IA DOCUMENTATION

Security Target

Cellcrypt Mobile for Secret client version 1.0

PP Ref: Protection Profile for Mobility – Voice Over IP Application, PP_MOBILITY_VOIP_V0.6, 2013- 01 -28.

Ref:	**ST001**
Version:	**3.2**
Date:	**14 April 2014**

DOCUMENT CONTROL

Version History

Author(s)	Version	Date	Update
RC	3.2	14 Apr 2014	Updates following validator review. Update to specify processor explicitly, and update build number to account for updating OpenSSL to v1.0.1g to fix heartbleed bug.
RC	3.1	31 Mar 2014	Updates following validator review.
RC	3.0	10 Mar 2014	Updates following validator review.
RC	2.0	10 Jan 2014	Update all versions numbers to final.
PG	1.9	1st Oct 2013	Update Table 8 Certificate numbers for version 2.0.5 of OpenSSL FIPS Object Module
PG	1.8	22nd Aug 2013	Align TOE version with F8002a. Removed reference to FCS_CKM.1 in Table 6
PG	1.7	20th Aug 2013	Update version of PJSIP
PG	1.6	14th Aug 2013	Update after drafting FS
PG	1.5	1st Aug 2013	Updated after lab review
PG	1.4	30th Jul 2013	Updated after lab review
PS	1.3	30th May 2013	Updated after lab review
PS	1.2	22nd Mar 2013	Updated after lab review
PS	1.1	27th Feb 2013	Re-issued after reformatting
PS	1.0	22nd Feb 2013	First Issue

CONTENTS

List of Figures

List of Tables

Conventions

The following conventions have been applied in this document:

The CC defines operations on Security Functional Requirements (SFR): assignments, selections, assignments within selections and refinements. This document uses the following font conventions to identify the operations defined by the CC:

- Assignment: Indicated with *italicized* text;
- Refinement made by PP author: Indicated by the word "Refinement" in **bold text** after the element number with additional **bold** text and deletions with strikethroughs, if necessary;
- Selection: Indicated with underlined text;
- Assignment within a Selection: Indicated with *italicized and underlined* text;
- Iteration: Indicated by appending the iteration number in parenthesis, e.g., (1), (2), (3).

Explicitly stated SFRs are identified by having a label 'EXT' after the requirement name for TOE SFRs.

1 SECURITY TARGET INTRODUCTION

This section identifies the Security Target (ST) and Target of Evaluation (TOE) identification, ST conventions, ST conformance claims, and the ST organization.

The TOE is comprised of Cellcrypt Mobile for Secret client version 1.0, a Secure Voice over Internet Protocol (SVoIP) application for smartphones, which enables users to have secure voice calls on an end-to-end encrypted session.

The Security Target contains the following additional sections:

- Conformance Claims (Section 2)—provides details of conformance of the security target against Common Criteria and provides rationale that the TOE conforms to the PP(s) for which conformance has been claimed.
- Security Problem Definition (Section 3)—specifies the assumptions and threats that define the security problem to be addressed by the TOE and its operational environment.
- Security Objectives (Section 4)—specifies the security objectives for the TOE and its operational environment necessary to counter the threats and satisfy the assumptions defining the security problem.
- Extended Components Definition (Section 5)—specifies any new components that define extended functional and extended assurance requirements.
- TOE Summary Specification (Section 6)—describes the security functions of the TOE and how they satisfy the security functional requirements.

1.1 Security Target Reference

ST Title – Cellcrypt Mobile for Secret client version 1.0 Security Target
ST Version – Version 3.2
ST Date – April 14, 2014

1.2 TOE Reference

TOE Identification – Cellcrypt Mobile for Secret client version 1.0
TOE Developer – Cellcrypt Inc.
Evaluation Sponsor – Cellcrypt Inc.
CC Identification – Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 4, September 2012
Build Number – v1.0.0-final-rc2

1.3 TOE Overview

Cellcrypt Mobile for Secret client version 1.0 is a VOIP application for secure encrypted voice calls designed to run on standard mobile phones. It comprises a handset software application and a back-end support infrastructure (SIP server). Only the handset software application 'Cellcrypt Mobile for Secret client version 1.0' is regarded as the TOE.

Cellcrypt Mobile for Secret client version 1.0 uses standard wireless packet-based connectivity over Global System for Mobile Communications (GSM)/Enhanced Data rates for GSM Evolution (EDGE) or Wideband Code Division Multiple Access (WCDMA) encrypted voice communication.

Authenticated connection set-up ensures that only Cellcrypt Mobile for Secret client version 1.0 enabled mobile phones can participate in secure sessions.

End-to-end encryption is achieved through the creation and use of session unique encryption keys. These are used by the handset software application when encrypting/decrypting secure voice traffic.

The following assumptions have been made:

- The mobile platform will be ARMv7 hardware with Android Jellybean 4.2 (API 17) OS.
- Cellcrypt Mobile for Secret client version 1.0 will only handle single session, unicast, secure voice calls.

Non-TOE Requirements

- Mobile OS (including VPN access), as defined by the Protection Profile for Mobile Device Fundamentals [2], is outside of the scope of this evaluation.
- SIP Server, as defined by the Protection Profile for SIP Server [3], is outside of the scope of this evaluation.
- Cellcrypt Mobile for Secret client version 1.0 will operate exclusively within the mobility ecosystem specified by the associated mobility Protection Profiles, and will assume that all associated resources (IPSEC VPN tunnel, PKI, SIP network) are in place.

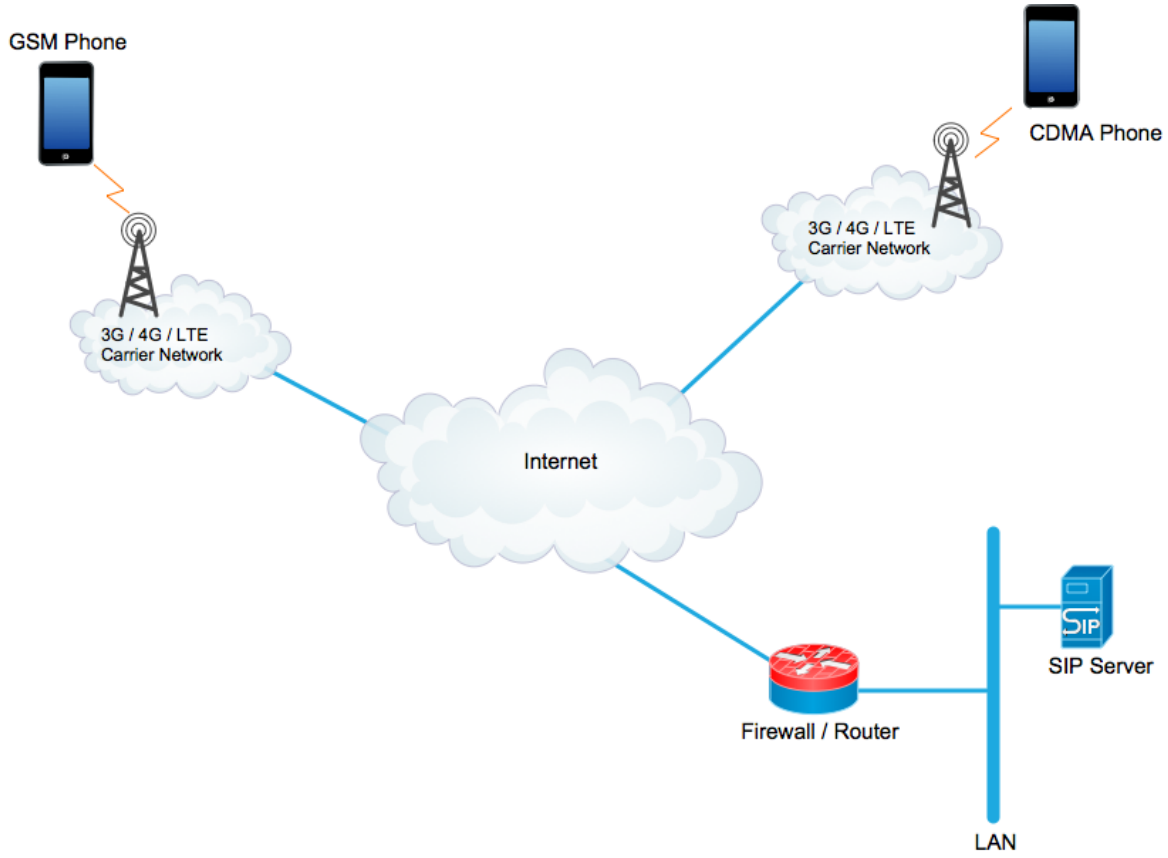

Figure 1: Sample Deployment Architecture

1.3.1 TOE Architecture

The following block diagram outlines the Cellcrypt Mobile for Secret client version 1.0 application architecture on the Android platform.

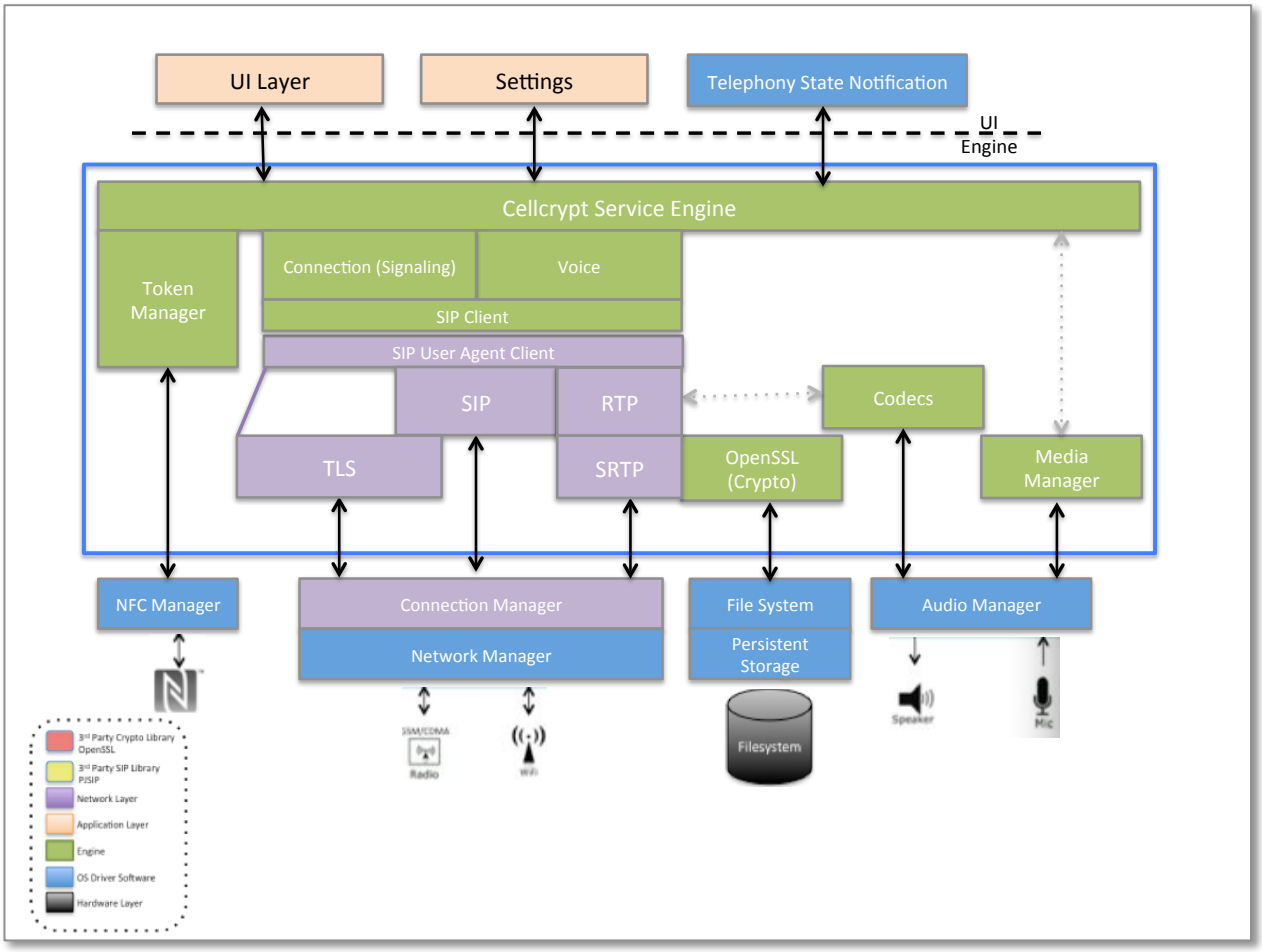

Figure 2: Cellcrypt Mobile for Secret Android Architecture

1.3.1.1 Physical Boundaries

The physical boundary of the TOE is the installation package from which the Cellcrypt Mobile for Secret client version 1.0 application is installed.

The TOE is described as Cellcrypt Mobile for Secret client version 1.0. In order to comply with the evaluated configuration, the following components should be used.

1.3.1.2 Mobile Platform

The TOE requires the following additional mobile platform components to operate:

- Android Jellybean 4.2 (API 17) operating system
- Smartphone handset compatible with the operating system[1]. The handsets tested at this time are:
    - Samsung Galaxy S4 running the Qualcomm Snapdragon 600 processor.

[1] The TOE is designed to be compatible with any Android 4.2 smartphone running on ARMv7 architecture CPU with or without NEON optimization.

The operating system and handset are considered non-TOE components.

1.3.1.3 Logical Boundaries

The Cellcrypt Mobile for Secret client version 1.0 application implements the following components within its logical boundary (application boundary shown by blue line):

- Cellcrypt Service Engine
- Token Manager
- Connection
- Voice
- Media Manager
- SIP Stack (Third party library)
- OpenSSL Crypto Library (Third party library)
- Codecs (Third party library)

The following sections describe each of the components within the application boundary.

1.3.1.3.1. SIP Stack

Cellcrypt Mobile for Secret client version 1.0 licenses the 3rd party commercial PJSIP stack to provide SIP protocol functionality and compliance with certain open standards including, SIP (RFC 3261), SDP (RFC 4566), SRTP (RFC 3711), and SDES (RFC 4568).

The SIP stack is used to implement:

- FCS_SRTP_EXT.1: Secure Real-Time Transport Protocol (SRTP)
- FIA_SIPC_EXT.1: Session Initiation Protocol (SIP) Client
- FTP_ITC.1(1): Inter-TSF Trusted Channel (SDES-SRTP) and iterations
- FTP_ITC.1(2): Inter-TSF Trusted Channel (TLS/SIP) and iterations

1.3.1.3.2. Crypto Library

Cellcrypt Mobile for Secret client version 1.0 uses the FIPS validated (cert. no. 1747) OpenSSL FIPS Object Model v.2.0.5 module for all its cryptographic operations. Cert. no. 1747 covers Android 4.2 running on ARMv7 CPU with or without NEON optimizations. The module is run in FIPS 140-2 Approved mode of operation. OpenSSL is sourced built and initialised as per FIPS guidelines without any modifications to source. The OpenSSL libraries (libcrypto and libssl) are dynamically linked to the application.

The TLS stack uses the OpenSSL module and is built into the application binary.

OpenSSL provides the following cryptographic functionality.

- FCS_CKM_EXT.4: Cryptographic key material destruction (Key Material)
- 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_TLS_EXT.1: Transport Level Security

OpenSSL also provides functionality to manage X.509 certificates as per FIA_X509_EXT.1 and iterations.

1.3.1.3.3. Codecs

Cellcrypt Mobile for Secret client version 1.0 implements the following codecs: G.711, iLBC, and Speex.

1.3.1.3.4. Cellcrypt Service Engine

Main application service, which contains the overall logic for maintaining call state, initiating calls, and interfacing with UI and audio. The Cellcrypt Service Engine provides the functionality to enable an Enterprise to query the current version of the TOE as per FPT_TUD_EXT.1.1.

1.3.1.3.5. Token Manager

Interface logic to a generalized token to request tap, store and retrieve data to/from a token. Currently the only token interface we use is NFC, which is out of the scope of the ST.

1.3.1.3.6. Connection

Generalized logic for call management (setup/teardown). Interfaces SIP specific events to more general call state events.

1.3.1.3.7. Voice

A "voice session" type which represents an individual established voice call. In-call events (eventually DTMF handling) would be handled here. Other session types (i.e. Messaging, Video) could be possibly added in future releases.

1.3.1.3.8. Media Manager

Manages starting and stopping of ringtones (for incoming calls), and ringing tones (on outgoing calls for far-end ringing, busy tone, fast-busy on network error, etc).

1.3.1.3.9. SRTP

Part of the SIP Stack which manages the Secure RTP (encrypted RTP) voice stream.

1.3.1.3.10. RTP

Part of the SIP Stack which manages the non-encrypted RTP voice stream.

1.3.1.3.11. SIP user agent client

A high level API for constructing SIP multimedia user agent applications. It wraps together the signaling and media functionalities into a call API, interfacing with the lower level SIP and RTP.

1.3.1.4 External Infrastructure Components

1.3.1.4.1. SIP Server

All secure mobile call requests are handled by (SIP) Server (Please see Figure 1). The SIP Server acts as a SIP Registrar/Proxy to provide device registration and coordination of calls between User Equipment.

1.4 TOE Description

The Target of Evaluation (TOE) is the Cellcrypt Mobile for Secret client version 1.0 smartphone application, which will run on an Android 4.2 (API 17) based platform. The Cellcrypt Mobile for Secret client version 1.0 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 achieves authenticated connection using the Identification and authentication (FIA) security functions (SF). X.509 Certificates are used to identify and authenticate each user (FIA_X509_EXT.1) to establish a Trusted Path/Channel (FTP) between the TOE and the SIP Server with TLS (SF FTP_ITC.1(2)). A user password is used to identify and authenticate each user to the SIP Server as part of the Session Initiation Protocol (SIP) Client (FIA_SIPC_EXT.1). Cellcrypt Mobile for Secret client version 1.0 requests that the user inputs her password whenever the TOE requires it.

The TOE achieves end-to-end encryption using the Trusted Path/Channel (FTP) SFs. The TOE establishes a trusted channel with the SIP Server using Inter-TSF Trusted Channel TLS/SIP (FTP_ITC.1(2)). The TOE establishes a trusted channel with another TOE on a secure voice call using Inter-TSF Trusted Channel SDES-SRTP (FTP_ITC.1(1)).

These SFs depend on Cryptographic Support (FCS): FCS-CKM_EXT.4, FCS_COP1(1-4), FCS_RBG_EXT.1, FCS_SRTP_EXT.1, FCS_TLS_EXT.1, and Trusted Update of the TOE (FPT_TUD_EXT.1).

2 CONFORMANCE CLAIMS

2.1 CC Conformance Claim

This ST and the TOE it describes are conformant to the following CC specifications:

- Common Criteria for Information Technology Security Evaluation Part 2: Security Functional Components, September 2012, Version 3.1, Revision 4, CCMB-2012-09-002
    - Part 2 Conformant with additional extended functional components.
- Common Criteria for Information Technology Security Evaluation Part 3: Security Assurance Components, September 2012, Version 3.1, Revision 4, CCMB-2012-09-003

2.2 Protection Profile Claim

The TOE claims to be strictly compliant with all the requirements as specified in the Protection Profile for Mobility – Voice Over IP Application, PP_MOBILITY_VOIP_V0.6, 2013- 01 -28. [1].

2.3 Package Claim

The ST does not claim to be conformant with any pre-defined packages.

2.4 Conformance Rationale

This security target claims strict conformance to only one PP [PP_MOBILITY_VOIP_V0.6] [1].

The security problem definition of this security target is consistent with the statement of the security problem definition in the PP, as the security target claims strict conformance to the PP and no other threats, organizational security policies and assumptions are added.

The security objectives of this security target are consistent with the statement of the security objectives in the PP as the security target claims strict conformance to the PP and no other security objectives are added.

The security requirements of this security target are consistent with the statement of the security requirements in the PP as the security target claims strict conformance to the PP.

3 SECURITY PROBLEM DEFINITION

This section describes the assumptions and threats that are relevant to both the TOE and its environment. The first section describes the secure usage assumptions, which are those items that the TOE itself cannot implement or enforce. The next two sections cover the threats that are expected to exist in a basic robustness environment and are grouped into threats to be addressed by the TOE and threats to be addressed by the TOE environment.

Both the assumptions and the threats are reproduced from the US Government Protection Profile for Security Requirements for Voice Over IP Application, Version 0.6, January 24, 2013.

3.1 Threats addressed by the TOE

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 IT entity may misrepresent itself as the TOE to obtain identification and authentication data.
T.UNAUTHORIZED_UPDATE	An update may be needed to a specific version of the TOE, but that specific version may not be known to the Enterprise (that is performing the update).

3.2 Organisational Security Policies

The PP does not specify any organisational security policies relevant to the operation of the TOE.

3.3 Assumptions

The following conditions are assumed to exist in the operational environment.

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.

4 SECURITY OBJECTIVES

This section defines the security objectives for the TOE and its supporting environment. The security objectives are intended to counter identified threats, comply with defined organizational security policies, and address applicable assumptions.

The security objectives are reproduced from the US Government Protection Profile for Security Requirements for Voice Over IP Application, Version 0.6, 24th January, 2013.

4.1 Security objectives for the TOE

Objective	Objective Description
O.PROTECTED_COMMUNICATIONS	The TOE will provide protected communication channels with authorized IT entities (SIP server and other VOIP applications)
O.TRUSTED_UPDATES	The TOE will provide the capability to report its current version.

Table 1: Security objectives for the TOE

4.2 Security objectives for the operating environment

All of the assumptions stated in section 3.1 are considered to be security objectives for the environment. The following are the non-IT security objectives, which, in addition to those assumptions, are to be satisfied without imposing technical requirements on the TOE. That is, they will not require the implementation of functions in the TOE hardware and/or software. Thus, they will be satisfied largely through application of procedural or administrative measures.

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.

Table 2: Security objectives for the operating environment

4.3 Security Objectives Rationale

4.3.1 Summary Mapping of Security Objectives

This section provides the summary that all security objectives are traced back to aspects of the addressed assumptions, threats, and Organizational Security Policies.

	Threats/Assumptions					
Objectives	T.UNAUTHORIZED_ACCESS	T.UNAUTHORIZED_UPDATE	A.AUTHORIZED_USER	A.AVAILABILITY	A.OPER_ENV	A.TRUSTED_ADMIN
O.PROTECTED_COMMUNICATIONS	x					
O.TRUSTED_UPDATES		x				
OE.AUTHORISED_USER			x			
OE_AVAILABILITY				x		
OE.OPER_ENV					x	
OE.TRUSTED_ADMIN						x
OE.VERIFIABLE_UPDATES		x				

Table 3: Mapping of Assumptions and Threats to Security Objectives

4.3.2 Security Objectives of the TOE Rationale

THREAT / POLICY / ASSUMPTION	**ADDRESSED BY**	**RATIONALE**
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 IT entity may misrepresent itself as the TOE to obtain identification and authentication data.	**O.PROTECTED_COMMUNICATIONS** The TOE will provide protected communication channels with authorized IT entities (SIP server and other VOIP applications)	**O.PROTECTED_COMMUNICATIONS** Contributes to mitigating this threat by requiring authorized users access to the SIP server and other VOIP applications. The data and voice paths are protected by a VPN connection. A mutually authenticated TLS tunnel further protects the data path.

T.UNAUTHORIZED_UPDATE An update may be needed to a specific version of the TOE, but that specific version may not be known to the Enterprise (that is performing the update).	**O.VERIFIABLE_UPDATES** The TOE will provide the capability to help ensure that the version of the TOE can be verified by the Enterprise.	**O.TRUSTED_UPDATES** Contributes to mitigating this threat by providing a facility to query the version of software installed. The integrity of origin is also verified when the software is installed.
A.AUTHORIZED_USER The cell phone user will follow all provided user guidance. An authorized user is not considered hostile or malicious.	**OE.AUTHORIZED_USER** The cell phone user of the TOE is non-hostile and follows all user guidance.	**OE.AUTHORIZED_USER** Restates the assumption.
A.AVAILABILITY Network resources shall be available to allow VoIP clients to satisfy mission requirements and to transmit information.	**OE.AVAILABILITY** Network resources will be available to allow VoIP clients to satisfy mission requirements and to transmit information.	**OE.AVAILABILITY** Addresses this assumption by requiring that the Enterprise has correctly configured the application to work with the SIP infrastructure and that the SIP infrastructure is operating correctly.
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.	**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.OPER_ENV** Addresses this assumption by requiring that the SVOIP application is operating within an environment that is compatible with the Protection Profiles for Mobile Device Fundamentals [2] and SIP Server [3]
A.TRUSTED_ADMIN TOE Administrators are trusted to follow and apply all administrator guidance in a trusted manner.	**OE.TRUSTED_ADMIN** TOE Administrators are trusted to follow and apply all administrator guidance in a trusted manner.	**OE.TRUSTED_ADMIN** Restates the assumption.

Table 4: Mapping of Assumptions and Threats to Objectives

5 EXTENDED COMPONENTS DEFINITION

The TOE implements the following extended components as defined in the PP [1]. Further details including iterations are provided in section 6.

Requirement Class	Requirement Component
FCS: Cryptographic support	FCS_CKM_EXT.4: Cryptographic key material destruction (Key Material)
	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

Table 5: Extended Components implemented by the TOE

[FCS_CKM.1] Cryptographic Key Generation
[FCS_CKM.1] is not formally part of the PP – denoted by enclosing in square brackets - so is not formally be included in these Security Requirements. As noted in the PP, the requirements of [FCS_CKM.1] are contained in the PP by reference in the specifications of the underlying protocols (TLS, DTLS and SDES).

The TOE is required by the PP to produce random keys and salts as specified in underlying protocols for TLS, DTLS and SDES. [FCS_CKM.1] is satisfied by implementation of FCS_RBG_EXT.1 and iterations as described above. TSF performs all RBG services required by the TOE and these are compliant with the NIST SP 800-90 standard.

6 SECURITY REQUIREMENTS

This section specifies the security requirements for the TOE. The statement of security functional requirements reproduces the security functional requirements (SFRs) specified in the US Government Protection Profile for Security Requirements for Voice Over IP Application with operations completed as appropriate. The requirements are all drawn from the CC Part 2.

6.1 Security functional requirements

The following table identifies the security functional requirements that are satisfied by the TOE.

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)

Table 6: Security Functional Requirements

6.1.1 Cryptographic Support (FCS)

FCS_CKM_EXT.4 Cryptographic key material destruction (Key Material)
FCS_CKM_EXT.4.1 The TSF shall zeroize all plaintext secret and private cryptographic keys and Critical Security Parameters (CSPs) when no longer required.

Note that FCS_CKM_EXT.4 depends on [FCS_CKM.1], as justified in the rationale section (6.3).

FCS_COP. 1(1) Cryptographic Operation (Encryption/Decryption)
FCS_COP.1.1 The TSF shall perform encryption and decryption in accordance with a specified cryptographic algorithm AES operating in *CTR and GCM modes* and cryptographic key size 128-bits, 256-bits and no other key sizes that meets the following:

- FIPS PUB 197 “Advanced Encryption Standard (AES)"
- NIST SP 800-38A
- NIST SP 800-38D

FCS_COP.1(2) Cryptographic Operation (Signature Verification)
FCS_COP.1.1(2) **Refinement:** The TSF shall perform **cryptographic signature** services in accordance with a **Elliptic Curve Digital Signature Algorithm (ECDSA) with a key size of 256 bits or greater** that meets the following:

Case: Elliptic Curve Digital Signature Algorithm

- **FIPS PUB 186-3, 'Digital Signature Standard"**
- **The TSF shall implement "NIST curves" P-256, P-384, and no other curves, (as defined in FIPS PUB 186-3, 'Digital Signature Standard")**

FCS_COP.1(3) Cryptographic Operation (Cryptographic Hashing)
FCS_COP.1.1(3) **Refinement**: The TSF shall perform cryptographic hashing services in accordance with a specified cryptographic algorithm SHA-1, SHA-256, SHA-384, and **message digest** sizes 160, 256, 384 bits that meet the following: *"FIPS Pub 180-3, 'Secure Hash Standard."*

FCS_COP. 1(4) Cryptographic Operation (For keyed-hash Message Authentication)
FCS_COP.1.1(4) **Refinement**: The TSF shall perform keyed-hash message authentication in accordance with a specified cryptographic algorithm *HMAC-SHA-1* and key size 128 bits, **and message digest size** 160 bits that meet the following: FIPS Pub 198-1, "The Keyed-Hash Message Authentication Code, and FIPS Pub 180-3, "Secure Hash Standard."

FCS_RBG_EXT.1 Extended: Cryptographic operation (Random Bit Generation)
FCS_RBG_EXT.1.1 The TSF shall perform all random bit generation (RBG) services in accordance with NIST Special Publication 800-90 using CTR_DRBG(AES) seeded by an entropy source that accumulates entropy from software-based and operational environment hardware-based noise source.

FCS_RBG_EXT.1.2 The deterministic RBG shall be seeded with a minimum number of bits of entropy at least equal to the greatest bit length required by the protocols and functions supported by the TOE.

FCS_SRTP_EXT.1 Secure Real-Time Transport Protocol (SRTP)
FCS_SRTP_EXT.1.1 The TSF shall implement the Secure Real-Time Transport Protocol (SRTP) that complies with RFC 3711, and use Security Descriptions for Media Streams (SDES) in compliance with RFC 4568 to provide key information for the SRTP connection.

FCS_SRTP_EXT.1.2 The TSF shall implement SDES-SRTP supporting the following ciphersuites in accordance with RFC 4568: AES_CM_128_HMAC_SHA1_80.

FCS_SRTP_EXT.1.3 The TSF shall ensure the SRTP NULL algorithm shall be disabled.

FCS_SRTP_EXT.1.4 The TSF shall allow the SRTP ports to be used for SRTP communications to be specified by the Enterprise.

FCS_TLS_EXT .1 Transport Level Security
FCS_TLS_EXT.1.1 The TSF shall implement the TLS 1.2 protocol (RFC 5246) compliant with Suite B Profile for TLS (RFC 6460) using mutual authentication with certificates and ciphersuites:

Mandatory ciphersuites:
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 using the 256-bit prime modulus elliptic curve specified in FIPS-186-2;

TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 using the 384-bit prime modulus elliptic curve specified in FIPS-186-2;

Optional Ciphersuites:
TLS_RSA_WITH_3DES_EDE_CBC_SHA
TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_DHE_DSS_WITH_AES_128_CBC_SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_DHE_DSS_WITH_AES_256_CBC_SHA
TLS_DHE_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA256
TLS_RSA_WITH_AES_256_CBC_SHA256
TLS_DHE_DSS_WITH_AES_128_CBC_SHA256
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
TLS_DHE_DSS_WITH_AES_256_CBC_SHA256
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
TLS_RSA_WITH_AES_128_GCM_SHA256
TLS_RSA_WITH_AES_256_GCM_SHA384
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
TLS_DHE_DSS_WITH_AES_128_GCM_SHA256
TLS_DHE_DSS_WITH_AES_256_GCM_SHA38
TLS_ECDH_ECDSA_WITH_3DES_EDE_CBC_SHA
TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA
TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA
TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
TLS_ECDH_RSA_WITH_3DES_EDE_CBC_SHA
TLS_ECDH_RSA_WITH_AES_128_CBC_SHA
TLS_ECDH_RSA_WITH_AES_256_CBC_SHA
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA256
TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA384
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
TLS_ECDH_RSA_WITH_AES_128_CBC_SHA256

TLS_ECDH_RSA_WITH_AES_256_CBC_SHA384
TLS_ECDH_ECDSA_WITH_AES_128_GCM_SHA256
TLS_ECDH_ECDSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
TLS_ECDH_RSA_WITH_AES_128_GCM_SHA256
TLS_ECDH_RSA_WITH_AES_256_GCM_SHA384

6.1.2 Identification and Authentication (FIA)

FIA_SIPC_EXT.1 Session Initiation Protocol (SIP) Client

FIA_SIPC_EXT.1.1 The TSF shall implement the Session Initiation Protocol (SIP) that complies with RFC 3261 using the Session Description Protocol (SDP) complying with RFC 4566 to describe the multimedia session that will be used to carry the VOIP traffic.

FIA_SIPC_EXT.1.2 The TSF shall require the user to enter a password to support the use of password authentication for SIP REGISTER function requests as specified in section 22 of RFC 3261.

FIA_SIPC_EXT.1.3 The TSF shall support SIP authentication passwords that contain at least *8* characters in the set of {upper case characters, lower case characters, numbers, and the following special characters: "!", “@”, "#", "$", “%", "^", “&”, "*”, "(", and ")" and no other characters}.

FIA_SIPC_EXT.1.4 Password entered by the user as per FIA_SIPC_EXT.1.2 shall be cleared by the TSF once the TSF is notified that the REGISTER request was successful.

X509 Certificates (FIA_X509_EXT)
The certificates used by the TSF are those for the distant end TLS connection and the user’s certificate (and associated private key). While it is acceptable for the TSF itself to store and protect these certificates, it is also allowable for the Mobile OS to provide these storage and protection functions. If the TSF provides these functions, then the FIA_X509_EXT.1.Y element shall be included in the body of the ST in this component.

F**IA_X509EXT.1 Extended: X509 certificates**

FIA_X509_EXT.1.Y elements have been included as the TSF relies on itself to provide the storage and protection functions.

FIA_X509_EXT.1.Y The TSF shall store and protect the certificate(s) from unauthorized deletion and modification.

FIA_X509_EXT.1.1 The TSF shall use X.509v3 certificates as defined by RFC 5280 to support authentication for TLS connections.

FIA_X509_EXT.1.2 The TSF shall provide the capability for the Enterprise to load the X.509v3 certificates into the TOE for use by the security functions specified in the PP.

FIA_X509_EXT.1.3 The TSF shall validate the certificate using the Online Certificate Status Protocol (OCSP) as specified in RFC2560 , a Certificate Revocation List (CRL) as specified in RFC 5759.

FIA_X509_EXT.1.4. The TSF shall not establish a TLS connection if a certificate is deemed invalid.

FIA_X509_EXT.1.5 When the TSF cannot establish a connection to determine the validity of a certificate, the TSF shall, as configured by the Enterprise, establish the TLS connection or disallow the establishment of the TLS connection.

6.1.3 Protection of the TOE Security Functions (FPT)

FPT_TUD_EXT .1 Extended: Trusted Update

FPT_TUD_EXT.1.1 The TSF shall provide the Enterprise the ability to query the current version of the TOE software.

6.1.4 Trusted Path/Channel (FTP)

FTP_ITC.1(1) Inter-TSF Trusted Channel (SDES-SRTP)

FTP_ITC.1.1(1) **Refinement:** The TSF shall provide a communication channel between itself and a **remote VoIP application using SDES-SRTP as specified in FCS_SRTP_EXT.1** that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification **and** disclosure.

FTP_ITC.1.2(1) The TSF shall permit the TOE or the remote VoIP application to initiate communication via the trusted channel.

FTP_ITC.1.3(1) The TSF shall initiate communication via the trusted channel for *all communications between the two devices*.

FTP_ITC.1(2) Inter-TSF Trusted Channel (TLS/SIP)

FTP_ITC.1.1(2) **Refinement:** The TSF shall provide a communication channel between itself and **a SIP Server using TLS "and no other protocol", as specified in FCS_TLS_EXT.1 "only",** that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification and ~~or~~ disclosure.

FTP_ITC.1.2(2) The TSF shall permit the TSF to initiate communication via the trusted channel.

FTP_ITC.1.3(2) The TSF shall initiate communication via the trusted channel for *all communications with the SIP server*.

6.2 Security Assurance Requirements

All assurance requirements are summarized in the table below.

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 User Guidance
AVA: Vulnerability assessment	AVA_VAN.1: Vulnerability Analysis
ALC: Lifecycle support	ALC_CMC.1: Labelling of the TOE
	ALC_CMS.1: TOE CM Coverage
ATE: Tests	ATE_IND.1: Independent Testing - Conformance

Table 7: Assurance Requirements

6.2.1 Class ADV: Development

6.2.1.1 ADV_FSP.1 Basic Functional Specification

Developer action elements:

ADV_FSP.1.1D	The developer shall provide a functional specification.
ADV_FSP.1.2D	The developer shall provide a tracing from the functional specification to the SFRs.

Content and presentation elements:

ADV_FSP1.1C	The functional specification shall describe the purpose and method of use for each SFR-enforcing and SFR-supporting TSFI.
ADV_FSP.1.2C	The functional specification shall identify all parameters associated with each SFR-enforcing and SFR-supporting TSFI.
ADV_FSP.1.3C	The functional specification shall provide rationale for the implicit categorization of interfaces as SFR-non-interfering.
ADV_FSP.1.4C	The tracing shall demonstrate that the SFRs trace to the TSFIs in the functional specification.

Evaluator action elements:

ADV_FSP.1.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
ADV_FSP.1.2E	The evaluator shall determine that the functional specification is an accurate and

	complete instantiation of the SFRs.

6.2.2 Class AGD: Guidance Documents

6.2.2.1 AGD_OPE.1 Operational User Guidance

Developer action elements:

AGD_OPE.1.1D	The developer shall provide operational user guidance.

Content and presentation elements:

AGD_OPE.1.1C	The operational user guidance shall describe ~~what~~ the authorized user-accessible functions and privileges that should be controlled in a secure processing environment, including appropriate warnings.
AGD_OPE.1.2C	The operational user guidance shall describe, for the authorized user, how to use the available interfaces provided by the TOE in a secure manner.
AGD_OPE.1.3C	The operational user guidance shall describe, for the authorized user, the available functions and interfaces, in particular all security parameters under the control of the user, indicating secure values as appropriate.
AGD_OPE.1.4C	The operational user guidance shall, for the authorized user, clearly present each type of security-relevant event relative to the user-accessible functions that need to be performed, including changing the security characteristics of entities under the control of the TSF.
AGD_OPE.1.5C	The operational user guidance shall identify all possible modes of operation of the TOE (including operation following failure or operational error), their consequences and implications for maintaining secure operation.
AGD_OPE.1.6C	The operational user guidance shall, for the authorized user, describe the security measures to be followed in order to fulfil the security objectives for the operational environment as described in the ST.
AGD_OPE.1.7C	The operational user guidance shall be clear and reasonable.

Evaluator action elements:

AGD OPE.1.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

6.2.2.2 AGD_PRE.1 Preparative procedures

Developer action elements:

AGD_PRE.1.1D	The developer shall provide the TOE including its preparative procedures.

Content and presentation elements:

AGD_PRE.1.1C	The preparative procedures shall describe all the steps necessary for secure acceptance of the delivered TOE in accordance with the developer's delivery procedures.
AGD_PRE.1.2C	The preparative procedures shall describe all the steps necessary for secure installation of the TOE and for the secure preparation of the operational environment in accordance with the security objectives for the operational environment as described in the ST.

Evaluator action elements:

AGD_PRE.1.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation evidence.

6.2.3 Class AVA: Vulnerability Assessment

6.2.3.1 AVA_VAN.1 Vulnerability survey

Developer action elements:

AVA_VAN.1.D	The developer shall provide the TOE for testing.

Content and presentation elements:

AVA_VAN.1.1C	The TOE shall be suitable for testing.

Evaluator action elements:

AVA_VAN.1.1E	The evaluator shall confirm that the information provided meets all the requirements for content and presentation of evidence.
AVA_VAN.1.2E	The evaluator shall perform a search of public domain sources to identify potential

	vulnerabilities in the TOE.
AVA_VAN.1.3E	The evaluator shall conduct penetration testing, based in the identified potential vulnerabilities, to determine that the TOE is resistant to attacks performed by an attacker possessing Basic attack potential.

6.2.4 Class ALC: Life-Cycle Support

6.2.4.1 ALC_CMC.1 Labelling of the TOE

Developer action elements:

ALC_CMC.1.1D	The developer shall provide the TOE and a reference for the TOE.

Content and presentation elements:

ALC_CMS.2.1D	The developer shall provide a configuration list for the TOE.

Evaluator action elements:

ALC_CMC.2.1E	The evaluator shall conform that the information provided meets all the requirements for content and presentation of evidence.

6.2.4.2 ALC_CMS.1 TOE CM coverage

Developer action elements:

ALC_CMS.2.1D	The developer shall provide a configuration list for the TOE.

Content and presentation elements:

ALC_CMS.2.1C	The configuration list shall include the following: the TOE itself, and the evaluation evidence required by the SARs.
ALC_CMS.2.2C	The configuration list shall uniquely identify the configuration items.

Evaluator action elements:

ALC_CMS.2.1E	The evaluator shall confirm that the information provided meets all requirements

	for content and presentation of evidence.

6.2.5 Class ATE: Test

6.2.5.1 ATE_IND.1 Independent testing – Conformance

Developer action elements:

ATE_IND.1.1D	The developer shall provide the TOE for testing.

Content and presentation elements:

ATE_IND.1.1C	The TOE shall be suitable for testing.

Evaluator action elements:

ATE_IND.1.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
ATE_IND.1.2E	The evaluator shall test a subset of the TSF to confirm that the TSF operates as specified.

6.3 Security Requirements Rationale

The RATIONALE Section of the Security Requirements for Voice Over IP Application PP provides rationale for the security requirements, demonstrating that the security requirements are suitable to address the IT security objectives. This rationale is valid for the PP requirements reproduced in the ST and is not further discussed.

FCS_CKM_EXT.4 dependency on FCS_CKM.1 is satisfied by reference in the specification of the underlying protocols. This approach is dictated by the PP.

7 TOE SUMMARY SPECIFICATION

Cellcrypt Mobile for Secret client version 1.0 is a Secure Voice over Internet Protocol (SVoIP) application for smartphones, which enables users to have secure voice calls on an end-to-end encrypted session. Cellcrypt Mobile for Secret client version 1.0 meets the requirements of the Protection Profile for secure VoIP Application [1], and is intended to operate in an environment specified by the Protection Profile for Mobile Device Fundamentals [2], and the Protection Profile for SIP Server [3].

The scope of evaluation is primarily applicable to Cellcrypt Mobile for Secret client version 1.0 running on a smartphone. The functionalities performed by other system components (Mobile OS, SIP Server, Certificate Authority, Mobile Device Manager) are beyond the scope of the evaluation.

7.1 Secure Services:

The Cellcrypt Mobile for Secret client version 1.0 application enables encrypted peer-to-peer voice (secure Voice over Internet Protocol (VoIP)) calls between mobile handsets. The application implements the following secure services:

- Secure Client Registration and Call Signalling (data tunnel)
- Secure Session Key negotiation between the clients (voice tunnel)
- Encryption of the media stream (voice tunnel)

The application relies on authenticated connection setup over a VPN tunnel to be provided by the infrastructure.

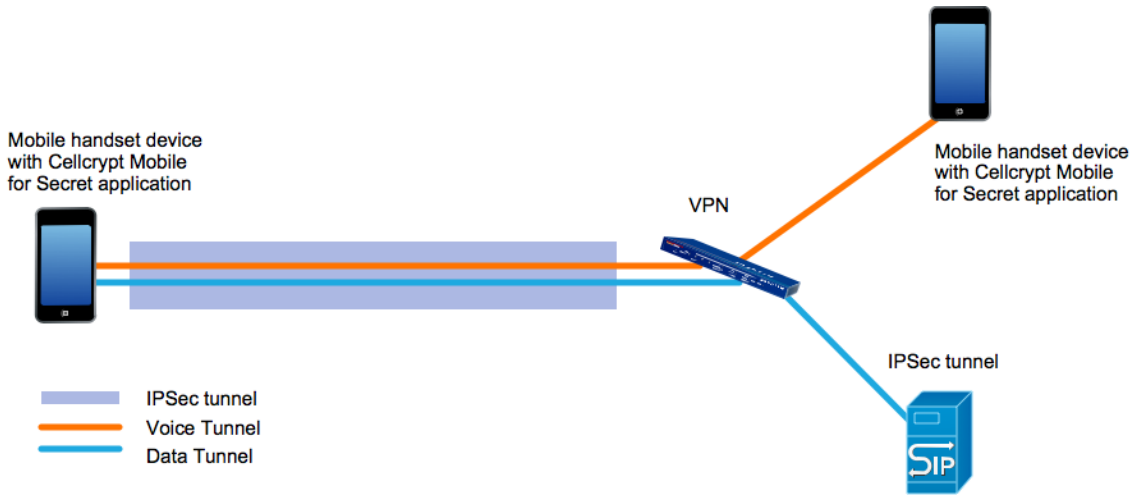

Figure 3: Two tunnels of the enterprise mobility solution encapsulated by a VPN

7.2 TOE Security functions

7.2.1 Cryptographic Support

All cryptographic functions used by the TOE, viz., implementation of SIP TLS tunnel and media encryption/decryption are performed by a FIPS 140-2 approved crypto library running in FIPS Approved mode. The Cellcrypt Mobile for Secret client version 1.0 application uses the OpenSSL FIPS Object module v2.0.5, (FIPS Certificate No. 1747), which supports all crypto functions required in the Protection Profile.

The software (TOE) will be run without modification on Android Jellybean 4.2 (API 17) running on an ARMV7 CPU with or without NEON optimization. The table below gives the corresponding FIPS/CAVP algorithm certificate numbers where applicable.

The deterministic RBG used by OpenSSL is seeded using a hardware entropy source with a minimum number of bits of entropy at least equal to the greatest bit length required by the protocols and functions supported by the TOE. Cellcrypt Mobile for Secret accumulates this hardware entropy from the phone's microphone. On initial start up of the application, the microphone is sampled for 30 seconds. The raw audio samples are combined with device entropy, and cryptographically hashed to generate the initial seed.

The OpenSSL FIPS Object Modules v2.0.5 was sourced, compiled, installed, and used in accordance to the guidance provided by the "User Guide for the OpenSSL FIPS Object Module v2.0 (including v2.0.1, v2.0.2, v2.0.3, v2.0.4, v2.0.5)", and the "OpenSSL FIPS 140-2 Security Policy". Specifically,

- The source code was obtained via "trusted path" by the vendor of record (OpenSSL Software Foundation) on physical media (CD).
- The source file openssl-fips-2.0.5.tar.gz has been verified to have the correct SHA-1 digest of 8b44f2a43d098f6858eb1ebe77b73f8f027a9c29.
- The OpenSSL FIPS Object Module has been compiled using the Android NDK, which includes gcc 4.6, using the specified build procedure.
- The FIPS_mode_set() function at runtime validates the embedded HMAC-SHA-1 digest with a digest generated from the FIPS Object Module object code.

The Cryptographic support security function is designed to satisfy the following security functional requirements as summarised 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 (covers Android 4.2 running on an ARMv7 CPU architecture with or without NEON optimizations)

	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 module to provide cryptographic functionality as required in the standards. The following mandatory ciphersuite is implemented: AES_CM_128_HMAC_SHA1_80	N/A
	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_WITH_AES_128_GCM_SHA256 using the 256-bit prime modulus elliptic curve specified in FIPS-186-2; TLS_ECDHE_ECDSA_WITH_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

Table 8: Implementation of Cryptographic Support

The TOE is designed to zeroize secret and private keys when they are no longer required by the TOE. The following table summarizes how the values are zeroized.

CSP	CSP use	Where stored	When Zeroized	How Zeroized
Symmetric key	HMAC authentication for SRTP stream	RAM	After call terminates.	Overwrite with '0' 2 times
Symmetric key	AES Encrypt/decrypt SRTP stream	RAM	After call terminates.	Overwrite with '0' 2 times
Symmetric key	Encrypt/decrypt TLS data stream to SIP Server	RAM	After TLS session terminates.	Overwrite with '0' 2 times
Private key	TLS connection to SIP Server	RAM and encrypted Flash on filesystem	RAM: after TLS session terminates. Flash: on application uninstallation.	RAM: Overwrite with '0' 2 times Flash: Mobile Device OS dependent
Seed file	Seed data for PRNG	RAM and encrypted Flash on filesystem	On application uninstallation.	Mobile Device OS dependent

Table 9: Zeroization

7.2.2 Protected communications

7.2.2.1 VPN tunnel

The Cellcrypt Mobile for Secret client version 1.0 application connects to the enterprise (SIP Server and other clients) with layered encryption and authentication. All data between Cellcrypt Mobile for Secret client version 1.0 clients and the Enterprise Infrastructure is protected in an IPSec Virtual Private Network (VPN) tunnel. The IPSec VPN connection must be established before connections to enterprise services are permitted. Within the VPN tunnel, application traffic is encrypted to provide an additional layer of protection.

7.2.2.2 Inter-TSF Trusted Channel (SDES –SRTP)

Cellcrypt Mobile for Secret client version 1.0 is a standards-based secure VoIP client, which supports SDES and SRTP. The Inter-TSF Trusted Channel (SDES-SRTP) security function is designed to satisfy the following security functional requirements: FTP_ITC.1.1(1), FTP_ITC.1.2(1), FTP_ITC.1.3(1).

The SRTP ciphers and keys are negotiated using SDES (RFC 4568), as part of the Session Description Protocol (SDP) attachment of the SIP messages. The keying information is protected by the TLS session

encrypting the SIP link, and is being exchanged between two strongly authenticated endpoints through the SIP server.

The calling client will append the SDES "crypto" header to the outgoing INVITE message, specifying its ciphersuite and encryption key. The SIP Server will process and route this message to the called client. Upon receiving an INVITE with an SDES "crypto" header, the TOE will validate that it supports the offered ciphersuite, and use the key as appropriate.
On the call being answered, the called client will append the SDES "crypto" header to the outgoing 200 OK message, specifying its ciphersuite and encryption key. The calling client will validate that it supports the offered ciphersuite, and use the key as appropriate.
Cellcrypt Mobile for Secret requires the use of SRTP (an RTP only stream is not allowable), and the NULL ciphersuite has been disabled. The only allowable ciphersuite supported by the TOE is: AES_CM_128_HMAC_SHA1_80.
If an unsupported (or NULL) ciphersuite is offered, the TOE will reject the call.

The SRTP UDP port is configurable by the enterprise. The default configuration is to use an ephemeral port (i.e. the port number used may vary per call). If an explicit port is specified in the settings, the TOE will only use the configured port value.

7.2.2.3 Inter-TSF Trusted Channel (TLS/SIP)

Cellcrypt Mobile for Secret is a standards-based secure VoIP client, which supports SIP over TLS 1.2. The Inter-TSF Trusted Channel (TLS/SIP) security function is designed to satisfy the following security functional requirements: FTP_ITC.1.1(2), FTP_ITC.1.2(2), FTP_ITC.1.3(2).

7.2.3 Identification and authentication

7.2.3.1 SIP Client

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 this regard these messages behave as 'keep alive' messages. In the evaluated default configuration, the password will need to be re-entered by the user for each REGISTER request.

The Identification and Authentication security function is designed to satisfy the following security functional requirements: FIA_SIPC_EXT.1.1, FIA_SIPC_EXT.1.2, FIA_SIPC_EXT.1.3, FIA_SIPC_EXT.1.4.

Once registered to the SIP server, the TOE is available to make or receive calls.

To initiate a call, the user dials another user's SIP address. The TOE generates a SIP INVITE request and sends it to the SIP server. The SIP server processes and routes the INVITE message (including SDP) to the called party.

On receiving an incoming INVITE request, the receiving TOE processes the message. If acceptable, and the client is available to take incoming calls, the user will be alerted by ringing the phone.
The user has the choice of rejecting the call, or accepting the call.
If the user rejects the call, a 603 "Call Declined" message is returned, and the call is torn down.
If the call is accepted, the called TOE will send back a 200 OK with SDP, and encrypted media streams are established peer-to-peer.

Once a call has been established, either side may terminate the call, which initiates a SIP BYE/200 exchange, tearing down the media streams, and the call.

7.2.3.2 X.509v3 Certificates

The TSF uses X.509v3 uses certificates to authenticate the user to the SIP server via a mutually authenticated TLS connection. Both the Users Private Key file and the certificate for the TLS connection are stored and protected by the TSF itself.

The TOE allows setting of the path for X.509v3 certificate and users Private key file for the TLS connection used by the TSF. The long-lived TLS certificates and private key are stored encrypted in the TOE private area of the filesystem on the phone's flash-memory. The private key is removed by uninstalling the application, which is the responsibility of the Mobile Device Platform, outside of the scope of the TOE. The certificates and private keys are decrypted and loaded from Flash into RAM by the TOE to use it in order to establish a TLS connection.

The TSF performs validity checks on the CA path and that either the SubjectAltName or SubjectDN match what was provided on the distant connection certificate. The TSF also performs OCSP or CRL (whichever is available) validity checks on the certificate. Connection attempts are made only if the certificate is deemed valid.

In the case where it is not possible to check the validity of the Certificate via an online check the TSF will either attempt to establish a TLS connection or not dependent on whether this is configured by the Enterprise.

The Identification and Authentication security function is designed to satisfy the following security functional requirements: FIA_X509_EXT.1.Y, FIA_X509_EXT.1.1, FIA_X509_EXT.1.2, FIA_X509_EXT.1.3, FIA_X509_EXT.1.4, FIA_X509_EXT.1.5.

7.2.4 TSF protection

7.2.4.1 Integrity of origin

Cellcrypt digitally signs the Cellcrypt Mobile for Secret application to provide integrity of origin. The operating system on the device verifies the signature whenever it installs the Cellcrypt Mobile for Secret application. Installation can complete only if this verification succeeds.

7.2.4.2 TOE software version information

The user can verify the version of Cellcrypt Mobile for Secret that is running on their device. Version and device ID information can be obtained by displaying the details in the application settings menu.

This process ensures that an administrator can verify that all updates are unaltered and from a trusted source, and it prevents:

- An adversary from making unauthorized updates to the Cellcrypt Mobile for Secret application.
- A malicious user, process, or external IT entity misrepresenting itself as the application to obtain identification and authentication data.

The TOE version information is also provided to the Android Operating System using the standard Android application APIs. The enterprise can use an MDM to obtain the version information of the TOE from the OS.

The TSF protection security function is designed to satisfy the following security functional requirement: FPT_TU D_EXT.1.1.

7.2.5 TOE Documentation

Cellcrypt offers a User and Administrator guide for the Cellcrypt Mobile for Secret client version 1.0 product. This describes how the Enterprise may Provision, Install, Configure and Operate the product

8 APPENDIX A - TERMINOLOGY AND ACRONYMS

Term	Description
AES	Advanced Encryption Standard
CA	Certificate Authority
CAVP	Cryptographic Algorithm Validation Program
CC	Common Criteria for Information Technology Security Evaluation
CIK	Crypto Ignition Key
CM	Cellcrypt Mobile
CRADA	Cooperative Research And Development Agreement
DTLS-SRTP	Datagram Transport Layer Security (DTLS) Extension to Establish Keys for Secure Real-time Transport Protocol (SRTP), (RFC 5764)
FIPS	Federal Information Processing Standard
KEK	Key Encryption Key
NAT	Network Address Translation
NIAP	National Information Assurance Partnership
NIST	National Institute of Standards and Technology
PKI	Public Key Infrastructure
PP	NIAP Protection Profiles
PRNG	Pseudo-Random Number Generator
RNG	Random Number Generator
RTP	Real Time Protocol (RFC 3550)
SDES	SDP Security Descriptions for Media Streams (RFC 4568)
SDP	Session Description Protocol (RFC 4566)
SIP	Session Initiation Protocol (RFC 3261)
SRTP	Secure Real Time Protocol (RFC 3711)
STUN	Session Traversal Utilities for NAT
SVoIP	Secure Voice over Internet Protocol
TEE	ARM Trusted Execution Environment
TOE	Target Of Evaluation
TSF	TOE Security Functions
VPN	Virtual Private Network
VoIP	Voice over Internet Protocol

9 APPENDIX B – REFERENCED DOCUMENTS

[1] Protection Profile for Mobility – Voice Over IP Application, PP_MOBILITY_VOIP_V0.6, 2013- 01 - 28.
[2] Protection Profile for Mobile Device Fundamentals, PP_MD_V1.1, 2014-02-24.
[3] Protection Profile - Network Device Protection Profile (NDPP) Extended Package SIP Server Version 1.0, 2013-02-06.
[4] NIST Special Publication 800-53 - Security and Privacy Controls for Federal Information Systems and Organizations, Revision 4, April 2013.

10 APPENDIX C – NIST SP 800-53/CNSS 1253 MAPPING

Several of the NIST SP 800-53/CNSS 1253 controls [4] are either fully or partially addressed by the TOE. This section outlines the requirements that are addressed when the TOE is incorporated into its operational configuration.

The following table is taken from the Protection Profile, [1].

Identifier	Name	Applicable SFRs
AC-4	Information Flow Enforcement	FTP_ITC.1(*)
SC-8	Transmission Integrity	FCS_COP.1(2), FCS_COP.1(3), FCS_COP.1(4), FCS_TLS_EXT.1.1, FTP_ITC.1(*), FCS_COMM_PROT_EXT.1,FCS_SIP_EXT.1, FCS_SRPT_EXT.1.1, FCS_DTLS_EXT.1
SC-9	Transmission Confidentiality	FCS_COP.1(1), FCS_SRTP_EXT.1, FCS_SIP_EXT.1, FTP_ITC.1(*), FCS_TLS_EXT.1, FCS_COMM_PROT_EXT.1, FCS_DTLS_EXT.1
SC-12	Cryptographic Key Establishment and Management	FCS_TLS_EXT.1, FCS_CKM.1, FCS_CKM_EXT.4, FCS_COMM_PROT_EXT.1, FCS_RBG_EXT.1, FCS_DTLS_EXT.1
SC-13	Use of Cryptography	FCS_COP.1(*), FIA_UAU.5, FPT_TUD_EXT.1

END OF DOCUMENT