



Auslesen und Prüfen digitaler Impfnachweise

Aktuelle Kurz-Information 40

Stichwörter: COVID-19-Pandemie – Digitales COVID-Zertifikat – Genesenennachweis – Impfnachweis – Testnachweis | **Stand:** 24. März 2022

Was sind die Kernaussagen dieser Aktuellen Kurz-Information?

- ▶ Ein gesicherter digitaler Impfnachweis ist nur im QR-Code enthalten und kann zuverlässig mit technischen Hilfsmitteln geprüft werden.
- ▶ Zur Prüfung kann die CovPassCheck-App verwendet werden. Die CovPass-App oder die Corona-WarnApp darf dafür nicht verwendet werden.
- ▶ Bei der Prüfung muss der Grundsatz der Datenminimierung beachtet werden.

Eine Zutrittskontrolle im Rahmen von gesetzlichen 2G- oder 3G-Zutrittsregeln wirft neben zahlreichen Fragen des rechtlichen auch Fragen des technisch-organisatorischen Datenschutzes auf. Dies betrifft etwa die Sichtkontrollen, die auf gesetzlicher Grundlage anlässlich des Zugangs zu bestimmten Einrichtungen in Bezug auf die Impf-, Genesenen- oder Testnachweise von Besucherinnen, Besuchern oder Beschäftigten vorgenommen und gegebenenfalls dokumentiert werden dürfen.¹

Impf-, Genesenen- oder Testnachweise haben grundsätzlich in „verkörperter oder digitaler Form“ vorzuliegen, vgl. § 22a Abs. 1 Satz 1, Abs. 2 und 3 Infektionsschutzgesetz (IfSG). Ein Großteil der kontrollierten Personen wird zur Sichtkontrolle einen digitalen Nachweis vorlegen, der beispielsweise in der CovPass-App des Robert Koch-Instituts gespeichert wurde.

Ausgangspunkt der Überlegungen ist die Feststellung, dass bei der Sichtkontrolle stets personenbezogene Daten – Gesundheitsdaten im Sinne von Art. 4 Nr. 15 Datenschutz-Grundverordnung (DSGVO) – betroffen sind, bei deren Verarbeitung der Verantwortliche Maßnahmen nach Art. 25 Abs. 1 DSGVO zu treffen hat.

1. Digitale Nachweise

In der Verordnung (EU) 2021/953² wurde der Rahmen für die Ausstellung, Überprüfung und Anerkennung interoperabler Zertifikate zur Bescheinigung von COVID-19-Impfungen und COVID-19-Tests sowie der Genesung von einer COVID-19-Erkrankung (digitales COVID-Zertifikat der Europäischen Union) festgelegt. Damit ist sichergestellt, dass Zertifikate in einem Format vorliegen, das mit standardisierten Werkzeugen ausgelesen und geprüft werden kann. Mit Hilfe einer Public-Key-Infrastruktur wurde eine Vertrauenskette von den Gesundheitsbehörden bis zu den einzelnen Stellen geschaffen, welche die COVID-19-Zertifikate ausstellen. Der Vertrauensrahmen ermöglicht es, Betrug – insbesondere Fälschungen – zu erkennen.

- 5 Ein digitales Zertifikat enthält neben den Grunddaten (Name und Vornamen, Geburtsdatum und Typ des Nachweises) insbesondere folgende Daten:
 - bei einem Impfnachweis: Impfstoff; Impfstoffhersteller; Anzahl der Impfungen; jeweiliges Datum der einzelnen Impfungen; Land, in dem die jeweilige Impfung erfolgte;
 - bei einem Testnachweis: Art des Tests; Herstellerdaten; Datum der Testdurchführung; Ergebnis des Tests; Testzentrum; Land, in dem die Testung stattfand;
 - bei einem Genesenennachweis: Datum des ersten positiven Tests; Land, in dem der Test durchgeführt wurde.
- 6 Diese Daten sind im QR-Code (2D-Barcode), den beispielsweise die CovPass-App anzeigt, enthalten und dort mit mathematischen Verfahren zuverlässig gegen Manipulation gesichert. Der digitale Nachweis an sich besteht somit nicht aus den angezeigten Texten der App, sondern ist im QR-Code gespeichert.

2. Sicherheit der Prüfung

a) Prüfung ohne technische Hilfsmittel

- 7 In der Kontrollpraxis dürfte wohl oftmals lediglich der angezeigte Text in der CovPass- oder in der CoronaWarn-App auf dem Mobiltelefon der zu überprüfenden Person gelesen und daraus auf den entsprechenden Nachweis geschlossen werden. Dabei ist aber zu bedenken, dass der Nachweis auf einem Gerät angezeigt wird, über das die prüfende Person keine Kontrolle und Kenntnis hat. So kann nicht ausgeschlossen werden, dass die angezeigten Daten nicht mit dem Inhalt des QR-Codes übereinstimmen, oder dass der QR-Code nicht valide Daten enthält. Es könnte sich beispielsweise einfach um einen Screenshot oder den Nachweis einer anderen Person handeln.
- 8 Nach Art. 25 DSGVO hat ein Verantwortlicher allerdings unter Berücksichtigung des **Standes der Technik**, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der mit der Verarbeitung verbundenen Risiken für die Rechte und Freiheiten natürlicher Personen **geeignete technische und organisatorische Maßnahmen** zu treffen, die dafür ausgelegt sind, die Datenschutzgrundsätze wie etwa Datenminimierung (siehe Rn. 16 ff.) wirksam umzusetzen und die notwendigen Garantien in die Verarbeitung aufzunehmen, um den Anforderungen der Datenschutz-Grundverordnung zu genügen und die Rechte der betroffenen Personen zu schützen.
- 9 Der Verantwortliche hat unter anderem nachzuweisen, dass er im Rahmen der von ihm durchgeführten Zutrittskontrollen geeignete technische oder organisatorische Maßnahme im vorgenannten Sinn ergriffen hat. Daher ist es letztlich unumgänglich, für die Überprüfung von digitalen Nachweisen auf hierfür spezifisch vorgesehene technische Hilfsmittel nach dem Stand der Technik zurückzugreifen.

b) Prüfung mit technischen Hilfsmitteln

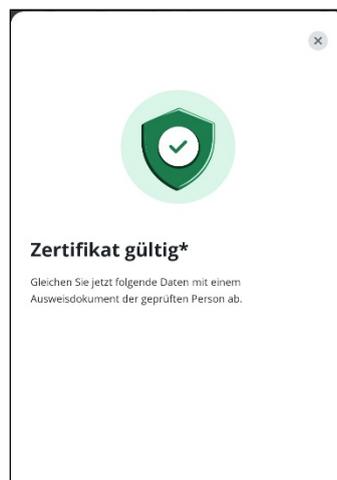
Um eine digitale Signatur („den QR-Code“) zu prüfen, muss zuerst die mathematische Korrektheit (also die Tatsache, dass der Zertifikatsinhalt nicht verändert wurde) und dann die Zertifikatskette (also die Tatsache, dass der Inhalt von einer vertrauenswürdigen Stelle und nicht etwa von der Person, die das Zertifikat vorlegt, selbst erstellt und unterschrieben wurde) verifiziert werden.³ 10

Eine zuverlässige Prüfung kann beispielsweise mit einer App durchgeführt werden, die auf einem dienstlichen Gerät der prüfenden Person installiert ist. Analog zur CovPass-App bietet das Robert Koch-Institut hierzu auch eine CovPassCheck-App an.⁴ Mit Hilfe dieser App erfasst man den QR-Code und bekommt beispielsweise für diesen QR-Code 11



angezeigt, dass es sich nicht um ein gültiges Zertifikat handelt. Rein manuell geprüft ist ein Unterschied zu einem gültigen Zertifikat nicht erkennbar. Prüft man aber mit Hilfe der App, so erhält man umgehend folgendes Ergebnis:

Ein korrektes Zertifikat würde hingegen die folgende Anzeige liefern:



Mit einer Prüf-App lässt sich somit sicherstellen, dass das Zertifikat gültig und sein Inhalt unverändert ist. Zusätzlich zur Gültigkeit zeigt die CovPassCheck-App auch noch den Namen und das Geburtsdatum der Person an, über die das Zertifikat Auskunft gibt (im Beispiel anonymisiert). 12

- 13 Mit Hilfe dieser Daten und einem geeigneten Ausweisdokument kann der Status der zu prüfenden Person sodann zuverlässig erhoben werden.
- 14 Zusammenfassend sind für eine dem Stand der Technik entsprechende Prüfung mit technischen Hilfsmitteln folgende Bedingungen einzuhalten:
 - CovPassCheck-App nutzen,
 - Zertifikate mit der App scannen.
- 15 Auch wenn es offensichtlich sein sollte: Für eine Prüfung ist ausschließlich eine Prüf-App zu nutzen (CovPassCheck) und nicht eine App, die zum Speichern der Zertifikate verwendet wird (**CovPass-** oder **CoronaWarn-App**), da ansonsten die **Zertifikate nicht geprüft, sondern** auf dem Mobiltelefon der prüfenden Person dauerhaft **gespeichert** werden.

3. Datenminimierung

- 16 Nach Art. 5 Abs. 1 Buchst. c DSGVO müssen personenbezogene Daten dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein. Möchte ein Verantwortlicher beispielsweise den 3G-Status einer Person prüfen, so ist es dafür nicht notwendig, den verwendeten Impfstoff zu erheben. Grundsätzlich ist es im Rahmen von 3G-Zutrittsregeln nicht einmal nötig, zwischen Impf-, Genesenen- und Testnachweis zu unterscheiden.
- 17 Die **CovPassCheck-App** zeigt grundsätzlich nur an, ob ein gültiges Zertifikat zum Zeitpunkt der Prüfung vorliegt und ob der Status der geprüften Person den Mindestanforderungen genügt. Eine derartige Prüfung ist daher im Ansatz **datensparsamer** als eine vollständige Prüfung des Zertifikats.
- 18 Eine vollständige – manuelle – Einsicht in alle in den Apps gespeicherten Daten ist nur dann zulässig, wenn alle diese Daten nötig sind, um die Prüfung durchzuführen und gegebenenfalls im Rahmen der gesetzlichen Vorgaben zu dokumentieren.⁵
- 19 Seit der Version 1.17 der CovPassCheck-App lässt sich in Bezug auf den 2G- oder 3G-Status festlegen, welche Nachweise akzeptiert werden sollen. Danach reicht ein Scannen des QR-Codes aus, eine manuelle Prüfung etwa einzelner Impfungen ist dann nicht mehr nötig.
- 20 Für eine Prüfung ist im Rahmen der gesetzlichen Anforderungen an eine Nachweiskontrolle und an eine etwaige Dokumentation immer das datensparsamste Verfahren zu wählen.

¹ Siehe dazu im Einzelnen Bayerischer Landesbeauftragter für den Datenschutz, 3G-Zutrittsregel im bayerischen öffentlichen Dienst, Aktuelle Kurz-Information 38, Nr. 3, Internet: <https://www.datenschutz-bayern.de>, Rubrik „Datenschutzreform 2018 – Aktuelle Kurz-Informationen“.

² Verordnung (EU) 2021/953 des Europäischen Parlaments und des Rates vom 14. Juni 2021 über einen Rahmen für die Ausstellung, Überprüfung und Anerkennung interoperabler Zertifikate zur Bescheinigung von COVID-19-Impfungen und -Tests sowie der Genesung von einer COVID-19-Infektion (digitales COVID-Zertifikat der EU) mit der Zielsetzung der Erleichterung der Freizügigkeit während der COVID-19-Pandemie (ABl. L 211 vom 15. Juni 2021, S. 1).

- ³ Bundesamt für Sicherheit in der Informationstechnik, Grundlagen der elektronischen Signatur, Internet: <https://www.bsi.bund.de/DE/Themen/Oeffentliche-Verwaltung/Moderner-Staat/ElektronischeSignatur/Signaturanwendungen/signwpruefung.html>.
- ⁴ Die CovPassCheck-App ist ein Projekt im Auftrag des Bundesministeriums für Gesundheit. Die Anwendung wurde von den Unternehmen UBIRCH und IBM Deutschland entwickelt. Das Robert Koch-Institut ist als Herausgeber für die Ausgestaltung der Anwendung sowie für die sorgfältige Prüfung der Anforderungen an Datenschutz und Datensicherheit verantwortlich, Internet: <https://www.digitaler-impfnachweis-app.de/covpasscheck-app/>.
- ⁵ Vgl. zu „3G am Arbeitsplatz“ insoweit Aktuelle Kurz-Information 38 (Endnote 1), Nr. 3 d).