HTBLA Grieskirchen

4710 Grieskirchen, Parzer Schulstraße 1

**Fachrichtung Informatik**

**Schuljahr 2021/2022**

**Pflichtenheft**

**Betreuer:**

Dipl.-Inf. Torsten Welsch

**Ausgeführt von:**

Jan Schwendtner, 4BHIF

Florian Nadler, 4BHIF

Fabian Fischer, 4BHIF

Sandro Greinecker, 4BHIF

**Grüner Pass**

Inhaltsverzeichnis

[1 Funktionsweise eures Systems 1](#_Toc99964178)

[1.1 Allgemein 1](#_Toc99964179)

[1.2 Vorteile 1](#_Toc99964180)

[1.3 Architekturdiagramm 1](#_Toc99964181)

[1.4 Sequenzdiagramm 1](#_Toc99964182)

[2 Umsetzungsschwierigkeiten/Schwachstellen 2](#_Toc99964183)

[2.1 Umsetzungsschwierigkeiten 2](#_Toc99964184)

[2.2 Schwachstellen/Nachteile 2](#_Toc99964185)

[3 Kosten und Datenschutz 2](#_Toc99964186)

[3.1 Kosten 2](#_Toc99964187)

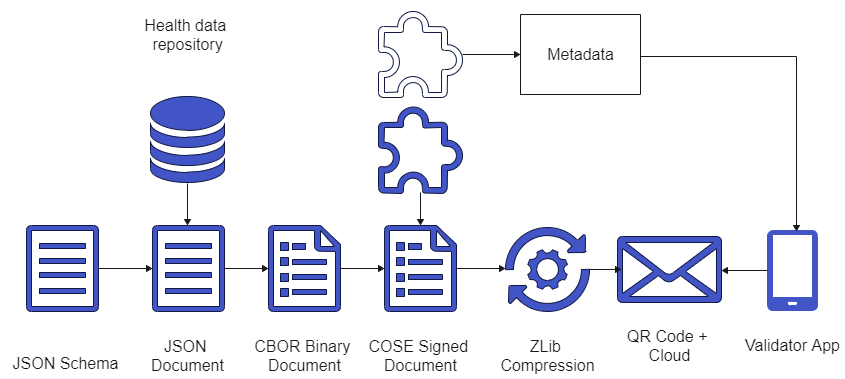
[3.2 Datenschutz 2](#_Toc99964188)

1. Funktionsweise eures Systems
   1. Allgemein

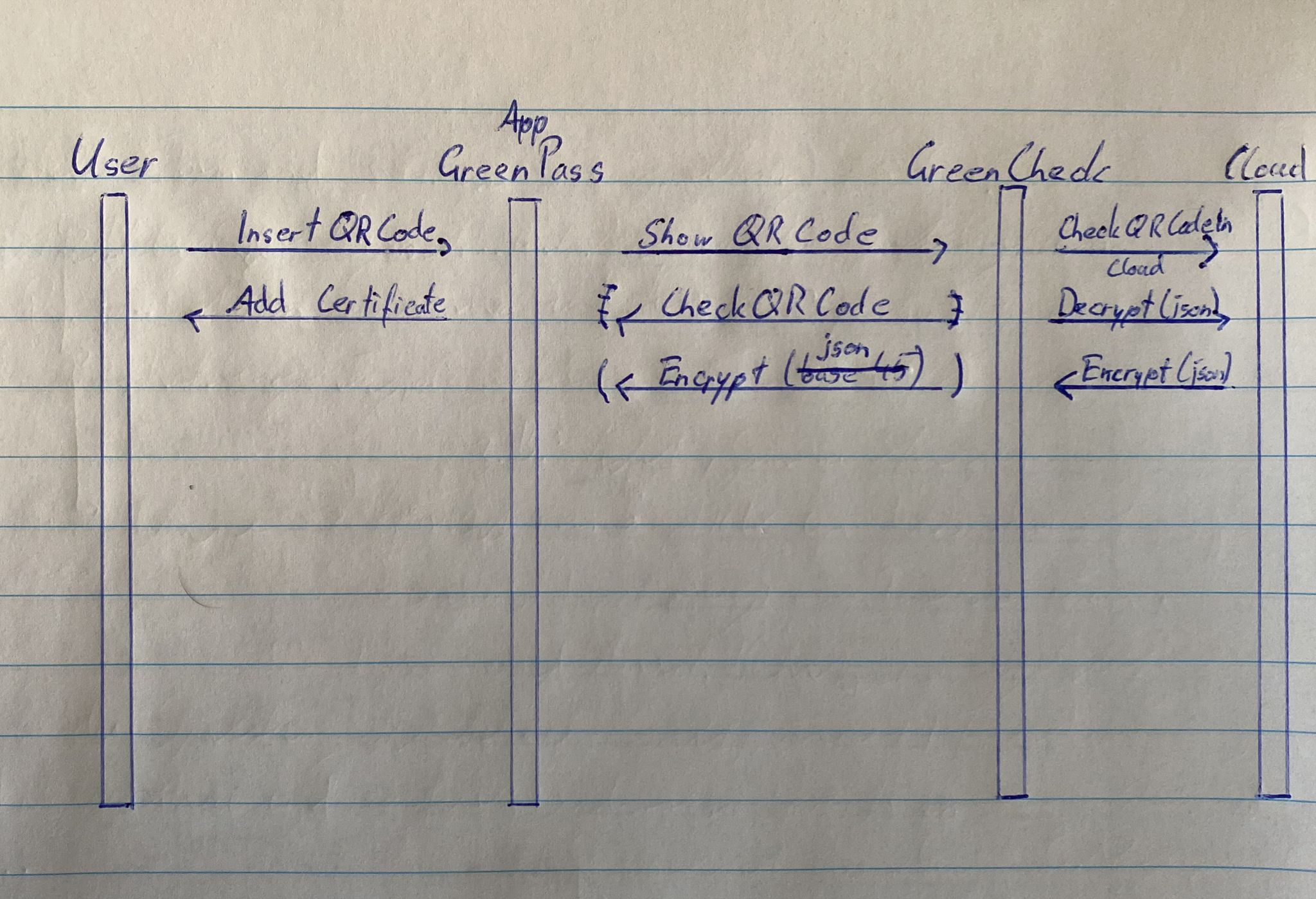
Speicherung der Zertifikate in einer Cloud, um zu überprüfen, ob Zertifikat tatsächlich gültig ist.

Bessere Verschlüsselung der json-Datei, da diese lediglich durch base45 verschlüsselt sind und somit leicht zu fälschen sind.

* 1. Vorteile
* Zertifikate fälschen fast nicht möglich der einzige Weg wäre, den Grünen Pass einer anderen Person zu nehmen und hoffen, dass die kontrollierende Person nicht einen Lichtbildausweis verlangt.
* Da die Zertifikate in der Cloud gespeichert sind kann man auch die Zertifikate löschen und die Personen benachrichtigen, dass das Zertifikat abgelaufen ist. Somit auch Sicherheit, dass Personen keine abgelaufenen Zertifikate verwenden.
* Zertifikate können auch ohne etwas neu einscannen zu müssen von außen verändert werden, falls z.B etwas falsch angegeben wurde kann man dies ganz leicht wieder ausbessern.
  1. Architekturdiagramm



* 1. Sequenzdiagramm



1. Umsetzungsschwierigkeiten/Schwachstellen
   1. Umsetzungsschwierigkeiten
   2. Schwachstellen/Nachteile

Mitarbeiter die Zugang zur Cloud haben könnten Daten ändern somit wieder erhöhte Korruption

Falls Cloud nicht erreichbar könnten die Nutzer ihre Zertifikate nicht abrufen -> Lösung wäre sozusagen ein offline Dokument noch auf dem Gerät zu speichern welches aber bei jeder Nutzung der App aktualisiert wird, falls Cloud erreichbar ist.

Notfalls könnten die Nutzer aber auch einfach selbst Initiative ergreifen und Screenshots machen.

1. Kosten und Datenschutz
   1. Kosten
   2. Datenschutz

Höchstens für Mitarbeiter wären die Daten einsehbar man könnte aber wirklich private Namen auch verschlüsseln, sodass die Mitarbeiter nur Datum und ähnliches der Zertifikate sehen können