**Crownpass: A Covid-19 Tracking System**

**Abstract**

This document is the requirements definition of a cloud-based mobile application system called Crownpass for tracking and preventing the spread of Covid-19 coronavirus. The document states the goal and objectives of the system, defines the scope of the system, analysed the target user types and their characteristics of digital literacy. It defines the functional and quality requirements for each user type and the required design features of the system.

**Table of Contents**

[1. Introduction 1](#_Toc55146857)

[2. Types of Targeted Users 2](#_Toc55146858)

[3. Functional Requirements 2](#_Toc55146859)

[3.1. Functional Requirements of Crownpass Holders 2](#_Toc55146860)

[3.2. Functional Requirements of Owner of Controlled Area 3](#_Toc55146861)

[3.3. Functional Requirements of Operation Staff of Controlled Area 3](#_Toc55146862)

[3.4. Functional Requirements of Test Centre Staff 4](#_Toc55146863)

[3.5. Functional Requirements of Staff in Disease Control Centres 4](#_Toc55146864)

[3.6. Functional Requirements of System Operators 4](#_Toc55146865)

[3.7. Functional Requirements of Police Officers 4](#_Toc55146866)

[4. Required Design Features 5](#_Toc55146867)

[5. Quality Requirements 6](#_Toc55146868)

[5.1. Scalability. 6](#_Toc55146869)

[5.2. Performance 6](#_Toc55146870)

[5.3. Reliability 7](#_Toc55146871)

[5.4. Security and Privacy Protection 8](#_Toc55146872)

[5.5. Platform Compatibility 8](#_Toc55146873)

[5.6. Usability 9](#_Toc55146874)

[References 9](#_Toc55146875)

# Introduction

To combat the pandemic of coronavirus Covid-19, experts in public health have called for a virus tracking system to stop the spread of the virus in public areas. This document defines the functional and non-functional requirements of such a Covid-19 tracking system called *Crownpass*.

As stated in [[[1]](#endnote-2)], the basic idea of the tracking system is to set all public in-door spaces where people physically contact with each other as controlled areas so that the potential infection of the virus can be monitored and traced. Typical examples of such areas are *restaurants*, *pubs*, *shops*, *museums*, *schools*, *offices*, *cinemas*, *theatres*, *airports*, *waiting rooms of bus stations*, *public transportation vehicles* (like *buses*, *taxis*, *airplane*, *ferry boats*, *trains*), etc. Every individual who enters such a space must be recorded of the period of time that the individual stayed in the area.

When a person is tested positive on Covid-19 virus, those individuals have stayed in a same controlled area within *2 days[[2]](#footnote-1)* and had an overlap of the periods more then *15 minutes[[3]](#footnote-2)* have the potential being infected, thus they should be informed to self-isolate for *14 days[[4]](#footnote-3)* and recommended to take a Covid-19 test. Those required to self-isolate are not allowed to enter any controlled area before the completion of self-isolation or be tested negative on Covid-19.

The goal of the project is to develop a computer application to enable tracking people who are in controlled areas and notifying people automatically for self-isolation. To achieve this gaol, the system should fulfil the following objectives.

1. Each individual who enters a controlled area must have a unique identifier, called “*Crownpass*” in the sequel, so that it can be physically checked against an individual, say, through matching a photo of the pass holder. The state of Covid-19 infection can be stored and retrieved from computer records quickly. An initial design of the appearance of the Crownpass is to have
* a photo of the pass holder, and
* a 2D bar code as the pass holder’s digital identifier.
1. The system will store the covid-19 infection state for each pass holder and automate the state transitions in real-time when information become available due to Covid-19 virus test or self-isolation finishes. Three states have been identified:
* *Green*: No Covid-19 infection;
* *Amber*: Suspected to be infected by Covid-19;
* *Red*: Confirmed infection by Covid-19.
1. An owner of a controlled area should be able to easily install a mobile APP to scan the 2D bar code of Crownpass when a person enters the area and leaves the area. The APP should be able to ensure the area is not too crowded and only allows the Green pass holders to enter the area. The data about when and who enters and leaves an area must be sent to the computer system automatically and the records are stored for trace back.
2. The system should provide the *Disease Control Centres* of local and central governments with statistical data on the total number of confirmed cases of Covid-19 infections in a geographic area, such as a city or a town, so that a regional lockdown decision can be made promptly based on accurate data.
3. The police officers should be equipped with an APP installed on their mobile computing devices to enable law enforcement related to Covid-19 social distance rule.

The scope of the system at its first stage of development will limited to providing the above key functions.

The document consists of the following sections. Section 2 defines the target user types. Section 3 defines the functional requirements for each user type. Section 3 defines the key design features on how the functions of the system are to be delivered to various types of users. Section 4 defines the quality requirements of the system.

# Types of Targeted Users

The main types of the users of the system will be:

1. *Crownpass holder*. They are individuals of the general public who want to enter and leave controlled areas by shown their Crownpass to the area staff. They may have different digital literacy and experiences of using smart mobile devices such as mobile phones. Some may have no mobile phones; and some may be unable to use mobile phones for some reason, such as disability.
2. *Owner of controlled area*. They are the owner or host of a controlled area and in responsible of setting up the operations of the area in compliance to the social distancing and virus tracking rules. It is assumed that they have a basic digital literacy and capable of using smart mobile devices, such as mobile phones. It is also assumed that they own smart mobile devices on which a Mobile App can run.
3. *Operation staff of controlled area.* They are in responsible to operate a controlled area to ensure people enters the area are checked-in and leaves the area are checked-out so that they period of stays in the area can be correctly recorded, and only people in the green state will enter the area. It is assumed that they have a basic digital literacy and capable of using smart mobile devices, such as mobile phones, to complete simple routine works. They should be able to learn how to use a mobile App quickly with or without lengthy trainings.
4. *Staff of Covid-19 Virus Test Centres.* They are responsible for entering correct test results into the system when the test results for a Crownpass holder become available. It is assumed that they have a basic digital literacy and capable of using smart mobile devices, such as mobile phones, to complete simple routine works. They should be able to learn how to use a mobile App quickly with a short training.
5. *Staff of Disease Control Centres.* They are interested in monitoring the situation of Covid-19 infections in an area or a country by using statistical data. Informed by accurate and real-time data, they may make decisions to change system parameters and social distancing and virus tracking rules. It is assumed that they have good digital literacy and are capable of operating desktop computer systems through web-browsers and other graphic user interfaces after short trainings.
6. *System Operators.* They are responsible for setting the system parameters and other operations of the system. They are assumed to be IT professionals and capable of operating desktop computer systems after a short training.
7. *Police officers.* They are responsible of law enforcement of the social distancing and virus tracking rules. They are assumed of basic digital literacy and capable of using smart mobile devices with or without short trainings on simple routine tasks.

# Functional Requirements

The functional requirements are structured according to the user types.

## Functional Requirements of Crownpass Holders

**FR-CH-01: Registration**. Any general public should be able to register to the Crownpass system to obtain an identifier. The minimal information required for registration is a real photo of the person. A Crownpass holder may also submit, but optional, the following data to the system: mobile phone number, email address, home address, name, gender, and date of birth. (*Priority: High*)

**FR-CH-02: Print Pass.** A successfully registered Crownpass holder should be able to print his/her pass on a normal sheet of paper that consists of a photo of the pass and a QR code (also known as 2D bar code) that represents the pass holder’s identifier. (*Priority: High*)

**FR-CH-03: Display Pass.** A successfully registered Crownpass holder should be able to display his/her pass on the screen of his/her mobile phone where the Crownpass Holder App runs. It should contain a photo of the pass and a QR code (also known as 2D bar code) that represents the pass holder’s identifier. (*Priority: High*)

**FR-CH-04: Check state**. A successfully registered Crownpass holder should be able to show the state of his/her pass on the screen of his/her mobile phone where the Crownpass Holder App runs. (*Priority: Medium*)

**FR-CH-05: Check trace**. A successfully registered Crownpass holder should be able to display his/her movement trace (i.e. the sequence of areas) that he/she has entered in a period of time of his/her choice on the screen of his/her mobile phone where the Crownpass Holder App runs. (*Priority: Medium*)

**FR-CH-06: Web Access.** A successfully registered Crownpass holder should be able to access the following data of the pass holder by entering his/her pass identifier: (a) Pass state, (b) Contact details, (c) Movement trace; where contain details can be reset, while other data cannot be modified by the pass holder. (*Priority: Low*)

**FR-CH-07: Notification.** The system should be able to notify the Crownpass holder when his/her pass state is changed. (*Priority: Medium*)

**FR-CH-08: Self Check-in and Check-out**. The system should be able to enable the Crownpass holders to check-in to and/or check-out from a controlled area using the Crownpass Holder App running on a mobile phone. (*Priority: Low*)

## Functional Requirements of the Owner of Controlled Area

**FR-OC-01: Registration**. The owner of a controlled area should be able to register to the system as the owner of the area to get an identifier of the area. The following data are required to register a controlled area: (a) Name of the area; (b) Address of the area; (c) Type of the area, (such as pub, restaurant, etc.); (d) Capacity of the area (how many persons can be in the area simultaneously; (e) Contact numbers. (*Priority: High*)

**FR-OC-02: Update**. The owner of a registered controlled area should be able to update the registration data. (*Priority: Medium*)

**FR-OC-03: View Registration Data**. The owner of a registered controlled area should be able to view the registration data. (*Priority: Medium*)

**FR-OC-04: Notification**. The owner of a registered controlled area should be notified when a Crownpass holder in the controlled area is tested positive or his/her state changes into Red. (*Priority: High*)

**FR-OC-05: Setup Staff Account**. The owner of a registered controlled area should be able to set up a number of staff accounts on a number of mobile devices to operate the controlled area. (*Priority: High*)

**FR-OC-06: View Operation State.** The owner of a registered controlled area should be able to view the state of the area in terms of the number of customers (i.e. Crownpass holders) in the area. (*Priority: Low*)

## Functional Requirements of Operation Staff of Controlled Area

**FR-SC-01: Check-in Customer.** The system should enable the operational staff to check-in Crownpass holders into the controlled area. A pass holder should be allowed to enter the area only if: (a) The customer is the Crownpass holder; (b) the state of the Crownpass is Green; and (c) the number of persons in the area is less than the capacity of the area. After a customer is checked-in, the number of persons in the area must be increased by 1. (*Priority: High*)

**FR-SC-02: Check-out Customer.** The system should enable the operational staff to check-out Crownpass holders out of the controlled area. After a customer is checked-out, the number of persons in the area must be decreased by 1. (*Priority: High*)

**FR-SC-03: Evacuation of Area.** The system should support quick evacuation of the controlled area by letting all customers leave the area and set all the customers previous in the area to be out of the area as if they were checked out one by one. (*Priority: High*)

**FR-SC-04: Notify and Close**. The system should notify the operation staffs when a customer’s Crownpass state changed into Red while the customer is in the area, instruct the operation staff to evacuate the area, and to automatically disable the check-in function. (*Priority: High*)

**FR-SC-05: Reset Area State**. The system should support resetting the number of customers in the controlled area so that pass holders who failed to check out when leaves the area can be removed from the system. The exit time of the pass holder who failed to check-out will be the time when reset operation is performed. (*Priority: Medium*)

## Functional Requirements of Test Centre Staff

**FR-ST-01: Enter Test Result**. The system should enable the staff of Covid-19 Virus Test Centres to enter test result to the Crownpass tracking system. When a test result of a Crownpass holder becomes available, the test result will trigger the transition of the state of the Crownpass as follows:

1. If the test result is POSITIVE, the Crownpass state must be changed into RED, no matter which even state the Crownpass is currently in.
2. If the test result is NEGATIVE, the Crownpass state should be changed into GREEN no matter whichever state the Crownpass is currently in.
3. If the test result is UNDECIDED, the state of the Crownpass should remain as it is.

(*Priority: High*)

**FR-ST-02: Create New Crownpass**. The system should enable the staff of Covid-19 Virus Test Centres to create a Crownpass for a person who is being tested but has not been registered to the Crownpass tracking system in the same process as if he/she is registering for him/herself. (*Priority: Medium*)

## Functional Requirements of Staff in Disease Control Centres

**FR-SD-01: Setup Monitoring Regions**. The staff of a Disease Control Centre should be able to set the geographical region that it is monitoring. Each disease control centre should have a specific monitoring region, which should be able to be divided hierarchically into a number of disjoint sub-regions, and sub-sub-regions, etc. (*Priority: High*)

**FR-SD-02: Setup Monitoring Staff Accounts**. The system should enable the setting up of a number of staff accounts for them to perform monitoring tasks. (*Priority: High*)

**FR-SD-03: Monitor Covid-19 Situation**. The system should enable the staff members of a Disease Control Centre to view the overall statistical data of its monitoring region and also the statistical data of its sub-regions in the hierarchical structure. (*Priority: High*)

## Functional Requirements of System Operators

**FR-SO-01: Setup Test Centre Accounts**. The system operator should be able to set up test centre accounts for the staff of test centres. (*Priority: High*)

**FR-SO-02: Setup Disease Control Centre Accounts**. The system operator should be able to set up accounts for the staff of disease control centres. (*Priority: High*)

**FR-SO-03: Manage System Parameters**. The system operators should be able to set and modify the system parameters, which include:

1. The length of backtracking period,
2. The length of effective overlap period,
3. The length of quarantine period,

(*Priority: High*)

**FR-SO-04: Manage Crownpass Accounts**. The system operators should be able to manage the Crownpass accounts following a guideline of Crownpass account management (to be further detailed). The following operations on the accounts should be supported:

* suspending an account,
* merging two accounts,
* modifying the state of a pass,
* adding new photo(s) of the pass holder

(*Priority: Medium*)

## Functional Requirements of Police Officers

**FR-PO-01: View State of Controlled Area**. The system should enable police officers to view the following data of a controlled area: (a) Name, Address, Type of the controlled area; (b) The Capacity of the controlled area; (c) The current number of persons in the area as recorded in the system. (*Priority: High*)

**FR-PO-02: Report Incident of A Controlled Area**. The system should enable to policy office to report incidents that a controlled area breaches the social distance rules and the actions taken by the police officer. (*Priority: High*)

**FR-PO-03: View the state of a Crownpass**. The system should enable the police officers to view the state of a Crownpass. (*Priority: High*)

**FR-PO-04: Report incident of Crownpass holder**. The system should enable the police officer to report incidents of that a Crownpass holder breaches the social distance rules and to record the actions taken by the police. (*Priority: High*)

# Required Design Features

This section presents the required design features of the system. They are essential for the use of the system to achieve its goals and objectives.

**DF-01: Delivery of Functions**. The functions of the system should be delivered to different types of users with a set of mobile Apps and Web-Based applications. In particular, the following different mobile applications should be developed:

* *Crownpass Holder*: To deliver the functions for Crownpass holders;
* *Crownpass Controller*: To deliver the functions for the operation staff of controlled area;
* *Crownpass Area Owner*: To deliver the functions for controlled area owners and all the functions to the operation staff of controlled areas;
* *Crownpass Policing*: To deliver the functions for police officers;
* *Crownpass Tester*: To deliver the functions for staff of test centres;

The following web-based applications should be developed:

* *Crownpass Covid-19 Monitoring System*: To deliver the functions to staff of disease control centres
* *Crownpass Operation System*: To deliver the functions to system operators

**DF-02: Storage and Processing of Data**. A cluster of computer system should be developed to store and process the following data:

* The registration information of Crownpass holders;
* The movement information of Crownpass holders;
* The states of Crownpasses and their transitions;
* The registration information of controlled areas;
* The movement information of controlled areas;
* The incidents reports;
* The setup information of disease control centres;
* The virus test results.

**DF-03: Application of AI Technology**. The face recognition and identification technique should be used to ensure that each person has no more than one Crownpass.

**DF-04: QR Code**. QR code (also known as 2D barcode) should be used to enable quick access to the cloud services for check-in/check-out a controlled area and entering the result of a virus test, etc. In particular, the following uses of QR code should be implemented.

1. Each Crownpass should be presented in the form of an identity photo of the pass holder plus a QR code that uniquely represents the identifier of the pass. The pass should be able to be displayed on the screen of a mobile phone and also be printed out on a normal sheet of paper. When the pass holder uses the pass to check-in to a controlled area, the operation staff of a controlled area should scan the QR code to get the state of the pass and a photo of the registered pass holder to match the photo on the pass and also the person to achieve the purpose of authentication. When a pass holder checks out a controlled area, the QR code will also be scanned and the photo on the pass will be matched against the person.
2. When a Crownpass holder is tested for Covid-19 virus, the same authentication process as check-in to a controlled area should take place. The QR Code should be associated to the test sample and used to enter the test result into the system.
3. A unique QR code should also be produced for each controlled area to enable police officers to inspect the operation of controlled areas. It can also potentially be used to enable self check-in and/or check-out by the Crownpass holders to scan the QR code of a controlled area when entering and leaving the area.

# Quality Requirements

This section gives the quality requirements on the system.

## Scalability.

**QR-SC-01: Crownpass Holder**. The system must be able to provide services to around 40 million Crownpass holders nationally, who will register at the beginning period when the system rolls out (predicted to be 80% in the first 2 weeks).

**QR-SC-02: Controlled Area**. The system must be able to provide services to around 5 million controlled areas nationally, who will register at the beginning period when the system rolls out (predicted to be 90% in the first 3 days)

**QR-SC-03: Check-in and Check-out**. The system should be able to provide services of check-in and check-out of controlled areas to the scale that the total numbers of check-ins and check-outs to controlled areas are predicted to be around 200 million per day during the weekends and holidays seasons, and around 100 million per day on other days.

**QR-SC-04: Test Centre**. The system should be able to provide services to staffs of test centres to the scale that the total number of Test Centres is around 10,000 nationally, and on average about 20 staff members in each test centre. The setup operations for test centres will take place in the first 3 days when the system rolls out. The number of tests of virus per day may increase from current 200,000 to 500,000.

**QR-SC-05: Disease Control Centre**. The system should be able to provide services to all disease control centres of the country to the scale that the total number of disease control centres is around 50 nationally, and the number of staffs in each centre ranges from 30 to 100 with an average of 60. The setup operations for disease centres will take place in the first 3 days when the system rolls out. The monitoring operations will be continuous, i.e. 24 hours day and 7 days a week for at least one year.

**QR-SC-06: Police**. The system should be able to provide services to the police officers all over the country to the scale that the total number of police officers is around 30,000. The total number of incident reports to be entered to the system per day is estimated to be around 1,500 nationally.

## Performance

The following quality requirements on response times to various types of operations are based on using mobile applications when the mobile device is connected to the internet via Wi-Fi to broadband networks.

**QR-PF-01: Registration of Crownpass**. The response time for each interactive operation in the process of registration for a Crownpass should be no more than 20 seconds.

**QR-PF-02: Check-in**. The response time for check-in a Crownpass holder into a controlled area should be no more than 3 seconds.

**QR-PF-03: Check-out**. The response time for check-out a Crownpass holder out of a controlled area should be no more than 10 seconds.

**QR-PF-04: Change Pass State to Red**. The time that a Crownpass’ state is changed into RED should be no more than 1 second after the Crownpass holder’s virus test result being positive is entered into the system.

**QR-PF-05: Change Pass State to Amber**. The time that a Crownpass’ state is changed into Amber should be no more than 5 seconds after a Crownpass holder’s virus test result being positive in entered into the system.

**QR-PF-06: Change Pass State to Green**. The time that a Crownpass’ state is changed into Green should be no more than 5 seconds after the pass holder’s virus test result being negative is entered into the system.

**QR-PF-07: Notification of State Change**. The notification of the state change to a Crownpass holder should be send out within 10 seconds after the state change takes place, if the notification is required.

**QR-PF-08: Setup Controlled Area**. The response time for each interactive operation in the process of setting up a controlled area should be no more than 10 seconds.

**QR-PF-09: Notification to Controlled Area**. When notifying a controlled area for the existence of Red pass holder in the area should be send out no more than 1 second once a pass state is changed into RED state.

**QR-PF-10: Setting up Test Centre**. The response time for each operation in the process of setting up the mobile application for a staff of a test centre should be no more than 5 seconds.

**QR-PF-11: Enter Test Result**. The response time for the operation of entering a test result to the system should be no more than 5 seconds.

**QR-PF-12: Setup Police Officer Account**. The response time of each operation in the process of setting up a police officer’s account should be no more than 5 seconds.

**QR-PF-13: Report Incident**. The response time for each operation in the process of police officer’s reporting of an incident should be no more than 3 seconds.

**QR-PF-14: Inspect Controlled Area**. The Response time for inspecting the data of a controlled area should be no more than 3 seconds.

The following performance requirements are based on assumptions that the desktop computers used by the staff in a disease control centre is connected to the internet via a fibre broadband computer network.

**QR-PF-15: Setup Disease Control Monitoring System.** The response time of each operation in the process of setting up the computer system of a disease control centre should be no more than 10 seconds.

**QR-PF-16: Update Monitoring Data**. The response time (i.e. the latency) for updating the statistical data for a disease control centre should be no more than 1 second.

## Reliability

**QR-RE-01: Cloud Availability**. The services provided by the system running on the cloud should be available 24 hours a day and 7 days a week with a yearly accumulated downtime no more than 10 hours including for planned maintenance and unplanned failures.

**QR-RE-02: Cloud Meantime to Recovery**. The services provided by the system running on the cloud should be able to recover quickly from failures with a mean-time-to-recover less than 1 hour over the period of 1 calendar year.

**QR-RE-03: Cloud Meantime to Failure**. The services provided by the system running on the cloud should not fail frequently with a meantime to failure greater than 1000 hours in a period of one calendar year.

**QR-RE-04: Mobile Apps Failure Rate**. For each mobile App on each platform and for each type of users, the failure rate should be lower than 0.3% per use.

**QR-RE-05: Disease Control Centre Availability**. The computer systems used by a Disease Control Centre should be able to operate continuously 24 hours a day and 7 days a week all year round with a failure rate lower than 100 hours per year in any consecutive operation period of one calendar year.

**QR-RE-06: Disease Control Centre Meantime to Failure**. The computer systems used by a Disease Control Centre should not failure frequently. Its meantime to failure should be greater than 720 hours in any operation period of one calendar year.

**QR-RE-07: Disease Control Centre Meantime to Recover**. The computer systems used by a Disease Control Centre should be able to recover quickly with a meantime to recover less than 2 hours in any operation period of one calendar year.

**QR-RE-08: Functional Error Rate**. Error to perform various functions of the system should be lower than the following error rates according to the types of functions.

1. Crownpass registration: The failure rate to prevent own multiple passes should be less than 0.001%;
2. Check-in with fake Crownpass: The failure rate to prevent a person to check-in to a controlled area using other people’s pass (exclude self-check-in) should be less than 0.005%.
3. Check-in/Check-out error: The failure rate to record the correct data of entering and leaving a controlled area should be lower than 0.002%.
4. Entering Test Result: The failure rate to entering the test results to the system correctly should be lower than 0.0001%.
5. Update Crownpass state: The failure rate to update Crownpass states should be lower than 0.0001%.
6. Update statistical data: The failure rate to update statistical data should be lower than 0.0%.
7. Report incidents: The failure rate for correctly recording the incidences reported by a police officer should lower than 0.01%.

**QR-RE-09: Accuracy of statistical data.** The precision of statistical data is 2 decimal points and the data should be accurate to the true state of the system within 10 minutes.

## Security and Privacy Protection

In general, the system must comply with the European law of General Data Protection Regulation (GDPR) [[[5]](#endnote-3)]. The following gives the details of the requirements on security and data protection requirements on the system.

**QR-SE-01: Individual User Data Privacy Protection**. The access to data of Crownpass holders are restricted to the following rules. No any other uses of the data are allowed.

1. The following elements of a Crownpass holder’s data are private and can only be accessed for both viewing and modification by the user of the Crownpass holder:
	1. Name and address,
	2. Contact details,
	3. The times and dates of entering and leaving controlled areas,
2. The Crownpass holder can view the virus test results and the state of the pass of his/her own, but not modify these data.
3. The registered photos of a Crownpass pass holder and the state of the pass should be viewed by the operation staff of controlled areas through scanning the QR code of the Crownpass in order to authenticate the person when using the Crownpass to enter a controlled area.
4. The user’s data can be viewed and modified by the system operation staff when managing Crownpass accounts as requested by a Crownpass holder and restricted to access only the part of relevant data.

**QR-SE-02: Statistical Data Protection**. The generation and uses of statistical data from the users’ individual data must follow the rules below.

1. The results of statistical calculation and analysis can only be presented to registered disease control centres as requested and limited to the statistical data of the geographic region set for the disease control centre to monitor.
2. The results of statistical calculations and analysis of the states of Crownpasses for a period of time and in a geographic region and pass holders’ presences in controlled areas must be presented after removing the identities of Crownpass holders.

**QR-SE-03: Controlled Area Data Protection**. The data associated to any controlled area must be protected according to the following rules.

1. The data of the numbers of Crownpass holders’ presences in a specific controlled area at any given time should only be viewed by the owner of the controlled area and police officers.
2. The registration data of a controlled area is regarded as public information and thus not protected for viewing, but the data can only be modified by the owner of the controlled area.

**QR-SE-04: User Authentication**. The uses of the system must be authenticated according to the following rules.

1. The system should prevent a person to own more than one Crownpass.
2. A Crownpass holder check-in to a controlled area using a Crownpass must be authenticated to be the true owner on the pass.
3. The user who uses a mobile App for any give type of users must be authenticated to be the true user of the mobile devices.

## Platform Compatibility

**QR-PC-01: Mobile Apps Platform.** The mobile App for each type of users must be available for top 5 smart mobile phone operating systems (including different versions), and top 10 makes and models.

**QR-PC-02: Disease Control Centre Platform**. The computer systems for a disease control centre should be available for the Windows, Mac and Linux operating systems.

## Usability

**QR-US-01: Mobile Apps GUI**. For each user type, the mobile app should provide a graphic user interface and a short operation procedure with no more than three steps for users to use the mobile application. The HCI design of the mobile apps should have the following properties.

1. The user interface and operation procedure of each mobile app running on different platforms should be recognisably identical.
2. The user interface should comply to the accessibility standard [[[6]](#endnote-4)].
3. The user interface should adapt to the screen size automatically.

**QR-US-02: Online Helps**. For each user type, online helps should be provided in the form of video clips shown how to use the systems in various scenarios.

1. [↑](#endnote-ref-2)
2. The length of the trace-back period may change when the advices from the domain experts are updated. [↑](#footnote-ref-1)
3. The lengths of the overlap may change when the advices from the domain experts are updated. [↑](#footnote-ref-2)
4. The length of the isolation may change when the advices from the domain experts are updated. [↑](#footnote-ref-3)
5. [↑](#endnote-ref-3)
6. [↑](#endnote-ref-4)