QR Code Gate Pass System Design and Implementation

Design: Yilmaz AMCA
Development: Ali CANDEMIR
Project Consultant: Prof. Dr. Hasan AMCA

June 2021

PROJECT DETAILS

QR Based Facility Access System (QR-FAS) proposed here is a specially designed and customized project by our expert group to fit the needs of many business, government and nongovernment institutions to control authorized access to the business premises. A typical example is shown in Figure 1 below. The software will be provided via a Cloud Servers and hosting will be provided as long as the business demands. The authorization process to enter the target facility will begin with the click of the **Application for Appointment** button on the service providers web page. The user will choose the purpose to enter the facility, the date and time period from the drop-down menu. Once the date and time are entered, a message will be received by the system admin for approval. The system admin will approve or turn down access after checking the purpose and time required for access. The system will then send an email to the customer with the QR code and the institution details, purpose of access, date and time for the access demanded. The system can be upgraded to support additional services such as SMS in the second phase of the project on a new contract if demanded by the company. Please note that the SMS service get charged differently depending on the location and service provider.

Once the ticket to access the facility is received, the customer is ready to visit the business premises. On the entrance door, the customer will show the QR code on the smart phone screen or on a printout paper and the person at the gate will read the QR code with any QR code reader such as Google Authenticator. The system will direct the data to the server and the server will verify the code and allow access to the facility.

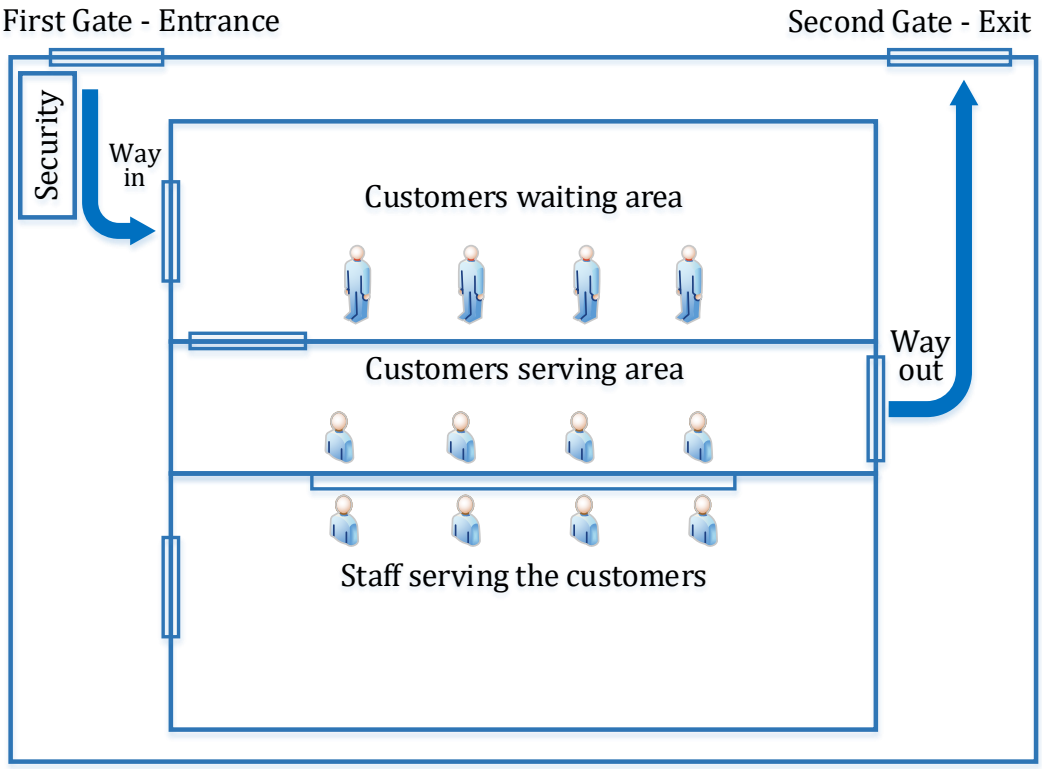

Fig. 1: The Company premises where the QR Based Facility Access System will be implemented.

DESCRIPTION OF THE FACILITY ACCESS SYSTEM AND ITS USAGE WITH GOOGLE AUTHENTICATOR (OR ANY COMPATIBLE AUTHENTICATOR APP)

The Time-Based One-Time Passwords (TOTP), is a very effective way of generating short duration authentication tokens commonly used for the applications which require authentication. The TOPT or similar algorithms are open standard applications which can be implemented in a compatible way in many different

applications such as Authy or Google Authenticator. However, there are numerous other options including Duo and Microsoft Authenticator. Implementing and enabling the Facility Access System is half of the battle of improving account security to give the customers flexibility over which authenticator app they should use. The Authy API is a means of enrolling the user in the Authy App. The Authy App is a free mobile / desktop app for Two-Factor Authentication, as well as security partner and SMS delivery service for many websites that want to make Two-Factor Authentication work better for their users. It is required for verifying and account ownership and also to register the app.

The Operating Principles of the TOTP

The TOPT algorithm requires a secret key and the system time as its inputs, which are in return used in a one-way function that creates a truncated, readable token, as shown in Figure 2. Since these inputs are available offline, the whole system can successfully work offline. This is a big advantage for users who may have unstable cellular network connections for receiving SMS 2FA or for users who want a more secure channel than SMS 2FA.

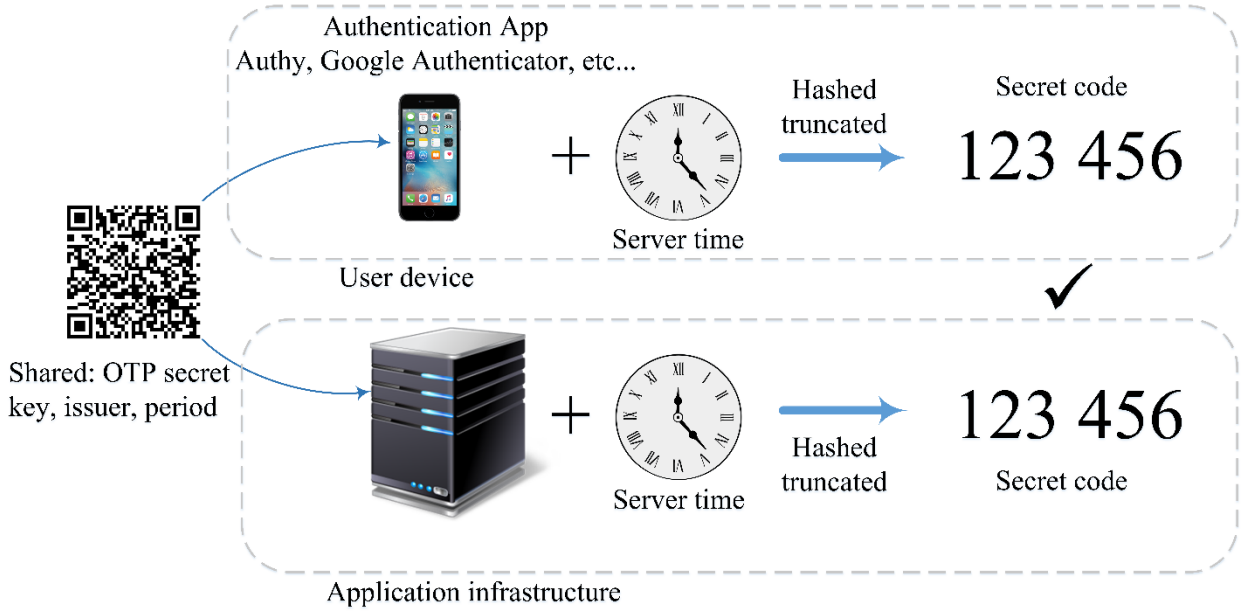

Fig. 2. The TOPT algorithm providing Two-Factor-Authentication.

Implementing TOTP Facility Access System in an Application

The use of applications such as Authy API is recommended to implement TOTP in your application since it a) manages passcode generation and checking for you, b) it is SOC2 compliant, c) it includes our end-user support and finally d) it has SMS, voice and email channels to support fallback or user choices.

To register a user of your application for any authenticator app takes a couple steps.

Step 1: Sign into your application account (or create a new account if you already didn't) and create an application in the application console.

Step 2: Enable the generic TOTP tokens in the console and save your data.

Step 3: To validate TOTP codes, you need to register each user with the API to generate a unique ID.

Registering Users to your Application

Users can register to the application through the console using the user's phone number and/or email address. On the user's tab of your application in the console, click the add a new user button. You need to enter your email address and phone number.

SYSTEM INITIATION AND SOFTWARE DOCUMENTATION

The developed cloud software will be executed and run on the Internet. Users trained by the system developers will be able to moderate and manage the system via "Admin Interface" of the software anywhere by signing into the system.

Technology Compilation

The software will be designed as a Progressive Web App (PWS). A progressive web application is a type of application software delivered through the web, built using common web technologies including PHP, HTML, CSS and JavaScript. It is intended to work on any platform that uses a standards-compliant browser, including both desktop and mobile devices. Both system admin and customers will be able to install the application via the website and open with one click in their mobile devices. For the maximum scalability, the app will be hosted on cloud servers and no additional installation or configuration will be required for System Admins.

System Description and Use Case Scenarios

The following section describes the system in more details with reference to the specific use case where access is granted via the *Generic Permission System*:

a) The users will register to the appointment system using their Booking Number or Container Number, whichever one they have as shown in Figure 3.
b) System admin can manually approve the validity of the Booking Number or Container Number by comparing the entered numbers with the database and grant permission in advance as shown in Figure 4. This step should ideally be automatic if access is given to an isolated copy of the set of Booking Numbers or Container Numbers currently in process. System admin will be able to configure any necessary system setting as shown in Figure 5.
c) Generic permissions will be defined and assigned to the QR code for the particular user as a TOTP token. The QR code will be scanned at the entrance gate for access.
d) If there are more than one gate (or different access levels), system admin can assign this permission on the issued QR code before creating the invitation.

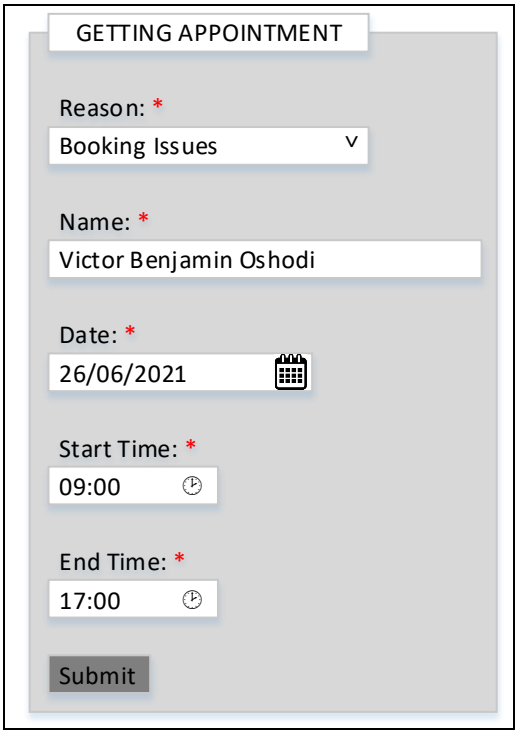

Fig. 3: Application for appointment.

Tickets will be designed to show all necessary information, including the company logo, any Personally Identifiable Information (PII) and user credentials.

The operating principles of the generic QR Coded Facility Access process is summarized in the flowchart depicted in Figure 5 below.

Fig. 4: The Smart Appointment System invitation ticket layout.

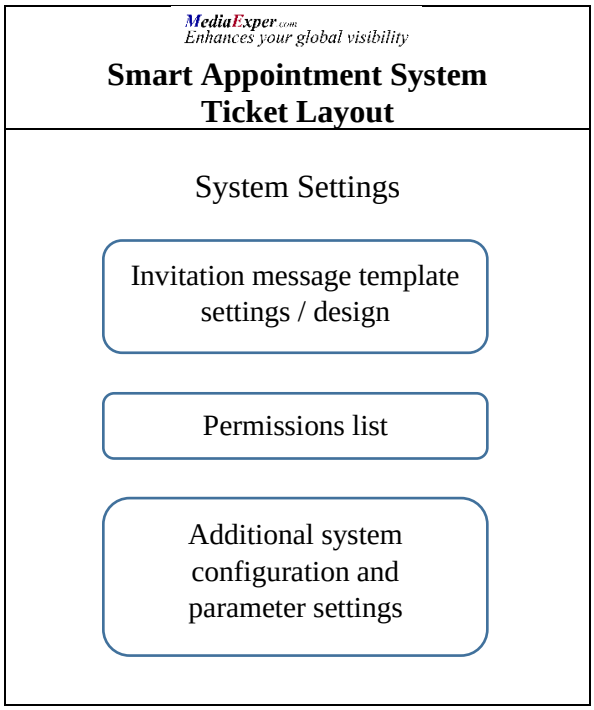

Fig. 5: The Smart Appointment System invitation ticket layout.

Budget Breakdown

The system design, implementation, testing and training the admins and the end users as a turn-key solution will cost $1000 (One Thousand US Dollars).

The software development and project management consultation fee will be 500 USD.

The advertising, promotion, business development, quality of service and customer relationship consultation charge for the host company will be 500 USD.

In addition to the purchasing price, there will be a 25% annual maintenance fee to ensure that the technical support team will attempt to solve any problem, unexpected fault or misuse within a three hours period.

Any additional function will be added to the system for a price of 500 USD.

Future Work

The first version of the application will involve manual approval by the system admin of the status that the related person has an issue to deal with in the facility and sending the approval to the customer in the form of QR code by email. At the second version of the application, the manual approval will be made automatic based on the automatic checking of the container number or the ticket number of the customer and sending the QR code of the gate pass ticket.

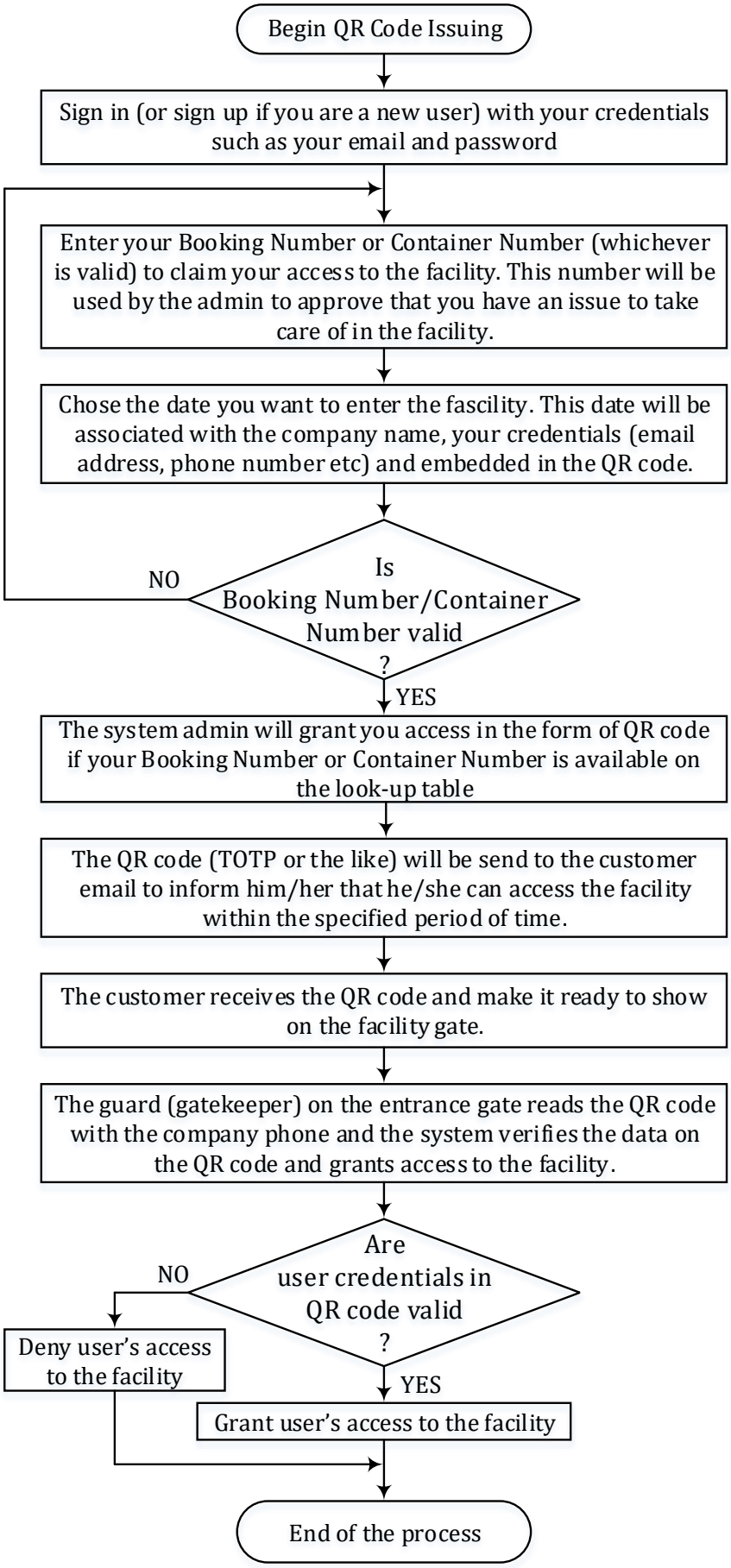

Fig. 6: The pictorial representation of the QR coded facility access process.

References

[1] Personally Identifiable Information (PII), https://www.plurilock.com/answers/pii-what-does-pii-mean/
[2] QRickit, https://qrickit.com/qrickit_apps/qrickit_qrcode_creator_email_checkin.php
[3] Twilio Docs, https://www.twilio.com/docs/authy/api
[4] Twilio / authy-python, https://github.com/twilio/authy-python
[5] Twilio Authy, https://authy.com/guides/discord/
[6] How to generate a QR Code for Google Authenticator that correctly shows Issuer displayed above the OTP? https://stackoverflow.com/questions/34520928/how-to-generate-a-qr-code-for-google-authenticator-that-correctly-shows-issuer-d
[7] OTP - Time based One Time Password, https://www.error509.com/2018/05/otp-time-based-one-time-password/
[8] QR Code Generator, CREATE YOUR QR CODE FOR FREE, https://www.qr-code-generator.com/