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 sieght 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 laufen zwei Services: die Datenbank ein Backend für die Validierungs-App. 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/