National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

Validation Report

for

Cellcrypt Android Mobile Client v 5.0

Report Number: CCEVS-VR-VID11599-2025
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
Marybeth Panock
Mike Quintos

The Aerospace Corporation

Common Criteria Testing Laboratory

Allen Sant
Josh Marciante

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 Android Mobile Client 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:

- Protection Profile for Application Software, Version 1.4, 7 October 2021 ([5])
- Functional Packages for Transport Layer Security (TLS), Version 2.0, 19 December 2022 ([6])
- Protection Profile Module for Voice and Video over IP (VVoIP), Version 1.0, 28 October 2020 ([7])

as clarified by all applicable Technical Decisions.

The TOE is Cellcrypt Android Mobile Client v 5.0 (running on Android 14).

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 Android Mobile Client v 5.0
Security Target	Security Target Cellcrypt Android Mobile Client v 5.0, Version 0.5.1, November 26, 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	• Protection Profile for Application Software, Ver. 1.4, 7 October 2021 • PP-Module for Voice and Video over IP (VVoIP), Ver. 1.0, 28 October 2020 • Functional Package for Transport Layer Security (TLS), Ver. 2.0, 19 December 2022
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	Allen Sant Josh Marciante
Validation Personnel	Swapna Katikaneni Marybeth Panock Mike Quintos

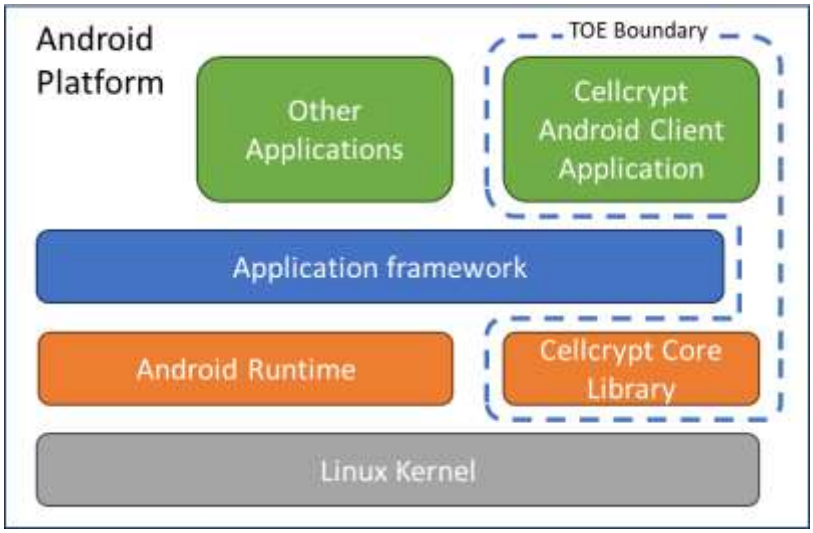
3 TOE Architecture

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

The Cellcrypt Android Mobile Client, the TOE, is a secure multimedia application for Android smartphones. It implements end-to-end encryption and authentication of voice, video, text messages and file attachments between two or more users of Cellcrypt Android Mobile Client and other compatible applications. The Cellcrypt system comprises a handset software application (Cellcrypt Android Mobile Client, i.e. the TOE) and the back-end support infrastructure (Cellcrypt Server). The TOE is the handset software application, Cellcrypt Android Mobile Client, on a specific hardware platform (described in section 8 of this report).

Cellcrypt Android Mobile Client uses standard wireless packet-based connectivity that can be provided by a cellular network or a Wi-Fi data connection.

The Cellcrypt Android Mobile Client application is a software cryptographic application for smartphones. The core function of the TOE is to allow users' voice and video calls to be encrypted with end-to-end security.



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 Cryptographic Support

The TOE implements cryptography to protect data in transit. For data in transit, the TOE implements TLS as a client. The TOE supports TLS connections both with and without mutual authentication. The TOE also implements SRTP to transmit voice and video data.

The TOE implements all cryptography used for these functions using its own implementations of OpenSSL with NIST-approved algorithms. The TOE's DRBG is seeded using entropy from the underlying OS platform.

For data at rest, the TOE relies on its operational environment to control access to stored credential data.

4.2 Communications

The TOE transmits voice and video data using a constant bit rate vocoder.

4.3 User Data Protection

The TOE relies on platform provided credential storage mechanisms to protect sensitive data at rest.

The TOE enforces the media transmission policies for controlling the transmission of voice and video data to a remote peer.

The TOE relies on network connectivity and the credential repository provided by its host OS platform. All uses of network connectivity are user-initiated.

4.4 Identification and Authentication

The TOE supports X.509 certificate validation as part of establishing TLS connections. The TOE implements functionality to support various certificate validity checking methods, including the checking of certificate revocation status using OSCP. If the validity status of a certificate cannot be determined, the certificate will be rejected.

4.5 Security Management

The TOE itself and the configuration settings it uses are stored in locations recommended by the platform vendor. The TOE is launched by the OS user and runs in the session context of that user; there is no interface for a non-administrator to act as an administrator through separate authentication. The TOE's primary management function is to configure the ESC server parameters and set the parameters that are used for the TLS channel (ciphersuites) or the Voice and Video connection channels (vocoder codecs and SRTP parameters).

4.6 Privacy

The TOE does not transmit PII.

4.7 Protection of the TSF

The TOE enforces various mechanisms to protect itself against unauthorized modification and use. The TOE implements address space layout randomization (ASLR), does not allocate any memory with both write and execute permissions, does not write user-modifiable files to directories that contain executable files, is compiled using stack overflow protection, and is compatible with the security features of its host OS platform.

The TOE contains libraries and invokes system APIs that are well-known and explicitly identified.

The TOE has a mechanism to determine its current software version. Software updates to the TOE are acquired through the application's connection to the Controller in the operational environment and subsequently applied using the TOE platform. All updates are digitally signed to guarantee their authenticity and integrity.

4.8 TOE Access

The TOE terminates voice and video connections after the configured inactivity time-period elapses.

4.9 Trusted Path/Channels

The TOE encrypts sensitive data in transit between itself and its operational environment using TLS and SRTP. These interfaces are used to secure all data in transit between the TOE and its operational environment.

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

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 Protection Profile for Application Software, Version 1.4, 7 October 2021 ([5]), Protection Profile Module for Voice and Video over IP (VVoIP), Version 1.0, October 28 2020 ([7]) and Functional Packages for Transport Layer Security (TLS), Version 2.0, December 19, 2022 ([6]) 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 Android Mobile Client v 5.0, Version 0.5.1, November 26, 2025 ([8]). Any functionality not covered by the Protection Profiles is outside the scope of this evaluation.
- The TOE consists solely of software and relies on its operational environment for supporting security functionality, as identified in the ST [8].
- Any capabilities and functionality provided by other devices in the TOE's operational environment are not covered by this evaluation.
- 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.

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 Guidance Cellcrypt Android Mobile Client, Version 0.2.0, June 3, 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 Android Mobile Client v5.0 Common Criteria Test Report and Procedures, Version 1.1, November 26, 2025 ([12])

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

- Assurance Activities Report for Cellcrypt Android Mobile Client v5.0, Version 1.1, 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 Protection Profile for Application Software ([5]), Protection Profile Module for Voice and Video over IP (VVoIP) ([7]) and Functional Packages for Transport Layer Security (TLS) ([6]).

The evaluation team devised a Test Plan based on the Testing Assurance Activities specified in Protection Profile for Application Software, Protection Profile Module for Voice and Video over IP (VVoIP) and Functional Packages for Transport Layer Security (TLS). 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 May 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 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 Protection Profile for Application Software, Protection Profile Module for Voice and Video over IP (VVoIP), and Functional Packages for Transport Layer Security (TLS) were fulfilled.

7.1 Test Configuration

The evaluation team established a test configuration consisting of the TOE (Cellcrypt Android Mobile Client v 5.0) installed on the following device:

- Samsung Galaxy S23 running Android 14.0 on a Qualcomm Snapdragon 8 Gen2 processor

Testing environment:

- TLS Test Server: used for TLS client/server testing and port scanning.
- Revocation Test Server: used for OSCP revocation responses.
- DNS Server: resolve DNS queries.
- Cellcrypt ESC Server: Used to broker voice and video calls with a remote resource.
- Android Phone: A second phone to place and receive calls with.

8 Evaluated Configuration

The TOE consists of the Cellcrypt Android Mobile Client version 5.0 software application, that communicates only with the Cellcrypt Server using TLS 1.2 or TLS 1.3 provided by OpenSSL. The TOE is evaluated on the Android 14 system. The TOE runs on the platform OS as a standalone component.

8.1 TOE Evaluated Configuration

The following prerequisites must apply in the use of the TOE:

- The TOE hardware platforms are:
  - Samsung Galaxy S23 running Android 14.0 on a Qualcomm Snapdragon 8 Gen2 processor with Processor Algorithm Accelerators (PAA).
  - Samsung Galaxy S21 running Android 14.0 on a Qualcomm Snapdragon 888 processor with Processor Algorithm Accelerators (PAA).
- The TOE runs on a NIAP-validated configuration of a mobile platform (including VPN), as defined by the Protection Profile for Mobile Device Fundamentals. The mobile platform is outside the scope of the evaluation.
- ESC Server, as defined by the PP-Module for Enterprise Session Controller (ESC) is outside the scope of this evaluation.
- The TOE operates exclusively within the mobility ecosystem specified by the associated mobility Protection Profiles and will assume that all associated resources (IPSEC VPN tunnel, SIP network) are in place.

The TOE requires the following non-TOE components in its operational environment:

- OCSP responder for use in the verification of X.509 certificates.
- Cellcrypt Server for client authentication and other services e.g. SIP, messaging/attachments and check for updated software.

8.2 Excluded Functionality

In the case of Cellcrypt to Cellcrypt device communication, there is an additional cryptographic layer that is tunnelled through the call for additional security. The presence or functionality of this is outside the scope of the Protection Profiles and therefore is outside the scope of the evaluation.

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 Android Mobile Client v5.0 ([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 Protection Profile for Application Software, Version 1.4, 7 October 2021 ([5]), Protection Profile Module for Voice and Video over IP (VVoIP), Version 1.0, October 28, 2020 ([7]) and Functional Packages for Transport Layer Security (TLS), Version 2.0, December 19, 2022 ([6]). The evaluation determined the TOE satisfies the conformance claims made in the Cellcrypt Android Mobile Client v 5.0 Security Target ([8]), of Part 2 extended and Part 3 extended. The TOE satisfies the requirements specified in:

- Protection Profile for Application Software, Version 1.4, 7 October 2021 ([5]).
- Protection Profile Module for Voice and Video over IP (VVoIP), Version 1.0, October 28, 2020 ([7])
- Functional Packages for Transport Layer Security (TLS), 2.0, December 19, 2022 ([6])

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 Vulnerability Notes Database (https://www.kb.cert.org/vuls/)

The searches were performed on August 8, 2025, updated on September 3, 2025, and on November 5, 2025, using the following search terms:

- CellCrypt
- CellCrypt Android Client
- Android 14
- libSRTP v1.5.4
- OpenSSL v3.5
- Libvphone

- TLS 1.2
- TLS 1.3
- SRTP
- PJSIP
- mp3lame
- SIP
- Crashlytics
- Image Processing Util JNI
- jnidispatch
- tokio
- serde
- request
- rayon
- hyper
- thiserror
- sqlcipher

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 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.

9.7 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 prerequisites identified in the ST and in section 8 of this report, with the TOE configured per the guidance document listed in section 6. The evaluated functionality is scoped exclusively to the security functional requirements specified in the Security Target. Other functionality included in the product, such as the additional cryptographic layer described in section 8.2, were not assessed as part of this evaluation. No other versions of the TOE, either earlier or later, were evaluated.

Additional functionality provided by other non-TOE devices in the operational environment 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 in other sections of this document.

11 Security Target

The ST for this product's evaluation is Cellcrypt Android Mobile Client v 5.0 Security Target, Version 0.5.1, November 26, 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 for Information Technology Security Evaluation: Part 1: Introduction and general model, Version 3.1, Revision 5, April 2017.

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

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

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

[5] Protection Profile for Application Software, Version 1.4, October 7, 2021.

[6] Functional Packages for Transport Layer Security (TLS), Version 2.0, December 19, 2022.

[7] Protection Profile Module for Voice and Video over IP (VVoIP), Version 1.0, October 28, 2020

[8] Security Target Cellcrypt Android Mobile Client v 5.0, Version 0.5.1, November 26, 2025.

[9] Common Criteria Guidance Cellcrypt Android Mobile Client, Version 0.2.0, June 3, 2025.

[10] Evaluation Technical Report for Cellcrypt Android Mobile Client v5.0 (Proprietary), Version 1.1, November 26, 2025.

[11] Assurance Activities Report for Cellcrypt Android Mobile Client v5.0, Version 1.1, November 26, 2025.

[12] Cellcrypt Android Mobile Client v5.0 Common Criteria Test Report and Procedures, Version 1.1, November 26, 2025.

[13] Cellcrypt Android Mobile Client v5.0 Vulnerability Analysis, Version 1.1, November 26, 2025.