Grüner Pass & GreenCheck

Die Frage / das Problem:

Wie funktioniert das aktuell eingesetzte System in seiner digitalen und analogen Form und ist es geeignet, eine effektive Corona-Zugangskontrolle zu gewährleisten?

Welche Schwachstellen hat das aktuelle System mit seinen beiden Apps?

Wie unterscheiden sich der digitale und der analoge Ausstellungs- und Kontrollprozess?

Welche Daten speichert der QR-Code und wie wird er erzeugt?

Wie kann ein QR-Code ohne Impfung erstellt und wie kann eine solche Fälschung erkannt werden?

Ist die zusätzliche analoge Kontrolle eines Lichtbildausweis sinnvoll und wovor schützt sie?

Wie sieht das Architekturdiagramm des aktuellen Systems aus?

Wie sieht das Sequenzdiagramm des aktuellen Systems im digitalen und analogen Fall aus?

Funktion des aktuellen Systems

Der grüne Pass ist im Grunde nur ein gespeichertes Zertifikat, in dem dein Name und die Anzahl der Impfungen mit den jeweiligen Impfstoffen enthalten ist. Die Kontrolle ob das Zertifikat gültig ist erfolgt dabei über einen QR-Code der über die GreenCheck Website der gv.at eingescannt wird.
In GreenCheck gibt man die benötigte Anzahl Impfungen an (G2, G3, etc.) und nach dem Scannen des QR-Codes wird entweder ein grünes Häkchen oder ein rotes Kreuz zurückgegeben. Ein Boolean (true oder false) also.
Um die Zertifikate in den grünen Pass zu laden hat man zwei Möglichkeiten. Entweder man lässt sich ein Dokument in der Apotheke ausdrucken und scannt dann den QR-Code oder man loggt sich per Handysignatur ein und lädt es direkt auf das Handy herunter.

Sicherheit

Im QR-Code werden die Informationen verschlüsselt gespeichert und er ist auch digital signiert, der verwendete Schlüssel geheim. Somit kann das Zertifikat theoretisch nur von offizieller Seite ausgestellt werden und eine Fälschung würde auffallen.
Mitte Juli haben Studenten der FH Hagenberg allerdings festgestellt das die Grüner Pass App die Gültigkeit des QR-Codes nicht überprüft wird, man also einen gefälschten QR-Code verwenden könnte.
Angeblich soll dieser Fehler schon gelöst sein und die Validierung der elektronischen Signatur erfolgen. Die App zeigt seitdem direkt an ob Zertifikate gültig sind oder nicht.
Aber: Es wird nicht überprüft ob man tatsächlich sein eigenes Impfzertifikat verwendet. Auch kann die Echtheit des Zertifikates nur dann gewährleistet werden wenn der QR-Code mit der GreenCheck-App kontrolliert, was im echten Leben häufig nicht der Fall ist. So kann man leicht einen QR-Code fälschen der, wird er nicht per GreenCheck überprüft, für einen Impfnachweise gehalten wird.

Generell sind QR-Codes eher eine schlechte Möglichkeit sensible Daten zu speichern, eben da sie so leicht gefälscht und kopiert werden können. Solange der QR-Code im Spiel ist wird es immer eine Möglichkeit geben einen gültigen Code zu generieren oder kopieren wodurch die aktuelle Grüne Pass App keine absolute Sicherheit gewährleisten kann.

Zusätzlich gibt es bereits Algorithmen um QR-Codes zu generieren die selbst den GreenCheck austricksen. Selbst bei rechtlich korrekter Kontrolle kann also keine Sicherheit gewährleistet werden da die gefälschten QR-Codes als real erkannt werden. So sind unter anderem Adolf Hitler und Spongebob gültig geimpft, selbst nach Scan.

Digitale und Analoge Nutzung
Auf dem digitalem Weg wird das Zertifikat als Pdf heruntergeladen und dann in die Grüner Pass App gespeichert, als QR-Code. Dort wird dann, seit einem Update, sofort überprüft ob der QR-Code gültig ist und zeigt den grünen Hacken an. Jedoch muss der QR-Code noch durch die GreenCheck App kontrolliert werden und auch ein Lichtbildpass sollte vorgezeigt werden da sonst die Identität des Passinhabers nicht festgestellt werden kann.

Analog könnte man auch einfach zur Apotheke gehen und sich das Zertifikat ausdrucken lassen. So hat man denselben QR-Code, aber auf Papier. Wie im digitalen Verfahren muss hierbei wieder der QR-Code per GreenCheck überprüft und ein Ausweis dazu hergezeigt werden.

Wir haben also in beiden Fällen das Problem der Kontrolle, die realistisch gesehen kaum passiert und das Problem des QR-Codes die gefälscht sein können.

Selbstversuch
Was also wenn sie nun ihren QR-Code fälschen wollen oder etwa sogar den Code knacken und aufdröseln damit sie gültige QR-Codes in Massen produzieren können?

Ich habe einen kleinen Versuch gestartet um an den Aufbau des QR-Codes zu kommen. Dabei habe ich also einfach den QR-Code meines Zertifikates abfotografiert und dann mit dem normalen Handyreader eingescannt. Tatsächlich habe ich dann eine lange Zeichenfolge herausbekommen.

Diese Zeichen sind die verschlüsselten Daten hinter dem QR-Code. Wenn man also diese Verschlüsselung knackt kann man sich ganz einfach QR-Codes für Menschen erstellen die es gar nicht gibt. Aber es geht auch einfacher.

Ich habe die Zeichenfolge in einen Online-QR-Code-Generator kopiert. Diese Website erstellt einen QR-Code aus einem Pdf, einer URL oder auch einfach nur Text. Meine Erwartung hat sich bestätigt, es ist der komplett gleiche QR-Code den ich abfotografiert habe, warum sollte es auch etwas anders sein.

Man hat nun also den QR-Code aus dem Grünen Pass nicht nur als Foto sondern als Datei, als JGP zum Beispiel. Als Test habe ich nun diesen QR-Code mit dem Grünen Pass gescannt und er hat ihn problemlos akzeptiert. Ich könnte diesen QR-Code nun an alle meine Freunde senden und sie könnten ihn einfach in ihren Grünen Pass laden. Das einzige Problem ist das sie alle meinen Namen im Pass stehen hätten, aber dann währen wir wieder beim Problem Kontrolle.

Bei näherer Überlegung und einem kleinen Test ist mir dann aufgefallen das diese offensichtliche Sicherheitslücke ein Feature ist. Man kann die QR-Codes ja sogar direkt aus dem Grünen Pass eines anderen Importieren. Das dient dazu sämtliche Grüne Pässe einer Familie auf dem gleichen Gerät zu speichern.

Dadurch ist aber sämtliche Überprüfung ohne einen Ausweis sinnlos und eben dieser Identitätscheck wird so gut wie nie durchgeführt.