**Problemanalyse „Grüner Pass“**

**Einleitung**

Seit 2020 ist die Welt von der Covid-19-Pandemie betroffen. Im Zuge der Öffnungsschritte, welche vom Gesetzgeber durchgeführt wurden, kam es zur Einführung der sogenannten „G-Regeln“. Mit den „EU Digital COVID Certificates“ wurde eine einheitliche Lösung der EU-Mitgliedstaaten für dieses Problem geschaffen, um unter Anderem den Reiseverkehr bei den aktuell geltenden Regeln zu vereinfachen.

Mit den „EU Digital COVID Certificates“, bzw. in Österreich als „Grüner Pass“ bekannt, können

* Impfungen
* Genesungen oder
* Negative Testergebnisse

Im Zusammenhang mit SARS-CoV-2 dokumentiert werden. Jedes Zertifikat ist mit einem speziellen QR-Code versehen, mit welchem die Überprüfung der Zertifikate vorgenommen werden können.

In Österreich wird dieses System mit zwei einfach zu bedienenden Apps umgesetzt:

* Grüner Pass: Dient zur Speicherung von Zertifikaten
* GreenCheck: Dient zur schnellen und einfachen Überprüfung der Zertifikate (abhängig der geforderte G-Regel)

Jedoch hat dieses, im Eiltempo entwickeltes, System einige Schwachstellen, welche oft auf einfachem Wege ausgenützt werden können.

**QR-Code**

Inhalt

Der genaue Inhalt des QR-Codes ist abhängig vom Zertifikattyp. Folgende Daten sind in jedem Zertifikat enthalten:

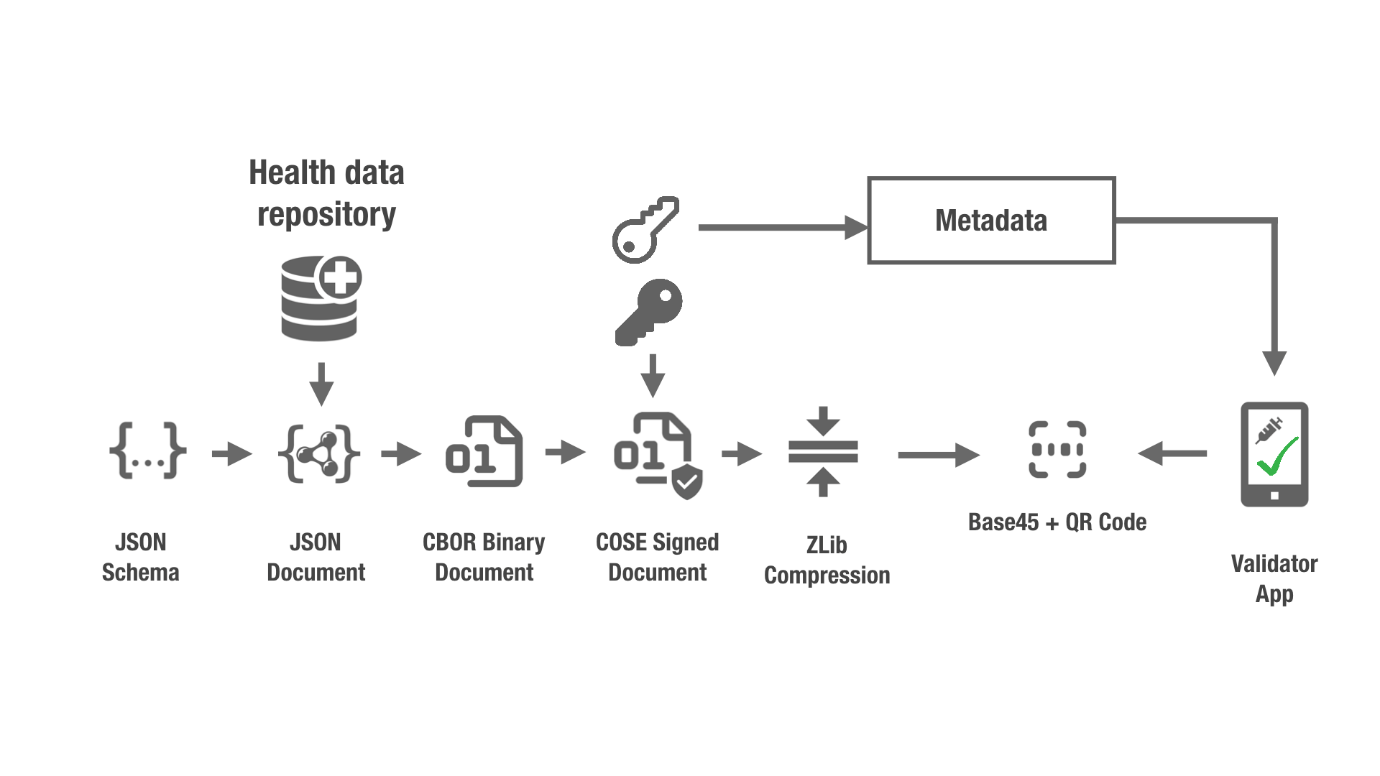
* Identität des Inhabers
  + Geburtsdatum
  + Vor- und Nachname
* Metadaten des Zertifikats
  + Austeller
  + Eindeutige Kennung
  + Datum der Generierung
  + Verfallsdatum

Abhängig vom Typ enthält das Zertifikat die spezifischen Daten:

* Impfzertifikat
  + Informationen über den Impfstoff (Hersteller, …)
  + Anzahl der verabreichten Dosen
  + Datum der letzten Impfung
* Genesungszertifikat
  + Informationen über frühere Infektionen des Inhabers nach einem positiven Testergebnis
* Testzertifikat
  + Informationen über die Art des Tests (z.B. Antigen oder PCR)
  + Datum der Testung
  + Ort der Testung

Generierung

Die folgende Grafik beschreibt übersichtsmäßig die Generierung des QR-Codes:



Die oben genannten Daten werden in ein JSON-Schema verpackt, welches fest von der EU vorgegeben wird:

Ein Bild, das Text enthält.

Automatisch generierte Beschreibung

Die genaue Spezifikation dieses Schemas ist öffentlich einsehbar.

Das entstandene JSON-Dokument wird nun schrittweise in verschiede Datenformate umgewandelt:

* CBOR (Concise Binary Object Representation)
* CWT (CBOR Web Token)
* COSE (Signatur)
* Compressed COSE (Base 45)

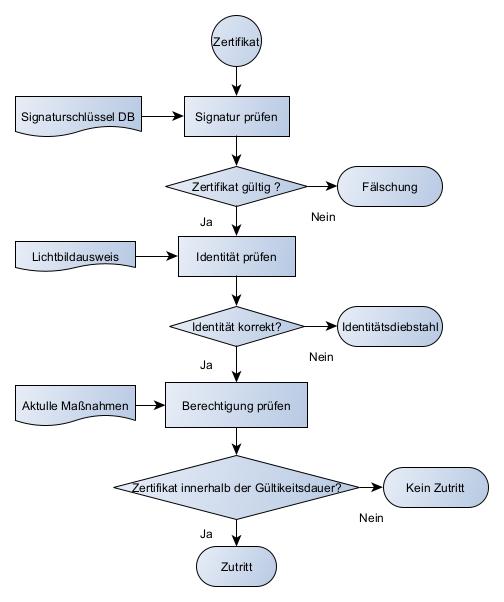
Schließlich wird aus dem entstandenen Code ein QR-Code erzeugt.

Verifizierung

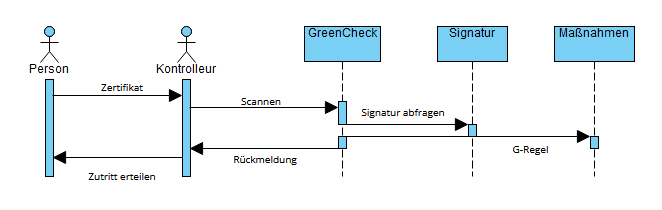
Eine Public-Key-Infrastruktur soll die zuverlässige und sichere Ausstellung und Überprüfung der Echtheit, Gültigkeit und Integrität der Zertifikate ermöglichen, um Betrug und Fälschungen aufzudecken. Dazu enthält das digitale COVID-Zertifikat eine elektronische Signatur. Jede ausstellende Stelle hat ihren eigenen digitalen Signaturschlüssel. Sämtliche Schlüssel sind EU-weit in einer Datenbank gespeichert. Die EU-Kommission hat eine Schnittstelle eingerichtet, über die alle Zertifikat-Signaturen überprüft werden können

**Funktionsweise des Systems**

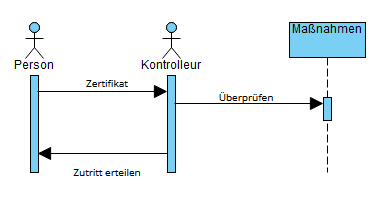
Architekturdiagramm



Sequenzdiagramm digital



Sequenzdiagramm analog



**Schwachstellen**

Digital

Die digitale Zugriffskontrolle hat nur wenige Schwachstellen, aber auch nur, wenn die Kontrolle sorgfältig und vollständig erfolgt. Bei einer vollständigen Kontrolle (mit Lichtbildausweis und GreenCheck) ist es einfacher, Fälschungen zu erkennen, weil bei diesem oft die Signatur fehlt. Wird jedoch nur kontrolliert, ob ein Code vorhanden ist (Sichtkontrolle z.B. in der Grüner Pass-App) wird eine Fälschung lange unerkannt bleiben. Hinzu kommt, das fast der gesamte technische Hintergrund öffentlich bekannt ist (bzw. sein muss). Auch der Datenschutz ist ein Problem, da er die schnelle und genaue Überprüfung erschwert (GreenCheck überprüft nicht das Impfregister)

Analog

Bei dem analogen Verfahren (ohne Internet) wird eine sichere Feststellung der Gültigkeit unmöglich, da weder eine Signatur noch ein Eintrag ins Impfregister überprüft werden können. Besonders der herkömmliche Impfpass ist ein beliebtes Schlupfloch, weil die Aufkleber des Impfstoffes legal gekauft werden können und auch der Stempel ist einfach zu fälschen.

Quellen:

<https://greencheck.gv.at/datenschutz>

<https://www.sozialministerium.at/Informationen-zum-Coronavirus/Coronavirus---Haeufig-gestellte-Fragen/FAQ-Gruener-Pass.html>

<https://de.wikipedia.org/wiki/Digitales_COVID-Zertifikat_der_EU>

<https://gir.st/blog/greenpass.html>

<https://github.com/ehn-dcc-development/hcert-spec>

<https://dgc.a-sit.at/ehn/>

<https://dgc.a-sit.at/ehn/testsuite>

<https://ec.europa.eu/health/system/files/2021-06/covid-certificate_json_specification_en_0.pdf>