OXFORD BROOKES UNIVERSITY

**School of Engineering, Computing and Mathematics**

**COMP6030 Software Engineering**

Case Study for Coursework

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

**Requirements Definition**

(Version 2.00, 1st Sept. 2021)

**Hong Zhu**

School of Engineering, Computing and Mathematics

Oxford Brookes University

Oxford OX33 1HX, UK

Email: [hzhu@brookes.ac.uk](mailto:hzhu@brookes.ac.uk)

**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 as well as the required design features of the system.

**Table of Contents**

[1 Introduction 1](#_Toc81489020)

[2 Types of Targeted Users 2](#_Toc81489021)

[3 Functional Requirements 3](#_Toc81489022)

[3.1 Functional Requirements of Crownpass Holders 3](#_Toc81489023)

[3.2 Functional Requirements of the Owner of Controlled Area 3](#_Toc81489024)

[3.3 Functional Requirements of Operation Staff of Controlled Area 4](#_Toc81489025)

[3.4 Functional Requirements of Test Centre Staff 4](#_Toc81489026)

[3.5 Functional Requirements of Staff in Disease Control Centres 4](#_Toc81489027)

[3.6 Functional Requirements of Managers of Vaccine Station/Centre 5](#_Toc81489028)

[3.7 Functional Requirements of Operation Staff of Vaccine Stations/Centres 5](#_Toc81489029)

[3.8 Functional Requirements of System Operators 6](#_Toc81489030)

[4 Required Design Features 6](#_Toc81489031)

[5 Quality Requirements 7](#_Toc81489032)

[5.1 Scalability. 7](#_Toc81489033)

[5.2 Performance 8](#_Toc81489034)

[5.3 Reliability 9](#_Toc81489035)

[5.4 Security and Privacy Protection 10](#_Toc81489036)

[5.5 Platform Compatibility 10](#_Toc81489037)

[5.6 Usability 10](#_Toc81489038)

[6 References 11](#_Toc81489039)

# 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*.

The basic idea of the 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 on 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[[1]](#footnote-1)* and had an overlap of the periods more then *15 minutes[[2]](#footnote-2)* have the potential being infected, thus they should be informed to self-isolate for *14 days[[3]](#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 above isolation rule and access restriction rules for controlled areas are exempted for those who have completed two doses of Covid-19 vaccines.

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. With the rapid and large scale roll out of Covid19 vaccines, the system is also required to record and maintain vaccination states for the Crownpass holders and to enable control of the accesses to public controlled areas according to their vaccine status. It is therefore required to provide facilities to vaccine stations and centres so that the status of vaccine can be systematically recorded and managed efficiently.

To achieve this gaol, the system should fulfil the following objectives.

1. Each individual has no more than one unique identifier, called “*Crownpass ID*” in the sequel, and a Crownpass holder can be checked physically to be the right person, say, through matching a photo of the pass holder. For privacy protection purposes, this Crownpass ID will be independent to any other personal identifications like passport, driving licence, or any other travel documents. An initial design of the appearance of the Crownpass is to have

* a photo of the pass holder,
* a 2D bar code as the pass holder’s Crownpass ID,
* the colour code of infection state,
* the colour code of vaccination.

1. The system will collect and store the covid-19 infection and vaccination state for each pass holder and automate the state transitions in real-time when information become available due to Covid-19 virus test, self-isolation finishes, or vaccination. The state of Covid-19 infection and vaccination are retrieved from computers running on the cloud quickly. Three states of infection have been identified:

* *Green*: No infection by Covid-19;
* *Amber*: Suspected of infection by Covid-19;
* *Red*: Confirmed infection by Covid-19.

The states of vaccination are:

* *White*: no vaccination is done,
* *Light* *Blue*: the vaccination of the first dose is completed,
* *Dark* *Blue*: the vaccination of the second dose is completed.

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 in a geographic area of the total number and percentage in the population of confirmed cases of Covid-19 infections, suspected infections, persons in isolation, the first dose vaccinations performed, the second dose performed, etc. A disease control centre is responsible to monitor the state of Covid-19 epidemic in a geographic area, which is called a disease control region, which can be a town, a city, a district, a county, etc. The system must provide disease control centres with real-time accurate data so that a regional lockdown decision can be made promptly based on accurate data.
3. The system should provide facilities to support the staff members of vaccine stations for recording the vaccinations of Crownpass holders so that their vaccination states can be changed immediately.

The scope of the system at this 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. *Managers of Vaccination Stations/Centres*: They are individuals in responsible of the management of vaccine station and/or vaccine centres. They may have variant digital literacy and experiences of using desktop computers and/or mobile devices. They will be provided either a desktop computer and/or a mobile device (such as iPad and tablet computers) to perform the related tasks.
7. *Operation Staff Members of Vaccine Stations/Centres*: They are individuals working in the vaccine stations/centres and responsible for recording the vaccinations performed. They may have variant digital literacy and experiences of using mobile devices. They will be provided a mobile device (such as an iPad or a mobile phone) to perform the related tasks.
8. *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.

# 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 a Crownpass ID. 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 holder and a QR code (also known as 2D bar code) that represents the pass holder’s identifier, and the infection state of the pass in colour code of *Green*, *Amber* and *Red* as defined in Section 1, and the vaccination state in colour code of *White*, *Light Blue, Dark Blue* as defined in Section 1. (*Priority: High*)

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

**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 Crownpass ID: (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: Medium*)

**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: Medium*)

**FR-CH-09: Book Vaccination**. A Crownpass holder should be provided a facility to book a vaccination at a vaccine station/centre on an available date and time slot of his/her choice. (*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.

**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 infection 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*)

**FR-OC-07: Set Entry Condition.** An owner of a controlled area should be able to set and update the entry condition to be *Green* or *Light Blue* or *Dark Blue*. If the entry condition is *Green*, it allows all Crownpass holders of *Green* infection state, and all *White*, *Light Blue* and *Dark Blue* states of vaccination to enter the area. If the entry condition is *Light Blue*, it only allows Crownpass holders whose vaccination states ate either *Light Blue* or *Dark Blue* and infection state is *Green* to enter. If the entry condition is *Dark Blue*, it only allows Crownpass holders whose vaccination states are *Dark Blue* and infection state *is Green*. If no entry condition is specified, the default is *Green*. (*Priority: High*)

## 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 satisfies the area’s entry condition; 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 the statistical data of its sub-regions in the hierarchical structure. The statistical data that the system enables monitoring should also include the total numbers and percentage of the population of the following data

* Tests of Covid-19,
* Tests with positive results,
* Tests with negative results,
* Tests with nonconclusive results,
* Suspected infections (in the Amber infection state),
* Vaccinations of the first dose,
* Vaccinations of the second dose.

(*Priority: High*)

## Functional Requirements of Managers of Vaccine Station/Centre

**FR-MV-01: Registration of Operational Staff of Vaccine Stations/Centres.** The managers of vaccine stations/centre should be provided with a facility to register users of operation staff working in vaccine stations/centres. The registration data of operation staff members should contain the following contents:

1. Name of the account holder,
2. Photo of the account holder,
3. Personal information of the account holder, including age and gender.
4. Home address,
5. Contact telephone number,
6. Contact email address,
7. Staff number of the employment (optional),
8. Job title, which can be either a *nurse,* a *receptionist*, a *doctor*, or *onsite manager*,
9. Crownpass user ID.

(*Priority: High*)

**FR-MV-02: Setup Operation Timetable and Capacities.** The managers of vaccine stations/centres should be provided with a facility to set up the operation time tables for the vaccine stations/centres. An operation timetable for a vaccine station/centre should include the following information:

1. Dates that the vaccine station/centre opens.
2. For each date that it is open, the time slots available and the number of vaccine injections can be delivered for each time slot.

(*Priority: High*)

**FR-MV-03: Assignment of Operation Staff**. The managers of a vaccine station/centre should be provided with a facility to assign operation staffs to the open dates and time slots.

(*Priority: High*)

**FR-MV-04: View Booking and Operation States of Vaccine Station/Centre**. The managers of a vaccine station/centre should be provided with a facility to view the booking states and completion states of the vaccine station/centre.

(*Priority: High*)

## Functional Requirements of Operation Staff of Vaccine Stations/Centres

**FR-OV-01: Record Vaccinations.** The operation staff members of a vaccine station/centre should be provided with a facility to record the vaccinations done for Crownpass holders. The following data of vaccination should be recorded:

1. The person’s unique Crownpass ID number,
2. The date that the vaccine is injected,
3. The time slot that the vaccine is injected,
4. The name of the vaccine injected,
5. The batch number of the vaccine,
6. The vaccine station/centre where the vaccine is injected,
7. The nurse who conducted the injection,
8. The staff Id of the person who entered the record into the system.

The initial state of vaccination is *White*. When a vaccination is performed and/or a record of the vaccination is entered to the system, the event will trigger the transition of the state of the Crownpass as follows:

1. the Crownpass state is changed to Light Blue if it is the first vaccine of the Crownpass holder.
2. The Crownpass state is changed to Dark Blue if it is the second vaccine of the Crownpass holder.

The other rules of Crownpass state transition as stated in **FR-ST-01** remain valid.

(*Priority: High*)

**FR-OV-02: Registration and Management of User Account**. The operation staff members of vaccine stations/centres should be provided with a facility to view, setup and update the data associated to his/her user account. (*Priority: High*)

**FR-OV-03: Managing Vaccination Bookings**. The operation staff members of a vaccine station/centre should be able to view the bookings of a date and time slot, to add new bookings into the system and remove an existing booking from the system on behalf of a Crownpass holder. The operation staff members should also be able to update the booking state from booked to completed when a vaccination is done. (*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*)

**FR-SO-05: Setup and Manage the Manager Accounts of Vaccine Station/Centre**. The system operators should be able to set up and manage the accounts for vaccine stations/centres. (*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/Desktop computer applications. In particular, the following subsystems should be developed:

* *Crownpass Holder*: To deliver the functions for Crownpass holders in the form of mobile App.
* *Crownpass Controller*: To deliver the functions for the operation staff of controlled area in the form of a mobile App.
* *Crownpass Owner*: To deliver the functions for owners of controlled area plus all the functions of the operation staff of controlled areas in the form of a mobile App.
* *Crownpass Tester*: To deliver the functions for staff of test centres in the form of a mobile App.
* *Crownpass vaccinator*: To deliver the functions for the operation staffs of vaccination stations in the form of a mobile App.

The following desktop/web-based computer applications should be developed:

* *Crownpass Monitor*: To deliver the functions to staff of disease control centres in the form of a desktop/web-based computer application.
* *Crownpass Operation System*: To deliver the functions to system operators in the form of desktop/web-based computer application.
* *Crownpass Vaccine Manager:* To deliver the functions to the managers of vaccination stations in the form of desktop/web-based computer application.

**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 infection and vaccination states of Crownpass holders and their state transitions.
* The registration information of controlled areas.
* The movement information of controlled areas.
* The setup information of disease control centres.
* The virus test results.
* The registration information of the managers and operation staff members of test centres.
* The registration information of the managers and operation staff members of vaccine stations /centres.
* The vaccination data of each Crownpass holder.
* Entry conditions of controlled areas.

**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: Vaccine Station**. The system should be able to provide services to all vaccine stations of the country to the scale of the total number of vaccine stations is around 20,000 nationally. The numbers of staffs in a vaccine station range between 20 to 200 and on average is around 50. The number of vaccinations may reach 100,000 per day in total 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 vaccination station**. The response time of each operation in the process of setting up a vaccination station should be no more than 5 seconds.

**QR-PF-13: Enter vaccination data**. The response time for each operation in the process of entering vaccination data should be no more than 3 seconds.

**QR-PF-14: View State of Controlled Area**. The response time for viewing 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 and vaccination data: The failure rate to entering the test results and vaccination data to the system 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) [[[4]](#endnote-2)]. 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 vaccination data 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: Desktop/Web-based Application Platform**. The desktop/web-based computer systems for a disease control centre, test centre and vaccination management should be available for the Windows, Mac and Linux operating systems and compatible with Chrome, Firefox and Safari web browsers.

## 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 [[[5]](#endnote-3)].
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.

# References

1. The length of the trace-back period may change when the advices from the domain experts are updated. [↑](#footnote-ref-1)
2. The lengths of the overlap may change when the advices from the domain experts are updated. [↑](#footnote-ref-2)
3. The length of the isolation may change when the advices from the domain experts are updated. [↑](#footnote-ref-3)
4. [] Gdpr.eu, Complete guide to GDPR compliance, URL: <https://gdpr.eu>. (last Access: 1 Nov. 2020) [↑](#endnote-ref-2)
5. [] European Telecommunications Standards Institute, Accessibility requirements suitable for public procurement of ICT products and services in Europe, EN 301 549, V1.1.1, Feb. 2014. (URL: <https://www.etsi.org/deliver/etsi_en/301500_301599/301549/01.01.01_60/en_301549v010101p.pdf>) [↑](#endnote-ref-3)