Multipass

Inhalt, Apps und Datenschutz: So funktioniert das digitale Impfzertifikat

Das digitale Impfzertifikat ist da, und damit die Teilhabe an der neuen Normalität zum Greifen nahe: App starten, QR-Code zeigen und ab in den Urlaub. Im QR-Code des Zertifikats stecken jedoch mehr Daten, als zur Überprüfung der Gültigkeit notwendig sind.

Von Gerald Himmelein

Das digitale Impfzertifikat ist da und verspricht denjenigen, die schon durchgeimpft sind, neue, alte Freiheiten: Urlaubsflüge ohne Test und Quarantäne, Kinovergnügen und Konzertbesuche, Massenveranstaltungen. Und das ganz komfortabel per App, ohne vorher das gelbe Impfbuch aus der Tasche zu kramen. Wer das digitale Zertifikat auf dem Smartphone gespeichert hat, muss am Einlass nur kurz die App zücken und darf rein. Die dazugehörige Kontroll-App gibt es gratis, damit Geschäfte, Restaurants und Kinos den Impfstatus zuverlässig überprüfen können.

Zur gewissenhaften Kontrolle gehören auch Personalausweis oder Reisepass – um sicherzustellen, dass Person und Zertifikat zusammenpassen. Der Geimpfte speichert den QR-Code seines Zertifikats in einer App. Das Gegenüber scannt den Code zur Validierung mit einer Kontroll-App ein. Das Robert-Koch-Institut (RKI) verspricht, dass ihre CovPass-Check-App dabei nur die nötigsten Daten offenlegt: Vorname, Nachname und Geburtsdatum. Das ist korrekt, jedoch steckt in dem vorgezeigten QR-Code noch mehr. Doch dazu gleich mehr.

Seit dem 14. Juni ist das digitale Impfzertifikat offiziell verfügbar. Wer nach diesem Termin im Impfzentrum geimpft wurde, bekam das Zertifikat mit etwas Glück gleich ausgehändigt – letztlich handelt es sich dabei nur um ein faltbares DIN-A4-Blatt mit QR-Code. Früher beim Impfzentrum Geimpfte sollen das Zertifikat per Post erhalten, in Hamburg und Niedersachsen lässt es sich inzwischen auch online abrufen (siehe ct.de/ycxj).

Wer in einer Arztpraxis geimpft wurde, kann dort vorsprechen oder, zur Entlastung der Praxen, eine geeignete Apotheke aufsuchen. Der Deutsche Apothekerverband DAV hat seine Online-Apothekensuche hierfür um das Kriterium „Digitales Impfzertifikat“ erweitert. (siehe ct.de/ycxj). Benötigt werden lediglich ein aktueller Personalausweis sowie die Impfnachweise. Für Impflinge soll die Ausstellung des Zertifikats kostenlos bleiben. Apotheken bekamen pro Zertifikat vom Gesundheitsministerium zunächst 18 Euro, ab dem 1. Juli sind es nur noch 6 Euro. Bei einigen Impfzentren stehen auf den Bescheinigungen schon länger QR-Codes. Da diese jedoch nicht dem EU-Standard entsprechen, lassen sie sich nicht in die Apps einscannen.

Ein Zertifikat pro Impfung

Vollständig Geimpfte erhalten zwei digitale Zertifikate ausgehändigt, eines pro Impfung. Eine Ausnahme bilden nur die Empfänger des Impfstoffs von Johnson & Johnson: Hier reicht eine Impfdosis, demzufolge gibt es auch nur ein Zertifikat. Die QR-Codes können mit einer von drei Apps eingescannt und aufbewahrt werden: Die Corona-Warn-App (CWA) und der CovPass stammen beide vom RKI. Seit dem 18. Juni verarbeitet auch die Luca-App von Culture4Life das Zertifikat.

Die RKI-Apps kommen ohne Registrierung aus und lesen die QR-Codes beliebiger Personen ein. Ganz anders die Luca-App: Darin müssen sich Anwender zunächst mit Name, Anschrift und Telefonnummer ausweisen. Anschließend liest Luca einen digitalen Impfnachweis nur ein, wenn der Name, auf den er ausgestellt wurde, zum Namen des Luca-Nutzers passt. Ansonsten meldet die App

einen Fehler: „Das Dokument konnte nicht importiert werden. […] Bitte prüfe, ob dein Name richtig in der App hinterlegt ist.“ Das passiert auch, wenn man sich in der App nur mit dem ersten Vornamen angemeldet hat, das digitale Impfzertifikat aber auf den ersten und zweiten Vornamen ausgestellt wurde.

Wenig begrüßenswert ist das Einverständnis, das die Luca-App ihren Anwendern abfordert: Darin räumt sich der Anbieter das Recht ein, personenbezogene Daten „pseudonymisiert“ zu übermitteln. „Dies dient ausschließlich der Vorbeugung von Missbrauch, indem ein Dokument durch unterschiedliche Personen genutzt wird.“ Datensparsamkeit sieht anders aus. CovPass speichert auch die Impfdaten mehrerer Personen – das kann praktisch sein, um vor einer Reise beispielsweise die gesammelten QR-Codes der Familie zu speichern. Die CWA soll mit Version 2.5 in Kürze nachziehen.

„CovPass Check“, die App des RKI zur Überprüfung digitaler Impfzertifikate (siehe ct.de/ycxj), ist für Veranstalter, Gastwirte und andere Betriebe sowie öffentliche Einrichtungen gedacht. Ein Test der CovPass-Check-App mit den zum Ausprobieren eingeholten Zertifikaten des Autors führte zu kurzem Herzflattern: Alle Zertifikate, ob aus der App oder Papiervorlage, führten hartnäckig zur Fehlermeldung „Impfstatus nicht gültig“.

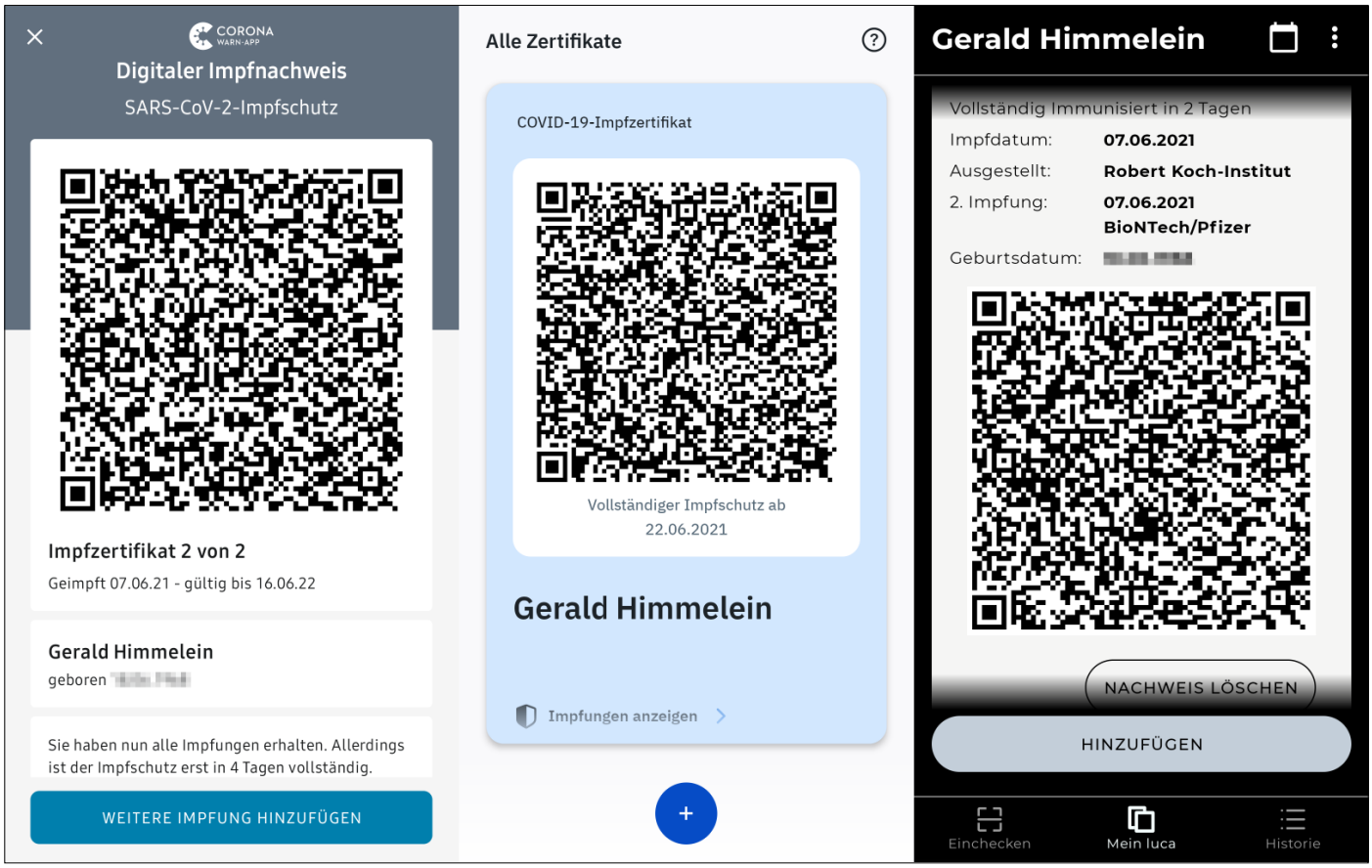
Zum Glück bedeutet die Meldung nur, dass der letzte Impftermin noch keine 14 Tage zurückliegt. Das RKI ist der Ansicht, dass der volle Impfschutz erst nach Ablauf dieser Karenzzeit gegeben ist. Ein tatsächlich ungültiges Zertifikat resultiert hingegen in der Fehlermeldung „Prüfung nicht erfolgreich“.

Die von den Apps angezeigten QR-Codes sind inhaltlich mit den Codes auf Papier identisch – im Fall des Autors handelt es sich sogar um 1:1-Kopien der Papiercodes. Ebenso wie die Vorbilder auf Papier enthalten die App-Codes alle Daten, die bei der Erstellung des Impfzertifikats erfasst wurden: darunter Datum und Dosis der Impfungen, alle Nachnamen, alle Vornamen und Geburtsdatum.

Dies mag den ein oder anderen überraschen, da im Vorfeld in mehreren Medien betont wurde, dass beim Überprüfen der Codes nur Impfstatus, Name und Geburtsdatum des Geimpften eine Rolle spielen. Ein Blick in die FAQ des RKI (siehe ct.de/ycxj) klärt das Missverständnis jedoch schnell auf: „Der QR-Code enthält dieselben Daten wie das Corona-Impfzertifikat. Bei der Überprüfung des QR-Codes mit der CovPass-Check-App werden jedoch nur die nötigsten Informationen angezeigt: Impfstatus, Name, Vorname und Geburtsdatum.“ Es ist also nur die CovPass-Check-App, die sich bei der Anzeige der Daten einschränkt.

Aufbau des QR-Codes

Der QR-Code des digitalen Impfzertifikats ist relativ komplex aufgebaut. Beim Scan des Codes mit einer regulären QR-Reader-App kommt nach dem Präfix „HC1:“ nur Buchstaben- und Zahlensalat heraus. Er enthält die JSON-formatierten Impfdaten, die gemäß RFC 7049 in eine kompaktere Binärdarstellung (Concise Binary Object Representation, CBOR) überführt und anschließend zlib-komprimiert und Base45-kodiert wurden. Im



Die Corona-Warn-App (links) zeigt den zweiten Impfnachweis zuerst an. Bei der CovPass-App (Mitte) und Luca (rechts) muss man sich zu den einzelnen Zertifikaten durchklicken, um sie zu betrachten.

Netz kursiert ein Python-Skript, das die im Zeichenwirrwarr transportierten Daten lesbar macht (siehe ct.de/ycxj):

```
import zlib, base45, cbor, pprint
print("Inhalt des QR-Codes?", end="")
pprint.pprint(
 cbor.loads(
  cbor.loads(
   zlib.decompress(
    base45.b45decode(
     input()[4:]))).value[2]))
```

Bei der Sichtung der Klartextdaten überraschte uns das Ablaufdatum in Form eines Unix-Zeitstempels, exakt ein Jahr nach dem Ausstellungsdatum – und unabhängig davon, wann die letzte Impfung erfolgt ist. Wer also bei der Impfung keinen QR-Code erhalten hat und sich mit dem Gang in die Apotheke Zeit lässt, dessen Impfnachweis ist mit einem entsprechend späteren Ablaufdatum versehen.

Gestatten: Maus, Micky Maus. Die Corona-Warn-App akzeptiert auch gefälschte Zertifikate. Das ist aber halb so schlimm.

Revozieren (widerrufen) lassen sich die Zertifikate aktuell nicht.

Die EU-Spezifikation für digitale Covid-Zertifikate (Version 1.30) sieht weitere Felder vor, etwa für Testergebnisse und Genesungsbescheinigungen (siehe ct.de/ycxj). Derzeit ist im deutschen Impfzertifikat jedoch nur kodiert, was unbedingt rein muss. Für von einer Covid-Infektion Genesene soll das digitale Zertifikat zum Erscheinen dieses Hefts freigeschaltet sein. Hierfür sind noch Anpassungen an EU-Gegebenheiten nötig. In Deutschland wird eine Infektion wie eine Erstimpfung gehandhabt: Wer Corona schon hinter sich hat, bekommt danach nur eine Dosis mRNA-Impfstoff. Andere EU-Staaten handhaben das anders; hier bekommen auch Genesene zwei Stiche.

Was das Skript nicht ausgibt, ist die im CBOR-Objekt enthaltene digitale Signatur des QR-Codes. Diese ist beim digitalen Impfzertifikat von zentraler Bedeutung, da sie sicherstellt, dass die im Zertifikat angegebenen Daten, etwa der Name, nicht unbemerkt geändert werden können. Die Aussteller nutzen einen privaten Schlüssel, um die Daten zu signieren. Und die Prüf-App zieht sich online die dazugehörigen Public Keys, um damit die Gültigkeit der Signatur zu überprüfen. Das ist auch der Grund dafür, dass CovPass Check zumindest von Zeit zu Zeit eine Internetverbindung benötigt, obwohl die Überprüfung der Signaturen grundsätzlich offline abläuft.

Eine Manipulation der Daten würde mit der Check-App sofort auffallen, da sich die digitale Signatur auf den Inhalt des Impfnachweises bezieht. Auch der Einsatz selbst erstellter und selbst signierter Zertifikate fliegt auf. Im Fall der Fälle meldet CovPass Check „Prüfung nicht erfolgreich“. Irritiert hat uns zunächst, dass die Apps für die Impflinge sehr unterschiedlich mit den Signaturen umgehen: Während die CovApp ungültige Impfnachweise verschmäht, konnten wir mit der Corona-Warn App ungehindert einen auf „Micky Maus“ ausgestellten QR-Code einlesen, den wir zu Testzwecken erzeugt hatten. Anschließend war der Test-Code wie ein gültiger Impfnachweis in der App hinterlegt.

Das ist jedoch nur auf den ersten Blick ein Problem. Denn der Kontrolleur muss den Code ohnehin mit CovPass Check scannen, um zu erfahren, ob er gültig ist. Und dabei fällt die falsche Signatur auf. Das erklärt auch, warum die EU-Spezifikation keine explizite Überprüfung der Signatur für sogenannte Wallet-Apps wie die CWA vorsieht. Das, was auf dem Smartphone-Display des Besuchers angezeigt wird, mag zwar augenscheinlich passen, es könnte sich aber genauso gut um einen manipulierten Screenshot der CWA handeln, in den ein anderer Name eingesetzt wurde. Eine bloße Sichtkontrolle reicht also nicht aus. Auf die Kontrolle von Personalausweis oder Reisepass lässt sich deshalb ebenso wenig verzichten.

Wozu das Ganze

Derzeit lassen sich die praktischen Einsatzzwecke des digitalen Impfzertifikats noch

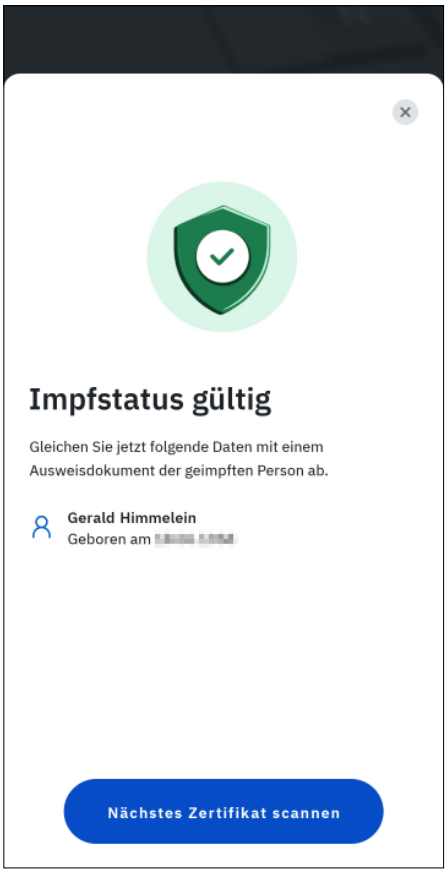
Beispieldatensatz eines digitalen Impfzertifikats

Feldname	Bedeutung	Beispielwert
dob	Geburtsdatum	1964-08-12
fn	Familienname(n)	Mustermann
fnt	Familienname(n) (Transliteration)	MUSTERMANN
gn	Vorname(n)	Erika
gnt	Vorname(n) (Transliteration)	ERIKA
ci	ID des Impfzertifikats	URN:UVCI:01DE/IZ12345A/5CWLU12RNOB9RXSEOP6FG8
co	Land der Impfung	DE
dn	Nummer der Impfdosis	2
dt	Datum der Impfdosis	2021-05-29
is	Zertifikatsaussteller	Robert Koch-Institut
ma	Impfstoffhersteller	ORG-100031184 (Moderna Biotech Spain S.L.)
mp	Impfstoff	EU/1/20/1507 (COVID-19 Vaccine Moderna)
sd	Gesamtzahl der Impfdosen	2
tg	Zielkrankheit	840539006 (COVID-19)
vp	Impfstoffart	1119349007 (SARS-CoV-2 mRNA vaccine)
ver	Version des Impfzertifikats	1.0.0
1	Land der Zertifikatsausstellung	DE
4	Ablaufdatum des Zertifikats	1655547702 (18. Juni 2022, 12:21:42)
6	Ausstellungsdatum des Zertifikats	1624011702 (18. Juni 2021, 12:21:42)

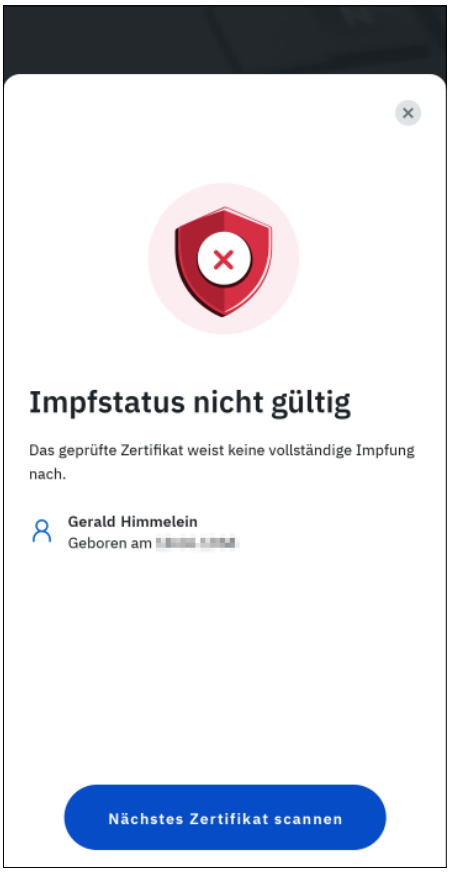
an einer Hand abzählen. Das Hauptziel der Early Adopters dürfte darin bestehen, es in Kombination mit einem Personalausweis oder Reisepass als Unbedenklichkeitsbescheinigung bei Reisen zu benutzen. Interessant ist das Zertifikat auch für Restaurants, Läden und öffentliche Einrichtungen – insbesondere, falls es wieder zu einem Lockdown kommt. Sollten vor dem Einlass wieder Test- und Impfnachweise nötig werden, lässt sich ein QR-Code auf dem Smartphone deutlich schneller verarbeiten als der gelbe Impfpass, der tief im Rucksack vergraben ist.

Und Veranstalter könnten Besuchern die Möglichkeit bieten, den Impfstatus schon vor einem Event online verifizieren zu lassen, um Schlangen im Einlassbereich zu vermeiden. Unter Umständen profitiert man schon jetzt von dem Impfnachweis: Wer etwa in Bayern eine Urlaubsunterkunft sucht, muss einen aktuellen Corona-Test vorlegen und diese während seines Aufenthalts alle 48 Stunden wiederholen. Davon ausgenommen sind neben Kindern bis 6 Jahre auch Genesene und vollständig Geimpfte – wer nachweisen kann, dass er dazugehört, erspart sich viele Tests.

Die im QR-Code gespeicherten Daten wecken natürlich Begehrlichkeiten. Und an dieser Stelle wird es dann vom Datenschutz her kitzelig: Zwar mag die offizielle CovPass-Check-App diskret mit den Daten umgehen und nur ein Minimum davon anzeigen. Doch das ist natürlich kein wirksamer Schutz vor Datenklau. Schon ein Foto des QR-Codes reicht aus, um die Daten zu einem späteren Zeitpunkt in Ruhe auswerten zu können.



Alles im grünen Bereich: Die App „CovPass Check“ überprüft die Gültigkeit der digitalen Impfnachweise, zum Beispiel bei einer Einlasskontrolle.



Keine Panik: Wenn die CovPass-Check-App „Impfstatus nicht gültig“ melden sollte, weist das eventuell nur darauf hin, dass die letzte Impfung weniger als 14 Tage zurückliegt (Impfschutz noch nicht vollständig).

Zumindest erwähnenswert ist in diesem Kontext, dass CovPass Check nicht verhindert, dass man während des Einlesens des QR-Codes einen Screenshot macht, auf dem der Code klar lesbar ist. Die Schweizer sind da vorsichtiger: Die App „COVID Certificate Check“ des Schweizer Bundesamts für Gesundheit blockiert während der Nutzung die Screenshot-Funktion des Smartphones.

Im Übrigen muss hinter einer dauerhaften Speicherung der Impfdaten nicht einmal böse Absicht stecken: Setzt ein Gastwirt versehentlich die für Impflinge gedachte CovPass-App ein statt das für ihn bestimmte CovPass Check, hat er am Ende des Tages ein schönes Sammelalbum mit Name, Geburtstag und Impfzertifikat jedes Gasts.

Technisch ist der gläserne Impfling derzeit nicht zu verhindern – zumindest nicht beim Einsatz der App. Wer fürchtet, dass seine Daten beim Scan des QR-Codes digital gespeichert werden, kann jedoch weiterhin das gelbe Heftchen mitführen, das als Impfnachweis ebenso gut taugt. *(rei@ct.de)* c't

Apothekenfinder, Apps & Spezifikationen: ct.de/ycxj

Bild: EU-Spezifikation „Digitales COVID-Zertifikat der EU“

In der EU-Spezifikation sind die Anforderungen an die digitalen Impfausweise („Digital Green Certificates“) und die daran beteiligte Infrastruktur umfassend dokumentiert, darunter auch die Verifikation samt Signaturcheck.