National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme Validation Report

Cellcrypt Mobile for Secret Client Version 1.0

Report Number:	**CCEVS-VR-VID10535-2014**
Dated:	**April, 14, 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

ACKNOWLEDGEMENTS

Validation Team

Dr. Patrick Mallett

The MITRE Corporation

McLean, VA

Bradford O'Neill

The MITRE Corporation

Bedford, MA

Common Criteria Testing Laboratory

Ms. Nithya Rachamadugu

CygnaCom Solutions

McLean, Virginia

Mr. Kirill Sinitski

CygnaCom Solutions

Ottawa, Ontario

Some of the material in this report was extracted from evaluation material prepared by the CCTL. Most of the product descriptions in this report were extracted from the Cellcrypt Mobile for Secret client version 1.0 Security Target.

Table of Contents

Executive Summary

This Validation Report documents the National Information Assurance Partnership (NIAP) validation team’s assessment of the CCEVS evaluation of Cellcrypt Mobile for Secret client version 1.0. This report is not an endorsement of the IT product by any agency of the U.S. Government, and no warranty of the IT product is either expressed or implied.

This report is intended to assist the end-user of this product with determining the suitability of the Target of Evaluation (TOE) in their IT environment and security posture. End-users should review both the Security Target (ST) where specific security claims are made and this Validation Report (VR) that describes how these claims were evaluated.

The TOE is Cellcrypt Mobile for Secret client version 1.0. The TOE is a software VoIP application for encrypted voice communication designed to run on an Android-based platform.

The TOE is designed to:

- Establish authenticated secure connection with a SIP server
- Establish end-to-end secure connection between multiple instances of the TOE to facilitate voice traffic

The TOE achieves authenticated connection by implementing X509 certificates. X509 certificates are used to identify each user and to establish a TLS Trusted Channel between the TOE and the SIP Server. A SIP Password is used to authenticate each user to the SIP Server as part of the Session Initiation Protocol (SIP) complying with RFC 4566.

Cellcrypt Mobile for Secret client version 1.0 requires a SIP client authentication password to be entered in order to connect to the SIP server. The user is prompted to manually enter their SIP client authentication password, which is used for authentication in REGISTER requests, whenever registration is required. The SIP client authentication password needs to be sent regularly (in REGISTER and other SIP messages as per the SIP protocol) to the SIP proxy in order to maintain the connection with the SIP server and for the VoIP service to operate.

In the evaluated default configuration, the password will need to be re-entered by the user for each REGISTER request.

The TOE achieves end-to-end encryption with the SIP Server using TLS. The TOE establishes a trusted channel with another TOE on a secure voice call using SDES-SRTP. All cryptographic functions used by the TOE are performed by a FIPS 140-2 certified module running in a FIPS mode.

The TOE provides the following security functionality: cryptography, identification and authentication, TSF protection, and trusted path/channels.

The TOE is intended for use with certified mobile devices controlled by a certified mobile device management system in the enterprise settings. In such computing environment, there is a low level threat of malicious attacks. The assumed level of expertise of the attacker for all the threats is unsophisticated.

The evaluation was performed by the CygnaCom Common Criteria Testing Laboratory (CCTL), and was completed in April 2014. The information in this report is derived from the Evaluation Technical Report (ETR) and associated test reports, all written by the CygnaCom CCTL. The evaluation team determined that the product is Common Criteria version 3.1 R4 [CC] Part 2 extended and Part 3 conformant.

The Security Target is contained within the document Cellcrypt Mobile for Secret client version 1.0 Security Target v3.2. This Security Target claims exact compliance to Protection Profile for Mobility – Voice Over IP Application, PP_MOBILITY_VOIP_V0.6, 2013- 01 -28. Exact compliance indicates that the TOE implements the security functions exactly as specified by the PP; however, functions not described in the ST may be used but were not tested as part of this evaluation.

The evaluation and validation were consistent with National Information Assurance Partnership (NIAP) Common Criteria Evaluation and Validation Scheme (CCEVS) policies and practices as described on the web site www.niap-ccevs.org.

Identification

Target of Evaluation:	Cellcrypt Mobile for Secret client version 1.0 build number v1.0.0-final-rc2
Evaluated Software and Hardware:	Installation package from which the Cellcrypt Mobile for Secret client version 1.0 application is installed.
Developer:	Cellcrypt Inc.
CCTL:	CygnaCom Solutions 7925 Jones Branch Dr, Suite 5400 McLean, VA 22102-3321
Evaluators:	Nithya Rachamadugu, Kirill Sinitski
Validation Scheme:	National Information Assurance Partnership CCEVS
Validators:	Dr. Patrick Mallett, MITRE, and Bradford O’Neill, MITRE
CC Identification:	Common Criteria for Information Technology Security Evaluation, Version 3.1 R4, September 2012
CEM Identification:	Common Methodology for Information Technology Security Evaluation, Version 3.1 R4, September 2012

Security Policy

The TOE's security policy is expressed in the security functional requirements identified in Section 6.1 of the ST. Potential users of this product should confirm that functionality implemented is suitable to meet the user's requirements.

The following Security Functions are supported by the TOE:

- Cryptography
- Identification and Authentication
- Protection of the TSF
- Trusted Path/Channels

Cryptography

TOE performs the following key cryptographic functions:

- SDES-SRTP secure channel for point-to-point communications,
  - AES_CM_128_HMAC_SHA1_80
- TLS 1.2 compliant with Suite B Profile for SIP Server registration;
  - TLS_ECDHE_ECDSA_WlTH_AES_128_GCM_SHA256
  - TLS_ECDHE_ECDSA_WlTH_AES_256_GCM_SHA384

Supporting cryptographic functions:

- encryption/decryption
  - AES operating in CTR and GCM modes and key size 128-bits, 256-bits
- signature verification
  - ECDSA with a key size of 256 bits or greater and "NIST curves" P-256 and P-384.
- hashing
  - SHA-1, SHA-256, SHA-384 and message digest 160, 256, 384 bits
- message authentication
  - HMAC-SHA-1 and key size 128 bits
- random bit generation
  - CTR_DRBG(AES) with hardware noise source
- key material destruction using zeroization

Implementation of SIP TLS tunnel and media encryption/decryption are performed by a FIPS 140-2 approved crypto library running in FIPS mode. The TOE uses the OpenSSL FIPS Object module v2.0.5, (Certificate No. 1747), which supports all crypto functions.

The TOE is intended to be run on Android Jellybean 4.2 (API 17)smartphone with an ARMv7 CPU with or without NEON optimization. This configuration is analogous to operational environment listed in the OpenSSL v2.0.5 FIPS 140-2 Security Policy. The table below provides the corresponding CAVP algorithm certificate numbers where applicable.

The Cryptographic support security function is designed to satisfy the following security functional requirements as summarized in the table below:

Requirement Class	Requirement Component	Cellcrypt Mobile for Secret Implementation	Certificate #
FCS: Cryptographic support	FCS_CKM_EXT.4: Cryptographic key material destruction (Key Material)	Zeroization of all CSPs is performed by the OpenSSL v2.0.5 FIPS object module. The following CSPs are used by Cellcrypt Mobile for Secret: • **ECDSA SGK**: ECDSA (All NIST defined B, K, and P curves) signature generation key • **AES EDK**: AES encrypt / decrypt key • **HMAC Key**: Keyed hash key • **CTR_DRBG CSPs**: V and Key (AES), entropy input (length dependent on security strength)	FIPS #1747
	FCS_COP.1(1): Cryptographic Operation (Encryption/Decryption)	AES implemented via OpenSSL v2.0.5 FIPS object module (FIPS #1747).	CAVP #1884, #2116, #2234, #2342, #2394, #2484
	FCS_COP.1(2): Cryptographic Operation (Signature Verification)	ECDSA implemented via OpenSSL v2.0.5 FIPS object module (FIPS #1747).	CAVP #264, #270, #315, #347, #378, #383, #394, #413
	FCS_COP.1(3): Cryptographic Operation (Cryptographic Hashing)	SHA implemented via OpenSSL v2.0.5 FIPS object module (FIPS #1747).	CAVP #1655, #1840, #1923, #2019, #2056, #2102
	FCS_COP.1(4): Cryptographic Operation (for keyed-hash Message Authentication)	HMAC implemented via OpenSSL v2.0.5 FIPS object module (FIPS #1747).	CAVP #1126, #1288, #1363, #1451, #1485, #1526
	FCS_RBG_EXT.1: Cryptographic operation (Random Bit Generation)	CTR_DRBG(AES) implemented via OpenSSL v2.0.5 FIPS object module (FIPS #1747).	CAVP #157, #229, #264, #292, #316, #342
	FCS_SRTP_EXT.1: Secure Real-Time Transport Protocol (SRTP)	Implemented via PJSIP v2.1 library that relies on the OpenSSL v2.0.5 FIPS object module (FIPS #1747). Cellcrypt Mobile for Secret client version 1.0 implements Secure Real Time Transport Protocol (SRTP) using the PJSIP v 2.1 library. PJSIP is compatible with SRTP (RFC 3711) and SRTP SDES (RFC 4568). PJSIP uses the OpenSSL FIPS Object	N/A

		module to provide cryptographic functionality as required in the standards. The following mandatory ciphersuite is implemented: AES_CM_128_HMAC_SHA1_80	
	FCS_TLS_EXT.1: Transport Level Security	Implemented via OpenSSL v2.0.5 FIPS object module running in FIPS Approved mode (FIPS #1747). Cellcrypt Mobile for Secret client version 1.0 supports TLS 1.2 protocol (RFC 5246) compliant with Suite B Profile for TLS implements the TLS 1.2 protocol (RFC 5246) compliant with Suite B Profile for TLS (RFC 6460) using mutual authentication with certificates and all the mandatory ciphersuites as listed below. TLS_ECDHE_ECDSA_WlTH_AES_128_GCM_SHA256 using the 256-bit prime modulus elliptic curve specified in FIPS-186-2; TLS_ECDHE_ECDSA_WlTH_AES_256_GCM_SHA384 using the 384-bit prime modulus elliptic curve specified in FIPS-186-2;	N/A
	FCS_CKM_.1: Cryptographic Key Generation	Implemented via OpenSSL v2.0.5 FIPS object module running in FIPS Approved mode (FIPS #1747). Cellcrypt Mobile for Secret client version 1.0 generates all random keys and salts as per NIST SP 800-90 CTR_DRBG(AES) using a hardware based entropy source.	N/A

Identification and Authentication Functions

The TOE uses password authentication for SIP REGISTER function and utilizes X509 certificates for TLS secure channel operation.

The user is prompted to manually enter their SIP client authentication password, which is used for authentication in REGISTER requests, whenever registration is required.

The SIP client authentication password must be sent regularly (in REGISTER and other SIP messages as per the SIP protocol) to the SIP proxy in order to maintain the connection with the SIP server and for the VoIP service to operate.

Additionally, the TOE utilizes X.509v3 certificates to authenticate the user to the SIP server via a mutually authenticated TLS connection. The certificates are loaded when a TLS connection is made. The TOE performs validity checks on the CA path and that either the SubjectAltName or SubjectDN match what was provided on the distant connection certificate. The TOE also performs OCSP or CRL validity checks on the certificate. A secure channel is successfully established only if the certificate is deemed valid.

Protection of Security Functions

Protection of TSF achieved by following methods: verifying integrity of origin and reporting software version information. The actual update functionality is implemented in the Enterprise, the TOE only reports current version to the user and Enterprise. Cellcrypt digitally signs the TOE installation package to provide integrity of origin, the OS on the device verifies the signature whenever it installs any application. Installation can be completed only if this verification succeeds.

Trusted Path/Channels

The TOE implements and requires a secured method of communications between the TOE and SIP Server, and TOE and other client applications. All data is protected by IPSec Virtual Private Network (VPN) tunnel. The VPN connection must be established before any other connection is permitted. Within VPN connection, the communication between client applications is protected by SDES-SRTP and communication with SIP Server is protected with TLS 1.2

Summary

Security functional Requirements

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)

Operational Environment Objectives

The TOE's operating environment must satisfy the following objectives:

Objective	Objective Description
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 it has determined such an update is necessary.

Assumptions and Clarification of Scope

Usage Assumptions

For secure usage, the operational environment must be managed in accordance with the documentation associated with the following PP-specified assurance requirements.

a) AGD_OPE.1 Operational user guidance

b) AGD_PRE.1 Preparative procedures

Assumptions

The ST provides additional information on the assumptions made and the threats countered.

Assumption Name	Assumption Description
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 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.

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:

1. As with any evaluation, this evaluation only shows that the evaluated configuration meets the security claims made, with a certain level of assurance specified in the protection profile.
2. This evaluation only covers the specific version of the product identified in this document, and not any earlier or later versions released or in process.
3. As specified by the assurance activities specified in 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.
4. The following are not included in the evaluation scope:
    a. *Mobile OS (including VPN access), as defined by the Mobility Capability Package v 2.0 and the Protection Profile for Mobile Operating Systems*
    b. *SIP Server, as defined by the Mobility Capability Package v2.0*
5. The IT environment needs to provide the following capabilities:

a. SIP Server

b. Mobile device management system

The ST provides additional information on the assumptions made and the threats countered.

Note*: The evaluation team did not evaluate the underlying Mobile OS as it is outside the evaluation scope.*

Architectural Information

The TOE is classified as a VoIP application for Common Criteria purposes. The TOE is a mobile software application designed to run on Android OS and provide secure voice communication over data connection.

The following block diagram outlines the TOE application architecture:

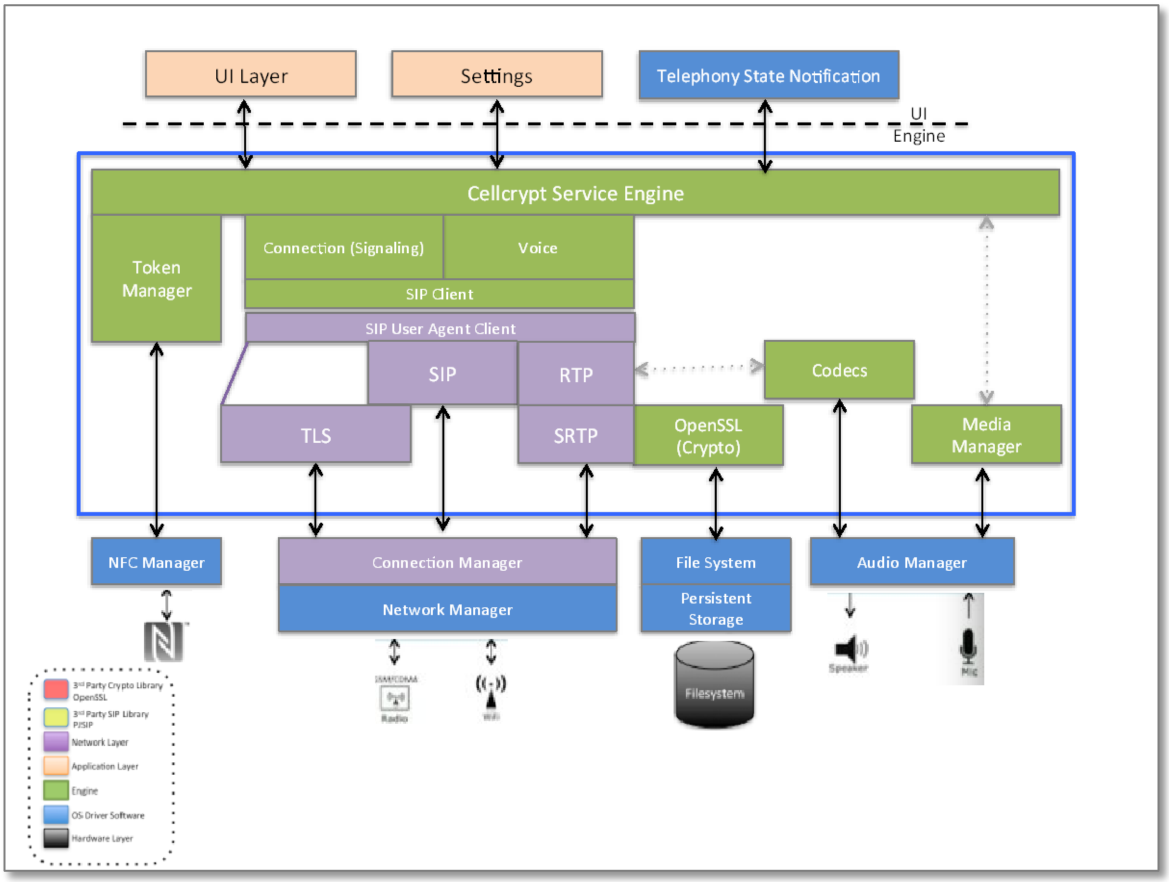

Figure 1: TOE Boundary

The physical boundary of the TOE is the installation package. The TOE requires the following components to operate:

- Android Jellybean 4.2 (API 17) operating system
- The Samsung Galaxy S4 running the Qualcomm Snapdragon 600 processor

The TOE is designed to be compatible with any Android 4.2 smartphone running on ARMv7 CPU with or without NEON optimization. The mobile operating system and smartphone hardware and firmware are considered non-TOE components.

Documentation

The Cellcrypt Inc. documents provided to the consumer are as follows:

- Cellcrypt Mobile for Secret client version 1.0 User and Administrator Guide Issue 2.2, 14 April 2014

The Cellcrypt Inc. documents maintained by the vendor are as follows:

- Cellcrypt Mobile for Secret Zeroization Procedure v0.3
- Cellcrypt Mobile for Secret Bearers v1.0
- Cellcrypt Mobile for Secret Configuration and Software Dependencies v1.0
- Cellcrypt Mobile for Secret Functional Specification v1.0

IT Product Testing

This section describes the testing efforts of the evaluation team.

Independent Testing

The evaluation team performed all of the test activities specified in the Protection Profile for Mobility – Voice Over IP Application v0.6. Additionally, the evaluation team repeated a representative sample of the developer's QA tests, and a number of team-defined tests. Combined, these tests exercised a broad range of TOE security functionality.

The test environment consisted of:

- Two Samsung Galaxy S4 (SCH-1545) smartphones running Android 4.2.2 OS
- Network Hardware
- A laptop running Oracle VM Virtual Box and
  - OpenSIP v1.7.2 running in VM
  - OpenSSL Toolkit v1.0.1e running in VM
  - Wireshark v.1.8.7

Vulnerability Analysis and Penetration Testing

The evaluation team performed an independent search for vulnerabilities affecting the TOE available from public domains including National Vulnerability Database, Open Sourced Vulnerability Database, and Security Focus.

The search for publicly known vulnerabilities included the search for vulnerabilities that affected the Mobile Device class of products that could potentially be applicable to the TOE. The evaluator also considered vulnerabilities that affected components that are part of the TOE implementation, and Android OS. Additionally, the evaluator also considered vulnerabilities affecting mobile applications operating in the comparable environment.

The evaluation team found no directly applicable public vulnerabilities, and a number of potential areas of concern to further investigate. Based on this information, four targeted penetration tests were formulated to test the product against potential, but not publically disclosed vulnerabilities. These tests identified a minor product configuration flaw that was corrected by the vendor.

Conduct of Testing

Cellcrypt Mobile for Secret client version 1.0 was subjected to a comprehensive suite of formally documented tests. The testing took place onsite at the vendor's development facility. The detailed testing activities, including exact configurations, procedures, test cases, expected results and observed results are documented in a separate Evaluator Test Report document.

Testing Results

The TOE passed all required testing activities.

Results of Evaluation

The evaluation was carried out in accordance with the Common Criteria Evaluation and Validation Scheme (CCEVS) processes and procedures. The TOE was evaluated against the criteria contained in the Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 4. The evaluation methodology used by the Evaluation Team to conduct the evaluation is the Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 4.

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 version 3.1 R3 of the CC and the CEM. Additionally the evaluators performed the assurance activities specified in the Protection Profile for Mobility – Voice Over IP Application, January 2013, Version 0.6. The evaluation determined the Cellcrypt Mobile for Secret client version 1.0 TOE meets the SARs contained the PP.

The details of the evaluation are recorded in the Evaluation Technical Report (ETR), which is controlled by CygnaCom CCTL.

Below lists the assurance requirements the TOE was required to be evaluated at Evaluation Assurance Level 1. All assurance activities and work units received a passing verdict. The following components are taken from CC part 3:

ADV_FSP.1	Basic functional specification
AGD_OPE.1	Operational user guidance
AGD_PRE.1	Preparative procedures
ALC_CMC.1	Labelling of the TOE
ALC_CMS.1	TOE CM coverage
ASE_CCL.1	Conformance claims
ASE_ECD.1	Extended components definition
ASE_INT.1	ST Introduction
ASE_OBJ.1	Security objectives
ASE_REQ.1	Derived security requirements
ASE_TSS.1	TOE summary specification
ATE_IND.1	Independent testing – conformance
AVA_VAN.1	Vulnerability survey

The evaluators concluded that the overall evaluation result for the target of evaluation is **PASS**. The validators reviewed the findings of the evaluation team, and have concurred that the evidence and documentation of the work performed support the assigned rating.

Validators Comments/Recommendations

None.

Security Target

Cellcrypt Mobile for Secret client version 1.0 Security Target, Version 3.2, April 14, 2014

Glossary

Acronyms

The following are product specific and CC specific acronyms. Not all of these acronyms are used in this document.

AES	Advanced Encryption Standard
CA	Certificate Authority
CAVP	Cryptographic Algorithm Validation Program
CC	Common Criteria [for IT Security Evaluation]
CM	Configuration Management
DTLS-SRTP	Datagram Transport Layer Security Extension to Establish Keys for Secure Real-time Transport Protocol
FIPS	Federal Information Processing Standards Publication
KEK	Key Encryption Key
NAT	network Address Translation
IT	Information Technology
NIAP	National Information Assurance Partnership
NIST	National Institute of Standards and Technology
PKI	Public Key Infrastructure
PP	Protection Profile
PRNG	Pseudo-Random Number Generator
RNG	Random Number Generator
SIP	Session Initiation Protocol
SF	Security Function
SFR	Security Functional Requirements
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions
TSFI	TOE Security Functions Interface
VPN	Virtual Private Network
VoIP	Voice over Internet Protocol

Bibliography

URLs

[1] Common Criteria Evaluation and Validation Scheme (CCEVS): (http://www.niap-ccevs.org).

[2] CygnaCom Solutions CCTL (http://www.cygnacom.com).

CCEVS Documents

[1] Common Criteria for Information Technology Security Evaluation - Part 2: Security functional components, September 2012 Version 3.1 Revision 4, CCMB-2012-09-002.

[2] Common Criteria for Information Technology Security Evaluation - Part 3: Security assurance components, September 2012, Version 3.1 Revision 4, CCMB-2012-09-003.

[3] Common Methodology for Information Technology Security Evaluation - Evaluation methodology, September 2012, Version 3.1 Revision 4, CCMB-2012-09-004.

[4] Protection Profile for Mobility – Voice Over IP Application, January 2013, Version 0.6, PP_MOBILITY_VOIP_V0.6