Honeywell

# Smart Talk 2.1

For Android and iOS

# Security Guide

# Disclaimer

Honeywell International Inc. (“HII”) reserves the right to make changes in specifications and other information contained in this document without prior notice, and the reader should in all cases consult HII to determine whether any such changes have been made. HII makes no representation or warranties regarding the information provided in this publication

HII shall not be liable for technical or editorial errors or omissions contained herein; nor for incidental or consequential damages resulting from the furnishing, performance, or use of this material. HII disclaims all responsibility for the selection and use of software and/or hardware to achieve intended results.

This document contains proprietary information that is protected by copyright. All rights are reserved. No part of this document may be photocopied, reproduced, or translated into another language without the prior written consent of HII.

Copyright © 2024 Honeywell Group of Companies. All rights reserved.

Web Address: sps.honeywell.com

# Trademarks

Android is a trademark of Google LLC.

Other product names or marks mentioned in this document may be trademarks or registered trademarks of other companies and are the property of their respective owners.

# Patents

For patent information, refer to www.hsmpats.com.

# TABLE OF CONTENTS


Customer Support ..... v
Technical Assistance ..... v

**Chapter 1 - Security Guide ..... 1**

About Smart Talk ..... 1
Protocol and Ports ..... 2
Flow Security ..... 2
TLS Flow ..... 2
Media Flow of Application Server ..... 3
Media Flow of WebChat Interface ..... 3
Authentication ..... 3
Identification, Authentication, and Authorization ..... 4
Secure Communication ..... 4
Defense in Depth ..... 5
Android Certificate Pinning ..... 6
Secure File Exchange ..... 6
Secure Operation and Key Management ..... 6
Mobile Application ..... 6
Web Application ..... 6
Threats ..... 7
Agents ..... 7
Scenarios ..... 7

# Customer Support

## Technical Assistance

To search our knowledge base for a solution or to log in to the Technical Support portal and report a problem, go to honeywell.com/PSStechnicalsupport.

CHAPTER

# 1 SECURITY GUIDE

## About Smart Talk

Smart Talk is a comprehensive and secure business communication solution that allows instant connection between remote teams. It is a fully customizable solution, tailored to the size and scope of any organization.

The Smart Talk app is designed for Android and iPhone. The browser-based version is called WebChat.

The supported services are:

- Safe and fully controlled environment
- Team management
- Business processes and business rules management
- Digital service for large organizations and companies
- Reliable solution for communication during crisis and/ or emergency situations.

Smart Talk supports users for both mobile and desktop systems:

- Mobile users access the Smart Talk solution through the dedicated application installed on their mobile equipment.
- Web (PC) users' access the Smart Talk solution through the WebChat application. WebChat is compatible with Firefox or Chrome.

Smart Talk consists of three main components: the Smart Talk Android and Smart Talk iOS Mobile applications and the Smart Talk Application Server.

- Smart Talk Application Server is designed to manage the mobile communication process and automation of notifications and consolidate all Instant Messenger, Voice, Video, File Transmission and GPS services, scheduling, reporting, and memberships management in a centralized management interface.
- Smart Talk Android and Smart Talk iOS are mobile applications for Android/iOS that provide an online chat with real-time data transmission. Messages can consist of text, images, videos, voices, files, or other content.

This document scopes the security of the application, analyzing the interactions and communication between modules and external devices, the local security, and potential threats.

# Protocol and Ports

The main protocols between application elements are:

- Configuration services: HTTP via TLS on port 443
- Messaging services: SIP over TLS on port 5228
- Exchange of attachments: HTTP over TLS on port 5223
- Media flow (audio, video): SRTP on UDP ports 20000 to 40000

The following table lists application modules facing the Internet and corresponding port numbers.

| Source | Destination | Protocol L4 | Dest Port | Application | Protocol | Comment |
|---|---|---|---|---|---|---|
| *Public network* | Backend | TCP | 5228<br>5223 | SwEngine | SIPS<br>HTTPS | SIPS for app Mobile<br>HTTPS upload/download for mobile client |
| *Public network* | Frontend / voip | TCP | 5228 | SwEngine | SIPS | SIPS for VoIP |
| *Public network* | Frontend / voip | TCP | 5063 | SwEngine | SIP over WSS | SIPS for WebChat |
| *Public network* | Frontend / voip | UDP | 7000-7300 | SwEngine | UDP | Flux SRTP |
| *Public network* | Frontend / voip | TCP | 9999 | SwEngine | TCP | ICE TCP for browsers |
| *Public network* | Frontend / voip | UDP | 10000-20000 | SwEngine | UDP | Media |
| *Public network* | Frontend / web | UDP | 20000-40000 | SwEngine | SRTP | Media, Flux SRTP |
| *Public network* | Frontend / web | TCP | 80, 443 | Nginx | HTTPS | Webchat - User Interface<br>Conf Service for Android App registration |
| *Public network* | Frontend / web | TCP | 443 | Nginx | HTTPS | SwAPI request interface |
| *Administrator network* | Frontend | TCP | 443 | Nginx | HTTPS | Superadmin web interface for TOTR Server administration |
| *Administrator network* | SwAPI Backend | TCP | 443 | Nginx | HTTPS | Communication between SwAPI Manager interface to SwAPI Backend |
| *Administrator network* | Backend | TCP | 443 | Nginx | HTTPS | Communication between Frontend to ResourceManager interface |
| *Public network* | Frontend / web | TCP | 443 | Nginx | HTTPS | Admin web interface for Organization administrators and SwAPI web interface |
| Frontend | Backend | TCP | 443 | Nginx | HTTPS | Communication between SwApi Frontend to SwAPI Backend fqdn |
| Backend | Frontend | TCP | 5063 | SwEngine | TCP | ResourceManager cron check the media resource |
| Backend | Frontend | TCP | 5228 | SwEngine | TCP | ResourceManager cron check the voip resource |
| Backend | Backend | TCP | 5228 | SwEngine | TCP | ResourceManager cron check the voip resource |
| Frontend | Backend | TCP | 8080 | Nginx | HTTPS | Communication between Frontend and Backend |
| Backend | Frontend | TCP | 8080 | Nginx | HTTPS | Web Service between Backend to Frontend |
| Frontend | Backend | TCP | 8080 | Nginx | HTTPS | Communication between SwApi Frontend and Backend |
| Frontend | Backend | TCP | 6379 | Redis | Redis | Redis from Frontend to Backend |
| *Public network* | Frontend / voip | TCP | 5080 | SwEngine InterAS | SIPS | communication between TOTR servers (Only for InterAS) |
| *Public network* | Frontend / voip | UDP | 10000 - 40000 | SwEngine InterAS | SRTP | communication between TOTR servers (Only for InterAS) |
| *Administrator network* | TOTR Server | TCP | 5080 | SwEngine InterAS | SIPS | communication between TOTR servers (Only for InterAS) |
| *Public network* | Backend | TCP | 8080 | Nginx InterAS | HTTPS | communication between TOTR servers (Only for InterAS) |
| *Administrator network* | Backend | TCP | 5080 | SwEngine InterAS | SIPS | communication between TOTR servers (Only for InterAS) |
| Frontend | Maps | TCP | 443 | Maps | HTTPS | |
| Backend | LDAP Server | TCP | 389 | LDAP | TCP | Communication for LDAP Sync to LDAP Server |
| Frontend | LDAP Server | TCP | 389 | LDAP | TCP | Communication for LDAP Login to LDAP Server |
| PBX Gateway | Frontend / voip | UDP | 5060 | SwEngine | SIP | Call-in feature from an external PBX Gateway |
| PBX Gateway | Frontend / voip | UDP | 10000-20000 | SwEngine | RTP | Call-in feature from an external PBX Gateway |
| Frontend / voip | PBX Gateway | UDP | 5060 | SwEngine | SIP | Call-out feature to an external PBX Gateway |
| Frontend / voip | PBX Gateway | UDP | 10000-20000 | SwEngine | RTP | Call-out feature to an external PBX Gateway |
| Frontend / voip | PCRF | TCP | 3868 | SwEngine | DIAMETER | |
| Frontend / voip | BMSC | TCP | 3868 | SwEngine | DIAMETER | |

# Flow Security

## TLS Flow

All TLS flows are configured to accept only the following configurations:

- TLS 1.2/1.3 protocol version
- No TLS_FALLBACK
- No TLS compression

- Only the following Ciphers:
  - ECDHE-RSA-AES256-GCM-SHA384
  - ECDHE-RSA-AES128-GCM-SHA256

Additionally, the mobile application does not use the list of certification authorities offered by the system, but it includes a private list inside the APK package, allowing certificate pinning.

By default, this list contains only a single authority provided by the customer. The list is set up at build time.

## Media Flow of Application Server

The media flows are encrypted using the AES256 algorithm with the keys generated on each session of the signalization flow.

## Media Flow of WebChat Interface

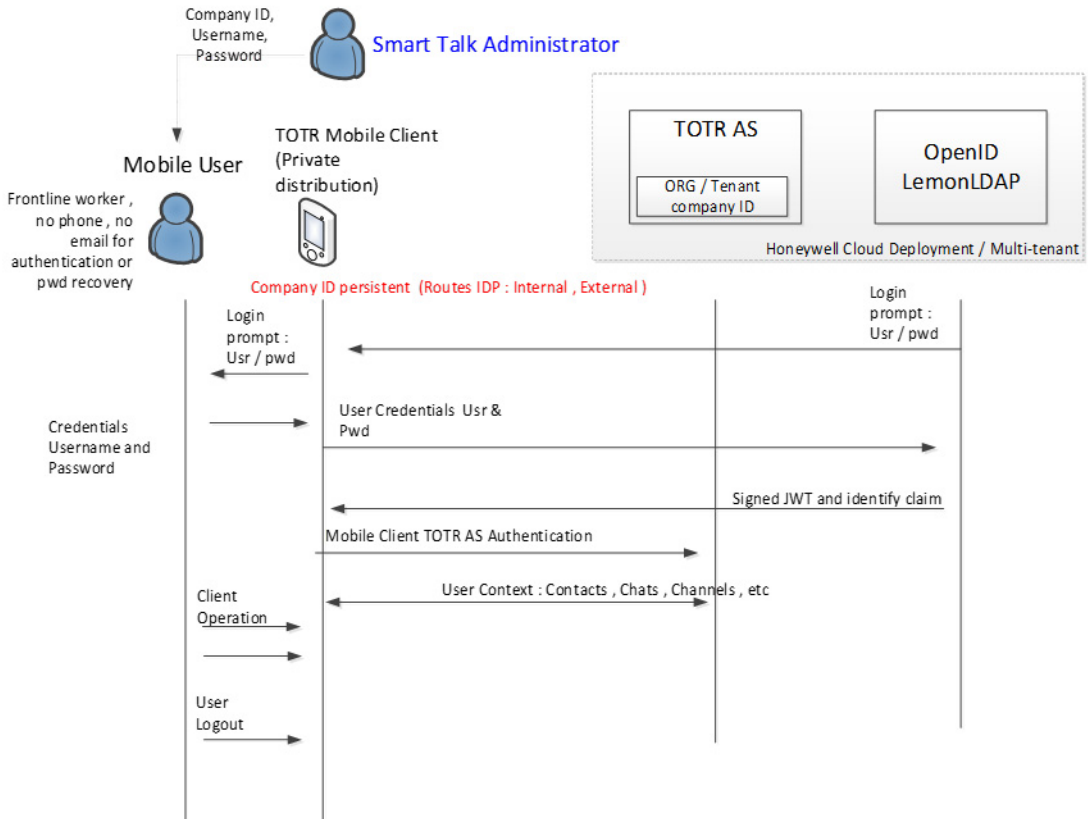
The media flows are encrypted using the AES128 (SRTP_AES128_CM_HMAC_SHA1_80) algorithm with the keys generated during the DTLS negotiation as defined by the standard WebRTC (TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 cipher suite and the P-256 curve.)

# Authentication

During installation, the user is required to provide three pieces of information provided by their Smart Talk administrator:

- Company ID
- Username
- Password

Based on these three pieces of information, the following takes place:




# Identification, Authentication, and Authorization

All users must authenticate with the solution before any information exchange.

After authentication, the server manages the access rights of the authenticated user and is responsible for sending to the application only the data that the user is authorized to access.

# Secure Communication

Messages and attachments (including private and group messages, files, geolocation, etc.) exchanged between users of the Mobile application are protected by the TLS 1.2/1.3 protocol. Real-time data is transported using the SRTP / SRTCP protocol. The protocols used are as follows:

- SIPS for messages and call signaling
- SRTP / SRTCP for real-time media streams (voice and video)
- HTTPS for attachments

The TLS session uses X.509v3 certificates installed on the server to validate the identity of the server. These certificates are signed by a certification authority provided by the customer. The certificate for this authority is included in the Android APK package and the application ignores certificates from the OS (certificate pinning).

For cryptographic operations, the application leverages the TLS 1.2/1.3 implementation provided by the Android OS and iOS for its SIPS/TLS and HTTPS / TLS communications. Additionally, the application disables the use of older versions of TLS.

In its use of the TLS library, the application limits cryptographic suites to the following two suites:

- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256

Media streams are protected using the SRTP_AES256_CM_HMAC_SHA1_80 cryptographic suite. (SHA1 is used for HMAC signature of packets due to the limitation of available suites in SRTP.)

SRTP session keys are generated in memory on the server and transmitted to the client during SDP negotiation included in SIPS call signaling messages.

# Defense in Depth

## Android

On startup, the Android Smart Talk app checks that:

- The terminal has the storage encryption feature enabled.
- The operating system is not “rooted.”
- The screen lock mechanism is active.
- The content of notifications on the lock screen is hidden.

If any of these conditions are not met, the application refuses to start.

The app allows screen capture when it is in the foreground.

In the event of theft or loss of the mobile device, it is possible to trigger the erasure of the data from the user management interface.

## iOS

Conditions for iOS are:

- The device is not jail-broken.
- The screen lock mechanism is active.
- The application does not start until the user first authenticates (unlock device).

If the user restarts the device and does not enter the access code, the app will not start. Once the user enters the code for the first time, the app will be accessible.

In the event of theft or loss of the mobile device, it is possible to trigger the erasure of the data from the user management interface.

## Android Certificate Pinning

The Smart Talk Mobile (both iOS and Android) application implements a certificate pinning mechanism to protect users against the threat of a rogue certificate authority that would allow a “man in the middle” attack. Pinning helps ensure that network data is not compromised even if the user has a malicious root certificate installed on their mobile device.

# Secure File Exchange

To limit the risk of infection, a message filtering system has been integrated. It allows attachments to be passed to a third-party web service. In the case of the antivirus, the web service checks with the antivirus whether the attachment is valid or not. If the attachment is invalid, the entire message is declined, and the sender is notified.

The antivirus is the responsibility of the customer. The web service must meet the specification on the next page.

***Note:*** *The antivirus feature is not available in the current Honeywell Smart Talk application.*

# Secure Operation and Key Management

## Mobile Application

The Smart Talk Mobile (both iOS and Android) application implements a certificate pinning mechanism to protect users against the threat of a rogue certificate authority that would allow a “man in the middle” attack. Pinning helps ensure that network data is not compromised even if the user has a malicious root certificate installed on their mobile device.

## Web Application

The Smart Talk Mobile (both iOS and Android) application implements a certificate pinning mechanism to protect users against the threat of a rogue certificate authority that would allow a “man in the middle” attack. Pinning helps ensure that network data is not compromised even if the user has a malicious root certificate installed on their mobile device.

# Threats

Threat agents are typically characterized by several factors such as expertise, available resources, and motivation, with the motivation being linked directly to the value of the assets at stake.

## Agents

Threat agents could be:

- External entities that are not authorized to access the application. These entities may attempt to get access to the application either by masquerading as an authorized entity or by attempting to use the application without proper authorization. External threat agents may also passively capture data transmitted between the TOE and the back-end server or actively manipulate such data.
- Local users that unintentionally try to read notifications even when the screen is locked, access information, or use resources stored locally that they are not authorized for. Moreover, a local user could try to access information or use resources that are accessible through Smart Talk but not stored locally, for instance, impersonate another user, subscribe to receive calls or messages intended for another user, etc.
- Other software that can be installed or downloaded on mobile equipment and give hackers the opportunity to gain access to the application and capture/ manipulate data belonging to it.

## Scenarios

The following threat scenarios are identified:

- T1 Network Attack: An attacker is positioned on a communications channel or elsewhere on the network infrastructure to perform a “man in the middle” attack and threatens the transmission of messages, attachments, media, or management data. The goal of the attacker is to gain access to or compromise (i.e., replacing or modifying the content) sensitive information (e.g., identifiers, certificates, secret keys, messages, voices, videos, files, etc.) exchanged between the Smart Talk Android application and the Smart Talk back-end server.
- T2 Local Access

  Physical: An attacker who has access to the mobile equipment (equipment theft) may try to:

  - Access sensitive data (encryption key, pre-shared key, messages, voices, videos, files) at rest stored by the Smart Talk Android application.
  - Interact with the Smart Talk Application Server to access information or use resources that are accessible through Smart Talk but not stored locally by the Smart Talk Android application.

Logical: Other software on the same mobile equipment might try to access sensitive data.

- T3 Limited Physical Access: An attacker having physical access may attempt to read sensitive data from notifications even when the screen of the mobile equipment is locked.
- T4 Privilege Escalation: A privilege escalation may occur which allows an attacker to add members to a discussion, take the PTT floor when not allowed, or access the location of other users, thus stealing sensitive data.

Honeywell
855 S. Mint St.
Charlotte, NC  28202

sps.honeywell.com