1. Welche Schwachstellen hat das aktuelle System mit seinen beiden Apps?

* QR Code kann leicht gefälscht werden
* Ohne Kontrolle eines Ausweises ist das System noch unsicherer (man weiß nicht, ob das Zertifikat wirklich zu der Person gehört oder nicht)
* Wird das Zertifikat ohne scannen des QR-Codes kontrolliert, ist es ganz leicht möglich über Word ein gleiches Dokument einfach nachzubauen.
* Die Kartennummer der e-Card dient als Schlüssel für den Zugang zu den Gesundheitsdaten aus dem Covid-Pass. Das heißt man kann mit geringem technischen Aufwand den Corona-Status einer Person aus einem zentralen System abfragen.
* Es ist ebenfalls möglich durch ein massenhaftes Abrufen dir Daten aller sozialversicherten Personen in Österreich zu erlangen.

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

**Digital: „Grüner Pass“ -Dokument eingescannt in der *Grüner Pass* App**

Ausstellung:

* Das Dokument kann auf der Gesundheit.gv.at Seite gedownloaded werden (dazu wird eine Handysignatur benötigt)
* Beim Anmelden mittels Handysignatur wird Telefonnummer und das Signaturpasswort benötigt
* In der *Grüner Pass* App kann man dann das erhaltene Dokument scannen und man bekommt den QR-Code in der App angezeigt (auch Eingabe mehrerer Impfnachweise/Genesungsnachweise ist möglich)

Kontrolle:

* Kontrolliert werden die QR-Codes mit der *GreenCheck* App
* Eingescannt wird praktisch nur der QR-Code-> man sieht dann Name, Geburtsdatum und Gültigkeit des Zertifikates

**Analog: Grüner Pass als PDF Dokument ausgedruckt**

Ausstellung:

* Das Zertifikat kann bei der Gemeinde, Apotheke oder bei den Bezirksverwaltungsbehörden kostenlos ausgedruckt werden

Kontrolle:

* Kontrolliert werden die QR-Codes mit der *GreenCheck* App
* Eingescannt wird praktisch nur der QR-Code-> man sieht dann Name, Geburtsdatum und Gültigkeit des Zertifikates

1. Welche Daten speichert der QR-Code und wir wird er erzeugt/ wie ist er aufgebaut?

Der QR-Code speichert den Vor- und Nachnamen, das Geburtsdatum und die Gültigkeit des Zertifikates.

Ein QR Code besteht aus mehreren Teilen:

* Positionsmarkierungen
* Damit Scanner den Code genau erkennen und mit hoher Geschwindigkeit lesen können
* Zeigt Richtung an, in die der Code gedruckt ist



* Ausrichtungsmarkierungen
* Helfen bei Verarbeitung des QR Codes auf unebenen Oberflächen



* Synchronisationslinien/Taktzellen
  + Definiert das Datenraster genau -> Scanner können bestimmen, wie groß die Datenmatrix ist



* Versionsfelder
* Diese Markierungen spezifizieren, welche der mittlerweile über 40 existierenden QR Code Versionen verwendet wird (Version 1-7 am geläufigsten)



* Formatfelder
  + Enthalten Informationen über Fehlertoleranz und Datenmaske des Codes -> erleichtern Scannen



* Datenfeld/ Nutz- und Fehlerkorrektur-Daten
* Enthält alle Daten, sowie Elemente zur Fehlerkorrektur -> können eine Beschädigung von bis zu 30% kompensieren



* Randzone
  + Bietet Struktur und verbessert Verständnis -> für Scan Programm
  + Wichtig, um QR Code von Umgebung zu unterscheiden

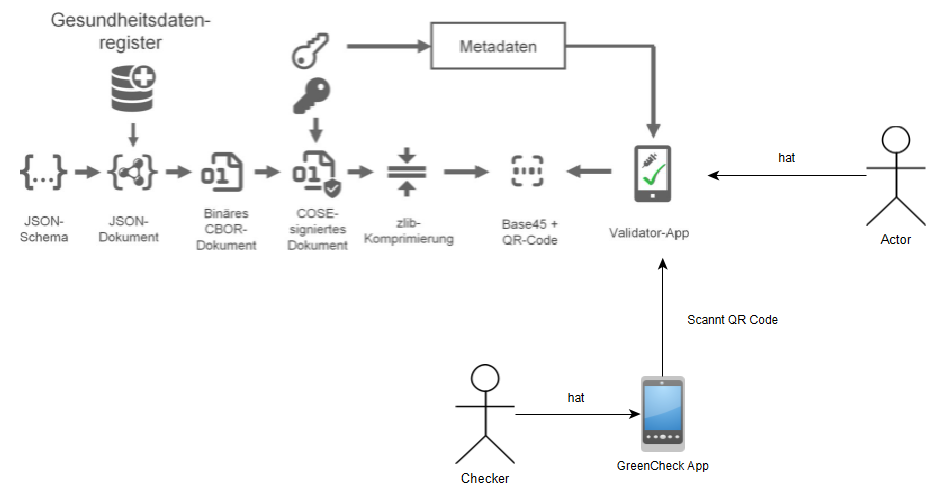
1. Wie kann ein QR-Code ohne Impfung erstellt und wie kann eine solche Fälschung erkannt werden?

* Mithilfe einer entsprechenden/ frei verfügbaren Software kann jeder innerhalb weniger Minuten einen QR-Code erstellen der „Grüner Pass“ Daten enthält. Dies ist so leicht möglich, da der Aufbau und die Codierung eines QR-Codes öffentlich bekannt sind und z.B. sogar auf Wikipedia genau beschrieben.
* Es kann nur das EU-konforme Zertifikat und dessen QR-Code als richtig eingelesen wird, das heißt, wenn der QR-Code nicht den EU vorgaben entspricht wird, kann dieser nicht richtig eingelesen werden. Ohne das Scannen des QR-Codes kann das ausgedruckte PDF ganz leicht gefälscht werden indem man einfach ein Textdokument in Word, etc. erstellt und dieses einfach mit einem originalen Zertifikat nachbaut und man sich kostenlos online einen QR-Code erstellen lässt.

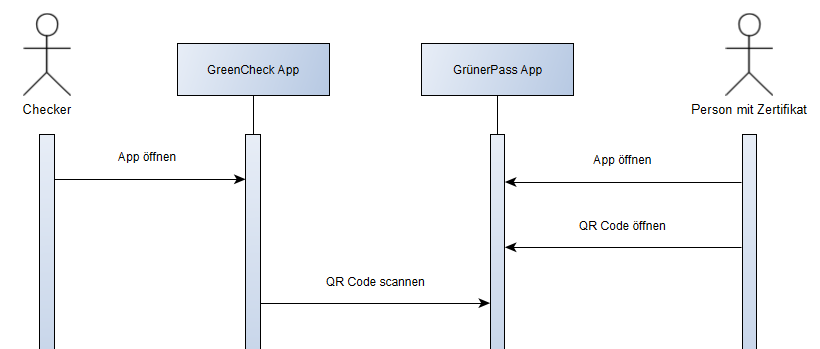
1. Ist die zusätzliche analoge Kontrolle eines Lichtbildausweis sinnvoll und wovor schützt sie?

Ja, die zusätzliche Kontrolle eines Lichtbildausweises ist sehr sinnvoll/ nötig, denn ohne sie kann man nie sichergehen, ob die Person, die das Zertifikat vorzeigt, wirklich die Person ist, der das Zertifikat gehört. (Man könnte z.B. einfach das Handy eines Freundes vorzeigen) Sie schützt sich so vor Betrug.

1. Wie sieht das Architekturdiagramm des aktuellen Systems aus?



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



Lösungsvorschlag für Grüner Pass:

Die Grundlage unserer Lösung wird ein System, auf Basis von biometrischer Verifizierung, sein.

So würde das System aufgebaut werden:

Erhalt des Grünen Passes Digital:

Durch Impfung:

* Nach der Impfung wird vom Personal der Fingerabdruck der geimpften Person, sicher verschlüsselt durch RSA256, über das Internet an eine Datenbank wo dieser mit dem Impfstatus gespeichert wird, aber ohne Daten wie Name, Geburtstag, Wohnort, … . Es wird der Person dann noch ein Blatt mit einem Code ausgehändigt der in der Grünen Pass App eingetragen werden kann und den Status des Passes zeigt, wobei aber auf dem Blatt auch das Gültigkeitsdatum des Passes steht.

Durch Genesung:

* Nach einer Genesung kann man sich mit dem Bescheid einer Behörde, bei einer Impfstelle oder bei einer Behörde, die Genesung eintragen lassen, indem man den Fingerabdruck einscannt und mit dem behördlichen Bescheid, verschlüsselt zur Datenbank schickt. Man erhält dann einen Code den man in der Grünen Pass App eintragen kann und sehen kann wie lange er noch gültig ist.
* Auch kann man sich nach einer Genesung zuhause den Grünen Pass holen, solange man einen Fingerabdruckscanner, am Handy oder am PC, zur Verfügung hat, indem man den behördlichen Schein einscannt oder abfotografiert und auf einer Webseite, den Fingerabdruck und den Bescheid hochlädt, welche verschlüsselt an die Datenbank gesendet werden.

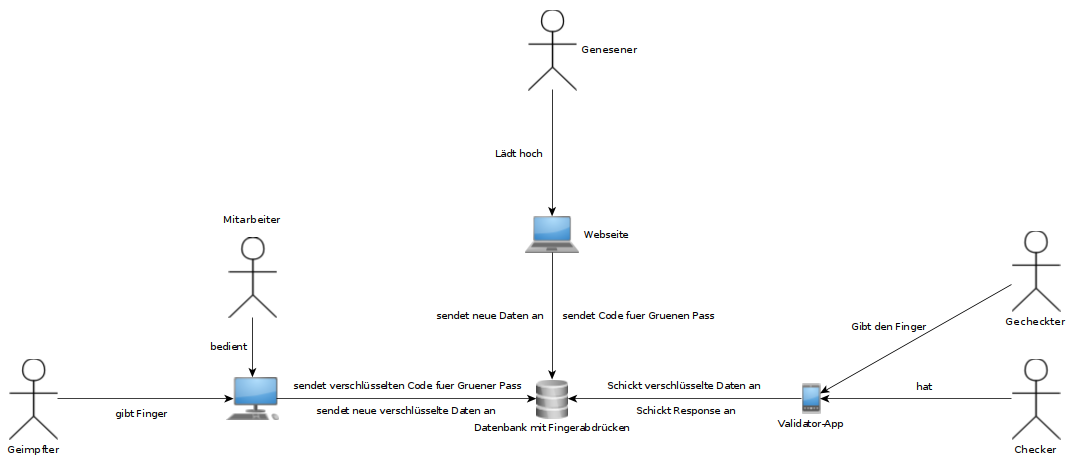
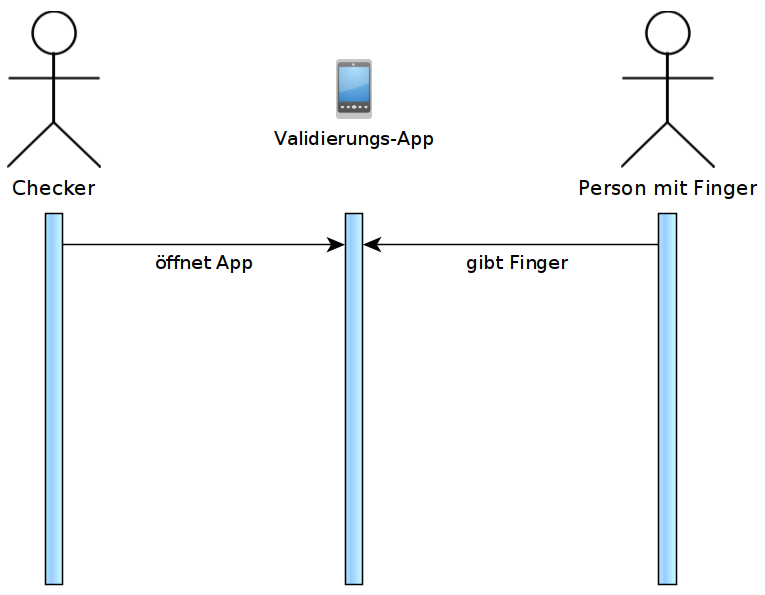
Kontrolle des Grünen Passes:

* Für die Kontrolle des Grünen Passes wird eine Internetverbindung und ein Fingerabdruckscanner benötigt, da ansonsten nicht auf die Daten zugegriffen werden kann. Bei jeder Person wird der Fingerabdruck gescannt und verschlüsselt zur Datenbank geschickt, wo dieser mit dem Private Key entschlüsselt wird und mit allen vorliegenden Fingerabdrücken verglichen wird. Falls der Fingerabdruck nicht vorhanden ist oder der Grüne Pass nicht mehr gültig ist schickt das System einen Response in dem der Einlass abgelehnt wird. Wird der Fingerabdruck gefunden und der grüne Pass ist gültig wird ein Response gesendet in dem der Einlass erlaubt wird.

Erhalt des Grünen Passes Analog:

* Es wird kein Analoger Pass benötigt, da der Grüne Pass über den Fingerabdruck kontrolliert wird und nicht über einen QR-Code, wie es beim aktuellen System der Fall ist.

Wie sieht das Sequenzdiagramm des neuen Systems aus?

Wie sieht das Architekturdiagramm des aktuellen Systems aus?

Welche Schwachstellen hat das neue System?

* Ohne Internetverbindung können die Daten nicht abgerufen werden und der Einlass nicht kontrolliert werden.
* Sollte der Private Key ausversehen geleakt werden, könnte man zwar keine neuen Zertifikate erstellen aber man könnte alle Fingerabdrücke in der Datenbank und jene die zur neuaufnahme/kontrolle an die Datenbank gesendet werden, entschlüsseln, speichern und viel schlechtes damit machen.

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

Nein, da der Fingerabdruck eines jeden Menschen einzigartig ist muss keine zusätzliche Überprüfung des Lichtbildausweises erfolgen da dieses im Prinzip „fürd Wurscht“ ist da der Fingerabdruck eindeutiger ist als der Lichtbildausweis.

Welche Apps werden für die Kontrolle des Grünen Passes benötigt?

* Einerseits würde für das eigene Hochladen des Fingerabdrucks und des Bescheids eine 0815 Angular Webseite benötigt werden, die auf allen Geräten läuft.
* Andererseits wird eine App benötigt die auf allen Geräten läuft, um den Grünen Pass zu kontrollieren.
* Es wird auch eine „Grüne Pass“ App benötigt um den Status/Gültigkeitsdauer einzusehen.

Welchen Kosten würden anfallen?

* Der Großteil der Kosten käme von der Webseite und der Smartphone App, für die auch gewartet werden müssen, aber wenn man überlegt das aktuell eine Validator-App (GreenCheck), die Grüne Pass App und eine Webseite laufen würden es durch die Umstellung günstiger werden das System zu betreiben.
* Ein weiterer Teil würde für die Datenbank und deren Betreibung und Wartung anfallen.
* Etwas das man vielleicht auch übernehmen müsste wären Fingerabdruck scanner zur Eingangskontrolle.

Wie steht es um den Datenschutz?

* Da im Endeffekt nur der Fingerabdruck gespeichert wird und dieser nicht (ohne weiteres) einfach zugeordnet werden kann und diese verschlüsselt in der Datenbank liegen gibt es keine größeren Bedenken. Auch da der gesamte Datenverkehr zwischen den Systemen verschlüsselt ist.
* Das einzige Bedenken, wie im Punkt Schwachstellen erwähnt, wäre falls jemand den Private Key in die Hände bekommt denn dann könnte diese Person alle Fingerabdrücke entschlüsseln und auch den Datenverkehr zwischen den Systemen und somit wären Fingerabdruckscanner, bei z.B. Tresoren oder Häusern.

Detaillierte Beschreibung des Systems:

Im Hintergrund des Systems läuft die Datenbank. Im Vordergrund sind die Webseite, die Validierungs-App, eine App die die Fingerabdruckscanns zur Datenbank schickt und eine App zum Anzeigen des Status des Grünen Pass. Nach der Impfung einer Person muss diese bei der Impfstelle eine Fingerabdruckscan machen bzw. mehrere, welche über die Webseite verschlüsselt zur Datenbank gesendet werden, welche dort auch verschlüsselt gespeichert werden. Ist jemand genesen und hat einen Bescheid kann dieser mit dem Fingerabdruck, den man selbst am PC oder Smartphone durchgeführt hat, verschlüsselt über die Webseite an die Datenbank geschickt. Wird eine Zutrittskontrolle durchgeführt muss ein internetfähiges Gerät mit Fingerabdrucksensor (Smartphone, Laptop, PC mit externem Fingerabdrucksensor, …) vorhanden sein. Es wird der Finger der Person gescannt und der Scan von der Validierungs-App an die Datenbank zum abgleichen gesendet, welche dann einen Response schickt ob die Person eintretten darf oder nicht.

Quellen:

<https://www.quarks.de/gesellschaft/wissenschaft/wie-einzigartig-ist-der-fingerabdruck/>

Quellen:

<https://speechcode.de/de/gruner-pass-qr-code-als-zertifikat-ungeeignet/> [16.02.2022]

<https://www.qrcode-generator.de/qr-code-marketing/qr-codes-basics/> [16.03.2022]

<https://epicenter.works/content/sicherheitsluecken-im-gruenen-pass-gefaehrden-gesundheitsdaten-aller-sozialversicherten> [16.03.2022]

<https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32021D1073&from=EN> [16.03.2022]