Cisco Jabber for Android and iPhone/iPad

Security Target

Version 1.0

17 March 2017

Table of Contents

List of Tables

Acronyms

The following acronyms and abbreviations are common and may be used in this Security Target:

Table 1 Acronyms

Acronyms / Abbreviations	Definition
AES	Advanced Encryption Standard
CC	Common Criteria for Information Technology Security Evaluation
CEM	Common Evaluation Methodology for Information Technology Security
CM	Configuration Management
DRBG	Deterministic Random Bit Generator
EAL	Evaluation Assurance Level
EC-DH	Elliptic Curve-Diffie-Hellman
ECDSA	Elliptic Curve Digital Signature Algorithm
ESP	Encapsulating Security Payload
GCM	Galois Counter Mode
HMAC	Hash Message Authentication Code
IT	Information Technology
NGE	Next Generation Encryption
OS	Operating System
PP	Protection Profile
PRF	Pseudo-Random Functions
RFC	Request For Comment
SDES	Security Descriptions for Media Streams
SDP	Session Description Protocol
SHS	Secure Hash Standard
SIP	Session Initiation Protocol
SRTP	Security Real-Time Transport Protocol
ST	Security Target
TCP	Transport Control Protocol
TLS	Transport Layer Security
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Function
TSP	TOE Security Policy
UCM	Unified Communications Manager
UDP	User datagram protocol
VoIP	Voice over IP

Terminology

Table 2 Terminology

Term	Definition
Authorized Administrator	Any user which has been assigned to a privilege level that is permitted to perform all TSF-related functions.
Client Device Platform	The device (part of the Operational Environment of the TOE) on which the VoIP Application (the TOE) is installed.
CUCM	Cisco Unified Communications Manager (CUCM) serves as the software-based call-processing component of the Cisco Unified Communications family of

Term	Definition
	products. The CUCM extends enterprise telephony features and functions to packet telephony network devices such as IP phones, media processing devices, voice-over-IP (VoIP) gateways, and multimedia applications.
Security Administrator	Synonymous with Authorized Administrator for the purposes of this evaluation.
SIP Server	The SIP Server (in this evaluation it is the Cisco Unified Communications Manager (CUCM)) interacts with a VoIP client (TOE) and provides registrar and proxy capabilities required for call-session management as well as establishing, processing, and terminating VoIP calls.
User	Any entity (human user or external IT entity) outside the TOE that interacts with the TOE.

DOCUMENT INTRODUCTION

Prepared By:
Cisco Systems, Inc.
170 West Tasman Dr.
San Jose, CA 95134

This document provides the basis for an evaluation of a specific Target of Evaluation (TOE), Jabber for iPhone and Android. This Security Target (ST) defines a set of assumptions about the aspects of the environment, a list of threats that the product intends to counter, a set of security objectives, a set of security requirements, and the IT security functions provided by the TOE which meet the set of requirements. Administrators of the TOE will be referred to as administrators, Authorized Administrators, TOE administrators, semi-privileged, privileged administrators, and security administrators in this document.

REVISION HISTORY

Rev	Date	Description
1.0	March	Initial Publication

1 SECURITY TARGET INTRODUCTION

The Security Target contains the following sections:

- Security Target Introduction [Section 1]
- Conformance Claims [Section 2]
- Security Problem Definition [Section 3]
- Security Objectives [Section 4]
- IT Security Requirements [Section 5]
- TOE Summary Specification [Section 6]
- References [Section 7]

The structure and content of this ST comply with the requirements specified in the Common Criteria (CC), Part 1, Annex A, and Part 2.

1.1 ST and TOE Reference

This section provides information needed to identify and control this ST and its TOE.

Table 3 ST and TOE Identification

Name	Description
ST Title	Cisco Jabber for Android and iPhone/iPad Security Target
ST Version	1.0
Publication Date	17 March 2017
Vendor and ST Author	Cisco Systems, Inc.
TOE Reference	Cisco Jabber for Android and iPhone/iPad
TOE Software Version	11.7
Keywords	VoIP Client, Telephony

1.2 TOE Overview

The TOE is Cisco Jabber v11.7 for Android and iPhone/iPad (herein after referred to as Cisco Jabber, VoIP Client, or the TOE). Cisco Jabber is an application that provides a single, intuitive interface for integration of collaborative communications including:

- Presence - View real-time availability of co-workers and colleagues within the enterprise network.
- Instant messaging (IM) - Chat in real time using instant messaging to save time and reduce phone tag.
- Voice over Internet Protocol (VoIP), voice messaging, and video calling capabilities with the ability to escalate calls into a Cisco WebEx meeting.

The focus of the evaluation is on the VoIP capabilities of Cisco Jabber.

1.2.1 TOE Product Type

The TOE product type is a VoIP client. A VoIP client provides a protected transmission of private voice data between two endpoints.

1.2.2 Required non-TOE Hardware and Software

The TOE requires the following IT Environment Components when configured in its evaluated configuration:

Table 4 Required IT Environment Components

Component	Usage/Purpose Description
Certification Authority	This includes any IT Environment Certification Authority on the TOE network. This can be used to validate certificates.
Mobile Platform	The TOE relies on any of the following CC validated Android or Apple mobile device platforms: • iPhone 6/6Plus, iPhone 5S, iPad Mini3, iPad Mini2, iPad Air 2, iPad Air; • Samsung Galaxy S7/S7 Edge, S6/S6 Edge, Galaxy Note 5, Galaxy Tab S2
SIP Server	The Cisco Unified Communications Manager (CUCM) is the SIP Server that provides call-control and management.
Enterprise Mobility Management	The TOE relies upon Enterprise Mobility Management to enable FIPS mode and to enable certificate revocation checking on Samsung mobile platforms.
Remote VoIP Application	Peer VoIP Application that the TOE interacts with using Security Real Time Transport Protocol (SRTP).

1.3 TOE DESCRIPTION

This section provides an overview of the Cisco Jabber Target of Evaluation (TOE). The TOE is a mobile VoIP client application that protects voice data in transit across a public network between itself and a remote endpoint. The TOE implements Security Real-Time Transport Protocol (SRTP) to establish a cryptographic tunnel protecting the transmission of voice data to a remote VoIP Application. In addition, Cisco Jabber protects signaling channel communications between itself and the SIP Server by using Transport Layer Security (TLS). For SIP Server call-control and management, Cisco Jabber requires Cisco Unified Communications Manager (CUCM).

The Cisco Jabber TOE allows users in an organization to securely make, receive, and control phone calls with a variety of call-control options including mute, call transfer, call forwarding, and impromptu conferencing.

1.4 TOE Evaluated Configuration

The Cisco Jabber TOE requires a Common Criteria certified Android or Apple iOS mobile device as listed below:

Android version 6 on:

- Samsung Galaxy S7/S7 Edge
- Samsung S6/S6 Edge
- Samsung Galaxy Note 5
- Samsung Galaxy Tab S2

Refer to the Samsung Galaxy Devices with Android 6 Security Target[1] and the Samsung Galaxy S7 Devices on Android 6 Security Target[2] for information regarding the evaluated configuration requirements of the Samsung devices.

Apple iOS version 9.2 or 9.3 on:

- iPhone 6/6Plus
- iPhone 5S
- iPad Mini3
- iPad Mini2
- iPad Air 2
- iPad Air

Refer to the Apple iOS 9.2 Security Target[3] and the Apple iOS 9.3 Security Target[4] for information regarding the evaluated configuration requirements of the iPhone/iPad devices.

The TOE also requires support of Cisco Unified Communications Manager (CUCM), release 11.0 or later as the SIP Server. Cisco CUCM serves as the call-processing component for voice that includes IP telephony, mobility features and calls controls. In addition, there are configuration settings pushed to the Cisco Jabber TOE that are required in the evaluated configuration. This form of management is permitted in [VoIP PP].

The Cisco CUCM is required to deploy Cisco Jabber for *On-Premise* deployment scenario, that is one in which the Administrator set ups, manages, and maintains all services on the organization’s network. Additionally, Cisco Jabber must be deployed in *Phone Mode*, where the user's primary authentication is to Cisco Unified Communications Manager. In Phone Mode, the user is provisioned with VoIP capabilities without the functionality of presence or instant messaging (IM).

1.5 Physical Scope of the TOE

The TOE is a software-only VoIP mobile application. The underlying mobile platform, which is part of the IT environment, provides some of the security functionality required in the [VoIP PP]. This is denoted with the phrase “TOE Platform” in this Security Target.

[1] https://www.niap-ccevs.org/Product/Compliant.cfm?pid=10726
[2] https://www.niap-ccevs.org/Product/Compliant.cfm?pid=10739
[3] https://www.niap-ccevs.org/Product/Compliant.cfm?pid=10695
[4] https://www.niap-ccevs.org/Product/Compliant.cfm?pid=10725

1.6 Logical Scope of the TOE and Platform

The TOE is comprised of several security features. Each of the security features identified above consists of several security functionalities, as identified below.

- Cryptographic Support
- User Data Protection
- Identification and Authentication
- Security Management
- Protection of the TSF
- Trusted Channels

These features are described in more detail in the subsections below. In addition, the TOE implements all RFCs of the [VoIP PP], as necessary to satisfy testing/assurance measures prescribed therein.

1.6.1 Cryptographic Support

The TOE provides cryptography in support of SIP connections via 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. The TOE also protects communications between itself and the CUCM SIP Server by using a Transport Layer Security (TLS)-protected signaling channel.

The cryptographic algorithm implementation has been validated for CAVP conformance. See Table 14 in section 6 for certificate references.

The TOE Client Device Platform provides cryptography to support digital signature verification of X.509v3 certificates used to authenticate TLS and SDES/SRTP connections.

1.6.2 User Data Protection

The TOE ensures that voice data is not transmitted when a call is placed on hold, call placed on mute and when not connected.

1.6.3 Identification and authentication

The TOE performs authentication using passwords for SIP Register functions. The passwords must be at least eight (8) characters and include the use of upper and lower case characters, numbers and special characters.

The TOE Client Device Platform provides validates certificates using Online Certificate Status Protocol (OCSP). The certificates are used to support authentication for SDES/SRTP and TLS connections

1.6.4 Security Management

The TOE provides the capability to manage the following functions:

- Identify SIP Servers used for communications;
- Specify the credentials used for connections;

- Define the password requirements for SIP authentications;
- Cryptographic functionality; and
- Update to the TOE.

The TOE supports the administrative user to perform the above security relevant management functions.

The TOE Client Device Platform provides the capability to manage the following functions:

- Configure cryptographic algorithms;
- Load X5.09v3 certificates;
- Configure certificate revocation check; and
- Ability to update the TOE, and to verify the updates.

The TOE Client Device Platform supports the administrative user to perform the above security relevant management functions

1.6.5 Protection of the TSF

The TOE protects against interference and tampering by untrusted subjects by implementing authentication and access controls to limit configuration the administrative user.

The TOE is able to verify any software updates prior to the software updates being installed on the TOE to avoid the installation of unauthorized software.

The TOE Client Device Platform protects against interference and tampering by untrusted subjects by implementing authentication and access controls to limit configuration to the administrative user.

1.6.6 Trusted path/Channels

The TOE allows secure communications between itself and a remote VoIP application using SDES-SRTP.

The TOE allows secure communications between itself and a remote CUCM SIP Server using TLS.

1.7 Excluded Functionality

The following functionality is excluded from the evaluation.

Table 5 Excluded Functionality

Excluded Functionality	Exclusion Rationale
Non-FIPS 140-2 mode of operation	This mode of operation includes non-FIPS allowed operations.
Presence, instant messaging (IM), voice messaging, and video functionality.	These functions are not covered in the CC evaluation.

These services will be disabled by configuration. The exclusion of this functionality does not affect compliance to the Protection Profile for Voice Over IP (VoIP) Applications, version 1.3.

2 CONFORMANCE CLAIMS

2.1 Common Criteria Conformance Claim

The TOE and ST are compliant with the Common Criteria (CC) Version 3.1, Revision 4, dated: September 2012. For a listing of Assurance Requirements claimed see section 5.6.

The TOE and ST are CC Part 2 extended and CC Part 3 conformant.

2.2 Protection Profile Conformance

The TOE and ST are conformant with the Protection Profiles as listed in Table 6 below:

Table 6 Protection Profiles

Protection Profile	Version	Date
Protection Profile for Voice Over IP (VoIP) Applications	1.3	3 November 2014

This ST applies the following NIAP Technical Decisions:

- TD0068: Addition of SRTP Ciphersuites
- TD0079: RBG Cryptographic Transitions per NIST SP 800-131A Revision 1
- TD0088: Revision to FDP_VOP_EXT.1.1 in VoIP PP v1.3
- TD0106: Removing SDES/SRTP from FIA_X509_EXT.2

2.3 Protection Profile Conformance Claim Rationale

2.3.1 TOE Appropriateness

The TOE provides all of the functionality at a level of security commensurate with that identified in the U.S. Government Protection Profile:

- Protection Profile for Voice Over IP (VoIP) Applications, Version 1.3

2.3.2 TOE Security Problem Definition Consistency

The Assumptions, Threats, and Organizational Security Policies included in the Security Target represent the Assumptions, Threats, and Organizational Security Policies specified in the Protection Profile for Voice Over IP (VoIP) Applications, Version 1.3 for which conformance is claimed verbatim. All concepts covered in the Protection Profile Security Problem Definition are included in the Security Target Statement of Security Objectives Consistency.

The Security Objectives included in the Security Target represent the Security Objectives specified in the VoIP PPv1.3 for which conformance is claimed verbatim. All concepts covered in the Protection Profile's Statement of Security Objectives are included in the Security Target.

2.3.3 Statement of Security Requirements Consistency

The Security Functional Requirements included in the Security Target represent the Security Functional Requirements specified in the VoIP PPv1.3 for which conformance is claimed verbatim. All concepts covered in the Protection Profile’s Statement of Security Requirements are included in this Security Target. Additionally, the Security Assurance Requirements included in this Security Target are identical to the Security Assurance Requirements included in VoIP PPv1.3.

3 SECURITY PROBLEM DEFINITION

This section identifies the following:

- Significant assumptions about the TOE's operational environment.
- IT related threats to the organization countered by the TOE.
- Environmental threats requiring controls to provide sufficient protection.
- Organizational security policies for the TOE as appropriate.

This document identifies assumptions as A.assumption with "assumption" specifying a unique name. Threats are identified as T.threat with "threat" specifying a unique name. Organizational Security Policies (OSPs) are identified as P.osp with "osp" specifying a unique name.

3.1 Assumptions

The specific conditions listed in the following subsections are assumed to exist in the TOE's environment. These assumptions include both practical realities in the development of the TOE security requirements and the essential environmental conditions on the use of the TOE.

Table 7 TOE Assumptions

Assumption	Assumption Definition
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_CONFIG	Personnel configuring the TOE and its operational environment will follow the applicable security configuration guidance.

3.2 Threats

The following table lists the threats addressed by the TOE and the IT Environment. The assumed level of expertise of the attacker for all the threats identified below is Enhanced-Basic.

Table 8 Threats

Threat	Threat Definition
T.TSF_CONFIGURATION	Failure to allow configuration of the TSF may prevent its users from being able to adequately implement their particular security policy, leading to a compromise of user information.
T.TSF_FAILURE	Security mechanisms of the TOE may fail, leading to a compromise of the TSF.
T.UNAUTHORIZED_ACCESS	A user may gain unauthorized access to the TOE data. 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

Threat	Threat Definition
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.
T.USER_DATA_REUSE	Voice data may be inadvertently sent to a destination not intended because it is sent outside the voice call.

3.3 Organizational Security Policies

The VoIP PPv1.3 does not define organizational security policies.

4 SECURITY OBJECTIVES

This section identifies the security objectives of the TOE and the IT Environment. The security objectives identify the responsibilities of the TOE and the TOE's IT environment in meeting the security needs.

- This document identifies objectives of the TOE as O.objective with objective specifying a unique name. Objectives that apply to the IT environment are designated as OE.objective with objective specifying a unique name.

4.1 Security Objectives for the TOE

The following table, Security Objectives for the TOE, identifies the security objectives of the TOE. These security objectives reflect the stated intent to counter identified threats and/or comply with any security policies identified. An explanation of the relationship between the objectives and the threats/policies is provided in the rationale section of this document.

Table 9 Security Objectives for the TOE

TOE Objective	TOE Security Objective Definition
O.PROTECTED_COMMUNICATIONS	The TOE will provide protected communication channels with authorized IT entities (SIP Server and other VoIP applications).
O.TSF_SELF_TEST	The TOE will provide the capability to test some subset of its security functionality to ensure it is operating properly.
O.VERIFIABLE_UPDATES	The TOE will provide the capability to help ensure that any updates to the TOE can be verified by the administrator to be unaltered and (optionally) from a trusted source.

4.2 Security Objectives for the Environment

All of the assumptions stated in section 3.1 are considered to be security objectives for the environment. The following are the Protection Profile 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.

Table 10 Security Objectives for the Environment

Environment Security Objective	IT Environment Security Objective Definition
OE.AUTHORIZED_USER	The user of the TOE is non-hostile and follows all user guidance.
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.

Environment Security Objective	IT Environment Security Objective Definition
OE.TRUSTED_ADMIN	TOE Administrators are trusted to follow and apply all administrator guidance in a trusted manner.

5 SECURITY REQUIREMENTS

This section identifies the Security Functional Requirements for the TOE. The Security Functional Requirements included in this section are derived from Part 2 of the Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 4, dated: September 2012 and all international interpretations.

5.1 Conventions

The CC defines operations on Security Functional Requirements: 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 within brackets;
- Refinement: Indicated with **bold** text;
- Selection: Indicated with [<u>underlined</u>] text within brackets;
- 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. Formatting conventions outside of operations and iterations matches the formatting specified within the NDPP.

5.2 TOE Security Functional Requirements

This section identifies the Security Functional Requirements for the TOE. The TOE Security Functional Requirements that appear in the following table are described in more detail in the following subsections.

Table 11 Security Functional Requirements

Class Name	Component Identification	Component Name
Security Functional Requirements for VoIP Applications (TOE)		
FCS: Cryptographic support	FCS_CKM_EXT.2(1)	Cryptographic Key Storage
	FCS_SRTP_EXT.1	Secure Real-Time Transport Protocol (SRTP)
FDP: User data protection	FDP_VOP_EXT.1	Voice Over IP Data Protection
FIA: Identification and authentication	FIA_SIPC_EXT.1	Session Initiation Protocol (SIP) Client
FMT: Security Management	FMT_SMF.1	Specification of Management Functions
FPT: Protection of the TSF	FPT_TUD_EXT.1	Extended: Trusted Update
FTP: Trusted path/channels	FTP_ITC.1(1)	Inter-TSF Trusted Channel (SDES-SRTP)
Security Functional Requirements for VoIP Client Applications or Client Platforms		
FCS: Cryptographic support	FCS_CKM.1(1)	Cryptographic Key Generation (Asymmetric Keys)
	FCS_CKM.1(2)	Cryptographic Key Generation
	FCS_CKM_EXT.4	Cryptographic key material destruction (Key Material)
	FCS_COP.1(1)	Cryptographic Operation (Data Encryption/Decryption)
	FCS_COP.1(2)	Cryptographic Operation (for cryptographic signature)

Class Name	Component Identification	Component Name
	FCS_COP.1(3)	Cryptographic Operation (for cryptographic hashing)
	FCS_COP.1(4)	Cryptographic Operation (For keyed-hash Message Authentication)
	FCS_RBG_EXT.1	Extended: Cryptographic operation (Random Bit Generation)
	FCS_TLS_EXT.1	Transport Level Security
FIA: Identification and authentication	FIA_X509_EXT.1	Extended: X509 Certificate Validation
	FIA_X509_EXT.2(1)	Extended: X509 Certificate Use and Management
	FIA_X509_EXT.2(2)	Extended: X509 Certificate Use and Management
FMT: Security management	FMT_SMF.1	Specification of Management Functions
FPT: Protection of the TSF	FPT_TST_EXT.1	Extended: TSF Self Test
	FPT_TUD_EXT.1	Extended: Trusted Update
FTP: Trusted Path/Channels	FTP_ITC.1(2)	Inter-TSF Trusted Channel (TLS/SIP)

5.3 SFRs Drawn from VoIP PP for VoIP Applications (TOE)

5.3.1 Cryptographic Support (FCS)

FCS_CKM.2(1) Refinement: Cryptographic Key Storage / FCS_CKM_EXT.2(1) Cryptographic Key Storage

FCS_CKM_EXT.2.1(1) The VoIP client application shall store persistent secrets and private keys when not in use in platform-provided key storage.

FCS_SRTP_EXT.1 Secure Real-Time Transport Protocol (SRTP)

FCS_SRTP_EXT.1.1 The VoIP client application 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 VoIP client application shall implement SDES-SRTP supporting the following ciphersuites: AES_CM_128_HMAC_SHA1_80 in accordance with RFC 4568 and [AEAD_AES_256_GCM in accordance with RFC 7714].

Application Note: *The above SFR applies NIAP Technical Decision TD0068*

FCS_SRTP_EXT.1.3 The VoIP client application shall ensure the SRTP NULL algorithm can be disabled.

FCS_SRTP_EXT.1.4 The VoIP client application shall allow the SRTP ports to be used for SRTP communications to be specified by an Authorized Administrator.

5.3.2 User data protection (FDP)

FDP_VOP_EXT.1 Voice Over IP Data Protection

FDP_VOP_EXT.1.1 The VoIP Client Application shall stop the transmission of voice data when a VoIP call is placed on mute, a VoIP call is not connected, [a VoIP call is placed on hold] and [*no other actions*].

Application Note: *The above SFR applies NIAP Technical Decision TD0088*

5.3.3 Identification and authentication (FIA)

FIA_SIPC_EXT.1 Session Initiation Protocol (SIP) Client

FIA_SIPC_EXT.1.1 The VoIP client application 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 VoIP client application 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 VoIP client application 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 supported special characters*]}.

FIA_SIPC_EXT.1.4 The password entered by the user as per FIA_SIPC_EXT.1.2 shall be cleared by the VoIP client application once the VoIP client application is notified that the REGISTER request was successful.

5.3.4 Security management (FMT)

FMT_SMF.1 Specification of Management Functions

FMT_SMF.1.1 The VoIP client application shall be capable of performing the following management functions:

- Specify the SIP Server to use for connections,
- Specify VoIP client credentials to be used for connections,
- Specify password requirements for SIP authentication,
- Ability to configure all security management functions identified in other sections of this PP,
- [no other functions].

5.3.5 Protection of the TSF (FPT)

FPT_TUD_EXT.1 Extended: Trusted Update

FPT_TUD_EXT.1.1 The TSF shall provide the client device platform the ability to query the current version of the TOE firmware/software.

5.3.6 Trusted Path/Channels (FTP)

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

FTP_ITC.1.1(1) Refinement: The VoIP Client Application 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 VoIP Client Application shall permit the TSF or the remote VoIP application to initiate communication via the trusted channel.

FTP_ITC.1.3(1) The VoIP Client Application shall initiate communication via the trusted channel for [*all communications between the two devices*].

5.4 SFRs from the VoIP PP VoIP Client Applications or Client Platforms

5.4.1 Cryptographic Support (FCS)

FCS_CKM.1(1) Cryptographic Key Generation (Asymmetric Keys)

FCS_CKM.1.1(1) Refinement: The [VoIP client application] **shall generate asymmetric** cryptographic keys **used for key establishment** in accordance with:

- NIST Special Publication 800-56B, “Recommendation for Pair-Wise Key Establishment Schemes Using Integer Factorization Cryptography” for RSA-based key establishment schemes and
- [No other algorithms]

and specified cryptographic key sizes equivalent to, or greater than, a symmetric key strength of 112 bits.

FCS_CKM.1(2) Cryptographic Key Generation

FCS_CKM.1.1(2) Refinement: The [VoIP client application] shall generate **asymmetric** cryptographic keys **used for authentication** in accordance with a specified cryptographic key generation algorithm [

- FIPS PUB 186-4, “Digital Signature Standard (DSS)”, Appendix B.3 for RSA schemes;]

and specified cryptographic key sizes *equivalent to, or greater than, a symmetric key strength of 112 bits.*

FCS_CKM_EXT.4 Cryptographic key material destruction (Key Material)

FCS_CKM_EXT.4.1 Refinement: The [VoIP client application, client device platform] shall zeroize all plaintext secret and private cryptographic keys and Critical Security Parameters (CSPs) when no longer required.

FCS_COP.1(1) Cryptographic Operation (Data Encryption/Decryption)

FCS_COP.1.1(1) Refinement: The [VoIP client application, client device platform] shall perform *encryption and decryption* in accordance with a specified cryptographic algorithm AES operating in **CTR, CBC,** and [GCM (as defined in NIST SP800-38D), [no other modes] and cryptographic key sizes 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 SP800-38D

FCS_COP.1(2) Cryptographic Operation (for cryptographic signature)

FCS_COP.1.1(2) Refinement: The [client device platform] shall perform **cryptographic signature services (generation and verification)** in accordance with a specified cryptographic algorithm

- **FIPS PUB 186-4, “Digital Signature Standard (DSS)”, Appendix B.3 for RSA schemes**

[

- FIPS PUB 186-4, “Digital Signature Standard (DSS)”, Appendix B.4 for Elliptic Curve Digital Signature Algorithm (ECDSA) schemes and implementing “NIST curves” P-256, P-384, and [no other curves]
- No other algorithms]

and cryptographic key sizes [**equivalent to, or greater than, a symmetric key strength of 112 bits**].

FCS_COP.1(3) Cryptographic Operation (for cryptographic hashing)

FCS_COP.1.1(3) **Refinement:** The [VoIP client application, client device platform] shall perform **cryptographic hashing** in accordance with a specified cryptographic algorithm SHA-1 and [SHA-256, SHA-384] and [no other algorithms] and **message digest sizes** 160 bits and [256, 384] and [no other message digest sizes] 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 [VoIP client application] shall perform *keyed-hash message authentication* in accordance with a specified cryptographic algorithm *HMAC-SHA-1 and*

[HMAC-SHA-256, HMAC- SHA-384] and cryptographic key sizes [*160, 256, 384*], **and message digest sizes 160 and** [256, 384] 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 [client device platform] shall perform all deterministic random bit generation services in accordance with *NIST Special Publication 800-90A using* [CTR_DRBG (AES)].

Application Note*: The above SFR applies NIAP Technical Decision TD0079*

FCS_RBG_EXT.1.2 The deterministic RBG shall be seeded by an entropy source that accumulates entropy from [a platform-based RBG] with a minimum of [256 bits] of entropy at least equal to the greatest security strength (according to NIST SP 800-57) of the keys and hashes that it will generate.

FCS_TLS_EXT.1 Transport Level Security

FCS_TLS_EXT.1.1 The [VoIP client application] shall implement one or more of the following protocols [TLS 1.0 (RFC 2246), TLS 1.2 (RFC 5246)] using mutual authentication with certificates and supporting the following ciphersuites:

Mandatory Ciphersuites:
TLS_RSA_WITH_AES_128_CBC_SHA

Optional Ciphersuites:
[
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289
TLS_ECDHE_RSA_WITH _AES_256_GCM_SHA384 as defined in RFC 5289
].

FCS_TLS_EXT.1.2 The [VoIP client application] shall not establish a trusted channel if the distinguished name (DN) contained in a certificate does not match the expected DN for the peer.

5.4.2 Identification and authentication (FIA)

FIA_X509_EXT.1 Extended: X509 Certificate Validation

FIA_X509_EXT.1.1 The [client device platform] shall validate certificates in accordance with the following rules:

- RFC 5280 certificate validation and certificate path validation.
- Validate the certificate path by ensuring the basicConstraints extension is present and the cA flag is set to TRUE for all CA certificates.

- Validate the revocation status of the certificate using [the Online Certificate Status Protocol (OCSP) as specified in RFC 2560, a Certificate Revocation List (CRL) as specified in RFC 5759].
- Validate the extendedKeyUsage field according to the following rules:
  - Certificates used for trusted updates and executable code integrity verification shall have the Code Signing purpose (id-kp 3 with OID 1.3.6.1.5.5.7.3.3).
  - Server certificates presented for TLS shall have the Server Authentication purpose (id-kp 1 with OID 1.3.6.1.5.5.7.3.1) in the extendedKeyUsage field.

FIA_X509_EXT.1.2 The [client device platform] shall only treat a certificate as a CA certificate if the basicConstraints extension is present and the CA flag is set to TRUE.

FIA_X509_EXT.2 (1) Extended: X509 Certificate Use and Management

FIA_X509_EXT.2.1(1) The [client device platform] shall use X.509v3 certificates as defined by RFC 5280 to support authentication for TLS and [no additional uses].

FIA_X509_EXT.2.2(1) When the [client device platform] cannot establish a connection to determine the validity of a certificate, the [VoIP client Application] shall [accept the certificate].

FIA_X509_EXT.2.3(1) The [client device platform] shall not establish a trusted communication channel if the peer certificate is deemed invalid.

***Application Note**: The above SFR iteration applies to iOS platforms*

FIA_X509_EXT.2 (2) Extended: X509 Certificate Use and Management

FIA_X509_EXT.2.1(2) The [client device platform] shall use X.509v3 certificates as defined by RFC 5280 to support authentication for TLS and [no additional uses].

FIA_X509_EXT.2.2(2) When the [client device platform] cannot establish a connection to determine the validity of a certificate, the [VoIP client Application] shall [allow the administrator to choose whether to establish or not establish the trusted channel in these cases].

FIA_X509_EXT.2.3(2) The [client device platform] shall not establish a trusted communication channel if the peer certificate is deemed invalid.

***Application Note**: The above SFR iteration applies to Android platforms*

5.4.3 Security management (FMT)

FMT_SMF.1 Specification of Management Functions

FMT_SMF.1.1 The [VoIP client Application, client device platform] shall be capable of performing the following management functions:

- Configure cryptographic algorithms associated with protocols mandated in this PP,
- Load X5.09v3 certificates used for security functions in this PP,
- Configure certificate revocation check,
- Ability to update the TOE, and to verify the updates
- Ability to configure all security management functions identified in other sections of this PP,
- [no other actions].

5.4.4 Protection of the TSF (FPT)

FPT_TST_EXT.1 Extended: TSF Self Test

FPT_TST_EXT.1.1 The [VoIP Client Application] shall run a suite of self tests during initial start-up (on power on) to demonstrate correct operation of the TSF.

FPT_TST_EXT.1.2 The [VoIP Client Application] shall provide the capability to verify the integrity of stored TSF executable code when it is loaded for execution through the use of the TSF-provided cryptographic services.

FPT_TUD_EXT.1 Extended: Trusted Update

FPT_TUD_EXT.1.2 The [client device platform] shall provide authorized administrators the ability to initiate updates to the TOE firmware/software.

FPT_TUD_EXT.1.3 The [client device platform] shall provide a means to verify firmware/software updates to the TOE using a digital signature mechanism and [no other functions] prior to installing those updates.

5.4.5 Trusted Path/Channels (FTP)

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

FTP_ITC.1.1(2) Refinement: The [VoIP Client Application] 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 disclosure.

FTP_ITC.1.2(2) The [VoIP Client Application] shall permit the TSF to initiate communication via the trusted channel.

FTP_ITC.1.3(2) The [VoIP Client Application] shall initiate communication via the trusted channel for [all communications with the SIP server].

5.5 TOE SFR Dependencies Rationale for SFRs Found in PP

The Security Functional Requirements (SFRs) in this Security Target represent the SFRs identified in the VoIP PPv1.3. As such, the VoIP PPv1.3 SFR dependency rationale is deemed acceptable since the PP itself has been validated.

5.6 Security Assurance Requirements

5.6.1 SAR Requirements

The TOE assurance requirements for this ST are taken directly from the NDPP which are derived from Common Criteria Version 3.1, Revision 4. The assurance requirements are summarized in the table below.

Table 12: Assurance Measures

Assurance Class	Components	Components Description
Development	ADV_FSP.1	Basic Functional Specification
Guidance Documents	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative User guidance
Life Cycle Support	ALC_CMC.1	Labeling of the TOE
	ALC_CMS.1	TOE CM coverage
Tests	ATE_IND.1	Independent testing - conformance
Vulnerability Assessment	AVA_VAN.1	Vulnerability analysis

5.6.2 Security Assurance Requirements Rationale

The Security Assurance Requirements (SARs) in this Security Target represent the SARs identified in the VoIP PPv1.3. As such, the VoIP PPv1.3 SAR rationale is deemed acceptable since the PP itself has been validated.

5.7 Assurance Measures

The TOE satisfies the identified assurance requirements. This section identifies the Assurance Measures applied by Cisco to satisfy the assurance requirements. The table below lists the details.

Table 13 Assurance Measures

Component	How requirement will be met
ADV_FSP.1	There are no specific assurance activities associated with ADV_FSP.1. The requirements on the content of the functional specification information are implicitly assessed by virtue of the other assurance activities being performed. The functional specification is comprised of the information contained in the AGD_OPE and AGD_PRE documentation, coupled with the information provided in the TSS of the ST. The assurance activities in the functional requirements point to evidence that should exist in the documentation and TSS section; since these are directly associated with the SFRs, the tracing in element ADV_FSP.1.2D is implicitly already done and no additional documentation is necessary.
AGD_OPE.1	The Administrative Guide provides the descriptions of the processes and procedures of how the administrative users of the TOE can securely administer the TOE using the interfaces that provide the features and functions detailed in the guidance.
AGD_PRE.1	The Installation Guide describes the installation, generation, and start-up procedures so that the users of the TOE can put the components of the TOE in the evaluated configuration.
ALC_CMC.1	

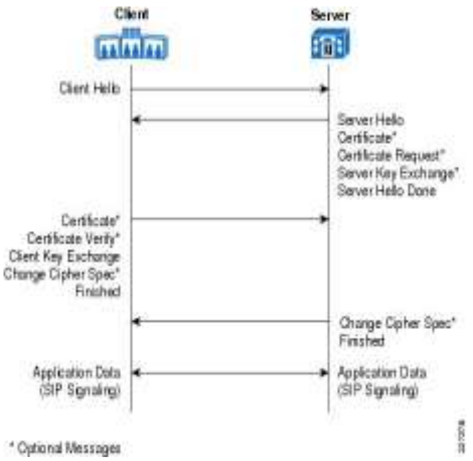
Component	How requirement will be met
ALC_CMS.1	The AGD and ST implicitly meet this assurance requirement. The evaluator shall check the ST to ensure that it contains an identifier (such as a product name/version number) that specifically identifies the version that meets the requirements of the ST. Further, the evaluator shall check the AGD guidance and TOE samples received for testing to ensure that the version number is consistent with that in the ST.
ATE_IND.1	Cisco provided the TOE for testing and, in coordination with the evaluation team, determined that the TOE was suitable for testing. All information provided met the requirements for content and presentation of evidence and testing was successfully completed based upon the requirements of the PP.
AVA_VAN.1	Cisco provided the TOE for testing and it was determined to be suitable for completion of the requirements. All information provided met the requirements for content and presentation of evidence. The evaluation team conducted a public search of potential vulnerabilities and ensured no issues resulted in a potential risk to the end user(s).

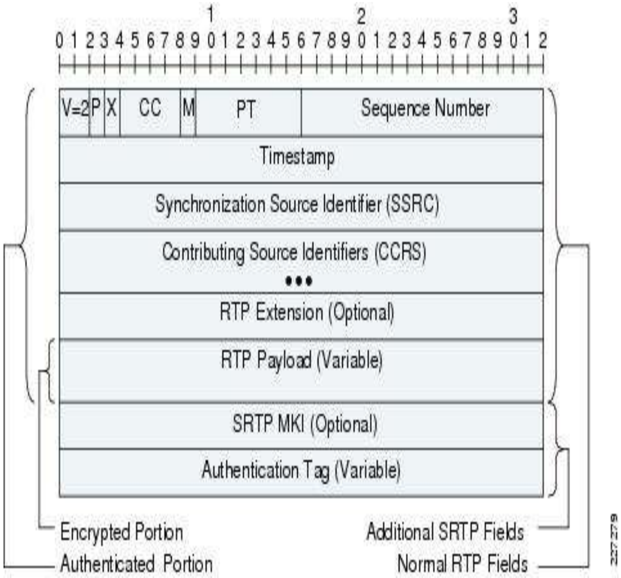
6 TOE SUMMARY SPECIFICATION

6.1 TOE Security Functional Requirement Measures

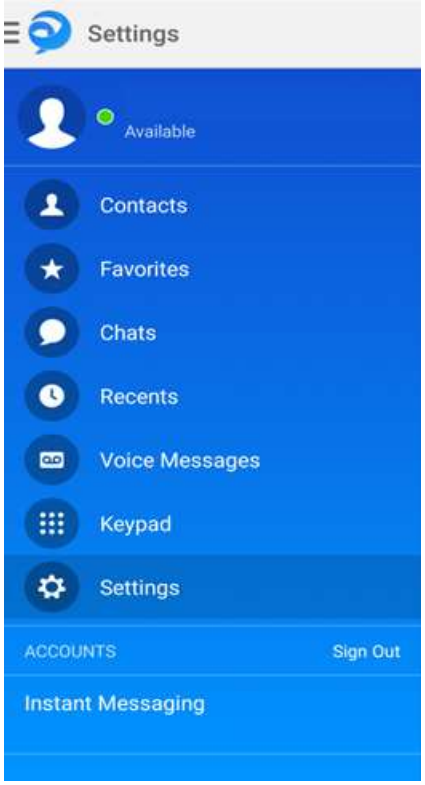
This section identifies and describes how the Security Functional Requirements identified above are met by the TOE.

Table 14 How TOE SFRs are Met

TOE SFRs	How the SFR is Met
Security Functional Requirements for VoIP Applications (TOE)	
FCS_CKM_EXT.2(1)	During the initial configuration and setup, the Jabber certificate with its private key is generated. The private key and credentials are securely stored in the Android KeyStore or iOS Keychain on the respective mobile device platform. The mobile device platform includes a key isolation service that is designed specifically to host secret and private keys in a protected process to mitigate tampering or access to sensitive key materials. Jabber also stores the user's name, password, and related information for the authentication service for the CUCM SIP Server in the iOS Keychain or Android KeyStore. There is no interface available to access to this file. The user only presents the credentials during the initial configuration, after which time the Client Platform manages the credentials. The storage and encryption process is also managed and performed by the Client Platform. The Jabber certificate with its private key as described above is also used for mutually authenticated SIP/TLS connections between the TOE and CUCM SIP Server.
FCS_SRTP_EXT.1	Incoming and outgoing calls are handled the same per RFC4568. Following is an overview of the TLS handshake, noting the client in the diagram is the TOE and Server is the CUCM SIP Server.  Client Server Client Hello Server Hello Certificate* Certificate Request* Server Key Exchange* Server Hello Done Certificate* Certificate Verify* Client Key Exchange Change Cipher Spec* Finished Change Cipher Spec* Finished Application Data (SIP Signaling) Application Data (SIP Signaling) * Optional Messages The TLS Handshake protocol layer is designed to operate in a lock-step manner, meaning that messages received in incorrect order will cause the - handshake to fail. The TOE must be configured to support an encrypted secure connection. This configuration is pushed to the TOE by the CUCM SIP Server. Therefore the TOE, will then establish an encrypted secure signaling connection with CUCM SIP Server using the SRTP protocol. This is provided through the use of encryption and message authentication headers.

TOE SFRs	How the SFR is Met
	SRTP Packet Format  1 2 3 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 V=2 P X CC M PT Sequence Number Timestamp Synchronization Source Identifier (SSRC) Contributing Source Identifiers (CCRS) ••• RTP Extension (Optional) RTP Payload (Variable) SRTP MKI (Optional) Authentication Tag (Variable) Encrypted Portion Authenticated Portion Additional SRTP Fields Normal RTP Fields 227279 The following example are the fields that appear within a normal RTP packet: • *Version (V)*—2-bit field indicating the protocol version. • *Padding (P)*—1-bit field indicating padding at the end of the RTP packet. • *Extension Header (X)*—1-bit field indicating the presence of an optional extension header. • *Marker (M)*—1-bit marker bit, used to identify events such as frame boundaries. • *Payload Type (PT)*—7-bit field which identifies the format of the RTP payload. • *Sequence Number*—16-bit field which increments by one for each RTP packet sent. This field can be used by the receiver to identify lost packets. • *Timestamp*—32-bit field which reflects the sampling instant of the first octet of the RTP packet. • *Synchronization Source Identifier (SSRC)*—32-bit field which uniquely identifies the source of a stream of RTP packets. • *Contributing Source Identifiers (CSRCs)*—Variable length field which contains a list of sources of streams of RTP packets that have contributed to a combined stream produced by an RTP mixer. • *RTP Extension (Optional)*—Variable length field which contains a 16-bit profile specific identifier and a 16-bit length identifier, followed by variable length extension data. • *RTP Payload*—Variable length field which holds the real-time application data (i.e. voice, video, etc). SRTP adds the following two additional fields to the packet: • *Master Key Identifier (MKI)*—Optional field of configurable length, used to indicate the master key, from which the individual session keys were derived for encryption and/or authentication, within a given cryptographic context.

TOE SFRs	How the SFR is Met
	- *Authentication Tag*—Recommended field of configurable length, used to hold the message authentication data for the RTP header and payload for the particular packet. With SRTP, encryption applies only to the payload of the RTP packet. Message authentication, however, is applied to both the RTP header as well as the RTP payload. Since message authentication applies to the RTP sequence number within the header, SRTP indirectly provides protection against replay attacks. In the evaluated configuration, the TOE is configured for a secure connection with CUCM SIP Server, the TOE returns its certificates when client certificate is requested during TLS handshake. When the TOE receives CUCM SIP Server certificates during the TLS handshake, the TOE ensures that the received certificate is the same as the CUCM SIP Server certificate in its truststore. The TOE relies upon the mobile device platform to perform certificate authentication and validation. In the evaluated configuration the SIP session is established over TLS, during the negotiation, Jabber offers all the SRTP ciphers it supports. The CUCM SIP Server is responsible for the configuration of the policy regarding which ciphers are acceptable, including what to do when no cipher can be negotiated. The CUCM SIP Server has configuration settings per-device to require all calls to be secure. The TOE cannot override this configuration as it is pushed from the CUCM SIP Server. Therefore when the administrator of the CUCM SIP Server selects 'Authenticated' as the value for the Device Security Mode field on the phone security profile, the SIP connection is over TLS using NULL-SHA encryption. However when the administrator of the CUCM SIP Server selects 'Encrypted' as the value for the Device Security Mode field on the phone security profile, the SIP connection is over TLS using AES 128 or AES 256 or SHA encryption. As a result, when the CUCM SIP Server is configured to only allow secure/encrypted calls, then TOE must also be set 'encrypt' otherwise the calls would fail if the TOE was set to 'authenticate' using NULL-SHA encryption. The evaluated configuration must be set to 'secure/encrypted calls'. The key is generated randomly by the client platform when building its SDP offer. The TOE supports AES_CM_128_HMAC_SHA1_80 and AEAD_AES_256_GCM.
FDP_VOP_EXT.1	The following diagram is an example of Jabber for Android and iPhone/iPad 'hub window'.

TOE SFRs	How the SFR is Met
	 Settings Available Contacts Favorites Chats Recents Voice Messages Keypad Settings ACCOUNTS Sign Out Instant Messaging There are several features that suspend or stop voice media on a call; such as setting the call to park, on hold, transfer, or end call. Call Park is conceptually similar to Hold, except the call can also be retrieved from elsewhere if the park slot is known and if Park has been enabled by the administrator. When a call is placed on voice mute (silence), SRTP is not stopped, but voice data from the microphone is no longer being sent. Instead, silence or comfort noise packets are sent depending on the configuration settings by CUCM SIP Server. From the in-call view, tap the 'Mute' icon to mute the voice audio. Selecting the 'Mute' icon again will unmute. When on mute, the TOE audio component is no longer transmitting a signal. Hold always results in the existing SRTP streams being stopped and new SRTP streams (with new keys) being negotiated over SIP/SDP with the Music on Hold service. From the in-call view, tap 'More' icon, then selecting 'Hold" will place the call on hold or resume the call. Transfer always results in the existing SRTP streams being stopped and new SRTP streams (with new keys) being negotiated over SIP/SDP with the new remote party. From the in-call view, tap 'More' icon, then tap 'Transfer, then enter the number you wish to transfer the call to and tap 'Call'. End the call by selecting the telephone icon, sends a SIP BYE (or CANCEL if it occurs very early in the call) and always stops the SRTP streams. For all these functions, the implementation is via SIP and SDP messaging, and the SDP messaging includes the necessary crypto options. Any change of participant results in re-keying.

TOE SFRs	How the SFR is Met
FIA_SIPC_EXT.1	Passwords are enforced by the CUCM SIP Server; password policy is configured and enforced as configured on the CUCM SIP Server. For the user-entered password, a minimum of eight (8) characters is required and all of the following characters are supported (letters a-z (upper and lower case), numbers (0-9) and special characters ("!", "@", "#", "$", "%", "^", "&", "*", "(", and ")",). The password is entered by the user when requested by the CUCM SIP Server to register and complete the call. The password is passed to the CUCM SIP REGISTER that will be kept in a SecureString which uses platform-specific means to guard the credential while it is memory, except for the instant when it is actually used to perform an operation. Once the call is completed (ended), the memory space holding the password is zeroized and released for use by other functions. For outgoing calls, ports are reserved for media (as configured by the CUCM SIP Server (5060 for SIP call signalling and 5061 for Secure SIP call signalling))), then the build SDP (SIP Session Description Protocol (SDP) messages (sometimes referred to as Security Descriptions or SDES) to exchange keying material within the call signalling during call establishment) and send an INVITE with the SDP and then sends a 180 Ringing message. When the user answers, then send a 200 Ok with the SDP. For incoming calls, the TOE receives an INVITE, to which it respond immediately with 100 Trying, reserve ports for media, build the SDP and send a 180 Ringing message. When the user answers, we send a 200 Ok with the SDP.
FMT_SMF.1	The TOE retrieves its configuration from the CUCM SIP Server. The CUCM SIP Server administrator configures the access to manage the VoIP client (TOE). The CUCM SIP Server pushes the required configuration settings for establishing secure connections to the prescribed CUCM SIP Server. This is to ensure organizational policies and settings are applied and enforced accordingly. The VoIP client (TOE) provides limited security management functions listed below and described in guidance documentation: • The TOE provides the ability to prompt/specify the SIP Server to use for connections. • The TOE provides the ability to prompt/specify VoIP credentials to be used for connections. • The TOE provides the ability to prompt/specify password credentials for SIP authentication.
FPT_TUD_EXT.1	TOE versioning can be queried by the user through the TOE Platform. If updates are made available by Cisco, the user can obtain an updated version of the TOE from the mobile app store.
FTP_ITC.1(1)	There is no direct admin or user interaction on Jabber to configure or set the SRTP channel. The CUCM SIP Server administrator configures appropriately, and then each time a call is made the clients automatically start SRTP streams as negotiated. There is no user or admin interaction per-SRTP-channel. The CUCM SIP Server administrator can configure the port ranges for the voice and video streams. If network loss on the SRTP sessions occurs, the TOE automatically attempts to recover. If the user remains dissatisfied with the result, they can end the call and redial. The communication is initiated on the TOE by the user dialling a number or the SIP URI.
Security Functional Requirements for VoIP Client Applications or Client Platforms	
FCS_CKM.1(1)	

<table>
<tr><th>TOE SFRs</th><th>How the SFR is Met</th></tr>
<tr><td>FCS_CKM.1(2)</td><td>
<p>To support key establishment and authentication for TLS and SRTP/SDES connections, the TOE generates asymmetric keys using RSA-based key establishment schemes conformant to NIST Special Publication 800-56B and FIPS PUB 186-4, Appendix B.3.</p>
<table>
<tr><th>Algorithm</th><th>NIST CAVP Cert # (iOS)</th><th>NIST CAVP Cert # (Android)</th></tr>
<tr><td>RSA</td><td>2403</td><td>2404</td></tr>
</table>
<p>Key generation is invoked by the CUCM admin setting the device into CAPF “Install/Upgrade” mode, and will take place when the user inputs the PIN. Only RSA (at least 2048 and 3072 bits) are supported and this is determined by CUCM configuration.</p>
<p>Jabber does not generate any certificates – any generated certificates are generated server-side and transported to authenticated clients over TLS before storing securely.
Key generation is invoked by the CUCM SIP Server admin setting the device into Cisco Certificate Authority Proxy Function (CAPF) “Install/Upgrade” mode, and will take place when the user proceeds with the initial configuration and setup. During this initial configuration and setup of the TOE, CAPF may create certificates under its own authority or it can be used as a proxy to request certificates from an external Certificate Authority (CA) and these certificates can then be used to establish secure, authenticated connections for protocols such as SIP signalling over TLS. The certificates are stored on the client device platform in the certificate store.</p>
</td></tr>
<tr><td>FCS_CKM_EXT.4</td><td>
<p>The TOE maintains the following keys and secrets in volatile memory:</p>
<ul>
<li>Private key used for certificate generation via CAPF</li>
<li>TLS Session Keys for SIP-TLS connections</li>
<li>sRTP Session Keys</li>
<li>User password (secret)</li>
</ul>
<p>When no longer needed by the TLS/SIP and SDES-SRTP trusted channels, the TOE destroys non-persistent plaintext cryptographic keys and secrets by overwriting with zeros.</p>
</td></tr>
<tr><td>FCS_COP.1(1)</td><td>
<p>The TOE provides symmetric encryption and decryption. For the TLS sessions, the TOE supports the following cipher list as defined by the CUCM SIP Server:
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_RSA_WITH _AES_256_GCM_SHA384</p>
<p>For SRTP connections, the TOE supports CTR (NIST SP 800-38A) and GCM (NIST SP 800-38D) mode as required for the following ciphersuites defined in FCS_SRTP_EXT.1 Secure Real-Time Transport Protocol (SRTP).
AES_CM_128_HMAC_SHA1_80
AEAD_AES_256_GCM</p>
<p>The relevant CAVP certificate numbers are listed below:</p>
<table>
<tr><th>Algorithm</th><th>Mode</th><th>NIST CAVP Cert # (iOS)</th><th>NIST CAVP Cert # (Android)</th></tr>
<tr><td>AES</td><td>CBC (128, 256)
CTR (128)
GCM (256)</td><td>4128</td><td>4240</td></tr>
</table>
</td></tr>
<tr><td>FCS_COP.1(2)</td><td>The TOE only performs digital signature verification as required by client TLS sessions, in order to validate the server certificate. The RSA schemes are supported and required in order to meet the requirements. Also, the certificate key is required to be at least 2048 bits in length.</td></tr>
</table>

<table>
<tr><th>TOE SFRs</th><th>How the SFR is Met</th></tr>
<tr><td></td><td>
<p>The TOE also relies upon the TOE platform to provide cryptographic signature verification services for the TOE software during the trusted update process.</p>
<p>All digital signature functionality in the TOE is handled by client device platform on behalf of the TOE as part of TLS session setup.</p>
<p>On iOS platforms, the TOE calls the SecTrustEvaluate API for Cert Validation https://developer.apple.com/library/prerelease/mac/documentation/Security/Reference/certifkeytrustservices/#//apple_ref/c/func/SecTrustEvaluate</p>
<p>On Android, platforms, the TOE calls the X509TrustManager:: checkServerTrusted API http://developer.android.com/reference/javax/net/ssl/X509TrustManager.html</p>
<p>Refer to section 6.1 of the Samsung Galaxy Devices with Android 6 Security Target[1] and the Samsung Galaxy S7 Devices on Android 6 Security Target[2] for information regarding CAVP certificate information.</p>
<p>Refer to section 7.2.2 of the Apple iOS 9.2 Security Target[3] and section 8.2.3 of the Apple iOS 9.3 Security Target[4] for information regarding CAVP certificate information.</p>
</td></tr>
<tr><td>FCS_COP.1(3)</td><td>
<p>The TOE provides cryptographic hashing to ensure data integrity for the SRTP and SIP digest protocol using SHA-1, SHA-256 and SHA-384 as specified in FIPS Pub 180-4 “Secure Hash Standard.”</p>
<p>The relevant CAVP certificate numbers are listed below:</p>
<table>
<tr><th>Algorithm</th><th>Mode</th><th>NIST CAVP Cert # (iOS)</th><th>NIST CAVP Cert # (Android)</th></tr>
<tr><td>SHS</td><td>SHA-1, SHA-256, SHA-384</td><td>3398</td><td>3478</td></tr>
</table>
</td></tr>
<tr><td>FCS_COP.1(4)</td><td>
<p>The TOE provides keyed-hashing message authentication services for SRTP and SIP digest protocol HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-384</p>
<p>The relevant CAVP certificate numbers are listed below:</p>
<table>
<tr><th>Algorithm</th><th>Mode</th><th>NIST CAVP Cert # (iOS)</th><th>NIST CAVP Cert # (Android)</th></tr>
<tr><td>HMAC</td><td>SHA-1, SHA-256, SHA-384</td><td>2701</td><td>2779</td></tr>
</table>
</td></tr>
<tr><td>FCS_RBG_EXT.1</td><td>
<p>When required, the TOE acquires random from the platform random number generator. For both Android and iOS, this is /dev/random.</p>
<p>The mobile device platform’s deterministic random bit generation (DRBG) is implemented in accordance with NIST Special Publication 800-90A.</p>
<p>Refer to section 6.1 of the Samsung Galaxy Devices with Android 6 Security Target[1] and the Samsung Galaxy S7 Devices on Android 6 Security Target[2] for information regarding CAVP certificate information.</p>
<p>Refer to section 7.2.2 of the Apple iOS 9.2 Security Target [3]and section 8.2.3 of the Apple iOS 9.3 Security Target[4] for information regarding CAVP certificate information.</p>
<p>The client device platform is Common Criteria certified and it is assumed that the source for the seeding provides at least 256 bits of entropy which is needed to meet the FCS_RBG_EXT.1.1 requirement.</p>
</td></tr>
<tr><td>FCS_TLS_EXT.1</td><td>For TLS sessions, Jabber supports the following ciphers:</td></tr>
</table>

TOE SFRs	How the SFR is Met
	TLS_RSA_WITH_AES_128_CBC_SHA TLS_ECDHE_RSA_WITH_AES256_GCM_SHA384 TLS_ECDHE_RSA_WITH_AES128_GCM_SHA256, Cisco Jabber compares the hostname/FQDN of the server it is establishing connectivity with, against the Subject CN or the Subject Alternate Name-dnsName attributes in the certificate. If Jabber determines there is a DN mismatch, it will not establish the trusted channel.

FIA_X509_EXT.1
FIA_X509_EXT.2(1)
FIA_X509_EXT.2(2)
	The client device platform is responsible for validating the X509 certificate. During the initial configuration and setup of the TOE, CAPF may create certificates under its own authority or it can be used as a proxy to request certificates from an external Certificate Authority (CA) and these certificates can then be used to establish secure, authenticated connections for protocols such as SIP signalling over TLS. The certificates are stored on the client device platform in the certificate store. The Authorized Administrator may also have to import root certificates into the certificate store if the certificates are signed by a CA that does not already exist in the trust store. The following certificates are required for the on premises server configurations to establish secure connection with the TOE:
	
	Server **Certificate**
	CUCM HTTP (Tomcat) and CallManager certificate (secure SIP call signalling for secure phone)
	
	The TOE uses the client device platform to verify the certificate information at the point in time when it receives the server certificate as part of the process of establishing a secure connection to any server. All of the certificates in the certificate chain are also validated in the process.
	
	Certificate validity and chain is validated via the client device platform including CRL/OCSP revocation status checks. The client device platform also validates the extendedKeyUsage field according to the following rules:
	• Certificates used for trusted updates and executable code integrity verification shall have the Code Signing purpose (id-kp 3 with OID 1.3.6.1.5.5.7.3.3).
	• Server certificates presented for TLS shall have the Server Authentication purpose (id-kp 1 with OID 1.3.6.1.5.5.7.3.1)
	
	This validation is done by the client device platform. Both OCSP and CRL's are supported depending on the information supplied in the certificate. For iOS platforms, if the TOE is unable to connect to the revocation server, for example due to a network error, the TOE will allow the certificate to be accepted. For Android, the TOE will allow the administrator to choose to accept it. The TOE will reject the certificate if other validation rules in FIA_X509_EXT.1.1 fail.
	
	For more information regarding certificate validation, refer to the Security Targets for the Common Criteria certified mobile device platforms and associated documentation.

FMT_SMF.1	The TOE retrieves its configuration from the CUCM SIP Server. The CUCM SIP Server administrator configures the access to manage the VoIP client (TOE). The CUCM SIP Server pushes the required configuration settings for establishing secure connections to the prescribed CUCM SIP Server. This is to ensure organizational policies and settings are applied and enforced accordingly. • The CUCM SIP Server specifies crypto ciphersuites that may be used in the TLS and SDES-SRTP protocols, • The mobile device platform provides the ability to load X.509v3 certificates, • The mobile device platform provides certificate revocation check,

TOE SFRs	How the SFR is Met
	• The mobile device platform provides the ability to update the TOE, and verifying the updates, • The TOE provides the ability to configure the security management functions identified in FMT_SMF.1 for the VoIP client Application.
FPT_TST_EXT.1	The TOE runs a suite of self-tests during start-up to verify its correct operation. These tests include: • AES Known Answer Test - For the encrypt test, a known key is used to encrypt a known plain text value resulting in an encrypted value. This encrypted value is compared to a known encrypted value to ensure that the encrypt operation is working correctly. The decrypt test is just the opposite. In this test a known key is used to decrypt a known encrypted value. The resulting plaintext value is compared to a known plaintext value to ensure that the decrypt operation is working correctly. • HMAC Known Answer Test - For each of the hash values listed, the HMAC implementation is fed known plaintext data and a known key. These values are used to generate a MAC. This MAC is compared to a known MAC to verify that the HMAC and hash operations are operating correctly. • SHA-1/256/512 Known Answer Test – For each of the values listed, the SHA implementation is fed known data and key. These values are used to generate a hash. This hash is compared to a known value to verify they match and the hash operations are operating correctly. During initial start-up of the TOE, a software integrity test is performed. The TOE's Software Integrity Test is run automatically whenever the Cisco Jabber for Android and iPhone/iPad application is loaded and confirms through use of digital signature verification provided by the platform that the application that's about to be loaded was properly signed and has maintained its integrity since being signed by Cisco prior to being made available for download from authorized mobile application stores.
FPT_TUD_EXT.1	Either the iOS App Store or the Google Play Store app can be used to initiate updates depending on the mobile device platform. If there is an update to the Jabber software TOE, the app store will indicate a new version is available. The process to update is the same as a new installation and is described in the Cisco Jabber for IPhone and Android Common Criteria Configuration Guide. Upon installation of a TOE update, a digital signature verification check will automatically be performed to ensure it has not been modified since distribution. The authorized source for the digitally signed updates is "Cisco Systems, Inc.". Verification includes a check that the certificate is valid and has a Code Signing Value of 1.3.6.1.5.5.7.3.3 in the EKU field. If an invalid software image is attempted to be installed, the TOE will display an error and will reject the software image as an invalid or corrupt. If this happens, the Administrator is instructed to contact Cisco Technical Assistance Center (TAC).
FTP_ITC.1(2)	There is no direct admin or user interaction on Jabber to configure or set the SRTP channel. The CUCM SIP Server administrator configures appropriately, and then each time a call is made the clients automatically start SRTP streams as negotiated. There is no user or admin interaction per-SRTP-channel. The CUCM SIP Server administrator can configure the port ranges for the voice and video streams. All communications with the CUCM SIP Server is protected by TLS.

TOE SFRs	How the SFR is Met
	If network loss on the SRTP sessions occurs, the TOE automatically attempts to recover. If the user remains dissatisfied with the result, they can end the call and redial. The communication is initiated on the TOE by the user dialling a number or the SIP URI.

7 Annex A: References

The following documentation was used to prepare this ST:

Table 15: References

Identifier	Description
[CC_PART1]	Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model, dated September 2012, version 3.1, Revision 4, CCMB-2012-009-001
[CC_PART2]	Common Criteria for Information Technology Security Evaluation – Part 2: Security functional components, dated September 2012, version 3.1, Revision 4, CCMB-2012-009-002
[CC_PART3]	Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance components, dated September 2012, version 3.1, Revision 4, CCMB-2012-009-003
[CEM]	Common Methodology for Information Technology Security Evaluation – Evaluation Methodology, dated September 2012, version 3.1, Revision 4, CCMB-2012-009-004
[VoIP PP]	Protection Profile for Voice Over IP (VoIP) Applications, version 1.3, 3 Nov 2014
[800-38A]	NIST Special Publication 800-38A Recommendation for Block 2001 Edition Recommendation for Block Cipher Modes of Operation Methods and Techniques December 2001
[800-56A]	NIST Special Publication 800-56A, March, 2007 Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography (Revised)
[800-56B]	NIST Special Publication 800-56B Recommendation for Pair-Wise, August 2009 Key Establishment Schemes Using Integer Factorization Cryptography
[FIPS PUB 186-3]	FIPS PUB 186-3 Federal Information Processing Standards Publication Digital Signature Standard (DSS) June, 2009
FIPS PUB 186-4]	FIPS PUB 186-4 Federal Information Processing Standards Publication Digital Signature Algorithm Validation System (DSA2VS) March, 2010
[FIPS PUB 198-1]	Federal Information Processing Standards Publication The Keyed-Hash Message Authentication Code (HMAC) July 2008
[800-90]	NIST Special Publication 800-90A Recommendation for Random Number Generation Using Deterministic Random Bit Generators January 2012
[FIPS PUB 180-3]	FIPS PUB 180-3 Federal Information Processing Standards Publication Secure Hash Standard (SHS) October 2008
Client Platform CC certification	http://www.commoncriteriaportal.org/products/