SecuSUITE v5.0 and SteelBox v5.0 Security Target

Version 0.6
12/08/22

Prepared for:

BlackBerry Limited

Prepared By:

www.gossamersec.com

LIST OF TABLES

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 represented by the SecuSUITE/SteelBox Client provided by BlackBerry Limited. The TOE is being evaluated as a Voice/Video over IP (VVoIP) endpoint.

The Security Target contains the following additional sections:

- Conformance Claims (Section 2)
- Security Objectives (Section 3)
- Extended Components Definition (Section 4)
- Security Requirements (Section 5)
- TOE Summary Specification (Section 6)

Conventions

The following conventions have been applied in this document:

- Security Functional Requirements – Part 2 of the CC defines the approved set of operations that may be applied to functional requirements: iteration, assignment, selection, and refinement.
    - Iteration: allows a component to be used more than once with varying operations. In the ST, iteration is indicated by a parenthetical number placed at the end of the component. For example FDP_ACC.1(1) and FDP_ACC.1(2) indicate that the ST includes two iterations of the FDP_ACC.1 requirement.
    - Assignment: allows the specification of an identified parameter. Assignments are indicated using bold and are surrounded by brackets (e.g., [**assignment**]). Note that an assignment within a selection would be identified in italics and with embedded bold brackets (e.g., [***[selected-assignment]***]).
    - Selection: allows the specification of one or more elements from a list. Selections are indicated using bold italics and are surrounded by brackets (e.g., [***selection***]).
    - Refinement: allows the addition of details. Refinements are indicated using bold, for additions, and strike-through, for deletions (e.g., "… **all** objects …" or "… ~~some~~ **big** things …").
- Other sections of the ST – Other sections of the ST use bolding to highlight text of special interest, such as captions.

1.1 Security Target Reference

ST Title – SecuSUITE v5.0 and SteelBox v5.0 Security Target

ST Version – Version 0.6

ST Date – 12/07/22

1.2 TOE Reference

TOE Identification – SecuSUITE v5.0 and SteelBox v5.0

TOE Developer – BlackBerry Limited

Evaluation Sponsor – BlackBerry Limited

1.3 TOE Overview

The Target of Evaluation (TOE) is SecuSUITE v5.0 and SteelBox v5.0.

The TOE, herein referred to as the SecuSUITE/SteelBox Client or the TOE, is a VoIP application that executes on an Android 11 or iOS 14 mobile device operating system. The TOE executes on the following mobile devices[1]:

Samsung Galaxy devices with Android 11:

a) Samsung Devices (US Carrier)
- Snapdragon 888: **Galaxy S21 Ultra 5G**
  i. equivalent:
    1. Galaxy S21 5G
    2. Galaxy S21+ 5G
- Snapdragon 865: **Galaxy S20+ 5G**
  i. **equivalent**
    1. Galaxy Z Fold2 5G
    2. Galaxy Note20 Ultra 5G
    3. Galaxy Note20 5G
    4. Galaxy Tab S7/S7+
    5. Galaxy Z Flip 5G
    6. Galaxy S20 Ultra 5G
    7. Galaxy S20 5G/FE

b) Samsung Devices (International Carriers)
- Exynos 2100: **Galaxy S21 Ultra 5G**
  i. equivalent:
    1. Galaxy S21 5G
    2. Galaxy S21+ 5G
- Exynos 990: **Galaxy S20+ 5G**
  i. **equivalent**
    1. Galaxy S20 Ultra 5G
    2. Galaxy S20+ LTE
    3. Galaxy S20 5G/LTE/FE
    4. Galaxy Note20 Ultra 5G/LTE
    5. Galaxy Note20 5G/LTE
- Exynos 9611: Galaxy **XCover Pro**
  i. equivalent:
    1. Samsung A51

Apple devices running iOS14:

- **iPhone, Xs**, Xs Max, XR
- **iPhone 12**, 12 Pro, 12 Pro Max, 12 Mini
- **iPhone 11**, 11 Pro, 11 Pro Max

[1] Note the list of equivalent devices is taken from the evaluated devices' Security Targets.

The mobile devices have been NIAP certified as follows:

Samsung Galaxy Devices on Android 11 - Spring (**VID11160):** https://www.niap-ccevs.org/Product/Compliant.cfm?PID=11160

Apple iOS 14: iPhones (**VID11146**): https://www.niap-ccevs.org/product/Compliant.cfm?PID=11146

1.4 TOE Description

The TOE, herein referred to as the SecuSUITE/SteelBox Client or the TOE, is a VoIP application that executes on an evaluated mobile device operating system.

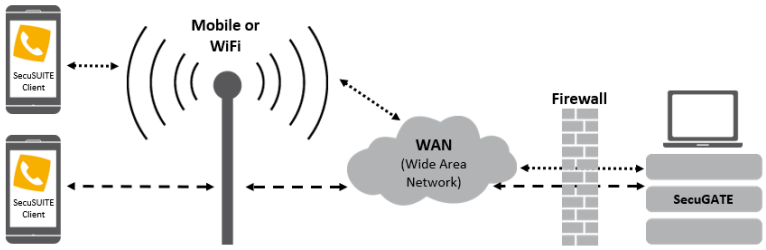

Figure 1-1 TOE Usage

User Context

The TOE user downloads the TOE from an app store (e.g. Apple Store, Google Play) or it is pushed via a Mobile Device Management (MDM) server (e.g. BlackBerry Enterprise Server) and installs the app to their mobile device. On first use of the app, the user must go through a registration process in order to register to a specified BlackBerry SecuGATE (identified by URI).

Once registered, the user can place secure VoIP calls using the app with largely the same interactions as with a normal phone call. The SecuSUITE Client provides encryption of user call signaling and voice data.

Users are typically invited to join SecuSUITE/SteelBox service via an activation email initiated by their corporate IT administrator who adds users via the BlackBerry SecuGATE administration portal. The activation email includes the activation credentials as well as the option to scan a QR code to initiate the registration with the SCA server.

SecuSUITE Context

The TOE is part of the SecuSUITE Security Solution shown in Figure 1-2. The TOE does not work in isolation but relies on BlackBerry SecuGATE components to enable a secure VoIP communication.

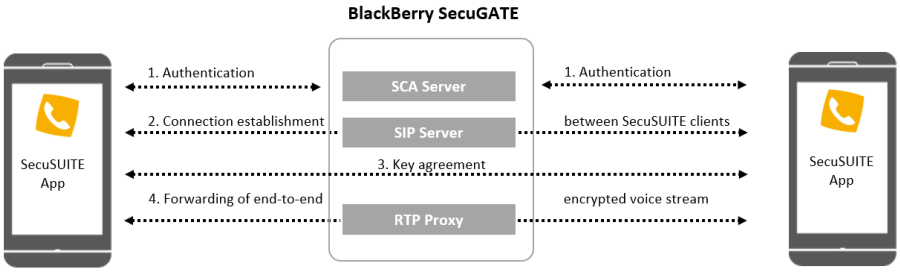

Figure 1-2 SecuSUITE Security Solution

As shown in Figure 1-2, the SecuSUITE VoIP process flow is as follows:

a) Step 1 Initial Registration. Every participating client has to register first to the Secure Client Authentication (SCA) server. The SCA server authenticates users and enrolls required client and user certificates as well as client configuration. Only clients that have been enrolled via the SCA service are able to connect to the SIP server and are allowed to establish end-to-end encrypted communication to other SecuSUITE/SteelBox

clients. Note: Clients must also register to the SIP server using a SIP password. This is in addition to initial client registration with the SCA server.

b) Step 2 Connection establishment. The Session Initiation Protocol (SIP) together with TLS is used to establish a secure connection between mobile devices. The use of a TLS connection, providing encryption and mutual authentication, ensures that the devices connect with authorized SIP servers and the dialed call numbers are transmitted encrypted. The BlackBerry SecuGATE SIP Server Security Target defines the SIP Server TOE.

c) Step 3 Key agreement. When a call is placed and accepted, SecuSUITE/SteelBox clients exchange SIP messages that include digital certificates used to confirm caller identity and perform key agreement for SRTP encryption.

d) Step 4 End-to-end encrypted voice communication established. Clients utilize the SRTP protocol to exchange encrypted voice communications. The voice stream remains encrypted while traversing the BlackBerry SecuGATE and only the clients have access to the SRTP session keys.

e) Step 5 Forwarding of end-to-end encrypted voice stream. During connection signaling, the SIP server sets up the RTP/RTCP packet bridging in the Real-Time Transport Protocol (RTP) Proxy for this connection. The RTP Proxy relays / bridges the encrypted data stream between clients. The main purpose of the RTP Proxy is to make the communication between SIP user agents behind NAT/NAPT possible.

VoIP Client

The SecuSUITE Client establishes a secure tunnel for voice communications with another SecuSUITE/SteelBox client or the SecuGATE SIP server. The tunnel provides confidentiality, integrity, and data authentication for information that travels across the public network. This occurs using the Secure 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 supports SDES-SRTP.

The TOE Client also protects communications between itself and the SIP Server by using a Transport Layer Security (TLS)-protected signaling channel. To register the TOE within the domain, the TOE is required to be password authenticated by the SIP Server. The TOE also makes use of certificates to authenticate both the SIP server end and the TOE itself through the TLS connection.

Group/Conference Calls

Besides the peer-to-peer calls between two instances of the TOE, the SecuSUITE/SteelBox solution also allows the set-up of a secure conference call between a group of SecuSUITE users. For that, individual calls and trusted channels are established between all TOEs participating in the group call (for a group call between 4 participants every TOE has 3 individual calls to the members of the group). The individual SIP and SRTP connections are established exactly the same way the peer to peer calls are set-up via the SecuGATE. They are encrypted end-2-end and the individually decrypted audio streamed are mixed only locally by each client so that no clear text representations of the audio streams exists in a central component.

Secure Text Messaging

The TOE client allows encrypted instant message transfer between client applications. Secure Text Messaging utilizes the same TLS protected communication channel that is used during initial SCA registration used to transfer client configuration settings and SIP credentials between SecuGATE and client.

Group Messaging

Besides the peer-to-peer text messaging between two instances of the TOE, the SecuSUITE/SteelBox solution also allows the set-up of messaging groups between an arbitrary number of SecuSUITE users. The messages are individually encrypted for all TOE users participating in the group messaging session the same way peer to peer messages are protected.

Calls Destined Beyond the SecuGATE SIP server

The TOE always encrypts the user's call signaling and data (voice) transmitted to other TOE VoIP endpoints registered with the SecuGATE and transmitted to the SecuGATE itself. The SecuGATE administrator can configure calling to additional endpoints, endpoints reached through a PBX (another SIP server connected to local/internal landline phones and potentially connected to outside phone lines). If so configured, the TOE can then place calls to additional

endpoints beyond the SecuGATE through the configured PBX; however, because the call signaling and call data travels beyond the SecuGATE itself, its security ultimately lies beyond the TOE and SecuGATE SIP server's control.

While the ability of the SecuGATE SIP server to route calls to additional endpoints through a PBX lies beyond the scope of this ASPP14/PKGTLS11/VVoIPAS10 evaluation, the TOE can indicate when a user's call travels beyond the SecuGATE SIP server.

The SecuGATE SIP server allows an administrator to configure (refer to BlackBerry SecuGATE evaluation VID 11281 against the Enterprise Session Controller Protection Profile) which phone number prefixes the administrator deems to "land secure" and which calls "breakout" to external phone lines (with unknown security). By default, the SecuGATE SIP server treats all calls routed to the PBX as "breakout" calls. These designations cause an image indicating this disposition of the call to appear on the TOE's User Interface (UI) as described in the Common Criteria Configuration Guide. Again, while beyond the scope of this evaluation, the concepts of "Secure Landing" and "Breakout Calls" are useful for TOE users to understand, in the event that their administrator has configured their SecuGATE SIP server to route calls to additional endpoints through a PBX.

CACI SteelBox Client

The SteelBox Client is a branded version of the SecuSUITE client that is identical from functional and security implementation perspective. The SteelBox client is distributed by BlackBerry's partner CACI and differs basically in the used UI assets and product publishing. The relevant deltas are:

- Different splash screens during client start-up
- Replaced UI Assets and Text elements (e.g., SteelBox logo, product name, app icon, status bar icon, EULA text and About screen).
- Changes required to distribute the client under an independent publisher/developer in the App Stores (e.g. developer signing).

Client configuration and UI flows are identical otherwise, same guidance document applies to both clients.

The clients are created out of the same build process at the same point of time and have always matching major/minor release numbers.

All descriptions and security claims in this document apply always to both clients even if only SecuSUITE is mentioned in the text.

1.4.1 TOE Architecture

The TOE boundary is illustrated in Figure 1-3.

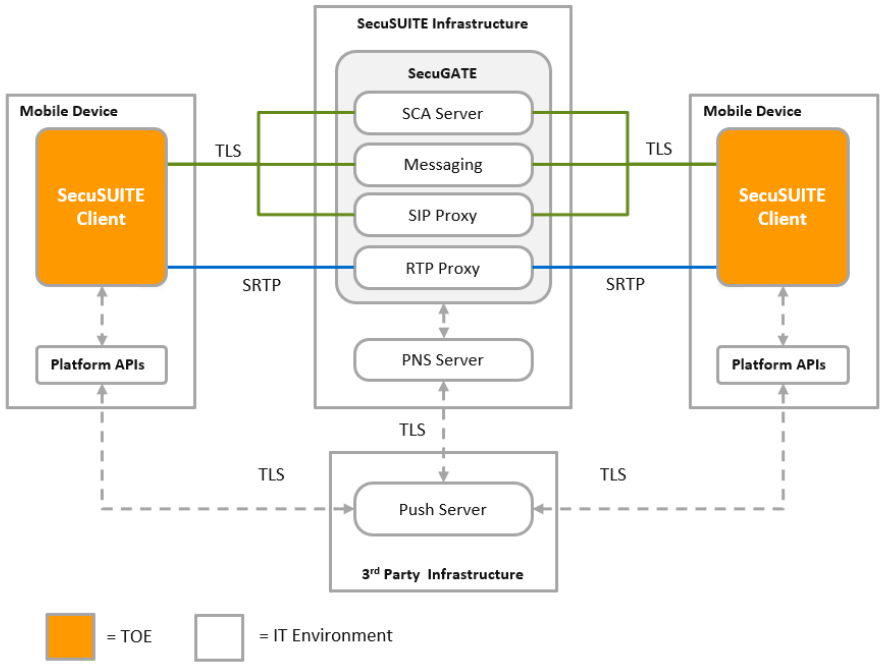

Figure 1-3 TOE Boundary

The TOE is comprised of the SecuSUITE v5.0 and SteelBox v5.0.

To operate the SecuSUITE Client must be registered to *SecuSUITE* and to the BlackBerry SecuGATE SIP Server (also referred to as the Enterprise Session Controller, or ESC). Once properly registered, the Client can initiate or receive a "Call". Call data is exchanged with a VVoIP endpoint through SecuGATE which provides an SRTP proxy. The Enterprise Session Controller is also referred to as the SIP server.

Client Registration to SecuSUITE

Before a SecuSUITE client can exchange messages with the SIP Server, it must first be registered to the BlackBerry SecuGATE via the SCA Server. This initial client registration is briefly described below to provide context to the reader:

1. SecuSUITE administrator adds a user to the SecuSUITE via the Admin Portal which generates activation codes that are delivered to the user via some out of band method (e.g. email / printed).
2. User downloads the SecuSUITE client application from supported app store (or it is pushed via an MDM) and launches client app.
3. Client app running on mobile device prompts the user to enter the activation code as well as the SCA Server URL and initiates a TLS connection to SCA Server.
4. The user is notified to define a device password in case no device password is defined yet.
5. SCA Server validates client for registration via secure remote password protocol using the activation code as the shared secret (this is not the SIP password).
6. Client generates multiple certificate signing requests and submits to SCA Server.
7. SCA server's embedded CA creates, signs and returns the certificates. Alternatively, the signing requests can be forwarded to an existing external CA for certificate signing.
8. Client gets its client configuration settings from SCA server.
9. Client gets its SIP settings from SCA server (which retrieves settings from the database server). Settings include:
    a. E.164 telephone number (SIP alias)

b. SIP Server URI
c. TLS version (TLS 1.2 only)
d. SIP domain to which client belongs
e. SIP user name and password

10. User performs the following:

a. Enter unique activation code
b. Enter the SCA Server URL

Client SIP Registration with SIP Server

The client registers with the SIP server every time a new connection with the SIP server is established. That is, after:

- Client app was installed and SCA procedure was successfully passed, or
- Client was restarted, or
- Client had lost TLS connection to SIP server (e.g. because of network change or problems)

Procedure:

- Client opens two-way authenticated TLS session with SIP server
- Client registers using SIP REGISTER
- Once registered with the SIP server the client can operate in one of two modes:
  - Constant connection mode, where the client uses periodic requests with the SIP server to keep the TLS connection open.
  - Push Service connection mode where the client registers with a PUSH notification service on the mobile device and provides that information to the SIP server. When a call is targeted at the client, the SIP server communicates with the PUSH service to awaken the client. Once the mobile device OS wakes the client, the client reconnects to the SIP server to establish a current TLS connection.
- SIP server authenticates client's SIP REGISTER request messages with SIP username and password / digest access authentication.

Digest Access Authentication

The SIP username and password are used to authenticate SIP REGISTER messages using digest access authentication per RFC 3261 as follows:

- Client and server have a shared secret (H(A1) of SIP password)
- Client sends request message to server
- Server rejects request with request message containing challenge ("nonce")
- Client calculates digest from challenge and H(A1) of SIP password
- Client sends request message again with request message now containing digest
- Server also calculates digest and compares this with value received from client
- If digest values match, server accepts request

Call Setup

Preconditions:

- Client A ("Alice") and client B ("Bob") have registered with SCA server.
- Alice and Bob can establish TLS sessions with the SIP server

Alice calls Bob:

- The SIP Server routes SIP messages between Alice and Bob (using a PUSH server to awaken Bob's client if necessary).
- Alice and Bob do not exchange media packets (RTP/RTCP) directly. The SecuSUITE encompasses an RTP proxy which works as an RTP bridge. Alice sends her media packets to the RTP proxy which forwards them to Bob, and vice versa. During connection signaling, the SIP server sets up the RTP/RTCP packet bridging in the RTP proxy for this connection.

The messages are as follows:

- Alice's SIP INVITE message includes:
  - Alice's VoIP Encryption Certificate
- Bob's SIP 200 OK message includes within the SDP:
  - Bob's VoIP Encryption Certificate
  - Bob's SDP message
  - Bob's SRTP master uplink key and salt (i.e. the key and salt Bob is using when sending RTP and RTCP packets to Alice, see (RFC4568, 2006) section 5.1.1) in a message block containing a CMS EnvelopedData ASN.1 structure.
- Alice's SIP ACK includes:
  - Alice's SDP message
  - Alice's SRTP master uplink key and salt (i.e. the key and salt Alice is using when sending RTP and RTCP packets to Bob; similar encoding as Bob)

User Plane (Media)

The main purpose of the RTP Proxy is to make the communication between SIP user agents behind NAT/NAPT possible:

- Typically, the client has an internal (non-routable) IP address and will select some UDP port for RTP and another one for RTCP. NAPT will change the IP address and UDP ports to external values. The internal values however appear in the SDP, and the remote client would use them as destination IP address and ports, which would not work. The solution is to replace the IP address and ports in the SDP: The new IP address is a routable IP address of an RTP proxy, and the RTP/RTCP ports are replaced and used as session identifiers. This replacement happens in the SIP server during call establishment:
- When the SIP server receives the first SIP message with SDP content during call setup (e.g. 200 OK), it extracts the Call-ID, selects an RTP proxy, and sends the Call ID to this RTP Proxy using the RTPproxy Control Protocol.
- The RTP Proxy creates a new session by allocating randomly two subsequent unused UDP ports from a range of UDP ports to that session and returns these port numbers to the SIP server via the RTP Proxy Control Protocol. The first port is for RTP, and the second one for RTCP.
- After receiving the reply from the RTP Proxy, the SIP server replaces the RTP and RTCP media IP addresses and UDP ports in the SDP content of the message with the RTP Proxy IP address and the UDP ports the RTP Proxy has allocated.
- Then the SIP server forwards this modified SIP message as usually to the intended destination.
- When the SIP server receives a SIP follow-up message (e.g. ACK) containing SDP information from the other peer, it sends again the Call-ID to the RTP proxy via the RTPproxy Control Protocol.
- Using the Call-ID as a key, the RTP proxy performs a lookup among existing sessions, allocates randomly another pair of subsequent UDP ports to this session and returns these port numbers to the SIP server.
- After receiving the second pair of port numbers from the RTP proxy, the SIP server replaces the media IP address and Ports in the SDP content of the SIP follow-up message so that it now also points to the RTP proxy. The SIP server forwards the SIP message as usually to the intended destination.
- For RTP, the RTP proxy now listens on the two ports it has allocated for that session and waits for receiving at least one UDP message from Alice and one from Bob. When such a packet is received, the proxy fills one of two IP address/UDP port structures associated to this call with the source IP address and the source UDP port of that packet. When both structures are filled in, the RTP proxy starts relaying UDP/RTP packets between the Alice and Bob.
- The same happens for RTCP.

- The RTP proxy tracks idle time for each of the existing sessions (i.e. the time within which there were no packets relayed), and automatically cleans up sessions whose idle times exceed a specified value (e.g. 60 seconds).

Call Termination

Users can terminate an ongoing call anytime by pushing the "End call" button. The client sends a SIP BYE message and the other party confirms with a SIP OK message. The SIP server then terminates the SRTP session by sending a Delete message for that call to the RTPProxy.

Clients will also terminate a call when no RTP data is received for more than 15 seconds.

1.4.1.1 Physical Boundaries

The TOE executes on the following mobile devices:

a) Samsung Devices (US Carrier)
- Snapdragon 888 : Galaxy S21 Ultra 5G
  i. equivalent:
    1. Galaxy S21 5G
    2. Galaxy S21+ 5G
- Snapdragon 865: Galaxy S20+ 5G
  i. equivalent
    1. Galaxy Z Fold2 5G
    2. Galaxy Note20 Ultra 5G
    3. Galaxy Note20 5G
    4. Galaxy Tab S7/S7+
    5. Galaxy Z Flip 5G
    6. Galaxy S20 Ultra 5G
    7. Galaxy S20 5G/FE

b) Samsung Devices (International Carriers)
- Exynos 2100 : Galaxy S21 Ultra 5G
  i. equivalent:
    1. Galaxy S21 5G
    2. Galaxy S21+ 5G
- Exynos 990: Galaxy S20+ 5G
  i. equivalent
    1. Galaxy S20 Ultra 5G
    2. Galaxy S20+ LTE
    3. Galaxy S20 5G/LTE/FE
    4. Galaxy Note20 Ultra 5G/LTE
    5. Galaxy Note20 5G/LTE
- Exynos 9611: Galaxy XCover Pro
  i. equivalent:
    1. Samsung A51

Apple devices running iOS14:

- iPhone, Xs, Xs Max, XR
- iPhone 12, 12 Pro, 12 Pro Max
- iPhone 11, 11 Pro, 11 Pro Max

Non-TOE Components

The TOE is part of the SecuSUITE security solution and requires the following components to be present in the environment:

a) SecuSUITE SCA Server. The SCA Server authenticates users and facilitates VoIP client enrollment and pushes client SIP configuration to the client.

b) SecuSUITE SIP Server. The SIP Server is used to establish the secure connection between the mobile devices. The use of a TLS connection, providing encryption and mutual authentication, ensures that the devices connect with authorized SIP servers only and the dialed call numbers are transmitted encrypted.

c) SecuSUITE RTP Proxy. The Real-time Transport Protocol (RTP) Proxy bridges media packets sent between clients. The RTP Proxy is part of the SecuSUITE SIP Server. The SIP Server creates and deletes RTP and Real-time Transport Control Protocol (RTCP) bridging sessions in the RTP Proxy.

1.4.1.2 Logical Boundaries

This section summarizes the security functions provided by SecuSUITE/SteelBox Client:

- Communication
- Cryptographic support
- User data protection
- Identification and authentication
- Security management
- Privacy
- Protection of the TSF
- TOE access
- Trusted path/channels

1.4.1.2.1 Communication

The TOE utilizes the Opus codec by default to transmit voice media. The Opus codec utilizes a fixed bit-rate.

The TOE also includes the SILK vocoder to transmit voice media. The vocodec has been modified to pad the bit-rate in order to provide a constant bit-rate. This codec's purpose is to provide backwards compatibility with the TOE's previous versions, and this codec is only used if the peer VoIP client does not support the Opus codec.

1.4.1.2.2 Cryptographic support

The TOE includes its own cryptographic module to perform operations in support of authentication actions and network communications using the TLS and SRTP protocol. The TOE implements TLS version 1.2 with mutual authentication using elliptic-curve cryptography. The TOE also relies upon its platform for certain cryptographic operations including providing random data to seed the TOE's own DRBG. The TOE relies upon the platform (i.e., iOS and Android) cryptographic libraries for operations related to protecting keys in platform offer storage (i.e., a key store).

1.4.1.2.3 User data protection

The TOE enforces the media transmission policy when communicating with remote VVoIP endpoints which use TLS and SRTP protocols. The TOE also ensures that communication with an SCA server is protected using TLS. The TOE protects user data by utilizing platform services for data storage.

1.4.1.2.4 Identification and authentication

The TOE authenticates TLS peers using X.509v3 certificates. It performs extensive X.509 certificate validation checks on these certificates rejecting invalid or revoked certificates.

1.4.1.2.5 Security management

The TOE receives configuration setting during its registration with an SCA server. The client allows management operations that specify the SIP Server to use for connections.

1.4.1.2.6 Privacy

The TOE does not transmit Personally Identifiable Information over any network interfaces.

1.4.1.2.7 Protection of the TSF

The TOE relies on the physical boundary of the evaluated platform as well as the Android and iOS operating systems for the protection of the TOE's application components.

The TOE relies upon these platforms to indicate the current TOE version. If an update is needed, it is obtained from the platform's application store. The TOE's software is digitally signed in accordance with the requirements of each application store.

The native Apple and Android cryptographic library, which provides some of the TOE's cryptographic services, have built-in self-tests that are run at client start-up to ensure that the algorithms are correct. If any self-tests fail, the TOE will not be able to perform its cryptographic services. The TOE includes its own cryptographic library that also includes self-tests that are run when the client starts.

1.4.1.2.8 TOE access

The TOE includes a 15 second default timeout that can terminate idle voice/video transmission. This timeout value can be changed by the configuration obtained from the SCA server.

1.4.1.2.9 Trusted path/channels

The TOE encrypts all data transmitted with an SCA server or Enterprise Session Controller using TLS. The TLS channel established with an ESC can be used to exchange SIP messages or to initiate the use of SRTP for voice/video traffic.

1.4.2 TOE Documentation

BlackBerry Limited offers documentation that describes the installation process for the TOE as well as guidance for subsequent use and administration of the applicable security features of the TOE. The following list of documents were examined as part of the evaluation.

- Common Criteria Configuration Guide SecuSUITE v5.0 SteelBox v5.0, Version 1.1, 05-Dec-2022

2. Conformance Claims

This TOE is conformant to the following CC specifications:

- Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1, Revision 5, April 2017.
  - Part 2 Extended
- Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1, Revision 5, April 2017.
  - Part 3 Extended
- Package Claims:
  - PP-Configuration for Application Software and Voice/Video over IP (VVoIP) Endpoints, Version 1.1, 31 May 2022
    - Protection Profile for Application Software, Version 1.4, 2021-10-07 (ASPP14)

Technical Decision Number	Applied?	Rationale (if not applied)
TD0669	Yes	
TD0664	Yes	
TD0659	Yes	
TD0655	Yes	
TD0650	No	MOD_VPNC is not claimed.
TD0628	Yes	
TD0626	Yes	
TD0624	Yes	

    - PP-Module for Voice/Video over IP (VVoIP) Endpoints, Version 1.0, 28 October 2020 (VVoIPAS10)

Technical Decision Number	Applied?	Rationale (if not applied)
TD0589	No	SFR not claimed

  - Functional Package for Transport Layer Security (TLS), 1.1, 2019-02-12 (PKGTLS11) with applied technical decisions:

Technical Decision Number	Applied?	Rationale (if not applied)
TD0588	No	SFR not claimed
TD0513	Yes	
TD0499	Yes	
TD0469	No	SFR not claimed
TD0442	Yes	

2.1 Conformance Rationale

The ST conforms to the ASPP14/VVoIPAS10/PKGTLS11. The security problem definition, security objectives, and security requirements have been drawn from the PP.

3. Security Objectives

The Security Problem Definition may be found in the ASPP14/VVoIPAS10 and this section reproduces only the corresponding Security Objectives for operational environment for reader convenience. The ASPP14/VVoIPAS10/PKGTLS11 offers additional information about the identified security objectives, but that has not been reproduced here and the ASPP14/VVoIPAS10/PKGTLS11 should be consulted if there is interest in that material.

In general, the ASPP14/VVoIPAS10/PKGTLS11 has defined Security Objectives appropriate for software applications that provide Voice/Video over IP (VVoIP) endpoints and as such are applicable to the SecuSUITE/SteelBox Client TOE.

3.1 Security Objectives for the Operational Environment

OE.PLATFORM The TOE relies upon a trustworthy computing platform for its execution. This includes the underlying operating system and any discrete execution environment provided to the TOE.

Section 4.3 Security Objectives Rationale is replaced by TD0498.

OE.PROPER_ADMIN The administrator of the application software is not careless, willfully negligent or hostile, and administers the software within compliance of the applied enterprise security policy.

Section 4.3 Security Objectives Rationale is replaced by TD0498.

OE.PROPER_USER The user of the application software is not willfully negligent or hostile, and uses the software within compliance of the applied enterprise security policy.

Section 4.3 Security Objectives Rationale is replaced by TD0498.

OE.UPDATE_SOURCE The operational environment will have TOE software/firmware made available on either the call control server that the TOE connects to or a separate file server managed by the organization.

4. Extended Components Definition

All of the extended requirements in this ST have been drawn from the ASPP14/VVoIPAS10/PKGTLS11. The ASPP14/VVoIPAS10/PKGTLS11 defines the following extended requirements and since they are not redefined in this ST the ASPP14/VVoIPAS10/PKGTLS11 should be consulted for more information in regard to those CC extensions.

Extended SFRs:

- VVoIPAS10:FCO_VOC_EXT.1: Fixed-Rate Vocoder
- ASPP14:FCS_RBG_EXT.1: Random Bit Generation Services
- ASPP14:FCS_RBG_EXT.2: Random Bit Generation from Application
- VVoIPAS10:FCS_SRTP_EXT.1: Secure Real-Time Transport Protocol
- ASPP14:FCS_STO_EXT.1: Storage of Credentials
- PKGTLS11:FCS_TLS_EXT.1: TLS Protocol
- PKGTLS11:FCS_TLSC_EXT.1: TLS Client Protocol
- PKGTLS11:FCS_TLSC_EXT.2: TLS Client Support for Mutual Authentication
- PKGTLS11:FCS_TLSC_EXT.3: TLS Client Support for Signature Algorithms Extension
- PKGTLS11:FCS_TLSC_EXT.4: TLS Client Support for Renegotiation
- PKGTLS11:FCS_TLSC_EXT.5: TLS Client Support for Supported Groups Extension
- ASPP14:FDP_DAR_EXT.1: Encryption Of Sensitive Application Data
- ASPP14:FDP_DEC_EXT.1: Access to Platform Resources
- ASPP14:FDP_NET_EXT.1: Network Communications
- ASPP14:FIA_X509_EXT.1: X.509 Certificate Validation
- ASPP14:FIA_X509_EXT.2: X.509 Certificate Authentication
- ASPP14:FMT_CFG_EXT.1: Secure by Default Configuration
- ASPP14:FMT_MEC_EXT.1: Supported Configuration Mechanism
- ASPP14:FPR_ANO_EXT.1: User Consent for Transmission of Personally Identifiable
- ASPP14:FPT_AEX_EXT.1: Anti-Exploitation Capabilities
- ASPP14:FPT_API_EXT.1: Use of Supported Services and APIs
- ASPP14:FPT_IDV_EXT.1: Software Identification and Versions
- ASPP14:FPT_LIB_EXT.1: Use of Third Party Libraries
- ASPP14:FPT_TUD_EXT.1: Integrity for Installation and Update
- VVoIPAS10:FPT_TUD_EXT.1: Trusted Update
- ASPP14:FPT_TUD_EXT.2: Integrity for Installation and Update
- ASPP14:FTP_DIT_EXT.1: Protection of Data in Transit
- VVoIPAS10:FTP_DIT_EXT.1: Protection of Data in Transit

Extended SARs:

- ALC_TSU_EXT.1: Timely Security Updates

5. Security Requirements

This section defines the Security Functional Requirements (SFRs) and Security Assurance Requirements (SARs) that serve to represent the security functional claims for the Target of Evaluation (TOE) and to scope the evaluation effort.

The SFRs have all been drawn from the ASPP14/VVoIPAS10/PKGTLS11. The refinements and operations already performed in the ASPP14/VVoIPAS10/PKGTLS11 are not identified (e.g., highlighted) here, rather the requirements have been copied from the ASPP14/VVoIPAS10/PKGTLS11 and any residual operations have been completed herein. Of particular note, the ASPP14/VVoIPAS10/PKGTLS11 made a number of refinements and completed some of the SFR operations defined in the Common Criteria (CC) and that PP should be consulted to identify those changes if necessary.

The SARs are also drawn from the ASPP14/VVoIPAS10/PKGTLS11. The ASPP14/VVoIPAS10/PKGTLS11 should be consulted for the assurance activity definitions.

5.1 TOE Security Functional Requirements

The following table identifies the SFRs that are satisfied by SecuSUITE/SteelBox Client TOE.

Requirement Class	Requirement Component
FCO: Communication	VVoIPAS10:FCO_VOC_EXT.1: Fixed-Rate Vocoder
FCS: Cryptographic support	ASPP14:FCS_CKM.1: Cryptographic Key Generation Services
	ASPP14:FCS_CKM.1/AK: Cryptographic Asymmetric Key Generation
	ASPP14:FCS_CKM.2: Cryptographic Key Establishment
	ASPP14:FCS_COP.1/Hash: Cryptographic Operation - Hashing
	ASPP14:FCS_COP.1/KeyedHash: Cryptographic Operation - Keyed-Hash Message Authentication
	ASPP14:FCS_COP.1/Sig: Cryptographic Operation - Signing
	ASPP14:FCS_COP.1/SKC: Cryptographic Operation - Encryption/Decryption
	VVoIPAS10:FCS_COP.1/SRTP: Cryptographic Operation (Encryption/Decryption for SRTP)
	ASPP14:FCS_RBG_EXT.1: Random Bit Generation Services
	ASPP14:FCS_RBG_EXT.2: Random Bit Generation from Application
	VVoIPAS10:FCS_SRTP_EXT.1: Secure Real-Time Transport Protocol
	ASPP14:FCS_STO_EXT.1: Storage of Credentials
	PKGTLS11:FCS_TLS_EXT.1: TLS Protocol
	PKGTLS11:FCS_TLSC_EXT.1: TLS Client Protocol
	PKGTLS11:FCS_TLSC_EXT.2: TLS Client Support for Mutual Authentication
	PKGTLS11:FCS_TLSC_EXT.3: TLS Client Support for Signature Algorithms Extension
	PKGTLS11:FCS_TLSC_EXT.4: TLS Client Support for Renegotiation
	PKGTLS11:FCS_TLSC_EXT.5: TLS Client Support for Supported Groups Extension
FDP: User data protection	ASPP14:FDP_DAR_EXT.1: Encryption Of Sensitive Application Data
	ASPP14:FDP_DEC_EXT.1: Access to Platform Resources
	VVoIPAS10:FDP_IFC.1: Subset Information Flow Control
	VVoIPAS10:FDP_IFF.1: Simple Security Attributes

	ASPP14:FDP_NET_EXT.1: Network Communications
FIA: Identification and authentication	ASPP14:FIA_X509_EXT.1: X.509 Certificate Validation
	ASPP14:FIA_X509_EXT.2: X.509 Certificate Authentication
FMT: Security management	ASPP14:FMT_CFG_EXT.1: Secure by Default Configuration
	ASPP14:FMT_MEC_EXT.1: Supported Configuration Mechanism
	ASPP14:FMT_SMF.1: Specification of Management Functions
	VVoIPAS10:FMT_SMF.1/VVoIP: Specification of Management Functions (VVoIP Communications)
FPR: Privacy	ASPP14:FPR_ANO_EXT.1: User Consent for Transmission of Personally Identifiable
FPT: Protection of the TSF	ASPP14:FPT_AEX_EXT.1: Anti-Exploitation Capabilities
	ASPP14:FPT_API_EXT.1: Use of Supported Services and APIs
	ASPP14:FPT_IDV_EXT.1: Software Identification and Versions
	ASPP14:FPT_LIB_EXT.1: Use of Third Party Libraries
	ASPP14:FPT_TUD_EXT.1: Integrity for Installation and Update
	VVoIPAS10:FPT_TUD_EXT.1: Trusted Update
	ASPP14:FPT_TUD_EXT.2: Integrity for Installation and Update
FTA: TOE access	VVoIPAS10:FTA_SSL.3/Media: /Media TSF-Initiated Termination (Media Channel)
FTP: Trusted path/channels	ASPP14:FTP_DIT_EXT.1: Protection of Data in Transit
	VVoIPAS10:FTP_DIT_EXT.1: Protection of Data in Transit
	VVoIPAS10:FTP_ITC.1/Control: Inter-TSF Trusted Channel (Signaling Channel)
	VVoIPAS10:FTP_ITC.1/Media: Inter-TSF Trusted Channel (Media Channel)

Table 1 TOE Security Functional Components

5.1.1 Communication (FCO)

5.1.1.1 Fixed-Rate Vocoder (VVoIPAS10:FCO_VOC_EXT.1)

VVoIPAS10:FCO_VOC_EXT.1.1

The TSF shall transmit voice media using a constant bit rate voice vocoder.

5.1.2 Cryptographic support (FCS)

5.1.2.1 Cryptographic Key Generation Services (ASPP14:FCS_CKM.1)

ASPP14:FCS_CKM.1.1

The application shall [***invoke platform-provided functionality for asymmetric key generation (iOS implementation only), implement asymmetric key generation (Android implementation only)***].

Application Note: The Android application will implement this functionality. The iOS application will invoke platform provided functionality.

5.1.2.2 Cryptographic Asymmetric Key Generation (ASPP14:FCS_CKM.1/AK)

ASPP14:FCS_CKM.1.1/AK

The application shall [***invoke platform-provided functionality, implement functionality***] to

generate asymmetric cryptographic keys in accordance with a specified cryptographic key generation algorithm [***[ECC schemes] using 'NIST curves' P-384 and [P-256] that meet the following: FIPS PUB 186-4, 'Digital Signature Standard (DSS)', Appendix B.4***]. (TD0659 applied)

5.1.2.3 Cryptographic Key Establishment (ASPP14:FCS_CKM.2)

ASPP14:FCS_CKM.2.1

The application shall [***implement functionality***] to perform cryptographic key establishment in accordance with a specified cryptographic key establishment method: [***Elliptic curve-based key establishment schemes that meets the following: NIST Special Publication 800-56A, 'Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography'***].

5.1.2.4 Cryptographic Operation - Hashing (ASPP14:FCS_COP.1/Hash)

ASPP14:FCS_COP.1.1/Hash

The application shall perform cryptographic hashing services in accordance with a specified cryptographic algorithm [***SHA-1, SHA-256, SHA-384, SHA-512***] and message digest sizes [***160, 256, 384, 512***] bits that meet the following: FIPS Pub 180-4.

5.1.2.5 Cryptographic Operation - Keyed-Hash Message Authentication (ASPP14:FCS_COP.1/KeyedHash)

ASPP14:FCS_COP.1.1/KeyedHash

The application shall perform keyed-hash message authentication in accordance with a specified cryptographic algorithm [***HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512***] and [***HMAC-SHA-1***] with key sizes [**160, 256, 384, 512**] and message digest sizes [***256, 384, 512***] and [***160***] bits that meet the following: FIPS Pub 198-1, 'The Keyed-Hash Message Authentication Code' and FIPS Pub 180-4, 'Secure Hash Standard'. (TD0626 applied)

5.1.2.6 Cryptographic Operation - Signing (ASPP14:FCS_COP.1/Sig)

ASPP14:FCS_COP.1.1/Sig

The application shall perform cryptographic signature services (generation and verification) in accordance with a specified cryptographic algorithm [

- ***RSA schemes using cryptographic key sizes of 2048-bit or greater that meet the following: FIPS PUB 186-4, 'Digital Signature Standard (DSS)', Section 4***
- ***ECDSA schemes using 'NIST curves' P-256, P-384 and [no other curves] that meet the following: FIPS PUB 186-4, 'Digital Signature Standard (DSS)', Section 5***].

5.1.2.7 Cryptographic Operation - Encryption/Decryption (ASPP14:FCS_COP.1/SKC)

ASPP14:FCS_COP.1.1/SKC

The application shall perform encryption/decryption in accordance with a specified cryptographic algorithm [***AES-GCM (as defined in NIST SP 800-38D) mode***] and cryptographic key sizes [***256-bit***].

5.1.2.8 Cryptographic Operation (Encryption/Decryption for SRTP) (VVoIPAS10:FCS_COP.1/SRTP)

VVoIPAS10:FCS_COP.1.1/SRTP

The following SFR shall be claimed by the TOE if 'SRTP' is selected in FTP_DIT_EXT.1 or FPT_ITC.1/Media:

The TSF shall perform encryption/decryption to support SDES-SRTP in accordance with a specified cryptographic algorithm [***AES-CTR (as defined in NIST SP 800-38A)***] and cryptographic key sizes [***256-bit***].

5.1.2.9 HTTPS Protocol (ASPP14:FCS_HTTPS_EXT.1/Client)

ASPP14:FCS_HTTPS_EXT.1.1/Client
The application shall implement the HTTPS protocol that complies with RFC 2818.

ASPP14:FCS_HTTPS_EXT.1.2/Client
The application shall implement HTTPS using TLS as defined in the Functional Package for TLS.

ASPP14:FCS_HTTPS_EXT.1.3/Client
The application shall [***notify the user and not establish the user-initiated connection***] if the peer certificate is deemed invalid.

5.1.2.10 Random Bit Generation Services (ASPP14:FCS_RBG_EXT.1)

ASPP14:FCS_RBG_EXT.1.1
The application shall [***implement DRBG functionality***] for its cryptographic operations.

5.1.2.11 Random Bit Generation from Application (ASPP14:FCS_RBG_EXT.2)

ASPP14:FCS_RBG_EXT.2.1
The application shall perform all deterministic random bit generation (DRBG) services in accordance with NIST Special Publication 800-90A using [***CTR_DRBG (AES)***].

ASPP14:FCS_RBG_EXT.2.2
The deterministic RBG shall be seeded by an entropy source that accumulates entropy from a platform-based DRBG and [***no other noise source***] 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.

5.1.2.12 Secure Real-Time Transport Protocol (VVoIPAS10:FCS_SRTP_EXT.1)

VVoIPAS10: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.

VVoIPAS10:FCS_SRTP_EXT.1.2
The TSF shall implement SDES-SRTP supporting the following cipher suites: [***AES_256_CM_HMAC_SHA1_80, in accordance with RFC 6188, AEAD_AES_256_GCM, in accordance with RFC 7714***].

VVoIPAS10:FCS_SRTP_EXT.1.3
The TSF shall ensure the SRTP NULL algorithm can be disabled.

VVoIPAS10:FCS_SRTP_EXT.1.4
The TSF shall allow the SRTP ports to be used for SRTP communications to be specified by an Authorized Administrator.

5.1.2.13 Storage of Credentials (ASPP14:FCS_STO_EXT.1)

ASPP14:FCS_STO_EXT.1.1
The application shall [***invoke the functionality provided by the platform to securely store [secret and private keys]***] to non-volatile memory.

5.1.2.14 TLS Protocol (PKGTLS11:FCS_TLS_EXT.1)

PKGTLS11:FCS_TLS_EXT.1.1
The product shall implement [***TLS as a client***]

5.1.2.15 TLS Client Protocol (PKGTLS11:FCS_TLSC_EXT.1)

PKGTLS11:FCS_TLSC_EXT.1.1
The product shall implement TLS 1.2 (RFC 5246) and [***no earlier TLS versions***] as a client that

supports the cipher suites [***TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289, TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289***] and also supports functionality for [***mutual authentication***] (TD0442 applied)

PKGTLS11:FCS_TLSC_EXT.1.2

The product shall verify that the presented identifier matches the reference identifier according to RFC 6125.

PKGTLS11:FCS_TLSC_EXT.1.3

The product shall not establish a trusted channel if the server certificate is invalid [***with no exceptions***]

5.1.2.16 TLS Client Support for Mutual Authentication (PKGTLS11:FCS_TLSC_EXT.2)

PKGTLS11:FCS_TLSC_EXT.2.1

The product shall support mutual authentication using X.509v3 certificates.

5.1.2.17 TLS Client Support for Signature Algorithms Extension (PKGTLS11:FCS_TLSC_EXT.3)

PKGTLS11:FCS_TLSC_EXT.3.1

The product shall present the signature_algorithms extension in the Client Hello with the supported_signature_algorithms value containing the following hash algorithms: [***SHA384, SHA512***] and no other hash algorithms.

5.1.2.18 TLS Client Support for Renegotiation (PKGTLS11:FCS_TLSC_EXT.4)

PKGTLS11:FCS_TLSC_EXT.4.1

The product shall support secure renegotiation through use of the 'renegotiation_info' TLS extension in accordance with RFC 5746.

5.1.2.19 TLS Client Support for Supported Groups Extension (PKGTLS11:FCS_TLSC_EXT.5)

PKGTLS11:FCS_TLSC_EXT.5.1

The product shall present the Supported Groups Extension in the Client Hello with the supported groups [***secp384r1***]

5.1.3 User data protection (FDP)

5.1.3.1 Encryption Of Sensitive Application Data (ASPP14:FDP_DAR_EXT.1)

ASPP14:FDP_DAR_EXT.1.1

The application shall [***protect sensitive data in accordance with FCS_STO_EXT.1***] in non-volatile memory.

5.1.3.2 Access to Platform Resources (ASPP14:FDP_DEC_EXT.1)

ASPP14:FDP_DEC_EXT.1.1

The application shall restrict its access to [***network connectivity, camera, microphone, Bluetooth, [biometrics, notifications, external storage]***].

ASPP14:FDP_DEC_EXT.1.2

The application shall restrict its access to [***address book***].

5.1.3.3 Subset Information Flow Control (VVoIPAS10:FDP_IFC.1)

VVoIPAS10:FDP_IFC.1.1

The TSF shall enforce the media transmission policy on voice/video media transmitted by the TOE.

5.1.3.4 Simple Security Attributes (VVoIPAS10:FDP_IFF.1)

VVoIPAS10:FDP_IFF.1.1
The TSF shall enforce the media transmission policy based on the following types of subject and information security attributes: TOE hook state, VVoIP call connection status, and VVoIP call control server status.

VVoIPAS10:FDP_IFF.1.2
The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold:
- The TOE is [***registered with a VVoIP call control server***],
- A call has been established with a telephony device (VVoIP endpoint),
- The TOE is in the off-hook state,
- The TOE is not in the mute state,
- [***no other rules***].

VVoIPAS10:FDP_IFF.1.3
The TSF shall enforce no additional information flow control policy rules.

VVoIPAS10:FDP_IFF.1.4
The TSF shall explicitly authorize an information flow based on the following rules: no additional rules.

VVoIPAS10:FDP_IFF.1.5
The TSF shall explicitly deny an information flow based on the following rules: all TCP and UDP ports used by the TOE are closed when not in active use.

5.1.3.5 Network Communications (ASPP14:FDP_NET_EXT.1)

ASPP14:FDP_NET_EXT.1.1
The application shall restrict network communication to [***user-initiated communication for [registration of the client with an SCA, initiation of an outgoing call, and sending encrypted instant messages], respond to [an incoming call, receipt of an encrypted instant message]***].

5.1.4 Identification and authentication (FIA)

5.1.4.1 X.509 Certificate Validation (ASPP14:FIA_X509_EXT.1)

ASPP14:FIA_X509_EXT.1.1
The application shall [***implement functionality***] to validate certificates in accordance with the following rules:
- RFC 5280 certificate validation and certificate path validation.
- The certificate path must terminate with a trusted CA certificate.
- The application shall validate a certificate path by ensuring the presence of the basicConstraints extension, that the CA flag is set to TRUE for all CA certificates, and that any path constraints are met.
- The application shall validate that any CA certificate includes caSigning purpose in the key usage field
- The application shall validate the revocation status of the certificate using [***CRL as specified in RFC 8603***]
- The application shall validate the extendedKeyUsage (EKU) field according to the following rules:

o 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) in the extendedKeyUsage field.

o 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 EKU field.

o Client certificates presented for TLS shall have the Client Authentication purpose (id-kp 2 with OID 1.3.6.1.5.5.7.3.2) in the EKU field.

o S/MIME certificates presented for email encryption and signature shall have the Email Protection purpose (id-kp 4 with OID 1.3.6.1.5.5.7.3.4) in the EKU field.
o OCSP certificates presented for OCSP responses shall have the OCSP Signing purpose (id-kp 9 with OID 1.3.6.1.5.5.7.3.9) in the EKU field.
o Server certificates presented for EST shall have the CMC Registration Authority (RA) purpose (id-kpcmcRA with OID 1.3.6.1.5.5.7.3.28) in the EKU field.

ASPP14:FIA_X509_EXT.1.2
The application shall treat a certificate as a CA certificate only if the basicConstraints extension is present and the CA flag is set to TRUE.

5.1.4.2 X.509 Certificate Authentication (ASPP14:FIA_X509_EXT.2)

ASPP14:FIA_X509_EXT.2.1
The application shall use X.509v3 certificates as defined by RFC 5280 to support authentication for [***HTTPS, TLS***]

ASPP14:FIA_X509_EXT.2.2
When the application cannot establish a connection to determine the validity of a certificate, the application shall [n***ot accept the certificate***].

5.1.5 Security management (FMT)

5.1.5.1 Secure by Default Configuration (ASPP14:FMT_CFG_EXT.1)

ASPP14:FMT_CFG_EXT.1.1
The application shall provide only enough functionality to set new credentials when configured with default credentials or no credentials.

ASPP14:FMT_CFG_EXT.1.2
The application shall be configured by default with file permissions which protect the application's binaries and data files from modification by normal unprivileged user.

5.1.5.2 Supported Configuration Mechanism (ASPP14:FMT_MEC_EXT.1)

ASPP14:FMT_MEC_EXT.1.1
The application shall [***invoke the mechanisms recommended by the platform vendor for storing and setting configuration options***]

5.1.5.3 Specification of Management Functions (ASPP14:FMT_SMF.1)

ASPP14:FMT_SMF.1.1
The TSF shall be capable of performing the following management functions [***[Specify the SIP Server to use for connections.]***].

5.1.5.4 Specification of Management Functions (VVoIP Communications) (VVoIPAS10:FMT_SMF.1/VVoIP)

VVoIPAS10:FMT_SMF.1.1/VVoIP
The TSF shall be capable of performing the following management functions:
- Ability to [***register the TOE to an ESC [manually]***];
[***No other capabilities***].

5.1.6 Privacy (FPR)

5.1.6.1 User Consent for Transmission of Personally Identifiable (ASPP14:FPR_ANO_EXT.1)

ASPP14:FPR_ANO_EXT.1.1
The application shall [***not transmit PII over a network***].

5.1.7 Protection of the TSF (FPT)

5.1.7.1 Anti-Exploitation Capabilities (ASPP14:FPT_AEX_EXT.1)

ASPP14:FPT_AEX_EXT.1.1
The application shall not request to map memory at an explicit address except for [**none**].

ASPP14:FPT_AEX_EXT.1.2
The application shall [***not allocate any memory region with both write and execute permissions***].

ASPP14:FPT_AEX_EXT.1.3
The application shall be compatible with security features provided by the platform vendor.

ASPP14:FPT_AEX_EXT.1.4
The application shall not write user-modifiable files to directories that contain executable files unless explicitly directed by the user to do so.

ASPP14:FPT_AEX_EXT.1.5
The application shall be built with stack-based buffer overflow protection enabled.

5.1.7.2 Use of Supported Services and APIs (ASPP14:FPT_API_EXT.1)

ASPP14:FPT_API_EXT.1.1
The application shall use only documented platform APIs.

5.1.7.3 Software Identification and Versions (ASPP14:FPT_IDV_EXT.1)

ASPP14:FPT_IDV_EXT.1.1
The application shall be versioned with [***/a multi-part unique release number/***]

5.1.7.4 Use of Third Party Libraries (ASPP14:FPT_LIB_EXT.1)

ASPP14:FPT_LIB_EXT.1.1
The application shall be packaged with only **[*libraries shown in the following table***].

Android & iOS	Android Only	iOS Only
• webrtc 1.1.0 • Boost 1.79.0 • ZLIB 1.2.13 • BZip2 1.0.8 • Openssl 1.0.2zf • pjproject 2.12.1 • PocoCpp 1.9.1 • libphonenumber 8.12.25 • icu 63.1 • protobuf 3.21.8 • opus 1.1.3 • silk 1.0.9 • libsrtp 2.4.2 • pcsclite 1.8.9	• com.android.tools:desugar_jdk_libs:1.1.5 • androidx.lifecycle:lifecycle-common-java8:2.4.0 • org.androidannotations:androidannotations:4.8.0 • com.github.bumptech.glide:compiler:4.12.0 • org.androidannotations:androidannotations-api:4.8.0 • com.github.bumptech.glide:glide:4.12.0 • com.github.bumptech.glide:annotations:4.12.0 • com.github.chrisbanes:PhotoView:2.3.0 • androidx.appcompat:appcompat:1.2.0 • androidx.swiperefreshlayout:swiperefreshlayout:1.1.0 • androidx.biometric:biometric:1.1.0 • androidx.constraintlayout:constraintlayout:2.1.3 • androidx.recyclerview:recyclerview-selection:1.1.0 • androidx.lifecycle:lifecycle-process:2.4.0 • com.google.android.material:material:1.2.1 • joda-time:joda-time:2.1 • com.madgag.spongycastle:core:1.54.0.0 • com.madgag.spongycastle:prov:1.54.0.0 • com.madgag.spongycastle:pkix:1.54.0.0 • com.madgag.spongycastle:pg:1.54.0.0 • com.facebook.shimmer:shimmer:0.5.0 • androidx.emoji:emoji:1.2.0-alpha03	• YYImage 1.0.4

	• androidx.emoji:emoji-bundled:1.2.0-alpha03 • com.google.android.gms:play-services-base:18.1.0 • com.google.firebase:firebase-messaging:23.0.0 • com.journeyapps:zxing-android-embedded:4.3.0	

5.1.7.5 Integrity for Installation and Update (ASPP14:FPT_TUD_EXT.1)

ASPP14:FPT_TUD_EXT.1.1
The application shall [***leverage the platform***] to check for updates and patches to the application software.

ASPP14:FPT_TUD_EXT.1.2
The application shall [***leverage the platform***] to query the current version of the application software.

ASPP14:FPT_TUD_EXT.1.3
The application shall not download, modify, replace or update its own binary code.

ASPP14:FPT_TUD_EXT.1.4
Application updates shall be digitally signed such that the application platform can cryptographically verify them prior to installation.

ASPP14:FPT_TUD_EXT.1.5
The application is distributed [***as an additional software package to the platform OS***].

5.1.7.6 Trusted Update (VVoIPAS10:FPT_TUD_EXT.1)

VVoIPAS10:FPT_TUD_EXT.1.1
The application shall [***leverage the platform***] to check for updates and patches to the application software.

VVoIPAS10:FPT_TUD_EXT.1.2
The application shall [***leverage the platform***] to query the current version of the application software.

VVoIPAS10:FPT_TUD_EXT.1.3
The application shall not download, modify, replace or update its own binary code.

VVoIPAS10:FPT_TUD_EXT.1.4
Application updates shall be digitally signed such that the application platform can cryptographically verify them prior to installation.

VVoIPAS10:FPT_TUD_EXT.1.5
The application is distributed [***as an additional software package to the platform OS***].

5.1.7.7 Integrity for Installation and Update (ASPP14:FPT_TUD_EXT.2)

ASPP14:FPT_TUD_EXT.2.1
The application shall be distributed using **[*the format of the platform-supported package manager*]**. (TD0628 applied)

ASPP14:FPT_TUD_EXT.2.2
The application shall be packaged such that its removal results in the deletion of all traces of the application, with the exception of configuration settings, output files, and audit/log events

ASPP14:FPT_TUD_EXT.2.3
The application installation package shall be digitally signed such that its platform can cryptographically verify them prior to installation.

5.1.8 TOE access (FTA)

5.1.8.1 Media TSF-Initiated Termination (Media Channel) (VVoIPAS10:FTA_SSL.3/Media)

VVoIPAS10:FTA_SSL.3.1/Media
The TSF shall terminate voice/video transmission after inactivity longer than [***[15] seconds***].

5.1.9 Trusted path/channels (FTP)

5.1.9.1 Protection of Data in Transit (ASPP14:FTP_DIT_EXT.1)

ASPP14:FTP_DIT_EXT.1.1

The application shall [***encrypt all transmitted [data] with [TLS as a client as defined in the Functional Package for TLS, HTTPS as a client in accordance with FCS_HTTPS_EXT.1/Client]***] between itself and another trusted IT product.

5.1.9.2 Protection of Data in Transit (VVoIPAS10:FTP_DIT_EXT.1)

VVoIPAS10:FTP_DIT_EXT.1.1

The application shall [***- encrypt all transmitted [data] with TLS as defined in the TLS Package and [Secure Real-Time Transport Protocol (SRTP)]***]
between itself and another trusted IT product.

5.1.9.3 Inter-TSF Trusted Channel (Signaling Channel) (VVoIPAS10:FTP_ITC.1/Control)

VVoIPAS10:FTP_ITC.1.1/Control

The TSF shall be capable of using [***Session Initiation Protocol (SIP)***] to provide a trusted communication channel between itself and a VVoIP call control server that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from disclosure and detection of modification of the channel data.

VVoIPAS10:FTP_ITC.1.2/Control

The TSF shall permit the TSF, the VVoIP call control server to initiate communication via the trusted channel.

VVoIPAS10:FTP_ITC.1.3/Control

The TSF shall initiate communication via the trusted channel for establishment of call control.

5.1.9.4 Inter-TSF Trusted Channel (Media Channel) (VVoIPAS10:FTP_ITC.1/Media)

VVoIPAS10:FTP_ITC.1.1/Media

The TSF shall be capable of using [***SRTP***] to provide a trusted communication channel between itself and another VVoIP endpoint or other telephony device that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from disclosure and detection of modification of the channel data.

VVoIPAS10:FTP_ITC.1.2/Media

The TSF shall permit the TSF, another VVoIP endpoint or other telephony device to initiate communication via the trusted channel.

VVoIPAS10:FTP_ITC.1.3/Media

The TSF shall initiate communication via the trusted channel for transmission of voice/video media.

5.2 TOE Security Assurance Requirements

The SARs for the TOE are the components as specified in Part 3 of the Common Criteria. Note that the SARs have effectively been refined with the assurance activities explicitly defined in association with both the SFRs and SARs.

Requirement Class	Requirement Component
ADV: Development	ADV_FSP.1: Basic Functional Specification
AGD: Guidance documents	AGD_OPE.1: Operational User Guidance
	AGD_PRE.1: Preparative Procedures
ALC: Life-cycle support	ALC_CMC.1: Labelling of the TOE
	ALC_CMS.1: TOE CM Coverage
	ALC_TSU_EXT.1: Timely Security Updates

ATE: Tests	ATE_IND.1: Independent Testing Conformance
AVA: Vulnerability assessment	AVA_VAN.1: Vulnerability Survey

Table 2 Assurance Components

5.2.1 Development (ADV)

5.2.1.1 Basic Functional Specification (ADV_FSP.1)

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.

ADV_FSP.1.1c
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 TSFIs in the functional specification.

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.

5.2.2 Guidance documents (AGD)

5.2.2.1 Operational User Guidance (AGD_OPE.1)

AGD_OPE.1.1d
The developer shall provide the TOE, including its preparative procedures.

AGD_OPE.1.1c
The operational user guidance shall describe, for each user role, the 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 each user role, 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 each user role, 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 each user role, 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 each user role, describe the security measures to be followed in order to fulfill 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.

AGD_OPE.1.1e

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

5.2.2.2 Preparative Procedures (AGD_PRE.1)

AGD_PRE.1.1d

The developer shall provide the TOE, including its preparative procedures.

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.

AGD_PRE.1.1e

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

AGD_PRE.1.2e

The evaluator shall apply the preparative procedures to confirm that the TOE can be prepared securely for operation.

5.2.3 Life-cycle support (ALC)

5.2.3.1 Labelling of the TOE (ALC_CMC.1)

ALC_CMC.1.1d

The developer shall provide the TOE and a reference for the TOE.

ALC_CMC.1.1c

The application shall be labelled with a unique reference.

ALC_CMC.1.1e

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

5.2.3.2 TOE CM Coverage (ALC_CMS.1)

ALC_CMS.1.1d

The developer shall provide a description in the TSS of how timely security updates are made to the TOE. Application developers must support updates to their products for purposes of fixing security vulnerabilities.

ALC_CMS.1.1c

The configuration list shall include the following: the TOE itself; and the evaluation evidence required by the SARs.

ALC_CMS.1.2c

The configuration list shall uniquely identify the configuration items.

ALC_CMS.1.1e
The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.2.3.3 Timely Security Updates (ALC_TSU_EXT.1)

ALC_TSU_EXT.1.1d
The developer shall provide a description in the TSS of how timely security updates are made to the TOE. Note: Application developers must support updates to their products for purposes of fixing security vulnerabilities.

ALC_TSU_EXT.1.2d
The developer shall provide a description in the TSS of how users are notified when updates change security properties or the configuration of the product.

ALC_TSU_EXT.1.1c
The description shall include the process for creating and deploying security updates for the TOE software.

ALC_TSU_EXT.1.2c
The description shall express the time window as the length of time, in days, between public disclosure of a vulnerability and the public availability of security updates to the TOE.

ALC_TSU_EXT.1.3c
The description shall include the mechanisms publicly available for reporting security issues pertaining to the TOE.

Note: The reporting mechanism could include web sites, email addresses, as well as a means to protect the sensitive nature of the report (e.g., public keys that could be used to encrypt the details of a proof-of-concept exploit).

ALC_TSU_EXT.1.1e
The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.2.4 Tests (ATE)

5.2.4.1 Independent Testing - Conformance (ATE_IND.1)

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

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

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.

5.2.5 Vulnerability assessment (AVA)

5.2.5.1 Vulnerability Survey (AVA_VAN.1)

AVA_VAN.1.1d
The developer shall provide the TOE for testing.

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

AVA_VAN.1.1e
The evaluator shall confirm that the information provided meets all 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 on the identified potential vulnerabilities, to determine that the TOE is resistant to attacks performed by an attacker possessing Basic attack potential.

6. TOE Summary Specification

This chapter describes the security functions:

- Communication
- Cryptographic support
- User data protection
- Identification and authentication
- Security management
- Privacy
- Protection of the TSF
- TOE access
- Trusted path/channels

6.1 Communication

The Communication function satisfies the following security functional requirements:

- VVoIPAS10:FCO_VOC_EXT.1: The TOE uses the Opus codec by default, which utilizes a fixed bit-rate value. The TOE also includes the SILK codec as a secondary codec for backwards compatibility with older versions of the TOE. SILK is a variable bit-rate codec by default, however the TOE utilizes a custom build that includes a bit-rate padding to make the codec a fixed bit-rate value. The SILK codec is only used if the peer device doesn't support the Opus codec.

6.2 Cryptographic support

The TOE contains its own internal FIPS cryptographic object module for cryptographic algorithm support. The module also uses OpenSSL 1.0.2zf with support for vulnerability patches. The TOE uses OpenSSL for TLS and certificate checking. The TOE generates random numbers using the internal module's SP 800-90A AES-CTR DRBG. The TOE leverages the client device platform RBG to seed the internal FIPS object module DRBG. The client device platform RBG functionality is invoked as follows.

- On Samsung devices, random seed data is read by invoking the java.security.SecureRandom cryptographic security API
- On Apple devices, random seed data is obtained by invoking SecRandomCopyBytes that reads random data from /dev/random.

The CAVP certificates shown as **A2639** in **Table 3 Cryptographic Functions** were obtained during the evaluation testing.

Samsung Galaxy S20 5G

Apple iPhone 11

Table 3 Cryptographic Functions

Functions	Requirement	Cert #
Encryption/Decryption		
AES GCM (256 bits)	ASPP14:FCS_COP.1/SKC	**A2639**
Cryptographic hashing		
SHA-1, SHA-256, SHA-384, SHA-512 (digest sizes 160, 256, 384, 512)	ASPP14:FCS_COP.1/Hash VVoIPAS10:FCS_COP.1/SRTP	**A2639**
Cryptographic signature services		

FIPS 186-4 Elliptic Curve Digital Signature Algorithm (ECDSA) with an elliptical curve size of 256 or 384 bits FIPS 186-4 RSA Digital Signature with 2048 or 3072 bit keys (verification only)	ASPP14:FCS_COP.1/Sig	**A2639**
Keyed-hash message authentication		
HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512 (digest sizes 160, 256, 384, 512)	ASPP14:FCS_COP.1/KeyedHash VVoIPAS10:FCS_COP.1/SRTP	**A2639**
Encryption/Decryption for SRTP		
AES-CTR (256 bit) AES-GCM (256-bit)	VVoIPAS10:FCS_COP.1/SRTP	**A2639**
Random bit generation		
SP 800-90A CTR_DRBG with sw based noise sources with a minimum of 256 bits of non-determinism	ASPP14:FCS_RBG_EXT.2	**A2639**
Asymmetric Key Generation		
FIPS 186-4 ECDSA Key Generation P-256, 384	ASPP14:FCS_CKM.1/AK	**A2639**
Key Establishment		
SP 800-56Ar3 Elliptic curve-based key establishment schemes	ASPP14:FCS_CKM.2	**A2639**

The TOE generates TLS key exchange keys using P-384. The TOE also supports generating P-256 keys for backwards compatibility with older Blackberry SecuGATE SIP servers. On Android, the TOE uses the internal cryptographic module's asymmetric key generation services to generate asymmetric keys. On iOS, the TOE invokes platform provided functionality to generate asymmetric keys. The TOE uses Security Framework from iOS, specifically the APIs in /System/Library/Frameworks/Security.framework/Security.

The TOE supports SRTP protocol as described by RFC 3711 using Security Descriptions for Media Streams (SDES) in compliance with RFC 4568. The SRTP session is negotiated via the SecuGATE SIP server (also known as the ESC). The TOE supports both AEAD_AES_256_GCM and AES_256_CM_HMAC_SHA1_80 ciphersuites for SDES-SRTP. The TOE and its VoIP peer must be registered to a SIP server (SecuGATE) in order to communicate with each other. The TOE does not allow the NULL algorithm to be specified and will reject connections from an endpoint that use any invalid algorithm, including the NULL ciphersuite. The SRTP destination ports that shall be used for a specific call are ‘negotiated’ between RTP Proxy and SIP Server and included into the SDES body of the forwarded SIP messages. The admin can restrict the port range in the SIP server configuration.

The TOE uses SHA-256 as the SIP message digest authentication mechanism during a SIP transaction. All SIP messages are protected via TLS. The TOE supports HMAC-SHA-1 in the SRTP ciphersuite. The TOE supports both SHA-256 and SHA-384 in digital signatures. The TOE supports SHA-384 and SHA-512 in the TLS signature algorithms extension.

The SRTP destination ports that shall be used for a specific call are ‘negotiated’ between RTP Proxy and SIP Server and included into the SDES body of the forwarded SIP messages. The admin can restrict the port range in the SIP server configuration.

The TOE presents the signature_algorithms extension in the Client Hello with the supported signature algorithms. The TOE supports SHA-384 and SHA-512 only. These are the values supported by default and cannot be changed. The TOE rejects any connection in which a certificate is not using a supported signature algorithm.

The TOE supports the following ciphersuites with only TLS v1.2 communication:

- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384

- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384

All older versions of TLS are rejected. The TOE also support mutual authentication during a TLS negotiation.

The Cryptographic support function satisfies the following security functional requirements:

- ASPP14:FCS_CKM.1: On the Android platform, the TOE uses its internal FIPS object module to generate keys. For the iOS platform, the TOE uses platform provided API to generate keys.
- ASPP14:FCS_CKM.1/AK: The TOE supports asymmetric key generation for TLS key exchange. The TOE generates TLS key exchange keys using P-384. The TOE also supports generating P-256 keys for backwards compatibility with older Blackberry SecuGATE SIP servers.
- ASPP14:FCS_CKM.2: The TOE supports key establishment using Elliptic curve-based schemes described above for TLS key exchange.
- ASPP14:FCS_COP.1/Hash: The TOE performs hashing operations using the internal FIPS object module SHA cryptographic functions described above.
- ASPP14:FCS_COP.1/KeyedHash: The TOE performs HMAC operations using the internal FIPS object module HMAC cryptographic functions described above.
- ASPP14:FCS_COP.1/Sig: The TOE performs signature operations using the internal FIPS object module cryptographic functions described above. The TOE supports RSA key sizes of 2048 and 3072 bits, and ECDSA curve sizes of P-256 and P-384.

  The TOE performs RSA signature verification only. The TOE only has an ECDSA certificate for mutual authentication. The TOE can connect to a SecuGATE server that might be configured to send an RSA server certificate to the TOE. In this case, the TOE can only verify the RSA certificate signature, and the TOE will send an ECDSA certificate to the server during mutual authentication.
- ASPP14:FCS_COP.1/SKC: The TOE performs encryption and decryption operations using the internal FIPS object module AES cryptographic functions described above.
- VVoIPAS10:FCS_COP.1/SRTP: The TOE supports SDES-SRTP as described above, in accordance with AES-CTR (as defined in NIST SP 800-38A) using 256-bit keys.
- ASPP14:FCS_HTTPS_EXT.1/Client: The TOE conforms to RFC 2818 by securing HTTPS with TLSv1.2. The TOE uses TLS to protect communications with SecuGATE for all activities such as client configuration and certificate enrollment. The TOE's TLS implementation has been tested in accordance with the activities in the Functional Package for Transport Layer Security (TLS), version 1.1. The TOE always checks the peer's certificate.
- ASPP14:FCS_RBG_EXT.1: The TOE leverages platform RBG services to seed its own internal FIPS object module CTR_DRBG(AES) as described above.
- ASPP14:FCS_RBG_EXT.2: The TOE implements its own CTR_DRBG(AES) which is seeded from platform RBG services with a minimum of 256 bits of entropy.
- VVoIPAS10:FCS_SRTP_EXT.1: The TOE supports SRTP as described above.
- ASPP14:FCS_STO_EXT.1: The TOE stores X509v3 certificate private keys and the SRTP encryption key persistently. The TOE uses X509 certificates to authenticate to SecuGATE when performing TLS. The TOE uses an AES key to encrypt SRTP media during a call session. The TOE stores the data when not in use in client device platform-provided key storage as follows:
  - Samsung: Android KeyStore
  - Apple: iOS keychain
- PKGTLS11:FCS_TLS_EXT.1: The TOE acts as a TLS client.
- PKGTLS11:FCS_TLSC_EXT.1: The TOE supports TLS communication with mutual authentication as described above. The TOE uses the connection URL as the reference identifier to compare against the identifier in the peer's certificate. The TOE supports both CN and SAN reference identifier checking, with

the SAN check preferred over CN. The TOE verifies the certificate received matches the reference identifier for the expected peer. The TOE does not accept certificates that cannot be determined to be valid, with no exceptions. The TOE does not support pinned certificates and URIs. Wildcards are not supported.

- PKGTLS11:FCS_TLSC_EXT.2: The TOE authenticates its TLS peer using x509v3 certificates and presents a certificate at the request of its peer.
- PKGTLS11:FCS_TLSC_EXT.3: The TOE sends a client hello with a signature_algorithms extension to show supported signature algorithms as described above.
- PKGTLS11:FCS_TLSC_EXT.4: The TOE supports session renegotiation in accordance with RFC 5746. The TOE includes the SCSV ciphersuite in the Client Hello handshake message.
- PKGTLS11:FCS_TLSC_EXT.5: The TOE supports the Supported Groups Extension in the TLS handshake process. The TOE uses secp384r1 as the supported group in the TLS key exchange packets.

6.3 User data protection

The TOE enforces a media transmission policy between registered VVoIP endpoints. The VVoIP endpoints are identified by an E.164 telephone number (SIP alias). The TOE mediates the creation of SRTP channels between registered VVoIP endpoints, ensuring that both endpoints are properly identified. The TOE permits SRTP traffic only when the following conditions are true:

- the client TOE must be registered with the ESC,
- a call has been established with a VVoIP endpoint,
- the TOE is not in the 'off-hook' state, and
- the TOE is not in the 'mute' state.

The TOE allows messages to be sent securely between two VVoIP endpoints. The TOE uses the same SIP-TLS protections on the secure text messages sent between two users of the TOE application.

The TOE enforces no additional information flow control policy rules, nor does it explicitly authorize or deny any information flows.

All TCP and UDP ports previously used by the TOE are closed when a call is terminated.

The User data protection function satisfies the following security functional requirements:

- ASPP14:FDP_DAR_EXT.1: The TOE's sensitive data includes secret and private keys. The TOE also receives a SIP password sent by the SecuGATE. The TOE protects secret and private keys by storing the keys using the platform provided key storage. This is in accordance with the selection made in FCS_STO_EXT.1. The TOE protects the SIP password storage on Android by saving the password in a file with the MODE_PRIVATE flag set, which is Android's default mode for creating files that give exclusive access to the application. On iOS, the TOE relies on the default iOS NSFileProtectionCompleteUntilFirstUserAuthentication data protection class to store all application files.
- ASPP14:FDP_DEC_EXT.1: The TOE restricts its access to the network connectivity, camera, microphone, Bluetooth, biometrics, notifications, and external storage.

  Network connectivity - SecuSUITE requires access to a network to communicate with the SecuGATE server.

  · Camera - SecuSUITE allows scanning of a QR code using the phone's camera.

  · Microphone - SecuSUITE uses the microphone to record voice data.

  · Bluetooth - SecuSUITE can use Bluetooth devices, such as Bluetooth headsets.

  · Biometrics - The platform OS might use biometrics as the authentication factor. SecuSUITE requests access to use the platform keystore via biometrics if the phone is set up with a biometric authentication factor.

  · Notifications - SecuSUITE sends notifications to the user of incoming calls, texts and alerts.

· External Storage - SecuSUITE's text messaging system allows attachments, which are possibly stored in the phone's external storage.

The TOE also restricts its access to the address book as the only sensitive information repository.

- VVoIPAS10:FDP_IFC.1: The TOE enforces its voice/video media transmission policy as described above.
- VVoIPAS10:FDP_IFF.1: The TOE enforces its voice/video media transmission policy as described above.
- ASPP43:FDP_NET_EXT.1: The TOE restricts its network communication to include only registration of the client with an SCA, initiation of an outgoing call, accepting/rejecting an incoming call, and sending/receiving a secure text message.

6.4 Identification and authentication

The Identification and authentication function satisfies the following security functional requirements:

- ASPP14:FIA_X509_EXT.1: Certificates are validated as part of the authentication process when they are presented to the TOE and when they are loaded into the TOE. The TOE requires the certificate to contain a SAN extension. The following fields are verified as appropriate: SAN checks, key usages, chain validation, expiration status, and revocation status. Chain validation includes ensuring that all certificates representing a CA indicate so using the basicConstraints CA flag having a value of TRUE. Revocation checking is also performed using a Certificate Revocation List. Wildcards are not allowed in certificates.
- ASPP14:FIA_X509_EXT.2: The TOE utilizes OpenSSL version 1.0.2zf to perform TLS communications and X509 certificate checking. The TOE has multiple interfaces that use TLS:

  SCA Registration (TCP port 3978): This channel is for the initial set up to register the TOE to the SecuGATE.

  SIP communications (TCP port 5061): This channel is used for securing the media channel setup between the TOE and SecuGATE.

  Secure client authentication (TCP port 5062): This channel is used in secure communications with SecuGATE for activities such as updating configuration and secure contacts.

  In all cases, the TOE checks the TLS peer's certificate. The TOE only supports mutual authentication when it connects to SecuGATE for SIP communications and secure client authentication. Certificates are provisioned by the SecuGATE SIP Server during SCA registration. The TOE uses certificates automatically, and these certificates are exchanged during TLS negotiations for the media and configuration communications with SecuGATE. If the TOE determines the certificates from the peer are not valid, the certificates are not accepted and the TOE rejects the connection attempt. If an otherwise valid certificate cannot have its CRL checked to confirm that the certificate is not revoked, the certificate is not accepted and the TOE rejects the connection.

6.5 Security management

The SIP client and server use username and passwords to allow the client to access the SIP server and SCA server (separate passwords). These passwords are transmitted during initial SCA registration in the SIP Settings response and are stored persistently by the TOE. The TOE uses soft key storage to protect these secrets.

During initial start-up, the user needs to enter an activation code to start the initial registration. The Activation code is a shared secret between the server and the client used only during initial registration. Without the initial registration the client application cannot communicate with the SIP server. The client does not install with any default credentials and the TOE does not require any credentials to provide access to the TOE.

The key chain of the TOE soft key store anchors in a secret stored to the platform key stores (key chain) and hence the user must unlock the keystore (using platform features such as fingerprint or device password) to open the application.

The TOE supports the following management functions[2]:

- Specify the SIP Server to use for connections. User can enter SCA Server address during the activation phase which determines the SIP server. Note: This is the only parameter that the user can configure via the TOE.

The SCA server pushes configuration settings including username and password during registration. This configuration is created on the ESC and is used by the TOE. These setting configure the following:

- SIP Password which is a randomly generated 24 character alphanumeric values that is generated on the SCA server and transmitted within the SIP settings response of the SCA protocol.
- Configure cryptographic algorithms associated with protocols mandated in this PP. The algorithms are selected by the SIP server during TLS handshake.
- Load X5.09v3 certificates used for security functions in this PP – the client's X.509v3 certificates are generated during registration with the SCA server.
- Configure certificate revocation check. There are no configurable parameters for revocation checking.

The client device platform performs the following management functions:

- Ability to update the TOE, and to verify the updates. The user may uninstall or update the TOE using the mobile device operating system and app store. Downloaded TOE updates (apps) are verified using digital signatures in accordance with supported mobile device Security Targets for Android and iOS platforms.

The Security management function satisfies the following security functional requirements:

- ASPP14:FMT_CFG_EXT.1: Prior to registration with the SCA server, the client is presented with the activation screen and cannot leave that screen until a valid Activation Code is presented to the SIP server.
- ASPP14:FMT_MEC_EXT.1: The TOE stores application configuration options for Android platforms in an XML file at location /data/data/package/shared_prefs, For iOS platforms the TOE stores application configuration options using the user defaults system (which includes UserDefaults and NSUserDefaults APIs). The TOE's SIP configuration is stored locally, but established and modified by the remote SCA or SIP server. Neither the TOE nor platform offer the ability to configure the TOE's SIP settings locally.
- ASPP14:FMT_SMF.1: The TOE provides management functions identified above.
- VVoIPAS10:FMT_SMF.1/VVoIP: The TOE provides the following management operations:
  - Ability to register the TOE to an ESC manually

  The TOE requires the operator to enter in the server address to register the TOE with the ESC. This is done either by manual input or by scanning a QR code.

6.6 Privacy

The Privacy function satisfies the following security functional requirements:

- ASPP14:FPR_ANO_EXT.1: The TOE does not collect any PII and does not transmit any PII over a network.

6.7 Protection of the TSF

The TOE is physically protected by the boundary of the evaluated device. The TOE is executed on an evaluated Android 11 or iOS 14 device. Under Android, the TOE is constructed as a Java Application that executes most security relevant code in the native layer implemented in C/C++ (as a shared library). This Java code primary purpose is to provide the UI Implementation. For iOS, the TOE is constructed as a native application implemented in objective C and C++.

Memory mapping and permissions on memory regions are not functions applicable to a Java application. However, some 3rd party libraries are written in a language other than Java and thus are subject to the requirement for Anti-Exploitation Capabilities. However, none of the 3rd party libraries used by the TOE request memory mapping at explicit addresses, and none allocate memory for both write and execute permission.

Android's application management requires application updates to be signed with an Android key, thus allowing the secure updates of its applications. The Android OS Linux kernel is capable of ASLR (address space layout randomization), ensuring that no application uses the same address layout on two different devices.

The TOE libraries are also compiled with the '-fstack-protector-all -fno-exceptions' flags in order to enable ASLR and stack-based buffer over flow protections. On iOS the ASLR feature (-pie) is not set by a compiler flag, because it is on by default on the C-language compiler. This setting is required by the Apple App store.

The TOE is assigned a version[3] number by the vendor which is constructed using the following convention.

<major release>.<minor release>. <build number>.<year><week><debug>

For example, a release number might be 3.0.244.19100. This is interpreted as follows:

Major: 3
Minor: 0
Build: 244
Year: 2019
Week:10
Debug:0 (0:release; 1:debug build)

Major numbers represent significant product changes, while minor numbers are incremented for feature improvements and bug fixes. The Build number, year, week and debug state round out the identification of the software providing increased uniqueness.

The product includes the following 3rd party libraries:

Android & iOS	Android Only	iOS Only
• webrtc 1.1.0 • Boost 1.79.0 • ZLIB 1.2.12 • BZip2 1.0.8 • Openssl 1.0.2zf • pjproject 2.12.1 • PocoCpp 1.9.1 • libphonenumber 8.12.25 • icu 63.1 • protobuf 3.19.4 • opus 1.1.3 • silk 1.0.9 • libsrtp 2.4.2 • pcsclite 1.8.9	• com.android.tools:desugar_jdk_libs:1.1.5 • androidx.lifecycle:lifecycle-common-java8:2.4.0 • org.androidannotations:androidannotations:4.8.0 • com.github.bumptech.glide:compiler:4.12.0 • org.androidannotations:androidannotations-api:4.8.0 • com.github.bumptech.glide:glide:4.12.0 • com.github.bumptech.glide:annotations:4.12.0 • com.github.chrisbanes:PhotoView:2.3.0 • androidx.appcompat:appcompat:1.2.0 • androidx.swiperefreshlayout:swiperefreshlayout:1.1.0 • androidx.biometric:biometric:1.1.0 • androidx.constraintlayout:constraintlayout:2.1.3 • androidx.recyclerview:recyclerview-selection:1.1.0 • androidx.lifecycle:lifecycle-process:2.4.0 • com.google.android.material:material:1.2.1 • joda-time:joda-time:2.1 • com.madgag.spongycastle:core:1.54.0.0 • com.madgag.spongycastle:prov:1.54.0.0 • com.madgag.spongycastle:pkix:1.54.0.0 • com.madgag.spongycastle:pg:1.54.0.0 • com.facebook.shimmer:shimmer:0.5.0 • androidx.emoji:emoji:1.2.0-alpha03 • androidx.emoji:emoji-bundled:1.2.0-alpha03	• YYImage 1.0.4

[3] The vendor refers to this identifier as a release number.

	• com.google.android.gms:play-services-base:18.0.1 • com.google.firebase:firebase-messaging:23.0.0 • com.journeyapps:zxing-android-embedded:4.3.0	

The user may install or update the TOE using the respective mobile device operating system app store. Alternatively, an MDM may be used to push the TOE app and updates to the user's mobile device – in such cases user interaction/acceptance is still required. In either case, the TOE platform checks the signature of any update before the update is applied. TOE updates are signed with the BlackBerry software signing key associated with each platform. Downloaded TOE updates (apps) are verified using digital signatures in accordance with supported mobile device Security Targets (as mentioned in the TOE Overview).

Candidate updates are obtained via each TOE platform's respective app store or via an MDM. The TOE platform always checks the signatures of the update files before the updates are applied, whether the app is obtained via the app store or through an MDM.

The Protection of the TSF function satisfies the following security functional requirements:

- ASPP14:FPT_AEX_EXT.1: The TOE does not make requests to map memory at an explicit address, nor does it allocate any memory region with both write and execute permissions. Refer to the above discussion for more information.
- ASPP14:FPT_API_EXT.1: The TOE uses platform services by using only documented platform provided APIs. The specific interfaces used by the TOE on Android and iOS platforms are provided in section 7.
- ASPP14:FPT_IDV_EXT.1: The TOE identifies software as described above.
- ASPP14:FPT_LIB_EXT.1: The TOE includes the 3rd party libraries listed above.
- ASPP14:FPT_TUD_EXT.1/ASPP14:ALC_TSU_EXT.1: The TOE is distributed using the Android application package (APK) format on an Android platform and using the IPA format on an iOS platform. The TOE is distributed as an additional software package, and is installed using the respective app store of each platform.

  The TOE relies upon the platform to provide a mechanism that can check for product updates, to query the current version of the TOE, and to support the installation of an update as described above. The Android platform uses the Google Play Store, and the iOS platform uses the Apple App Store. Both app stores require developers to digitally sign their applications with a key recognized by each respective app store. This signature is used to verify that the application is from a trusted source. BlackBerry provides timely security updates for the TOE in case vulnerabilities have been discovered. Reported vulnerabilities and defects are investigated and rated based on the threat and result of the impact analysis and then scheduled for an upcoming bug fix release based on the severity. BlackBerry aims for a security update between 10 and a maximum of 50 days. Third party library updates are also included as a part of the TOE's update. BlackBerry accepts vulnerability reports through the BlackBerry form at https://www.blackberry.com/us/en/forms/enterprise/contact-us.
- ASPP14:FPT_TUD_EXT.2: These platforms force the TOE to write all data within the application working directory (sandbox), thus ensuring the application's removal results in the deletion of all traces of the application, with the exception of configuration settings, output files, and audit/log events. Blackberry is an authorized source as they are a vendor that obtained official signing keys from Google and Apple in order to publish the TOE application on both the Google Play Store and Apple App Store. The application signature is verified by each respective platform.

6.8 TOE access

SecuGATE enforces a default timeout of 15 seconds for the SRTP channel. Only SecuGATE can configure the SRTP timeout value via SCA registration between the TOE and SecuGATE.

The TOE access function satisfies the following security functional requirements:

- VVoIPAS10:FTA_SSL.3/Media: The configuration loaded into the TOE during registration includes the configured interval for termination of an idle voice/video transmission.

6.9 Trusted path/channels

The Trusted path/channels function satisfies the following security functional requirements:

- ASPP14:FTP_DIT_EXT.1: This SFR is superseded by FTP_DIT_EXT.1 from VVoIPAS10, which allows communication using SRTP as well as TLS.
- VVoIPAS10:FTP_DIT_EXT.1: The TOE encrypts all data transmitted between itself, an Enterprise Session Controller and another VVoIP endpoint using SIP over TLS, TLS and SRTP. The TOE uses these protocols to protect SIP signaling, VoIP calls, and secure text messaging.
- VVoIPAS10:FTP_ITC.1/Control: The TOE uses SIP for all data transmitted between itself and an Enterprise Session Controller for the purpose of communicating with another VVoIP endpoint. The SIP communication occurs within the context of an already established TLS session. The TOE or ESC can initiate SIP communication in the existing TLS session.
- VVoIPAS10:FTP_ITC.1/Media: The TOE uses SRTP as a trusted channel to communicate with a proxy on SecuGATE. Using this proxy, the TOE can communicate with another VVoIP endpoint for media traffic. The STRP cryptographic parameters are passed between the TOE and the other VVoIP endpoint using SIP messages protected by TLS (traffic that is part of FTP_ITC.1/Control). The TOE can either initiate or receive voice/video media traffic.

7. API used by the TOE

The TOE uses platform services by using only documented platform provided APIs.

7.1 Android platform interfaces invoked by the TOE

The following are the platform APIs invoked by the TOE when running on an Android platform.

android.animation.Animator
android.animation.AnimatorListenerAdapter
android.animation.ArgbEvaluator
android.animation.LayoutTransition
android.animation.ObjectAnimator
android.animation.PropertyValuesHolder
android.animation.ValueAnimator
android.annotation.SuppressLint
android.annotation.TargetApi
android.app.Activity
android.app.ActivityManager
android.app.AlarmManager
android.app.AlertDialog
android.app.Application
android.app.Dialog
android.app.IntentService
android.app.KeyguardManager
android.app.Notification
android.app.NotificationChannel
android.app.NotificationManager
android.app.PendingIntent
android.app.Service
android.app.TimePickerDialog
android.bluetooth.BluetoothAdapter
android.bluetooth.BluetoothHeadset
android.bluetooth.BluetoothProfile
android.content.ActivityNotFoundException
android.content.BroadcastReceiver
android.content.ClipboardManager
android.content.ClipData
android.content.ComponentName
android.content.ContentResolver
android.content.ContentValues
android.content.Context
android.content.CursorLoader
android.content.DialogInterface
android.content.Intent
android.content.IntentFilter
android.content.pm.ActivityInfo
android.content.pm.PackageInfo
android.content.pm.PackageManager
android.content.res.ColorStateList
android.content.res.Configuration
android.content.res.Resources
android.content.RestrictionsManager
android.content.res.TypedArray
android.content.res.XmlResourceParser
android.content.ServiceConnection
android.content.SharedPreferences
android.database.ContentObserver
android.database.Cursor
android.database.DataSetObserver
android.graphics.Bitmap
android.graphics.BitmapFactory
android.graphics.Canvas
android.graphics.Color
android.graphics.ColorFilter
android.graphics.DashPathEffect
android.graphics.drawable.BitmapDrawable
android.graphics.drawable.Drawable
android.graphics.LinearGradient
android.graphics.Matrix
android.graphics.Paint
android.graphics.PathEffect
android.graphics.PixelFormat
android.graphics.PorterDuff
android.graphics.PorterDuffXfermode
android.graphics.Rect
android.graphics.RectF
android.graphics.Region
android.graphics.Shader
android.graphics.Typeface
android.hardware.fingerprint.FingerprintManager
android.hardware.Sensor
android.hardware.SensorEvent
android.hardware.SensorEventListener
android.hardware.SensorManager
android.Manifest
android.media.AudioDeviceInfo
android.media.AudioManager
android.media.AudioRecordingConfiguration
android.media.ExifInterface
android.media.MediaPlayer
android.media.RingtoneManager
android.media.ThumbnailUtils
android.net.ConnectivityManager
android.net.NetworkInfo
android.net.Uri
android.net.wifi.WifiManager
android.os.Binder
android.os.Build
android.os.Bundle
android.os.Environment
android.os.Handler
android.os.IBinder
android.os.Looper
android.os.Parcelable
android.os.PowerManager

android.os.PowerManager.WakeLock
android.os.SystemClock
android.os.Vibrator
android.preference.PreferenceManager
android.provider.CallLog
android.provider.ContactsContract
android.provider.ContactsContract
android.provider.DocumentsContract
android.provider.MediaStore
android.provider.Settings
android.provider.Telephony
android.security.KeyPairGeneratorSpec
android.security.keystore.KeyGenParameterSpec
android.security.keystore.KeyPermanentlyInvalidated Exception
android.security.keystore.KeyProperties
android.security.keystore.KeyProtection
android.telephony.PhoneNumberFormattingTextWat cher
android.telephony.PhoneNumberUtils
android.telephony.SmsManager
android.telephony.SmsMessage
android.telephony.TelephonyManager
android.text.Editable
android.text.format.DateFormat
android.text.Html
android.text.Layout
android.text.Spannable
android.text.SpannableString
android.text.style.AlignmentSpan
android.text.style.StyleSpan
android.text.TextUtils
android.text.TextWatcher
android.util.AttributeSet
android.util.Base64
android.util.Base64
android.util.Log
android.util.Log
android.util.LongSparseArray
android.util.Pair
android.util.SparseArray
android.util.SparseBooleanArray
android.util.TypedValue
android.view.ActionMode
android.view.animation.AccelerateInterpolator
android.view.animation.Animation
android.view.animation.AnimationUtils
android.view.animation.DecelerateInterpolator
android.view.animation.ScaleAnimation
android.view.ContextMenu
android.view.Display
android.view.GestureDetector
android.view.Gravity
android.view.inputmethod.InputMethodManager
android.view.KeyEvent
android.view.LayoutInflater
android.view.Menu
android.view.MenuInflater
android.view.MenuItem
android.view.MotionEvent
android.view.SubMenu
android.view.View
android.view.ViewGroup
android.view.ViewGroup.LayoutParams
android.view.View.OnClickListener
android.view.View.OnFocusChangeListener
android.view.View.OnLongClickListener
android.view.View.OnTouchListener
android.view.Window
android.view.WindowManager
android.widget.AbsListView
android.widget.Adapter
android.widget.AdapterView
android.widget.AdapterView.OnItemClickListener
android.widget.AdapterView.OnItemLongClickListe ner
android.widget.ArrayAdapter
android.widget.BaseAdapter
android.widget.BaseExpandableListAdapter
android.widget.Button
android.widget.Checkable
android.widget.CheckBox
android.widget.CheckedTextView
android.widget.Chronometer
android.widget.EditText
android.widget.ExpandableListView
android.widget.Filter
android.widget.Filterable
android.widget.FrameLayout
android.widget.ImageButton
android.widget.ImageView
android.widget.LinearLayout
android.widget.ListAdapter
android.widget.ListView
android.widget.ProgressBar
android.widget.RelativeLayout
android.widget.ScrollView
android.widget.SectionIndexer
android.widget.SeekBar
android.widget.SeekBar.OnSeekBarChangeListener
android.widget.TextView
android.widget.TimePicker
android.widget.Toast
androidx.annotation.CallSuper
androidx.annotation.NonNull
androidx.annotation.Nullable
androidx.appcompat.app.ActionBar
androidx.appcompat.app.ActionBarDrawerToggle
androidx.appcompat.app.AlertDialog
androidx.appcompat.app.AppCompatActivity
androidx.appcompat.graphics.drawable.DrawerArro wDrawable

androidx.appcompat.widget.SearchView
androidx.biometric.BiometricConstants
androidx.biometric.BiometricManager
androidx.biometric.BiometricPrompt
androidx.biometric.BiometricPrompt.Authentication Callback
androidx.core.app.ActivityCompat
androidx.core.app.NotificationCompat
androidx.core.content.ContextCompat
androidx.core.view.GestureDetectorCompat
androidx.core.view.MenuItemCompat
androidx.core.view.ViewCompat
androidx.core.view.ViewPropertyAnimatorListener
androidx.drawerlayout.widget.DrawerLayout
androidx.fragment.app.DialogFragment
androidx.fragment.app.Fragment
androidx.fragment.app.FragmentActivity
androidx.fragment.app.FragmentManager
androidx.fragment.app.ListFragment
androidx.lifecycle.Lifecycle
androidx.lifecycle.LifecycleObserver
androidx.lifecycle.OnLifecycleEvent
androidx.lifecycle.ProcessLifecycleOwner
androidx.localbroadcastmanager.content.LocalBroadcastManager
androidx.swiperefreshlayout.widget.SwipeRefreshLayout
java.io.BufferedReader
java.io.ByteArrayInputStream
java.io.ByteArrayOutputStream
java.io.File
java.io.FileInputStream
java.io.FileOutputStream
java.io.FileReader
java.io.InputStream
java.io.InputStreamReader
java.io.IOException
java.io.IOException
java.io.Serializable
java.io.Serializable
java.io.UnsupportedEncodingException
java.lang.reflect.Field
java.lang.reflect.Method
java.math.BigInteger
java.net.Inet4Address
java.net.Inet6Address
java.net.InetAddress
java.net.NetworkInterface
java.nio.ByteBuffer
java.nio.file.Path
java.nio.file.Paths
java.security.cert.Certificate
java.security.cert.CertificateException
java.security.cert.CertificateFactory
java.security.cert.CertificateParsingException
java.security.cert.X509Certificate
java.security.InvalidAlgorithmParameterException
java.security.KeyFactory
java.security.KeyPair
java.security.KeyPairGenerator
java.security.KeyStore
java.security.KeyStoreException
java.security.NoSuchAlgorithmException
java.security.NoSuchProviderException
java.security.Principal
java.security.PrivateKey
java.security.PublicKey
java.security.SecureRandom
java.security.Security
java.security.Signature
java.security.spec.PKCS8EncodedKeySpec
java.security.spec.X509EncodedKeySpec
java.text.DateFormat
java.text.ParseException
java.text.SimpleDateFormat
java.util.ArrayList
java.util.Arrays
java.util.Calendar
java.util.Collection
java.util.Collections
java.util.Comparator
java.util.concurrent.atomic.AtomicBoolean
java.util.concurrent.atomic.AtomicInteger
java.util.concurrent.Callable
java.util.concurrent.ConcurrentHashMap
java.util.concurrent.ConcurrentSkipListMap
java.util.concurrent.CopyOnWriteArrayList
java.util.concurrent.CopyOnWriteArraySet
java.util.concurrent.Executors
java.util.concurrent.ExecutorService
java.util.concurrent.Future
java.util.concurrent.LinkedBlockingQueue
java.util.concurrent.TimeUnit
java.util.Date
java.util.Enumeration
java.util.HashMap
java.util.HashSet
java.util.Iterator
java.util.List
java.util.Locale
java.util.Map
java.util.Queue
java.util.regex.Matcher
java.util.regex.Pattern
java.util.Scanner
java.util.Set
java.util.SortedMap
java.util.StringTokenizer
java.util.UUID
java.util.zip.ZipEntry
java.util.zip.ZipInputStream
javax.crypto.BadPaddingException

javax.crypto.Cipher
javax.crypto.CipherInputStream
javax.crypto.CipherOutputStream
javax.crypto.IllegalBlockSizeException
javax.crypto.KeyGenerator
javax.crypto.SecretKey
javax.crypto.spec.IvParameterSpec
javax.security.auth.x500.X500Principal
javax.xml.parsers.SAXParser
javax.xml.parsers.SAXParserFactory

7.2 iOS platform interfaces invoked by the TOE

The following are the platform interfaces invoked by the TOE when running on an iOS platform.

Payload/SecuSUITE.app/SecuSUITE:

/System/Library/Frameworks/PushKit.framework/PushKit (compatibility version 1.0.0, current version 1.0.0)
/System/Library/Frameworks/AddressBook.framework/AddressBook (compatibility version 1.0.0, current version 1.0.0)
/System/Library/Frameworks/AddressBookUI.framework/AddressBookUI (compatibility version 1.0.0, current version 33.0.0)
/System/Library/Frameworks/AudioToolbox.framework/AudioToolbox (compatibility version 1.0.0, current version 492.0.0)
/System/Library/Frameworks/AVFoundation.framework/AVFoundation (compatibility version 1.0.0, current version 2.0.0)
/System/Library/Frameworks/CFNetwork.framework/CFNetwork (compatibility version 1.0.0, current version 975.0.3)
/System/Library/Frameworks/Contacts.framework/Contacts (compatibility version 0.0.0, current version 0.0.0)
/System/Library/Frameworks/CoreAudio.framework/CoreAudio (compatibility version 1.0.0, current version 1.0.0)
/System/Library/Frameworks/CoreGraphics.framework/CoreGraphics (compatibility version 64.0.0, current version 1245.9.2)
/System/Library/Frameworks/CoreTelephony.framework/CoreTelephony (compatibility version 1.0.0, current version 0.0.0)
/System/Library/Frameworks/Foundation.framework/Foundation (compatibility version 300.0.0, current version 1560.10.0)
/System/Library/Frameworks/UIKit.framework/UIKit (compatibility version 1.0.0, current version 61000.0.0)
/System/Library/Frameworks/SystemConfiguration.framework/SystemConfiguration (compatibility version 1.0.0, current version 963.200.27)
/System/Library/Frameworks/Accelerate.framework/Accelerate (compatibility version 1.0.0, current version 4.0.0)
/System/Library/Frameworks/CoreFoundation.framework/CoreFoundation (compatibility version 150.0.0, current version 1560.10.0)
/System/Library/Frameworks/QuartzCore.framework/QuartzCore (compatibility version 1.2.0, current version 1.11.0)
/System/Library/Frameworks/Security.framework/Security (compatibility version 1.0.0, current version 58286.222.2)
/System/Library/Frameworks/UserNotifications.framework/UserNotifications (compatibility version 1.0.0, current version 1.0.0)
/usr/lib/libc++.1.dylib (compatibility version 1.0.0, current version 400.9.4)
/usr/lib/libobjc.A.dylib (compatibility version 1.0.0, current version 228.0.0)