National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

Validation Report

for the

Cellcrypt Android Mobile Client version 4.40

Report Number: CCEVS-VR-11278-2022

Dated: 9/19/2022

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 George G. Meade, MD 20755-6982

ACKNOWLEDGEMENTS

Validation Team

DeRon Graves
Swapna Katikaneni
Jerome Myers

Common Criteria Testing Laboratory

Siddhant Kasley

Rupendra Kadtan

Rahul Joshi

Kenneth Lasoski

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 Android Mobile Client version 4.40 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 September 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 Protection Profile for Application Software Version 1.3, 2019-03-01 (AppPP), PP-Module for Voice/Video over IP (VVoIP) Endpoints Version 1.0, 2020-10-28 (MOD_VVoIP), Functional Package for Transport Layer Security (TLS) Version 1.1, 2019-03-01 (TLS-PKG).

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 Protection Profile for Application Software Version 1.3, 2019-03-01 (AppPP), PP-Module for Voice/Video over IP (VVoIP) Endpoints Version 1.0, 2020-10-28 (MOD_VVoIP), Functional Package for Transport Layer Security (TLS) Version 1.1, 2019-03-01 (TLS-PKG). 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 Common Evaluation Methodology (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 Android Mobile Client version 4.40
Protection Profile	Protection Profile for Application Software Version 1.3, 2019-03-01 (AppPP), PP-Module for Voice/Video over IP (VVoIP) Endpoints Version 1.0, 2020-10-28 (MOD_VVoIP), Functional Package for Transport Layer Security (TLS) Version 1.1, 2019-03-01 (TLS-PKG)
Security Target	Cellcrypt Android Mobile Client version 4.40 Security Target, Version 1.2.4, 2022-09-19
Evaluation Technical Report	Evaluation Technical Report for Cellcrypt Android Mobile Client version 4.40, Version 1.3, 2022-09-19
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	DeRon Graves Swapna Katikaneni Jerome Myers

3 Architectural Information

Product Description:

Cellcrypt Android Mobile Client 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 below).

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

Mutually authenticated connection set-up ensures that only mobile phones on which the TOE runs can participate in secure sessions with the Cellcrypt Server, and that the users of the TOE can be assured to always connect to a legitimate Cellcrypt server. End-to-end encryption is achieved through the creation and use of session-unique encryption/decryption keys used by the TOE to encrypt and decrypt voice traffic, messages, and attachments. Long-term static keys and other sensitive user data are stored by the TOE in an encrypted database (SQLCipher) with the SQLCipher master key being protected by the operating system.

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

- The Android mobile platform is the Samsung Galaxy S20 running Android 11.0 on a Qualcomm Snapdragon 865 ARMv8 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 non-TOE components required by the TOE are the following:
- CRL or OCSP server 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.

Physical Scope:

The Target of Evaluation (TOE) is the Cellcrypt Android Mobile Client application (Figure 1), which runs on Android 11. 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.

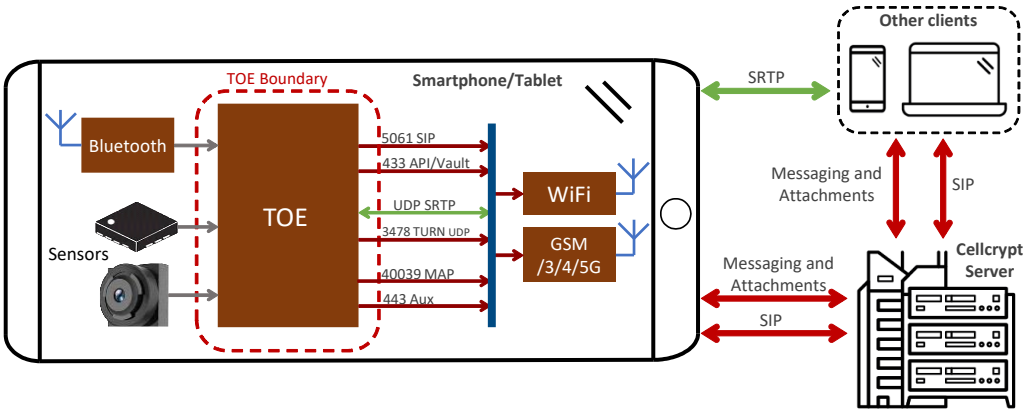

Figure 1 TOE Boundary

The physical scope of the TOE comprises of the following:

- The TOE Software, i.e. the Cellcrypt Android Mobile Client version 4.40.
- TOE Security Guidance: Common Criteria Guidance - Cellcrypt Android Mobile Client, AG-FED-MCL-And-1, Version 1.1.2, Sep, 19 2022.

4 Security Policy

The logical scope of the TOE comprises of the following:

- Authenticated call set-up with the Cellcrypt Server.
- End-to-end encryption of secure voice and video traffic.
- Security management functions restricted to authorized personnel.
- Protection measures for ensuring the integrity and authenticity of the TOE.

The TOE uses X.509 Certificates for mutual authentication on the trusted channel between itself and the Cellcrypt Server. The validity of the X.509 certificates is checked by querying a CRL or an OCSP responder. The TOE uses TLSv1.2 protocol to protect all communications between itself and the Cellcrypt Server from modification and disclosure. In addition to the X.509 Certificate authentication, the TOE also authenticates the user to the Cellcrypt Server using a password. The TOE does not store the authentication password but requests the user to enter it each time it is required.

The TOE achieves end-to-end encryption using an SDES-SRTP trusted channel. The keys for the SDES-SRTP trusted channel are protected by the TLS/SIP channel during key establishment.

The TOE mitigates side channel attacks by utilizing a fixed rate vocoder. This prevents an attacker from inferring information about the audio from the bitrate being transmitted. The TOE also enables ASLR and stack-based overflow protections.

All TOE cryptography is performed by the Cellcrypt CCoreV4 FIPS 140-2 validated crypto module. CAVP Certificate references are given in Table 1. 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.

Table 1 CAVP Certificate References

Algorithms	Options	Certificates
AES (FIPS 197)	Modes: CTR, CBC, GCM (SP 800-38D) Key lengths: 128, 256 bits	CAVP: A1999
SHA-1 (FIPS 180-4)	Hash lengths: 160 bits	CAVP: A1999
SHA2 (FIPS 180-4)	Hash lengths: 256, 384, 512 bits	CAVP: A1999
HMAC (FIPS 198)	Hash lengths: 160, 256, 384, 512 bits	CAVP: A1999
RSA (FIPS 186-4)	KeyGen, SigGen, SigVer Key length: 2048 bits	CAVP: A1999
DH	KeyExch Key Length: 2048 bits	CAVP: A1999
KAS-ECC (SP 800-56Ar1)	KeyExch	CAVP: A1999

Algorithms	Options	Certificates
	Curves: P-256, P-384	
ECDSA (FIPS 186-4)	KeyGen, SigGen, SigVer Curves P-256, P-384	CAVP: A1999

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:

- Protection Profile for Application Software Version 1.3, 2019-03-01 (AppPP)
- PP-Module for Voice/Video over IP (VVoIP) Endpoints Version 1.0, 2020-10-28 (MOD_VVoIP)
- Functional Package for Transport Layer Security (TLS) Version 1.1, 2019-03-01 (TLS-PKG)

5.2 Threats

The following table 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 drawn from:

- Protection Profile for Application Software Version 1.3, 2019-03-01 (AppPP)
- PP-Module for Voice/Video over IP (VVoIP) Endpoints Version 1.0, 2020-10-28 (MOD_VVoIP)
- Functional Package for Transport Layer Security (TLS) Version 1.1, 2019-03-01 (TLS-PKG)

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 Protection Profile for Application Software Version 1.3, 2019-03-01 (AppPP), PP-Module for Voice/Video over IP (VVoIP) Endpoints Version 1.0, 2020-10-28 (MOD_VVoIP), Functional Package for Transport Layer Security (TLS) Version 1.1, 2019-03-01 (TLS-PKG).
- 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.
- 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.

6 Documentation

The following documents were provided by the vendor with the TOE for evaluation:

- Cellcrypt Android Mobile Client Common Criteria Guidance v1.1.2 dated September 19, 2022 [AGD]

Any additional customer documentation provided with the product, or that is available online was not included in the scope of the evaluation and therefore should not be relied upon when configuring or operating the device as evaluated. . Consumers are encouraged to download the evaluated administrative guidance documentation from the NIAP website.

7 TOE Evaluated Configuration

7.1 Evaluated Configuration

- 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 below).
- Cellcrypt Android Mobile Client version 4.40 uses standard wireless packet-based connectivity that can be provided by a cellular network or a Wi-Fi data connection.
- The Android mobile platform is the Samsung Galaxy S20 running Android 11.0 on a Qualcomm Snapdragon 865 ARMv8 processor with Algorithm Accelerators (PAA).

7.2 Excluded Functionality

- The Cellcrypt Android Mobile Client 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.

8 IT Product Testing

This section describes the testing efforts of the developer and the evaluation team. It is derived from information contained in ETR for the TOE, which is not publicly available. The AAR provides an overview of testing and the prescribed assurance activities.

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 Protection Profile for Application Software Version 1.3, 2019-03-01 (AppPP), PP-Module for Voice/Video over IP (VVoIP) Endpoints Version 1.0, 2020-10-28 (MOD_VVoIP), Functional Package for Transport Layer Security (TLS) Version 1.1, 2019-03-01 (TLS-PKG). The Independent Testing activity is documented in section 3.1 of the AAR, 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 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 TOE Name to be Part 2 extended, and meets the SARs contained in the PP. Additionally, the evaluator performed the Assurance Activities specified in the claimed PP.

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 TOE 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 Protection Profile for Application Software Version 1.3, 2019-03-01 (AppPP), PP-Module for Voice/Video over IP (VVoIP) Endpoints Version 1.0, 2020-10-28 (MOD_VVoIP), Functional Package for Transport Layer Security (TLS) Version 1.1, 2019-03-01 (TLS-PKG).

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 ST's TOE Summary Specification. Additionally, the evaluator performed the Assurance Activities specified in the Protection Profile for Application Software Version 1.3, 2019-03-01 (AppPP), PP-Module for Voice/Video over IP (VVoIP) Endpoints Version 1.0, 2020-10-28 (MOD_VVoIP), Functional Package for Transport Layer Security (TLS) Version 1.1, 2019-03-01 (TLS-PKG) 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 Protection Profile for Application Software Version 1.3, 2019-03-01 (AppPP), PP-Module for Voice/Video over IP (VVoIP) Endpoints Version 1.0, 2020-10-28 (MOD_VVoIP), Functional Package for Transport Layer Security (TLS) Version 1.1, 2019-03-01 (TLS-PKG) 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 Protection Profile for Application Software Version 1.3, 2019-03-01 (AppPP), PP-Module for Voice/Video over IP (VVoIP) Endpoints Version 1.0, 2020-10-28 (MOD_VVoIP), Functional Package for Transport Layer Security (TLS) Version 1.1, 2019-03-01 (TLS-PKG) and recorded the results in a Test Report, summarized in the ETR and AAR.

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 Protection Profile for Application Software Version 1.3, 2019-03-01 (AppPP), PP-Module for Voice/Video over IP (VVoIP) Endpoints Version 1.0, 2020-10-28 (MOD_VVoIP), Functional Package for Transport Layer Security (TLS) Version 1.1, 2019-03-01 (TLS-PKG), 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 evaluator documented their analysis and testing of potential vulnerabilities in section 6.4.1 of the AAR.

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 Protection Profile for Application Software Version 1.3, 2019-03-01 (AppPP), PP-Module for Voice/Video over IP (VVoIP) Endpoints Version 1.0, 2020-10-28 (MOD_VVoIP), Functional Package for Transport Layer Security (TLS) Version 1.1, 2019-03-01 (TLS-PKG), 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 Protection Profile for Application Software Version 1.3, 2019-03-01 (AppPP), PP-Module for Voice/Video over IP (VVoIP) Endpoints Version 1.0, 2020-10-28 (MOD_VVoIP), Functional Package for Transport Layer Security (TLS) Version 1.1, 2019-03-01 (TLS-PKG), 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.

Please note that the functionality evaluated is scoped exclusively to the security functional requirements specified in the Security Target. The excluded functionality is specified in section 7.2 of this report. All other items and scope issues have been sufficiently addressed elsewhere in this document.

11 Annexes

Not applicable.

12 Security Target

Cellcrypt Android Mobile Client version 4.40, Version 1.2.4

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. Assurance Activity Report for Cellcrypt Android Mobile Client version 4.40 Version 1.2, 2022-09-19
2. Common Criteria for Information Technology Security Evaluation - Part 1: Introduction and general model, Version 3.1 Revision 5.
3. Common Criteria for Information Technology Security Evaluation - Part 2: Security functional requirements, Version 3.1 Revision 5.
4. Common Criteria for Information Technology Security Evaluation - Part 3: Security assurance requirements, Version 3.1 Revision 5.
5. Common Evaluation Methodology for Information Technology Security Evaluation, Version 3.1 Revision 5.
6. Evaluation Technical Report for Cellcrypt Android Mobile Client version 4.40 Version 1.3, 2022-09-19
7. Cellcrypt Android Mobile Client Common Criteria Guidance Version 1.1.2, 2022-09-19
8. Protection Profile for Application Software Version 1.3, 2019-03-01 (AppPP)
9. PP-Module for Voice/Video over IP (VVoIP) Endpoints Version 1.0, 2020-10-28 (MOD_VVoIP)
10. Functional Package for Transport Layer Security (TLS) Version 1.1, 2019-03-01 (TLS-PKG)
11. Cellcrypt Android Mobile Client version 4.40 Security Target Version 1.2.4, 2022-09-19