National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme
Validation Report

Security Requirements for Voice Over IP Application

Protection Profile for Mobility – Voice Over IP Application, Version 0.6

Report Number:	**CCEVS-VR-PP-0005**
Dated:	**May 20, 2014**
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

Table of Contents

1 Executive Summary

This report documents the assessment of the National Information Assurance Partnership (NIAP) validation team of the evaluation of the *Security Requirements for Voice Over IP Application Protection Profile for Mobility – Voice Over IP Application*, *Version 0.6, 2013-01-28*. It presents a summary of the Voice Over Internet Protocol (VOIP) PP and the evaluation results.

In order to promote thoroughness and efficiency, the evaluation of the VOIP PP was performed concurrent with the first product evaluation against the PP's requirements. In this case the Target of Evaluation (TOE) was the Cellcrypt Mobile for Secret client version 1.0 provided by Cellcrypt Inc. The evaluation was performed by the *CygnaCom Solutions* Common Criteria Testing Laboratory (CCTL) in McLean, Virginia, United States of America, and was completed in April 2014.

The information in this report is largely derived from the Evaluation Technical Reports (ETRs), written by the CCTL listed above.

The evaluation determined that the VOIP PP is both **Common Criteria Part 2 Extended and Part 3 Conformant**. The PP 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 3) for conformance to the Common Criteria for IT Security Evaluation (Version 3.1, Rev 3). Because the ST contains only material drawn directly from the VOIP PP, performance of the majority of the ASE work units serves to satisfy the APE work units as well. Where this is not the case, the lab performed the outlying APE work units as part of this evaluation.

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 found that the evaluation showed that the VOIP PP meets the requirements of the APE components. 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.

In order to promote thoroughness and efficiency, the evaluation of the VOIP PP was performed concurrent with the first product evaluation against the PP. In this case the TOE for this first product was the *Cellcrypt Mobile for Secret client version 1.0* provided by Cellcrypt Inc. The evaluation was performed by the CygnaCom Solutions Common

Criteria Testing Laboratory (CCTL) in McLean, Virginia, United States of America, and was completed in April 2014.

The VOIP PP contains a set of “base” requirements that all conformant STs must include, and in addition contain a set of “optional” requirements that may be included based on the selections made in the base requirements and the capabilities of the TOE. Because the optional requirements do not have to be included in a particular ST, the initial use of the PP will address (in terms of the PP evaluation) the base requirements as well as any optional requirements that are incorporated into the initial ST. Tables 5 and 6 below list the actual requirements covered in the evaluation. Subsequently, TOEs that are evaluated against the VOIP PP that incorporate optional requirements that have not been included in any ST prior to that will be used to evaluate those requirements (APE_REQ), and the appropriate updates to this validation report will be made.

The following identifies the PP subject to the evaluation/validation, as well as the supporting information from the base evaluation performed against this PP, as well as subsequent evaluations that address additional optional requirements in the VOIP PP.

Protection Profile	*Security Requirements for Voice Over IP Application Protection Profile for Mobility – Voice Over IP Application, Version 0.6, January 28, 2013.*
ST	*Cellcrypt Mobile for Secret client version 1.0 Security Target*, Version 3.2, April 14, 2014
Evaluation Technical Report	*Evaluation Technical Report for Cellcrypt Mobile for Secret client Version 1.0, Volumes 1 & 2: Evaluation of the ST Security Target*, Version 3.0, March 10, 2014
CC Version	Common Criteria for Information Technology Security Evaluation, Version 3.1, rev 3
Conformance Result	CC Part 2 extended, CC Part 3 conformant
CCTL	CygnaCom Solutions Common Criteria Testing Laboratory (CCTL) in McLean, Virginia, United States of America
CCEVS Validators	Bradford O’Neill and Dr. Patrick Mallett, The MITRE Corporation

3 VOIP PP Description

The PP provides a minimal, baseline set of requirements that are targeted at mitigating well defined and described threats for VOIP applications. The PP describes the features of a compliant Target of Evaluation (TOE).

The VoIP application in the context of this PP is part of the cell phone workspace that the enterprise can install for use by the phone user. The VoIP infrastructure for an enterprise can vary greatly, both in size and complexity. Many kinds of functionality are possible, often desirable, and sometimes necessary – including Session Border Controllers (SBC), gateways, trunking, and Network Address Translation (NAT) and firewall traversal. The VoIP application is considered to be a VoIP client that interacts with a Session Initiation Protocol (SIP) Server which provides registrar and proxy capabilities required for call-session management via SIP requests and responses to establish, process, and terminate

VoIP calls. The VoIP application will interact with a peer application using the Security Real-Time Transport Protocol (SRTP) that has been established using the Session Description Protocol (SDP) and the Security Descriptions for Media Streams (SDES) for SDP.

Compliant TOEs will provide security functionality that addresses threats to the TOE. They must also protect the communications between itself and another VoIP client (i.e., cell phone) by using a SDES-SRTP-protected channel. Likewise, compliant TOEs must also protect communications between itself and the SIP Server by using a Transport Layer Security (TLS)- and (optionally) a Datagram Transport Layer Security (DTLS)-protected signaling channel. To register the TOE within the domain, the TOE is required to be password authenticated by the SIP Server. The TOE is required by this PP to make use of certificates to authenticate the both the SIP server end and the TOE itself through the TLS connection. The TOE must provide the ability to report its version to the Enterprise so that a determination as to whether it can be updated can be made.

4 Security Problem Description and Objectives

4.1 Assumptions

The specific conditions listed in the following subsections are assumed to exist in the TOE's Operational 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 1: TOE Assumptions

Assumption Name	Assumption Definition
A.AUTHORIZED_USER	The cell phone user will follow all provided user guidance. An authorized user is not considered hostile or malicious.
A.AVAILABILITY	Network resources shall be available to allow VoIP clients to satisfy mission requirements and to transmit information.
A.OPER_ENV	The operational environment of the TOE appropriately addresses those requirements, threats, and policies not applicable to the TOE itself, but that are necessary to support the correct operation of the TOE.
A.TRUSTED_ADMIN	TOE Administrators are trusted to follow and apply all administrator guidance in a trusted manner.

4.2 Threats

Table 2: Threats

Threat Name	Threat Definition
T.UNAUTHORIZED_ACCESS	A user may gain unauthorized access to the TOE data and TOE executable code. A malicious user, process, or external IT entity may masquerade as an authorized entity in order to gain unauthorized access to data or TOE resources. A malicious user, process, or external

Threat Name	Threat Definition
	IT entity may misrepresent itself as the TOE to obtain identification and authentication data.
T.UNAUTHORIZED_UPDATE	A malicious party attempts to supply the end user with an update to the product that may compromise the security features of the TOE.

4.3 Security Objectives for the TOE

Table 3: Security Objectives for the TOE

TOE Security Obj.	TOE Security Objective Definition
O.PROTECTED_COMMUNICATIONS	The TOE will provide protected communication channels for administrators, other parts of a distributed TOE, and authorized IT entities.
O.TRUSTED_UPDATES	The TOE will provide the capability to report its current version.

The following table contains objectives for the Operational Environment.

Table 4: Security Objectives for the Operational Environment

TOE Security Obj.	TOE Security Objective Definition
OE.AUTHORIZED_USER	The cell phone user of the TOE is non-hostile and follows all user guidance.
OE.AVAILABILITY	Network resources will be available to allow VoIP clients to satisfy mission requirements and to transmit information
OE.OPER_ENV	The operational environment will provide a SIP infrastructure to establish a VoIP connection; a PKI to provide certificates; and an execution domain to support correct operation of the TOE.
OE.TRUSTED_ADMIN	TOE Administrators are trusted to follow and apply all administrator guidance in a trusted manner.
OE.VERIFIABLE_UPDATES	The Enterprise will provide the capability to update the TOE after that it has determine such an update is necessary.

5 Requirements

This section identifies the Security Functional and Assurance Requirements that were validated as part of the CellCrypt Application evaluation activity referenced above.

Table 5: Functional Requirements Summary

Requirement Class	Requirement Component
FCS: Cryptographic support	FCS_COP.1(1): Cryptographic Operation (Encryption/Decryption)
	FCS_COP.1(2): Cryptographic Operation (Signature Verification)
	FCS_COP.1(3): Cryptographic Operation (Cryptographic Hashing)
	FCS_COP.1(4): Cryptographic Operation (for keyed-hash Message Authentication)
	FCS_RBG_EXT.1: Cryptographic operation (Random Bit Generation)
	FCS_SRTP_EXT.1: Secure Real-Time Transport Protocol (SRTP)
	FCS_TLS_EXT.1: Transport Level Security
FIA: Identification and authentication	FIA_SIPC_EXT.1: Session Initiation Protocol (SIP) Client
	FIA_X509_EXT.1 X.509 Certificates
FPT: Protection of the TOE security functions	FPT_TUD_EXT.1 Extended: Trusted Update
FTP: Trusted Path/Channel	FTP_ITC.1(1) Inter-TSF Trusted Channel (SDES-SRTP)
	FTP_ITC.1(2) Inter-TSF Trusted Channel (TLS/SIP)

The following are the assurance requirements contained in the VOIP PP:

Table 6: Assurance Requirements Summary

Requirement Class	Requirement Component
ADV: Development	ADV_FSP.1 Basic functional specification
AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
ALC: Life-cycle support	ALC_CMC.1 Labelling of the TOE
	ALC_CMS.1 TOE CM coverage
ATE: Tests	ATE_IND.1 Independent testing - conformance
AVA: Vulnerability assessment	AVA_VAN.1 Vulnerability survey

6 Results of the Evaluation

The overall results of the TOE evaluation are summarized in Table 7-1: Summary of Results of Evaluation as verdicts for each evaluator activity and assurance component. The subsections below provide detailed evaluation results corresponding to these tables.

Table 7: Summary of Results of Evaluation

Class	Component	Action Element	Verdict
ADV			**Pass**
	ADV_FSP.1		
		ADV_FSP.1.1E	
		ADV_FSP.1.2E	
AGD			**Pass**
	AGD_OPE.1		
		AGD_OPE.1.1E	
	AGD_PRE.1		
		AGD_PRE.1.1E	
		AGD_PRE.1.2E	
ALC			**Pass**
	ALC_CMC.1		
		ALC_CMC.1.1E	
	ALC_CMS.1		
		ALC_CMS.1.1E	
ATE			**Pass**
	ATE_IND.1		
		ATE_IND.1.1E	
		ATE_IND.1.2E	
AVA			**Pass**
	AVA_VAN.1		
		AVA_VAN.1.1E	
		AVA_VAN.1.2E	
		AVA_VAN.1.3E	

7 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 as interpreted by the supplemental guidance in the VOIP PP Assurance Activities to determine whether or not the claims made are justified.
- **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.

8 Bibliography

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

[1] Common Criteria Project Sponsoring Organisations. *Common Criteria for Information Technology Security Evaluation: Part 1: Introduction and General Model*, Version 3.1, Revision 2, dated: September 2007.

[2] Common Criteria Project Sponsoring Organisations. *Common Criteria for Information Technology Security Evaluation: Part 2: Security Functional Requirements*, Version 3.1, Revision 2, dated: September 2007.

[3] Common Criteria Project Sponsoring Organisations. *Common Criteria for Information Technology Security Evaluation: Part 3: Security Assurance Requirements*, Version 3.1, Revision 2, dated: September 2007

[4] Common Criteria Project Sponsoring Organisations. *Common Evaluation Methodology for Information Technology Security* – Part 2: Evaluation Methodology, Version 3.1, Revision 2, dated: September 2007.

[5] Common Criteria, Evaluation and Validation Scheme for Information Technology Security, *Guidance to Validators of IT Security Evaluations*, Scheme Publication #3, Version 1.0, January 2002.

[6] Evaluation Technical Report for Cellcrypt Mobile for Secret client Version 1.0, Volumes 1 & 2: Evaluation of the ST Security Target, Version 3.0, March 10, 2014

[7] *Cellcrypt Mobile for Secret client version 1.0 Security Target,* Version 3.2, April 14, 2014

[8] *Security Requirements for Voice Over IP Application Protection Profile for Mobility – Voice Over IP Application, Version 0.6, January, 28, 2013.*