National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

TM

Validation Report

for the

Cellcrypt Classified 2

Report Number:	**CCEVS-VR-VID10929**
Dated:	**22 April 2019**
Version:	**1.0**

National Institute of Standards and Technology
Information Technology Laboratory
100 Bureau Drive
Gaithersburg, MD 20899

National Security Agency
Information Assurance Directorate
9800 Savage Road STE 6940
Fort George G. Meade, MD 20755-6940

ACKNOWLEDGEMENTS

Validation Team

Jim Donndelinger

Ken Elliott

Ken Stutterheim

The Aerospace Corporation

Common Criteria Testing Laboratory

Danielle F Canoles

Kenji Yoshino

Rutwij Kulkarni

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 Classified 2 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 2019. The information in this report is largely derived from the proprietary Evaluation Technical Report (ETR) and associated test report, all written by Acumen Security as summarized in the Cellcrypt Classified 2 Assurance Activity Report. The evaluation determined that the product is both Common Criteria Part 2 Extended and Part 3 Conformant, and meets the assurance requirements defined in the Protection Profile for Application Software Version 1.2 [App] and Extended Package for Voice and Video over IP VVoIP Version 1.0 [VVoIP].

The Target of Evaluation (TOE) identified in this Validation Report has been evaluated at a NIAP approved Common Criteria Testing Laboratory using the Common Methodology for IT Security Evaluation (Version 3.1, Rev. 4) for conformance to the Common Criteria for IT Security Evaluation (Version 3.1, Rev. 4), as interpreted by the Assurance Activities contained in the Protection Profile for Application Software Version 1.2 [App] and Extended Package for Voice and Video over IP VVoIP Version 1.0 [VVoIP] and all applicable NIAP technical decisions for the technology. This Validation Report 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 evaluation technical report 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 Security Target (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 evaluation technical report are consistent with the evidence produced.

2 Identification

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards 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 Protection Profile containing Assurance Activities, which are interpretation 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 information technology 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 Compliance List.

The target of evaluation is the Cellcrypt Classified 2 and the associated TOE guidance documentation.

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 - Identification

Item	Identifier
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
TOE	Cellcrypt Classified 2
Protection Profile	Protection Profile for Application Software Version 1.2 [App] and Extended Package for Voice and Video over IP VVoIP Version 1.0 [VVoIP]
Security Target	Cellcrypt Classified 2 Security Target Version 1.1
Evaluation Technical Report	VID10929 Assurance Activity Report, version 1.2
CC Version	Version 3.1, Revision 4
Conformance Result	CC Part 2 Extended and CC Part 3 Extended
Sponsor	Cellcrypt Inc.
Developer	Cellcrypt Inc.
Common Criteria Testing Lab (CCTL)	Acumen Security, LLC
CCEVS Validators	Jim Donndelinger Ken Elliott Ken Stutterheim

3 Architectural Information

The Target of Evaluation (TOE) is the Cellcrypt Classified 2 version 2.10.0 smartphone application, which will run on an Android 7 based platform. The Cellcrypt Classified 2 application is a software cryptographic application for smartphones, which enables users to have secure voice calls on an end-to-end encrypted session.

4 Security Policy

The logical scope of the TOE comprises:

- Authenticated connection set-up with a SIP server
- End-to-end encryption used by the TOE when encrypting/decrypting secure voice traffic

The TOE utilizes X.509 Certificates to provide a mutual authentication for the trusted channel with the SIP server. The validity of the X.509 certificates is checked by querying a CRL. The TOE uses the TLSv1.2 protocol to protect all communications with the SIP server from modification and disclosure. In addition to the X.509 Certificate authentication, the TOE authenticates to the SIP server using a password as an additional layer of security. The TOE does not store the password and requires the user to enter the password whenever the TOE requires it.

The TOE achieves end-to-end encryption using SDES-SRTP trusted channel. The keys for the SDES-SRTP trusted channel are protected by the TLS/SIP channel while the keys are being established.

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

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.

Table 2 – Assumptions

Assumption	Description
A.PLATFORM	The TOE relies upon a trustworthy computing platform for its execution. This includes the underlying platform and whatever runtime environment it provides to the TOE.
A.PROPER_USER	The user of the application software is not willfully negligent or hostile, and uses the software in compliance with the applied enterprise security policy.
A.PROPER_ADMIN	The administrator of the application software is not careless, willfully negligent or hostile, and administers the software within compliance of the applied enterprise security policy.

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.

Table 3 - Threats

Threat	Description
T.NETWORK_ACCESS	An attacker is positioned on a communications channel or elsewhere on the network infrastructure. Attackers may engage in communications with the application software or alter communications between the application software and other endpoints in order to compromise it.
T.NETWORK_EAVSDROP	An attacker is positioned on a communications channel or elsewhere on the network infrastructure. Attackers may monitor and gain access to data exchanged between the application and other endpoints.
T.LOCAL_ATTACK	An attacker can act through unprivileged software on the same computing platform on which the application executes. Attackers may provide maliciously formatted input to the application in the form of files or other local communications.
T.PHYSICAL_ACCESS	An attacker may try to access sensitive data at rest.
T.UNDETECTED_TRANSMISSION	An attacker may cause the TOE to exfiltrate audio and/or video media over a remote channel while in a state where the user has a reasonable expectation that no media is being transmitted.

Threat	Description
T.CLOCK_DESYNC	An attacker may cause the TOE to use incorrect clock data, resulting in a denial of service from causing encryption and/or authentication connection failures.
T.MEDIA_DISCLOSURE	An attacker can use the encrypted variable rate vocoder frames to their advantage to decode transmitted data.

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 1.2 [App] and Extended Package for Voice and Video over IP VVoIP Version 1.0 [VVoIP].
- Consistent with the expectations of the Protection Profile, 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 PP and applicable Technical Decisions. Any additional security related functional capabilities that may be included in the product were not covered by this evaluation.

6 Documentation

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

- Cellcrypt Classified 2 Security Target, Version 1.1 [ST]
- Administrative Guidance Document - Cellcrypt Classified 2, version 1.2 [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 to be relied upon when configuring or operating the device as evaluated.

7 TOE Evaluated Configuration

7.1 Evaluated Configuration

The Target of Evaluation (TOE) is the Cellcrypt Classified version 2.10.0 smartphone application, which will run on an Android 7 based platform. The Cellcrypt Classified version 2.10.0 application is a software cryptographic application for smartphones, which enables users to have secure voice calls on an end-to-end encrypted session.

The logical scope of the TOE comprises:

- Authenticated connection set-up with a SIP server
- End-to-end encryption used by the TOE when encrypting/decrypting secure voice traffic

The TOE utilizes X.509 Certificates to provide a mutual authentication for the trusted channel with the SIP server. The validity of the X.509 certificates is checked by querying a CRL. The TOE uses the TLSv1.2 protocol to protect all communications with the SIP server from modification and disclosure. In addition to the X.509 Certificate authentication, the TOE authenticates to the SIP server using a password as an additional layer of security. The TOE does not store the password and requires the user to enter the password whenever the TOE requires it.

The TOE achieves end-to-end encryption using SDES-SRTP trusted channel. The keys for the SDES-SRTP trusted channel are protected by the TLS/SIP channel while the keys are being established.

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

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 the Cellcrypt Classified 2, which is not publicly available. The Assurance Activities Report 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 the vendor-provided guidance documentation and ran the tests specified in the Protection Profile for Application Software Version 1.2 [App] and Extended Package for Voice and Video over IP VVoIP Version 1.0 [VVoIP]. The Independent Testing activity is documented in the Assurance Activities Report, which is publicly available, and is not duplicated here. Multiple test beds were constructed to exercise Application Software capabilities and claimed security functionality. The following tooling was used as part of the test activities,

- Android Studio
- GHIDRA
- JADX
- Nmap
- Wireshark
- Peer VoIP Endpoint
- Acumen TLS
- ESC (OpenSSL/OpenSIPS)
- CRL server

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) and as summarized in the Cellcrypt Classified 2 Assurance Activity Report, Version 1.2. The reader of this document can assume that 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 4 and CEM version 3.1 rev 4. The evaluation determined the Cellcrypt Classified 2 to be Part 2 extended, and meets the SARs contained in the PP. Additionally the evaluator performed the Assurance Activities specified in the [App] and [VVoIP].

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 Classified 2 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 1.2 [App] and Extended Package for Voice and Video over IP VVoIP Version 1.0 [VVoIP].

The validators 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 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 [App] and [VVoIP] related to the examination of the information contained in the TOE Summary Specification.

The validators 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 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 [App] and [VVoIP] related to the examination of the information

contained in the operational guidance documents.

The validators 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 found that the TOE was identified. Additionally, the team verified that both the TOE and its supporting documentation are consistently reference the same version and use the same nomenclature. The evaluation team also verified that the vendor website identified the TOE version accurately.

The validators 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 ran the set of tests specified by the Assurance Activities in the [App] and [VVoIP] and recorded the results in a Test Report, summarized in the Evaluation Technical Report and Assurance Activities Report.

The validators 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 [App] and [VVoIP], and that the conclusion reached by the evaluation team was justified.

9.6 Vulnerability Assessment Activity

The evaluation team performed a public search for vulnerabilities on March 22, 2019 and did not discover any issues with the TOE. The following sources of public vulnerability information were searched:

- https://www.cvedetails.com/

The search terms used included:

- Cellcrypt
- OpenSSL 2.0.10
- PJSIP 2.1
- libSRTP v1.5.4

The evaluation team also performed a general Google search for “cellcrypt vulnerabilities” on April 12, 2019 and did not discover any vulnerabilities.

The validators 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 [App] and [VVoIP], 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 [App] and [VVoIP], and correctly verified that the product meets the claims in the ST.

10 Validator Comments & Recommendations

The Validation Team has no additional comments or recommendations.

11 Annexes

Not applicable.

12 Security Target

Please see the Cellcrypt Classified 2 Security Target, Version 1.1 [ST].

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 4.
2. Common Criteria for Information Technology Security Evaluation - Part 2: Security functional requirements, Version 3.1 Revision 4.
3. Common Criteria for Information Technology Security Evaluation - Part 3: Security assurance requirements, Version 3.1 Revision 4.
4. Common Evaluation Methodology for Information Technology Security Evaluation, Version 3.1 Revision 4.
5. Cellcrypt Classified 2 Security Target, Version 1.1 [ST]
6. Administrative Guidance Document - Cellcrypt Classified 2, version 1.2 [AGD]
7. Protection Profile for Application Software Version 1.2 [App]
8. Extended Package for Voice and Video over IP VVoIP Version 1.0 [VVoIP]
9. Cellcrypt Classified 2 Assurance Activity Report