Administrative Guidance Document

Cellcrypt Classified 2

Ref:	AGD
Ver:	1.2
Date:	April 12, 2019
Author:	Acumen Security, LCC

Table of Contents

1. Introduction

1.1. Target of Evaluation

The Cellcrypt Classified 2 (hereafter referred to as the TOE) is a VOIP application for secure encrypted voice calls designed to run on standard mobile phones, blending features such as authenticated connection set-up , end-to-end encryption, mutual authentication with the SIP server (also known as ESC server) by implementing X509 certificates etc., into a single software package.

The TOE runs on Android 7.0 based platform. The logical scope of the TOE comprises:

- Authenticated connection set-up with a SIP server
- End-to-end encryption used by the TOE when encrypting/decrypting secure voice traffic

1.1. Typical Deployment

The TOE is available for Business to Business communications that is typically deployed on end user's mobile phone, and is paired with a SIP server and one VOIP peer. The SIP server facilitates the secure encrypted voice calls between and provides a centralized location for collecting information from two or more endpoints. A typical deployment would include one TOE , one SIP server and one peer. The following diagram illustrates this visually.

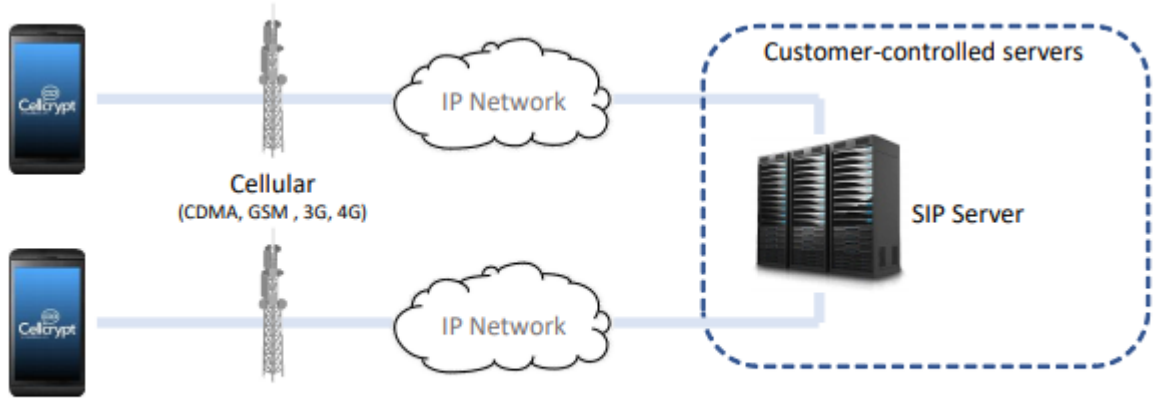


Figure 1 Cellcrypt Classified Architecture

2. Evaluation Platforms

Certification evaluation has been performed on the following Android platform:

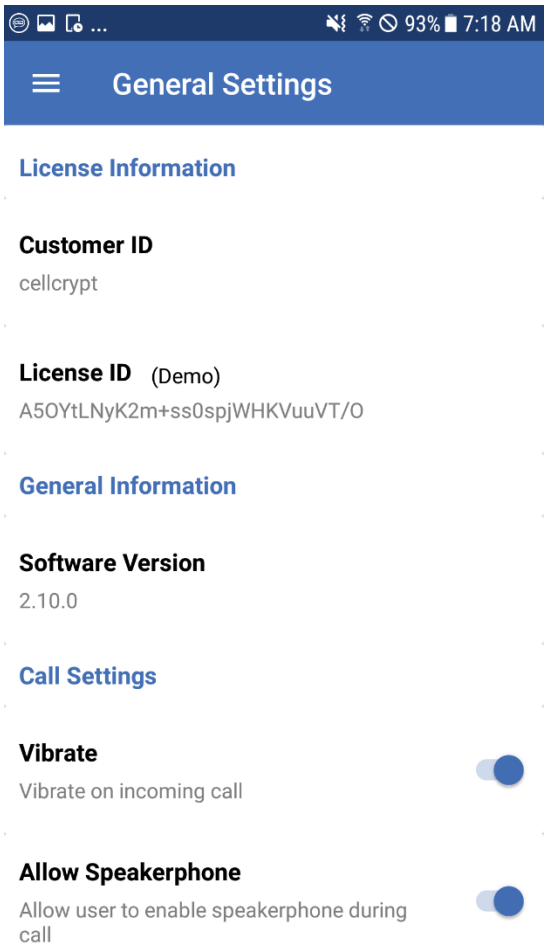
- Samsung Galaxy S7 running Android 7.0
  - Snapdragon 820 ARMv8 processor

2.1. Versioning

The following selection in in the GUI prompts the TOE to verify the running version of software.

- **General Settings -> Software Version**

The following screenshot shows an example of the command being executed,


93% 7:18 AM
General Settings
License Information
Customer ID
cellcrypt
License ID (Demo)
A5OYtLNyK2m+ss0spjWHKVuuVT/O
General Information
Software Version
2.10.0
Call Settings
Vibrate
Vibrate on incoming call
Allow Speakerphone
Allow user to enable speakerphone during call

3. Installation

The TOE is installed on end user devices using the Android Debug Bridge (ADB). To steps to install the TOE:

1. Download the TOE APK from CellCrypt (e.g. CCV2-2.10.0.apk).
2. Enable USB debugging on the user device.
3. Connect the user device to the computer running ADB using a USB cable.
4. On the command line run, “adb install CCV2-2.10.0.apk”

Follow the same process to update the TOE; however, add the “-r” flag in step 4 (e.g. “adb install -r CCV2-2.10.0.apk”).

After installation, the user will need to configure details such as Customer ID, License ID, Username, SIP server address, X.509 certificates for mutual authentication etc… Such details can be configured in:

- General Settings,
- SIP Settings and
- TLS Settings.

The cryptographic engine does not require any user configuration.

4. Uninstallation

The TOE can be uninstalled directly from the Android 7.0 platform by going to the Android home screen, tapping and holding the TOE icon for two seconds, and tapping “Uninstall”. Alternatively ADB can be used to uninstall the TOE by running “adb uninstall com.cellcrypt.cellcryptclassified”.

5. External Communications

The TOE restricts its communications to user-initiated communication for a SIP server, a VOIP peer, certificate validation using CRL, and retrieving idle timeout settings from a configuration server. No other communications are available. The TOE achieves end-to-end encryption using SDES-SRTP trusted channel. The keys for the SDES-SRTP trusted channel are protected by the TLS/SIP channel while the keys are being established. No configuration of the TLS version is necessary. The TOE only supports supported TLS version 1.2.

The supported ciphersuites include:

- TLS_RSA_WITH_AES_128_CBC_SHA as defined in RFC 5246
- TLS_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5246
- TLS_RSA_WITH_AES_256_CBC_SHA256 as defined in RFC 5246
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5246
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 as defined in RFC 5246
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5289
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5289
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289

Ciphersuites can be configured under “TLS Settings” → “TLS Cipher Suites”

The following elliptic curves are supported:

- secp256r1
- secp384r1
- secp521r1

Elliptic curves cannot be configured.

The following signature hash algorithms are supported:

- SHA-256
- SHA-384
- SHA-512

Signature hashes cannot be configured.

The supported SDES-SRTP ciphersuites include,

- AES_CM_128_HMAC_SHA1_80, in accordance with RFC 4568,
- AES_CM_128_HMAC_SHA1_32, in accordance with RFC 4568,
- AES_256_CM_HMAC_SHA1_80, in accordance with RFC 6188,
- AES_256_CM_HMAC_SHA1_32, in accordance with RFC 6188,
- AEAD_AES_128_GCM, in accordance with RFC7714,
- AEAD_AES_256_GCM, in accordance with RFC 7714.

5.1. Network Connectivity

The TOE requires network access. The connectivity is required for the following interactions:

- User-initiated communication for
  - a SIP server,
  - a VVoIP endpoint,
  - check for updates
- Certificate validation using CRL and
- Fetch timeout configuration from the configuration server.

The SIP server can be configured under “SIP Settings” while the update and configuration servers can be configured under “General Settings”.

6. X509 Certificate Usage

The TOE utilizes X509 Certificates to provide a mutual authentication for the trusted channel with the SIP server. The validity of the X509 certificates is checked by querying CRL(s). The TOE uses the TLSv1.2 protocol to protect all communications with the SIP server from modification and disclosure (described above). In addition to the X.509 Certificate authentication, the TOE authenticates to the SIP server using a password as an additional layer of security.

Navigate to TLS Settings → Certificate Settings to

- Load CA Certificate Chain
- Load existing X509 certificate,
- Configure CRL settings.

Navigate to TLS Settings → CRL Settings to

- Configure CRL Locations
- Configure CRL Refresh Interval

6.1. Setting Reference Identifier

In Cellcrypt Classified 2, navigate to “SIP settings” and Enter the IP address or FQDN of the SIP server.

6.2. Revocation Checking

Cellcrypt Classified 2 performs revocation checking on presented SIP server certificate via Certificate Revocation Lists (CRLs). The CRL can be configured in “TLS settings” -> “TLS Certificate Validation” -> CRL. The user should configure the “CRL Update Behaviour’ to “Connect only if all CRLs are up-to-date”. CRL location(s) can be configured in the TOE at “TLS Settings” -> “CRL 1 Location”. If the TOE is not able to confirm revocation status of the presented certificates, the TOE will reject the communications.

7. Additional Resource Requirements

In addition to requiring network access from the underlying platform, the TOE additionally requires access to the microphone and storage for local configuration.

End of Document