Bericht zur Datenschutz-Folgenabschätzung

Digitale COVID-Zertifikate (CovPass)

Version 1.4, 07.09.2021

1 Vorausgehende Hinweise

Dieses Dokument enthält die Version 1.4 des Berichts zur **Datenschutz-Folgenabschätzung (DSFA)**[1] für das Verfahren der Verarbeitung personenbezogener Daten im Rahmen der digitalen COVID-Zertifikate, das vom **Robert Koch-Institut (RKI)** im Auftrag der Bundesregierung durchgeführt wird.

Die DSFA wird laufend überprüft, um zu bewerten, ob die bisherigen DSFA-Ergebnisse weiterhin gültig sind oder eine Aktualisierung erforderlich ist. Daher handelt es sich bei dem vorliegenden DSFA-Bericht um ein „lebendiges Dokument", das von Zeit zu Zeit aktualisiert und in einer neuen Version zur Verfügung gestellt wird.

In diesem DSFA-Bericht wird ausschließlich aus Gründen der leichteren Lesbarkeit auf eine Verwendung von geschlechtsspezifischen juristischen und technischen Fachbegriffen und Personenbezeichnungen verzichtet (z. B. „Nutzer", „Angreifer"). Selbstverständlich bezieht sich der jeweilige Begriff auf Personen jeglicher Geschlechtsidentität.

[1] Aus Gründen der besseren Lesbarkeit werden die Begriffe „DSFA" und „DSFA-Bericht" nachfolgend teilweise synonym bzw. in Abhängigkeit des jeweiligen Kontexts verwendet.

Änderungshistorie

Änderung			Beschreibung der Änderung	Freigabe	Stadium
Nr.	Datum	Version			
1	22.05.2021	0.9	Finalisierung des vorläufigen DSFA-Berichts	-	-
2	31.05.2021	1.0	Erstellung DSFA Bericht 1.0	-	Final
3	17.06.2021	1.1	Berücksichtigung von Release 1.3	-	Final
4	31.07.2021	1.2	Berücksichtigung von Release 1.4, 1.5 und 1.6	-	Final
5	12.08.2021	1.3	Berücksichtigung von Release 1.7	-	Final
6	07.09.2021	1.4	Berücksichtigung von Release 1.8		Laufend

2 Inhalt

3 Über diesen DSFA-Bericht

3.1 Einleitung

Dieser Bericht dokumentiert die Ergebnisse der vom RKI durchgeführten DSFA für die unter Abschnitt 5 beschriebenen Verarbeitungsvorgänge.

Eine Herausforderung der DSFA und ihrer Dokumentation stellt das pandemiebedingt äußerst dynamische und schnelllebige Umfeld dar, wodurch im Projektverlauf laufend Risikobetrachtungen in Architekturentscheidungen eingeflossen sind, die bis zuletzt zu Änderungen geführt haben. In der vorliegenden DSFA wird der finale Stand der umfassenden Risikobetrachtungen zum aktuellen Release berücksichtigt und dokumentiert. Dies gilt insbesondere mit Blick auf die parallel zur DSFA-Durchführung stattgefundenen Verhandlungen zu der **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 15.6.2021, S. 1–22) (DCC-VO)**, die seit dem 1. Juli 2021 EU-weit anwendbar ist (Art. 17 DCC-VO). In Deutschland werden bereits seit dem 1. Juni 2021 auf Basis nationalen Rechts (§ 22 Abs. 5 bis 7 IfSG) sogenannte COVID-19-Zertifikate ausgegeben und verwendet, die den Anforderungen der DCC-VO entsprechen. Seit Geltung der DCC-VO können die bereits ausgegebenen nationalen COVID-19-Zertifikate daher sowohl für nationale Zwecke als auch für die Zwecke der DCC-VO verwendet werden (Art. 15 DCC-VO).

Nachfolgend werden sowohl die „COVID-19-Zertifikate“ im Sinne von § 22 IfSG als auch die „digitalen COVID-Zertifikate der EU“ im Sinne von Art. 2 Nr. 2 DCC-VO zusammenfassend als „digitale COVID-Zertifikate“ bezeichnet, sofern sich aus dem jeweiligen Verwendungskontext keine differenzierende Bedeutung ergibt. Entsprechendes gilt für die Begriffe „Impfzertifikat“, „Testzertifikat“ und „Genesenenzertifikat“.

Zur Verbesserung der Wirksamkeit, Transparenz und infolgedessen auch der Akzeptanz des Verfahrens zur Umsetzung der digitalen COVID-Zertifikate sind seitens des RKI Feedback und öffentliche Diskussionen gewünscht. Zielgruppe dieses DSFA-Berichts sind neben dem Verantwortlichen und den Entwicklern auch technische und juristische Experten, politische Entscheidungsträger und Datenschutzaufsichtsbehörden sowie Interessengruppen und sonstige Stakeholder.

Organisatorisch wurde sichergestellt, dass es bei der Durchführung der DSFA nicht zu Interessenkonflikten kommt und die Unabhängigkeit der Kontroll- und Prüfungsaufgabe gewahrt bleibt, indem externe Stellen mit der Durchführung dieses Prozesses beauftragt wurden und die behördliche Datenschutzbeauftragte des RKI nicht unmittelbar in die Durchführung der DSFA eingebunden war.

Seitens des RKI wurde Wert darauf gelegt, die öffentlichen Akteure eng in den Entwicklungsprozess einzubinden, um partizipativ mit breiter Expertise frühzeitig und schnell zu konsensfähigen Lösungen bezüglich der Anwendung von Datenschutzvorschriften und Bewertung von Risiken zu gelangen.

3.2 Name und Kontaktdaten des Verantwortlichen

Name / Bezeichnung der datenverarbeitenden Stelle	Robert Koch-Institut
Straße / Hausnummer	Nordufer 20
PLZ / Ort	13353 Berlin
Telefon	030 18754-0
Telefax	030 18754 2328
Internet-Adresse	www.rki.de

Leitung	Prof. Dr. Lothar H. Wieler, Präsident des RKI

Datenschutzbeauftragte	Claudia Enge
E-Mail-Adresse	datenschutz@rki.de

3.3 DSFA-Team

3.3.1 Rolle

Die DSFA wurde durch ein Team mit interdisziplinären Kompetenzen durchgeführt, dessen Mitglieder einerseits die verschiedenen Aspekte der für eine technische und datenschutzrechtliche Risikobewertung benötigten Fachkenntnisse abdecken, andererseits aber auch Bewertungen und Entscheidungen über Maßnahmen zur Risikominimierung sowie Bewertungen über deren Auswirkungen auf die digitalen COVID-Zertifikate treffen können. Durch die Einbindung der Entwicklerunternehmen bestand ein stetiger Austausch mit dem Entwicklerteam, so dass Zwischenergebnisse der DSFA laufend in Architekturentscheidungen einfließen konnten und die DSFA der umgesetzten Architektur entspricht.

3.3.2 Zusammensetzung

Das DSFA-Team setzt sich aus Vertretern des RKI und der Entwicklerunternehmen IBM Deutschland GmbH und Ubirch GmbH sowie Rechtsanwälten der Kanzlei Schürmann Rosenthal Dreyer Rechtsanwälte PartG mbB (im Auftrag des RKI) zusammen. Mit der

Durchführung der Risikoanalyse der technischen Aspekte des Prüfgegenstands hat das RKI die IBM Deutschland GmbH beauftragt. Die Zwischenergebnisse der DSFA wurden regelmäßig im Workstream Datenschutz abgestimmt. Die behördliche Datenschutzbeauftragte des RKI stand dem DSFA-Team beratend zur Seite, wobei eine regelmäßige Einbindung der Datenschutzbeauftragten in die Durchführung der DSFA nicht erfolgt ist, um die Unabhängigkeit bei der Prüfung der Ergebnisse der DSFA zu wahren.

Daneben hat das RKI den **Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI)** in Terminen am 17.04.2021, 12.05.2021, 25.05.2021 und 08.06.2021, 09.06.2021 sowie 02.8.2021 jeweils über den aktuellen Entwicklungsstand ausführlich unterrichtet und zu kritischen oder unklaren datenschutzrechtlichen Aspekten im Rahmen seiner gesetzlichen Aufgaben dessen Beratung in Anspruch genommen, so dass diese in der DSFA berücksichtigt werden konnten. Es wurde im Rahmen der Termine die geplante Architektur vor dem Hintergrund der DCC-VO vorgestellt und besprochen. Auch das geplante Setup des initialen Feldtests wurde vorab bei dem BfDI vorgestellt.

Auch nach Veröffentlichung des Release 1.0 wurde die Beratung des BfDI regelmäßig in Anspruch genommen, so dass geplante datenschutzrelevante Änderungen und Erweiterungen des Prüfgegenstands umfassend erörtert und die Beratungsergebnisse bei der Weiterentwicklung des Prüfgegenstands berücksichtigt werden konnten.

Abkürzungsverzeichnis

Begriff / Abkürzung	Bedeutung
BfDI	Bundesbeauftragter für den Datenschutz und die Informationsfreiheit
BMG	Bundesministerium für Gesundheit
Business Rules	Von den Mitgliedstaaten definierte Regelwerke über die Akzeptanzkriterien für Zertifikate
BSI	Bundesamt für Sicherheit in der Informationstechnik
CA	Certificate Authority
CWA	Corona-Warn-App
CBOR	Concise Binary Object Representation
CMS	Content Management System
COSE	CBOR Object Signing and Encryption
DCC-VO	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 15.6.2021, S. 1–22)
DRG	Deterministic Random Generator
DSGVO	Datenschutz-Grundverordnung
ECC	Elliptic Curve Cryptography
ECDH	Elliptic Curve Diffie Hellman (key exchange)
ECDSA	Elliptic Curve Digital Signature Algorithm
EDSA	Europäischer Datenschutzausschuss
FQDN	Fully Qualified Domain Name
GCM	Galois/Counter Mode
IAM	Identity and Access Management
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure (HTTP über TLS)

Begriff / Abkürzung	Bedeutung
IAM	Identity and Access Management
IBM	IBM Deutschland GmbH
IfSG	Infektionsschutzgesetz
JSON	JavaScript Object Notation
JWT	JSON Web Token
JWS	JSON Web Signature
KV	Kassenärztliche Vereinigung
mTLS	Mutual TLS
OCSP	Online Certificate Status Protocol
OIDC	OpenID Connect
PKI	Public-Key-Infrastruktur
PoC	Point of Certification
RKI	Robert Koch-Institut
RSA	Rivest-Shamir-Adleman (asymmetrisches Krypto-Verfahren)
SHA	Secure Hash Algorithm
SHA-256	SHA mit 256 Bit Hash-Wert
SMC-B	Security Module Card Typ B, Institutionenkarte
SNK	Sicheres Netz der KVen
SZZP	Sicherer Zentraler Zugangspunkt
TI	Telematikinfrastruktur
TLS	Transport Layer Security
TSL	Trust-service Status List
Value Set	Regelwerk, das die Interoperabilität der Zertifikate auf semantischer Ebene gewährleistet und eine einheitliche technische Umsetzung der DCC-VO ermöglicht.

Die vorstehenden Fachbegriffe und Abkürzungen werden bei erstmaliger Verwendung **fett** ausgeschrieben und die Abkürzung in Klammern angefügt.

4 Notwendigkeit der DSFA

Art. 35 Abs. 1 der Datenschutz-Grundverordnung (DSGVO) regelt die Pflicht zur Durchführung einer DSFA und schreibt diese vor, soweit aufgrund des Umfangs, Kontexts oder Zwecks der Verarbeitung personenbezogener Daten voraussichtlich ein hohes Risiko für die Rechte und Freiheiten der von der Datenverarbeitung betroffenen Personen besteht.

Zur weiteren Konkretisierung der gesetzlichen Anforderungen haben die Datenschutzaufsichtsbehörden gemäß Art. 35 Abs. 4 DSGVO Listen erstellt und veröffentlicht, in denen Datenverarbeitungsvorgänge benannt werden, für die jedenfalls eine DSFA durchzuführen ist (sogenannte „Muss-Listen“).

Der Prüfgegenstand unterfällt drei Datenverarbeitungsvorgängen auf der Muss-Liste des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit[2]:

> Es werden besondere Kategorien personenbezogener Daten nach Art. 9 Abs. 1 DSGVO verarbeitet, nämlich Gesundheitsdaten (Nr. 4 a.).
>
> Es handelt sich um eine Datenverarbeitung in einem großen Umfang, da mit einer hohen Verbreitung der digitalen COVID-Zertifikate und somit der Betroffenheit eines erheblichen Teils der Bevölkerung zu rechnen ist (Nr. 5).
>
> Bei der Verarbeitung werden neue Technologien oder organisatorische Lösungen in einer Art und Weise eingesetzt, die dem gegenwärtigen Stand der Technik voraus ist und deswegen die Abschätzung der Auswirkungen auf die Betroffenen und die Gesellschaft erschwert (Nr. 8). Zwar handelt es bei den Funktionalitäten und Komponenten der geplanten Lösung für sich genommen nicht um neue Technologien, und es gab bereits einzelne Projekte an verschiedenen Stellen, die App-basierte digitale Impf- oder Testnachweise zum Gegenstand hatten. Allerdings handelte es sich um Projekte, die auf bestimmte Regionen und vergleichsweise wenige Teilnehmer beschränkt waren, so dass Erfahrungswerte fehlen, die auf die bundesweite Einführung EU-weit interoperabler digitaler Zertifikate einer ungleich größeren Nutzerzahl übertragen werden könnten.

5 Beschreibung des Prüfgegenstands

Gegenstand der DSFA sind die nachfolgend beschriebenen Verarbeitungsvorgänge im Zusammenhang mit der Bereitstellung von digitalen COVID-Zertifikaten.

---

[2] BfDI: Liste von Verarbeitungsvorgängen gemäß Artikel 35 Abs. 4 DSGVO für Verarbeitungstätigkeiten öffentlicher Stellen des Bundes, Stand: Version 1.1-BfDI vom 01.10.2019, abrufbar unter: https://www.bfdi.bund.de/SharedDocs/Downloads/DE/Muster/Liste_VerarbeitungsvorgaengeArt35.pdf?__blob=publicationFile&v=5 (abgerufen am 15.06.2021).

Soweit auch Verarbeitungsvorgänge außerhalb des datenschutzrechtlichen Verantwortungsbereichs des RKI beschrieben werden, dient dies dem besseren Verständnis des Prüfgegenstands sowie der Nachvollziehbarkeit der Risikoanalyse, da diese auch Risikofaktoren außerhalb des Verantwortungsbereichs des RKI in den Blick nimmt. Darauf wird an entsprechender Stelle hingewiesen.

5.1 Hintergrund und Historie

Die vorliegende DSFA wurde im zeitlichen Zusammenhang mit der Erweiterung des IfSG im Hinblick auf die Erstellung und Bescheinigung von Impfungen sowie den negativen und positiven Erregernachweisen in §§ 22 Abs. 5 – 7 IfSG verfasst. Die Ausgabe der nationalen COVID-Zertifikate war damit bereits vor Verabschiedung der DCC-VO auf europäischer Ebene möglich. Nach Durchführung des Produktivtests an ausgewählten Standorten wurden die CovPass-App und die CovPassCheck-App mit Release 1.3 zu Beginn der Impfkampagne in Deutschland zur Verfügung gestellt. Der DSFA-Bericht wird sukzessive mit Erscheinen der weiteren Releases erweitert.

Ab Release 1.5 kann die CovPass-App die aktuellen „Value Sets“ interpretieren, über die die Darstellung der Inhalte der gespeicherten digitalen COVID-Zertifikate angepasst werden kann. Da die zu verwendenden Begrifflichkeiten in den verschiedenen Sprachfassungen der Zertifikate teilweise auf EU-Ebene bzw. von den anderen EU-Mitgliedsstaaten festgelegt werden, können auf diese Weise Änderungen ohne die Notwendigkeit einer Neuausstellung der Zertifikate oder neuer App-Releases berücksichtigt werden. Zum anderen wurde mit Release 1.5 die Funktion eingeführt, die Gültigkeit von digitalen COVID-Zertifikaten in der CovPass-App anhand der aktuell geltenden Business Rules der teilnehmenden Mitgliedstaaten prüfen zu können. Die Mitgliedstaaten können unterschiedliche Regeln dafür erlassen, unter welchen Voraussetzungen digitale COVID-Zertifikate als gültig akzeptiert werden. Mit Hilfe der Prüfung können Nutzer (z.B. im Zusammenhang mit der Reiseplanung) ermitteln, ob die gespeicherten digitalen COVID-Zertifikate zu einem bestimmten Zeitpunkt in einem Mitgliedsstaat voraussichtlich akzeptiert werden.

Mit Release 1.6 wurden die Apps für Nutzer auch in englischer Sprache verfügbar gemacht.

Mit dem anstehenden Release 1.7 wurde die CovPass-App um eine Funktion zum Exportieren von in der App bereits gespeicherten Impf- und Genesenenzertifikaten ergänzt („EU-Ausdruck“). Diese Funktion ermöglicht dem Nutzer die Erzeugung einer ausdruckbaren Papierversion eines Impf- oder Genesenenzertifikats im PDF-Format.

Mit Release 1.8 wurden Änderungen am Schema der Impfzertifikate für Auffrischungsimpfungen vorgenommen sowie die Namens-Darstellung in den Zertifikatdetails entsprechend der ICAO-Nomenklatur ergänzt.

5.2 Kontext der Datenverarbeitung

Mit den digitalen COVID-Zertifikaten wurden zunächst auf nationaler Ebene digitale Nachweismöglichkeiten für Impfungen, Genesungen und negative Testungen geschaffen. Die digitalen COVID-Zertifikate dienen daneben der Durchführung der DCC-VO. Die DCC-VO verpflichtet die Mitgliedsstaaten bzw. die zuständigen nationalen Behörden seit dem 1. Juli 2021 zur Ausstellung und Anerkennung des digitalen COVID-Zertifikats der EU (anfänglich als „digitales grünes Zertifikat“ bezeichnet) und soll den freien Personenverkehr während der COVID-19-Pandemie in der EU erleichtern. Ein digitales COVID-Zertifikat dient als Nachweis dafür, dass der Zertifikatsinhaber

- gegen COVID-19 geimpft ist (Impfzertifikat),
- negativ getestet wurde (Testzertifikat) oder
- von COVID-19 genesen ist (Genesungszertifikat).

Um eine Diskriminierung nicht geimpfter Personen zu verhindern, umfasst das digitale COVID-Zertifikat neben Impfzertifikaten auch Testzertifikate und Zertifikate für Personen, die von einer COVID-19-Erkrankung genesen sind. Alle Personen, die Inhaber eines COVID-Zertifikats sind, haben dieselben Rechte wie Bürger des jeweiligen besuchten Mitgliedstaats, die gegen COVID-19 geimpft sind, getestet wurden oder genesen sind.

Die DCC-VO ist sachlich nur auf grenzüberschreitende Sachverhalte anwendbar, denn sie bezieht sich nur auf die Ermöglichung des Rechts auf EU-Freizügigkeit. Rein nationale Zwecke fallen somit nicht in den Anwendungsbereich der DCC-VO. Die DCC-VO erwähnt in den ErwG 48 und 49 allerdings explizit, dass das digitale COVID-Zertifikat von den Mitgliedstaaten auch für nationale Zwecke verwendet werden kann, soweit dies im nationalen Recht vorgesehen ist.

Die DCC-VO schafft in ihrem Anwendungsbereich eine Rechtsgrundlage für die Verarbeitung personenbezogener Daten im Sinne von Art. 6 Abs. 1 lit. c und Art. 9 Abs. 2 lit. g DSGVO, die für die Ausstellung und Überprüfung der digitalen COVID-Zertifikate erforderlich sind (Art. 1 DCC-VO in Verbindung mit ErwG 48 DCC-VO).

Die Regelungen in § 22 Abs. 5 bis 7 IfSG betreffen hingegen die Verfahren und Zuständigkeiten bei der Ausstellung der deutschen digitalen COVID-Zertifikate (in § 22 IfSG als „COVID-19-Zertifikate“ bezeichnet). Die nationalen Rechtsgrundlagen ermöglichten damit zugleich die diesbezügliche Verarbeitung personenbezogener Daten durch das RKI schon in der Zeit vor dem Inkrafttreten der DCC-VO am 1. Juli 2021. Nach den Regelungen gem. § 22 Abs. 5 bis 7 IfSG werden die digitalen COVID-Zertifikate nicht automatisch, sondern nur „auf Wunsch“ des Geimpften/Getesteten/Genesenen ausgestellt.[3] Die geimpfte, getestete oder genesene Person hat somit einen Anspruch auf Ausstellung des Zertifikats.

[3] Art. 5 Abs. 1 und Art. 6 Abs. 1 DCC-VO sehen jeweils vor, dass Impf- und Testzertifikate „entweder automatisch oder auf Antrag“ der betreffenden Person ausgestellt werden.

In Deutschland wird den Bürgerinnen und Bürgern für die elektronische Nutzung der digitalen COVID-Zertifikate auf dem Smartphone durch das RKI die App „CovPass“ bereitgestellt. Durch die CovPass-App wird somit eine zusätzliche Möglichkeit zum (gelben) Impfausweis nach § 22 Abs. 1 IfSG bereitgestellt und eine Nachweismöglichkeit in Bezug auf den Impf-/Test-/Genesenenstatus auch für nicht grenzüberschreitende Sachverhalte geschaffen.

Das digitale COVID-Zertifikat darf nur auf Wunsch des Geimpften/Getesteten/Genesenen von den zur Bescheinigung von Impf-, Test- oder Genesenenstatus berechtigten Personen ausgegeben werden (§ 22 Abs. 5 bis 7 IfSG). Die zur Bescheinigung berechtigten Stellen sind die für die Durchführung der jeweiligen Impfung bzw. Testung berechtigten Personen sowie im Fall von nachträglich beantragten Impf- und Genesenenzertifikaten alle Ärzte und Apotheken. Das digitale COVID-Zertifikat wird dem potenziellen Zertifikatsinhaber in Papierform[4] ausgehändigt oder am Bildschirm oder elektronisch (beispielsweise im PDF-Format) zur Verfügung gestellt. Für die technische Erstellung und Generierung bzw. Ausstellung[5] des digitalen COVID-Zertifikats ist das RKI zuständig (§ 22 Abs. 5 bis 7 IfSG, dort jeweils Satz 3).

Jedes digitale COVID-Zertifikat enthält einen QR-Code, der das eigentliche digitale Zertifikat darstellt. Dieser QR-Code enthält in maschinenlesbarer Form Angaben zum jeweiligen Nachweisgegenstand (also zur Impfung und dem Impfstatus, dem Test und Testergebnis oder zur Genesung und dem Zeitpunkt, an dem eine Infektion festgestellt wurde) sowie den Namen und das Geburtsdatum des Zertifikatsinhabers (siehe 5.6.5**Fehler! Verweisquelle konnte nicht gefunden werden.**). Zum Auslesen des QR-Codes wird eine Software benötigt, die die Kodierung interpretieren kann, beispielsweise die CovPass-App und für die Prüfung eine Prüf-Anwendung wie beispielsweise die CovPassCheck-App des RKI.

Ein digitales COVID-Zertifikat kann vom Zertifikatsinhaber in Papierform und in elektronischer Form in einer geeigneten App verwendet werden. Um ein digitales COVID-Zertifikat elektronisch zu nutzen, muss der Zertifikatsinhaber den QR-Code mit der CovPass-App oder alternativ mit der Corona-Warn-App (ab CWA-Release 2.4) scannen. Die jeweilige App liest die Informationen aus dem QR-Code aus und speichert sie in einem gesicherten Bereich des Smartphones. Der Zertifikatsinhaber kann den QR-Code dann auf dem Bildschirm des Smartphones in Gestalt einer speziellen Prüfansicht anzeigen lassen und Dritten (z. B. Dienstleistern oder zuständigen Behörden) als Nachweis und zur Überprüfung mit einer geeigneten Prüfsoftware (z. B. CovPassCheck-App) vorlegen.

---

[4] Auch im Papierformat handelt es sich um ein „digitales“ COVID-Zertifikat, da es einen QR-Code mit einer digitalen (maschinenlesbaren) Repräsentation des Zertifikatsinhalts enthält und dieses dadurch für die elektronische Nutzung etwa auf einem Smartphone verfügbar macht.

[5] § 22 IfSG spricht von der „technischen Generierung“ der digitalen COVID-Zertifikate durch das RKI, wohingegen die DCC-VO von den für die „Ausstellung der Zertifikate […] zuständigen Behörden“ spricht. Es wird davon ausgegangen, dass beide Ausdrucksweisen den gleichen Sachverhalt, also insbesondere die elektronische Signierung der digitalen COVID-Zertifikate betreffen. Daher werden in diesem DSFA-Bericht beide Ausdrucksweisen synonym verwendet. Der Vorgang des „Ausstellens“ eines digitalen COVID-Zertifikats (durch das RKI) ist nicht mit dessen „Ausgabe“ an den Zertifikatsinhaber (durch berechtigte Ärzte, Testanbieter und Apotheker) zu verwechseln.

Daneben kann eine geimpfte Person ihren Impfstatus auch weiterhin mit dem Impfausweis oder einer sonstigen Impfbescheinigung nach § 22 Abs. 1 IfSG nachweisen oder das Impfzertifikat mit dem QR-Code in Papierform verwenden. Entsprechendes gilt für den Nachweis von negativen Testergebnissen und Genesungen.

Das Angebot des digitalen COVID-Zertifikats wird zeitlich begrenzt sein. Die konkrete Angebotsdauer ist noch nicht festgelegt und richtet sich maßgeblich nach den tatsächlichen und rechtlichen Entwicklungen im Zusammenhang mit dem Pandemiegeschehen auf nationaler und EU-Ebene. Aufgrund der in Art. 17 DCC-VO geregelten Anwendbarkeitsdauer bis zum 30. Juni 2022 wird zurzeit von einer Angebotsdauer von einem Jahr ausgegangen. Voraussichtlich wird die Angebotsdauer in Bezug auf die CovPass- und CovPassCheck-App jedoch kürzer sein, da die elektronische Patientenakte gemäß § 341 SGB V, die am 01.01.2022 eingeführt werden soll, eine mit dem Prüfungsgegenstand vergleichbare Funktionalität haben und diesen somit ersetzen soll.

5.3 Zweck der Datenverarbeitung

Die Datenverarbeitungsvorgänge im Rahmen des Prüfgegenstands dienen folgendem Zweck:

Personen, für die bestimmte Erleichterungen oder Ausnahmen von Schutzmaßnahmen des Bundes, der Länder oder in anderen EU-Mitgliedsstaaten zur Eindämmung der Corona-Pandemie gelten, soll eine einfache und EU-weit anerkannte Möglichkeit an die Hand gegeben werden, um nachzuweisen, dass sie von diesen Erleichterungen oder Ausnahmen erfasst sind.

Dieser Zweck umfasst auch die Durchführung der DCC-VO, welche die koordinierte Aufhebung von Beschränkungen des Rechts auf Freizügigkeit für Unionsbürger ermöglichen soll.

5.4 Funktionale Beschreibung

Nachfolgend erfolgt eine funktionale Beschreibung der Verarbeitungstätigkeiten bei der Erstellung, Ausgabe und Nutzung der vom RKI ausgestellten digitalen COVID-Zertifikate.

5.4.1 Anbindung der bescheinigenden Stellen an den Zertifikatsservice

Zunächst wird die Verarbeitungstätigkeit bei der technischen Anbindung der die digitalen COVID-Zertifikate bescheinigenden bzw. ausgebenden Stellen an den Zertifikatsservice des RKI betrachtet. Deren technische Anbindung ist eine Grundvoraussetzung für das Ausstellen von digitalen COVID-Zertifikaten, da in erster Linie die für die Durchführung der Impfungen bzw. Testungen verantwortlichen Stellen die digitalen COVID-Zertifikate ausgeben sollen (§ 22

Abs. 5 bis 7 IfSG, dort jeweils Satz 1).[6] Zudem können Impf- und Genesenenzertifikate auch nachträglich von Ärzten und in Apotheken ausgegeben werden. Eine nachträgliche Ausgabe von Testzertifikaten ist nicht vorgesehen.

Die zur Bescheinigung bzw. Ausgabe von digitalen COVID-Zertifikaten verpflichteten Personen, d. h. die gemäß § 22 Abs. 5 bis 7 IfSG zur Durchführung von Impfungen und Testungen berechtigten Personen üben ihre Tätigkeiten in unterschiedlichen Umfeldern aus. Dabei stellt insbesondere die Ärzteschaft keine einheitliche Berufsgruppe dar, da sich neben den niedergelassenen und Klinikärzten beispielsweise auch Betriebsärzte, Amtsärzte sowie Impfärzte in Impfzentren in teilweise erheblichem Umfang an der Durchführung von Schutzimpfungen beteiligen. Daher müssen unterschiedliche Einrichtungen mit einer heterogenen Softwarelandschaft technisch an den Zertifikatsservice angebunden werden:

- Impfzentren (nur Impfzertifikate)
- Arztpraxen (Impf-, Test- und Genesenenzertifikate)
- Apotheken (Impf- und Genesenenzertifikate)
- Teststellen (Testzertifikate)
- Betriebsärzte in Unternehmen
- Gesundheitsämter

Die technische Anbindung an den Zertifikatsservice erfolgt per Webbrowserüber über eine Web-Anwendung (der internen technischen Dokumentation entsprechend nachfolgend als Web-Frontend bezeichnet) oder über eine in die jeweilige Fachanwendung der ausgebenden Stelle integrierte Lösung, die jeweils über die Issuer Service API (diese ist Bestandteil des Health Certificate Issuance Service) auf den Zertifikatsservice zugreifen, wobei im Fall einer integrierten Lösung der Anbieter bzw. Betreiber der jeweiligen Fachanwendung ein beim RKI zu beantragendes mTLS-Zertifikat zur Authentifizierung gegenüber der Issuer Service API benötigt. Die konkrete technische Umsetzung unterscheidet sich im Übrigen je nach Zertifikatstyp und technischer Ausstattung der ausgebenden Stelle.

5.4.1.1 Anbindung von Impfzentren

Die Anbindung der Impfzentren erfolgt über einen Zugang für das Web-Frontend des Zertifikatsservice, der über das **Sichere Netz der KVen (SNK)**, welches über die TI erreichbar ist, bereitgestellt wird. Das RKI ist für den Betrieb der TI und ihre Verarbeitungsvorgänge nicht verantwortlich. Dieser DSFA liegt die Annahme zugrunde, dass die von den Impfzentren verwendeten Komponenten und Dienste der TI dem Stand der Technik entsprechend sicher und datenschutzrechtskonform von den jeweiligen Verantwortlichen betrieben werden (siehe hierzu unter 5.5.6).

Das Personal in Impfzentren kann auf den Zertifikatsservice nur per Web-Frontend nach Anmeldung bei einem persönlichen Benutzerkonto zugreifen, wobei eine X.509-Clientauthentifizierung (Gruppenzertifikat) und ein Authenticator in Form eines FIDO2-Sticks

[6] Vgl. auch die Anmerkung des Ausschusses für Gesundheit, BT-Drucksache 19/29870 S. 33.

als zusätzliche Faktoren zur Zugriffskontrolle verwendet werden. Die Benutzerkonten für die berechtigten Personen werden vom Impfzentrumsleiter über eine spezielle Benutzeroberfläche (PoC Manager, siehe 5.5.3.1.2) angelegt, da nur sein Benutzerkonto über die hierfür notwendigen erweiterten Berechtigungen verfügt.

Dieses Benutzerkonto wird dem Impfzentrumsleiter nach einer persönlichen Identifizierung über das Videoident-Verfahren des Anbieters WebID Solutions GmbH durch Bekanntgabe der Zugangsdaten sowie Bereitstellung der von den Clients der berechtigten Personen benötigten X.509-Clientzertifikate über den Datenaustauschdienst CryptShare zur Verfügung gestellt. Certificate Authority (CA) ist eine Intermediate-CA der Ubirch GmbH. Die X.509-Clientzertifikate müssen durch den Impfzentrumsleiter dann auf den Clients der berechtigten Personen manipulationssicher im Zertifikatsspeicher des Betriebssystems installiert werden.

5.4.1.2 Anbindung von Arztpraxen

Arztpraxen können über das Web-Frontend oder eine in ihr **Praxisverwaltungssystem (PVS)** integrierte Lösung auf den Zertifikatsservice zugreifen.

In beiden Fällen muss der Zugriff über die TI erfolgen. Der Zugriff über das Web-Frontend erfolgt über das **SNK**, welches über die TI angebunden ist. Der Zugriff über das PVS erfordert eine Anmeldung mittels des SMB-C-Verfahrens. Das Benutzerkonto für den Zertifikatsservice wird dabei aus dem Token bzw. der Zugriffsberechtigung für die TI abgeleitet.

Dieser DSFA liegt die Annahme zugrunde, dass die von den Arztpraxen verwendeten Komponenten und Dienste der TI dem Stand der Technik entsprechend sicher und datenschutzrechtskonform von den jeweiligen Verantwortlichen betrieben werden (siehe hierzu unter 5.5.6).

5.4.1.3 Anbindung von Apotheken

Apotheken können über eine in das **Verbändeportal der deutschen Apothekerschaft unter www.mein-apothekenportal.de (Apotheken-Verbändeportal)** integrierte Lösung auf den Zertifikatsservice zugreifen. Voraussetzung ist, dass die Apotheke im Apotheken-Verbändeportal angemeldet ist und das Modul für die Anforderung von digitalen COVID-Zertifikaten aktiviert hat.

Dieser DSFA liegt die Annahme zugrunde, dass die vom Apotheken-Verbändeportal verwendeten Komponenten und Dienste dem Stand der Technik entsprechend sicher und datenschutzrechtskonform von den jeweiligen Verantwortlichen betrieben werden.

5.4.1.4 Anbindung von Teststellen

Zugriff auf den Zertifikatsservice sollen grundsätzlich nur Teststellen erhalten, die nach § 6 Abs. 1 Satz 1 Nr. 1 und 3 der **Coronavirus-Testverordnung (TestV)** zur Durchführung von Bürgertestungen oder bestätigenden PCR-Testungen zugelassen sind (beispielsweise die zuständigen Stellen des öffentlichen Gesundheitsdienstes und die von ihnen betriebenen Testzentren sowie die von den KVen betriebenen Testzentren) und die von diesen gemäß § 6 Abs. 1 Satz 1 Nr. 2 TestV mit der Durchführung von Testungen beauftragten Dritten (beispielsweise Apotheken, medizinische Labore und sonstige qualifizierte Anbieter). Daneben sollen auch Anbieter von Softwarelösungen/PoC-Systemen für Teststellen Zugriff auf den Zertifikatsservice erhalten, so dass auch deren Anwender (also die nach § 6 Abs. 1 TestV zugelassenen bzw. beauftragten Teststellen ohne eigene Fachanwendung) Testzertifikate anfordern und an ihre Kunden (Testpersonen) ausgeben können.

Teststellen werden, sofern sie nicht bereits als Arztpraxen oder Apotheken an den Zertifikatsservice angebunden und insoweit zum Anfordern von Testzertifikaten in der Lage sind, über das Web-Frontend und integrierte Lösungen angebunden.

Außerdem haben Teststellen und insbesondere Labore, die auf Basis eines Anbindungsvertrags mit der T-Systems an das CWA-System (Test Result Server der CWA) angebunden sind und auf diesem Wege Antigen-Schnelltest- und PCR-Testergebnisse an das RKI übermitteln, seit dem CWA-Release 2.4 auch die Möglichkeit zum Anfordern eines Testzertifikats bei dem Zertifikatsservice. CWA-Nutzer können dann in der CWA im Rahmen der Registrierung eines Coronatests für den Fall eines negativen Testergebnisses die Ausstellung eines entsprechenden Testzertifikats beantragen.

5.4.1.5 Anbindung von Betriebsärzten

Betriebsärzte können nur über eine in eine Fachanwendung integrierte Lösung bzw. über die Issuer Service API auf den Zertifikatsservice zugreifen. Neben den bereits verfügbaren Standardlösungen mit integrierter Anbindung an den Zertifikatsservice können Betriebsärzte somit grundsätzlich auch eine eigene betriebsärztliche Fachanwendung verwenden, sofern diese mit einer Schnittstelle zur Issuer Service API ausgestattet worden und der Betreiber vom RKI zu deren Nutzung zugelassen[7] worden ist.

5.4.1.6 Anbindung von Gesundheitsämtern

Amtsärzte und weiteres impf- oder testberechtigtes Personal der Gesundheitsämter können nur über das Web-Frontend nach Anmeldung bei einem persönlichen Benutzerkonto auf den Zertifikatsservice zugreifen, wobei eine X.509-Clientauthentifizierung (Gruppenzertifikat) und

[7] Das heißt, dass das RKI dem Betreiber der jeweiligen Fachanwendung das zur Authentifizierung des Fachanwendungs-Backends gegenüber der Issuer Service API erforderliche mTLS-Zertifikat nach entsprechender Beantragung und Prüfung ausgestellt hat.

ein Authenticator in Form eines FIDO2-Sticks als zusätzliche Faktoren zur Zugriffskontrolle verwendet werden. Die Benutzerkonten für die berechtigten Personen werden von dem IT-Verantwortlichen über den PoC Manager (siehe 5.5.3.1.2) angelegt, da nur sein Benutzerkonto über die hierfür notwendigen erweiterten Berechtigungen verfügt. Insoweit entspricht das Verfahren auch im Übrigen dem Verfahren bei der Anbindung von Impfzentren, so dass auf die Darstellung unter 5.4.1.1 entsprechend verwiesen werden kann.

5.4.2 Erstellung von digitalen COVID-Zertifikaten

Wenn eine Person die Ausstellung eines digitalen COVID-Zertifikats wünscht und ihre Berechtigung durch Vorlage der gemäß § 22 Abs. 5 bis 7 IfSG jeweils erforderlichen Impf- oder Testdokumentation nachweist, muss das jeweilige digitale COVID-Zertifikat von der bescheinigenden und ausgebenden Stelle bei dem Zertifikatsservice unter Angabe der jeweils erforderlichen Daten zum Impf-, Test- oder Genesungsstatus angefordert werden. Der diesbezügliche Prozess sieht vor, dass dem Geimpften oder Getesteten von dem Personal der das digitale COVID-Zertifikat ausgebenden Stelle zunächst die Datenschutzhinweise zum COVID-Zertifikat ausgehändigt werden. Der Antragsteller erhält somit Gelegenheit diese zu lesen, eventuelle Fragen zu stellen und schließlich seinen Wunsch nach Ausstellung des digitalen COVID-Zertifikats mündlich zu äußern.

Zudem besteht die Möglichkeit, über die **Corona-Warn-App (CWA)**[8] ein Testzertifikat zu einem in der CWA registrierten Test anzufordern.

Die weiteren Vorgehensschritte hängen davon ab, auf welche Weise die das digitale COVID-Zertifikat ausgebende Stelle auf den Zertifikatsservice zugreift.

5.4.2.1 Zugriff per Web-Frontend

Nach der Anmeldung im Web-Frontend des Zertifikatsservices über den Browser (in Abbildung 1 als WebApp bezeichnet) muss das Personal der ausgebenden Stelle die Funktion für die Anforderung des jeweiligen Zertifikatstyp aufrufen und die Eingabemaske mit den für das jeweilige digitale COVID-Zertifikat notwendigen Daten zum Impf-, Test- oder Genesenenstatus des Antragstellers ausfüllen. Das Web-Frontend erzeugt auf Grundlage dieser Daten die eindeutige Zertifikatskennung und leitet aus dieser und den Angaben zum Impf-, Test- oder Genesenenstatus einen eindeutigen Hash-Wert ab. Als Hash-Algorithmus wird SHA-256 eingesetzt. Diese Datenverarbeitung findet ausschließlich lokal im Webbrowser statt, d. h. es werden zunächst keine Daten an den Zertifikatsservice übermittelt.

[8] Die CWA ist nicht vom Prüfungsgegenstand dieser DSFA umfasst. Die Funktion der CWA App zur Speicherung eines digitalen COVID-Zertifikats ist Gegenstand der DSFA für das CWA-Release 2.4.

Nach der Ableitung des Hash-Werts wird dieser an den Endpunkt der Issuer Service API für das Web-Frontend übermittelt, der mit dem Health Certificate Issuance Service und dem Signing Service eine digitale Signatur erstellt.

Der Health Certificate Issuance Service nimmt den Hash-Wert entgegen und übergibt ihn dem Signing Service. Der Signing Service erzeugt eine Signatur, indem er den Hash-Wert mit dem für die jeweilige ausgebende Stelle aktuell genutzten privaten Schlüssel des Siegel-Zertifikats des RKI verschlüsselt. Die Signierung erfolgt in Form einer auf Kryptografie mit elliptischen Kurven basierenden Verschlüsselung (ECDSA-Signatur) des Hash-Wertes entsprechend den Vorgaben und Empfehlungen der Technischen Richtlinie BSI TR-03111.

Die Signatur wird sodann über die Issuer Service API an das Web-Frontend zurückgegeben. Dieses generiert anhand der lokal vorliegenden Daten (Zertifikatsaussage, Hash-Wert, elektronische Signatur) den QR-Code des COVID-Zertifikats. Das aus diesen Elementen zusammengesetzte digitale COVID-Zertifikat wird schließlich von dem Personal der ausgebenden Stelle ausgedruckt und dem Antragsteller bzw. nunmehrigen Zertifikatsinhaber übergeben.

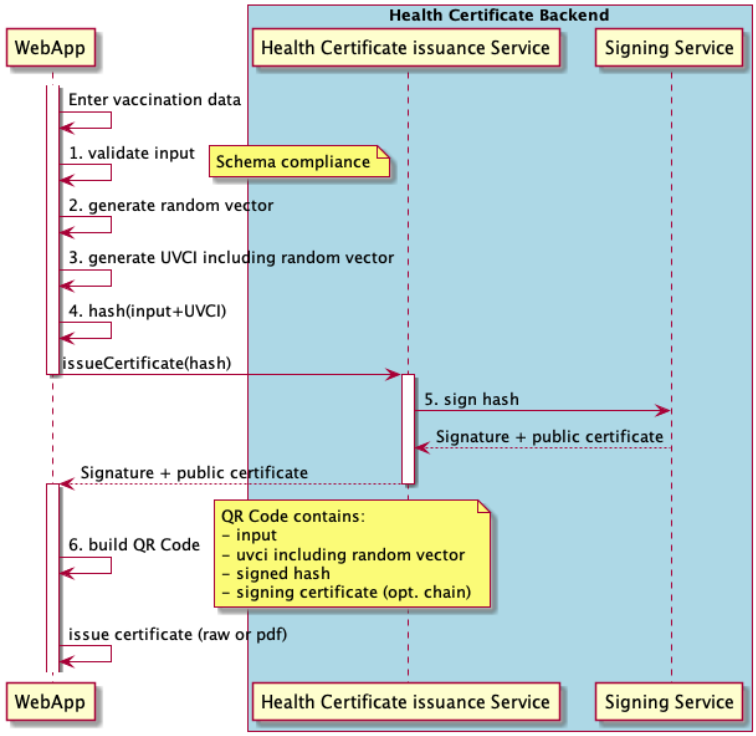

Abb. 1: Ablauf der Zertifikatserstellung über Web-Frontend (am Beispiel eines Impfzertifikats)

Sofern der Zugriff über das Web-Frontend nicht durch die TI (SNK oder SMB-C-Verfahren) erfolgt oder es sich um ein Impfzentrum handelt, werden zur Authentifizierung neben persönlichen Zugangsdaten mTLS mit X.509-Zertifikate und ein FIDO2-Stick als zusätzliche Faktoren zur Zugriffskontrolle verwendet, die der bescheinigenden Stelle auf Antrag zur Verfügung gestellt werden (sofern die bescheinigende Stelle ihre Berechtigung zur Ausgabe der betreffenden digitalen COVID-Zertifikate nachgewiesen hat).

5.4.2.2 Zugriff über Fachanwendung

Wenn der Zugriff auf den Zertifikatsservice über eine in die Fachanwendung der bescheinigenden Stelle integrierte Lösung erfolgt (z. B. PVS oder Apotheken-Verbändeportal), müssen die dort für das jeweilige digitale COVID-Zertifikat notwendigen Daten mit der entsprechenden Zertifikatsanforderung an den Endpunkt der Issuer Service API für die betreffende Anwenderkategorie übermittelt und von diesem durch den Health Certificate Issuance Service zunächst gehasht werden. Ein lokales Hashing in der jeweiligen Fachanwendung ist in dieser Konstellation – anders als bei dem Zugriff über das Web-Frontend – zurzeit nicht geplant, da aufgrund der heterogenen Softwarelandschaft die Entwicklung eines zuverlässigen und sicheren lokalen Zertifikatserstellungsprozesses mit allen relevanten Fachanwendungen und Systemen in der pandemiebedingt erforderlichen Kurzfristigkeit nicht gewährleistet werden kann.

Der Health Certificate Issuance Service übergibt den berechneten Hash-Wert an den Signing Service. Dort wird der Hash in eine Signatur übersetzt (s.o.) und diese dann an den Health Certificate Issuance Service zurückgegeben. Der Health Certificate Issuance Service erstellt dann das digitale COVID-Zertifikat und übergibt dieses der jeweiligen Fachanwendung (in Abbildung 2 als „PVS/SDK“ bezeichnet). Das digitale COVID-Zertifikat wird schließlich vom Personal der ausgebenden Stelle ausgedruckt und dem Zertifikatsinhaber übergeben und/oder in elektronischer Form auf einem Bildschirm als QR-Code angezeigt, so dass der Zertifikatsinhaber es mit der CovPass-App oder der CWA elektronisch speichern kann.

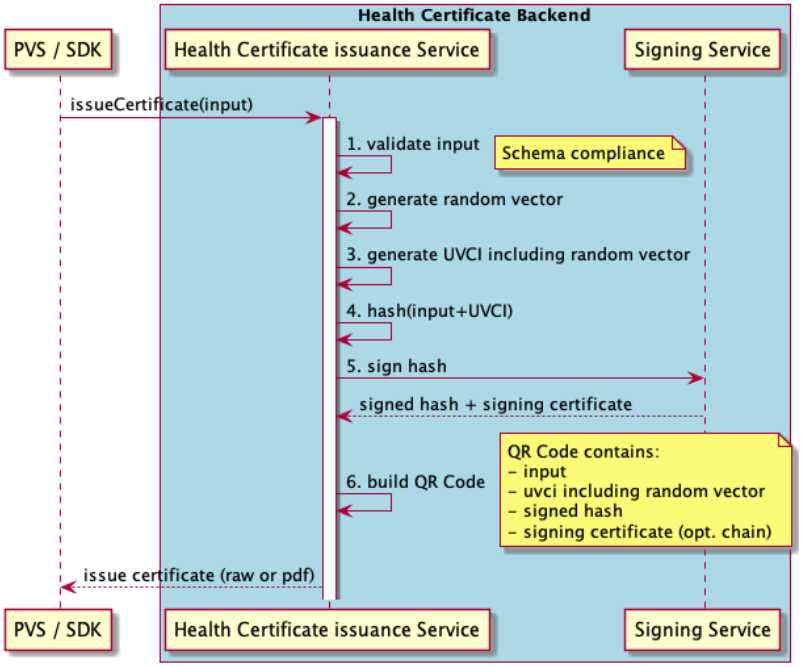

Abb. 2: Ablauf der anwendungsintegrierten Zertifikatserstellung

Zur Authentifizierung des PVS bzw. des Backend-Systems der Fachanwendung an der Issuer Service API des Zertifikatsservice wird das mTLS-Verfahren mit X.509-Zertifikaten verwendet, die der bescheinigenden Stelle auf Antrag des jeweiligen Anwenders/Betreibers nach einer Einzelfallprüfung durch das RKI zur Verfügung gestellt werden, nachdem der Antragsteller seine Berechtigung zur Ausgabe der betreffenden digitalen COVID-Zertifikate nachgewiesen

hat. Handelt es sich bei dem Antragsteller um einen Software-/Systembetreiber, der selbst keine digitalen COVID-Zertifikate ausgibt, erfordert die Ausgabe eines X.509-Zertifikats den Abschluss eines Vertrags, in dem sich der Antragsteller gegenüber dem RKI zu angemessenen Maßnahmen für die Überprüfung der Berechtigung der Anwender zur Ausgabe der betreffenden digitalen COVID-Zertifikate verpflichten muss.

5.4.2.3 Zugriff über das CWA-System

Damit der Zugriff durch eine Teststelle über das CWA-System erfolgen kann, wurde das CWA-Serversystem mit dem CWA-Release 2.4 um eine weitere Komponente erweitert. Dieser CWA DCC Server ist an den Zertifikatsservice angebunden. Auch wenn es sich bei dem CWA-System auf technischer Ebene um das Backend-System einer Fachanwendung für Teststellen handelt, erfolgt die Anbindung nicht über einen der regulären Issuer-Service-API-Endpunkte für integrierte Lösungen (z. B. ein PVS), sondern über eine funktional mit der Web-Frontend-API vergleichbare Hash-API, die auf den Health Certificate Issuance Service zugreift.

Der CWA DCC Server erzeugt auf Grundlage der im CWA-System vorliegenden Daten die eindeutige Zertifikatskennung und leitet aus dieser und den Angaben zum Teststatus des CWA-Nutzers einen eindeutigen Hash-Wert ab und gibt diesen an die hierfür vorgesehene CWA-API des Health Certificate Issuance Service weiter. Als Hash-Algorithmus wird SHA-256 eingesetzt. Die weitere Verarbeitung durch den Zertifikatsservice entspricht derjenigen beim Einsatz des Web-Frontends mit der Maßgabe, dass der CWA DCC Server die Aufgaben des Web-Frontends übernimmt und das von ihm technisch generierte Testzertifikat in elektronischer Form an die CWA des CWA-Nutzers übermittelt, der das Testzertifikat angefordert hat.

Zur Authentifizierung des CWA DCC Servers am CWA-API-Endpunkt des Zertifikatsservice wird das mTLS-Verfahren mit X.509-Zertifikaten verwendet

Die Datenverarbeitung durch die CWA-Komponenten ist Gegenstand der DSFA für das CWA-Release 2.4 und daher kein Bestandteil dieses DSFA-Berichts.

5.4.3 Speicherung des digitalen COVID-Zertifikats in der CovPass-App

Um eine elektronische Version des digitalen COVID-Zertifikats auf dem Smartphone speichern zu können, muss zunächst die CovPass-App oder eine andere Wallet-App (z. B. CWA) installiert werden. Die CWA und die Speicherung der COVID-Zertifikate in der CWA gehören nicht zum Prüfgegenstand dieser DSFA.

Die CovPass-App wird vom RKI in den deutschen Versionen der App-Stores von Google (Play Store), Apple (App Store) und Huawei (Huawei AppGallery) kostenlos bereitgestellt. Auf der App-Store-Beschreibungsseite der CovPass-App kann der Nutzer vor dem Download die Datenschutzerklärung und eine Zusammenfassung der wesentlichen Funktionen und Merkmale der CovPass-App aufrufen. Falls die CovPass-App nicht auf dem Smartphone oder

Betriebssystem betrieben werden kann (z. B. weil das Gerätemodell nicht unterstützt wird), kann die CovPass-App nicht installiert werden. Nach Abschluss des Downloads wird die CovPass-App automatisch auf dem Smartphone installiert und kann anschließend jederzeit benutzt werden.

Nachdem ein Zertifikatsinhaber den Onboarding-Prozess durchlaufen hat, kann er mittels der Funktion „Zertifikat hinzufügen“ digitale COVID-Zertifikate in die CovPass-App überführen und somit auch elektronisch nutzen. Hierzu muss er mit der Kamera seines Smartphones den auf dem digitalen COVID-Zertifikat enthaltenen QR-Code einscannen. Die CovPass-App prüft mit Hilfe des öffentlichen Schlüssels, ob die Signatur von der das Zertifikat ausstellenden Stelle stammt. Anschließend wird in der CovPass-App der Status zu der betreffenden Impfung, Testung oder Genesung angezeigt. Die Anzeige erfolgt entsprechend den von der ausstellenden Stelle veröffentlichten Value Sets. Die Value Sets werden aktualisiert, wenn der Nutzer die Zertifikatsübersicht aufruft und eine Internetverbindung zur Verfügung steht. Es wird eine Anfrage zum Herunterladen des aktuellen Value Sets an den Zertifikatsservice gesendet. Sollte das Value Set seit dem letzten Download aktualisiert worden sein, wird das aktuelle Paket heruntergeladen.

Der Nutzer der CovPass-App kann elektronisch gespeicherte digitale COVID-Zertifikate jederzeit löschen.

Für jede einzelne Impfung (auch im Fall von Folge- oder Auffrischimpfungen einer bereits bescheinigten Impfung), Testung oder Genesung muss gemäß Art. 3 Abs. 3 DCC-VO ein neues, eigenständiges digitales COVID-Zertifikat ausgestellt werden. Die vorstehende Beschreibung gilt daher entsprechend bei der Speicherung von weiteren eigenen COVID-Zertifikaten sowie gegebenenfalls bei der Speicherung von digitalen COVID-Zertifikaten von anderen Personen (z. B. minderjährige Familienmitglieder ohne eigenes Smartphone).

5.4.4 Verwendung des digitalen COVID-Zertifikats zu Nachweiszwecken

Um mittels eines COVID-Zertifikats den Impf-, Test- oder Genesenenstatus gegenüber einem Dritten nachzuweisen, kann der Zertifikatsinhaber den erhaltenen QR-Code vorzeigen, so dass der Dritte ihn mit einem Prüf-System, bestehend aus einem QR-Code-fähigen Scanner und einer Anwendung, die den gescannten QR-Code interpretieren kann, wie beispielsweise der CovPassCheck-App, auf Gültigkeit überprüfen kann. Es sind sowohl stationäre als auch mobile, also App-basierte Prüf-Systeme möglich. Stationäre Prüfsysteme könnten beispielsweise in Ausweisscanner, wie sie im Reisebereich üblich sind, integriert werden. Die CovPassCheck-App ist ebenso wie die CovPass-App kostenlos in den App-Stores erhältlich. Die Nutzung der CovPassCheck-App erfordert keine Registrierung oder Anmeldung.

Der Zertifikatsinhaber kann der prüfenden Stelle den QR-Code in Papier- oder digitaler Form in der CovPass-App vorlegen. In der CovPass-App steht hierzu die Funktion „Aktuellen QR-Code anzeigen“ zu dem entsprechenden digitalen COVID-Zertifikat zur Verfügung. Daraufhin werden auf dem Bildschirm des Smartphones eine großformatige Abbildung des QR-Codes, sowie der Name und das Geburtsdatum des Zertifikatsinhabers angezeigt. Zusätzlich hat der

Zertifikatsinhaber auch die Möglichkeit eine isolierte Darstellung des QR-Codes in der CovPass-App aufzurufen und diese zur Prüfung vorzulegen.

Die prüfende Stelle kann den QR-Code mit einem Prüfsystem scannen und das darin kodierte digitale COVID-Zertifikat (siehe 5.6.4) für die Dauer des Prüfvorgangs temporär in den Speicher des Prüfsystems übertragen, um über die Signatur und den signierten Hash-Wert anhand der Public Keys des verwendeten, in der Prüfanwendung lokal gespeicherten gültigen Siegel-Zertifikates die Authentizität und Integrität eines vorgezeigten digitalen COVID-Zertifikats zu validieren.

Gemäß der Forderung in ErwG 22 DCC-VO werden die jeweils aktuellen, gültigen Siegel-Zertifikate regelmäßig von dem CA Distribution Service in das Prüfsystem geladen und von diesem lokal gespeichert, so dass digitale COVID-Zertifikate – da in der konkreten Prüfungssituation nun kein Serverzugriff mehr notwendig ist – auch offline überprüft werden können. Ebenso lädt die CovPassCheck-App regelmäßig die aktuellen deutschen Business Rules herunter, um auch diese im Rahmen der Prüfung berücksichtigen zu können. Die geladenen und lokal gespeicherten Siegel-Zertifikate und Business Rules enthalten keine personenbezogenen Daten. Der Zeitpunkt der letzten Aktualisierung der Siegel-Zertifikate wird in der CovPassCheck-App angezeigt.

Die CovPassCheck-App zeigt dem Nutzer nach dem Scannen eines QR-Codes an, ob das vorgelegte digitale COVID-Zertifikat gültig ist. Im Falle eines gültigen digitalen COVID-Zertifikats wird zusätzlich der Name und das Geburtsdatum des Zertifikatsinhabers mitgeteilt, so dass die prüfende Stelle in Verbindung mit einem Identitätsnachweis (siehe 5.6.8) ggf. feststellen kann, ob der das digitale COVID-Zertifikat vorzeigende Nutzer tatsächlich die Person ist, auf die sich die Zertifikatsaussage bezieht. Bei einem ungültigen digitalen COVID-Zertifikat unterbleibt die Anzeige von Namen und Geburtsdatum, da das mit der Vorlage des COVID-Zertifikats angestrebte Ziel des Nutzers unabhängig von der Bekanntgabe dieser Daten nicht mehr erreicht werden kann und die Bekanntgabe somit nicht erforderlich ist. Zusätzlich wird in der CovPassCheck-App angezeigt, ob es sich um ein Testzertifikat handelt oder nicht. Bei Testzertifikaten wird dann auch der Zeitpunkt der Probenahme angezeigt, damit die prüfende Person beurteilen kann, ob das zugrunde liegende Testergebnis noch gültig ist. Zwischen Impf- und Genesenenzertifikate wird bei der Anzeige des Prüfergebnisses nicht differenziert.

Eine dauerhafte Speicherung der gescannten digitalen COVID-Zertifikate in der CovPassCheck-App oder auf einem Serversystem des RKI erfolgt im Rahmen der Prüfung nicht. Der Identitätsnachweis sowie das ausgelesene digitale COVID-Zertifikat können und dürfen mit der CovPassCheck-App oder anderen im Einklang mit der DCC-VO gestalteten Prüf-Systemen im Anwendungsbereich der DCC-VO nicht über den konkreten Prüfvorgang hinaus gespeichert werden (Art. 10 Abs. 3 DCC-VO). Auf rein technischer Ebene wäre dies jedoch möglich, worauf im Rahmen der Risikoanalyse eingegangen wird.

5.4.5 Exportieren eines digitalen COVID-Zertifikats (EU-Ausdruck)

Seit Release 1.7 kann der Nutzer mit der Funktion „EU-Ausdruck“ von einem in der CovPass-App gespeicherten, gültigen Impf- oder Genesenenzertifikat eine ausdruckbare PDF-Version erzeugen, die dann über die Teilen-Funktion des jeweiligen Betriebssystems an eine PDF-fähige Systemfunktion (z. B. AirPrint) oder App übergeben und ausgedruckt werden kann. Das von der CovPass-App generierte PDF-Dokument wird lokal im Smartphone auf Basis der zum jeweiligen Zertifikat gespeicherten Zertifikatsaussagen erzeugt und basiert auf der in der CovPass-App hinterlegten „offiziellen“ Dokumentenvorlage des RKI, die auch der Zertifikatsservice bzw. das Web-Frontend zur Zertifikatsgenerierung verwendet. Somit ist das ausgedruckte PDF-Dokument formal und inhaltlich mit der bspw. von einer an den Zertifikatsservice angebundenen Arztpraxis oder Apotheke ausgegebenen Papierversion des digitalen COVID-Zertifikats identisch. Nachdem das PDF-Dokument aus der CovPass-App exportiert worden oder der Exportvorgang vom Nutzer abgebrochen wird (etwa durch Schließen des Teilen-Menüs des Betriebssystems), wird das PDF-Dokument aus dem App-Speicher gelöscht.

Der Export von Testzertifikaten und ausländischen, d. h. nicht vom RKI elektronisch signierten digitalen COVID-Zertifikaten ist nicht möglich.

Da das lokal erzeugte PDF-Dokument personenbezogene Gesundheitsdaten des Zertifikatsinhabers (Zertifikatsaussage) enthält, erfolgt in der CovPass-App vor dem Export vorsorglich ein Hinweis auf die Vertraulichkeitsrisiken bei einem Teilen des PDF-Dokuments mit Dritten. Zudem soll der Nutzer auch durch die Bezeichnung als „EU-Ausdruck“ daran erinnern werden, dass der Zweck der Exportfunktion in erster Linie darin besteht, bei Bedarf die Herstellung einer Papierversion eines digitalen COVID-Zertifikats zu ermöglichen.

5.4.6 Prüfung der Gültigkeit des Zertifikats

Seit Version 1.5 der CovPass-App kann der Nutzer zudem die Gültigkeit der Zertifikate in der CovPass-App überprüfen. So kann der Nutzer (z.B. im Rahmen der Reiseplanung) ermitteln, ob die Zertifikate in einem bestimmten Land zu einem bestimmten Zeitpunkt wahrscheinlich als Nachweis akzeptiert werden.

Der Nutzer löst die Prüfung aus, indem er in der Zertifikat-Übersicht den Button „Gültigkeit prüfen“ antippt. Anschließend muss der Nutzer das Land auswählen, dessen Gültigkeitsregeln (Business Rules) berücksichtigt werden sollen und das Datum festlegen, für das die Gültigkeitsprüfung durchgeführt werden soll. Die App lädt dann die Gültigkeitsregeln der Mitgliedstaaten vom Zertifikatsservice herunter. Es werden immer die Regelwerke sämtlicher Mitgliedstaaten heruntergeladen. Das Laden des Gesamtpaketes verhindert, das anhand der Anfragen auf dem Server Reiserouten einzelner Nutzer nachvollzogen werden können. Die Prüfung der Zertifikate gegen die Business Rules des ausgewählten Mitgliedstaates findet lokal auf dem Endgerät des Nutzers statt. Anschließend wird dem Nutzer angezeigt, ob das geprüfte Zertifikat dem Regelwerk des gewählten Mitgliedstaates entspricht. Ist das nicht der

Fall, wird dem Nutzer auch mitgeteilt, welche Regeln nicht eingehalten werden bzw. welche Regeln nicht geprüft werden konnten.

5.4.7 Technischer Support

Das RKI betreibt jeweils eine Hotline für die Nutzer der CovPass- und der CovPassCheck-App (Bürger-Hotlines) sowie die Anwender des Zertifikatsservice, die bei technischen Fragen kostenlos kontaktiert werden kann. Jede Hotline verfügt über eine eigene Telefonnummer, die auf der CovPass-Website des RKI bekanntgegeben wird. Die Hotlines werden von zwei externen Callcenter-Dienstleistern im Auftrag des RKI betrieben (siehe 5.8.7).

Die Hotlines bieten keine medizinische Beratung an. Die Systeme der Hotlines haben keine Verbindung zu den übrigen Komponenten und Systemen des Prüfungsgegenstands.

Die Callcenter-Betreiber haben sich gegenüber dem RKI verpflichtet, keine personenbezogenen Daten von Personen in der Rolle eines Zertifikatsinhabers zu erfassen, die eventuell von einem anrufenden Zertifikatsinhaber selbst oder von anderen Anrufern (z. B. Personal der Impfstellen) eigeninitiativ mitgeteilt werden. Darüber hinaus hat sich der für die Bürger-Hotlines zuständige Callcenter-Betreiber gegenüber dem RKI verpflichtet, keine personenbezogenen Anruferdaten (z. B. Telefonnummern) über die Dauer des jeweiligen Telefongesprächs hinaus zu speichern.

Zu den Büros der Callcenter-Betreiber haben nur ausgewählte und zugewiesene Personen Zutritt. Im Hinblick auf das Homeoffice-Gebot findet eine Verarbeitung außerhalb dieser Büros nur ausnahmsweise mit der Maßgabe statt, dass Zugriffe auf die Telekommunikationssysteme der Hotlines nur unter Verwendung einer gesicherten Verbindung (VPN) erfolgen. Die Personen, die die Hotlines betreuen, werden ausschließlich durch die jeweils verantwortlichen Projekt- und Teammanager benannt. Das Hotline-Personal erhält ausschließlich Anrufe zu dem Supportgegenstand der jeweiligen Hotline (CovPass-App, CovPassCheck-App oder Zertifikatsservice).

5.5 Systemarchitektur

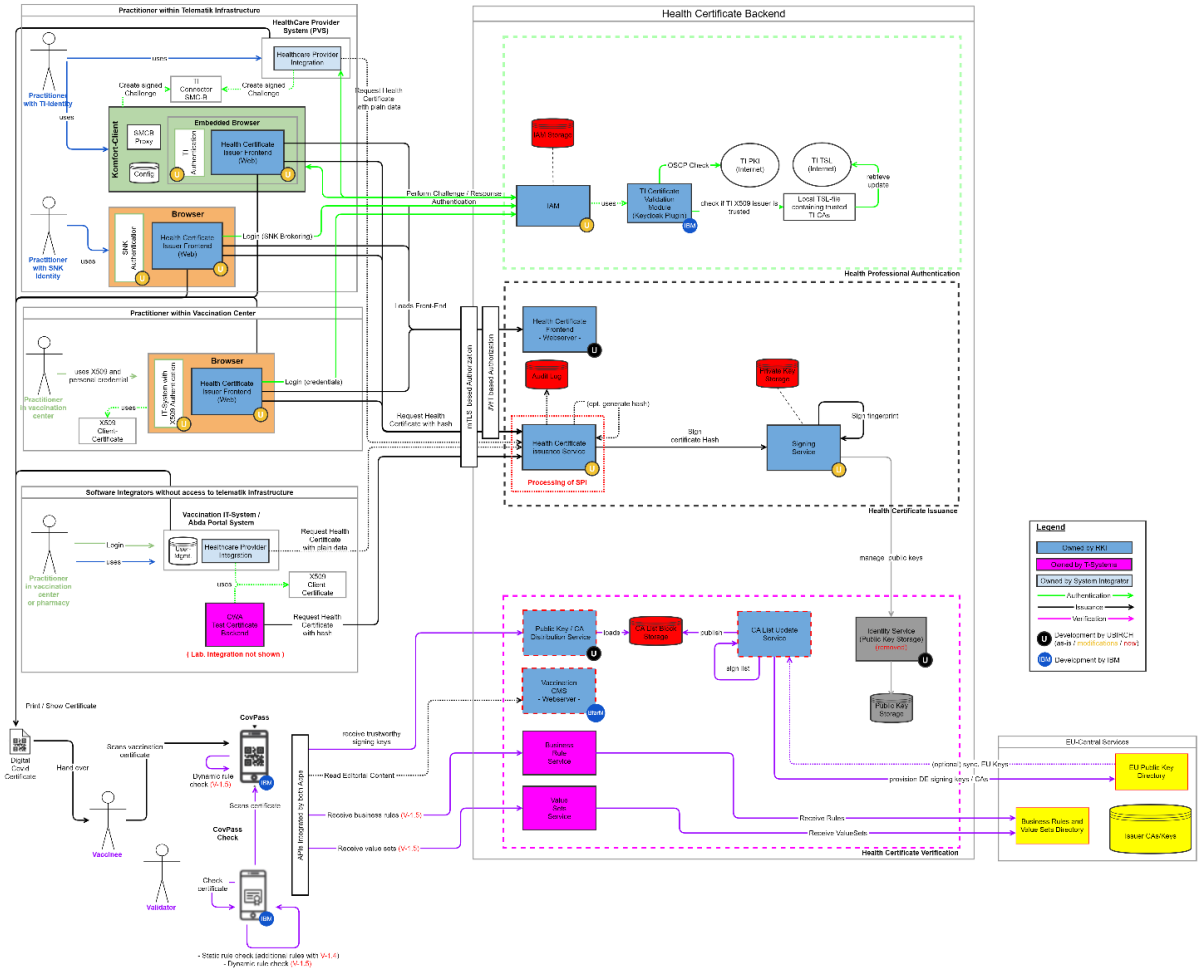

Abb. 3: Architekturüberblick

Nachfolgend werden die Systeme, Dienste und Schnittstellen des Prüfgegenstands beschrieben. Die technische Lösung des RKI für CovPass besteht in erster Linie aus drei Komponenten, nämlich

- einer Wallet-App zur elektronischen Nutzung von digitalen COVID-Zertifikaten (CovPass-App),
- einer Prüfungs-App zur Prüfung der Gültigkeit von digitalen COVID-Zertifikaten (CovPassCheck-App) und
- dem Zertifikatsservice zur technischen Erstellung der COVID-Zertifikate.

Wie bei der CWA sollen die Quellcodes dieser technischen Kernkomponenten bei GitHub veröffentlicht.

5.5.1 Wallet-App / CovPass-App

Für die elektronische Verwendung der digitalen COVID-Zertifikate soll den Zertifikatsinhabern nach den Leitlinien des eHealth-Netzwerks eine sogenannte Wallet-App bereitgestellt werden.[9] Nachdem der Zertifikatsinhaber eine Wallet-App auf einem Smartphone mit Kamera installiert hat, kann er innerhalb der Wallet-App den auf dem COVID-Zertifikat enthaltenen QR-Code scannen. Die Wallet-App speichert dann eine lokale elektronische Version des digitalen COVID-Zertifikats auf dem Smartphone, welches auf dem Smartphone-Bildschirm als QR-Code angezeigt und Dritten zur Prüfung vorgelegt werden kann.

Alle EU-Mitgliedsstaaten müssen ihren Bürgern seit dem 1. Juli 2021 die elektronische Nutzung der von ihnen bzw. den zuständigen nationalen Behörden oder sonstigen Stellen ausgestellten digitalen COVID-Zertifikate durch eine kostenlose Wallet-App ermöglichen. Zur Entwicklung einer solchen nationalen Wallet-App können sie auf die von der T-Systems International GmbH im Auftrag der EU-Kommission entwickelte Referenzimplementierung für eine Wallet-App für die Betriebssysteme iOS und Android zurückgreifen. Der Quellcode dieser Referenzimplementierung wird auf GitHub unter der Apache-2.0-Lizenz veröffentlicht.[10] Es könnten auch mehrere EU-Mitgliedsstaaten eine gemeinsame Wallet-App verwenden.[11]

Die offizielle deutsche Wallet-App ist die vom RKI herausgegebene CovPass-App. Die CovPass-App wird kostenlos angeboten und ermöglicht ihren Nutzern die Speicherung, Verwaltung und Nutzung von digitalen COVID-Zertifikaten mit einem gängigen iOS- oder Android-Smartphone. Es handelt sich um eine native App, d. h. sie ist spezifisch für die unterstützten Betriebssysteme und Endgeräte entwickelt worden und kann den Nutzern über die jeweiligen App-Stores bereitgestellt werden. Zum Funktionsumfang der CovPass-App siehe 5.4.3 und 5.4.4.

5.5.2 Prüfsystem / CovPassCheck-App

Für die Prüfung der digitalen COVID-Zertifikate (in Gestalt des QR-Codes) wird ein Prüfsystem benötigt. Ein geeignetes Prüfsystem für COVID-Zertifikate umfasst eine Kamera, mit der ein digitales Bild des zu prüfenden QR-Codes erzeugt werden kann, und eine Softwarekomponente (die nicht notwendiger Weise eine mobile App sein muss), mit der die im QR-Code kodierten Informationen dekodiert, also in Text umgewandelt und auf Validität überprüft werden können. Hierzu muss das Prüfsystem auch über ein Backend-System verfügen, welches die aktuellen Siegel-Zertifikate der angebundenen EU-Mitgliedsstaaten vom EU-Gateway lädt und der Softwarekomponente zur Verfügung stellt.

---

[9] eHealth-Netzwerk, Guidelines on Technical Specifications for Digital Green Certificates - Volume 4: European Digital Green Certificate Applications, Version 1.3 2021-04-21

[10] https://github.com/eu-digital-green-certificates/.

[11] eHealth-Netzwerk, Guidelines on Technical Specifications for Digital Green Certificates - Volume 4: European Digital Green Certificate Applications, Version 1.3 2021-04-21, S. 8.

Die Validierung der gescannten COVID-Zertifikate (QR-Code) durch das Prüfsystem umfasst eine technische und eine logische Validierung. Bei der technischen Validierung werden die Integrität und Authentizität des vorgelegten COVID-Zertifikats mittels der im QR-Code enthaltenen elektronischen Signatur geprüft. Bei der anschließenden logischen Validierung werden die in der Softwarekomponente konfigurierten aktuellen Business-Rules für den jeweilige Zertifikatskategorie auf die dekodierten Informationen zum Impf-, Test- oder Genesenenstatus angewendet. In der CovPassCheck-App werden die aktuell geltenden deutschen öffentlichen Schlüssel, Business Rules und Value Sets regelmäßig vom Zertifikatsservice heruntergeladen.

Alle Stellen und Personen (z. B. nationale Behörden, Reisedienstleister), die ein eigenes App-basiertes Prüfsystem entwickeln und anbieten möchten, können hierzu auf die von der T-Systems International GmbH im Auftrag der EU-Kommission entwickelte Referenzimplementierung für eine mobile Prüf-App (*Verifier App*) für die Betriebssysteme iOS und Android zurückgreifen. Der Quellcode dieser Referenzimplementierung wird auf GitHub unter der Apache-2.0-Lizenz veröffentlicht.[12]

Auch das RKI bietet mit der CovPassCheck-App ein App-basiertes Prüfsystem an. So wie die CovPass-App wird auch die CovPassCheck-App kostenlos angeboten. Sie ermöglicht die Prüfung von digitalen COVID-Zertifikaten mit einem gängigen iOS- oder Android-Smartphone. Zum Funktionsumfang der CovPassCheck-App siehe 5.4.4.

Für andere Prüfsysteme als die CovPassCheck-App sind die jeweiligen Anbieter verantwortlich. Für die Zwecke dieser DSFA wird vorläufig davon ausgegangen, dass die Datenverarbeitung durch Prüfsysteme anderer Anbieter sich nach den Festlegungen und Spezifikationen der DCC-VO und den dort in Bezug genommenen Interoperabilitätsrichtlinien des eHealth-Netzwerks[13] richten und somit mit der Datenverarbeitung durch die CovPassCheck-App vergleichbar ist.

5.5.3 Zertifikatsservice

Der Zertifikatsservice umfasst verschiedene Frontend- und Backend-Dienste, die nachfolgend beschrieben werden.

[12] https://github.com/eu-digital-green-certificates/.
[13] eHealth-Netzwerk, OUTLINE Interoperability of health certificates Trust framework V.1.0, 2021-03-12, online: https://ec.europa.eu/health/sites/default/files/ehealth/docs/trust-framework_interoperability_certificates_en.pdf (Abruf am 06.09.2021).

5.5.3.1 Frontend-Dienste

5.5.3.1.1 Web-Frontend

Das Web-Frontend ist eine lokale, d. h. im Webbrowser der Clients derjenigen Stellen, die digitale COVID-Zertifikate ausgeben, ablaufende Web-Anwendung, über die die ausgebenden Stellen auf den Zertifikatsservice zugreifen können. Nach erfolgter Authentifizierung können die berechtigten Personen der ausgebenden Stelle hier den Impf- oder Teststatus eines Geimpften oder Getesteten eingeben, Zertifikate als PDF-Dokument anfordern und diese ausdrucken. Da das Web-Frontend eine lokale Anwendung ist, werden – mit Ausnahme des aus dem Impf-, Test- oder Genesenenstatus errechneten Hash-Werts – keine weiteren Daten des Antragstellers an den Zertifikatsservice übermittelt.

5.5.3.1.2 PoC Manager

Der **PoC Manager** ist eine Web-Anwendung speziell für die Leiter von Impfzentren zur Verwaltung der Mitarbeiterzugänge. Über den PoC Manager wird auch die Erzeugung und Hinterlegung der X.509-Clientzertifikate über CryptShare ausgelöst. Durch den PoC Manager werden keinerlei Daten von Geimpften, sondern ausschließlich personenbezogene Daten des Personals der Impfstellen verarbeitet. Mit dem Hosting des Dienstes hat das RKI die KDO Service GmbH beauftragt.

5.5.3.2 Health Certificate Backend

Über das Health-Certificate-Backendsystem des Zertifikatsservice werden die folgenden Dienste bereitgestellt. Das Hosting des Health Certificate Backends erfolgt durch die KDO Service GmbH.[14]

5.5.3.2.1 Health Certificate Issuance Service

Zur Kommunikation mit dem Zertifikatsservice wird den verschiedenen die digitalen COVID-Zertifikate ausgebenden Stellen im Health Certitificate Issuance Service die Issuer Service API und verschiedenen Endpunkten bereitgestellt.

Der Health Certificate Issuance Service ist für den Empfang der vom Web-Frontend errechneten und verschlüsselt übermittelten Hash-Werte und deren Weiterleitung an den Signing Service zuständig.

[14] Im Rahmen einer Auftragsverarbeitung gemäß Art. 28 DSGVO. Für Einzelheiten siehe 5.8.7.

Wenn die das digitale COVID-Zertifikat ausgebende Stelle über eine integrierte Lösung (z. B. PVS, Apotheken-Verbändeportal) durch die Issuer Service API mit dem Zertifikatsservice interagiert, nimmt der Health Certificate Issuance Service – da in diesem Fall keine Client-seitige Errechnung des Hash-Werts wie im Web-Frontend möglich ist (siehe hierzu 5.4.2.1) – auch die von der ausgebenden Stelle in der jeweiligen Fachanwendung eingegebenen Daten zum Impf-, Test- oder Genesenenstatus entgegen, errechnet daraus den Hash-Wert und übergibt diesen an den Signing Service. Anschließend werden die Daten gelöscht, d. h. eine weitergehende Speicherung der verarbeiteten Daten im Health Certificate Issuance Service erfolgt nicht.

5.5.3.2.2 Signing Service

Der Signing Service ist für die Erzeugung der elektronischen Signatur auf Basis des vom Health Certificate Issuance Service übergebenen Hash-Werts zuständig. Für die Signierung werden qualifizierte Zertifikate für elektronische Siegel (nachfolgend „Siegel-Zertifikate“) verwendet, mit denen ein fortgeschrittenes elektronisches Siegel im Sinne der EU-Verordnung Verordnung Nr. 910/2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG (eIDAS-Verordnung) erzeugt wird. Die vom RKI verwendeten Siegel-Zertifikate werden von der D-Trust GmbH bezogen und mit dem zugehörigen privaten Schlüssel in einer gesonderten Datenbank innerhalb der Infrastruktur des Signing Service (Private Key Storage) sicher verschlüsselt verwahrt.

5.5.3.2.3 Public Key Storage / CA Distribution Service

Im Public Key Storage sind die öffentlichen Schlüssel (Public Keys) der gültigen Siegel-Zertifikate des RKI und der anderen Stellen hinterlegt, die COVID-Zertifikate in den am EU-Gateway angebundenen Länder ausgeben. Der CA Distribution Service stellt die öffentlichen Schlüssel den Nutzern der CovPass- und CovPassCheck-App zum Download bereit. Im Rahmen der Interoperabilität übermittelt der CA Distribution Service außerdem die vom RKI ausgestellten öffentlichen Schlüssel an das EU-Gateway und empfängt die von diesem bereitgestellten öffentlichen Schlüssel der anderen teilnehmenden Länder und überführt sie in den Public Key Storage.

5.5.3.2.4 Bereitstellungsdienste (Business Rules und Value Sets)

Im Bereitstellungsdienst sind die aktuellen Business Rules und Value Sets des RKI und der anderen am EU-Gateway angebundenen Länder hinterlegt. Der Bereitstellungsdienst stellt diese den Nutzern der CovPass- und CovPassCheck-App bei Bedarf zur Verfügung. Im Rahmen der Interoperabilität übermittelt der Bereitstellungsdienst die vom RKI veröffentlichten

Business Rules und Value Sets an das EU-Gateway und empfängt die von diesem bereitgestellten Datenpakete der anderen teilnehmenden Länder.

5.5.4 EU-Gateway

Zur Gewährleistung der Interoperabilität der in verschiedenen EU-Mitgliedsstaaten und weiteren teilnehmenden Ländern ausgestellten digitalen COVID-Zertifikate haben sich die EU-Kommission und die EU-Mitgliedsstaaten auf die Errichtung und den Betrieb einer europäischen **Public-Key-Infrastruktur (PKI)** verständigt. Zentrale Komponente dieser PKI ist ein zentraler Server, der eine Liste mit den öffentlichen Schlüsseln der in den einzelnen EU-Mitgliedsstaaten verwendeten gültigen Siegel-Zertifikate führt (im Sinne eines White-List-Dienstes) und diese an die Zertifikatsservices der am digitalen COVID-Zertifikat teilnehmenden Länder verteilt.

Über einen weiteren, ebenfalls zentralen Server erfolgt die Bereitstellung von DCC Business Rules und Value Sets. Diese werden von den Bereitstellungdiensten der am digitalen COVID-Zertifikat teilnehmenden Länder abgerufen. Vom deutschen Bereitstellungsdienst werden die Pakete dann im Bedarfsfall an die CovPass-App sowie die CovPassCheck-App verteilt.

Die zentralen Server bilden gemeinsam das sog. EU-Gateway. Die Architektur des EU-Gateway orientiert sich technisch an der Architektur des **European Federation Gateway Service (EFGS)**, über den die Warnungen der offiziellen Corona-Apps (in Deutschland die CWA) zwischen den teilnehmenden EU-Mitgliedsstaaten ausgetauscht werden können.

Der regulatorische und technische Rahmen des EU-Gateways wird in der DCC-VO und in den Interoperabilitätsrichtlinien des eHealth-Netzwerks[15] festgelegt. Das EU-Gateway kommuniziert nur mit den nationalen Zertifikatsservices der teilnehmenden Länder, wenn diese über eine Schnittstelle des EU-Gateways ihre eigenen öffentlichen Schlüssel übermitteln und die öffentlichen Schlüssel der jeweils anderen Länder herunterladen, so dass auf dem EU-Gateway keine personenbezogenen Daten (z. B. Zugriffsdaten, Angaben zum Impf-, Test- oder Genesenenstatus oder sonstige personenbezogenen Daten von Zertifikatsinhabern oder Mitarbeitern) verarbeitet werden.[16]

5.5.5 Smartphones der Nutzer

Das Smartphone (einschließlich des Betriebssystems) stellt die für den Betrieb der CovPass-App und von Prüf-Apps notwendigen Funktionalitäten und Konnektivitäten bereit. Für den

[15] eHealth Network, Guidelines on Technical Specifications for Digital Green Certificates, Volume 2: European Digital Green Certificate Gateway, Version 1.3 vom 21.04.2021; online unter https://ec.europa.eu/health/sites/default/files/ehealth/docs/digital-green-certificates_v2_en.pdf (Abruf am 06.09.2021).

[16] Die EU-Kommission hat im Vorfeld der initialen Erstellung des DSFA-Berichts auf Anfrage gegenüber dem BMG bestätigt, dass das EU-Gateway keine personenbezogenen Daten von Geimpften verarbeitet. Die Bestätigung liegt dem DSFA-Team vor.

Betrieb dieser Apps werden die folgenden Komponenten und Hintergrunddienste der Smartphones benötigt:

- Die Apps benötigen regelmäßig eine kurzfristige Internetverbindung, um die aktuellen Siegel-Zertifikate von dem CA Distribution Service (gegebenenfalls im Hintergrund) sowie die aktuellen Business Rules und Value Sets laden zu können. Die Prüfung von elektronischen Signaturen in COVID-Zertifikaten anhand der Siegel-Zertifikate erfolgt sodann lokal. Um die Internetverbindung herstellen zu können, benötigen die Apps die jeweiligen Systemberechtigungen zum Zugriff auf die Netzwerkkomponenten.
- Zum Scannen von QR-Codes benötigen die Apps Zugriff auf die Kamera des Smartphones.
- Das Smartphone muss unter iOS ab Version 12 oder Android ab Version 6 laufen.
- Der Nutzer muss bei der deutschen Version des jeweiligen App-Stores (Apple App Store, Google Play oder Huawei AppGallery) angemeldet sein.

Entsprechende Anforderungen gelten bei dem Einsatz von stationären Prüfsystemen (z. B. Systeme von Reisedienstleistern oder Grenzbehörden).

5.5.6 TI-Komponenten und -Dienste

Das zentrale Element der Authentifizierung von Arztpraxen, die über die TI auf den Zertifikatsservice zugreifen, ist das in der SMC-B enthaltene kryptografische Organisationszertifikat der Praxis, welches im Zusammenhang mit der Anbindung der Arztpraxis an die TI zur Verfügung gestellt wird. Dieser Identitätsnachweis wird dem Zertifikatsservice über den Konnektor bereitgestellt, der für das PVS die sichere Verbindung zur TI herstellt und ein Challenge/Response-Verfahren nutzt, um die Authentifizierung der Arztpraxis gegenüber dem IAM-Dienst des Zertifikatsservice durchführen zu können. Der Ablauf stellt sich entsprechend dem TI-Protokoll wie folgt dar:

(1) Der IAM-Dienst erstellt eine zufällige Challenge für den anfragenden Authentifizierungskontext
(2) Die SMC-B signiert die Challenge mit dem Organisationszertifikat der Arztpraxis
(3) Der IAM-Dienst erhält signierte Challenge und das Organisationszertifikat der Arztpraxis
(4) Der IAM-Dienst prüft die Signatur und die Gültigkeit des Organisationszertifikats durch den OSCP-Dienst und die lokale Trusted-Server-Liste der TI.
(5) Über die TI-Komponenten und -Dienste werden keine personenbezogenen Daten der Zertifikatsinhaber verarbeitet, sondern Organisationsdaten der Praxis.

Die SMC-B und der Konnektor sind Bestandteile der dezentralen TI. Die Funktionen von dezentralen TI-Komponenten liegen außerhalb des Wirkbereichs des RKI und sind nicht Gegenstand dieser DSFA. Verantwortlich für die Datenverarbeitung innerhalb der TI sind die Anwender bzw. Betreiber der jeweiligen TI-Dienste und -Komponenten. Die dezentralen TI-Komponenten sind Gegenstand einer vom Gesetzgeber durchgeführten DSFA, die in der Anlage zu § 307 Abs. 1 S. 3 SGB V in der Fassung des am 28.05.2021 verabschiedeten

Digitale-Versorgung-und-Pflege-Modernisierungs-Gesetz (DVPMG), deren Ergebnisse dieser DSFA zugrunde gelegt worden sind.[17]

5.6 Datenkategorien

Daten aus den folgenden Kategorien werden im Rahmen der oben beschriebenen Funktionen und Prozesse verarbeitet:

5.6.1 Zugriffsdaten

Bei den HTTPS-Requests der CovPass-App und der CovPassCheck-App und sonstigen Prüf-Systemen an den Zertifikatsservice fallen bei dem RKI als Betreiberin des Zertifikatsservice folgende Zugriffsdaten an:

- IP-Adresse
- Datum und Uhrzeit des Abrufs (Zeitstempel)
- Übertragene Datenmenge (bzw. Paketlänge)
- Meldung, ob der Abruf erfolgreich war

Der Zertifikatsservice speichert die Zugriffsdaten nach Erledigung des HTTPS-Requests in Protokolldateien, wobei die IP-Adresse zuvor durch Nullen der letzten 8 Bit anonymisiert wird.

Die Zugriffsdaten fallen auch bei dem Telekommunikationsunternehmen an, welches den Internetzugang des Nutzers bereitstellt.[18]

5.6.2 Zertifikatsaussage

Die als Zertifikatsaussage zusammengefassten Daten umfassen die in einem COVID-Zertifikat in menschen- und maschinenlesbarer Form jeweils enthaltenen überprüfbaren personenbezogenen Daten des Zertifikatsinhabers zu seinem Impf-, Test- oder Genesenenstatus.

Die Datenfelder der verschiedenen Zertifikatstypen entsprechen den jeweiligen Listen im Anhang der DCC-VO und den technischen Spezifikationen gemäß Durchführungsbeschluss (EU) 2021/1073 vom 28. Juni 2021 zur Festlegung technischer Spezifikationen und Vorschriften für die Umsetzung des mit der Verordnung (EU) 2021/953 des Europäischen Parlaments und des Rates geschaffenen Vertrauensrahmens für das digitale COVID-Zertifikat

[17] BR-Drucksache 357/21 S. 61 ff.
[18] Verkehrsdaten im Sinne des TKG.

der EU, mit der die für die länderübergreifende Prüfung und Anerkennung der digitalen COVID-Zertifikate erforderliche Einheitlichkeit gewährleistet wird. Für nationale Zwecke dürfen grundsätzlich zwar weitere Datenfelder aufgenommen werden. Von dieser Möglichkeit macht das RKI bei den in Deutschland ausgestellten COVID-Zertifikaten zurzeit jedoch keinen Gebrauch. Sollten in einem in einem anderen Land ausgestellten COVID-Zertifikat weitere Datenfelder verwendet werden, werden diese von der CovPassCheck-App in einer Prüfungssituation nicht berücksichtigt und auch nicht zu anderen Zwecken verarbeitet.

5.6.2.1 Impfstatus

Die Zertifikatsaussage bei Impfzertifikaten umfasst folgende Angaben zum Impfstatus des Zertifikatsinhabers:

Feld	Beispiel
Name	Mustermann
Vorname	Erika
Geburtsdatum	02.06.1965
Impfdatum	03.06.2021
Land	Deutschland
Aussteller	RKI
Krankheit	U07.1
Impfstoff	1119349007 (mRNA-Impfstoff), 1119305005 (Vektor-Impfstoff)
Produkt / Hersteller	Moderna, BioNTech
Nummer der Impfung	„1 von 1", „1 von 2", „2 von 2", „3 von 3"[19]
Eindeutige Zertifikatskennung	siehe unter 5.6.3

[19] Seit September 2021 werden in Deutschland auch sogenannte Auffrischungsimpfungen, also erneute Impfungen nach dem vollständigen Abschluss einer Impfserie, durchgeführt. Ab Release 1.8 werden daher auch entsprechende Impfzertifikate ausgestellt. Der zweite Wert des Felds „Nummer der Impfung" wird in diesem Fall gemäß Anhang II Nummer 5 des Durchführungsbeschluss (EU) 2021/1073 vom 28. Juni 2021 zur Festlegung technischer Spezifikationen und Vorschriften für die Umsetzung des mit der Verordnung (EU) 2021/953 des Europäischen Parlaments und des Rates geschaffenen Vertrauensrahmens für das digitale COVID-Zertifikat der EU dargestellt (z. B. „3 / 3"). Im Rahmen des eHealthNetworks haben die Mitgliedsländer hierzu eine einheitliche Darstellung für Auffrischungsimpfungen abgestimmt. COVID-Zertifikate für Auffrischungsimpfungen werden demnach auch grenzüberschreitend anerkannt werden.

5.6.2.2 Teststatus

Die Zertifikatsaussage bei Testzertifikaten umfasst folgende Angaben zum Teststatus des Zertifikatsinhabers:

Feld	Beispiel
Name	Mustermann
Vorname	Erika
Geburtsdatum	02.06.1965
Datum der Probenahme	03.06.2021
Datum der Ergebnisfeststellung	03.06.2021
Land	Deutschland
Aussteller	RKI
Krankheit	U07.1
Testtyp	Schnell-Immunassey
Testname	Roche LightCycler qPCR
Produkt / Hersteller	BIOSYNEX S.A., BIOSYNEX COVID-19 Ag BSS
Testzentrum	Testzentrum Hamburg 1
Testresultat	Erkannt
Eindeutige Zertifikatskennung	siehe unter 5.6.3

5.6.2.3 Genesungsstatus

Die Zertifikatsaussage bei Genesenenzertifikaten umfasst folgende Angaben zum Genesungsstatus des Zertifikatsinhabers:

Feld	Beispiel
Name	Mustermann
Vorname	Erika

Feld	Beispiel
Geburtsdatum	02.06.1965
Krankheit	U07.1
Datum des ersten positiven Tests	04.03.2021
Datum Nachweis gültig vom	18.03.2021
Datum Nachweis gültig bis	31.08.2021
Land	Deutschland
Aussteller	RKI
Eindeutige Zertifikatskennung	siehe unter 5.6.3

5.6.3 Eindeutige Zertifikatskennung

Die eindeutige Zertifikatskennung ist der Identifikator für ein COVID-Zertifikat. Sie besteht aus einer alphanumerischen Zeichenfolge und enthält keine Angaben, die sie mit anderen Dokumenten oder Kennungen wie Pass- oder Personalausweisnummern verknüpft, damit eine direkte Zuordnung zur Person des Zertifikatsinhabers verhindert wird. Durch die eindeutige Zertifikatskennung wird auch der länderübergreifende Widerruf von ungültigen COVID-Zertifikaten über das EU-Gateway ermöglicht, indem Zertifikatswiderrufslisten zwischen den am EU-Gateway angeschlossenen Ländern ausgetauscht werden. Im aktuellen Release werden derartige Widerrufslisten jedoch nicht umgesetzt.

Bei Impfzertifikaten wird der Unique Vaccination Certificate Identifier (UVCI) als eindeutige Zertifikatskennung in der Form von Option 2 der aktuellen Interoperabilitätsrichtlinien für Impfzertifikate des eHealth-Netzwerks[20] verwendet. Der UVCI besteht somit aus vier Blöcken: Die ersten zwei Blöcke sind für alle Nutzer gleich und werden mit dem Wert „01DE“ dargestellt. Der letzte Block enthält eine kryptografische Prüfsumme. Der dritte Block *Opaque Unique String* ist eine zufällige eindeutige Zeichenfolge, die kollisionssicher erzeugt wird.

Beispiel für eine UVCI zu einer Impfung im Impfzentrum Landkreis Altötting (84503):

```
01DE/84503/DXSGWLWL40SU8ZFKIYIBK39A3#S
```

Die Struktur von eindeutigen Zertifikatskennungen für Test- und Genesenenzertifikate wird vom eHealth-Netzwerk nicht detailliert vorgegeben. Die vom RKI festgelegte Struktur für diese

[20] eHealth Network, Guidelines on verifiable vaccination certificates – basic interoperability elements, Release 2 vom 12.03.2021.

Zertifikatstypen orientiert sich an der Struktur der UVCI. Dies entspricht der Empfehlung des eHealth-Netzwerks.[21]

5.6.4 Digitales COVID-Zertifikat

Ein digitales COVID-Zertifikat bestätigt gemäß den Vorgaben der DCC-VO und der technischen Spezifikationen gemäß Durchführungsbeschluss (EU) 2021/1073 vom 28. Juni 2021 zur Festlegung technischer Spezifikationen und Vorschriften für die Umsetzung des mit der Verordnung (EU) 2021/953 des Europäischen Parlaments und des Rates geschaffenen Vertrauensrahmens für das digitale COVID-Zertifikat der EU in den jeweiligen Amtssprachen und mindestens in englischer Sprache, dass der Zertifikatsinhaber in dem Land, das die Bescheinigung ausstellt, eine bestimmte Schutzimpfung erhalten hat, negativ getestet worden ist oder von einer COVID-19-Erkrankung genesen ist. Es wird dem potenziellen Zertifikatsinhaber nach einer nachgewiesenen Impfung, Testung oder Genesung auf seinen Wunsch hin von der das digitale COVID-Zertifikat bescheinigenden Stelle als Papierdokument oder PDF-Dokument ausgehändigt und/oder auf einem Bildschirm als QR-Code angezeigt.

Ein digitales COVID-Zertifikat enthält die jeweilige Zertifikatsaussage (siehe 5.6.2), also menschenlesbare Angaben zum bescheinigten Impf-, Test- oder Genesenenstatus, sowie den maschinenlesbaren (digitalen) QR-Code (siehe 5.6.5), mit dem das digitale COVID-Zertifikat in der CovPass-App elektronisch gespeichert und genutzt und von Dritten mit einem Prüfsystem geprüft werden kann. Das digitale COVID-Zertifikat in Papierform und die elektronische verwendbare Version in der CovPass-App sind gleichwertig (ErwG 18 DCC-VO). Jedes digitale COVID-Zertifikat muss gemäß Art. 3 Abs. 4 DCC-VO folgenden Hinweis enthalten:

> *„Dieses Zertifikat ist kein Reisedokument. Die wissenschaftlichen Erkenntnisse über COVID-19-Impfungen und -Tests sowie über die Genesung von einer COVID-19-Infektion entwickeln sich ständig weiter, auch im Hinblick auf neue besorgniserregende Virusvarianten. Bitte informieren Sie sich vor der Reise über die am Zielort geltenden Gesundheitsmaßnahmen und damit verbundenen Beschränkungen.“*

5.6.5 QR-Code

Der QR-Code ist auf dem digitalen COVID-Zertifikat enthalten und repräsentiert eine maschinenlesbare Version des digitalen COVID-Zertifikats. Er enthält in digitaler Form (als Binärcode) die jeweilige Zertifikatsaussage (siehe 5.6.2) und eine elektronische Signatur (siehe 5.6.7). Um ein digitales COVID-Zertifikat im Papierformat in die CovPass-App zu überführen, muss der QR-Code mit der CovPass-App ausgelesen werden. Der QR-Code auf

[21] eHealth Network, Guidelines on COVID-19 citizen recovery interoperable certificates – minimum dataset, Release 1 vom 15.03.2021, S. 7 (dort in der Zeile zum “Certificate Identifier”).

dem Papierdokument und in der CovPass-App kann mit einem Prüfsystem gescannt werden, um die Gültigkeit des COVID-Zertifikats zu prüfen.

5.6.6 Hash-Wert

Damit ein COVID-Zertifikat fälschungssicher, beweiskräftig und prüfbar ist, muss eine zentrale Signierung über das Trust Framework des eHealth-Netzwerks im Rahmen der PKI erfolgen. Um dabei auf eine Übertragung von personenbezogenen Daten über den Impf-, Test- oder Genesenenstatus an den Zertifikatsservice verzichten zu können, werden, soweit es die jeweilige Anbindungsart der bescheinigenden bzw. ausgebenden Stelle erlaubt, nicht alle Daten des auszugebenden COVID-Zertifikats einschließlich des Namens und Geburtsdatums der Person im Klartext, sondern lediglich ein daraus errechneter Hash-Wert übermittelt. Zurzeit ist dies nur bei der Anbindung per Web-Frontend und über das CWA-System möglich. Bei der Anbindung per PVS werden die Daten zum Impf-, Test- oder Genesenenstatus transportverschlüsselt im Klartext zum Zertifikatsservice übertragen und dort dann der Hash-Wert errechnet.

Auf Basis des Hash-Werts wird dann die Signatur generiert. Die Hash-Werte selbst enthalten keine Daten der gehashten Informationen und lassen somit, selbst wenn sie einer bestimmten Person zugeordnet werden sollten, außer dem Umstand, dass der Antragsteller die Ausgabe eines digitalen COVID-Zertifikats wünscht, keine weitergehenden Erkenntnisse zu dieser Person zu.

5.6.7 Elektronische Signatur

Der QR-Code enthält in maschinenlesbarer Form neben der Zertifikatsaussage auch eine elektronische Signatur, mit der im Rahmen der technischen Validierung die Integrität und Authentizität des COVID-Zertifikats geprüft werden kann (siehe 5.4.4 und 5.5.2).

5.6.8 Identitätsnachweis

Um den QR-Code mit einem Prüfsystem prüfen zu können, muss die prüfende Stelle feststellen, dass sich der vorgezeigte Nachweis auf die vorzeigende Person bezieht. Hierfür benötigt sie in der Regel ein amtliches Ausweisdokument mit Lichtbild als Identitätsnachweis, aus dem sich der Name und das Geburtsdatum seines Besitzers ergeben.

5.6.9 Anruferdaten (Hotline)

Bei Anrufen bei der Hotline fallen Daten aus verschiedenen Kategorien an, die in diesem DSFA-Bericht zusammengefasst als Anruferdaten bezeichnet werden. Anruferdaten

umfassen technische Verbindungsdaten (z. B. Telefonnummer des Anrufers) und die Inhalte des jeweiligen Gesprächs, soweit diese von den Hotline-Mitarbeitern notiert werden.

5.7 Löschung der personenbezogenen Daten

5.7.1 Daten in der CovPass-App

Die elektronischen Versionen der digitalen COVID-Zertifikate in der CovPass-App können vom Nutzer jederzeit manuell gelöscht werden. Eine automatische Löschung erfolgt nicht. Dies gilt auch dann, wenn ein digitales COVID-Zertifikat durch Zeitablauf ungültig geworden ist.

Wenn der Nutzer die Funktion „EU-Ausdruck“ zur Erstellung eines ausdruckbaren PDF-Dokuments eines in der CovPass-App gespeicherten digitalen Impf- oder Genesenenzertifikats nutzt, wird das PDF-Dokument unmittelbar nach der Weitergabe an das Betriebssystem oder eine PDF-fähige andere App aus dem App-Speicher gelöscht. Gleiches gilt, wenn der Exportvorgang vom Nutzer vorzeitig abgebrochen wird.

5.7.2 Daten in der CovPassCheck-App

Die aus dem QR-Code ausgelesenen oder daraus abgeleiteten Daten (Zertifikatsaussage, elektronische Signatur, Hash-Wert) werden unmittelbar nach Abschluss des einzelnen Prüfvorgangs aus dem lokalen Speicher gelöscht.

5.7.3 Daten im Zugriffsservice

Zur Löschung von Zugriffsdaten siehe unter 5.6.1.

Die von den die digitalen COVID-Zertifikate ausgebenden Stellen über die Issuer Service API des Health Certificate Issuance Service übermittelten (Zertifikatsaussage oder Hash-Wert) und die daraus abgeleiteten Daten (ggf. Hash-Wert, elektronische Signatur) werden nach der Rückgabe der elektronischen Signatur gelöscht. Eine Ausnahme wird mittelfristig für die in der Zertifikatsaussage enthaltene eindeutige Zertifikatskennung gelten, die für die Dauer der Gültigkeit des jeweiligen digitalen COVID-Zertifikats gespeichert werden wird, um den Widerruf von nachträglich ungültig erklärten digitalen COVID-Zertifikaten (z. B. wegen Manipulation oder weil sich eine bestimmte Impfstoffcharge als wirkungslos herausstellt) zu ermöglichen. Gegenwärtig wird eine Widerrufsmöglichkeit im aktuellen Release noch nicht umgesetzt.

5.8 An der Datenverarbeitung beteiligte Akteure

Nachfolgend werden die Akteure beschrieben und datenschutzrechtlich eingeordnet, die direkten Einfluss auf die Verarbeitung personenbezogener Daten im Rahmen des Prüfungsgegenstands nehmen können.

5.8.1 Zertifikatsinhaber

Die von der Verarbeitung im Rahmen des Prüfgegenstands betroffenen Personen sind in erster Linie die geimpften, getesteten oder genesenen Personen, die bei einer bescheinigenden Stelle die Ausgabe eines digitalen COVID-Zertifikats durch das RKI beantragen bzw. wünschen (Zertifikatsinhaber) und deren Daten durch eine Fachanwendung der bescheinigenden Stelle und den Zertifikatsservice des RKI verarbeitet werden.

Wenn ein Zertifikatsinhaber ein auf ihn ausgestelltes digitales COVID-Zertifikat bzw. dessen QR-Code einem Dritten zur Prüfung mit einem Prüfsystem vorlegt, ist der Zertifikatsinhaber auch von der Verarbeitung seiner Daten durch das Prüfsystem betroffen.

5.8.2 Nutzer der CovPass-App

Zertifikatsinhaber, die die CovPass-App nutzen, sind auch in der Rolle eines Nutzers der CovPass-App durch die Verarbeitung ihrer Zugriffsdaten durch den Zertifikatsservice betroffen.

Da die CovPass-App auch ausschließlich mit digitalen COVID-Zertifikaten von anderen Personen (z. B. Familienmitgliedern) verwendet werden kann, ist ein Nutzer der App nicht zwangsläufig auch als Zertifikatsinhaber betroffen.

5.8.3 Nutzer der CovPassCheck-App

Nutzer der CovPassCheck-App sind durch die Verarbeitung ihrer Zugriffsdaten durch den Zertifikatsservice während des Abrufs der aktuellen Siegel-Zertifikate betroffen. In der Regel wird es sich bei Nutzern der CovPassCheck-App um prüfende Stellen handeln. Die CovPassCheck-App kann jedoch auch von anderen Personen oder einem Zertifikatsinhaber selbst verwendet werden (etwa für die Prüfung eines eigenen digitalen COVID-Zertifikats).

5.8.4 Prüfende Stellen

Prüfende Stellen sind Personen, Behörden und Unternehmen, die ein Prüfsystem zur Prüfung von digitalen COVID-Zertifikaten einsetzen.

5.8.5 RKI

Für die technische Erstellung und Generierung bzw. Ausstellung des digitalen COVID-Zertifikats ist das RKI zuständig; die bescheinigenden Stellen müssen die Daten zum Impf-, Test- oder Genesenenstatus des Antragstellers an das RKI übermitteln (§ 22 Abs. 5 bis 7 IfSG, dort jeweils Satz 3).

Das RKI hat externe Dienstleister mit der für den Betrieb der Komponenten CovPass-App, CovPassCheck-App und Zertifikatsservice sowie den Betrieb der Hotlines für technischen Support notwendigen Datenverarbeitung beauftragt.

5.8.6 Bescheinigende Stellen

Der Kreis der bescheinigenden Stellen wird in § 22 Abs. 5 bis 7 IfSG, dort jeweils Satz 1, festgelegt. Zur Bescheinigung und Ausgabe von digitalen COVID-Zertifikaten berechtigt und potenziell verpflichtet sind demnach:

- Ärzteschaft (Impf-, Test- und Genesenenzertifikate)
- Zur Durchführung von Impfungen berechtigte Personen (Impfzertifikate)
- Apotheken (Impf- und Genesenenzertifikate)
- Zur Durchführung oder Überwachung von Testungen berechtigte Personen (Testzertifikate)

Die bescheinigenden Stellen sind die zur Bescheinigung und Ausgabe von digitalen COVID-Zertifikaten berechtigten und ggf. auch verpflichteten Stellen, das heißt für die Erhebung, ggf. Hashing und Übermittlung des (ggf. gehashten) Impf-, Test- oder Genesenenstatus an den Zertifikatsservice sowie die technische Ausgabe des digitalen COVID-Zertifikats sind die bescheinigenden Stellen jeweils eigenständig verantwortlich. Dass deren Datenverarbeitungsvorgänge nicht in den Verantwortungsbereich des RKI fallen, folgt aus Art. 10 Abs. 6 f. DCC-VO, welcher den bescheinigenden bzw. ausgebenden Stellen eine eigene Übermittlungspflicht an den Zertifikatsaussteller (hier: RKI) in Bezug auf den Impf- Test oder Genesungsstatus auferlegt. Entsprechendes ergibt sich auch aus §§ 22 Abs. 5-7 IfSG, welche die datenschutzrechtliche Grundlage im Sinne des Art. 6 Abs. 1 lit. e in Verbindung mit Art. 9 Abs. 2 lit. i DSGVO für die Übermittlung der für die Generierung des digitalen COVID-Zertifikats erforderlichen personenbezogenen Daten durch die bescheinigenden Stellen an das RKI schaffen.

Sofern die bescheinigenden Stellen eine integrierte Cloud-basierte Fachanwendung für die Nutzung des Zertifikatsservice über die Issuer Service API einsetzen, ist auch der Betreiber der Fachanwendung an der Datenverarbeitung beteiligt. Die datenschutzrechtliche Bewertung und Einbindung der Verarbeitungstätigkeiten des Betreibers obliegt den bescheinigenden Stellen als dessen Auftraggeber, wobei in der Regel ein Auftragsverarbeitungsverhältnis vorliegen wird.

5.8.7 Externe Dienstleister

Mit der Entwicklung und dem Betrieb der CovPass-Komponenten hat das RKI externe Dienstleister beauftragt. Soweit dabei eine Verarbeitung personenbezogener Daten von Bürgern oder Personal bei den bescheinigenden Stellen nicht ausgeschlossen werden kann, erfolgt diese Datenverarbeitung jeweils auf Grundlage eines schriftlichen Auftragsverarbeitungsvertrags nach Art. 28 Abs. 3 DSGVO.

5.8.7.1 Ubirch GmbH

Die Ubirch GmbH (Ubirch) hat den Prüfungsgegenstand zusammen mit der IBM Deutschland GmbH entwickelt. Gegenstand der Auftragsverarbeitung durch Ubirch für das RKI ist die Administration und der Betrieb des Zertifikatsservice.

Ubirch unterhält mit schriftlicher Genehmigung des RKI (Art. 28 Abs. 2 S. 1 DSGVO) Unterauftragsverhältnisse mit folgenden Dienstleistern als weitere Auftragsverarbeiter, die ebenfalls mit personenbezogenen Daten des RKI in Berührung kommen können:

- KDO Service GmbH (Hosting des Zertifikatservice)
- Telekom Deutschland GmbH (Hosting des Trust Service in der Open Telecom Cloud)
- WebID Solutions GmbH (Bereitstellung des Videoident-Dienstes für die Identifizierung der Impfzentrenleitung)
- Gronemeyer IT GmbH (Bereitstellung des Datenaustauschdienstes CryptShare für die Übermittlung der X.509-Clientzertifikate an die Impfzentrenleitung)
- Bechtle Onsite Services GmbH (1st-Level-Support für Personal der Impfstellen). Der Callcenter-Betreiber darf grundsätzlich keine personenbezogenen Daten von Zertifikatsinhabern speichern, die eventuell vom Personal der Impfstellen mitgeteilt werden. Dies ist in den jeweiligen Auftragsverarbeitungsvereinbarungen schriftlich festgelegt und wird organisatorisch in Form von entsprechenden TOMs sichergestellt
- global office GmbH (Anbieter der Hotlines).

5.8.7.2 BfArM

Die Website für die digitalen COVID-Zertifikate (www.digitaler-impfnachweis-app.de) wird vom BfArM auf einem von AWS als weiteren Auftragsverarbeiter (Sub-Dienstleister des BfArM) bereitgestellten Webserver betrieben. Über die Webseite werden allgemeine Informationen über die digitalen COVID-Zertifikate als Impfnachweis einschließlich zum Thema Datenschutz bereitgestellt. Die Webseite ist nicht an die sonstigen Komponenten zur Generierung und Ausgabe der digitalen COVID-Zertifikate angeschlossen und es werden keine Gesundheitsdaten über die Webseite erhoben.

5.8.8 Weitere Akteure

Ein weiterer zentraler Akteur ist das BMG als die für das RKI aufsichtsführende oberste Bundesbehörde. Das BMG hat im Februar und März 2021 ein europaweites Vergabeverfahren durchgeführt[22] und auf dieser Grundlage die IBM Deutschland GmbH, Ubirch GmbH, govdigital eG und Bechtle Onsite GmbH mit der Entwicklung des digitalen Impfnachweises und der Umsetzung der digitalen COVID-Zertifikate beauftragt. Das BMG hat im Rahmen seiner Aufgaben und Zuständigkeiten auf die Schaffung der erforderlichen nationalen Rechtsgrundlagen im IfSG unter Beratung durch den BfDI und eine mit der deutschen Anwendungspraxis des Datenschutzes vereinbare europäische Lösung im Rahmen der Abstimmungen zur EU-Verordnung über das digitale COVID-Zertifikat hingewirkt. Das RKI wurde regelmäßig über relevante laufende Entwicklungen und Gesetzesvorhaben auf nationaler und EU-Ebene unterrichtet, so dass diese bei der Entwicklung der vorliegenden Lösungen zum digitalen COVID-Zertifikat und der Durchführung der DSFA berücksichtigt werden können.

Mit Ausnahme der Ubirch GmbH und der Bechtle Onsite GmbH werden von den oben genannten weiteren Akteuren auf Seiten des RKI keine personenbezogenen Daten im Zusammenhang mit digitalen COVID-Zertifikaten verarbeitet, so dass insoweit keine Auftragsverarbeitungsverhältnisse mit dem RKI bestehen.

5.9 Begleitdokumente

Folgende Begleitdokumente konkretisieren die Beschreibung des Prüfungsgegenstands und sind Bestandteil dieses DSFA-Berichts:

(1) Anlage 1: Risikomatrix zum DSFA Bericht (Stand 11.08.2021)
(2) Anlage 2: Begleitdokumente
    a. BG 1: Technisch-organisatorische Maßnahmen der Ubirch GmbH in Bezug auf den Zertifikatsservice (Stand 06/2021)
    b. BG 2: Technisch-organisatorische Maßnahmen und Datenschutzkonzept der Bechtle Onsite GmbH in Bezug auf die technische Hotline (Version 4.0)
    c. BG 3: Technisch-organisatorische Maßnahmen der KDO Service GmbH in Bezug auf das Hosting des Zertifikatsservice (Stand: 06.05.2021)
    d. BG 4: Handbuch zum Zertifikatsservice für medizinisches Personal der Impfstellen
    e. BG 5: Handbuch zum Zertifikatsservice für IT-Verantwortliche der Impfstellen
    f. BG 6: Datenschutzhinweise CovPass-App (Fassung vom 19.08.2021)
    g. BG 7: Datenschutzhinweise CovPassCheck-App (Fassung vom 12.08.2021)
    h. BG 8: Datenschutzhinweise zum digitalen COVID-Zertifikat (Fassung vom 21.06.2021)

[22] https://ted.europa.eu/udl?uri=TED:NOTICE:116414-2021:TEXT:EN:HTML&src=0.

6 Einholung des Standpunktes der betroffenen Personen

Gemäß Art. 35 Abs. 9 DSGVO kann der Verantwortliche die Standpunkte der betroffenen Personen einholen, um deren Sichtweisen in Erfahrung zu bringen und somit möglicher Kritik frühzeitig zu begegnen und dadurch die Akzeptanz des in Rede stehenden Verfahrens zu fördern.

Die potenziell von dem Prüfungsgegenstand betroffenen Personen umfassen alle sich in Deutschland aufhaltenden Geimpften, Getesteten und Genesenen und somit die gesamte für eine COVID-19-Impfung oder Testung infrage kommende Bevölkerung. Daher war eine Einholung des Standpunkts der betroffenen Personen im Sinne von Art. 35 Abs. 9 DSGVO aus praktischen, insbesondere zeitlichen Gründen, nicht möglich.

Um dennoch Einblicke und Hinweise auf die Erwartungen und Prioritäten der betroffenen Personen und eventuell vom RKI übersehene Aspekte des Prüfungsgegenstands zu erhalten, hat das RKI verschiedene Quellen ausgewertet:[23]

- Individuelles und öffentliches Feedback aus der Entwicklercommunity auf die Veröffentlichung der Projektdokumentation, insbesondere zu dem mit Beteiligung der Ubirch GmbH durchgeführten Testprojekt in Altöttingen
- Medienberichterstattung
- Fachveröffentlichungen
- Stellungnahmen von Datenschutzbehörden und Datenschutzgremien
- Stellungnahmen von Verbänden und Interessensgruppen

Den darin geäußerten Standpunkten wurde bei der Entwicklung der Verfahren zum digitalen COVID-Zertifikat, soweit aus Sicht des RKI zweckmäßig und möglich, Rechnung getragen.

7 Datenschutzrechtliche Bewertung

Nachfolgend werden die maßgeblichen Aspekte der Verarbeitungstätigkeiten aus datenschutzrechtlicher Sicht bewertet, damit die datenschutzrechtlichen Anforderungen identifiziert und die geplanten Maßnahmen und Ergebnisse der Risikoanalyse einer datenschutzrechtlichen Beurteilung zugänglich gemacht werden können.

[23] Zur Klarstellung wird darauf hingewiesen, dass dies keine Einholung des Standpunkts im Sinne des Art. 35 Abs. 9 DSGVO darstellt.

7.1 Verarbeitung personenbezogener Daten

Personenbezogene Daten sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen (Art. 4 Nr. 1 DSGVO). Die im Rahmen des Prüfungsgegenstands verarbeiteten Daten haben teilweise, je nach ihrer Funktion, einen direkten oder indirekten Personenbezug. In welchem Umfang personenbezogene Daten verarbeitet werden, wird im Folgenden dargestellt.

7.1.1 Personenbezug

Es wird angenommen, dass es sich bei den im Rahmen des Prüfungsgegenstands verarbeiteten Daten um personenbezogene Daten handelt.

Der Personenbezug besteht hinsichtlich der Verarbeitung der Zertifikatsaussagen und den ggf. weiteren im Rahmen der Ausstellung des digitalen COVID-Zertifikats durch den Zertifikatservice verarbeiteten Daten, sofern die bescheinigende Stelle über ihr PVS angebunden ist. Sofern das Web-Frontend verwendet wird, wird nur der Hash-Wert verarbeitet, der ein (personenbezogenes) Pseudonym der betroffenen Person darstellt.

Für die bescheinigenden Stellen besteht der Personenbezug hinsichtlich der an das RKI übermittelten Zertifikatsaussagen sowie der Daten auf dem digitalen COVID-Zertifikat in Papierform, welches dem Zertifikatsinhaber von der bescheinigenden Stelle ausgehändigt wird.

Unabhängig davon, ob es sich bei den verarbeiteten Datenkategorien für das RKI für sich genommen um personenbezogene Daten eines Geimpften, Getesteten oder Genesenen handelt, folgt ihr Personenbezug bei der Nutzung der CovPass-App und der CovPassCheck-App für das RKI und den Internetzugangsanbieter potenziell auch aus ihrer – wenn auch nur kurzzeitigen – Verbindung mit der IP-Adresse, die für die Übermittlung dieser Daten an das RKI verarbeitet wird. Bei IP-Adressen handelt es sich für Anbieter von Online-Diensten um personenbezogene Daten, wenn sie über rechtliche Mittel verfügen, die es ihnen erlauben, ggf. auch mit Hilfe der zuständigen Behörde und dem Internetzugangsanbieter, die betreffende Person anhand der gespeicherten IP-Adressen bestimmen zu lassen.[24] Das RKI hat die rechtliche Möglichkeit, sich beispielsweise im Fall von Cyberattacken an die zuständige Behörde zu wenden, um die fraglichen Informationen zu erlangen bzw. die Strafverfolgung einzuleiten und infolgedessen auch eine IP-Adresse einer natürlichen Person zuzuordnen, die ohne das Zusatzwissen des Dritten für das RKI durch die nicht auflösbare Pseudonymisierung faktisch anonym sind. Sofern und solange das RKI diese Daten in Verbindung mit einer IP-Adresse speichert oder anderweitig verarbeitet, handelt es sich somit insgesamt um personenbezogene Daten der Nutzer der vorgenannten Apps.

[24] EuGH, Urt. v. 19.10.2016, Rs. Breyer, C-582/14.

Für die weiteren potenziell Verantwortlichen stellen lediglich der Impfstatus sowie der Name und das Geburtsdatum von anderen Personen, die ein Impfzertifikat vorzeigen, ein personenbezogenes Datum dar. Entsprechend gilt dies für Genesenen- und Testzertifikate.

7.1.2 Lokale Datenverarbeitung durch Apps

Der konkrete Ablauf der lokalen personenbezogenen Datenverarbeitung durch die CovPass-App und die CovPassCheck-App liegt außerhalb des Einfluss- und Kenntnisbereichs des RKI, da weder für die Speicherung oder den Export im PDF-Dokument (mit der Funktion „EU-Ausdruck“) des digitalen COVID-Zertifikats in der CovPass-App noch bei der Prüfung mittels der CovPassCheck-App eine Internetverbindung zum RKI aufgebaut wird. Für das RKI sind die nur lokal in den Apps verarbeiteten Daten der Nutzer bzw. Zertifikatsinhaber (z. B. Impfstatus) daher anonym.

Für die Bewertung des Personenbezugs kommt es nach der Rechtsprechung des EuGH auf die relative Bestimmbarkeit für den (eventuell) Verantwortlichen an, d. h. der (eventuell) Verantwortliche muss bei der Bewertung seiner möglichen Verantwortlichkeit nur die Mittel berücksichtigen, die er selbst oder eine andere Person nach allgemeinem Ermessen wahrscheinlich nutzen wird. Es ist somit zwar nicht Bedingung, dass alle für die Herstellung des Personenbezugs notwendigen Informationen oder Mittel für das RKI selbst verfügbar sind oder eingesetzt werden, d. h. das RKI muss sich das abstrakt verfügbare Drittwissen und die für Dritte zur Verfügung stehenden Mittel prinzipiell zurechnen lassen. Dies allerdings nur, soweit das Wissen und die Mittel durch das RKI vernünftigerweise eingesetzt werden (können). Mit der Rechtsprechung des EuGH wird man nach allgemeinem Ermessen davon ausgehen müssen, dass Verantwortliche (insbesondere, wenn es sich um eine öffentliche Stelle handelt) grundsätzlich keine rechtswidrigen Mittel einsetzen, um die faktische Anonymität oder Unauflöslichkeit von Pseudonyme aufzuheben.[25]

Geht man davon aus, dass das RKI vernünftigerweise keine entsprechenden Maßnahmen ergreifen wird (zumal die dafür notwendigen Änderungen der Source Codes aufgrund ihrer Veröffentlichung bei GitHub nicht unbemerkt bleiben würden), müssen die lokal verarbeiteten Daten vor diesem Hintergrund auch dann als anonym für das RKI angesehen werden, wenn sie im Einzelfall vom Nutzer oder einem Dritten (z. B. prüfende Stelle) einer Person zugeordnet werden können. Eine datenschutzrechtliche Verantwortlichkeit des RKI für die lokale Verarbeitung, die eine Verarbeitung von personenbezogenen Daten voraussetzt, ist daher nicht anzunehmen. Gleichwohl muss das Risiko einer Identifikation durch andere Stellen, wie insbesondere die Hersteller der mobilen Betriebssysteme, im Rahmen dieser DSFA in den

[25] Vgl. zusammenfassend und m.w.N. bei: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, DSGVO Art. 4 Nr. 1 Rn. 61 und 64.

Blick genommen und erforderlichenfalls entsprechende Maßnahmen zur Risikobehandlung ergriffen werden.[26]

7.1.3 Gesundheitsdaten

Gesundheitsdaten sind personenbezogene Daten, die sich auf die körperliche oder geistige Gesundheit einer natürlichen Person, einschließlich der Erbringung von Gesundheitsdienstleistungen, beziehen und aus denen Informationen über deren Gesundheitszustand hervorgehen (Art. 4 Nr. 15 DSGVO), wobei auch Informationen über Krankheitsrisiken einer Person als Gesundheitsdaten gelten (vgl. Erwägungsgrund 35). Daher wären beispielsweise auch Informationen zum Impfstatus als Gesundheitsdatum einzustufen. Denn aus diesen Informationen kann auf die Wahrscheinlichkeit einer COVID-19-Erkrankung des Betroffenen geschlossen werden. Gesundheitsdaten sind besondere Kategorien personenbezogener Daten im Sinne von Art. 9 Abs. 1 DSGVO.

Als Gesundheitsdaten anzusehen sind vor diesem Hintergrund folgende Datenkategorien:

- Zertifikatsaussage
- Eindeutige Zertifikatskennung
- Digitales COVID-Zertifikat
- QR-Code

7.2 Verantwortliche für die Verarbeitung

Gemäß Art. 4 Nr. 7 DSGVO ist für die Verarbeitung Verantwortlicher, wer allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet. Sind die Zwecke und Mittel dieser Verarbeitung durch das Unionsrecht oder das Recht der Mitgliedstaaten vorgegeben, so kann der Verantwortliche beziehungsweise können die bestimmten Kriterien seiner Benennung nach dem Unionsrecht oder dem Recht der Mitgliedstaaten festgelegt werden.

[26] Vgl. ähnlich bei *Kühling/Schildbach* in: Corona-Apps – Daten- und Grundrechtsschutz in Krisenzeiten (NJW 2020, 1545 (1549)), die jedoch erst mit dem Absetzen einer Infektionsmeldung von einem Personenbezug für das RKI ausgehen: „Es erschiene teleologisch wenig überzeugend, gerade das RKI, das über die Mittel und Zwecke der Datenverarbeitung entscheidet und das notwendige zentrale Element herstellt, aus dem Anwendungsbereich des Datenschutzrechts zu entlassen. Daher spricht vieles für die Anwendbarkeit der datenschutzrechtlichen Regelungen. Das gilt allerdings nicht bereits mit dem Zeitpunkt des Beginns der CWA App-Nutzung, sondern erst mit dem Absetzen einer Infektionsmeldung. Letztlich verbleibt gerade in dieser zentralen Frage jedoch eine erhebliche Rechtsunsicherheit."

7.2.1 Übermittlung der Zertifikatsaussage an den Zertifikatsservice

Für die Datenverarbeitung auf Seiten der bescheinigenden bzw. ausgebenden Stellen, das heißt die Erhebung, ggf. Hashing und Übermittlung des (ggf. gehashten) Impf-, Test- oder Genesenenstatus an den Zertifikatsservice sowie die technische Ausgabe des digitalen COVID-Zertifikats sind die bescheinigenden bzw. ausgebenden Stellen jeweils eigenständig verantwortlich. Dass deren Datenverarbeitungsvorgänge nicht in den Verantwortungsbereich des RKI fallen, folgt aus Art. 10 Abs. 6 und 7 DCC-VO, welcher den bescheinigenden bzw. ausgebenden Stellen eine eigene Übermittlungspflicht an den Zertifikatsaussteller (hier: RKI) in Bezug auf die Zertifikatsaussage auferlegt. Entsprechendes ergibt sich auch aus § 22 Abs. 5 bis 7 IfSG, welcher die datenschutzrechtlichen Grundlagen im Sinne des Art. 6 Abs. 1 lit. e in Verbindung mit Art. 9 Abs. 2 lit. i DSGVO für die Übermittlung der für die Generierung des jeweiligen digitalen COVID-Zertifikats erforderlichen personenbezogenen Daten durch die bescheinigenden Stellen an das RKI schafft.

7.2.2 Verarbeitung durch Zertifikatsservice

Für die technische Erstellung und Generierung bzw. Ausstellung des digitalen COVID-Zertifikats durch den Zertifikatsservice ist das RKI zuständig (§ 22 Abs. 5 bis 7 IfSG, dort jeweils Satz 3).

Vorliegend hat jedoch nicht das RKI, sondern der europäische Gesetzgeber die Zwecke und Mittel der Verarbeitung durch die DCC-VO weitgehend festgelegt. Weitere Konkretisierungen sind durch die Interoperabilitätsleitlinien des eHealth-Netzwerks erfolgt.

Dabei hat der europäische Gesetzgeber in Art. 10 Abs. 6 DCC-VO von der in Art. 4 Nr. 7 Hs. 2 DSGVO vorgesehenen Möglichkeit Gebrauch gemacht und Kriterien zur Bestimmung des Verantwortlichen festgelegt. Verantwortlich für die für die Durchführung der DCC-VO notwendige Datenverarbeitung ist demnach die Stelle, die die digitalen COVID-Zertifikate im jeweiligen Mitgliedsstaat ausstellt, in Deutschland also das RKI.

Da die DCC-VO nur Festlegungen zur Datenverarbeitung für die Ausstellung der digitalen COVID-Zertifikate zum Zweck der EU-Freizügigkeit trifft, folgt aus Art. 10 Abs. 6 DCC-VO jedoch keine Verantwortlichkeit des RKI auch für eine Verarbeitung zu anderen nationalen Zwecken, beispielsweise für die Erleichterung der Inanspruchnahme von Ausnahmen von Schutzmaßnahmen des Bundes oder der Länder.

Die Verantwortlichkeit des RKI für eine solche Verarbeitung zu nationalen Zwecken durch den Zertifikatsservice folgt aus § 22 Abs. 5 bis 7 IfSG. Mit diesen wurde eine nationale Rechtsgrundlage für die Verarbeitung der für die Generierung der digitalen COVID-Zertifikate erforderlichen personenbezogenen Daten durch das RKI und für die Übermittlung dieser Daten durch die bescheinigenden bzw. ausgebenden Stellen an das RKI geschaffen. Die für die digitalen COVID-Zertifikate erforderlichen Angaben ergeben sich für Impfzertifikate aus § 22 Abs. 5 in Verbindung mit § 22 Abs. 2 S. 1 und Abs. 4 IfSG, für Genesenenzertifikate aus § 22

Abs. 6 IfSG und für Testzertifikate aus § 22 Abs. 7 IfSG. Dadurch hat der deutsche Gesetzgeber den Zweck und die wesentlichen Mittel der Verarbeitung und die datenschutzrechtliche Verantwortlichkeit des RKI für die personenbezogene Datenverarbeitung für den Zweck der technischen Generierung und Signierung von digitalen COVID-Zertifikaten hinreichend konkret festgelegt.

Zudem werden die öffentlichen Schlüssel, Business Rules und Value Sets der Mitgliedstaaten regelmäßig von der CovPass-App sowie der CovPassCheck-App vom Zertifikatsservice heruntergeladen. Dabei fallen Zugriffsdaten an. Auch die Zugriffsdaten werden durch das RKI als Verantwortlichen verarbeitet.

7.2.3 Verarbeitung durch die CovPass-App

Eine datenschutzrechtliche Verantwortlichkeit der Nutzer der CovPass-App liegt nah, wenn und soweit diese die digitalen COVID-Zertifikate von anderen Personen in der CovPass-App speichern und dies nicht in den Bereich ausschließlich persönlicher oder familiärer Tätigkeiten (Art. 2 Abs. 2 lit. c DSGVO) fällt, beispielsweise bei einer Speicherung für einen Arbeitskollegen während einer beruflich motivierten Reise. Regelmäßig wird der ausschließlich persönliche oder familiäre Bereich jedoch nicht verlassen werden (z. B. bei einer Speicherung des digitalen COVID-Zertifikats durch den Nutzer als gesetzlicher Vertreter der anderen Person). Ob ein solcher Sachverhalt unter die Ausnahme des Art. 2 Abs. 2 lit. c DSGVO fällt, kann nur im konkreten Einzelfall bewertet werden.

7.2.4 Verarbeitung durch die CovPassCheck-App oder ein anderes Prüfsystem

Personen und Behörden, die ein vorgelegtes digitales COVID-Zertifikat im Papierformat ohne Verwendung eines elektronischen Prüfsystems prüfen (im Sinne einer bloßen Sichtprüfung durch eigenes Personal), verarbeiten regelmäßig keine personenbezogenen Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen, so dass dieser Vorgang nicht in den sachlichen Anwendungsbereich der DSGVO fällt (Art. 2 Abs. 1 DSGVO).

Verwendet die prüfende Stelle zur Prüfung die CovPassCheck-App oder ein anderes Prüfsystem, kommt es jedoch zu einer datenschutzrechtlich relevanten Verarbeitung von personenbezogenen Daten in Gestalt der im QR-Code enthaltenen Informationen auf dem Smartphone oder sonstigen Prüfsystem der prüfenden Stelle.

Zwar hat die prüfende Stelle bei Verwendung eines von einem Dritten hergestellten Prüfsystems (z. B. CovPassCheck-App des RKI) nur geringe Einwirkungsmöglichkeiten auf die Mittel und Zwecke der Datenverarbeitung, die abstrakt bereits durch den jeweiligen Hersteller oder Anbieter (z. B. RKI) vorgegeben worden ist. Regelmäßig hat dieser jedoch keinen Einfluss auf und keine Kenntnis von der möglichen konkreten Datenverarbeitung durch die prüfende Stelle, vielmehr ist diese für ihn anonym.

Die konkrete Festlegung der Zwecke (z. B. Einlasskontrolle) und Mittel (z. B. Auswahl des verwendeten Endgeräts) erfolgt allein durch die prüfende Stelle, zumal es keine Pflicht zur Nutzung eines bestimmten Prüfsystems gibt und geben soll. Die lokale Datenverarbeitung bei der prüfenden Stelle ist regelmäßig auch nicht durch Zwecke des Anbieters oder Herstellers, sondern durch solche der prüfenden Stelle motiviert (z. B. Beschleunigung des Einlasses zu einer Veranstaltung, Prüfung der Einreiseberechtigung). Daher liegt die alleinige Verantwortlichkeit für die lokale Datenverarbeitung durch das jeweilige Prüfsystem bei dem jeweiligen Anwender als die prüfende Stelle.

7.3 Rechtsgrundlagen

Eine Datenverarbeitung ist nur rechtmäßig, wenn sie durch eine wirksame Einwilligung oder einen anderen Zulässigkeitstatbestand legitimiert wird und im Einklang mit den in Art. 5 DSGVO festgelegten Grundsätzen erfolgt. Die Zulässigkeitstatbestände ergeben sich in erster Linie aus Art. 6 DSGVO sowie aus Art. 9 DSGVO, soweit Gesundheitsdaten verarbeitet werden.

7.3.1 RKI

Das RKI kann die in seiner Verantwortlichkeit erfolgende personenbezogene Datenverarbeitung durch die verschiedenen Komponenten und Dienste des Zertifikatsservice auf verschiedene gesetzliche Rechtsgrundlagen im Sinne von Art. 6 Abs. 1 lit. e DSGVO und, soweit Gesundheitsdaten verarbeitet werden, Art. 9 Abs. 2 lit. i DSGVO stützen. Für die lokale Datenverarbeitung durch das Web-Frontend (Hash-Berechnung und Übermittlung an Issuer Service API) benötigt das RKI keine Rechtsgrundlage, da diese Verarbeitung nicht in seiner Verantwortlichkeit erfolgt.

Rechtsgrundlage für die Verarbeitung zu Zwecken der technischen Generierung von digitalen COVID-Zertifikaten im sachlichen und zeitlichen (seit 1. Juli 2021) Anwendungsbereich der DCC-VO durch das RKI ist Art. 10 Abs. 2 DCC-VO, der bestimmt:

> *“Die personenbezogenen Daten, die in den gemäß dieser Verordnung ausgestellten Zertifikaten enthalten sind, dürfen für die Zwecke dieser Verordnung ausschließlich zum Zwecke des Abrufs und der Überprüfung der im Zertifikat enthaltenen Informationen verarbeitet werden, um die Ausübung des Rechts auf Freizügigkeit innerhalb der Union während der COVID-19-Pandemie zu erleichtern. Nach dem Ende der Geltungsdauer dieser Verordnung findet keine weitere Verarbeitung mehr statt.“*

Soweit die Verarbeitung zeitlich vor der Anwendbarkeit der DCC-VO erfolgte oder sie nicht in deren sachlichen Anwendungsbereich fällt ist die Rechtsgrundlage in Bezug auf Impfzertifikate § 22 Abs. 5 S. 4 IfSG, § 22 Abs. 5 IfSG:

> *„Zusätzlich zu der Impfdokumentation ist auf Wunsch der geimpften Person die Durchführung einer Schutzimpfung gegen das Coronavirus SARS-CoV-2 in einem*

digitalen Zertifikat (COVID-19-Impfzertifikat) durch folgende Personen zu bescheinigen:

1. *durch die zur Durchführung der Schutzimpfung berechtigte Person oder*
2. *nachträglich von jedem Arzt oder Apotheker*

Die Verpflichtung nach Satz 1 Nummer 2 besteht nur, wenn dem Arzt oder Apotheker eine Impfdokumentation über eine Schutzimpfung gegen das Coronavirus SARS-CoV-2 vorgelegt wird und er sich zum Nachtrag unter Verwendung geeigneter Maßnahmen zur Vermeidung der Ausstellung eines unrichtigen COVID-19-Impfzertifikats, insbesondere um die Identität der geimpften Person und die Authentizität der Impfdokumentation nachzuprüfen, bereit erklärt hat. Zur Erstellung des COVID-19-Impfzertifikats übermittelt die zur Bescheinigung der Schutzimpfung gegen das Coronavirus SARS-CoV-2 verpflichtete Person die in Absatz 2 Satz 1 und Absatz 4 genannten personenbezogenen Daten an das Robert Koch-Institut, das das COVID-19-Impfzertifikat technisch generiert. Das Robert Koch-Institut ist befugt, die zur Erstellung und Bescheinigung des COVID-19-Impfzertifikats erforderlichen personenbezogenen Daten zu verarbeiten."

Die entsprechende Rechtsgrundlage in Bezug auf Genesenenzertifikate ist § 22 Abs. 6 S. 4 IfSG und in Bezug auf Testzertifikate § 22 Abs. 6 S. 3 IfSG.

Rechtsgrundlage für die notwendige Verarbeitung von Zugriffsdaten der CovPass-App und der CovPassCheck-App in Zusammenhang mit dem Download von öffentlichen Schlüsseln, Business Rules und Value Sets ist Art. 6 Abs. 1 lit. e DSGVO in Verbindung mit § 3 BDSG.

Rechtsgrundlage für die Verarbeitung von Anruferdaten durch die Hotlines ist Art. 6 Abs. 1 lit. e DSGVO in Verbindung mit § 3 BDSG.

7.3.2 Bescheinigende Stellen

Hinsichtlich der Übermittlung der in der DCC-VO festgelegten Datenfelder ergibt sich für die bescheinigenden Stellen aus Art. 10 Abs. 6 DCC-VO eine Übermittlungspflicht an das RKI, die insoweit eine Rechtsgrundlage gemäß Art. 9 Abs. 2 lit. i DSGVO darstellt.

Gemäß § 22 Abs. 5 bis 7 IfSG sind die dort genannten Personen bei Vorliegen bestimmter Voraussetzungen verpflichtet, einer geimpften, getesteten oder genesenen Person auf ihren Wunsch hin ein entsprechendes digitales COVID-Zertifikat auszugeben und dürfen hierzu die zur Erstellung des digitalen COVID-Zertifikats notwendigen Daten an das RKI übermitteln. Insoweit stellt dies eine weitere Rechtsgrundlage für die Erhebung und Übermittlung von Daten

an das RKI dar, soweit diese Daten für die Generierung des gewünschten digitalen COVID-Zertifikats erforderlich sind.[27]

Voraussetzung für die Übermittlung und Verarbeitung ist stets der freiwillige Wunsch des potenziellen Zertifikatsinhabers, sich ein bestimmtes digitales COVID-Zertifikat ausstellen zu lassen.

7.3.3 Prüfende Stellen

Prüfer eines digitalen COVID-Zertifikats können sich auf die bereichsspezifischen Rechtsgrundlagen beispielsweise in der Corona-Einreiseverordnung und der COVID-19-Schutzmaßnahmen-Ausnahmenverordnung und zukünftig voraussichtlich weitere gesetzliche Rechtsgrundlagen stützen, wenn sie sich digitalen COVID-Zertifikate für die Prüfung der Gültigkeit mit der CovPassCheck-App oder einem anderen Prüfsystem vorzeigen lassen.

Sofern der prüfenden Stelle keine gesetzliche Rechtsgrundlage zur Verfügung steht, muss sie eine Einwilligung des Zertifikatsinhabers einholen. Da es sich um Gesundheitsdaten handelt, sind in diesem Fall zusätzlich die Anforderung aus Art. 9 Abs. 2 lit. a DSGVO zu beachten, d. h. es muss eine ausdrückliche Einwilligung eingeholt werden. Die Wirksamkeitsvoraussetzungen einer Einwilligung ergeben sich aus Art. 4 Nr. 7 DSGVO in Verbindung mit Art. 6 Abs. 1 S. 1 lit. a bzw. Art. 9 Abs. 2 lit. a DSGVO sowie Art. 7 DSGVO. Eine wirksame Einwilligung ist demnach jede

- freiwillig,
- für den bestimmten Fall,
- in Kenntnis der Sachlage und
- unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist.[28]

7.3.4 Nutzer der CovPass-App

Soweit digitale COVID-Zertifikate von anderen Personen gespeichert werden und dies nicht unter die Haushaltsausnahme fällt, muss der Nutzer die Zulässigkeit der Verarbeitung durch

[27] Deutscher Bundestag, Beschlussempfehlung und Bericht des Ausschusses für Gesundheit (14. Ausschuss) zu dem Gesetzentwurf der Fraktionen der CDU/CSU und SPD – Drucksache 19/29287 – vom 19.05.2021.

[28] Siehe zu diesen Anforderungen im Einzelnen EDSA, Guidelines 05/2020 on Consent under Regulation 2016/679, Version 1.1, Abschnitt 3, abrufbar unter https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202005_consent_en.pdf (zuletzt abgerufen am 15.10.2020).

Auswahl einer geeigneten Rechtsgrundlage selbst sicherstellen, beispielsweise durch Einholung einer Einwilligung. Die Ausführungen unter 5.8.3 gelten entsprechend.

7.4 Drittlandsübermittlung

Eine Übermittlung der Daten in ein Drittland ist nicht vorgesehen. Soweit das RKI die personenbezogenen Daten durch einen Auftragsverarbeiter verarbeitet, ist eine Übermittlung in ein Drittland im Anwendungsbereich DCC-VO zudem gemäß Art. 10 Abs. 8 untersagt.

7.5 Betroffenenrechte

Soweit das RKI personenbezogene Daten eines Zertifikatsinhabers oder Nutzers der CovPass- oder CovPassCheck-App verarbeitet, stehen dieser Person im Rahmen der gesetzlichen Voraussetzungen die folgenden Betroffenenrechte zu:

- die Rechte aus den Artikeln 15, 16, 17, 18und 21 DSGVO,
- das Recht, die behördliche Datenschutzbeauftragte des RKI zu kontaktieren und ihr Anliegen vorzubringen (Art. 38 Abs. 4 DSGVO) und
- das Recht, sich bei einer Aufsichtsbehörde für den Datenschutz zu beschweren.

Allerdings können diese Betroffenenrechte durch das RKI nur erfüllt werden, wenn das RKI die Daten, auf die sich die geltend gemachten Ansprüche beziehen, dauerhaft oder zumindest längerfristig verarbeitet, beziehungsweise in der Lage ist einzelne Betroffene zu identifizieren. Dies wäre nur möglich, wenn an das RKI übermittelte Daten zur betroffenen Person speichern würde. Dies ist für den Zweck des digitalen COVID-Zertifikats jedoch nicht erforderlich und gemäß Art. 10 Abs. 2 DCC-VO untersagt. Deshalb werden die vorgenannten Betroffenenrechte aus den Artikeln 15, 16, 17, 18 und 21 DSGVO in der Regel ins Leere laufen. Hierüber werden die betroffenen Personen in der Datenschutzerklärung des RKI informiert.

7.6 Weitere datenschutzrechtliche Anforderungen

Bei der Konzeption und Entwicklung des Prüfungsgegenstands wird versucht, die von verschiedenen fachkundigen Organisationen aufgestellten Datenschutzanforderungen an einen digitalen Impf- Test- und Genesenennachweis umzusetzen. Berücksichtigt wurden unter anderem folgende Dokumente:

- eHealth Network, Guidelines on verifiable vaccination certificates – basic interoperability elements, Release 2 vom 12.03.2021,

- Chaos Computer Club (CCC), Impfnachweise beenden keine Pandemie: Sachverständigenauskunft zur Änderung des Infektionsschutzgesetzes und weiterer Gesetze vom 16.05.2021.[29]

8 Bewertung der Notwendigkeit und Verhältnismäßigkeit

Die Verarbeitung von personenbezogenen Daten muss in Anbetracht des jeweils verfolgten Zwecks notwendig und verhältnismäßig sein. Notwendigkeit setzt dabei voraus, dass die Verarbeitung für die vollständige und rechtmäßige Erreichung des verfolgten Zwecks erforderlich ist. Die Verhältnismäßigkeit der Verarbeitung setzt voraus, dass es keine alternativen und datenschutzrechtlich weniger eingreifenden Verarbeitungsformen gibt, um den verfolgten Zweck mit gleicher Wirksamkeit zu erreichen.

8.1 Legitimer Zweck

Um die Ausbreitung von SARS-CoV-2 einzudämmen, haben alle EU-Mitgliedsstaaten umfangreiche Schutzmaßnahmen ergriffen, die mit teilweise intensiven Grundrechtseinschränkungen verbunden sind. Aufgrund wissenschaftlicher Erkenntnisse gilt es heute als erwiesen, dass geimpfte und genesene Personen für ihre Mitmenschen nicht mehr oder nur geringfügig ansteckend sind bzw. im Fall von negativ getesteten Personen eine geringere Ansteckungswahrscheinlichkeit besteht. Daher wurden durch Bund und Länder sowie auf EU-Ebene Erleichterungen und Ausnahmen von Schutzmaßnahmen für geimpfte, getestete und genesene Personen vorgesehen. So soll es ihnen etwa wieder möglich sein, mit einer negativen oder sogar ohne vorherige Testung Ladengeschäfte zu betreten, die Dienstleistungen von Friseuren in Anspruch zu nehmen oder in andere EU-Mitgliedsstaaten einzureisen. Mit dem digitalen COVID-Zertifikat, dessen Ausstellung und Verwendung durch den Prüfgegenstand ermöglicht wird, soll es Personen, die von den geplanten Erleichterungen und Ausnahmen erfasst sind, erleichtert werden, diese in Anspruch zu nehmen und insoweit von ihren Grundrechten und Grundfreiheiten wieder möglichst umfassend Gebrauch zu machen. Dies stellt einen legitimen Zweck dar.

8.2 Eignung

Die Verarbeitung durch den Prüfgegenstand ist zur Förderung des Zwecks geeignet, denn diese erleichtert Geimpften, negativ Getesteten und Genesenen die Verwendung des digitalen COVID-Zertifikats und somit die Inanspruchnahme der bestehenden und geplanten Erleichterungen und Ausnahmen von Schutzmaßnahmen. Dies gilt in besonderem Maße für die Funktion des elektronischen Nachweises mit der CovPass-App, da der überwiegende Teil

[29] https://www.ccc.de/system/uploads/315/original/IfSG_CCC_Marx.pdf (abgerufen am 26.05.2021).

der Bevölkerung ein Smartphone besitzt und dieses ständig mit sich führt. Das digitale COVID-Zertifikat macht das Mitführen und Vorzeigen des (gelben) Impfausweises, einer Impfbescheinigung oder eines Testdokuments überflüssig und beschränkt die zu offenbarenden Daten auf den erforderlichen Mindestdatensatz. Durch die Möglichkeit des Scannens des digitalen COVID-Zertifikats per App können Ladengeschäfte und Dienstleister die Prüfung des Impf- Test- und Genesenenstatus deutlich vereinfachen und beschleunigen, ohne dass weitere personenbezogene Daten der Zertifikatsinhaber (z. B. der Status anderer Schutzimpfungen oder spezifische Testergebnisse und durchgestandene COVID-19-Erkrankung) offenbart werden. Sollte der Zertifikatsinhaber eine Papierversion seines nur in der CovPass-App gespeicherten digitalen COVID-Zertifikats benötigen (beispielsweise weil er keine Papierversion erhalten hat oder sie ihm abhanden gekommen ist), kann er niedrigschwellig auf seinem Smartphone eine ausdruckbare PDF-Version des betreffenden digitalen COVID-Zertifikats erzeugen; das Aufsuchen einer Arztes oder einer Apotheke für das Anfordern einer nachträglichen (erneuten) Ausstellung des betreffenden digitalen COVID-Zertifikats und die dafür notwendige personenbezogene Datenverarbeitung durch die bescheinigende Stelle und das RKI werden dadurch obsolet. Auch können weitere Kontakte und Kosten vermieden werden. Die praktische Erleichterung des Nachweises stellt somit sicher, dass die ungehinderte Ausübung der Grundrechte und Grundfreiheiten möglichst umfassend ermöglicht wird. Solange die gegenwärtige Pandemielage die Aufrechterhaltung der Schutzmaßnahmen und somit Kontrollen des Impf- Test- und Genesenenstatus erfordert, wird somit möglichst umfassend verhindert, dass ein nicht mitgeführtes oder abhandengekommenes Papierdokument die Teilhabe am öffentlichen Leben verhindert.

8.3 Erforderlichkeit

Die Datenverarbeitung ist für die Erfüllung des in Rede stehenden Zwecks erforderlich. Gleich geeignete mildere Mittel sind nicht ersichtlich. Es wird eine konzeptionsbedingt datensparsame Systemarchitektur eingesetzt. Die personenbezogene Verarbeitung ist auf die Ermöglichung der Überprüfung der jeweiligen Zertifikatsaussage unter Verwendung eines QR-Codes beschränkt. Um digitale COVID-Zertifikate signieren und ihre Gültigkeit überprüfen zu können, müssen diese Daten durch eine zentrale Serverkomponente (Zertifikatsservice) verarbeitet werden. Eine darüberhinausgehende Verarbeitung der Daten auf einem zentralen Server erfolgt jedoch nicht, so dass die Datenverarbeitung mit Blick auf den verfolgten Zweck minimal ist. Insbesondere erfordern das Anzeigen der Prüfansicht des gespeicherten digitalen COVID-Zertifikats in der CovPass-App und die Überprüfung von digitalen COVID-Zertifikaten mit der CovPassCheck-App keine dauerhafte Internetverbindung. Die Erzeugung einer Papierversion eines in der CovPass-App gespeicherten digitalen COVID-Zertifikats findet ausschließlich lokal auf dem Smartphone statt. Es wird auch keine zentrale Datenverwaltung eingeführt. Die verwendeten Datenfelder werden durch die DCC-VO konkret vorgegeben. In diesem Umfang ist die Datenverarbeitung erforderlich, um die Interoperabilität zu ermöglichen. Dies galt auch bereits vor Inkrafttreten der DCC-VO, da die ausgegebenen Zertifikate auch ab dem 01.07.2021 europaweit genutzt werden können sollten. Durch die Verwendung der eindeutigen Zertifikatskennung wird bei der Verarbeitung ein Indikator verwendet, der von der tatsächlichen Identität der betroffenen Person so weit wie möglich entfernt ist. Dadurch wird bei der Verarbeitung ein Ansatz verfolgt, der die Beeinträchtigung der Rechte und Freiheiten der

betroffenen Personen auf ein Mindestmaß reduziert. Eine gänzlich anonyme Technikgestaltung würde die eindeutige Zuordenbarkeit der digitalen COVID-Zertifikate verhindern und dadurch das Ziel der Sicherstellung der Authentizität ausgestellter digitaler COVID-Zertifikate vereiteln. Sie kann daher kein gleich geeignetes, milderes Mittel darstellen. Im Rahmen der Ergebnisdarstellung in der CovPassCheck-App wurde sichergestellt, dass nur diejenigen spezifischen Angaben offengelegt werden, die für die prüfende Stelle im Rahmen der Prüfung relevant sind. Insbesondere wird zwischen Impf- und Genesenenzertifikaten bei der Ergebnisdarstellung nicht differenziert. Eine prüfende Stelle erfährt daher nicht, ob ein Impf- oder ein Genesenenzertifikat geprüft wurde. Für Testzertifikate kommt es aufgrund der regionalen Unterschiede für die Anforderungen an die Aktualität eines Negativtestats auf weitere Angaben an, so dass die die Art des geprüften Zertifikats und der Zeitpunkt der Probenahme im Rahmen der Prüfung offengelegt werden müssen, um die intendierten Zwecke des Verfahrens erreichen zu können. Name und Geburtsdatum des Zertifikatsinhabers werden in der CovPassCheck-App nur offengelegt, sofern das Zertifikat gültig ist. Andernfalls kann der Zweck der Vorlage des Zertifikats ohnehin nicht erreicht werden, so dass dann auch die Prüfung und Offenlegung der Identität nicht erforderlich ist.

8.4 Angemessenheit

Die Datenverarbeitung ist zur Erreichung des im Interesse der Allgemeinheit verfolgten und individuell gewünschten Ziels der Nutzer angemessen. Eine Verarbeitung ist zur Erreichung eines Zweckes angemessen, wenn die konkrete Interessenabwägung im Rahmen einer Zweck-Mittel-Relation zugunsten des Verantwortlichen ausfällt. Es sind daher die Interessen der betroffenen Personen mit den Interessen des Verantwortlichen abzuwägen. Im Fall des Prüfgegenstands stehen sich vor allem die Interessen des Verantwortlichen (RKI) und die Interessen der Zertifikatsinhaber gegenüber.

Soweit der Prüfgegenstand dem einfacheren Nachweis des Impf-, Test- oder Genesenenstatus unter Verwendung von digitalen COVID-Zertifikaten dient, sind die Interessen der (potenziellen) Zertifikatsinhaber und des Verantwortlichen insoweit gleichgerichtet. Demgegenüber stehen die Interessen der Zertifikatsinhaber, nicht einer Überwachung, gesellschaftlichem Druck zur Nutzung des digitalen COVID-Zertifikats oder rechtlichen, wirtschaftlichen oder sozialen Nachteilen infolge der Nichtnutzung ausgesetzt zu sein.

Zugunsten der Angemessenheit spricht die Freiwilligkeit der Nutzung. Damit wird dem Recht auf informationelle Selbstbestimmung des Einzelnen Ausdruck verliehen. Es soll niemand von staatlichen Stellen dazu gezwungen werden, die CovPass-App zu nutzen. Es steht jedem frei, ein digitales COVID-Zertifikat zu beantragen und dieses in der CovPass-App zu speichern. Entscheidet sich eine Person gegen die Erstellung des digitalen COVID-Zertifikats und dessen Verwendung mit der CovPass-App, kann sie ihren Impf-, Test- oder Genesenenstatus weiterhin auf herkömmliche Weise nachweisen, beispielsweise durch Vorlage des gelben Impfausweises. Zudem ist die Dauer der Verarbeitungsvorgänge zeitlich beschränkt. Es erfolgt im Rahmen der Ausstellung des COVID-Zertifikats nur eine temporäre Verarbeitung auf den Systemen des RKI. Eine Speicherung geprüfter Zertifikate bei der prüfenden Stelle oder eine sonstige Persistierung der COVID-Zertifikate erfolgt nicht, alle im Zusammenhang mit den

COVID-Zertifikaten verarbeiteten personenbezogenen Daten werden gem. Art. 10 Abs. 4 DCC-VO nur für den unbedingt erforderlichen Zeitraum gespeichert. Auch ist die Gesamtdauer des Verfahrens durch jedenfalls gem. Art. 17 DCC-VO zeitlich beschränkt. An der Freiwilligkeit der Nutzung bestehen keine Bedenken. Die den digitalen COVID-Zertifikaten zugrundeliegende Technologie ermöglicht auch keine Profilerstellung oder Bewegungsverfolgung und führt auch keinen zentralverwalteten Datenbestand im Sinne einer zentralen Impfdatenbank oder eines Genesenenregisters ein. Eine Verarbeitung der erhobenen Daten zu einem anderen als den durch die DCC-VO oder nationales Recht vorgesehenen Zwecken ist gemäß Art. 10 Abs. 2 DCC-VO ausgeschlossen. Somit ist die Verarbeitung im Hinblick auf Zweck, Umfang und Dauer eng beschränkt. Die Angemessenheit der Verarbeitung durch das RKI ist damit gewahrt.

9 Risikoanalyse

9.1 Methodik

Grundlage und Hilfsmittel für die Planung, Durchführung und Dokumentation der Risikoanalyse im Rahmen dieser DSFA ist die Excel-Tabelle (Risiko-Matrix), die auch bei der Risikoanalyse der CWA zum Einsatz kommt.

Die Risiko-Matrix ist konzipiert worden, um eine integrierte Betrachtung klassischer Datensicherheitsziele (Verfügbarkeit, Integrität, Vertraulichkeit) aus Unternehmens- bzw. Behördensicht einerseits und der Datenschutzziele andererseits, zu denen – neben Verfügbarkeit, Integrität und Vertraulichkeit – etwa auch Zweckbindung, Datenminimierung, Transparenz und Nichtverkettbarkeit gehören, zu ermöglichen. Sie ermöglicht ein systematisches Vorgehen unter Berücksichtigung verschiedener Blickwinkel (Betrachtung spezifischer Risikoquellen, Schadenspotentiale für verschiedene Betroffenengruppen) und die zeitversetzte Durchführung von Risikobewertungen durch verschiedene Projektbeteiligte sowie die flexible Anpassung an Designentscheidungen und Anforderungen von Entwicklern, externen Beratern und Aufsichtsbehörden.

9.2 Risiko-Identifikation

Um zu identifizieren, wie, durch wen oder was und unter welchen Umständen Risiken für die Rechte und Freiheiten natürlicher Personen ausgelöst werden können, wurde – dem Praxishandbuch des Forum Privatheit angelehnt[30] – in folgenden Schritten vorgegangen:

(1) Identifikation der Risikoquellen

[30] Martin/Friedewald/Schiering/Mester/Hallinan: „Die Datenschutzfolgenabschätzung nach Art. 35 DSGVO – Ein Handbuch für die Praxis“, Frauenhofer Verlag, 2020.

(2) Identifikation der Bedrohungen/Risiken
(3) Zuordnung von Bedrohungen/Risiken zu Betroffenen

9.3 Risikoquellen

Risikoquellen sind zum einen Personen, die ein Interesse daran haben könnten, die Verarbeitungsvorgänge und die damit verarbeiteten Daten in unrechtmäßiger Weise zu verwenden. Aber auch Stellen, die eine rechtmäßige Datenverarbeitung bezwecken, können ein Risiko darstellen.

Folgende Risikoquellen für die Rechte und Freiheiten natürlicher Personen wurden identifiziert:

- App-Nutzer/Zertifikatsinhaber
- Hacker
- (Kommerzielle) Datensammler
- Technologiehersteller (Hersteller der Betriebssysteme unterstützter Smartphones)
- Softwareentwickler
- Betreiber von im Rahmen der Erstellung der COVID-Zertifikate verwendeten Systemkomponenten
- (ehemaliges) Personal
- Versicherungen/Arbeitgeber
- Kriminelle
- (Medizinisches) Personal der bescheinigenden bzw. ausgebenden Stellen
- Geheimdienst/Regierung/Sicherheits- und Gesundheitsbehörden.

Einzelheiten können dem Tabellenblatt „Angreifertyp und Motivation“ der Risiko-Matrix entnommen werden.

9.3.1 Bedrohungen/Risiken

Die Bedrohungen/Risiken werden, ausgehend von den Schutzzielen und den Betroffenenrechten, den folgenden Risikokategorien zugeordnet:

- Unbefugte oder unrechtmäßige Verarbeitung
- Verarbeitung wider Treu und Glauben
- Für die Betroffenen intransparente Verarbeitung
- Ungerechtfertigter Datentransfer in Drittland
- Unbeabsichtigter Verlust, Zerstörung oder Schädigung von Daten
- Verweigerung der Betroffenenrechte;
- Verwendung der Daten zu inkompatiblen Zwecken;
- Verarbeitung nicht richtiger Daten;
- Fehlerhafte Verarbeitung (technische Störungen, menschliche Fehler);

- Verarbeitung über die Speicherfrist hinaus;
- Die Verarbeitung an sich, wenn der Schaden in der Durchführung der Verarbeitung selbst liegt.

Die identifizierten Bedrohungen/Risiken speisen sich aus folgenden Quellen:

- Risikoszenarien, die von fachkundigen Organisationen identifiziert worden sind
- Risikobetrachtungen durch die Projektbeteiligten
- Ergebnisse der Workstreams
- Ergebnisse aus dem Threat Modelling für die Komponenten CovPass-App CovPassCheck-App und Zertifikatsservice.

9.3.2 Zuordnung der Risiken zu Betroffenengruppen

Um eine differenzierte Bewertung der identifizierten Risiken zu ermöglichen, werden diese den potenziellen Betroffenengruppen zugeordnet. Vorliegend sind die von den Risiken betroffenen Personen primär die Zertifikatsinhaber, also Personen, die ein digitales COVID-Zertifikat beantragt haben.

9.3.3 Benennung des Risikoverantwortlichen

Jedes identifizierte Risiko wird einem primären Risikoverantwortlichen zugeordnet. Der Risikoverantwortliche hat die Aufgabe oder die Möglichkeit, Gegenmaßnahmen zur Bewältigung des identifizierten Risikos umzusetzen.

9.3.4 Bewertung der Eintrittswahrscheinlichkeit

Die Eintrittswahrscheinlichkeit (Wahrscheinlichkeit im Sinne der ISO 27005) ist ein Schätzwert für das Eintreten eines Risikos, der in dieser DSFA anhand des auf dem Tabellenblatts „Eintrittswahrscheinlichkeiten“ beschriebenen 4-Stufenmodells bestimmt worden ist. Die Wahrscheinlichkeit des Eintritts eines Ereignisses hängt von der Motivation, den Möglichkeiten und Fähigkeit sowie den Ressourcen des Angreifertyps sowie den implementierten technischen und organisatorischen Maßnahmen ab. Als Hilfestellung und auch zur Nachvollziehbarkeit der Grundlagen der DSFA werden in einem Tabellenblatt der Risiko-Matrix „Angreifertypen und Motive“ dargestellt.

9.3.5 Bewertung des Schadensausmaßes

Der potenzielle Schaden für betroffene Personen wird anhand der zu betrachtenden Gewährleistungsziele Datenminimierung, Vertraulichkeit, Integrität, Verfügbarkeit,

Authentizität, Resilienz, Intervenierbarkeit, Transparenz, Zweckbindung/Nichtverkettung geschätzt:

Schutzziel	Definition
Datenminimierung	Personenbezogene Daten müssen dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein. Hierzu gehört auch die Speicherbegrenzung / Löschung nach Zweckerreichung oder -wegfall.
Vertraulichkeit	Personenbezogene Daten dürfen nur einem berechtigten Personenkreis für bestimmte Zwecke offenbart werden. Sie sind vor unbefugter Veränderung zu schützen.
Integrität	Integrität von Daten ist die Abwesenheit von korrumpierten Daten. Integrität bedeutet insbesondere die Abwesenheit unautorisierter Veränderungen.
Verfügbarkeit	Verfügbarkeit von Informationen und Systemen ist Zugreifbarkeit und Nutzbarkeit durch autorisierte Entitäten bei Bedarf.
Authentizität	Authentizität bedeutet, dass die Daten tatsächlich von der Quelle kommen, die angegeben wird; also weder Fälschung noch Fehlzuschreibung.
Resilienz	Resilienz bezeichnet die Fähigkeit, Störungen ohne anhaltende Belastungen zu überwinden.
Intervenierbarkeit	Betroffene Personen müssen die Möglichkeit haben, ihre entsprechend der DSGVO gewährten Rechte ungehindert auszuüben. Datenverarbeitungen müssen so gestaltet werden, dass Daten berichtigt und gelöscht werden können.
Transparenz	Personenbezogene Daten müssen in einer für die betroffene Person nachvollziehbaren Weise erhoben und verarbeitet werden.
Zweckbindung/ Nichtverkettung	Personenbezogene Daten sind nur im Rahmen des ursprünglichen Zweckes der Verarbeitung zu verwenden und nicht mit anderen Daten zusammenzuführen. Dementsprechend darf im Laufe der Verarbeitungsprozesse stets nur der ursprünglich festgelegte Zweck verfolgt werden.

Es wird geprüft, inwiefern Bedrohungen/Ereignisse zum Eintritt eines physischen, materiellen oder immateriellen Schadens für die betroffenen Personen führen können. Für jedes Szenario wird dabei geprüft, welche Gewährleistungsziele tangiert sind.

Für die einzelnen Schutzziele wird im Risikoregister die potenzielle Schadenshöhe in Kategorie 1 – gering, Kategorie 2 – begrenzt, Kategorie 3 – hoch und Kategorie 4 – sehr hoch anhand des Tabellenblattes „Schadenskategorien“ in der Risikomatrix bestimmt.

Es handelt sich um eine qualitative Bewertung der jeweiligen Bedrohungen bezogen auf das jeweilige Schutzziel/Gewährleistungsziel. Dabei ist die Tabelle lediglich ein Hilfsmittel; die qualitative Bewertung kann unabhängig von der Risikozahl sowohl grundsätzlich als auch für bestimmte Aspekte ergänzend im DSFA-Bericht und in mitgeltenden Dokumenten beschrieben werden, soweit dies geboten erscheint. Dies betrifft insbesondere die Risiken hinsichtlich der verwendeten Rechtsgrundlagen, da die Risiken für betroffene Personen hier nicht nur auf einzelne Schutzziele wirken, sondern vielmehr auch grundsätzliche Fragen der Rechtmäßigkeit der Datenverarbeitung und Akzeptanz betreffen können.

Die folgende Abbildung zeigt die Klassifizierung der Risiken und enthält gleichzeitig einen Vorschlag für die Priorisierung durch Ampelfarben. Automatisch wird in der Risikomatrix durch Multiplikation des Wertes der Eintrittswahrscheinlichkeit mit dem Wert der Schadenskategorie eine Risikoklasse gebildet, wobei der höchste Schadenskategoriewert zugrunde gelegt wird.

Kategorie	Risikoklasse	Beschreibung
Niedrig	0-4	Die Auswirkungen des Schadens für betroffene Personen sind begrenzt und beherrschbar. Das Eintreten einer zu berücksichtigten Schadenssituation erscheint unmöglich.
Mittel	5-7	Der Schadenseffekt wäre nennenswert. Technische und organisatorische Maßnahmen SOLLEN vorgeschlagen werden. Als Teil der Kosten-Nutzen-Abwägung der notwendigen Maßnahmen kann das Risiko akzeptiert werden.
	8-10	Signifikante Schäden können nicht komplett ausgeschlossen werden, aber eine existenzbedrohende Situation erscheint unwahrscheinlich. Technische und organisatorische Maßnahmen MÜSSEN vorgeschlagen und innerhalb einer festgelegten Frist umgesetzt werden (siehe hierzu Tabellenblatt „Maßnahmenplanung“). Die Reduktion von Risiken durch technische und organisatorische Maßnahmen und/oder Kontrollen ist notwendig. Eine Risikoakzeptanz basierend auf einer Kosten-Nutzen-Betrachtung der geplanten Handlungen bedarf einer besonderen Managementbetrachtung. Die zuständige Aufsichtsbehörde SOLL konsultiert werden.
Hoch	11-16	Schadenseffekte können katastrophale oder existenzbedrohende Ausmaße annehmen. Das Eintreten des Risikos hat signifikante negative Auswirkungen. Dieses Risiko bedarf sofortiger Aufmerksamkeit. Eine Akzeptanz dieses Risikos ist ausgeschlossen. Eine Reduktion

		des Risikos durch hierauf abgestimmte technische und organisatorische Maßnahmen ist notwendig; die Berücksichtigung systematischer und strategischer Maßnahmen wird empfohlen. Die Aufsichtsbehörde MUSS konsultiert werden.

Die Maßnahmen können dem Katalog der Referenzmaßnahmen des Standard-Datenschutzmodells[31] (SDM) zugeordnet werden, die im Tabellenblatt „Maßnahmen“ hinterlegt sind. Nach dem SDM werden jedem Gewährleistungsziel spezifische technische und organisatorische Abhilfemaßnahmen zugeordnet, mittels derer das Ziel und die dahinterstehenden Anforderungen der DSGVO gewährleistet und der Eintritt des Schadensereignisses verhindert werden können.

Die Bewertung der Risiken erfolgt auf Basis der etablierten Schutzmaßnahmen und Designentscheidungen. Die Risikomatrix ist generell auf die Durchführung einer Brutto-Risikobetrachtung (ohne Maßnahmen) und einer Netto-Risikobetrachtung (nach Maßnahmenergreifung) angelegt.

9.4 Maßnahmen zur Risikobehandlung

Nachfolgend werden stichwortartig zentrale technische und organisatorische Maßnahmen aufgeführt, die vom RKI getroffen wurden, um die identifizierten Risiken für die betroffenen Personen zu reduzieren:

1. Pseudo- oder Anonymisierung, soweit möglich;
2. Trennung von Teilprozessen/Diensten durch Verwendung verschiedener Server;
3. Restriktive Berechtigungskonzepte und Autorisierungsprozesse für alle Backend-Komponenten zur Beschränkung der Zugriffsmöglichkeiten des Personals bei den an der Datenverarbeitung beteiligten Unternehmen (auch als Bestandteil von Pseudonymisierungsmaßnahmen);
4. Reduzierung von Datenübermittlungen;
5. Reduzierung der Übermittlung von direkt personenbezogenen Daten auf ein Minimum, d.h. lediglich bei der Ausstellung von Impfzertifikaten, falls die Anbindungslösung keine geeignete Hash-Wert-Bildung ermöglicht (PVS); sofortige Löschung dieser Daten nach Generierung des Hash-Wertes.
6. Verschlüsselte Datenübertragung zwischen CovPass-App bzw. der CovPassCheck-App und dem Public Key Storage/CA Distribution Service sowie zwischen Zertifikatsservice und den bescheinigenden Stellen;

[31] *DSK*, Das Standard-Datenschutzmodell Version 2.0b, abrufbar unter: https://www.datenschutzzentrum.de/sdm/ (zuletzt abgerufen am 25.05.2021).

7. Verzicht auf jegliche dauerhafte zentrale Speicherung von Zertifikatsaussagen oder COVID-Zertifikaten;
8. Die Speicherung der Daten auf allen Komponenten erfolgt verschlüsselt;
9. Keine dauerhafte Speicherung von den aus QR-Codes ausgelesenen und geprüften COVID-Zertifikaten in der CovPassCheck-App;
10. Verzicht der differenzierten Anzeige des geprüften Zertifikatstyps in der CovPassCheck-App (lediglich Testzertifikate werden als solche mit dem Typ und Zeitpunkt der Probenahme differenziert angezeigt);
11. Implementierung von Betriebs-, Sicherheits- und Datenschutzkonzepten zur Minimierung von Ausfallzeiten und zur Gewährleistung von Sicherheits- und Datenschutzanforderungen.

Konkrete technische und organisatorische Maßnahmen werden unter Ziffer 5 und in den Begleitdokumenten beschrieben.

Weitere Informationen (insbesondere in Form von Quellcode) zu bei der Durchführung der Risikoanalyse berücksichtigten technischen Maßnahmen hinsichtlich einzelner Komponenten können teilweise auch der bis zum jeweiligen Berichtszeitraum der Risikoanalyse versionierten GitHub-Projektdokumentation entnommen werden.[32]

9.5 Bewertung der Restrisiken

Die identifizierten Risiken und die diesbezüglich ergriffenen bzw. geplanten Risikobehandlungsmaßnahmen wurden im Rahmen der Durchführung der DSFA ausführlich behandelt und im Projektverlauf berücksichtigt.

Im Rahmen der fortgesetzten Risikoanalyse wurden weiterhin keine hohen Restrisiken identifiziert.

Die nach Umsetzung der Risikobehandlungsmaßnahmen noch verbleibenden Risiken werden als akzeptabel bewertet. Das RKI wird als verantwortliche Stelle jedoch fortlaufend beobachten müssen, ob Umstände eintreten, die eine Neubewertung der Ergebnisse der Risikoanalyse notwendig erscheinen lassen.

10 Nachhaltige Sicherung des Datenschutzes

In regelmäßigen Abständen müssen Kernelemente des Datenschutzes im Rahmen eines wirksamen Datenschutzmanagements überprüft werden.

[32] Vgl. Dokumentation auf GitHub, abrufbar unter https://github.com/Digitaler-Impfnachweis (zuletzt abgerufen am 12.08.2021).

10.1 Evaluierung

Die EU-Kommission wird gemäß Art. 16 der DCC-VO die Effektivität des digitalen COVID-Zertifikats auf Basis der von den Mitgliedstaaten zu meldenden Statistiken und Erkenntnisse insbesondere in Bezug auf die Auswirkungen auf die Erleichterung der Freizügigkeit von Unionsbürgern und ihren Familienangehörigen sowie auf den Schutz personenbezogener Daten während der COVID-19-Pandemie umfassend aus europäischer Perspektive bewerten. Dem Ergebnisbericht der EU-Kommission können Legislativvorschläge beigefügt werden, insbesondere zur Verlängerung der Geltungsdauer der DCC-VO, wobei die Entwicklung der epidemiologischen Situation der Pandemie zu berücksichtigen ist.

Die im Rahmen des Prüfungsgegenstands getroffenen technischen und organisatorischen Maßnahmen werden vom RKI laufend bewertet und erforderlichenfalls weiterentwickelt. Eine turnusmäßige systematische Evaluation des gesamten Prüfungsgegenstands durch das RKI ist aufgrund seines zeitlich und zweckbedingt begrenzten Einsatzes nicht vorgesehen. Jedoch werden die Erfahrungen aus dem Betrieb und das Feedback der Nutzer und der Öffentlichkeit vom RKI laufend ausgewertet werden, um die Qualität und die Eignung der Prozesse zu untersuchen und erforderlichenfalls zu verbessern.

10.2 Nächster Prüfungstermin

Der Einsatz des Prüfungsgegenstands ist befristet und wird einer laufenden Analyse und Weiterentwicklung mit begleitender DSFA unterliegen. Dies gilt auch für jedes Release einer neuen Version der CovPass-App, der CovPassCheck-App oder des Zertifikatsservice. Eine Festlegung von planmäßigen Wiederholungs- bzw. Aktualisierungsterminen für die vorliegende DSFA wäre zum jetzigen Zeitpunkt daher nicht sachgerecht und ist somit nicht vorgesehen.

10.2.1.1 Anlagen

(1) Anlage 1: Risikomatrix zum DSFA Bericht (Stand 11.08.2021)

(2) Anlage 2: Begleitdokumente

a. BG 1: Technisch-organisatorische Maßnahmen der Ubirch GmbH in Bezug auf den Zertifikatsservice (Stand 06/2021)

b. BG 2: Technisch-organisatorische Maßnahmen und Datenschutzkonzept der Bechtle Onsite GmbH in Bezug auf die technische Hotline (Version 4.0)

c. BG 3: Technisch-organisatorische Maßnahmen der KDO Service GmbH in Bezug auf das Hosting des Zertifikatsservice (Stand: 06.05.2021)

d. BG 4: Handbuch zum Zertifikatsservice für medizinisches Personal der Impfstellen

e. BG 5: Handbuch zum Zertifikatsservice für IT-Verantwortliche der Impfstellen

f. BG 6: Datenschutzhinweise CovPass-App (Fassung vom 19.08.2021)

g. BG 7: Datenschutzhinweise CovPassCheck-App (Fassung vom 12.08.2021)

h. BG 8: Datenschutzhinweise zum digitalen COVID-Zertifikat (Fassung vom 21.06.2021)