Dominik Schrahe, Thomas Städter

COVID-19-Impf- und -Testnachweise

Bewertung von Lösungen aus der Perspektive des Datenschutzes und der IT-Sicherheit

Mit Fortschreiten der COVID-19-Impfkampagnen und -Teststrategien rücken automatisierte Nachweissysteme in Form von Smartphone-Apps in den Fokus. Einige Systeme sind bereits im Einsatz oder befinden sich derzeit in Entwicklung. Der Beitrag stellt die Konzepte gegenüber und nimmt eine Bewertung aus der Perspektive des Datenschutzes und der IT-Sicherheit vor. Er zeigt auf, wie ein Mehr an Datenschutzfreundlichkeit bei gleicher Funktionalität erzielt werden kann.

1 Rückgabe von Freiheitsrechten durch COVID-19-Impfungen und -Tests

1.1 Motivation

Mit Beginn des Jahres 2021 sind weltweit COVID-19-Impfungen angelaufen. Sowohl von Virologen als auch von Politikern und der Wirtschaft werden die Impfkampagnen als große Hoffnung gesehen, ein Leben wie vor der Pandemie wiederherzustellen. Zugleich muss die Wirtschaft seit März 2020 und in vielen europäischen Staaten auch zu Beginn des Jahres 2021 durch anhaltende Lockdown-Regelungen erhebliche Umsatzeinbußen in Kauf nehmen. Viele Interessenverbände, unter anderem aus der Veranstaltungs- und Tourismusbranche, aber auch aus dem Einzelhandel, drängen daher auf schnelle Lockerungen. Erste Unternehmen aus der Veranstaltungsbranche [1] sowie der Luftfahrt [2] haben bereits zum Jahreswechsel angekündigt, zunächst nur nachweislich geimpften oder kürzlich negativ getesteten Personen den Zutritt zu ihren Veranstaltungen bzw. Flugzeugen zu gestatten.

Daraus ergibt sich aus Sicht der Wirtschaft mit Rücknahme der Lockdown-Regelungen die Frage, wie es Geimpften oder gerade negativ getesteten Personen ermöglicht werden kann, wieder am regulären gesellschaftlichen Leben teilzuhaben. Bei genauer Betrachtung des international gültigen gelben Impfausweises ergeben sich jedoch diverse Herausforderungen. So können diese Dokumente nicht als verlässlich erachtet werden, wie das Angebot gefälschter Ausweise im April zeigte [26]. Es ist aufgrund der Vielzahl – in vielen Fällen unleserlicher – Einträge schwer nachvollziehbar, ob die erforderlichen COVID-19-Impfungen vorschriftsgemäß im für den jeweiligen Impfstoff zulässigen zeitlichen Abstand durchgeführt wurden und der Impfausweis der Person gehört, die ihn vorlegt. Für den Nachweis eines negativen Testergebnisses gelten ähnliche Rahmenbedingungen. Israel verwendet daher einen elektronischen Impfnachweis via Smartphone-App; in Deutschland wird derzeit eine ähnliche Lösung entwickelt.

Trotz Impfungen ist davon auszugehen, dass die Infektionslage auch im Laufe des Jahres 2021 dynamisch bleiben wird und Gesundheitsbehörden auf regionaler Ebene Maßnahmen ergreifen werden. Neben der Kontaktnachverfolgung und Cluster-Erkennung ist somit eine aktuelle Datenlage zu Impfungen und Testergebnissen – zu allen Landkreisen und Städten in ganz Europa – unerlässlich für die weitere Bekämpfung der Pandemie. Die Erfahrungen im ersten Jahr der Pandemie zeigen, dass Daten zu Infektionen und Impfungen über nationale wie auch technische Systemgrenzen hinaus zur Verfügung stehen sollten.

1.2 Anforderungen an das Nachweissystem

Bürgerinnen und Bürgern sollte daher durch eine benutzerfreundliche und sichere technische Unterstützung schrittweise wieder die Wahrnehmung ihrer Rechte ermöglicht werden. Zugleich sollten Gesundheitsbehörden in ganz Europa in Echtzeit Zugriff auf Test- und Impfdaten haben, um weitere Maßnahmen

Dominik Schrahe

arbeitet als IT-Sicherheitsarchitekt bei der Versicherungskammer Bayern, an der FOM Hochschule für Oekonomie & Management beschäftigt er sich schwerpunktmäßig mit den Themen Informationssicherheit und Datenschutz.
E-Mail: dominik.schrahe@fom-net.de

Prof. Dr. Thomas Städter

lehrt Wirtschaftsinformatik an der FOM Hochschule für Oekonomie & Management, München. Schwerpunktmäßig beschäftigt er sich mit den Themen IT-Architekturen, IT-Sicherheitsmanagement und Datenschutz.
E-Mail: thomas.staedter@fom.de

zur Eindämmung der Pandemie kurzfristig und zielgerichtet umsetzen zu können. Als Anforderungen an ein umfassendes Nachweissystem wurden die folgenden aus der Literatur sowie der EU-DSGVO abgeleitet [3, 4, 5, 6]:

Tab. 1 | Anforderungen an ein Impf- und Test-Nachweis-System

Anforderung	Erläuterung
A-1	Vollzugriff für Patienten auf Impf-/Testdaten via eigenem Smartphone
A-2	Manipulationssicherer Nachweis der wirksam durchgeführten COVID-19-Impfungen
A-3	Manipulationssicherer Nachweis eines aktuellen negativen COVID-19-Testergebnisses
A-4	Benutzerfreundlicher Nachweis und Nachweisprüfung durch eine Smartphone-App
A-5	Kompatibilität zu anderen Systemen durch freien Datenzugriff oder offene Schnittstellen (z. B. SORMAS)
A-6	Datenschutzfreundlicher Nachweis durch Datenminimierung
A-7	Transparenz durch Nachvollziehbarkeit der erfolgten Nachweise
A-8	Interoperabilität über Staatsgrenzen hinaus, mindestens innerhalb der EU

Dagegen ist es nicht Ziel dieser Arbeit, die ethische Diskussion rund um die Gleichberechtigung zwischen geimpften und nicht geimpften Bürgerinnen und Bürgern zu führen. Auch wurde die Kontaktnachverfolgung ausgenommen. Hierfür werden in Deutschland neben der Corona-Warn-App mittlerweile neue Konzepte wie die Luca-App eingeführt, die ebenfalls wichtige Mittel in der Pandemiebekämpfung darstellen. Diese sind jedoch technisch anders gelagertes und daher separat zu betrachten.

2 Stand der Forschung und Lösungsansätze

2.1 Digitaler Impfausweis in Israel und Anforderungen des BMG in Deutschland

Ein App-basiertes Nachweissystem ausschließlich für COVID-19-Impfungen wird in Israel bereits seit Anfang des Jahres 2021 eingesetzt. Manipulationssicherheit und Datenschutz des dortigen Systems wurden jedoch mehrfach scharf kritisiert [7, 8]. Auch Deutschland hat im März 2021 angekündigt, einen elektronischen Impfnachweis entwickeln zu wollen. Dabei wurden durch das deutsche Bundesgesundheitsministerium Vorgaben definiert, die in Bezug auf die Sicherheit des Systems Fragen aufwerfen. So sollen Nachweise per Smartphone auch ohne Internetverbindung möglich sein [9]. Die Fälschungssicherheit des Impfnachweises muss somit auf lokalen Sicherheitsmechanismen der Smartphones von Geimpften basieren, da eine Validierung über einen vertrauenswürdigen Dritten offline nicht möglich ist. In Anbetracht der Verzögerungen bei Auslieferungen von Betriebssystem-Sicherheitsupdates bei Smartphones [10] scheint ein ausschließlicher Rückgriff auf lokale Sicherheitsmechanismen unzureichend. Doch selbst wenn Smartphones grundsätzlich als sichere Plattform betrachtet werden könnten, stellt sich die Frage, ob dem Gerät des Nachweisenden vertraut werden sollte, der ein Interesse an einer Manipulation haben könnte. Sofern zukünftig die Teilnahme an gesellschaftlichen Ereignissen nur mit Nachweis möglich sein sollte, sind wenigstens Versuche zur Fälschung eines Nachweises wahrscheinlich. Die gleiche Herausforderung ergibt sich mit herkömmlichen papierbasierten Nachweisen, die ebenfalls weiterhin gültig bleiben sollen [11]. Neben der Offline-Nachweis-Funktionalität soll die App jedoch auch eine Online-Nachweis-Funktion besitzen.

2.2 Umsetzung des Impfnachweises in Deutschland

Mit der Implementierung der Nachweis-App sowie einer separaten Kontroll-App und dem Backend-System wurde ein Zusammenschluss aus dem Startup Ubirch und der IBM beauftragt [12]. Da weder Code noch Konzept bisher veröffentlicht wurden, kann eine formale Sicherheitsanalyse noch nicht durchgeführt werden. Die aus den Presseveröffentlichungen übereinstimmend hervorgehenden Informationen zeigen das Umsetzungsdesign aber klar auf. Während der zweiten Impfung soll durch das Impfzentrum bzw. den Hausarzt ein Impfzertifikat ausgestellt werden, welches dem Patienten in Form eines QR-Codes – in der Regel auf einer Plastikkarte aufgedruckt – übergeben wird [13]. Dieser QR-Code enthält personenbezogene Daten wie Namen, Impfdatum, Impfstoff sowie einen Zufallswert [12]. Ein Hashwert derselben Daten wird darüber hinaus in Blockchains der Genossenschaft Govdigital abgelegt [14]. Als Nachweis gegenüber einem Dritten kann entweder der QR-Code auf der Plastikkarte verwendet werden oder die Nachweis-App, in die der QR-Code eingelesen wird. Das digitale Äquivalent zeigt jedoch ebenfalls nur die im QR-Code enthaltenen Daten sowie den QR-Code selbst an. Der Nachweis gelingt durch das Abscannen dieser Daten. Dabei werden dem Smartphone des Prüfers – in der Regel dürfte es sich dabei um einen unbekannten Dritten handeln – die Impfdaten inklusive Namen im Klartext übergeben. Das Smartphone des Prüfers berechnet aus diesen Daten dann erneut einen Hashwert und kann diesen mit dem auf der Blockchain gespeicherten Hashwert abgleichen [12].

Die skizzierte Vorgehensweise erfüllt somit die Anforderungen an einen fälschungssicheren Impfnachweis. Zwar könnten QR-Codes manipuliert werden, wie dies auch bereits in Israel erfolgreich durchgeführt wurde [8], dies würde jedoch bei der Kontrolle auffallen: entweder durch eine fehlerhafte Personenzuordnung oder durch den Misserfolg beim Abgleich der übermittelten Daten mit dem Hashwert auf der Blockchain. Angriffsmöglichkeiten ergeben sich bei einer Kontrolle ohne Internetverbindung, da hierbei nicht garantiert werden kann, dass eine Manipulation in der Personenzuordnung oder ein vollständig erfundener Impfdatensatz auffallen würde. Auch ist das System auf eine manuelle Kontrolle des Personalausweises angewiesen.

Unter Berücksichtigung der Datenminimierung (Art. 5 Abs. 1 EU-DSGVO), aber auch einer Umsetzung nach Stand der Technik, wie etwa in Art. 32 EU-DSGVO gefordert, ist dieses Vorgehen zu hinterfragen. Es ist davon auszugehen, dass mit der Impfnachweis-App ein De-Facto-Standard in Deutschland geschaffen wird, für den es für viele Bürgerinnen und Bürger – etwa bei der Nutzung des ÖPNV oder beim Grenzübertritt – keine Alternative geben wird. Gerade aus diesem Grund, sollte eine datenschutzfreundliche Umsetzung gewählt werden. Im Gegensatz dazu könnte das in Implementierung befindliche System ohne weitere Anpassungen zu einem praktischen Zwang zur regelmäßigen Weitergabe personenbezogener Daten führen. Transparenzfunktionen, die nachvollziehbar machen, an wen und zu welchem

Zweck eine Datenweitergabe erfolgt ist, fehlen ebenfalls. Datenschutzfreundlich wirkt sich zwar aus, dass die Impfdaten nicht im Klartext online übertragen werden [14], der Privacy-by-Design-Grundsatz der EU-DSGVO nach Art. 25 kann bei einer Klartextübermittlung der Impfdaten an das Smartphone des Prüfers dennoch nicht als umgesetzt betrachtet werden. So könnte die Abfrage eines Impfnachweises zukünftig auch vorgeschoben werden, um personenbezogene Daten von Kunden systematisch zu erfassen, den Betroffenen Kunden gegenüber wäre ein abweichender Zweck nicht ersichtlich. Gerade bei Verwendung der Blockchain-Technologie, die regelmäßig im Zusammenhang mit Pseudonymität, Anonymität und Zero-Knowledge-Proofs diskutiert wird, scheint hier weder die am Markt verfügbare Bestleistung[1] umgesetzt zu werden, noch das mildeste Mittel gewählt worden zu sein.

Auch die verwendete Technik wirft Fragen auf. Zwar wurden zunächst aufgetretene Sicherheitslücken mittlerweile nach Angabe des Herstellers behoben [15], doch bleibt offen, welchen Zweck die Blockchain erfüllt [16]. Die Distributed-Ledger-Technologie bietet insbesondere dann Vorteile, wenn Transaktionen zwischen mehreren Akteuren erfolgen, die sich gegenseitig nicht vertrauen und keine zentrale Vertrauensinstanz besteht. Im vorliegenden Fall sollen jedoch aus Redundanzgründen fünf Blockchains von einem einzigen Betreiber bereitgestellt werden [12], dem somit zwangsläufig vertraut werden muss. Der verbleibende Sinn in der Verwendung der Distributed-Ledger-Technologie im Vergleich zu einer relationalen Datenbank liegt somit im zusätzlichen Zeitstempel, der im Rahmen des Mining-Verfahrens jedem Datensatz zugeordnet werden kann [15]. Auch die Kompatibilität zu Impfnachweissystemen in ganz Europa wurde zwar als grundlegende Anforderung kommuniziert, mittlerweile sind jedoch auch hier Zweifel an der Umsetzung aufgekommen [17].

2.3 Anforderungen der Europäischen Union

Mitte März 2021 stellte auch die EU ihre Rahmenvorgaben für ein Nachweissystem vor. Dabei geht es weniger um die konkrete technische Ausgestaltung eines neuen Systems als um die Vorgabe eines verbindlichen Rahmens für alle europäischen Staaten durch eine EU-Verordnung, insbesondere um Grenzüberschreitende Reisen zu ermöglichen. Im Gegensatz zur in Deutschland angedachten Lösung sollen hier neben Impfungen explizit auch Testergebnisse berücksichtigt werden [3]. Auch technisch erlaubt die EU andere Wege als das deutsche Vorgehen. So ist die Verwendung einer Blockchain nicht angedacht. Der Wahrung der Integrität und Authentizität wird zwar eine große Bedeutung eingeräumt; diese Schutzziele können jedoch auch mittels elektronischer Signaturen sichergestellt werden. Diese werden bei Ausstellung des Zertifikats etwa durch Testzentren oder Krankenhäuser erstellt. Für die Zertifikatsprüfung soll keine Speicherung der Daten des Zertifikats in einem anderen als dem ausstellenden Land erfolgen. Eine Übermittlung der Impf- bzw. Testdaten im Klartext ist jedoch auch hier erforderlich [18, 19]. Neben der digitalen Fassung sieht auch die EU immer einen papierbasierten Barcode vor. Datenschutz und Interoperabilität werden im Entwurf der EU-Verordnung als Schlüssel zum Erfolg beschrieben, weshalb während der Verifikation nur die nötigsten Daten herausgegeben werden sollen und die EU sich auch um eine Kompatibilität zu Nachweissystemen außerhalb Europas bemühen möchte [3]. Der Europäische Datenschutzbeauftragte kritisiert dennoch mangelnde Klarheit bei Transparenzpflichten und Verantwortlichkeiten sowie eine mögliche zentrale Haltung personenbezogener Impf- und Testdaten [20].

3 Optimierung bestehender Ansätze

3.1 Gap-Analyse

Für die Praxis ergeben sich darüber hinaus weitere Herausforderungen. So decken alle realisierten oder in Realisierung befindlichen Nachweis-Apps bisher lediglich den Teilbereich des Impfens ab, wobei aktuelle Strategien der Gesundheitsbehörden sowie der Wirtschaft besonders auf negative Testergebnisse setzen [21]. Eine Nachweis-App sollte daher neben Impf- auch aktuelle Testnachweise verwalten können. Die Unterscheidung zwischen einer Nachweis- und einer Kontroll-App, wobei letztere nur z. B. Veranstaltern ausgegeben werden soll [14], ist in diesem Zusammenhang ebenfalls eher kurz gedacht. Stattdessen könnte die Nachweis-App auch eine Kontroll-Funktion besitzen, sodass Nachweise auch unkompliziert im privaten Umfeld ermöglicht werden.

Tab. 2 | Gegenüberstellung israelische „Green Card", geplante deutsche Impfnachweis-App sowie EU-Anforderungen an das „Green Certificate"

Anforderung	„Green Card" (Israel)	Impfnachweis-App (Deutschland)*	EU „Green Certificate"**
A-1: Patientenzugriff	✓/✗ Keine Testergebnisse	✓/✗ Keine Testergebnisse	✓
A-2: Impfnachweis	✗ manipulierbar	✓	✓
A-3: Testnachweis	✗ Keine Testergebnisse	✗ Keine Testergebnisse	✓
A-4: Benutzerfreundliche App	✓	✓	✓
A-5: Datenzugriff und Schnittstellen	✗ nicht vorgesehen	✗ nicht vorgesehen	✗ nicht vorgesehen
A-6: Datenminimierung	✗ EU-DSGVO nicht anwendbar	✓/✗ Nachweisdaten im Klartext	✓/✗ Nachweisdaten im Klartext
A-7: Transparenz	✗ nicht vorgesehen	✗ nicht vorgesehen	✗ nicht vorgesehen
A-8: Interoperabilität EU	✗	✓	✓

*) Nach Presseveröffentlichungen vom 15.04.2021 soll die deutsche Umsetzung an das europäische Green Certificate angeglichen werden. Eine Integration in die Corona Warn App wird angestrebt.

**) Das Green Certificate der EU soll via Verordnung beschlossen und durch alle EU-Staaten einzeln umgesetzt werden. Technische Details sind aus dem Gesetzestext daher nur vage ableitbar [3].

Der Ansatz der Europäischen Union für ein nationenübergreifendes Nachweissystem ist als durchweg positiv zu betrachten. Von zentraler Bedeutung sind auch die seitens der EU inkludierten Testnachweise. Dennoch muss festgestellt werden, dass alle betrachteten Systeme weder die Zurverfügungstellung der Test- und Impfdaten für das weitere Pandemiemanagement noch eine Transparenz im Sinne des Datenschutzes berücksichtigen. Letzteres wiegt besonders schwer, da die Lösungen zur Nachweisvalidierung jeweils sensible Gesundheitsdaten im Klartext an den Prüfer übermitteln. Die Literaturrecherche ergab, dass die An-

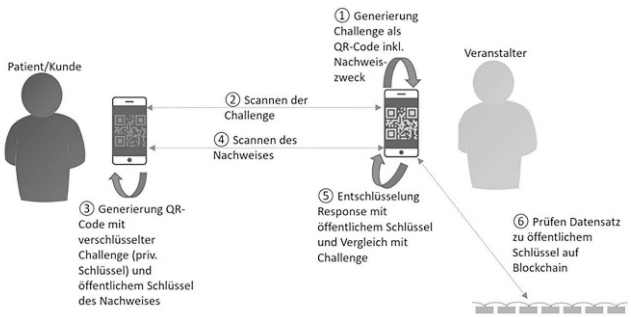
1 Der Stand der Technik, dessen Einhaltung u. a. auch von der DSGVO gefordert wird, ist als die am Markt verfügbare Bestleistung definiert (vgl. BVerfG, Beschluss vom 8. August 1978 – 2 BvL 8/77).

forderungen mit Stand April 2021 durch keine Lösung vollständig umgesetzt werden können. Ein von Wissenschaftlern entwickeltes Konzept, welches sich den Anforderungen annähert, jedoch ebenfalls stark auf Sicherheitsmechanismen mobiler Endgeräte setzt, wurde im März 2021 veröffentlicht [6]. Daher wird im Folgenden ein neuartiger Ansatz beschrieben.

3.2 Verbesserungsvorschläge

Um die genannten Problemfelder zu adressieren muss eine grundsätzlich andere Architektur gewählt werden, bei der Impf- und Testdatensätze als öffentlich verfügbare Daten, jedoch ohne Personenbezug gespeichert werden. Eine Wiederherstellung des Personenbezugs darf nur mittels durch Patienten verwaltete Identitäten möglich sein. Bei der Realisierung kann das Konzept der Self Sovereign Identitity (SSI) unterstützen. Während bei herkömmlichen elektronischen Identitäten (z. B. elektronischen Zertifikaten) während des Authentifizierungsvorgangs neben dem Besitzer und dem Prüfer der Identität auch der Aussteller des Zertifikates einbezogen wird, erfolgt die Validierung hier vergleichbar mit der analogen Welt. Dabei reicht die Prüfung eines Personalausweises durch den Prüfer aus. Die SSI-Technologie bildet dieses Vorgehen unter Verwendung der Distributed-Ledger-Technologie sowie eines kryptographischen Challenge-Response-Verfahrens auf die digitale Welt ab [23, 24]. In Anlehnung daran kann durch Patientenverwaltete Identitäten – nachgewiesen durch den Besitz eines privaten, nur auf dem Smartphone des Patienten gespeicherten Schlüssels – die Verbindung zu öffentlichen Impf- und Testdatensätzen hergestellt werden. Zum Zeitpunkt der Impfung oder des Tests muss sich der Patient mit einem Ausweisdokument authentifizieren und generiert ein ausschließlich für diesen Vorgang gültiges kryptographisches Schlüsselpaar. Nur der öffentliche Schlüssel wird per QR-Code an das Impf- bzw. Testzentrum übergeben. Das Impf- bzw. Testzentrum schreibt daraufhin durch das Auslösen einer Transaktion einen pseudonymen Datensatz mit der Impfbestätigung bzw. dem Testergebnis auf eine Blockchain.

Abb. 1 | Pseudonymer Nachweisvorgang nach den Verbesserungsvorschlägen



Hierbei handelt es sich um einen sogenannten *Public Permissioned Ledger*, der grundsätzlich öffentlich ist, wobei schreibende Zugriffe nur durch Gesundheitsbehörden möglich sind.

Zur Validierung eines Impf- bzw. Testnachweises sind zwei QR-Code-Scanvorgänge erforderlich. Im ersten Schritt muss der Nachweisempfänger dem Nachweisgeber (zuvor Patient) eine dynamisch generierte kryptographische Challenge zusammen mit dem Zweck des Nachweises als QR-Code übermitteln. Daraus berechnet das Smartphone des Nachweisgebers automatisch eine kryptographische Response, die mitsamt dem öffentlichen Schlüssel ebenfalls via QR-Code übergeben wird.

Der Zweck des Nachweises wird zusammen mit einem Zeitstempel auf dem Smartphone des Nachweisgebers gespeichert, sodass dieser nachvollziehen kann, wann zu welchem Zweck Nachweise übergeben wurden. Der Nachweisempfänger kann durch Prüfen der kryptographischen Response sowie Abfragen des entsprechenden öffentlichen Impf- bzw. Testdatensatzes den Nachweis verifizieren. Das Vorgehen kann Abb. 1 entnommen werden, wobei die Schritte 1, 3, 5 und 6 automatisiert ausgeführt werden.

Im Vergleich zu den bestehenden Konzepten ergeben sich dabei mehrere Vorteile:

- Während des Nachweisvorgangs werden lediglich Pseudonyme ausgetauscht.
- Es erfolgt keine Übertragung von Klartext-Daten an fremde – möglicherweise unsichere – Smartphones.
- Die Herausgabe von Impf- und Testnachweisen unterliegt Selbstbestimmtheit und Transparenz.
- Die bessere Verfügbarkeit von Impf- und Testdaten sorgt für schnellere Meldewege.
- Die Prüfung ist automatisierbar, da kein manueller Abgleich mit dem Personalausweis erforderlich ist.

3.3 Kritische Würdigung

Bei der vorgestellten Lösung fällt auf, dass diese im Gegensatz zu den heute verwendeten oder in Planung befindlichen Nachweissystemen zwei QR-Code-Scans benötigt; dies ist u. a. für den Nachweis der pseudonymen Identität erforderlich. Hierdurch entsteht ein zusätzlicher Aufwand bei der Prüfung, sowohl auf Seiten des Prüfers als auch auf Seiten des Geprüften. Ein einseitiger Scan wird jedoch nie zuverlässig eine Transparenz über die Zwecke eines Nachweises gewährleisten können, was in Kombination mit der Übergabe von Gesundheitsdaten im Klartext problematisch ist. Ein doppelseitiger QR-Code-Scan ist daher zu bevorzugen.

Die Selbstverwaltung der pseudonymen Identitäten geht mit einer erhöhten Eigenverantwortung auf Seiten der Patienten einher. Teilnehmen können an dem System nur Personen, die bereits vor Durchführung der Impfung bzw. Testung die Nachweis-App installiert haben. Bei Verlust des Smartphones können darüber hinaus keine weiteren Nachweise generiert werden. Hier ist die Benutzerfreundlichkeit gegenüber alternativen Systemen gemindert. Zur Lösung wäre eine Erweiterung um eine – ggf. automatisierte – kryptographisch gesicherte Backup-Funktion denkbar. Eine benutzerfreundliche Realisierung ist etwa durch den Messenger Threema mit dem sogenannten Threema-Safe implementiert; weitere Ansätze befinden sich in der Entwicklung [25]. Auch aus der Nachweisprüfung ergibt sich eine höhere Komplexität, da im beschriebenen Ansatz immer eine Internetverbindung erforderlich ist. Da eine solche jedoch nur auf Seiten des Prüfers benötigt wird, das zu übertragende Datenvolumen minimal ist und hierdurch die Manipulationssicherheit des Nachweises deutlich gesteigert wird, ist dies als geringe Einschränkung im Komfort zugunsten eines deutlichen Sicherheitsgewinns akzeptabel.

Einen besonderen Mehrwert soll das vorgestellte System zudem dadurch erbringen, dass alle anonymisierten Impf- und Testdaten frei verfügbar sind. Hier ist auch mit Blick auf zukünftige Entwicklungen kritisch zu hinterfragen, ob ein Personenbezug auch mittels Zusatzinformationen nicht wiederherstellbar ist. Bei Beschränkung auf die erforderlichen Daten wie Zeitstempel,

Ort, Impfstoff bzw. Art des Tests und Testergebnis und der Generierung eines neuen patientenseitig verwalteten Pseudonyms pro Impf- bzw. Testvorgang kann jedoch davon ausgegangen werden, dass eine Wiederherstellung des Personenbezugs nur mit unverhältnismäßig hohem Aufwand möglich wäre. Dagegen steht der Vorteil, dass z. B. Meldewege über Neuinfektionen und Impfungen je Landkreis beschleunigt werden können.

4 Fazit

Deutschland und die EU bereiten sich derzeit darauf vor, Impfungen mittels Apps nachweisbar zu machen. Nachweise für negative COVID-19-Testergebnisse werden dabei bisher nicht vollständig mitberücksichtigt. Die aktuellen Entwicklungen sind sehr dynamisch, derzeit bestehen Tendenzen einer Angleichung der deutschen Impfnachweis-App an das Europäische Green-Certificate [22]. Unter funktionalen Gesichtspunkten sind die im Aufbau befindlichen Systeme als solide zu bewerten. Dennoch ergeben sich Herausforderungen aus Sicht des Datenschutzes, da alle bekannten Nachweissysteme Gesundheitsdaten im Klartext übertragen und keinerlei Transparenz darüber bieten, wie diese auf Seiten des Empfängers weiterverarbeitet werden. Das vorgestellte Konzept zeigt auf, dass fälschungssichere Nachweise auch datenschutzfreundlicher möglich sind, indem diese pseudonym erfolgen, wobei nur die im datenschutzrechtlichen Sinne betroffene Person selbst eine Zuordnung des Datensatzes vornehmen kann. Dabei kommt den Patienten eine höhere Verantwortung zu, da diese ihre elektronischen Identitäten selbst verwalten müssen. Zwar wird das Nachweissystem hierdurch nicht einfacher, jedoch ergeben sich neben dem verbesserten Datenschutz weitere Vorteile wie Automatisierbarkeit des Nachweises und Erhöhung der Verfügbarkeit von Impf- und Testdaten, um das Management von Maßnahmen gegen die Pandemie zu verbessern und feingranularer steuern zu können. Derzeit handelt es sich bei dem beschriebenen Ansatz um ein erstes Konzept. Weiterer Forschungsbedarf besteht in der konkreten Umsetzung und der weiteren Erhöhung der Benutzerfreundlichkeit.

Literatur

[1] Decker, M. (2021). Veranstaltungen nur für Geimpfte? Lambrecht hat keine grundsätzlichen Einwände. https://www.rnd.de/politik/eventim-will-veranstaltungen-nur-fur-geimpfte-moglich-machen-lambrecht-spd-nicht-dagegen-LT5UHYLSBVCU3I43AQWHNGWOR4.html. Zugriff 14.03.2021.

[2] Alberti, I. (2020). Lufthansa: Langstrecke künftig wohl nur mit Corona-Test oder Impfnachweis. https://www.fnp.de/hessen/corona-lufthansa-verpflichtend-test-schnelltest-quarantaene-impfung-reisen-zr-90152935.html. Zugriff 14.03.2021.

[3] European Commission (2021). Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on a framework for the issuance, verification and acceptance of interoperable certificates on vaccination, testing and recovery to facilitate free movement during the COVID-19 pandemic (Digital Green Certificate). Brüssel.

[4] The Royal Society (2021). Twelve criteria for the development and use of COVID-19 vaccine passports. London.

[5] World Health Organization (2020). Smart Vaccination Certificate Working Group. https://www.who.int/groups/smart-vaccination-certificate-working-group. Zugriff 04.04.2021.

[6] Politis, I., Xenakis, C., Master, A. u.a. (2021). On an innovative architecture for digital immunity passports and vaccination certificates. arXiv preprint 2103.04142.

[7] Bar-Zik, R. (2021). Israel Rolls Out 'Green Passport' for Vaccinated. It's a Security Disaster. https://www.haaretz.com/israel-news/tech-news/.premium-israel-s-digital-green-pass-is-a-security-disaster-1.9582485. Zugriff 14.03.2021.

[8] Ziv, A. (2021). Anyone Can Fake Israel's Vaccination Certificate - Here's How Easy It Is. https://www.haaretz.com/israel-news/tech-news/.premium-anyone-can-fake-israel-s-vaccination-certificate-here-s-how-1.9537465. Zugriff 14.03.2021.

[9] Petereit, D. (2012). Blockchain gegen Corona: Digitaler Impfpass kommt von Kölner Startup Ubirch und IBM. https://t3n.de/news/corona-blockchain-digitaler-impfpass-1364737/. Zugriff 10.03.2021.

[10] Bíró, R., Zeisberg, S., Lell, J. u.a. (2019). The Android patch ecosystem – Still fragmented, but improving. https://srlabs.de/bites/android-patch-gap-2020/. Zugriff 14.03.2021.

[11] Bundesministerium für Gesundheit (2021). Fragen und Antworten zum digitalen Impfnachweis. https://www.bundesgesundheitsministerium.de/coronavirus/faq-covid-19-impfung/faq-digitaler-impfnachweis.html. Zugriff 14.03.2021.

[12] Beuth, P. (2021). Ubirch und IBM erhalten Zuschlag für deutschen digitalen Impfnachweis. https://www.spiegel.de/netzwelt/gadgets/ubirch-und-ibm-erhalten-zuschlag-fuer-deutschen-digitalen-impfnachweis-a-9f26439b-8fd8-4118-9221-eb8844946c69. Zugriff 10.03.2021.

[13] Ubirch (2021). Digitaler Impfnachweis. https://ubirch.de/fileadmin/Dokumente/Download-Doku/UBIRCH_Flyer_Digitaler_Impfnachweis_02.pdf. Zugriff: 12.03.2021..

[14] Fuest, B. (2021). Der Impfpass kommt von einem Startup aus Köln. https://www.businessinsider.de/gruenderszene/health/corona-digitaler-impfpass-ubirch/. Zugriff 10.03.2021.

[15] Böck, H. (2021). Blockchain-Impfausweis mit Schwächen. https://www.golem.de/news/ubirch-blockchain-impfausweis-mit-schwaechen-2102-153909.html. Zugriff 10.03.2021.

[16] Jansen, J. (2021). Dieses Kölner Start-up entwickelt mit IBM den digitalen Impfpass. https://www.faz.net/aktuell/wirtschaft/digitec/ibm-entwickelt-mit-start-up-ubirch-den-digitalen-impfpass-17235494.html. Zugriff 10.03.2021.

[17] Borchers, D. (2021). Digitaler Impfpass: Unklare Interoperabilität zwischen deutschem und EU-Pass. https://heise.de/-5493354. Zugriff 13.03.2021.

[18] European Union (2021). Digital Green Certificate. Brüssel.

[19] Europäische Kommission (2021). Corona: Digitale grüne Nachweise. https://ec.europa.eu/info/live-work-travel-eu/coronavirus-response/safe-covid-19-vaccines-europeans/covid-19-digital-green-certificates_de. Zugriff 18.03.2021.

[20] European Data Protection Board (2021). EDPB-EDPS Joint Opinion 04/2021 on the Proposal for a Regulation of the European Parliament and of the Council on a framework for the issuance, verification and acceptance of interoperable certificates on vaccination, testing and recovery to facilitate free movement during the COVID-19 pandemic (Digital Green Certificate). Brüssel.

[21] Waschinski, G., Specht, F., Kolf, F. u.a. (2021). Testrepublik Deutschland? Diese Fallstricke hat Spahns Konzept im Kampf gegen Corona. https://www.handelsblatt.com/politik/deutschland/pandemie-testrepublik-deutschland-diese-fallstricke-hat-spahns-konzept-im-kampf-gegen-corona/26965912.html. Zugriff 18.03.2021.

[22] Krempl, S. (2021). Digitaler EU-Impfnachweis soll in die Corona-Warn-App integriert werden. https://www.heise.de/-6017119. Zugriff 17.04.2021.

[23] Stokkink, Q., Pouwelse, J. (2018). Deployment of a blockchain-based self-sovereign identity. In *2018 IEEE international conference on Internet of Things (iThings)*. S. 1336-1342.

[24] Yang, X., Li, W. (2020). A zero-knowledge-proof-based digital identity management scheme in blockchain. In Computers & Security. *99*. 102050.

[25] Schillinger, F., Schindelhauer, C. (2020). Recovering Private User Storages in Online Social Networks. In Journal of Internet Technology and Secured Transactions. 8. S. 687-698

[26] Iskandar, K. (2021). Gefälschte Impfausweise in Umlauf. https://www.faz.net/aktuell/rhein-main/corona-impfung-gefaelschte-impfpaesse-auf-frankfurter-schwarzmarkt-17295828.html. Zugriff 17.04.2021