Digitaler Impfnachweis *ImpfPassDE*

Sicherheit und Datenschutz

* * * * *

erstellt von der **Gesellschaft zur Förderung der Impfmedizin mbH**
und der **zollsoft GmbH**

* * * * *

Autoren:

Dr. med. Hans-Jürgen Schrörs, Gesellschaft zur Förderung der Impfmedizin mbH

Johannes Zollmann, zollsoft GmbH

Dr. Sven Radszuwill, zollsoft GmbH

Martin Tschirsich, unabhängiger Informationssicherheitsberater

* * * * *

Zusammenfassung

Sowohl Deutschland als auch die europäischen Staaten haben beschlossen, der Bevölkerung einen einheitlichen Impfnachweis für Covid-19-Geimpfte zur Verfügung zu stellen. Unser Ziel ist es, eine möglichst datenschutzfreundliche und sichere technische Lösung für einen digitalen Impfnachweis zu schaffen und die Rahmenbedingungen, die diesem zugrunde liegen, darzustellen.

Unser Impfnachweis ImpfPassDE gewährt den Schutz vertraulicher Impf-, Meta- und Bewegungsdaten der Geimpften selbst in den Fällen, in denen die beteiligten Akteure wie Prüfer und Betreiber aktiv gegen die Interessen des Geimpften zu handeln versuchen. Erreicht wird dies durch konsequente Nutzung der dezentralen Infrastruktur. Die Lösung setzt auf das dezentrale Vorhalten aller Impfdaten sowie der Signatur des Arztes in einem QR-Code und die Nutzung der Telematikinfrastruktur. Durch Verzicht auf weitere, nicht zweckdienliche Instrumente wurde die Komplexität der Anwendung und somit die Angriffsfläche weitestgehend reduziert.

Aufgrund der dynamischen Entwicklung rund um den digitalen Impfnachweis und der möglichen Einsatzszenarien werden sich die Anforderungen auch an den Impfnachweis ImpfPassDE weiterentwickeln.

* * * * *

Version: 1.0, 6. April 2021

* * * * *

Inhaltsverzeichnis

Der digitale Impfnachweis

Digitale Impfnachweise wurden öffentlich bereits kontrovers diskutiert. Wir möchten uns an der Diskussion der grundsätzlichen rechtlichen Fragestellungen zu Privilegien für Geimpfte in diesem Dokument nicht beteiligen. Unser Ziel ist es, mit *ImpfPassDE* eine möglichst datenschutzfreundliche und sichere technische Lösung für einen digitalen Impfnachweis zu schaffen und die Rahmenbedingungen, die diesem zugrunde liegen, in diesem Dokument darstellen.

Zweck

Laut EU-Vorgaben[1] ist beim Zweck von Impfnachweisen grundsätzlich zu unterscheiden zwischen medizinischen Einsätzen oder Einsätzen im Reiseverkehr. Der hier betrachtete Impfnachweis ImpfPassDE soll initial nicht für medizinische Zwecke im Sinne einer Weiterbehandlung im Ausland dienen. Dafür sei auf die Projekte wie die elektronische Patientenakte bzw. den elektronischen Impfausweis[2] verwiesen.

Der hier betrachtete Impfnachweis ImpfPassDE kann ebenso zunächst nicht grundsätzlich als Impfnachweis gegenüber dem Arbeitgeber nach IfSG dienen. Laut Gesetz kann der Nachweis durch eine Impfdokumentation (Impfausweis) oder in Form eines ärztlichen Zeugnisses vorgelegt werden. Dies ist nur mit einer qualifizierten elektronischen Signatur (QES) möglich. Diese kann zwar durch die Nutzung des elektronischen Heilberufeausweises (eHBA) Bestandteil von ImpfPassDE sein, ist jedoch nicht notwendige Voraussetzung, denn aufgrund unzureichender Verbreitung des eHBA muss für die Signatur des Impfnachweises ebenfalls auf den Praxisausweis (SMC-B) zurückgegriffen werden.

Wir ergänzen den Zweck eines Impfnachweises um die Möglichkeit einer Einlasskontrolle zu bspw. Institutionen, Geschäften oder Veranstaltungen. Außerdem ist ein wichtiger, oft vernachlässigter Zweck die Information des Geimpften selbst. Ein Impfnachweis ermöglicht den kontinuierlichen und idealerweise barrierefreien Zugang zu Informationen bezüglich Impfstoff, Impfterminen und weiteren Informationen.

Beteiligte

An den Einsatzszenarien des digitalen Impfnachweises sind verschiedene Akteure beteiligt. Im Einzelnen sind dies:

Geimpfte - Inhaber des Impfnachweises, hier ebenfalls stellvertretend für gesetzliche Vertreter. Zukünftig wird es notwendig sein, auch ungeimpfte Personen, die bspw. aus medizinischen Gründen nicht geimpft werden können, mit aufzunehmen. Zur besseren Les- und Nachvollziehbarkeit sprechen wir in diesem Dokument verallgemeinernd von Geimpften.

Aussteller - Medizinisches Personal, welches zur Ausstellung von Impfnachweisen berechtigt ist. Nach IfSG ist in Deutschland jeder Arzt zur Durchführung von Schutzimpfungen berechtigt und daher berechtigt, einen Impfnachweis auszustellen.

Prüfer - Jede natürliche oder juristische Person, die den Impfnachweis eines Geimpften auf Gültigkeit überprüft.

---

[1] European eHealth Network: Guidelines on verifiable vaccination certificates - basic interoperability elements, Release 2, online: https://ec.europa.eu/health/sites/health/files/ehealth/docs/vaccination-proof_interoperability-guidelines_en.pdf

[2] Bundesministerium für Gesundheit: Der elektronische Impfpass, in: Nationales Gesundheitsportal, 18.12.2020, online: https://gesund.bund.de/elektronischer-impfpass

Betreiber - Neben dem Betreiber des digitalen Impfnachweises, welcher gleichzeitig auch Hersteller ist und sowohl den Betrieb der Build-Infrastruktur inklusive Code-Signing-Zertifikaten als auch die Betriebs-Infrastruktur mitsamt Update-Server für Aussteller-Komponenten und Webserver verantwortet, fallen hierunter auch die am Betrieb des Vertrauensraumes (PKI) beteiligten Akteure.

Dritte - Außenstehende Personen, darunter Ungeimpfte.

Anforderungen und deren Umsetzung

Analoge und digitale Nutzbarkeit für Endanwender - Für einen barrierefreien Zugang ist sowohl die analoge als auch die digitale Nutzung gleichberechtigt umzusetzen. Denn die Nachweismöglichkeit muss sowohl Nutzern ohne Zugang zu digitalen Lösungen ermöglicht werden als auch Nutzern, die ausschließlich digitale Lösungen nutzen möchten.

Diese Anforderung werden durch die Nutzung eines QR-Codes, der sowohl analog auf Papier also auch digital mit sich geführt werden kann, erfüllt.

Integration in Arztpraxen und Impfzentren - Eine Anforderung, die prozessual für die effiziente Nutzung von Impfnachweisen grundlegend ist, ist die Integration der zugehörigen Prozesse und Komponenten in die Arztpraxen und Impfzentren. Ohne eine direkte Integration in die bestehende Softwarelandschaft ist ein digitaler Impfnachweis zwar technisch umsetzbar - sogar deutlich einfacher - eine verbreitete Nutzung wird dadurch jedoch massiv eingeschränkt.

Diese Anforderung wird durch die Nutzung unserer bestehenden Impfsoftware ImpfDocNE für Arztpraxen sowie ImpfDocCE für Impfzentren und der Nutzung der Telematikinfrastruktur erfüllt. Für Nutzer, die kein ImpfDocNE nutzen können oder möchten, wird eine Web-Applikation zur Verfügung gestellt. Für Nutzer ohne TI kann eine alternative Public-Key-Infrastruktur (PKI) eingesetzt werden.

Unabhängige Validierung durch Dritte - Um die oben genannten Zwecke zu erfüllen, ist die unabhängige Überprüfbarkeit des Impfnachweises durch Dritte wesentlich. Der Impfnachweis muss eine Prüfung darauf ermöglichen, wer wann eine bestimmte Impfung bestätigt hat und ob diese Entität dazu berechtigt war.

Um dies zu gewährleisten wird auf die Telematikinfrastruktur als Vertrauensraum zurückgegriffen und Signaturen mittels Heilberufsausweis (eHBA) oder Institutionsausweis (SMC-B) genutzt. Die Impfdaten einer Impfung werden digital signiert. Dies hat den Vorteil, dass diese Infrastruktur in den deutschen Arztpraxen überwiegend bereits vorhanden ist.

Offline-Prüfung - Es kann nicht davon ausgegangen werden, dass eine Überprüfung zu jeder Zeit an jedem Ort über eine aktive Internetverbindung möglich ist. Daher muss eine gewisse Überprüfbarkeit der Impfnachweise auch ohne durchgehend verfügbare Internetverbindung möglich sein. Um dies zu gewährleisten werden die Impfdaten und die zugehörige Signatur in einem QR-Code zur Verfügung gestellt. Lediglich zur Statusprüfung von Signaturzertifikaten ist eine Online-Verbindung notwendig.

Im Offline-Modus wird auf die Statusprüfung der Signaturzertifikate verzichtet und ein entsprechender Warnhinweis ausgegeben. Ebenfalls ist zur Prüfung der Sperrliste eine Online-Verbindung notwendig.

Nachträgliche Ausstellung - Die nachträgliche Ausstellung eines Impfnachweises muss ermöglicht werden. Für Personen, die bereits vor Start des Impfnachweises vollständig geimpft waren, muss diese Möglichkeit ebenso bestehen wie im Fall des Verlusts des Impfnachweises und für Geimpfte aus nicht teilnehmenden Impfzentren oder Arztpraxen.

Die nachträgliche Ausstellung kann durch einen Arzt durchgeführt werden. Dabei ist wesentlich, wer die Impfung bestätigt, nicht, wer sie ausgeführt hat. Die Bestätigung muss auf Basis bestehender Dokumentation erfolgen.

Sperrung einzelner Impfnachweise - Beispielsweise im Fall von vorgetäuschten Impfungen muss es möglich sein, einzelne Impfnachweise zu invalidieren.

Zur Umsetzung dieser Anforderung wird nach Vorgaben der EU voraussichtlich eine EU-weite Sperrliste eingeführt werden, die jeweils nationale Bestandteile hat und von den jeweiligen Ländern administriert wird. Die Sperrliste beinhaltet die ungültigen UVCIs (Unique Vaccination Certificate Identifier) - also die eindeutigen Identifier jeder Impfung auf EU-Ebene.

Komponenten

Folgende Komponenten sind am Zusammenspiel des digitalen Impfnachweises beteiligt:

Impfdaten - die vom Aussteller erhobenen Daten bestehend aus Identitätsattributen des Geimpften sowie Zeitpunkt und Art der Impfung.

Impfnachweis - die vom Aussteller mittels Signaturzertifikat bzw. zugehörigem Signaturschlüssel signierten Impfdaten.

Impfnachweis-App *(Nutzung optional)* - die mobile App, welche den Impfnachweis sicher auf dem Mobilgerät des Geimpften oder seines Vertreters speichert.

Web-App *(Nutzung optional)* - eine Webanwendung zum Zweck der Selbstauskunft, welche die Impfdaten eines Impfnachweises verständlich darstellt und dessen Gültigkeit prüft.

Prüf-App - die mobile App, welche den auf einem Mobilgerät des Geimpften angezeigten oder in Papierform vorgelegten Impfnachweis in Form eines QR-Codes einliest und sowohl die eingelesenen Daten anzeigt als auch die Echtheit der Signatur bestätigt.

Vertrauensraum - fußt auf der Public-Key-Infrastructure (PKI) der Telematikinfrastruktur zum Ausstellen, Verteilen und Verifizieren von digitalen Zertifikaten und wird aufgespannt durch die Einträge in der sog. Trust Service Status List (TSL)[3].

Ausstellerkomponenten - dies sind die Software- und Hardwarekomponenten in Arztpraxen und Impfzentren, welche an der Ausstellung eines Impfnachweises beteiligt sind, darunter das Primärsystem[4] inkl. ImpfDocNE bzw. impf.app Praxis, die sichere Signaturerstellungseinheit auf der Signaturkarte sowie die Signaturanwendungskomponenten auf Konnektor, Primärsystem und E-Health-Kartenterminals.

Prozesse

Die zuvor beschriebenen Komponenten des digitalen Impfnachweises sind an den nachfolgenden Prozessen beteiligt:

Ausstellung - der Aussteller eines Impfnachweises erfasst in einer Arztpraxis oder einem Impfzentrum zunächst die Impfdaten des Geimpften bestehend aus dessen Identitätsattributen sowie Zeitpunkt und Art der Impfung. Eine Identitätsprüfung[5] wäre dabei

[3] gematik: TSL-Dienst, in: gematik Fachportal, online: https://fachportal.gematik.de/hersteller-anbieter/komponenten-dienste/tsl-dienst
[4] gematik: Primärsysteme in der TI, in: gematik Fachportal, online: https://fachportal.gematik.de/hersteller-anbieter/primaersysteme
[5] Eine Identitätsprüfung beispielsweise nach BSI TR-03147^.

zwar wünschenswert und zweckdienlich für den Impfnachweis, ist jedoch in der Praxis kaum umsetzbar, da die Voraussetzungen nicht gegeben sind. Anschließend signiert der Aussteller die Impfdaten mittels einem auf einer Signaturkarte sicher abgelegten Signaturschlüssel. Hierzu kann entweder der elektronische Heilberufsausweis (eHBA) oder der Institutionsausweis (SMC-B) zum Einsatz kommen.

Die signierten Impfdaten bilden den Impfnachweis, welcher durch den Aussteller in Form eines QR-Codes entweder ausgedruckt oder am Bildschirm angezeigt wird. Der Geimpfte kann diesen QR-Code nun über die Kamera mit der auf seinem Mobilgerät installierten Impfnachweis-App einlesen, dort wird der Impfnachweis sicher abgespeichert.

Selbsterklärung - bei Bedarf kann der Geimpfte jederzeit einem Dritten gegenüber eine Selbsterklärung über den eigenen Impfstatus abgeben. Hierzu kann der Geimpfte auf seinem Mobilgerät die Impfnachweis-App ImpfPassDE öffnen und sich und seinem Gegenüber den Impfstatus anzeigen lassen, ohne dabei weitere Daten zu offenbaren. Der Impfstatus bestimmt sich anhand des in der Impfnachweis-App hinterlegten Impfnachweises sowie einer noch zu bestimmenden Geltungsdauer und dem aktuellen Datum. Die Echtheit des behaupteten Impfstatus ist für Dritte dabei nicht erkennbar.

Prüfung - möchte der Geimpfte die Echtheit des behaupteten Impfstatus gegenüber einem Dritten nachweisen, kann er dazu den Impfnachweis auf Papier oder in Form eines QR-Codes in der Impfnachweis-App auf seinem Mobilgerät anzeigen lassen. Der Dritte in Rolle des Prüfers scannt den gezeigten QR-Code mit seiner Prüf-App, welche den Impfstatus analog zur Impfnachweis-App bestimmt, die Echtheit der Signatur im Impfnachweis prüft und die Identitätsdaten des Geimpften anzeigt. Der Prüfer führt anschließend eine Identitätsfeststellung des Geimpften durch, beispielsweise indem er sich einen Ausweis zeigen lässt und dessen Echtheit prüft. Ein Identitätsabgleich gibt Gewissheit darüber, ob der Impfnachweis tatsächlich zum Geimpften gehört.

Zu schützende Werte

Die Komponenten und Prozesse des digitalen Impfnachweises tragen zum Teil einen hohen Schutzbedarf, welcher sich aus dem Schadpotential für die Betroffenen - insbesondere Geimpfte - ergibt. Die zu schützenden Werte sind:

Impfdaten und Impfnachweis - Die Impfdaten des Geimpften identifizieren diesen eindeutig und lassen Rückschlüsse auf dessen körperlichen Gesundheitszustand zu. So lässt sich durch den Zeitpunkt der Impfung ermitteln, ob der Geimpfte einer Prioritätengruppe angehört und daher ein (sehr) hohes Risiko für einen schweren oder tödlichen Krankheitsverlauf nach einer Infektion mit dem Coronavirus trägt. Eine Verletzung des Rechts auf informationelle Selbstbestimmung kann für Betroffene zu einem hohen Schaden führen, sollten sich signierte Impfdaten in Form eines Impfnachweises nicht oder nur schwer abstreiten lassen.

Aus dem Impfnachweis geht eindeutig hervor, welcher Aussteller (Institution oder Arzt) die Impfdaten wann signiert hat. Eine Zusammenführung dieser Informationen lässt in gewissem Rahmen eine Leistungsbewertung zu. Zu Abrechnungszwecken werden diese Daten allerdings bereits heute erhoben. Eine Manipulation des Ausstellers kann für die betroffene Institution oder den betroffenen Arzt schwere Folgen haben, sollte es beispielsweise zu Regressforderungen kommen und sich signierte Impfdaten nicht oder nur schwer abstreiten lassen.

Falsche oder veränderte Impfdaten haben aufgrund des nicht-medizinischen Zwecks keinen direkten Einfluss auf die Patientensicherheit, können aber dazu führen, dass beispielsweise eine Auffrischung nicht rechtzeitig wahrgenommen wird und schaden dem Ansehen des und dem Vertrauen in den digitalen Impfnachweis.

Bei Verlust kann dagegen einfach auf den Impfausweis zurückgegriffen und ein neuer Impfnachweis ausgestellt werden.

Schutzbedarf: Es besteht ein hoher Schutzbedarf hinsichtlich Vertraulichkeit und Integrität, ein mittlerer Schutzbedarf hinsichtlich Verfügbarkeit.

Meta- und Bewegungsdaten von Geimpften - Bei Prüfung von Impfnachweisen wird als Metadatum die Information über den Aufenthalt des Geimpften an einem bestimmten Ort zu einer bestimmten Zeit an den Prüfer gegeben. Werden diese Informationen zusammengeführt, lassen sich daraus detaillierte Bewegungsprofile erstellen. Auch ohne Zusammenführung lässt bereits der Aussteller des Impfnachweises auf einen Herkunftsort des Geimpften schließen.

Schutzbedarf: Es besteht ein hoher Schutzbedarf hinsichtlich Vertraulichkeit.

Ausweisdaten - Die Prüfung eines Impfnachweises erfordert den Identitätsabgleich anhand eines echten Ausweisdokuments des Geimpften. Unter den darauf befindlichen Identitätsattributen gehört das biometrische Lichtbild zu den besonderen Kategorien personenbezogener Daten, die nach Art. 9 Abs. 1 DSGVO eines speziellen Schutzes bedürfen. Eine Verarbeitung im Sinne der DSGVO ist daher nicht vorgesehen.

Schutzbedarf: Es besteht ein hoher Schutzbedarf hinsichtlich Vertraulichkeit.

Weitere Metadaten von Prüfstellen - Bei Prüfung von Impfnachweisen werden durch den Prüfer indirekt auch Informationen über die Prüfstelle selbst erhoben. So lässt die Anzahl der Prüfvorgänge auf das Besucheraufkommen schließen, eine Auswertung der Impfnachweis-Aussteller gibt Aufschluss über das Einzugsgebiet.

Schutzbedarf: Es besteht ein mittlerer Schutzbedarf hinsichtlich Vertraulichkeit.

Der Schutzbedarf für weitere Prozesse und Komponenten des digitalen Impfnachweises wie die Impfnachweis-, Prüf- und Web-App, die Ausstellerkomponenten und den Vertrauensraum (PKI) leiten sich aus dem Schutzbedarf der oben genannten primären Werte ab.

Angreifer und Bedrohungen

Angreifer, Angreiferpotential, Motivation und Ziele

Angreifer können in jeder Rolle mit hohem Angriffspotential auftreten. Im Nachfolgenden sind exemplarisch Angreifermotivationen und Ziele in verschiedenen Rollen benannt.

Prüfer haben ein Interesse daran, anhand der Impfnachweise Bewegungsprofile von Geimpften zu erstellen, beispielsweise um Kaufverhalten zu analysieren. Andererseits haben Prüfer ein Interesse daran, die (Nicht-)Prüfung von Ungeimpften nachträglich abstreiten zu können, beispielsweise um ohne nachweisbare Pflichtverletzung auch Ungeimpften Einlass zu gewähren.

Aussteller haben ein Interesse daran, auch Ungeimpften einen Impfnachweis auszustellen, dies aber nachträglich abstreiten können, beispielsweise zum eigenen Vorteil oder als Anhänger einer Verschwörungsideologie.

Geimpfte haben ein Interesse daran, ihre Impfnachweise Ungeimpften zur Verfügung zu stellen, dies aber nachträglich abstreiten zu können, beispielsweise zum eigenen Vorteil oder als Anhänger einer Verschwörungsideologie.

Ungeimpfte haben ein Interesse daran, gültige Impfnachweise zu erlangen.

Dritte haben ein Interesse daran, die Impfdaten der Geimpften zu erlangen.

Bedrohungen

Es folgt eine Betrachtung der Bedrohungen der zu schützenden Werte des digitalen Impfnachweises.

Kompromittierte Ausstellerkomponenten

Angreifer könnten die Integrität der Ausstellerkomponenten verletzen, beispielsweise durch Einschleusen von Schadcode in die Infrastruktur zur Verteilung von Software-Updates oder in von der Software eingesetzte Programmbibliotheken. Durchführbar ist auch ein direkter Angriff auf die Primärsysteme vor Ort über das lokale Netzwerk oder eine unsichere Anbindung an externe Netze[6].

Im Erfolgsfall kann der Angreifer sowohl die Impfdaten und Impfnachweise der in den angegriffenen Einrichtungen Geimpften auslesen als auch beliebige Impfdaten signieren und damit gültige Impfnachweise ausstellen.

Kompromittierter Vertrauensraum

Ein Angreifer kompromittiert die Integrität des Vertrauensraumes beispielsweise durch unrechtmäßiges Erlangen eines Signaturzertifikats mit geheimem Signaturschlüssel[7]. Hierzu zählt auch ein Umgehen organisatorisch durchgesetzter Zugriffsbeschränkungen auf eine freigeschaltete Institutionskarte beispielsweise durch unberechtigtes Personal innerhalb einer Arztpraxis oder das Hinzufügen eines eigenen Signaturzertifikats in die Trust Service Status List (TSL).

Im Erfolgsfall kann der Angreifer beliebige Impfdaten signieren und damit gültige Impfnachweise ausstellen.

Kompromittierte oder falsche Impfnachweis-, Prüf- oder Web-App

Ein Angreifer kompromittiert die Integrität der Impfnachweis- oder Prüf-App, beispielsweise durch Einschleusen von Schadcode in die Infrastruktur zur Verteilung von Software-Updates oder von der Software eingesetzte Programmbibliotheken. Alternativ bringt der Angreifer eine unechte Impfnachweis- oder Prüf-App in Umlauf, indem er einen authentisch erscheinenden Nachbau in die bekannten Appstores mit ähnlichem Namen einstellt und bewirbt.

Im Erfolgsfall kann der Angreifer Impfdaten und Impfnachweise der angegriffenen Geimpften auslesen.

Gleiches gilt bei erfolgreichem Angriff auf die Integrität der Web-App, beispielsweise durch Kompromittierung des Webservers oder des Kommunikationskanals zum Browser.

Ein Angreifer kann auch der Betreiber selbst sein.

Auch Prüfer können bewusst falsche Prüf-Apps einsetzen, um die Impf- und Metadaten in eigenem Interesse weiterzuverarbeiten. Dies wird unter *Ausspähen und Tracking von Geimpften durch Prüfer* betrachtet.

[6] Detlef Borchers: rC3: Es krankt an der Sicherheit im Gesundheitswesen, in: Heise Online, 30.12.2020, online: https://www.heise.de/news/rC3-Es-krankt-an-der-Sicherheit-im-Gesundheitswesen-5001060.html

[7] Chaos Computer Club: CCC diagnostiziert Schwachstellen im deutschen Gesundheitsnetzwerk, 27.12.2019, online: https://www.ccc.de/de/updates/2019/neue-schwachstellen-gesundheitsnetzwerk

Kompromittierte Umgebung der Impfnachweis-, Prüf- oder Web-App

Ein Angreifer kompromittiert die clientseitige Umgebung der jeweiligen App auf dem Mobilgerät des Geimpften oder des Prüfers.

Der Angreifer erlangt direkt oder indirekt Zugriff auf die Impf- sowie der Metadaten. Durch Installation eines MitM-Zertifikats[8] im Zertifikatsspeicher des Mobilgeräts wird die Transportverschlüsselung bei Kommunikation mit der Web-App aufgebrochen.

Eine Kompromittierung nicht der Umgebung sondern der App selbst wird in *Kompromittierte oder falsche Impfnachweis-, Prüf- oder Web-App* betrachtet.

Ausspähen und Tracking von Geimpften durch Prüfer

Bei der Prüfung verarbeitet der Prüfer den vollständigen Impfnachweis des Geimpften mit den darin enthaltenen Impfdaten. Gleichzeitig führt der Prüfer eine Identitätsfeststellung anhand eines vorgelegten Ausweisdokuments durch, womit die Identitätsattribute im Impfnachweis eindeutig und sicher dem Geimpften zugeordnet werden.

Darüber hinaus können Prüfer sowohl die Impfdaten mitsamt Identitätsattributen oder allein nur die Signatur im Impfnachweis als eindeutiges Pseudonym dazu missbrauchen, um an verschiedenen Orten und zu verschiedenen Zeitpunkten durchgeführte Prüfungen eines Impfnachweises demselben Geimpften zuzuordnen. Die erlangten Meta- bzw. Bewegungsdaten der Geimpften können zu Bewegungsprofilen zusammengeführt werden.

Angriff auf Identitätsprüfung

Über die erfassten Identitätsattribute wie Vor- und Nachname in den signierten Impfdaten wird der Impfnachweis durch den Aussteller eindeutig an den Geimpften gebunden und kann somit nicht mehr missbräuchlich durch Dritte bei einer Prüfung vorgelegt werden, da ansonsten der vorgesehene Identitätsabgleich mit dem Ausweisdokument scheitert. Die notwendige Identitätsfeststellung sowohl durch den Aussteller als auch den Prüfer kann von verschiedener Seite angegriffen werden, wenn beispielsweise ein Impfkandidat gegenüber dem Aussteller oder Prüfer eine falsche Identität behauptet und der Aussteller oder Prüfer auf einen ungenügenden Identitätsnachweis wie beispielsweise die elektronische Gesundheitskarte[9] vertraut.

Die Bedrohung durch das Erlangen von Impfnachweisen auf Grundlage falscher Impfausweise wird unter *Fälschung von Impfausweisen* betrachtet.

Fälschung von Impfausweisen

Angreifer können eine Total- oder Teilfälschung von Impfausweisen mit den gewünschten Impfdaten herstellen (Herstellen einer unechten Urkunde oder Verfälschen einer echten Urkunde) und sich auf dieser Grundlage bei einem Arzt nachträglich einen digitalen Impfnachweis ausstellen lassen. Ärzte selbst können einen Impfausweis mit falschen Angaben herstellen (Herstellen einer falschen Urkunde).

Ausspähen von Metadaten bei Statusprüfung von Signaturzertifikaten

Bei Prüfung der Signatur des Impfnachweises wird der Status des Signaturzertifikates per Online Certificate Status Protocol (OCSP) geprüft. Dabei wird die Seriennummer des zu

[8] Bundesamt für Sicherheit in der Informationstechnik: Man-In-The-Middle-Angriff, in: Glossar, online: https://www.bsi.bund.de/SharedDocs/Glossareintraege/DE/M/Man-In-The-Middle-Angriff.html
[9] Chaos Computer Club: CCC diagnostiziert Schwachstellen im deutschen Gesundheitsnetzwerk, 27.12.2019, online: https://www.ccc.de/de/updates/2019/neue-schwachstellen-gesundheitsnetzwerk

prüfenden Zertifikats an den durch den verantwortlichen Trust Service Provider (TSP)[10] betriebenen OCSP-Responder übermittelt. Durch Zusammenführen der dabei übertragenen Informationen kann der TSP beispielsweise Einzugsgebiet und Besucherzahl einer Prüfstelle abschätzen.

Weitere Bedrohungen

Nicht aufgeführt sind weitere Bedrohungen, die bereits vor Einführung des digitalen Impfnachweises bestanden und denen bereits bekannte Sicherheitsanforderungen entgegenstehen.

Nicht berücksichtigt sind Bedrohungen, die sich nicht gegen zu schützende Werte des digitalen Impfnachweises richten. Dazu gehören beispielsweise Betrug beim Impfen durch den Arzt, unwirksame Impfungen oder Infektiosität trotz Impfung.

Sicherheitsziele, -anforderungen und Diskussion

Impfzentren und Arztpraxen erheben und verarbeiten bereits die zur Ausstellung der Impfnachweise notwendigen Daten der Geimpften. Zur Ausstellung von Impfnachweisen wird bestehende Software in geringem Umfang funktional erweitert, ohne dass zusätzliche Daten erhoben werden.

Für die Signatur in Arztpraxen wird auf die dezentralen Komponenten der Telematik-Infrastruktur zurückgegriffen, insbesondere auf die Signaturanwendungskomponenten in Konnektoren und E-Health-Kartenterminals.

Sichere Ausstellerkomponenten und sicherer Vertrauensraum

Zur Abwehr der Bedrohungen *Kompromittierte Ausstellerkomponenten* sowie *Kompromittierter Vertrauensraum* müssen keine gegenüber dem jetzigen Stand neuen Sicherheitsziele formuliert werden, da lediglich auf Bestehendes zurückgegriffen wird. Insbesondere ergeben sich keine neuen Sicherheitsanforderungen. Zu den bestehenden Sicherheitszielen zählen insbesondere:

Keine Verwundbarkeit durch praktisch durchführbare Quantencomputer-Angriffe: Auf elliptischen Kurven basierende kryptographische Primitiven, dazu gehört auch ECDSA, lassen sich auf ausreichend großen Quantencomputern mittels modifiziertem Shor-Algorithmus zur Berechnung des diskreten Logarithmus brechen.

Signaturerhalt: Es müssen Signaturverfahren genutzt werden, die gemäß BSI[11] noch mindestens drei Jahre verwendbar sind. Eine Erneuerung von Signaturen oder ein Übersignieren kann erfolgen.

Sichere Ausgabe von Zertifikaten: Aussteller von Impfnachweisen müssen sicher identifiziert werden und ihre Berechtigung zur Ausstellung von Impfnachweisen sicher nachweisen.

Authentische App, sichere Kommunikation und sicherer Bezugsweg

Zur Abwehr der unter *Kompromittierte oder falsche Impfnachweis-, Prüf- oder Web-App* betrachteten Bedrohungen der mobilen Impfnachweis- oder Prüf-App sind diese Apps quelloffen zu legen. Reproducible Builds liefern die Gewähr, dass die ausgelieferten mobilen

[10] gematik: Trust Service Provider X.509 (nonQES) – SMC-B, in: gematik Fachportal, online: https://fachportal.gematik.de/hersteller-anbieter/komponenten-dienste/trust-service-provider-x509-nonqes-smc-b

[11] Bundesamt für Sicherheit in der Informationstechnik, TR-02102 Kryptographische Verfahren: Empfehlungen und Schlüssellängen, online: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Technische-Richtlinien/TR-nach-Thema-sortiert/tr02102/tr-02102.html

Apps tatsächlich aus dem quelloffenen Programmcode gebaut wurden. Durch Signatur der ausgelieferten App durch den Hersteller wird eine Manipulation bei Auslieferung aus dem Appstore unterbunden. Um zu vermeiden, dass Geimpfte eine falsche, aber namensähnliche mobile App installieren, wird der Download über einen vertrauenswürdige URL[12] ermöglicht, welcher zusammen mit dem Impfnachweis ebenfalls an den Geimpften ausgehändigt wird.

Zur Abwehr der unter *Kompromittierte oder falsche Impfnachweis-, Prüf- oder Web-App* ebenfalls betrachteten Kompromittierung der Web-App ist diese und die serverseitige Infrastruktur entsprechend dem Stand der Technik zu härten und die Kommunikation zum Browser nach den Vorgaben des BSI[13] abzusichern. Die Bedrohung einer falschen Web-App gegen den Geimpften ist stark eingeschränkt, da die Web-App nur zur Selbstüberprüfung zur Verfügung steht. Zur Prüfung eines Impfnachweises dagegen darf allein die Prüf-App verwendet werden, um eine mögliche Täuschung des Prüfers auszuschließen. Der Einsatzzweck der Web-App ist daher auf die Selbstauskunft beschränkt und dies wird entsprechend kommuniziert.

Bei Selbstauskunft über die Web-App findet keine Übertragung von Impfdaten an den Webserver statt.

Sichere Mobilgeräte

Die Sicherheit der Anwendungsumgebung kann durch die Impfnachweis-, Prüf- oder Web-App selbst nicht gewährleistet werden und ist daher vorausgesetzt. Zur Abwehr der Bedrohung *Kompromittierte Umgebung der Impfnachweis-, Prüf- oder Web-App* werden Geimpfte daher bei Übergabe des Impfnachweises auf die Risiken bei der Verarbeitung von Gesundheitsdaten auf Mobilgeräten und geeignete Abhilfemaßnahmen[14] verwiesen. Zugleich warnen die Impfnachweis- und Prüf-App den Geimpften bei erkannter Manipulation des Geräts (Root oder Jailbreak) sowie bei Installation auf einem veralteten Betriebssystem.

Datensparsame Selbsterklärung anstelle der Prüfung

Zur Abwehr der Bedrohung *Ausspähen von Metadaten bei Statusprüfung von Signaturzertifikaten* wird auf ein zweistufiges Vertrauensniveau gesetzt. In den meisten Situationen wird eine Selbsterklärung über den Impfstatus des Geimpften ausreichend sein, so wie das auch bisher bei der Kontaktnachverfolgung anhand von Gästelisten gehandhabt wird. Hierbei ist sowohl ein Ausspähen personenbezogener Daten als auch ein Tracking durch Dritte ausgeschlossen.

Ein darüber hinaus gehendes Vertrauen in die Echtheit des behaupteten Impfstatus kann nur dann erreicht werden, wenn der Impfnachweis zur Prüfung zusammen mit einem Ausweisdokument zur Identitätsfeststellung vorgelegt wird. Denn die alleinige Vorlage eines Impfnachweises ohne Identitätsfeststellung bietet gegenüber der reinen Selbsterklärung nur unwesentlich mehr Sicherheit, da gültige Impfnachweise einfach kopiert und verteilt werden können, und ist daher weder zweck- noch rechtmäßig.

---

[12] Google: Linking to Google Play, in: Android Developers, online: https://developer.android.com/distribute/marketing-tools/linking-to-google-play

[13] Bundesamt für Sicherheit in der Informationstechnik: Mindeststandard des BSI zur Verwendung von Transport Layer Security (TLS) nach § 8 Absatz 1 Satz 1 BSIG, Version 2.1 vom 09.04.2020, online: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Mindeststandards/Mindeststandard_BSI_TLS_Version_2_1.pdf

[14] Bundesamt für Sicherheit in der Informationstechnik: Smartphone und Tablet effektiv schützen, in: Basistipps zur IT-Sicherheit, online: https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/Basisschutz-fuer-Computer-Mobilgeraete/Schutz-fuer-Mobilgeraete/schutz-fuer-mobilgeraete_node.html

Das dem Prüfer zur Identitätsfeststellung vorgelegte Ausweisdokument darf dabei nur einer manuellen haptischen und optischen Kontrolle unterzogen werden. Eine automatische Erfassung und Verarbeitung dürfen nicht stattfinden. Ausgenommen sind zertifizierte und versiegelte Ausweisprüfgeräte in sicherer Umgebung sowie ggf. zertifizierte Ausgestaltungen der elektronischen ID-Funktion[15].

Eine Prüfung muss zudem in einer sicheren Umgebung stattfinden. Dabei dürfen Dritte keinen Einblick in den gezeigten QR-Code und das vorgelegte Ausweisdokument haben.

Sichere Identitätsfeststellung und sichere Impfausweise

Die Bedrohung *Angriff auf Identitätsprüfung* muss zum Zeitpunkt der Ausstellung des papiergebundenen Impfausweises abgewehrt sein. Bisher wird in den Impfzentren und Arztpraxen keine Identitätsfeststellung durchgeführt. Zudem sind Aussteller nicht geschult in der Identitätsprüfung von Geimpften, eine derartige Identitätsfeststellung ist in der Praxis auch kaum praktikabel.

Die Bedrohung *Fälschung von Impfausweisen* dagegen muss zum Zeitpunkt der Ausstellung des digitalen Impfnachweises abgewehrt werden. Zum einen aber weist der papierne Impfausweis keine Sicherheitsmerkmale auf, auch sind Blanko-Ausweise frei verfügbar. Die Aufkleber mit Namen des Impfstoffs und Chargennummer können mittels handelsüblichem Etikettendrucker erzeugt werden und sind zudem nicht vorgeschrieben. Zum anderen bieten auch Arzt-Unterschrift und Stempel aufgrund fehlender Möglichkeit zum Unterschriftenabgleich vor Ort keine signifikante Sicherheit. Es bleibt die nicht immer ausreichend[16] abschreckende Wirkung drohender strafrechtlicher Verfolgung von Urkundenfälschung.

Daher wird mit dem digitalen Impfnachweis in Bezug auf die Echtheit des behaupteten Impfstatus insgesamt nur ein mittleres Vertrauensniveau erreicht werden können.

Ärzten droht bei Herstellung unrichtiger Gesundheitszeugnisse neben strafrechtlicher auch berufsrechtliche Verfolgung mit Entzug der Approbation. Auch Nutzern droht bei Urkundenfälschung Strafverfolgung.

Schlussbetrachtung und Ausblick

Das Ziel, eine möglichst datenschutzfreundliche und sichere technische Lösung für einen digitalen Impfnachweis zu schaffen, ist allein durch die konsequente Befolgung eines Security-by-Design-Ansatzes erreichbar.

Im Ergebnis gewährt ImpfPassDE den Schutz vertraulicher Impf-, Meta- und Bewegungsdaten der Geimpften selbst in den Fällen, in denen die beteiligten Akteure wie Prüfer und Betreiber aktiv gegen die Interessen des Geimpften zu handeln versuchen.

Erreicht wird dieses Ziel insbesondere durch konsequente Nutzung der dezentralen Infrastruktur. Nur absolut notwendige zentrale Komponenten wie Vertrauensanker sind in die Umsetzung eingeflossen. Maßgeblich ist auch die Erkenntnis, dass eine Prüfung eines Impfnachweises ohne intrusive und aufwändige Identitätsfeststellung gegenüber einer einfachen Selbsterklärung keinen wesentlichen Sicherheitsgewinn bietet und von daher in den meisten Fällen zugunsten letzterer entfallen kann.

[15] Bundesministerium des Inneren, für Bau und Heimat: Vor-Ort-Auslesen, online: https://www.personalausweisportal.de/Webs/PA/DE/buergerinnen-und-buerger/vor-ort-auslesen/vor-ort-auslesen-node.html

[16] Deutscher Apotheker Verlag: Immun gegen Argumente: Die Welt der Impfgegner, online: https://media.dav-medien.de/sample/9783777628493_p.pdf

Durch Verzicht auf nicht zweckdienliche Instrumente wurde die Komplexität der Anwendung und somit die Angriffsfläche auf das Wesentliche reduziert. So wurde das Einbringen von qualifizierten Zeitstempeln bzw. alternativ die zentrale Verankerung von Impfnachweisen verworfen, da diese das notwendige Vertrauen in den Aussteller, keine falschen Urkunden zu erzeugen, nicht ersetzen können.

Aufgrund der dynamischen Entwicklung rund um den digitalen Impfnachweis und den möglichen Einsatzszenarien werden sich die Anforderungen auch an ImpfPassDE weiterentwickeln. Bereits angedacht sind unter anderem die folgenden Ergänzungen:

Impfnachweis-Sperrliste - Ausgegebene und missbräuchlich verwendete Impfnachweise sollen künftig gesperrt werden können, so wie das bei den Signaturkarten bereits der Fall ist. Da die Durchführung einer Online-Statusprüfung analog zu OCSP ein Datenschutzproblem für den Client darstellen kann, der hohe linear wachsende Speicherverbrauch klassischer Sperrlisten dagegen nicht tragbar ist, wird eine Kompression mittels Bloom-Filter erwogen.

Zero-Knowledge-Impfnachweis - Zukünftig ist angedacht, den Geimpften eine Möglichkeit an die Hand zu geben, einen Impfnachweis gegenüber einem Prüfer auch ohne Offenbarung der vollständigen Impfdaten erbringen zu können, beispielsweise per Zero-Knowledge-Proof basierend auf CL- oder BBS+-Signaturen. Je nach Einsatzzweck kann es sinnvoll und zulässig sein, den Identitätsabgleich mit einem Ausweisdokument dabei weniger sicher auf Grundlage reduzierter Identitätsattribute wie den Initialen des Namens zu führen, anhand derer ein Tracking des Geimpften nicht möglich ist.

Nachweis für Ungeimpfte, Testnachweise, Titernachweise - Bei einer Ausweitung der unterstützten Einsatzszenarien des digitalen Impfnachweises kann es zukünftig notwendig werden, Impfnachweise auch an Ungeimpfte auszustellen, die nachweislich nicht geimpft werden können. Zudem sind Nachweise über durchgeführte Tests und Titernachweise mit der vorhandenen Lösung direkt umsetzbar.

Signatur ohne Heilberufs- und Institutionsausweis - Impfzentren und einige Arztpraxen verfügen nicht über die zur Ausstellung von Impfnachweisen notwendigen Komponenten wie Signaturkarten, Konnektoren und Kartenterminals. Es ist geplant, auch diesen Institutionen das Ausstellen von Impfnachweisen zu ermöglichen.