, dated March 31, 2022
9. Cellcrypt Federal Stack – Installation Manual, dated February 17, 2022
10. Cellcrypt Federal Stack – Maintenance Manual, dated February 17, 2022
11. Cellcrypt Federal Stack – Auditing and Monitoring, dated February 22, 2022
12. Cellcrypt Enterprise Management Portal (EMP) User Manual v1.5, dated May 2020
13. User Guide for the Enterprise Communications Service v1.0.10, dated March 24, 2016
14. Evaluation Technical Report for Cellcrypt Server v0.4, dated June 14, 2022
15. Assurance Activity Report for Cellcrypt Server v0.3, dated June 14, 2022