Technical Specifications for LeaveHomeSafe mobile app

Version: 1.7

April 2022

Office of the
Government Chief Information Officer

Revision History

Version	Description	Modified Date
1.0	Initial Draft	12 November 2020
1.1	Added App Version up to 1.1.7	24 March 2021
1.2	Added App Version from 1.1.8 to 2.0	1 June 2021
1.3	Up to App Version 2.0.1	15 June 2021
1.4	Up to App Version 2.1	21 July 2021
1.5	Up to App Version 3.0.0	20 November 2021
1.6	Up to App Version 3.0.2	14 January 2022
1.7	Up to App Version 3.2.0	12 April 2022

Table of Contents

1 Introduction

1.1. Background

The LeaveHomeSafe mobile app is to provide an effective QR-code based system for COVID-19 exposure notification in Hong Kong, based on a privacy-by-design and scalable approach. These technical specifications apply to app version from 1.1.7 to version 3.2.0.

(Note: Please refer to Section 5 for the glossary used in this document.)

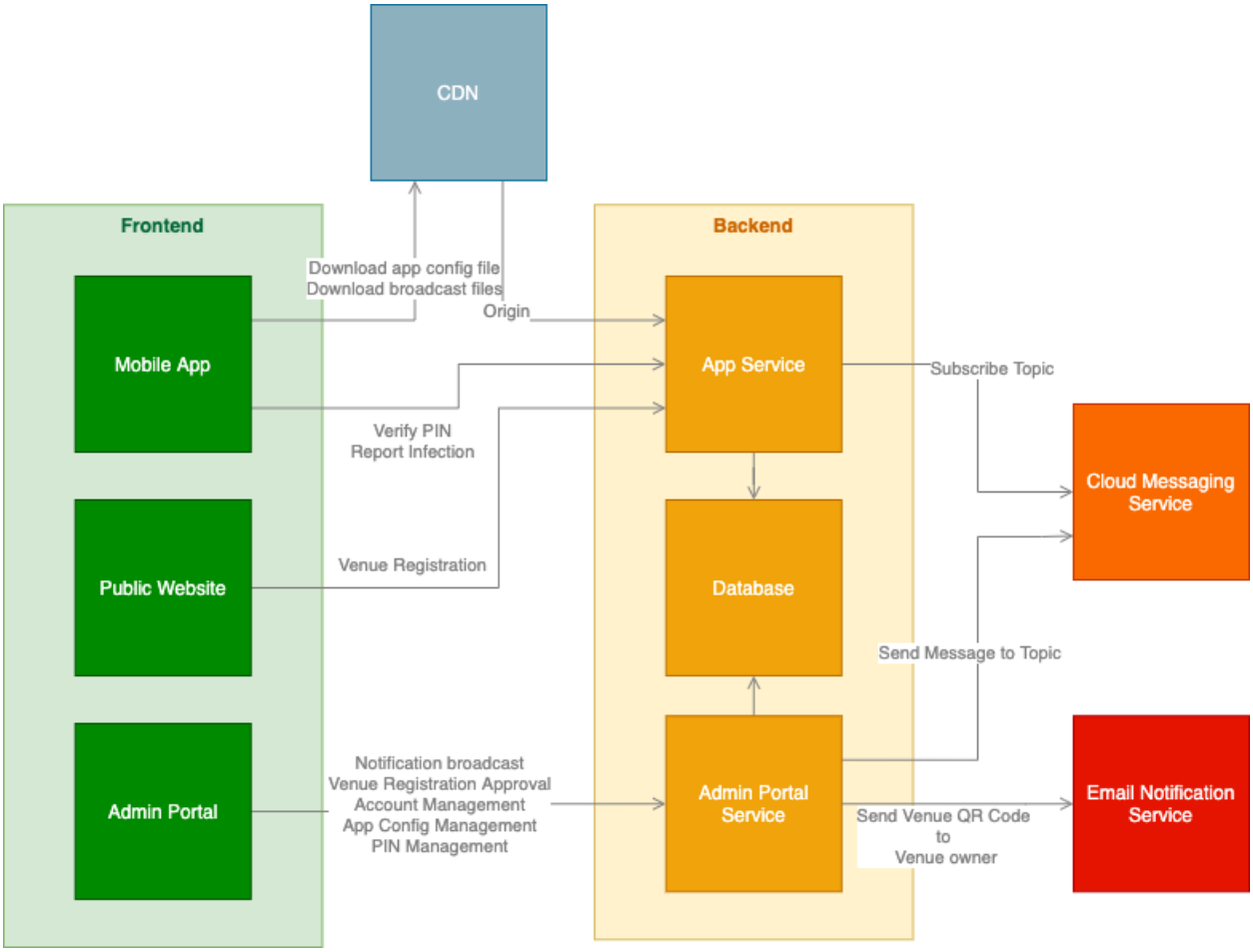
1.2. Objective

The purpose of this document is to provide the system design and the technical details of LeaveHomeSafe mobile app implementation.

2 System Design

2.1 System Diagram

This diagram shows the high-level functional blocks and the relationship among them.



Note: The arrow represents the dependency of the component.

Component	Description
Public website	LeaveHomeSafe introduction and venue registration submission (https://www.leavehomesafe.gov.hk)
Mobile App	LeaveHomeSafe mobile app
Admin Portal	Internal web portal which provides

Component	Description
	management functions for LeaveHomeSafe
App Service	Handles requests from website and mobile app
Admin Portal Service	Handles requests from Admin Portal and scheduled tasks including data cleansing
Database	Stores visit records of infected users, broadcasts files, LHS venues
Email Notification Service	Sends email with Venue QR Code to venue owner
Firebase Cloud Messaging Service	Sends silent push notification to mobile apps when a new broadcast file is ready for download for matching by mobile apps

2.2 Privacy By Design

The system is designed to preserve user privacy.

All users' visit record data are encrypted and stored locally only in their devices for a retention period (31 days). The visit records will be required to be uploaded via the Report Positive or Preliminary Positive function only if the user is tested positive on request by the Centre for Health Protection (CHP). The uploaded records can only be viewed by Admin portal users with access control. On the other hand, the records broadcast to app users contain no information that can identify the record belonging to which user.

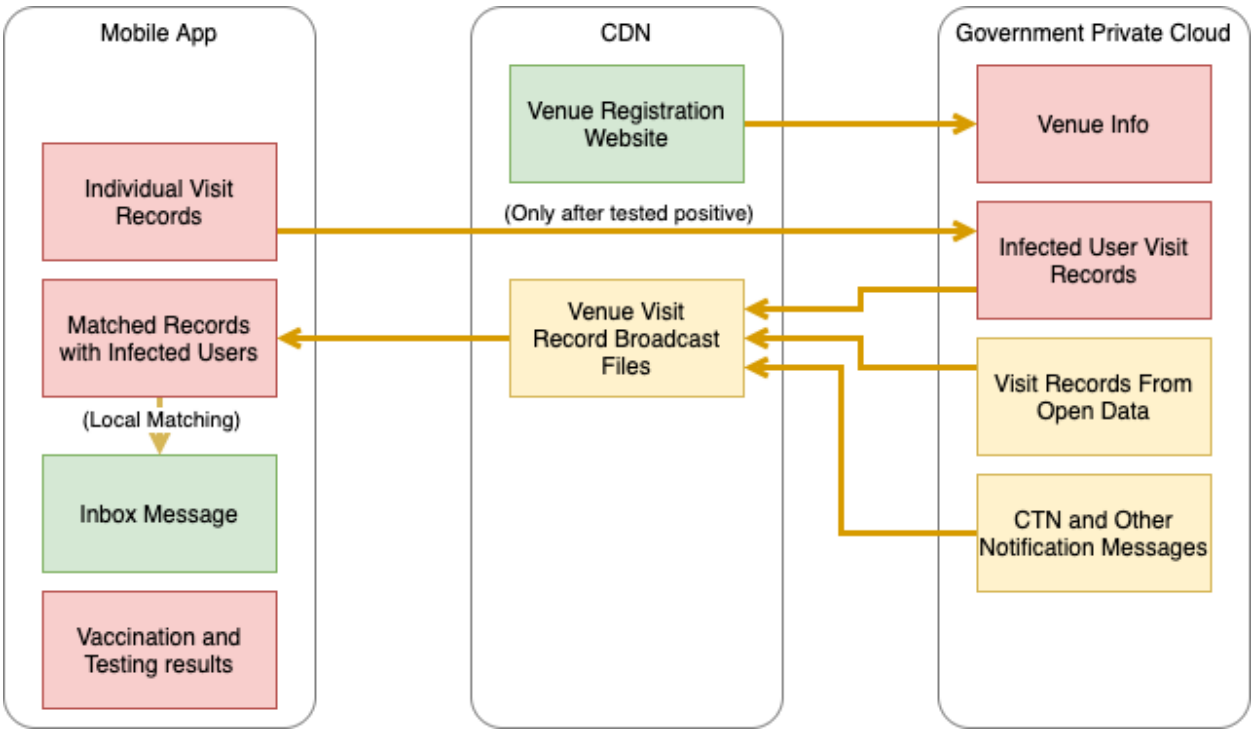
While visit records are encrypted in the mobile phones, as visit records can be viewed through the app, users should still protect their own personal devices against unauthorised access, in situations like stolen or lost mobile phones.

From version 2.0 onwards, users are able to keep their COVID-19 vaccination record and testing record voluntarily in the mobile app by scanning the QR code that contains the record details provided in the paper COVID-19 vaccination record or eHealth System or COVID-19 Electronic Vaccination and Testing Record System. The record details will then be encrypted with AES 256 encryption and stored in the local database of the app and protected by built-in biometric or password authentication which users use to unlock their phones. The encryption key will be stored in iOS Keychain/ Android Keystore. Local authentication that relies on OS biometric authentication or password is required to retrieve the key from the Keychain / Keystore.

Users will have complete control over the vaccination and testing records and the QR codes kept in the app, and may choose to show the information or not to any third parties, and can remove the records from the app at any time. The app will not upload the records to any computer systems including the government system.

2.3 Data Flow

The following diagram shows what data will be stored in the system, and how the data be transferred. All data transfers are protected by HTTPS protocol.



3 Mobile App

Users can use the LeaveHomeSafe app to check-in/out the venues they have visited. If a user is tested positive, he/she can upload their visit records to the system via the Report Positive or Preliminary Positive function. Other users can download the broadcast file and perform matching with their own visit records in the mobile phone to see whether the user has also visited the same venue in the same period of time. If so, the app will show a notification to the user.

3.1 Technology

Programming Language

Technology	Implementation	Version	Description
Framework	React Native	0.63.2	Framework for building both iOS, Android and Huawei app using React
Programming Language	Javascript	ES6	Language in which React Native app is programmed

Supported OS

Platform	Version
iOS	iOS 12 or above
Android	Android 8 or above (earlier versions down to Android 4.1 are allowed to install the app but it is not guaranteed to work)
Huawei	HarmonyOS 2.0 or above

3.2 Permissions

3.2.1 Android Permissions

- Camera – for scanning venue QR codes, taxi registration marks, vaccination and testing records
- Have full network access – for downloading broadcast files, using the Report Positive or Preliminary Positive function to upload visit records of confirmed users, and using the online OCR function (only applicable to version 1.1.6 or earlier)
- Receive data from internet – for downloading broadcast files and receiving silent push notifications
- Control vibration – for notification and confirming that scanning function has been successful
- Run at startup – for enabling the app to run at start so that it can download broadcast files in the background
- Prevent phone from sleeping - for enabling the app to download broadcast files in the background
- Foreground Service - for declaring the sensor monitoring service as a foreground service, so that it can continue running even if the app goes into the background (applicable to version 2.1 or above; the permission is required by the dynamic auto-leave module developed and provided by HKBU to retrieve motion sensors' data and detect check-out behavior).
- Retrieve running apps – for scheduled tasks to run in the background and checking status of previous task (The permission is required by the Module - react-native-background-fetch; Function call - getRecentTasks. (Usage - to determine if the MainActivity is alive or not, so that it knows when to fire Headless events in order to make sure that the scheduled tasks can be run even after the app is killed.)).

The permissions below are applicable to version 2.0 or above if the user opts to use the electronic vaccination and testing records function:

- Use Biometric (Android API level 28 or above) – for authentication to retrieve encryption key from the Keychain/ Keystore for protection of vaccination records and testing results
- Use Fingerprint (Android API level below 28) - for authentication to retrieve encryption key from the Keychain/ Keystore for protection of vaccination records and testing results

3.2.2 iOS Permissions

- Camera – for scanning venue QR codes, taxi registration marks, vaccination and testing record
- Notification – for displaying notifications
- Background App Refresh – for allowing the app periodically to run in the background

- Mobile data - for downloading broadcast file, using the Report Positive or Preliminary Positive function to upload visit records for confirmed users, and using the online OCR function (applicable to version 1.1.6 or earlier only)
- Face ID - to protect vaccination record and testing result (if users opt to use the electronic vaccination and testing records function)
- Motion & Fitness - to access the device's motion data (if users opt to use the taxi dynamic auto-leave function) (applicable to version 2.1 or above)
- Photo Library – for importing COVID-19 vaccination record and testing record from QR code images stored in the photo library (applicable to version 2.1 or above)

3.3 Visit Records and Matching

3.3.1 Visit Records

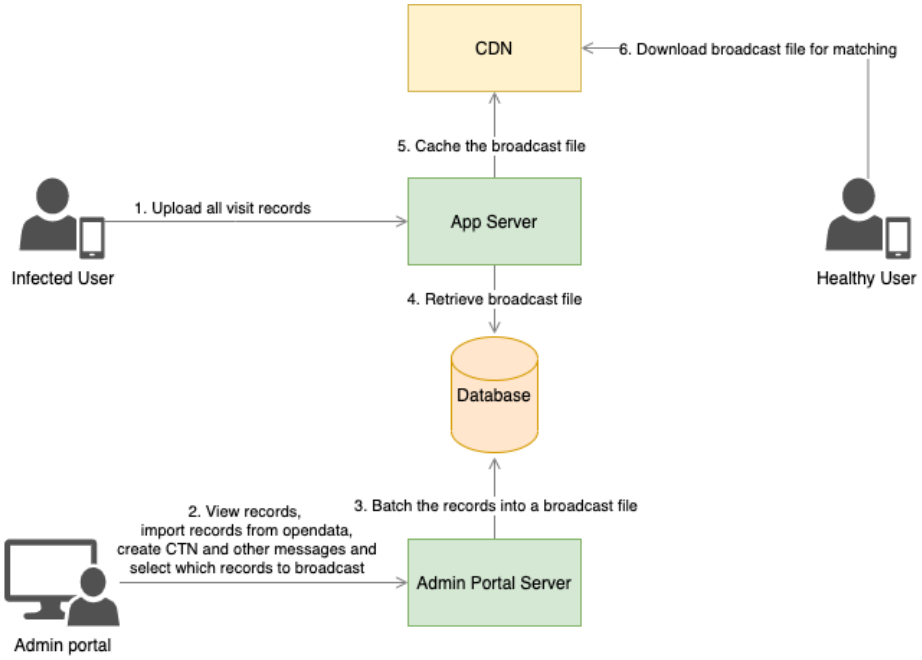
After users scan a venue QR code or taxi registration mark to check-in and then check-out, the record will be encrypted and stored in a local database of the app. The record contains the following information:

- Venue code
- Check-in timestamp
- Check-out timestamp
- Metadata including venue name, venue type, taxi registration mark.

As users use the mobile app to scan the venue QR code, the app will decode the QR code to collect the venue information including venue code, venue name, venue type, venue metadata and a SHA 256 hash. The QR code will be verified by computing a hash value from the venue information and then comparing it with the one in the QR code.

3.3.2 Matching Flow

The backend server will broadcast the list of venues with positive or preliminary positive cases reported (including the venue code and affected dates/periods). The app will trigger a download of the broadcast file from server to the user phone and match it with the stored visit records of the users locally in their phones. If matched, the app will generate an exposure notification to the user. The following diagram shows the user flow which uses the app to interact with the backend system for the process of matching records of infected users in the broadcast file.



3.3.3 Matching Parameters

The parameters can be configured in Admin Portal.

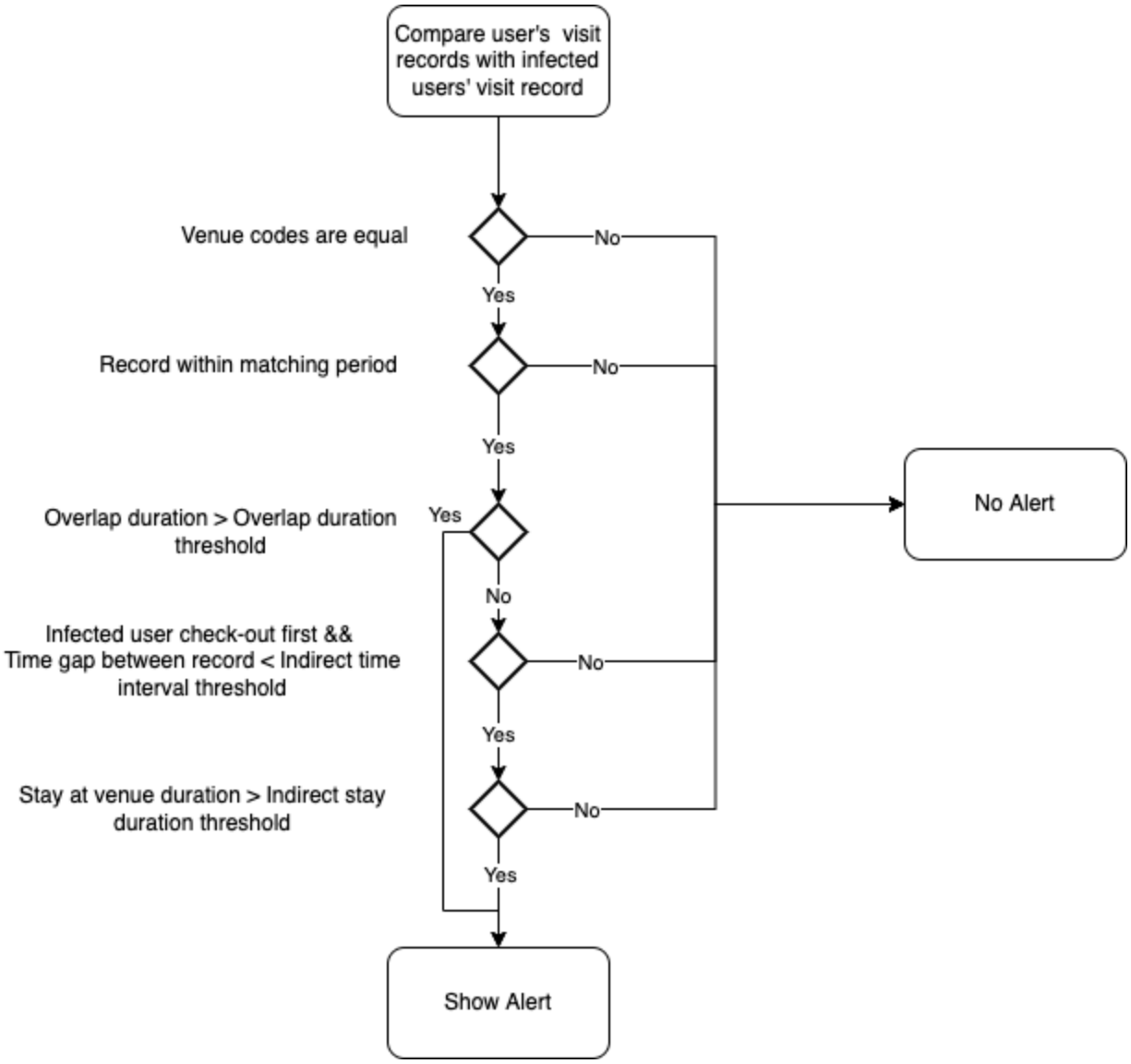
Name	Value	Description
Matching period (in days)	31	The matching will proceed if the day of check-in is within the matching period.
Overlap duration threshold (in seconds)	1	The threshold parameter of exposure duration. The duration is calculated by the check-in & out time of both visit records. If the duration is over the threshold value, alert will be prompted.
Indirect time interval threshold (in seconds)*	0 (venue) 86400 (taxi)	The threshold parameter of time gap between the infected user check-out time and the user check-in time. This is calculated by the checked-out time of visit records and the checked-in time of the user visit records. If the time is below the threshold value, the matching will be continued. If it is set to 0, the function to allow notification for indirect stay will be disabled.

Name	Value	Description
Indirect stay duration threshold (in seconds)*	0 (venue) 1 (taxi)	If the user stays in the venue in an indirect stay below the threshold, no notification will be prompted. If it is set to 0, the function to allow notification for indirect stay will be disabled.

Note: parameters marked with * are configurable independently for taxi and venues.

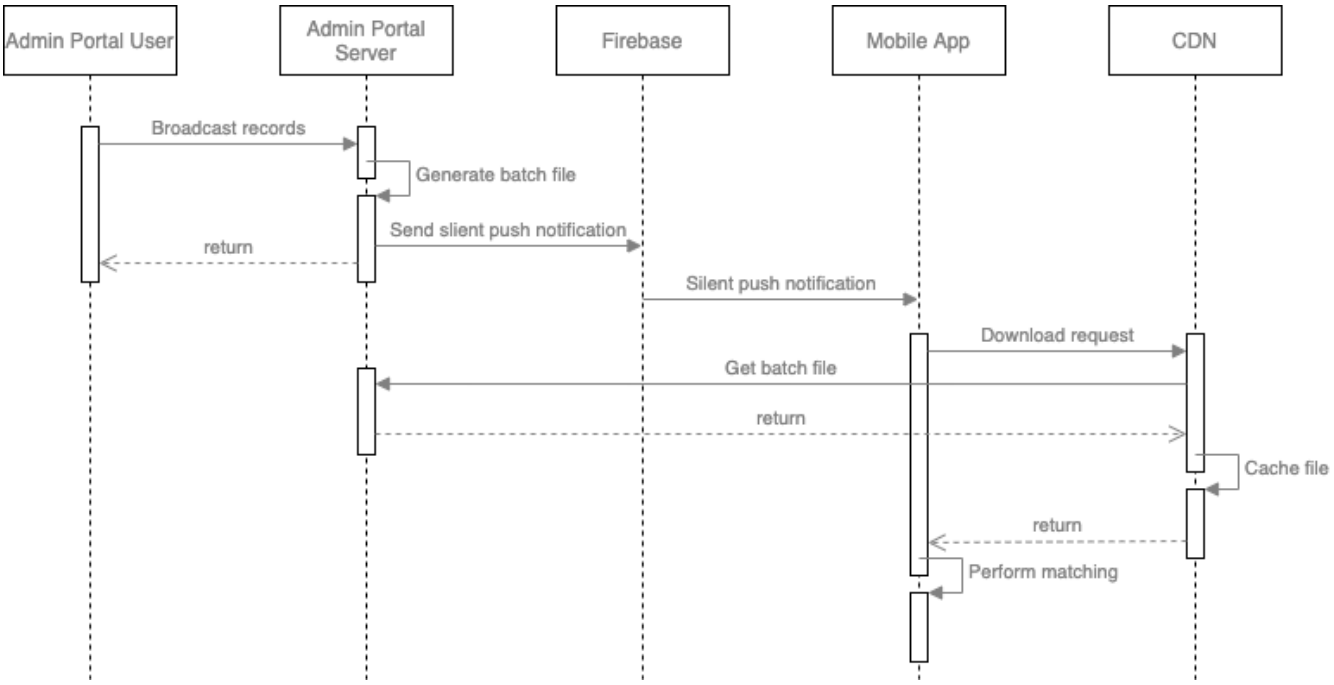
3.3.4 Matching Criteria

After users download the broadcast file, the app will perform matching locally to check possible exposure with the following criteria:



3.3.5 Silent Push Notification for Broadcast File Update

Due to the limitation of device OS, the scheduled task may not be executed properly. To ensure users are able to receive notifications, when a new broadcast file is available for download, a silent push notification will be broadcast to notify the app. The app will then wake up in the background and download the file from the server to perform matching (The “wake up” action will be running in most devices while it is subject to the device condition and operating systems.).



3.4 Compulsory Testing Notice Notification

From version 1.1.9 in Android and 1.1.12 in iOS onwards, the mobile app is able to receive and display compulsory testing notice (CTN) notification and other enhanced messages, when the mobile app user checked in at the restricted venues/taxis during specified periods. The matching criteria will be the same as ordinary exposure notification except that only the overlap duration will be checked, as only the users who was present in that period would receive the message. The notification messages will be created and sent with broadcast files via the Admin Portal. If the specified period of a CTN notification covers multiple visit records of the same venue, only 1 notification message will be displayed. A link to the relevant CTN will also be included in the message.

If the user is using version earlier than 1.1.9 in Android and 1.1.12 in iOS, the user will only receive the ordinary exposure notification message as the older versions of the app only support one message template.

3.5 Report Positive or Preliminary Positive

If an app user is tested positive, the user will be required to upload his/her visit records from the app to the LeaveHomeSafe server. The following information will need the user to input and upload along with the visit records:

- Case Number / Preliminary Case Number

- Name
- Contact Phone Number.

To upload the data to the LeaveHomeSafe Server, the CHP will provide a 6-digit PIN as verification code to the user. The user will then enter the PIN into the app and then upload the data to the server.

3.6 Configuration File

There are several configurations that can be controlled by the Admin Portal:

- Matching criteria's configurable parameters
- Data retention period
- Default checkout reminder periods for venues and taxis
- Force update version.

The configurations are defined in a JSON file and downloaded by the app.

3.7 Scheduled Task

Due to various reasons including the mobile OS's restriction on running background tasks, battery safer, the app killed by users, and low battery, there are chances that the user cannot receive the silent push notification from Firebase cloud messaging service, such that the user may only be able to receive the exposure notification, CTN or other messages from LeaveHomeSafe when the user launches the app.

In order to increase the chance that the user can receive notifications automatically and promptly, and to perform housekeeping, a scheduled task will be set in the app and executed at regular intervals (whether it is actually able to execute at regular intervals will be subject to the mobile OS's restriction). The task will delete the visit records that exceed the retention period and check whether a new broadcast file is available for download for matching. To ensure the task can be executed even when the app is in the background, a module "react-native-background-fetch" is used, which attempts to awaken the app in the background periodically, providing a short period of background running-time to execute the task (https://github.com/transistorsoft/react-native-background-fetch).

3.8 Taxi Registration Mark OCR

To ease users to check-in on taxis, an OCR function has been implemented on the app. The user would use the app to capture the taxi registration mark that is placed on the door. For version 1.1.6 or earlier, the taxi registration mark image will be sent to the LeaveHomeSafe server. The

server will pre-process the image and then perform OCR using Azure Cognitive Service. For iOS and Android version 1.1.7 or later, the OCR function is performed offline locally in the app and no internet connection is required for the OCR. From version 2.1 onwards, the offline OCR function available for Huawei devices uses HMS ML Computer Vision APIs. The result will be returned to the app and auto filled to the input field. Regardless of which app version, the image will not be stored in the system, including the mobile app and server.

3.9 Electronic COVID-19 Vaccination and Testing Record / COVID-19 Vaccination Medical Exemption Certificate/ COVID-19 Recovery Record

From version 2.0 onwards, users are able to keep their COVID-19 vaccination record and testing record in the mobile app by scanning the QR code that contains the record details provided in the paper COVID-19 vaccination record or eHealth System or COVID-19 Electronic Vaccination and Testing Record System. And from version 2.1 onwards, users are able to import and crop the QR code from images stored in the mobile devices. The QR code of COVID-19 Vaccination Medical Exemption Certificate is supported from version 3.0.2 onward and the QR code of COVID-19 Recovery Record is supported from version 3.2.0 onward. The QR code content contains a digital signature. After the mobile app scans the QR code or imports the QR code image, the code will be validated by comparing the hash value of the plain data against the message digest retrieved from the digital signature with a public key in X.509 standard. The record details will then be encrypted with AES 256 encryption and stored in the local database of the app. The encryption key will be stored in iOS Keychain/ Android Keystore. Local authentication is required to retrieve the key from the Keychain / Keystore. From 3.0.2 onwards, users could choose to opt in (i.e. enable because it is default off/ disabled) the local authentication for accessing the electronic vaccination and testing record function. Users could enable/disable the local authentication anytime in App Settings.

Local authentication relies on OS biometric authentication like face or fingerprint, providing a fallback like passcode or PIN when biometrics are not available. On Android, the biometric authentication would only be allowed if the OEM implementations meet the strength requirements (https://source.android.com/security/biometric/measure).

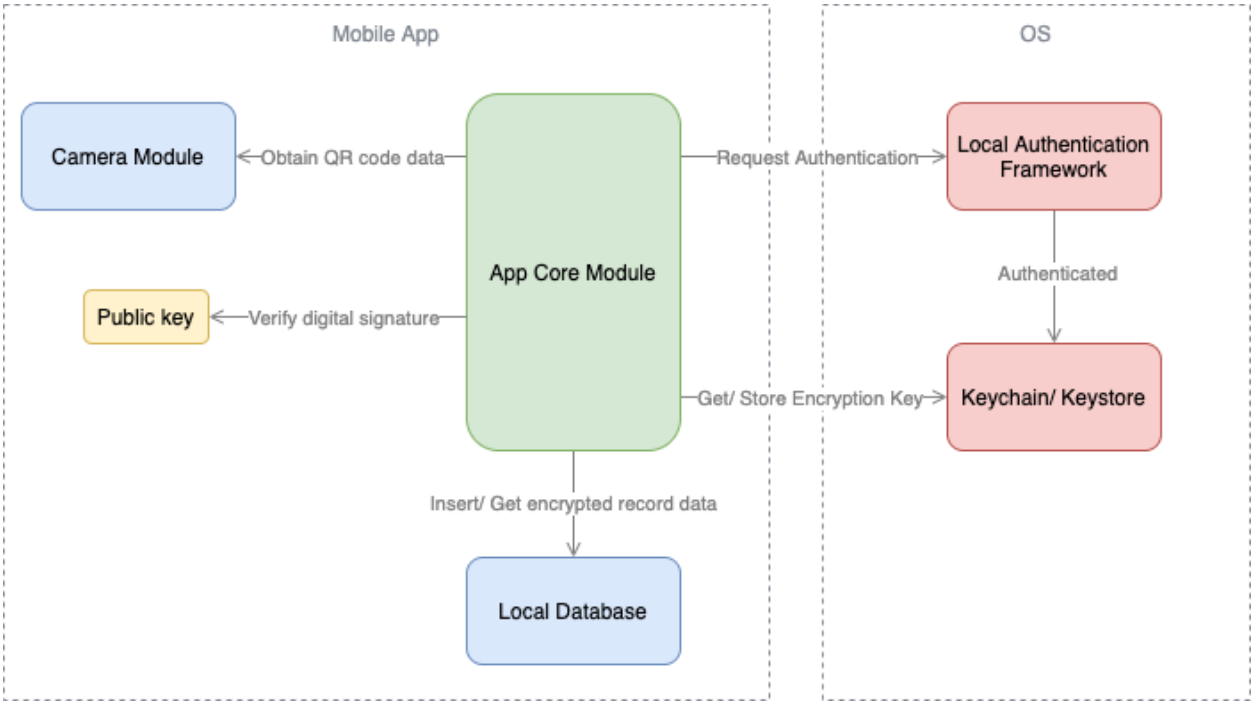
After a record is stored, if the device security credential is reset, the access of the record will become invalid, and users will need to delete the current one and re-import the record again.

Supported Biometric Options

Type	**Platform**
Face ID	iOS
Touch ID	iOS
Fingerprint	Android

Supported Fallback Options

Type	Platform
Passcode	iOS
Password	Android
PIN	Android
Pattern	Android



Note: The arrow represents the dependency of the component.

From 3.0.2, the local authentication is turned off by default and the QR code of Vaccine Pass (i.e. Electronic Vaccination Record / Medical Exemption Certificate / Recovery Record) can be automatically shown on the check-in page.

From 3.2.0 onwards, after users check-in a venue, the QR code of Vaccine Pass will be displayed in BLUE on the venue check-in page. If the displayed Vaccine Pass meets the requirements of Vaccine Pass, the QR code will have a blue frame; otherwise, the QR code will have a red frame. In case the app has stored more than one Vaccine Pass record, the record which has been set as default will be shown on the check-in page. If the local authentication is enabled, the QR code would not be displayed initially. The user is required to select to display the QR code on the page and perform local authentication.

If (a) there is no stored Vaccine Pass record or (b) the user disable the electronic vaccination and testing record function, the venue check-in page will display a RED QR code.

3.10 Venue QR Code Verification

From version 2.1 onwards, when a venue QR code is scanned, the mobile app could be able to further verify the content of venue QR code by comparing it against a venues file downloaded from QR code registration portal. The app will check whether the venue code exists in the venues file, and then comparing the SHA256 checksum which is produced by the venue information. If the checksum does not match, a warning message on 'Unidentified QR code' will be prompted on the mobile app, requesting users to report the relevant venues to OGCIO. Users could choose to report the venue information by email or by filling in an enquiry form in the LeaveHomeSafe website.

3.11 Dynamic Auto-leave Function developed and provided by HKBU

From version 2.1 onwards, users can enable the dynamic auto-leave function developed and provided by the Hong Kong Baptist University (HKBU) for automatically recording the leaving event when leaving a taxi. For Android users, their leaving event will be recognised through a tailored intelligent algorithm based on the motion sensors' data (including accelerometer, gyroscope and magnetometer) collected by the mobile phone. For iOS users, their activities will be logged by the iOS CMMotionActivityManager module. When the app is re-opened, the user activity log will be analysed for automatic recording of the leaving event.

For both iOS and Android users, the collected sensor data will not be stored in the system after the user activity recognition. The data analysis procedure is strictly restrained in the local mobile phone based on the sensor data. The app will not upload the sensor data or recognise user activities to any computer systems.

For Android users, the mobile phone should be equipped with accelerometer and gyroscope (or magnetometer) to facilitate the auto-leave function. If the phone model is Huawei, the "Auto Management" option in the "App Launch" of power management setting should be disabled. For Android 11 Samsung phones, it is strongly suggested to turn off the "Battery Optimization" option in the "Battery" setting of the LeaveHomeSafe app.

For details of the algorithm, please refer to the following technical report:
https://www.comp.hkbu.edu.hk/~db/butrace.pdf

3.12 Connection to Hong Kong Health Code System

From version 3.0 onwards, users can at their discretion enable the function of 'Connection to Hong Kong Health Code System (HCS)' for logging in their HCS accounts and uploading their visit records and notification records ("the records") to HCS. The function can be opted in or out upon the app installation or upgrade, and can also be turned on or off in the 'Settings' menu anytime. The following operations are available in the function.

Register/Apply for Hong Kong Health Code

When a user presses this button, the app will launch the default web browser of the mobile phone and go to HCS website for account registration. The user can then login HCS with their credentials through the authentication mechanism in HCS.

Upload Records to HCS

This operation allows users to upload their visit records and notification records in LHS mobile app to their own accounts in HCS in a secure manner.

First of all, users are required to undergo a two-factor authentication to login HCS, which includes user login information validation and one-time password (OTP) for user authentication. The login information includes the following data fields:

- Identity Document Type
- Identity Document Number
- Issuing Country/Region (if Other Identity Document Type is selected)
- Password

An option is provided for the app to 'remember' the login information (except the password) and then fill in automatically during subsequent user logins. The information is encrypted before being stored in the local database of the app.

For the uploading, a unique hash ID is generated and stored in the LHS mobile app at installation. The hash ID will be used by HCS to identify the source of uploading data, as users can upload their visit records and notification records from more than one device. The hash ID will be re-generated when the app is re-installed on the same device (in case of re-installing, all existing visit records and notification records in the app will be removed).

The login information together with the hash ID and the mobile app's first-use date will be sent to HCS for login authentication. If the authentication is successful, HCS will send an OTP to the HCS pre-registered mobile phone number via Short Message Service (SMS). The mobile phone here refers to the mobile phone number that the user has registered with HCS, but not necessarily the mobile phone that the LeaveHomeSafe app is currently installed (they can be the same though).

After the user enters the OTP, the OTP will be sent to HCS. If OTP authentication is successful, the login is completed successfully and HCS will return an API token to the app for subsequent records uploading.

The user needs to explicitly agree the following declarations before uploading the records to HCS:

- The user has read and agrees to the Personal Information Collection Statement and Privacy Policy Statement of the Hong Kong Health Code.
- The user declares that the user account above belongs to him/her and confirms that the records of LeaveHomeSafe are his/her personal records only. The user understands that it may be a criminal offence to knowingly provide false or misleading information.

After the user confirms the above agreement/declaration, the visit records and exposure notifications received will be retrieved and decrypted from the local database of the app, and then be uploaded to HCS along with the hash ID and the API token. The data fields and types of visit records and notification records to be submitted are as follows:

(a) Visit Record

Field	**Type**	**Description**
id	INT	Primary key of the visit record
venueCode	VARCHAR(8)	LHS venue code
checkinTs	VARCHAR(13)	Check in date time
checkOutTs	VARCHAR(13)	Check out date time
vehRegMark	VARCHAR(8)	Taxi Registration Mark
isAI	INT	Auto-leave triggered by dynamic auto-leave function

(b) Notification Record

Field	**Type**	**Description**
id	INT	Primary key of the visit record
venueCode	VARCHAR(8)	LHS venue code
vehRegMark	VARCHAR(8)	Taxi Registration Mark
checkinTs	VARCHAR(13)	Check in date time
checkOutTs	VARCHAR(13)	Check out date time
matchingTs	VARCHAR(13)	Matching date time
noticeDt	VARCHAR(13)	Notice date
type	VARCHAR(1)	Venue/ Taxi
msgType	VARCHAR(1)	Notice message type

After the records are uploaded successfully, the app will show the record counts of records uploaded. The uploaded records will overwrite previous data uploaded from the same device to HCS.

Hong Kong Health Code User Guide

When a user presses this button, the app will launch the default web browser of the mobile phone to go to HCS website for accessing Hong Kong Health Code user guide.

View Past Upload History

The user can view past upload history in the app. The upload history is stored in the local database of the app. It only contains the record counts in previous uploads but does not contain the details of the records being uploaded. The history of individual uploads will be deleted automatically after 31 days.

Web Single Sign On

From 3.0.1 onwards, a single sign on is implemented so that after the visit and notification records are uploaded, the user could access HCS from the app to continue the application for Health Code, without requiring to sign in to HCS again.

When user selects to continue the application, the app will make a request to HCS for single sign on with the document information and API token, HCS will return an access URL and token to the app. The app will use the provided URL and token to single sign on to the HCS Web System via web browser.

4 Data

Data collected by LeaveHomeSafe are presented in the table below:

Data	Storage	Removal
Visit Records (in general situation)	Encrypted using AES-256 and stored in local mobile phones.	Automatically removed after 31 days.
Visit Records (for patients who are tested positive)	Encrypted using AES-256 and stored in local mobile phones. Required to be uploaded to LeaveHomeSafe servers in Government Private Cloud for epidemiological investigation with name and contact number by verification of PIN provided by CHP. All internet incoming traffic will be protected by HTTPS protocol.	Inside the app: Automatically removed after 31 days. Uploaded to CHP: Will be kept for at least 7 years by the Department of Health as with the same policy for other data for epidemiological investigations.
Visit Records and Notification Records for uploading to HCS (for registered users of HCS)	The API call used for uploading visit records and notification records to HCS is transferred via the HTTPS protocol. Only with their express consent, users may at their sole discretion upload their visit records and notification records from the LeaveHomeSafe mobile app to the Hong Kong Health Code System for the application of Hong Kong Health Code and its related purposes as well as facilitating the work of the Government in controlling the spread of COVID-19 and related purposes. The API call used for uploading visit records and notification records to HCS is transferred via the HTTPS protocol.	Uploaded to HCS: The visit records and notification records to be uploaded will be subject to the collection, holding, processing or use of the data concerned by the Hong Kong Health Code System. Please read and agree the Hong Kong Health Code System's Personal Information Collection Statement and Privacy Policy Statement before you proceed.
Venue registration information	LeaveHomeSafe servers in Government Private Cloud. All internet incoming traffic will be protected by HTTPS protocol.	Will be kept for 7 years or less when the data are no longer required.

Data	Storage	Removal
Contact and enquiry information submitted through “Contact Us”	LeaveHomeSafe servers in Government Private Cloud. All internet incoming traffic will be protected by HTTPS protocol.	Will be kept for 7 years or less when the data are no longer required.
Electronic COVID-19 Vaccination and Testing record	Encrypted using AES-256 and stored in local mobile phones.	Can be manually removed by users at any time at their wish.
Motion Sensor data	No storage	Immediately removed after the user activity recognition.
HCS Login Information (except password) (Under “Remember Login Information” function)	Encrypted using AES-256 and stored in local mobile phones. The identity document number is masked when it is retrieved from the “Remember Login Information” function and displayed.	Can be manually removed by users at any time at their wish
History of Uploaded Visit Records and Notification Records to HCS (for registered users of HCS)	The identify document numbers in upload history is encrypted using AES-256 and stored in local mobile phones. The identity document numbers are masked in display.	Automatically removed after 31 days.

5 Glossary

CDN	Content Delivery Network
CHP	Centre for Health Protection
CTN	Compulsory Testing Notice
DH	Department of Health
OCR	Optical Character Recognition
OGCIO	Office of the Government Chief Information Officer
Broadcast file	A zip file that contains a batch of infected users visit records, CTN and other messages
HCS	Hong Kong Health Code System