►B

DURCHFÜHRUNGSBESCHLUSS (EU) 2021/1073 DER KOMMISSION

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

(Text von Bedeutung für den EWR)

(ABl. L 230 vom 30.6.2021, S. 32)

Geändert durch:

		Amtsblatt		
		Nr.	Seite	Datum
►M1	Durchführungsbeschluss (EU) 2021/2014 der Kommission vom 17. November 2021	L 410	180	18.11.2021
►M2	Durchführungsbeschluss (EU) 2021/2301 der Kommission vom 21. Dezember 2021	L 458	536	22.12.2021
►M3	Durchführungsbeschluss (EU) 2022/483 der Kommission vom 21. März 2022	L 98	84	25.3.2022
►M4	Durchführungsbeschluss (EU) 2022/1516 der Kommission vom 8. September 2022	L 235	61	12.9.2022

▼B

DURCHFÜHRUNGSBESCHLUSS (EU) 2021/1073 DER KOMMISSION

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

(Text von Bedeutung für den EWR)

Artikel 1

Die technischen Spezifikationen für das digitale COVID-Zertifikat der EU, in denen die allgemeine Datenstruktur, die Verschlüsselungsmechanismen und der Transportverschlüsselungsmechanismus in einem maschinenlesbaren optischen Format festgelegt sind, sind in Anhang I aufgeführt.

Artikel 2

Die Regelungen für das Füllen der in Artikel 3 Absatz 1 der Verordnung (EU) 2021/953 genannten Zertifikate sind in Anhang II aufgeführt.

Artikel 3

Die Anforderungen an die gemeinsame Struktur der eindeutigen Zertifikatkennung sind in Anhang III aufgeführt.

▼M1

Artikel 4

Die Vorschriften für die Verwaltung der Public-Key-Zertifikate in Bezug auf das „EU Digital COVID Certificate Gateway“ zur Unterstützung der Interoperabilitätsaspekte des Vertrauensrahmens sind in Anhang IV festgelegt.

Artikel 5

Eine gemeinsame koordinierte Datenstruktur für die in die Zertifikate gemäß Artikel 3 Absatz 1 der Verordnung (EU) 2021/953 aufzunehmenden Daten unter Verwendung eines JSON-Schemas (JavaScript Object Notation schema) ist in Anhang V dieses Beschlusses festgelegt.

▼M3

Artikel 5a

Austausch von Zertifikatswiderrufslisten

(1) Der Vertrauensrahmen für das digitale COVID-Zertifikat der EU ermöglicht den Austausch von Zertifikatswiderrufslisten über das zentrale Gateway für das digitale COVID-Zertifikat der EU (im Folgenden das „Gateway“) im Einklang mit den technischen Spezifikationen in Anhang I.

(2) Wenn Mitgliedstaaten digitale COVID-Zertifikate der EU widerrufen, können sie Zertifikatswiderrufslisten an das Gateway übermitteln.

▼M3

(3) Übermitteln Mitgliedstaaten Zertifikatswiderruflisten, so führen die ausstellenden Behörden eine Liste der widerrufenen Zertifikate.

(4) Werden personenbezogene Daten über das Gateway ausgetauscht, ist die Verarbeitung darauf beschränkt, den Austausch von Informationen über den Widerruf zu unterstützen. Diese personenbezogenen Daten dürfen nur zur Überprüfung des Widerrufsstatus von im Rahmen der Verordnung (EU) 2021/953 ausgestellten digitalen COVID-Zertifikaten der EU verwendet werden.

(5) Die an das Gateway übermittelten Informationen enthalten gemäß den technischen Spezifikationen in Anhang I folgende Angaben:

a) die pseudonymisierten eindeutigen Zertifikatkennungen der widerrufenen Zertifikate,

b) das Ablaufdatum der übermittelten Zertifikatswiderrufsliste.

(6) Widerruft eine ausstellende Behörde digitale COVID-Zertifikate der EU, die sie gemäß der Verordnung (EU) 2021/953 oder der Verordnung (EU) 2021/954 ausgestellt hat, und möchte sie entsprechende Informationen über das Gateway austauschen, so übermittelt sie die in Absatz 5 genannten Informationen im Einklang mit den technischen Spezifikationen in Anhang I in Form von Zertifikatswiderrufslisten in einem sicheren Format an das Gateway.

(7) Die ausstellenden Behörden bieten so weit wie möglich eine Lösung an, um die Inhaber widerrufener Zertifikate zum Zeitpunkt des Widerrufs über den Widerrufsstatus ihrer Zertifikate und den Grund für den Widerruf zu informieren.

(8) Über das Gateway werden die eingegangenen Zertifikatswiderrufslisten zusammengetragen. Zudem werden darüber Instrumente bereitgestellt, um die Listen an die Mitgliedstaaten weiterzugeben. Das Gateway löscht die Listen automatisch, wenn das von den übermittelnden Behörden für jede Liste angegebene Ablaufdatum erreicht ist.

(9) Die benannten nationalen Behörden oder amtlichen Stellen der Mitgliedstaaten, die personenbezogene Daten im Gateway verarbeiten, sind gemeinsam Verantwortliche für die verarbeiteten Daten. Die jeweiligen Zuständigkeiten der gemeinsam Verantwortlichen werden gemäß Anhang VI zugewiesen.

(10) Die Kommission ist die Auftragsverarbeiterin der personenbezogenen Daten, die im Gateway verarbeitet werden. In ihrer Eigenschaft als Auftragsverarbeiterin im Auftrag der Mitgliedstaaten gewährleistet die Kommission die sichere Übermittlung und das sichere Hosting personenbezogener Daten innerhalb des Gateways und erfüllt die Pflichten des Auftragsverarbeiters gemäß Anhang VII.

(11) Die Wirksamkeit technischer und organisatorischer Maßnahmen zur Gewährleistung der Sicherheit bei der Verarbeitung personenbezogener Daten im Gateway wird von der Kommission und den gemeinsam Verantwortlichen regelmäßig geprüft, beurteilt und bewertet.

▼M3

Artikel 5b

Übermittlung von Zertifikatswiderruflisten durch Drittländer

Drittländer, die COVID-19-Zertifikate ausstellen, für die die Kommission einen Durchführungsrechtsakt gemäß Artikel 3 Absatz 10 oder Artikel 8 Absatz 2 der Verordnung (EU) 2021/953 erlassen hat, können im Einklang mit den technischen Spezifikationen in Anhang I Listen widerrufener COVID-19-Zertifikate, die unter einen solchen Durchführungsrechtsakt fallen, zur Verarbeitung durch die Kommission im Auftrag der gemeinsam Verantwortlichen gemäß Artikel 5a über das Gateway übermitteln.

Artikel 5c

Verwaltung der Verarbeitung personenbezogener Daten im zentralen Gateway für das digitale COVID-Zertifikat der EU

(1) Der Entscheidungsprozess der gemeinsam Verantwortlichen wird von einer Arbeitsgruppe geregelt, die im Rahmen des in Artikel 14 der Verordnung (EU) 2021/953 genannten Ausschusses eingesetzt wird.

(2) Die benannten nationalen Behörden oder amtlichen Stellen der Mitgliedstaaten, die als gemeinsam Verantwortliche personenbezogene Daten im Gateway verarbeiten, entsenden Vertreter in diese Gruppe.

▼M1

Artikel 6

Dieser Beschluss tritt am Tag seiner Veröffentlichung im *Amtsblatt der Europäischen Union* in Kraft.

▼B

Dieser Beschluss tritt am Tag seiner Veröffentlichung im *Amtsblatt der Europäischen Union* in Kraft.

▼B

ANHANG I

FORMAT UND VERTRAUENSMANAGEMENT

Allgemeine Datenstruktur, Verschlüsselungsmechanismen und Mechanismus für die Transportverschlüsselung in maschinenlesbarer optischer Form (im Folgenden „QR“)

1. **Einleitung**

Die technischen Spezifikationen in diesem Anhang enthalten eine allgemeine Datenstruktur und Verschlüsselungsmechanismen für das digitale COVID-Zertifikat der EU (EU Digital COVID Certificate, DCC). Außerdem wird ein Transportverschlüsselungsmechanismus in einem maschinenlesbaren optischen Format (QR) festgelegt, das auf dem Bildschirm eines mobilen Geräts angezeigt oder ausgedruckt werden kann. Die in diesen Spezifikationen enthaltenen Containerformate für elektronische Gesundheitszertifikate sind generisch, werden aber in diesem Zusammenhang als Trägerformat für das DCC verwendet.

2. **Begriffe**

Für die Zwecke dieses Anhangs bezeichnet der Ausdruck „Aussteller“ Organisationen, die diese Spezifikationen für die Ausstellung von Gesundheitszertifikaten verwenden, und „Überprüfer“ Organisationen, die Gesundheitszertifikate als Nachweis des Gesundheitsstatus akzeptieren. Unter „Teilnehmer“ sind Aussteller und Überprüfer zu verstehen. Einige der in diesem Anhang behandelten Aspekte müssen zwischen den Teilnehmern koordiniert werden, etwa die Verwaltung eines Namensraums und die Verteilung kryptografischer Schlüssel. Es wird angenommen, dass eine Partei, im Folgenden als „Sekretariat“ bezeichnet, diese Aufgaben wahrnimmt.

3. **Containerformat für elektronische Gesundheitszertifikate**

Das Containerformat für elektronische Gesundheitszertifikate (Electronic Health Certificate Container Format, HCERT) soll ein einheitliches und standardisiertes Trägerformat für die Gesundheitszertifikate der verschiedenen Aussteller bieten. Die vorliegenden Spezifikationen dienen dazu, die Art und Weise, wie diese Gesundheitszertifikate dargestellt, verschlüsselt und signiert werden, im Interesse der Interoperabilität zu harmonisieren.

Damit das digitale COVID-Zertifikat der EU unabhängig vom Aussteller gelesen und verarbeitet werden kann, bedarf es einer gemeinsamen Datenstruktur und eines gemeinsamen Verständnisses über die Bedeutung der einzelnen Felder der Nutzdaten. Zur Erleichterung der Interoperabilität wird eine gemeinsame koordinierte Datenstruktur unter Verwendung eines JSON-Schemas festgelegt, das den Rahmen des DCC bildet.

3.1. *Struktur der Nutzdaten*

Die Nutzdaten werden als CBOR mit einer digitalen COSE-Signatur strukturiert und verschlüsselt. Dies wird gemeinhin als „CBOR Web Token“ (CWT) bezeichnet und ist in RFC 8392 ([1]) definiert. Die Nutzdaten werden gemäß den folgenden Abschnitten in einer hcert-Anforderung transportiert.

Die Integrität und die Authentizität der Herkunft der Nutzdaten müssen vom Überprüfer überprüft werden können. Zur Bereitstellung dieses Mechanismus muss der Aussteller den CWT mittels eines asymmetrischen elektronischen Signatursystems gemäß der COSE-Spezifikation (RFC 8152 ([2])) signieren.

3.2. *CWT-Anforderungen*

3.2.1. CWT-Struktur — Überblick

Geschützte Kopfzeile

([1]) rfc8392 (ietf.org)
([2]) rfc8152 (ietf.org)

▼B

— Signaturalgorithmus (alg, label 1)

— Schlüsselkennung (kid, label 4)

Nutzdaten

— Aussteller (iss, Anforderungsschlüssel 1, optional, ISO 3166-1 alpha-2 des Ausstellers)

— Ausgestellt am (iat, Anforderungsschlüssel 6)

— Verfallszeit (exp, Anforderungsschlüssel 4)

— Gesundheitszertifikat (hcert, Anforderungsschlüssel -260)

— Digitales COVID-Zertifikat der EU v1 (eu_DCC_v1, Anforderungsschlüssel 1)

Signatur

3.2.2. Signaturalgorithmus

Der Parameter Signaturalgorithmus (alg) gibt an, welcher Algorithmus für die Erstellung der Signatur verwendet wird. Er muss mindestens den geltenden SOG-IS-Leitlinien entsprechen, wie in den folgenden Absätzen zusammengefasst.

Es werden ein Primär- und ein Sekundäralgorithmus definiert. Der Sekundäralgorithmus sollte nur verwendet werden, wenn der Primäralgorithmus nach den dem Aussteller auferlegten Regeln und Vorschriften nicht akzeptabel ist.

Zur Gewährleistung der Systemsicherheit müssen alle Implementierungen den Sekundäralgorithmus enthalten. Aus diesem Grund muss sowohl der Primär- als auch der Sekundäralgorithmus implementiert werden.

Die für den Primär- und den Sekundäralgorithmus festgelegten SOG-IS-Werte sind:

— Primäralgorithmus: Der Primäralgorithmus ist ein auf elliptischen Kurven basierender Algorithmus für digitale Signaturen (Elliptic Curve Digital Signature Algorithm, ECDSA) gemäß ISO/IEC 14888-3:2006 Abschnitt 2.3, wobei die P–256-Parameter gemäß Anlage D (D.1.2.3) von (FIPS PUB 186–4) in Kombination mit dem Hash-Algorithmus SHA-256 gemäß (ISO/IEC 10118–3:2004) Funktion 4 verwendet werden.

Dies entspricht dem COSE-Algorithmus-Parameter ES256.

— Sekundäralgorithmus: Der Sekundäralgorithmus ist RSASSA-PSS gemäß Definition in (RFC 8230 ([1])) mit einem Modulus von 2048 Bit in Kombination mit dem Hash-Algorithmus SHA-256 gemäß (ISO/IEC 10118-3:2004) Funktion 4.

Dies entspricht dem COSE-Algorithmus-Parameter PS256.

3.2.3. Schlüsselkennung

Die Anforderung „Schlüsselkennung“ (kid) verweist auf das Dokumentensignierer-Zertifikat (DSC), das den öffentlichen Schlüssel enthält, der vom Überprüfer zur Überprüfung der digitalen Signatur zu verwenden ist. Die Verwaltung der Public-Key-Zertifikate, einschließlich der für DSC geltenden Anforderungen, ist in Anhang IV beschrieben.

([1]) rfc8230 (ietf.org)

▼B

Die Anforderung „Schlüsselkennung“ (kid) wird von den Überprüfern verwendet, um aus einer Liste von Schlüsseln, die dem in der Anforderung angegebenen Aussteller (iss) zugeordnet sind, den richtigen öffentlichen Schlüssel auszuwählen. Aus administrativen Gründen sowie bei der Durchführung von Schlüsselaktualisierungen (Rollover) können vom Aussteller mehrere Schlüssel parallel verwendet werden. Die Schlüsselkennung ist kein sicherheitskritisches Feld. Sie kann deshalb bei Bedarf auch in eine ungeschützte Kopfzeile gestellt werden. Die Überprüfer müssen beide Optionen akzeptieren. Bei Verwendung beider Optionen muss die Schlüsselkennung in der geschützten Kopfzeile verwendet werden.

Aufgrund der verkürzten Kennung (Begrenzung von Speicherplatz) ist es nicht ausgeschlossen, dass die von einem Überprüfer akzeptierte Gesamtliste der DSC Zertifikate mit doppelter kid enthält. Aus diesem Grund muss ein Überprüfer alle DSC mit der betreffenden kid überprüfen.

3.2.4. Aussteller

Die Anforderung „Aussteller“ (iss) ist ein Zeichenwert, der optional das ISO-3166-1-Alpha-2-Länderkürzel der Stelle enthalten kann, die das Gesundheitszertifikat ausstellt. Diese Anforderung kann von einem Überprüfer verwendet werden, um zu ermitteln, welcher DSC-Satz für die Überprüfung verwendet werden soll. Zur Identifizierung dieser Anforderung wird der Anforderungsschlüssel 1 verwendet.

3.2.5. Verfallszeit

Die Anforderung „Verfallszeit“ (exp) muss einen Zeitstempel im ganzzahligen NumericDate-Format (gemäß RFC 8392 ([1]), Abschnitt 2) tragen, der angibt, wie lange diese bestimmte Signatur für die Nutzdaten als gültig anzusehen ist und ab wann ein Überprüfer die Nutzdaten als verfallen abzulehnen hat. Der Verfallsparameter dient dazu, die Gültigkeit des Gesundheitszertifikats zeitlich zu begrenzen. Zur Identifizierung dieser Anforderung wird der Anforderungsschlüssel 4 verwendet.

Die Verfallszeit darf den Gültigkeitszeitraum des DSC nicht überschreiten.

3.2.6. Ausgestellt am

Die Anforderung „Ausgestellt am“ (iat) muss einen Zeitstempel im ganzzahligen NumericDate-Format (gemäß RFC 8392 ([2]), Abschnitt 2) tragen, der angibt, wann das Gesundheitszertifikat erstellt wurde.

Das Datum in „Ausgestellt am“ darf dem Gültigkeitszeitraum des DSC nicht vorausgehen.

Die Überprüfer können zusätzliche Maßnahmen anwenden, um die Gültigkeit von Gesundheitszertifikaten bezogen auf den Ausstellungszeitpunkt zu begrenzen. Zur Identifizierung dieser Anforderung wird der Anforderungsschlüssel 6 verwendet.

3.2.7. Gesundheitszertifikatsanforderung

Die Gesundheitszertifikatsanforderung (hcert) ist ein JSON-Objekt (RFC 7159 ([3])), das die Angaben zum Gesundheitsstatus enthält. Für dieselbe Anforderung kann es mehrere verschiedene Arten von Gesundheitszertifikaten geben, von denen das DCC eines ist.

Die JSON dient rein schematischen Zwecken. Das Darstellungsformat ist CBOR gemäß der Spezifikation in (RFC 7049 ([4])). In der Praxis ent- oder verschlüsseln Anwendungsentwickler möglicherweise nie aus dem bzw. in das JSON-Format, sondern verwenden lediglich die In-Memory-Struktur.

([1]) rfc8392 (ietf.org)
([2]) rfc8392 (ietf.org)
([3]) rfc7159 (ietf.org)
([4]) rfc7049 (ietf.org)

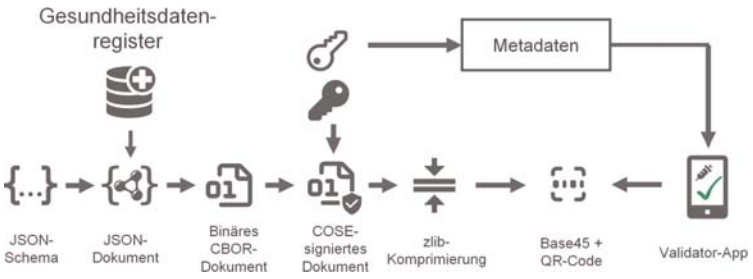
▼B

Zur Identifizierung dieser Anforderung wird der Anforderungsschlüssel -260 verwendet.

Die Zeichenfolgen im JSON-Objekt sollten der im Unicode-Standard definierten „Normalization Form Canonical Composition“ (NFC) entsprechen. Die Entschlüsselungsanwendungen sollten in diesen Aspekten jedoch durchlässig und robust sein, und es wird nachdrücklich empfohlen, alle geeigneten Typumwandlungen zu akzeptieren. Werden bei der Verschlüsselung oder in anschließenden Vergleichsfunktionen nicht normgerechte Daten identifiziert, so sollten die Implementierungen sich so verhalten, als würde die Eingabe dem NFC-Standard entsprechen.

4. **Serialisierung und Erstellung der DCC-Nutzdaten**

Als Serialisierungsmuster dient das folgende Schema:



Der Prozess beginnt mit der Extraktion von Daten, beispielsweise aus einem Gesundheitsdatenregister (oder einer externen Datenquelle), wobei die extrahierten Daten nach den festgelegten DCC-Schemata strukturiert werden. Bei diesem Vorgang können die Umwandlung in das festgelegte Datenformat und die Transformation in eine menschenlesbare Form stattfinden, bevor mit der Serialisierung nach CBOR begonnen wird. Vor der Serialisierung und nach der Deserialisierung müssen in jedem einzelnen Fall die Akronyme der Anforderungen den jeweiligen Anzeigenamen zugeordnet werden.

Optionale nationale Dateninhalte sind in Zertifikaten, die nach der Verordnung (EU) 2021/953 ([1]) ausgestellt werden, nicht zulässig. Der Dateninhalt beschränkt sich auf die definierten Datenelemente des Mindestdatensatzes, der im Anhang der Verordnung (EU) 2021/953 festgelegt ist.

5. **Transportverschlüsselungen**

5.1. *Roh*

Für arbiträre Datenschnittstellen gilt, dass der HCERT-Container und seine Nutzdaten unverändert, unter Verwendung einer beliebigen, 8-Bit-sicheren zuverlässigen Datenverbindung übertragen werden können. Bei diesen Schnittstellen kann es sich u. a. um Nahfeldkommunikation (NFC), Bluetooth oder die Übertragung über ein Anwendungsschichtprotokoll handeln, beispielsweise die Übertragung eines HCERT vom Aussteller auf das mobile Gerät des Inhabers.

Erfolgt die Übertragung des HCERT vom Aussteller zum Inhaber über eine Nur-Präsentation-Schnittstelle (z. B. SMS, E-Mail), so entfällt natürlich die Rohtransportverschlüsselung.

([1]) 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).

▼B

5.2. *Strichcode*

5.2.1. Komprimierung der Nutzdaten (CWT)

Um das HCERT zu verkleinern und den Lesevorgang schneller und zuverlässiger zu machen, ist der CWT unter Verwendung von ZLIB (RFC 1950 ([1])) und des Deflate-Kompressionsverfahrens in das in (RFC 1951 ([2])) festgelegte Format zu komprimieren.

5.2.2. 2D-QR-Strichcode

Zur besseren Einbeziehung auch älterer Geräte, die für die Verarbeitung von ASCII-Nutzdaten ausgelegt sind, wird der komprimierte CWT mittels Base45 als ASCII codiert, bevor er in einen 2D-Strichcode verschlüsselt wird.

Für die Generierung von 2D-Strichcodes ist das in ISO/IEC 18004:2015 definierte QR-Format zu verwenden. Empfohlen wird eine Fehlerberichtigungsquote von „Q“ (ca. 25 %). Wegen der Verwendung von Base45 ist für den QR-Code eine alphanumerische Verschlüsselung (Mode 2, angezeigt durch die Symbole 0010) zu verwenden.

Damit die Überprüfer die Art der verschlüsselten Daten erkennen und das richtige Entschlüsselungs- und Verarbeitungsschema auswählen können, müssen die Base45-codierten Daten (gemäß dieser Spezifikation) als Kontextkennung das Präfix „HC1:“ enthalten. In künftigen Versionen dieser Spezifikation, die sich auf die Rückwärtskompatibilität auswirken, ist eine neue Kontextkennung festzulegen, wobei das Zeichen nach „HC“ dem Zeichensatz [1-9 A-Z] entnommen werden muss. Die Schrittfolge muss diesem Muster folgen, d. h. erst [1-9] und anschließend [A-Z].

Der optische Code sollte auf dem Darstellungsmedium eine Diagonale zwischen 35 mm und 60 mm aufweisen, damit Lesegeräte mit fester Optik, bei denen das Medium auf die Oberfläche des Lesers gelegt werden muss, verwendet werden können.

Wird der optische Code mit niedrigauflösenden Druckern (< 300 dpi) auf Papier gedruckt, ist darauf zu achten, dass jedes Symbol (Rasterpunkt) des QR-Codes exakt quadratisch dargestellt wird. Bei einer nicht proportionalen Skalierung wären die Symbole in manchen Zeilen oder Spalten des QR-Codes nicht mehr quadratisch, was die Lesbarkeit häufig beeinträchtigt.

6. **Format der Vertrauenslisten (CSCA- und DSC-Liste)**

Jeder Mitgliedstaat ist verpflichtet, eine Liste mit einer oder mehreren Country Signing Certificate Authorities (CSCA) sowie eine Liste aller gültigen Dokumentensignierer-Zertifikate (DSC) bereitzustellen und diese Listen auf dem neuesten Stand zu halten.

6.1. *Vereinfachte CSCA/DSC*

Zum Zeitpunkt der vorliegenden Spezifikationsversion können die Mitgliedstaaten nicht davon ausgehen, dass Informationen aus Zertifikatsperrlisten (Certificate Revocation List, CRL) verwendet oder die Nutzungszeiträume privater Schlüssel von den Überprüfern überprüft werden.

Stattdessen besteht der Validierungsmechanismus primär darin zu überprüfen, ob das Zertifikat der aktuellen Version der betreffenden Zertifikatliste entspricht.

([1]) rfc1950 (ietf.org)
([2]) rfc1951 (ietf.org)

▼B

6.2. *ICAO-PKI für maschinenlesbare Reisedokumente (eMRTD) und Vertrauenszentren*

Die Mitgliedstaaten können eine gesonderte CSCA nutzen, aber auch ihre bestehenden CSCA-Zertifikate und/oder DSC für maschinenlesbare Reisedokumente bereitstellen; sie können sogar die Zertifikate bei (kommerziellen) Vertrauenszentren beschaffen und dann diese bereitstellen. In jedem Fall aber muss jedes DSC von der vom betreffenden Mitgliedstaat gemeldeten CSCA signiert werden.

7. **Sicherheitserwägungen**

Bei der Konzeption von Systemen, bei denen diese Spezifikation verwendet wird, müssen die Mitgliedstaaten bestimmte Sicherheitsaspekte ermitteln, analysieren und überwachen.

Dabei sind mindestens die folgenden Aspekte zu berücksichtigen:

7.1. *Gültigkeitsdauer der HCERT-Signatur*

Der Aussteller der HCERT muss die Gültigkeitsdauer der Signatur durch Angabe einer Verfallszeit begrenzen. Dadurch wird der Inhaber eines Gesundheitszertifikats verpflichtet, dieses in regelmäßigen Abständen zu erneuern.

Die zulässige Gültigkeitsdauer kann nach praktischen Erwägungen festgelegt werden. So kann es beispielsweise vorkommen, dass Personen während einer Auslandsreise das Gesundheitszertifikat nicht erneuern können. Es kann aber auch sein, dass ein Aussteller ein gewisses Sicherheitsrisiko vermutet und daraufhin ein DSC widerrufen muss (wodurch alle Gesundheitszertifikate, die unter Verwendung dieses nach wie vor gültigen Schlüssels ausgestellt wurden, ungültig werden). Die Auswirkungen solcher Ereignisse können durch regelmäßigen Wechsel der Aussteller-Schlüssel und die Anforderung, alle Gesundheitszertifikate in angemessenen Zeitabständen zu erneuern, beschränkt werden.

7.2. *Schlüsselmanagement*

Diese Spezifikation stützt sich in hohem Maße auf starke kryptografische Mechanismen zur Sicherung der Datenintegrität und Authentifizierung der Datenherkunft. Daher ist es notwendig, die Vertraulichkeit der privaten Schlüssel zu wahren.

Die Vertraulichkeit kryptografischer Schlüssel kann auf verschiedene Weise beeinträchtigt werden, z. B.:

— Der Vorgang der Schlüsselgenerierung kann fehlerhaft sein, was schwache Schlüssel zur Folge hat.

— Menschliches Versagen kann zu einer Offenlegung der Schlüssel führen.

— Die Schlüssel könnten intern oder extern durch Diebstahl entwendet werden.

— Die Schlüssel können durch Kryptoanalyse berechnet werden.

Zur Minderung der Risiken, dass der Signaturalgorithmus zu schwach ist und die privaten Schlüssel durch Kryptoanalyse somit beeinflusst werden können, wird in dieser Spezifikation allen Teilnehmern empfohlen, einen sekundären Rückfall-Signaturalgorithmus anzuwenden, der auf anderen Parametern oder einem anderen mathematischen Problem basiert als der Primäralgorithmus.

Hinsichtlich der genannten Risiken im Zusammenhang mit der Betriebsumgebung der Aussteller sind Minderungsmaßnahmen zur Gewährleistung einer wirksamen Kontrolle umzusetzen, z. B. die Generierung, Speicherung und Nutzung der privaten Schlüssel in Hardware-Sicherheitsmodulen (HSM). Die Verwendung von HSM für die Signatur von Gesundheitszertifikaten wird nachdrücklich empfohlen.

▼B

Unabhängig davon, ob ein Aussteller sich für die Verwendung von HSM entscheidet, sollte ein Zeitplan für den Schlüsselwechsel (Rollover) festgelegt werden, bei dem die Wechselhäufigkeit in angemessenem Verhältnis zur Exposition der Schlüssel gegenüber externen Netzen, anderen Systemen und Personal steht. Ein gut gewählter Rollover-Plan begrenzt auch die Risiken in Bezug auf irrtümlich ausgestellte Gesundheitszertifikate und ermöglicht es den Ausstellern, solche Zertifikate paketweise zu widerrufen, indem bei Bedarf ein Schlüssel für ungültig erklärt wird.

7.3. *Validierung der Eingabedaten*

Diese Spezifikationen können in einer Weise verwendet werden, die dazu führt, dass Daten aus nicht vertrauenswürdigen Quellen in betriebskritische Systeme Eingang finden. Um die mit diesem Angriffsvektor verbundenen Risiken möglichst gering zu halten, müssen alle Eingabefelder anhand der Datentypen, -längen und -inhalte ordnungsgemäß validiert werden. Auch die Signatur des Ausstellers muss überprüft werden, bevor der Inhalt des HCERT verarbeitet wird. Die Validierung der Signatur des Ausstellers setzt jedoch voraus, dass zuerst die geschützte Kopfzeile des Ausstellers abgefragt wird, die potenzielle Angreifer möglicherweise mit gezielten Informationen zu manipulieren versuchen, um die Sicherheit des Systems zu beeinträchtigen.

8. **Vertrauensmanagement**

Zur Überprüfung der Signatur des HCERT wird ein öffentlicher Schlüssel benötigt. Die Mitgliedstaaten müssen diese öffentlichen Schlüssel bereitstellen. Letztlich muss jeder Überprüfer (da der öffentliche Schlüssel nicht Teil des HCERT ist) über eine Liste aller öffentlichen Schlüssel verfügen, denen er vertrauen will.

Das System besteht aus (nur) zwei Schichten: für jeden Mitgliedstaat ein oder mehrere landesspezifische Zertifikate, mit denen jeweils ein oder mehrere, in der täglichen Praxis verwendete Dokumentensignierer-Zertifikate (DSC) signiert werden.

Die Zertifikate der Mitgliedstaaten werden als CSCA-Zertifikate (Country Signing Certificate Authority) bezeichnet und sind (in der Regel) selbstsignierte Zertifikate. Die Mitgliedstaaten können über mehr als eine CSCA verfügen, z. B. bei Dezentralisierung auf regionaler Ebene. Mit diesen CSCA-Zertifikaten werden die für die Signatur der HCERT verwendeten Dokumentensignierer-Zertifikate (DSC) regelmäßig signiert.

Das „Sekretariat“ ist eine funktionsbezogene Aufgabe. Es aggregiert und veröffentlicht regelmäßig die DSC der Mitgliedstaaten, nachdem sie anhand der Liste der (auf anderem Wege übermittelten und überprüften) CSCA-Zertifikate überprüft wurden.

Die daraus resultierende Liste der DSC enthält den aggregierten Satz der akzeptierten öffentlichen Schlüssel (und entsprechenden Schlüsselkennungen), die die Überprüfer verwenden können, um die Signaturen der HCERT zu validieren. Die Überprüfer müssen diese Liste regelmäßig beschaffen und aktualisieren.

Das Format dieser mitgliedstaatspezifischen Listen kann gemäß ihrer eigenen nationalen Festlegung angepasst werden. Das Dateiformat dieser Vertrauensliste kann somit variieren, sodass es sich beispielsweise um ein JWKS-signiertes (JWK-Set-Format gemäß RFC 7517 ([1]), Abschnitt 5) oder ein anderes Format handeln kann, das für die im betreffenden Mitgliedstaat verwendete Technologie spezifisch ist.

Zur Vereinfachung können die Mitgliedstaaten entweder ihre bestehenden CSCA-Zertifikate aus ihren ICAO/eMRTD-Systemen melden, oder aber — wie von der WHO empfohlen — ein gesondertes Zertifikat eigens für diesen Gesundheitsbereich erstellen.

([1]) rfc7517 (ietf.org)

▼B

8.1. *Schlüsselkennung (Key Identifier, kid)*

Die Schlüsselkennung (kid) wird bei der Erstellung der Liste der vertrauenswürdigen öffentlichen Schlüssel anhand der DSC berechnet und besteht aus einem (auf die ersten 8 Bytes) verkürzten, DER-codierten (roh) SHA-256-Fingerabdruck des DSC.

Die Überprüfer müssen die kid nicht anhand des DSC berechnen, sondern können die Schlüsselkennung eines vergebenen Gesundheitszertifikats unmittelbar mit der kid auf der Vertrauensliste abgleichen.

8.2. *Unterschiede zum PKI-Vertrauensmodell für maschinenlesbare Reisedokumente (eMRTD) der ICAO*

Als Orientierung dienten bewährte Praktiken im Rahmen des ICAO-PKI-Vertrauensmodells für maschinenlesbare Reisedokumente — für eine raschere Abwicklung sind allerdings eine Reihe von Vereinfachungen vorzunehmen:

— Ein Mitgliedstaat kann mehrere CSCA-Zertifikate bereitstellen.

— Die Gültigkeitsdauer des DSC (Schlüsselnutzung) kann beliebig festgelegt werden, solange sie die des CSCA-Zertifikats nicht überschreitet; auf eine Angabe kann auch ganz verzichtet werden.

— Das DSC kann für Gesundheitszertifikate spezifische Richtlinienkennungen (policy identifiers) enthalten (erweiterte Schlüsselverwendung).

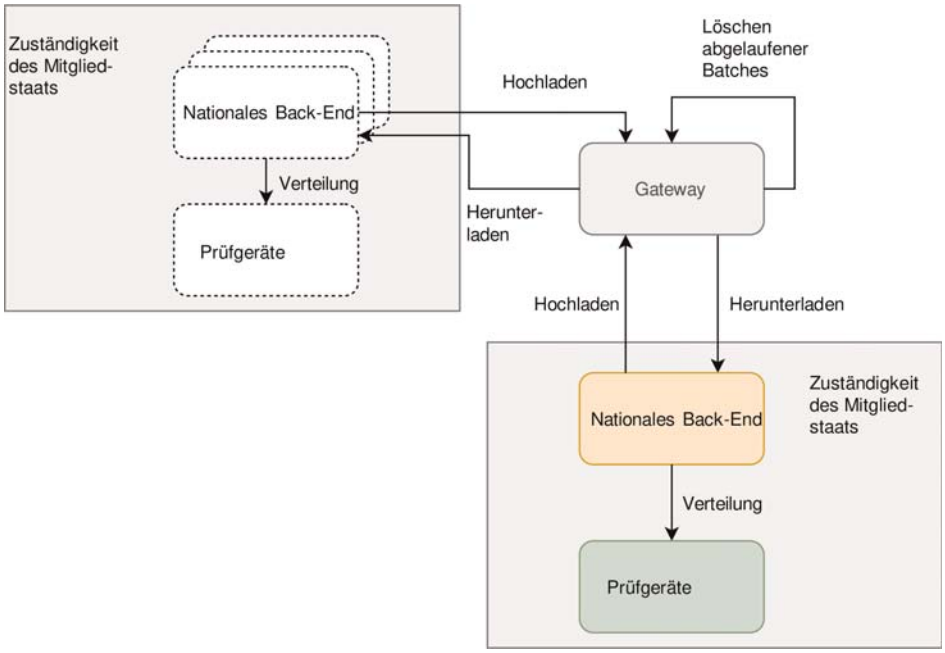
— Die Mitgliedstaaten können entscheiden, auf die Überprüfung veröffentlichter Widerrufe ganz zu verzichten und allein den DSC-Listen zu vertrauen, die sie täglich vom Sekretariat erhalten oder selbst erstellen.

▼M3

9. **Widerrufslösung**

9.1. *Bereitstellung der DCC-Widerrufsliste (DRL)*

Das Gateway stellt Endpunkte und Funktionen zur Speicherung und Verwaltung der Zertifikatswiderrufslisten bereit:



▼M3

9.2. *Vertrauensmodell*

Alle Verbindungen werden vom Standard-DCCG-Vertrauensmodell mithilfe von NB_{TLS}- und NB_{UP}-Zertifikaten hergestellt (siehe Verwaltung der Zertifikate). Alle Informationen werden in CMS-Nachrichten verpackt hochgeladen, um ihre Integrität zu gewährleisten.

9.3. *Erstellung der Batches*

9.3.1. Batch

Jede Widerrufsliste muss einen oder mehrere Einträge enthalten und wird in Batches verpackt, die eine Reihe von Hashwerten und ihre Metadaten enthalten. Ein Batch ist unveränderlich und definiert ein Ablaufdatum, an dem der Batch gelöscht werden kann. Das Ablaufdatum aller Elemente des Batches muss genau gleich sein, d. h., die Batches werden nach Ablaufdatum und dem Signatur-DSC gruppiert. Jeder Batch kann höchstens 1 000 Einträge enthalten. Umfasst die Widerrufsliste mehr als 1 000 Einträge, werden mehrere Batches erstellt. Jeder Eintrag kann in höchstens einem Batch erscheinen. Der Batch wird in einer CMS-Struktur verpackt und mit dem NB_{UP}-Zertifikat des hochladenden Landes signiert.

9.3.2. Batch-Index

Bei der Erstellung erhält der Batch vom Gateway eine eindeutige Kennung, die dem Index automatisch hinzugefügt wird. Der Batch-Index wird in aufsteigender chronologischer Reihenfolge des Änderungsdatums geordnet.

9.3.3. Gateway-Verhalten

Das Gateway verarbeitet Widerrufs-Batches ohne jegliche Änderung: Es kann Batches weder aktualisieren noch entfernen oder sie um weitere Informationen ergänzen. Die Batches werden an alle zugelassenen Länder weitergeleitet (siehe Kapitel 9.6).

Das Gateway beobachtet aktiv die Ablaufdaten der Batches und entfernt die abgelaufenen Batches. Wenn ein Batch gelöscht ist, gibt das Gateway für die gelöschte Batch-URL die Antwort „HTTP 410 Gone“ aus. Der Batch erscheint im Batch-Index daher als „gelöscht“.

9.4. *Hash-Typen*

Die Widerrufsliste enthält Hashwerte, die verschiedenen Arten/Attributen von Widerrufen entsprechen können. Diese Arten oder Attribute sind bei der Bereitstellung der Widerrufslisten anzugeben. Derzeit gibt es folgende Arten:

Art	Attribut	Hashwert-Berechnung
SIGNATURE	DCC Signature	SHA256 of DCC Signature
UCI	UCI (Unique Certificate Identifier)	SHA256 of UCI
COUNTRYCODEUCI	Issuing Country Code + UCI	SHA256 of Issuing Country-Code + UCI

Es werden nur die ersten 128 Bits der als Base64-Strings kodierten Hashwerte in die Batches aufgenommen und zur Identifizierung des widerrufenen DCC verwendet ([1]).

([1]) Für detaillierte API-Beschreibungen siehe auch Abschnitt 9.5.1.2.

▼M3

9.4.1. Hash-Typ: SHA256(DCC Signature)

In diesem Fall wird der Hashwert über die Bytes der COSE_SIGN1-Signatur des CWT berechnet. Bei RSA-Signaturen wird die gesamte Signatur verwendet. Die Formel für EC-DSA-signierte Zertifikate mit dem Wert r als Eingabe lautet:

SHA256(r)

[für alle neuen Umsetzungen vorgeschrieben]

9.4.2. Hash-Typ: SHA256(UCI)

In diesem Fall wird der Hashwert über den in UTF-8 kodierten UCI-String berechnet und in ein Byte-Array konvertiert.

[überholt ([1]), wird aber zur Gewährleistung der Rückwärtskompatibilität unterstützt]

9.4.3. Hash-Typ: SHA256(Issuing CountryCode+UCI)

In diesem Fall ist der als UTF-8-String kodierte Ländercode mit der als UTF-8-String kodierten UCI verkettet. Dies wird zu einem Byte-Array konvertiert und als Eingabe für die Hash-Funktion verwendet.

[überholt[2], wird aber zur Gewährleistung der Rückwärtskompatibilität unterstützt]

9.5. *API-Struktur*

9.5.1. API für die Bereitstellung von Widerrufseinträgen

9.5.1.1. Zweck

Die API stellt die Einträge der Widerrufslisten in Batches zusammen mit einem Batch-Index bereit.

9.5.1.2. Endpunkte

9.5.1.2.1. Endpunkt zum Download der Batch-Liste

Die Endpunkte sind einfach strukturiert und geben eine Liste von Batches zusammen mit einem kleinen Wrapper mit Metadaten aus. Die Batches werden nach *Datum* in *aufsteigender (chronologischer)* Reihenfolge geordnet:

/revocation-list

Verb: GET

Content-Type: application/json

Response: JSON Array

```
{
    ‘more‘:true|false,
    ‘batches‘:
            [{
                ‘batchId‘: ‘{uuid}‘,
                ‘country‘: ‘XY‘,
                ‘date‘: ‘2021-11-01T00:00:00Z‘
                ‘deleted‘: true | false
            }, ..
            ]
}
```

([1]) „Überholt“ bedeutet, dass diese Funktion bei neuen Umsetzungen nicht enthalten ist, aber für einen bestimmten Zeitraum für bestehende Umsetzungen unterstützt wird.

▼M3

Anmerkung: Das Ergebnis ist standardmäßig auf 1 000 begrenzt. Ist das Flag „more“ auf „true“ gesetzt, besteht die Antwort darin, dass weitere Batches heruntergeladen werden können. Um weitere Elemente herunterzuladen, muss der Client den Header If-Modified-Since auf ein Datum setzen, das nicht vor dem letzten abgerufenen Eintrag liegen kann.

Die Antwort enthält ein JSON-Array mit folgender Struktur:

Feld	Definition
more	Boolesches Flag, das angibt, dass es weitere Batches gibt
batches	Array der vorhandenen Batches
batchId	https://en.wikipedia.org/wiki/Universally_unique_identifier
country	Ländercode nach ISO 3166
date	Datum (UTC) nach ISO 8601. Datum, an dem der Batch hinzugefügt oder gelöscht wurde.
deleted	Boolesches Flag. Wahr, falls gelöscht. Wenn das Flag „deleted“ gesetzt wurde, kann der Eintrag nach 7 Tagen endgültig aus den Abfrageergebnissen entfernt werden.

9.5.1.2.1.1. Antwort*codes*

Code	Beschreibung
200	Alles ok
204	Kein Inhalt, wenn der Inhalt unter dem Header „If-Modified-Since“ keine Übereinstimmung aufweist.

Anfrage-Header

Header	Pflichtfeld	Beschreibung
If-Modified-Since	Ja	Dieser Header enthält das letzte Download-Datum, damit nur die neuesten Ergebnisse angezeigt werden. Bei Erstaufruf sollte der Header auf „2021-06-01T00:00:00Z“ gesetzt werden.

9.5.1.2.2. Endpunkt für den Batch-Download

Die Batches enthalten eine Liste von Zertifikatskennungen:

/revocation-list/{batchId}

Verb: GET

Accepts: application/cms

Response:CMS with Content

{

‘country‘: ‘XY‘,

‘expires‘: ‘2022-11-01T00:00:00Z‘,

▼M3

‘kid‘:‘23S+33f=‘,

‘hashType’:’SIGNATURE’,

‘entries‘:[{

‘hash‘:‘e2e2e2e2e2e2e2e2‘

}, ..]

}

Die Antwort enthält eine CMS mit einer Signatur, die mit dem NB_{UP}-Zertifikat des Landes übereinstimmen muss. Alle Elemente des JSON-Array umfassen folgende Struktur:

Feld	Pflichtfeld	Art	Definition
expires	Ja	String	Datum, an dem das Element entfernt werden kann. Datum/Uhrzeit (UTC) nach ISO 8601
country	Ja	String	Ländercode nach ISO 3166
hashType	Ja	String	Hash-Typ der bereitgestellten Einträge (siehe Hash-Typen)
entries	Ja	JSON Object Array	Siehe die Tabelle Einträge
kid	Ja	String	Base64-kodierte Schlüsselkennung (KID) des für die Signatur des DCC verwendeten DSC. Ist die KID nicht bekannt, kann der String 'UNKNOWN_KID' (ohne das Zeichen ') verwendet werden.

Anmerkungen:

— Die Batches werden nach Ablaufdatum und DSC gruppiert — alle Elemente laufen zum gleichen Zeitpunkt ab und wurden mit demselben Schlüssel signiert.

— Der Ablaufzeitpunkt wird als Datum/Uhrzeit in UTC angegeben, da das EUDCC ein weltweites System ist und der Zeitpunkt eindeutig sein muss.

— Das Ablaufdatum eines endgültig widerrufen DCC wird auf das Ablaufdatum des entsprechenden DSC, mit dem das DCC signiert wurde, oder auf das Ablaufdatum des widerrufenen DCC gesetzt (in letzterem Fall werden die numerischen Datums-/Epoch-Zeit-Angaben wie UTC-Zeitangaben behandelt).

— Das nationale Back-End (NB) entfernt Elemente aus der Widerrufsliste, wenn das **Ablauf**datum erreicht ist.

— Das NB kann Elemente aus seiner Widerrufsliste entfernen, wenn die für die Signatur des DCC verwendete **kid** widerrufen wird.

▼M3

9.5.1.2.2.1. Einträge

Feld	Pflicht-feld	Art	Definition
hash	Ja	String	Die ersten 128 Bits des als base64-String kodierten SHA256-Hashwerts

Anmerkung: Das Objekt Einträge enthält derzeit nur einen Hash, aber zur Gewährleistung der Kompatibilität mit künftigen Änderungen wurde anstelle eines JSON-Arrays ein Objekt gewählt.

9.5.1.2.2.2. Antwort-Codes

Code	Beschreibung
200	Alles ok
410	Batch entfernt. Batch kann im nationalen Back-End gelöscht werden.

9.5.1.2.2.3. Antwort-Header

Header	Beschreibung
ETag	Batch-Kennung

9.5.1.2.3. Endpunkt zum Hochladen von Batches

Das Hochladen erfolgt mit demselben Endpunkt über das Verb POST:

/revocation-list

Verb: POST

Accepts: application/cms

Request: CMS with Content

ContentType: application/cms

Content:

```
{
    ‘country‘: ‘XY‘,
    ‘expires‘: ‘2022-11-01T00:00:00Z‘,
    ‘kid‘:‘23S+33f=‘,
    ‘hashType‘:‘SIGNATURE‘,
    ‘entries‘:[{
        ‘hash‘:‘e2e2e2e2e2e2e2e2‘
        }, ..]
}
```

Der Batch wird mit dem NB_{UP}-Zertifikat signiert. Das Gateway überprüft, ob die Signatur vom NB_{UP} des jeweiligen *Landes* gesetzt wurde. Wird dies bei der Überprüfung der Signatur nicht festgestellt, ist das Hochladen nicht möglich.

ANMERKUNG: Jeder Batch ist unveränderlich und kann nach dem Hochladen nicht mehr geändert werden. Er kann jedoch gelöscht werden. Die Kennung jedes gelöschten Batches wird gespeichert, und es kann kein neuer Batch mit derselben Kennung hochgeladen werden.

▼**M3**

9.5.1.2.4. Endpunkt zum Löschen von Batches

Ein Batch kann mit demselben Endpunkt über das Verb DELETE gelöscht werden:

/revocation-list

Verb: DELETE

Accepts: application/cms

ContentType: application/cms

Request: CMS with Content

Content:

{

‘batchId‘: ‘...‘

}

Im Interesse der Kompatibilität kann der Batch auch mit dem folgenden Endpunkt über das Verb POST gelöscht werden:

/revocation-list/delete

Verb: POST

Accepts: application/cms

ContentType: application/cms

Request: CMS with Content

Content:

{

‘batchId‘: ‘...‘

}

9.6. *API-Schutz/DSGVO*

In diesem Abschnitt sind für die Umsetzung Maßnahmen zur Einhaltung der Bestimmungen der Verordnung (EU) 2021/953 hinsichtlich der Verarbeitung personenbezogener Daten festgelegt.

9.6.1. Vorhandene Authentifizierung

Das Gateway nutzt derzeit das NB_{TLS}-Zertifikat für die Authentifizierung von Ländern bei der Verbindung mit dem Gateway. Diese Authentifizierung kann verwendet werden, um die Identität des mit dem Gateway verbundenen Landes zu bestimmen. Diese Identität kann dann für die Zugangskontrolle genutzt werden.

9.6.2. Zugangskontrolle

Um personenbezogene Daten rechtmäßig verarbeiten zu können, wendet das Gateway einen Zugangskontrollmechanismus an.

Das Gateway nutzt eine Zugriffskontrollliste in Kombination mit einem rollenbasierten Sicherheitssystem (Role Based Security). Dabei werden zwei Tabellen geführt — eine Tabelle, die beschreibt, welche Rollen welche Vorgänge an welchen Ressourcen durchführen können, die andere beschreibt, welche Rollen welchen Nutzern zugewiesen sind.

Für die nach diesem Dokument vorgeschriebenen Kontrollen sind die folgenden drei Rollen erforderlich:

RevocationListReader

RevocationUploader

RevocationDeleter

▼**M3**

Die folgenden Endpunkte prüfen, ob der Nutzer die Rolle RevocationListReader hat; ist dies der Fall, wird der Zugang gewährt; falls nicht, erscheint HTTP 403 Forbidden:

GET/revocation-list/

GET/revocation-list/{batchId}

Die folgenden Endpunkte prüfen, ob der Nutzer die Rolle RevocationUploader hat; ist dies der Fall, wird der Zugang gewährt; ist dies nicht der Fall, erscheint HTTP 403 Forbidden:

POST/revocation-list

Die folgenden Endpunkte prüfen, ob der Nutzer die Rolle RevocationDeleter hat; ist dies der Fall, wird der Zugang gewährt; ist dies nicht der Fall, erscheint HTTP 403 Forbidden:

DELETE/revocation-list

POST/revocation-list/delete

Zudem bietet das Gateway eine zuverlässige Methode, mit der die Administratoren die mit den Nutzern verknüpften Rolle so verwalten können, dass die Wahrscheinlichkeit menschlicher Fehler verringert wird und die funktionalen Administratoren gleichzeitig nicht belastet werden.

▼M1

ANHANG II

VORSCHRIFTEN FÜR DAS FÜLLEN DES DIGITALEN COVID-ZERTIFIKATS DER EU

Die in diesem Anhang festgelegten allgemeinen Vorschriften bezüglich der Wertesätze sollen die Interoperabilität auf semantischer Ebene gewährleisten und ermöglichen eine einheitliche technische Umsetzung des digitalen COVID-Zertifikats der EU. Die Elemente in diesem Anhang können für die drei Anwendungsfälle (Impfung/Tests/Genesung) gemäß der Verordnung (EU) 2021/953 verwendet werden. In diesem Anhang sind nur die Elemente aufgeführt, die mittels codierter Wertesätze semantisch standardisiert werden müssen.

Die Übersetzung der codierten Elemente in die Landessprache fällt in die Zuständigkeit der Mitgliedstaaten.

Für alle Datenfelder, die nicht in den folgenden Beschreibungen der Wertesätze aufgeführt sind, wird die Codierung in Anhang V erläutert.

Sind aus irgendeinem Grund die nachstehenden bevorzugten Codesysteme nicht anwendbar, so können andere internationale Codesysteme verwendet werden, wobei Hinweise zur Umwandlung der Codes des anderen Systems in das bevorzugte Codesystem zu geben sind. Ist in den festgelegten Wertesätzen kein geeigneter Code enthalten, so kann in Ausnahmefällen auch Text (Anzeigenamen) als Sicherungsmechanismus verwendet werden.

Mitgliedstaaten, die in ihren Systemen eine andere Codierung verwenden, müssen die entsprechenden Codes den beschriebenen Wertesätzen zuordnen. Für diese Zuordnungen sind die Mitgliedstaaten zuständig.

►M4 Da sich einige auf den in diesem Anhang vorgesehenen Codesystemen basierende Wertesätze, z. B. für die Codierung von Impfstoffen und Antigentests, häufig ändern, werden sie von der Kommission mit Unterstützung des Netzwerks für elektronische Gesundheitsdienste und des Gesundheitssicherheitsausschusses veröffentlicht und regelmäßig aktualisiert. ◄ Die aktualisierten Wertesätze werden auf der einschlägigen Website der Kommission sowie auf der Website des Netzwerks für elektronische Gesundheitsdienste veröffentlicht. Alle Änderungen sind zu dokumentieren.

1. **Zielkrankheit oder -erreger/Krankheit oder Erreger, von der bzw. dem der Inhaber genesen ist: COVID-19 (SARS-CoV-2 oder eine seiner Varianten)**

   Zu verwenden in Zertifikat 1, 2 und 3.

   Folgender Code ist zu verwenden:

Code	Anzeige	Name des Codesystems	URL des Codesystems	OID des Codesystems	Version des Codesystems
840539006	COVID-19	SNOMED CT	http://snomed.info/sct	2.16.840.1.113883.6.96	2021-01-31

2. **COVID-19-Impfstoff oder -Prophylaxe**

   Bevorzugtes Codesystem: SNOMED CT oder ATC-Klassifikation.

   Zu verwenden in Zertifikat 1.

   Beispiele für Codes der bevorzugten Codesysteme: SNOMED-CT-Code 1119305005 (SARS-CoV-2-Antigen-Impfstoff), 1119349007 (SARS-CoV-2-mRNA-Impfstoff) oder J07BX03 (COVID-19-Impfstoffe).

   Ein Wertesatz mit den Codes, die gemäß den in diesem Abschnitt festgelegten Codesystemen zu verwenden sind, wird von der Kommission mit Unterstützung des Netzwerks für elektronische Gesundheitsdienste veröffentlicht und regelmäßig aktualisiert. Sobald neue Arten von Impfstoffen entwickelt und verwendet werden, ist der Wertesatz zu erweitern.

▼M1

3. **COVID-19-Impfstoff**

Bevorzugte Codesysteme (in der Reihenfolge ihrer Präferenz):

— Arzneimittelregister der Union für Impfstoffe mit EU-weiter Zulassung (Zulassungsnummern);

— ein globales Impfstoffregister, wie es die Weltgesundheitsorganisation einrichten könnte;

— Bezeichnung des Impfstoffes in anderen Fällen. Enthält die Bezeichnung Leerstellen, so sind diese durch einen Bindestrich (-) zu ersetzen.

Name des Wertesatzes: Impfstoff.

Zu verwenden in Zertifikat 1.

Beispiel für einen Code der bevorzugten Codesysteme: EU/1/20/1528 (Comirnaty). Beispiel für die Code-Bezeichnung eines Impfstoffes: Sputnik-V (für Sputnik V).

Ein Wertesatz mit den Codes, die gemäß den in diesem Abschnitt festgelegten Codesystemen zu verwenden sind, wird von der Kommission mit Unterstützung des Netzwerks für elektronische Gesundheitsdienste veröffentlicht und regelmäßig aktualisiert.

Impfstoffe werden mittels eines im veröffentlichten Wertesatz vorhandenen Codes codiert, und zwar auch dann, wenn sie in verschiedenen Ländern unterschiedliche Bezeichnungen haben. Der Grund dafür ist, dass es noch kein globales Impfstoffregister gibt, in dem alle derzeit verwendeten Impfstoffe erfasst sind. Beispiel:

— Für den Impfstoff „COVID-19 Vaccine Moderna Intramuscular Injection“ – so lautet die Bezeichnung des Impfstoffs Spikevax in Japan – ist der Code EU/1/20/1507 zu verwenden, da dieser der Bezeichnung dieses Impfstoffs in der EU entspricht.

Ist dies in einem speziellen Fall nicht möglich oder ratsam, wird in dem veröffentlichten Wertesatz ein separater Code vorgesehen.

▼M4

Beschließt ein Land, das das digitale COVID-Zertifikat der EU verwendet, während laufender klinischer Prüfungen Impfzertifikate für Probanden klinischer Prüfungen auszustellen, wird der Impfstoff nach folgendem Muster codiert:

CT*_clinical-trial-identifier*

Wurde die klinische Prüfung im EU-Register für klinische Prüfungen (EU-CTR) registriert, ist die Kennung der klinischen Prüfung aus diesem Register zu verwenden. In anderen Fällen können Kennungen aus anderen Registern (z. B. clinicaltrials.gov oder Australian New Zealand Clinical Trials Registry) verwendet werden.

Die Kennung der klinischen Prüfung enthält ein Präfix, das die Identifizierung des Registers für klinische Prüfungen ermöglicht (z. B. EUCTR für das EU-Register für klinische Prüfungen, NCT für clinicaltrials.gov, ACTRN für das australisch-neuseeländische Register für klinische Prüfungen).

Hat die Kommission vom Gesundheitssicherheitsausschuss, dem Europäischen Zentrum für die Prävention und die Kontrolle von Krankheiten (ECDC) oder der Europäischen Arzneimittel-Agentur (EMA) Leitlinien zur Anerkennung von Zertifikaten erhalten, die für einen in klinischer Prüfung befindlichen COVID-19-Impfstoff erlassen wurden, so werden die Leitlinien entweder als Teil des Wertesätze-Dokuments oder gesondert veröffentlicht;

▼M1

4. **Zulassungsinhaber oder Hersteller des COVID-19-Impfstoffs**

Bevorzugtes Codesystem:

— von der EMA verwendeter Code der Organisation (SPOR-System für ISO IDMP);

— ein globales Register der Zulassungsinhaber oder Hersteller, wie es die Weltgesundheitsorganisation einrichten könnte;

— Bezeichnung der Organisation in anderen Fällen. Enthält die Bezeichnung Leerstellen, so sind diese durch einen Bindestrich (-) zu ersetzen.

Zu verwenden in Zertifikat 1.

Beispiel für einen Code des bevorzugten Codesystems: ORG-100001699 (AstraZeneca AB). Beispiel für die Code-Bezeichnung einer Organisation: Sinovac-Biotech (für Sinovac Biotech).

Ein Wertesatz mit den Codes, die gemäß den in diesem Abschnitt festgelegten Codesystemen zu verwenden sind, wird von der Kommission mit Unterstützung des Netzwerks für elektronische Gesundheitsdienste veröffentlicht und regelmäßig aktualisiert.

Unterschiedliche Zweigniederlassungen desselben Zulassungsinhabers oder Herstellers müssen einen im veröffentlichten Wertesatz vorhandenen Code verwenden.

Generell gilt: Für ein und denselben Impfstoff ist der Code für dessen Zulassungsinhaber in der EU zu verwenden, da bislang noch kein international anerkanntes Register der Hersteller oder Zulassungsinhaber von Impfstoffen existiert. Beispiele:

— Für die Organisation „Pfizer AG“, die Zulassungsinhaber des Impfstoffs „Comirnaty“ in der Schweiz ist, muss der Code ORG-100030215 für die BioNTech Manufacturing GmbH verwendet werden, da Letztere Zulassungsinhaber von „Comirnaty“ in der EU ist.

— Für die Organisation „Zuellig Pharma“, die Zulassungsinhaber des Impfstoffs Covid-19 Vaccine Moderna (Spikevax) auf den Philippinen ist, muss der Code ORG-100031184 für Moderna Biotech Spain S.L. verwendet werden, da Letztere Zulassungsinhaber von Spikevax in der EU ist.

Ist dies in einem speziellen Fall nicht möglich oder ratsam, wird in dem veröffentlichten Wertesatz ein separater Code vorgesehen.

▼M4

Beschließt ein Land, das das digitale COVID-Zertifikat der EU verwendet, während laufender klinischer Prüfungen Impfzertifikate für Probanden klinischer Prüfungen auszustellen, so wird der Inhaber der Genehmigung für das Inverkehrbringen des Impfstoffs oder der Hersteller unter Verwendung des ihm zugewiesenen Wertesatzes, sofern verfügbar, codiert. In anderen Fällen wird der Inhaber der Genehmigung für das Inverkehrbringen des Impfstoffs oder der Hersteller unter Verwendung der in Abschnitt 3 (COVID-19-Impfstoff) beschriebenen Regel (*CT_clinical-trial-identifier*) codiert;

▼M1

5. **Nummer der Dosis in einer Impfserie und Gesamtzahl der Dosen der Impfserie**

Zu verwenden in Zertifikat 1.

Zwei Felder:

(1) Nummer der Dosis in einer Impfserie mit einem COVID-19-Impfstoff (N);

(2) Gesamtzahl der Dosen der Impfserie (C).

5.1. *Erste Impfserie*

Erhält die Person Dosen der ersten Impfserie, also der Impfserie, die anfangs einen ausreichenden Schutz bieten soll, so enthält das Feld (C) die Gesamtzahl der Dosen der standardmäßigen ersten Impfserie (d. h. 1 oder 2, je nach Art des verabreichten Impfstoffs). Dies schließt die Option einer kürzeren Serie (C = 1) ein, wenn das Impfprotokoll eines Mitgliedstaats die Verabreichung nur einer Dosis eines normalerweise in zwei Dosen zu verabreichenden Impfstoffs an Personen vorsieht, bei denen vor der Impfung eine Infektion mit SARS-CoV-2 festgestellt wurde. Eine abgeschlossene erste Impfserie ist daher mit N/C = 1 anzugeben. Zum Beispiel:

— 1/1 stünde für den Abschluss einer ersten Impfserie mit einem nur in einer Dosis zu verabreichenden Impfstoff oder für den Abschluss einer ersten Impfserie, bei der gemäß dem Impfprotokoll eines Mitgliedstaats eine Dosis eines normalerweise in zwei Dosen zu verabreichenden Impfstoffs an eine genesene Person verabreicht wurde.

— 2/2 stünde für den Abschluss einer ersten Impfserie mit einem in zwei Dosen zu verabreichenden Impfstoff.

Wird die erste Impfserie erweitert, etwa für Personen mit stark geschwächtem Immunsystem oder wenn der empfohlene Abstand zwischen den Primärdosen nicht eingehalten wurde, so sind solche Dosen als zusätzliche Dosen gemäß Abschnitt 5.2 anzugeben.

▼M2

5.2. *Auffrischungsdosen*

Erhält die Person Dosen nach der ersten Impfserie, so werden diese Auffrischungsdosen in den entsprechenden Zertifikaten wie folgt ausgewiesen:

— 2/1 steht für die Verabreichung einer Auffrischungsdosis nach einer ersten Impfserie mit einem nur in einer Dosis zu verabreichenden Impfstoff oder für die Verabreichung einer Auffrischungsdosis nach Abschluss einer ersten Impfserie, bei der gemäß dem Impfprotokoll eines Mitgliedstaats eine Einzeldosis eines auf zwei Dosen ausgelegten Impfstoffs an eine genesene Person verabreicht wurde. In der Folge sind Dosen (X), die nach der ersten Auffrischungsdosis verabreicht werden, mit (2+X)/(1) > 1 (z. B. 3/1) anzugeben;

— 3/3 steht für die Verabreichung einer Auffrischungsdosis nach einer ersten Impfserie mit einem in zwei Dosen zu verabreichenden Impfstoff. In der Folge sind Dosen (X), die nach der ersten Auffrischungsdosis verabreicht werden, mit (3+X)/(3+X) = 1 (z. B. 4/4) anzugeben.

Die Mitgliedstaaten setzen die in diesem Abschnitt festgelegten Kodierungsvorschriften bis zum 1. Februar 2022 um.

Die Mitgliedstaaten stellen automatisch oder auf Antrag der betroffenen Personen Zertifikate, in denen die Verabreichung einer Auffrischungsdosis im Anschluss an einen nur in einer Dosis zu verabreichenden Impfstoff so kodiert ist, dass sie nicht vom Abschluss der ersten Impfserie unterschieden werden kann, neu aus.

▼M2

Für die Zwecke dieses Anhangs sind Bezugnahmen auf „Auffrischungsdosen“ so zu verstehen, dass sie auch zusätzliche Dosen umfassen, die zum besseren Schutz von Personen verabreicht werden, die nach Abschluss der standardmäßigen ersten Impfserie unzureichende Immunreaktionen zeigen. Innerhalb des mit der Verordnung (EU) 2021/953 geschaffenen Rechtsrahmens können die Mitgliedstaaten Maßnahmen ergreifen, um der Situation vulnerabler Gruppen Rechnung zu tragen, denen vorrangig zusätzliche Dosen verabreicht werden können. Beschließt beispielsweise ein Mitgliedstaat, zusätzliche Dosen nur an bestimmte Untergruppen der Bevölkerung zu verabreichen, so kann er gemäß Artikel 5 Absatz 1 der Verordnung (EU) 2021/953 entscheiden, Impfzertifikate mit Angaben über die Verabreichung solcher zusätzlicher Dosen nur auf Anfrage und nicht automatisch auszustellen. Wenn solche Maßnahmen ergriffen werden, informieren die Mitgliedstaaten die betroffenen Personen entsprechend, auch darüber, dass sie die nach Abschluss der standardmäßigen ersten Impfserie erhaltenen Impfzertifikate weiter verwenden können.

▼M1

6. **Mitgliedstaat oder Drittland, in dem der Impfstoff verabreicht bzw. der Test durchgeführt wurde**

Bevorzugtes Codesystem: Länderkürzel nach ISO 3166.

Zu verwenden in Zertifikat 1, 2 und 3.

Inhalt der Wertesätze: vollständige Liste der 2-Buchstaben-Codes, verfügbar als Wertesatz gemäß FHIR (http://hl7.org/fhir/ValueSet/iso3166-1-2). Wenn die Impfung oder der Test von einer internationalen Organisation (wie UNHCR oder WHO) durchgeführt wurde und keine Informationen über das Land vorliegen, ist ein Code für die Organisation zu verwenden. Solche zusätzlichen Codes werden von der Kommission mit Unterstützung des Netzwerks für elektronische Gesundheitsdienste veröffentlicht und regelmäßig aktualisiert.

7. **Art des Tests**

Zu verwenden in Zertifikat 2 und immer dann in Zertifikat 3, wenn ein delegierter Rechtsakt die Unterstützung der Ausstellung von Genesungszertifikaten auf der Grundlage anderer Arten von Tests als NAAT vorsieht.

Folgende Codes sind zu verwenden:

Code	Anzeige	Name des Codesystems	URL des Codesystems	OID des Codesystems	Version des Codesystems
LP6464-4	Nukleinsäure-Amplifikation mit Sondennachweis	LOINC	http://loinc.org	2.16.840.1.113883.6.1	2.69
LP217198-3	Schnell-Immunoassay	LOINC	http://loinc.org	2.16.840.1.113883.6.1	2.69

▼M4

Der Code LP217198-3 (Schnell-Immunoassay) ist sowohl für Antigen-Schnelltests als auch für Antigentests auf Laborbasis zu verwenden;

▼M1

8. **Hersteller und Handelsname des durchgeführten Tests (beim NAAT-Test fakultativ)**

Zu verwenden in Zertifikat 2.

▼M4

Der Wertesatz muss alle Antigentests enthalten, die in der aktuellen gemeinsamen Liste der COVID-19-Antigentests aufgeführt sind, welche gemäß der Empfehlung 2021/C 24/01 des Rates erstellt und vom Gesundheitssicherheitsausschuss gebilligt wurde. Die Liste wird von der JRC in der Datenbank für In-vitro-Diagnostika und Testmethoden für COVID-19 geführt und ist unter folgender Adresse abrufbar: https://covid-19-diagnostics.jrc.ec.europa.eu/devices/hsc-common-recognition-rat.

▼M1

Für dieses Codesystem sind relevante Felder wie Kennung des Testgeräts, Bezeichnung des Tests und Name des Herstellers gemäß dem strukturierten Format der JRC zu verwenden, abrufbar unter https://covid-19-diagnostics.jrc.ec.europa.eu/devices

9. **Testergebnis**

Zu verwenden in Zertifikat 2.

Folgende Codes sind zu verwenden:

Code	Anzeige	Name des Codesystems	URL des Codesystems	OID des Codesystems	Version des Codesystems
260415000	Nicht nachgewiesen	SNOMED CT	http://snomed.info/sct	2.16.840.1.113883.6.96	2021-01-31
260373001	Nachgewiesen	SNOMED CT	http://snomed.info/sct	2.16.840.1.113883.6.96	2021-01-31

▼B

ANHANG III

GEMEINSAME STRUKTUR DER EINDEUTIGEN ZERTIFIKATKENNUNG

1. **Einleitung**

Jedes digitale COVID-Zertifikat der EU (DCC) muss eine eindeutige Zertifikatkennung (Unique Certificate Identifier, UCI) enthalten, die die Interoperabilität der Zertifikate unterstützt. Die UCI kann zur Überprüfung des Zertifikats verwendet werden. Die Mitgliedstaaten sind für die Umsetzung der UCI zuständig. Die UCI dient der Überprüfung der Unverfälschtheit des Zertifikats und gegebenenfalls der Verknüpfung mit einem Registrierungssystem (z. B. einem Immunisierungsinformationssystem). Diese Kennungen müssen es den Mitgliedstaaten auch ermöglichen zu bescheinigen (auf Papier und digital), dass eine Person geimpft oder getestet wurde.

2. **Zusammensetzung der eindeutigen Zertifikatkennung**

Die UCI besitzt eine gemeinsame Struktur und ein einheitliches Format, was die Menschen- und/oder Maschinenlesbarkeit erleichtert; sie kann Elemente wie den Mitgliedstaat der Impfung, den Impfstoff selbst und eine spezifische Kennung des Mitgliedstaats beinhalten. Die Mitgliedstaaten können die UCI flexibel und unter uneingeschränkter Einhaltung der Datenschutzvorschriften gestalten. Die Reihenfolge der einzelnen Elemente ist hierarchisch festgelegt, sodass künftige Änderungen der Blöcke unter Wahrung ihrer strukturellen Integrität möglich sind.

Die Lösungsmöglichkeiten für die Zusammensetzung der UCI bilden zusammen ein Spektrum, in dem Modularität und Menschenlesbarkeit die beiden wichtigsten Unterscheidungsparameter sind und das ein grundlegendes Merkmal hat:

— Modularität: der Grad, in dem der Code aus verschiedenen Bausteinen mit semantisch unterschiedlichen Informationen besteht;

— Menschenlesbarkeit: der Grad, in dem der Code aussagekräftig oder menschenlesbar ist;

— weltweit eindeutig: die Kennung des Landes oder der Behörde wird gut verwaltet, und es wird erwartet, dass jedes Land (jede Behörde) sein/ihr Segment des Namensraums gut verwaltet, indem Kennungen niemals wiederverwendet oder neu vergeben werden. All dies zusammen gewährleistet, dass jede Kennung weltweit eindeutig ist.

▼M1

3. **Allgemeine Anforderungen**

Die eindeutige Zertifikatkennung (Unique Certificate Identifier, UCI) muss folgenden übergeordneten Anforderungen entsprechen:

(1) Zeichensatz: Nur alphanumerische US-ASCII-Zeichen in Großschreibung („A“ bis „Z“, „0“ bis „9“) sind zulässig. Für die Trennung dürfen zusätzlich folgende Sonderzeichen gemäß RFC3986 ([1]) verwendet werden: {„/“, „#“, „:“}.

(2) Maximale Länge: Bei der Programmierung sollte eine Länge von 27-30 Zeichen nicht überschritten werden ([2]).

(3) Versionspräfix: Dieses bezieht sich auf die Version des UCI-Schemas. Das Versionspräfix besteht aus zwei Ziffern und lautet für das vorliegende Dokument „01“.

([1]) rfc3986 (ietf.org)

([2]) Für die Implementierung mit QR-Codes können die Mitgliedstaaten gegebenenfalls einen zusätzlichen Zeichensatz mit bis zu 72 Zeichen (inklusive der 27-30 Zeichen der eigentlichen Kennung) verwenden, um andere Informationen zu übermitteln. Für die Spezifizierung dieser Informationen sind die Mitgliedstaaten zuständig.

▼M1

(4) Länderpräfix: Der Ländercode ist in ISO 3166-1 festgelegt. Längere Codes (drei Zeichen und mehr (z. B. „UNHCR“) sind künftigen Verwendungen vorbehalten.

(5) Code-Suffix/Prüfsumme:

5.1 Die Mitgliedstaaten können eine Prüfsumme verwenden, wenn Übertragungen, Transkriptionen (durch den Menschen) oder andere Beeinflussungen auftreten könnten (d. h. bei Verwendung im Druckformat).

5.2 Die Prüfsumme darf nicht für die Validierung des Zertifikats verwendet werden und gehört technisch nicht zu der Kennung, sondern dient dazu, die Integrität des Codes zu überprüfen. Diese Prüfsumme muss die gesamte nach ISO-7812-1 (LUHN-10) ([1]) zusammengefasste UCI in digitalem Übertragungsformat sein. Die Prüfsumme wird durch das Zeichen „#“ von der übrigen UCI getrennt.

Die Rückwärtskompatibilität ist sicherzustellen: Mitgliedstaaten, die im Lauf der Zeit die Struktur ihrer Kennungen (basierend auf der aktuellen Hauptversion v1) ändern, müssen sicherstellen, dass zwei identische Kennungen auf dieselbe Impfbescheinigung bzw. dasselbe Zertifikat verweisen. Anders ausgedrückt bedeutet dies, dass die Mitgliedstaaten Kennungen nicht wiederverwenden dürfen.

▼B

4. **UCI-Optionen bei Impfzertifikaten**

Die EHN-Leitlinien zu überprüfbaren Impfzertifikaten und grundlegenden Elementen der Interoperabilität ([2]) sehen verschiedene Optionen vor, die den Mitgliedstaaten und anderen Beteiligten zur Verfügung stehen und in den einzelnen Mitgliedstaaten gleichzeitig bestehen können. Die Mitgliedstaaten können diese Optionen in unterschiedlichen Versionen des UCI-Schemas umsetzen.

([1]) Der Luhn-Mod-N-Algorithmus ist eine Erweiterung des Luhn-Algorithmus (auch als „Modulo-10-Algorithmus“ bezeichnet), der für numerische Codes funktioniert und beispielsweise zur Berechnung der Prüfziffer von Kreditkarten verwendet wird. Durch diese Erweiterung kann der Algorithmus für Wertereihen auf beliebiger Grundlage (in diesem Fall Buchstaben) verwendet werden.

([2]) https://ec.europa.eu/health/sites/default/files/ehealth/docs/vaccination-proof_interoperability-guidelines_en.pdf

▼B

ANHANG IV

VERWALTUNG DER PUBLIC-KEY-ZERTIFIKATE

1. **Einleitung**

Die Signaturschlüssel für die digitalen COVID-Zertifikate der EU (DCC) werden über das Gateway für das digitale COVID-Zertifikat der EU (DCCG), das als zentraler Speicher für die öffentlichen Schlüssel dient, auf sichere und vertrauenswürdige Weise zwischen den Mitgliedstaaten ausgetauscht. Über das DCCG können die Mitgliedstaaten die öffentlichen Schlüssel veröffentlichen, die den für die Signatur der digitalen COVID-Zertifikate verwendeten privaten Schlüsseln entsprechen. Die teilnehmenden Mitgliedstaaten können das DCCG nutzen, um rechtzeitig aktualisiertes öffentliches Schlüssel-Material zu erhalten. Das DCCG kann später erweitert werden, um zusätzliche vertrauenswürdige Informationen auszutauschen, die die Mitgliedstaaten bereitstellen, darunter Validierungsregeln für DCC. Das Vertrauensmodell des DCC-Rahmens ist eine Public-Key-Infrastruktur (PKI). Jeder Mitgliedstaat verfügt über eine oder mehrere Länder-Signatur-Zertifizierungsstellen (Country Signing Certificate Authority, CSCA), deren Zertifikate relativ langlebig sind. Bei der CSCA kann es sich nach Wahl der Mitgliedstaaten um die für maschinenlesebare Reisedokumente genutzte CSCA oder eine andere CSCA handeln. Die CSCA stellt Public-Key-Zertifikate für die kurzlebigen nationalen Dokumentensignierer (d. h. Signierer der DCC) aus, die als Dokumentensignierer-Zertifikate (DSC) bezeichnet werden. Die CSCA dient als Vertrauensanker, sodass die teilnehmenden Mitgliedstaaten das CSCA-Zertifikat verwenden können, um die Authentizität und Integrität der sich regelmäßig ändernden DSC zu validieren. Nach der Validierung können die Mitgliedstaaten diese Zertifikate (oder nur die darin enthaltenen öffentlichen Schlüssel) ihren DCC-Validierungsanwendungen bereitstellen. Außer für CSCA und DSC nutzt das DCCG die PKI auch, um Transaktionen zu authentifizieren und Daten zu signieren, sowie als Grundlage für die Authentifizierung und die Gewährleistung der Integrität der Kommunikationskanäle zwischen Mitgliedstaaten und dem DCCG.

Digitale Signaturen können genutzt werden, um die Integrität und Authentizität der Daten zu gewährleisten. Public-Key-Infrastrukturen stellen durch Zuordnung öffentlicher Schlüssel zu Teilnehmern mit überprüfter Identität (oder Ausstellern) Vertrauen her. Dies ist erforderlich, damit andere Teilnehmer die Herkunft der Daten und die Identität des Kommunikationspartners überprüfen und über die Vertrauenswürdigkeit entscheiden können. Im DCCG wird die Authentizität mithilfe mehrerer Public-Key-Zertifikate gewährleistet. In diesem Anhang ist festgelegt, welche Public-Key-Zertifikate verwendet werden und wie sie im Interesse einer umfassenden Interoperabilität zwischen den Mitgliedstaaten zu gestalten sind. Er enthält weitere Einzelheiten zu den erforderlichen Public-Key-Zertifikaten und Anleitungen für Mitgliedstaaten, die ihre eigene CSCA betreiben wollen, hinsichtlich der Vorlagen für Zertifikate und der Gültigkeitszeiträume. Da die DCC während eines definierten Zeitraums überprüfbar sein müssen (von der Ausstellung bis zum Verfall nach einer bestimmten Zeit), ist es erforderlich, ein Überprüfungsmodell für alle Signaturen festzulegen, das auf Public-Key-Zertifikate und die DCC angewandt wird.

2. **Begriffe**

Die folgende Tabelle enthält die in diesem Anhang verwendeten Abkürzungen und Begriffe.

Begriff	Begriffsbestimmung
Zertifikat	oder Public-Key-Zertifikat: ein X.509-v3-Zertifikat, das den öffentlichen Schlüssel einer Stelle enthält

▼B

Begriff	Begriffsbestimmung
CSCA	Country Signing Certificate Authority (Länder-Signatur-Zertifizierungsstelle)
DCC	Digitales COVID-Zertifikat der EU: ein signiertes digitales Dokument, das Informationen über Impfungen, Tests oder eine Genesung enthält
DCCG	Gateway für das digitale COVID-Zertifikat der EU: System für den Austausch von DSC zwischen den Mitgliedstaaten
$DCCG_{TA}$	Vertrauensanker-Zertifikat des DCCG. Der entsprechende private Schlüssel wird offline für die Signatur der Liste aller CSCA-Zertifikate verwendet.
$DCCG_{TLS}$	das TLS-Server-Zertifikat des DCCG
DSC	Document-Signer-Zertifikat (Dokumentensignierer-Zertifikat): das Public-Key-Zertifikat der nationalen Dokumentensignierungsstelle eines Mitgliedstaats (z. B. ein System, das DCC signieren darf). Dieses Zertifikat wird von der CSCA des Mitgliedstaats ausgestellt.
EC-DSA	Elliptic Curve Digital Signature Algorithm: auf elliptischen Kurven basierender Verschlüsselungsalgorithmus für digitale Signaturen
Mitgliedstaat	Mitgliedstaat der Europäischen Union
mTLS	Mutual TLS: Transport Layer Security Protocol (Transportschicht-Sicherheitsprotokoll) mit gegenseitiger Authentifizierung
NB	nationales Back-End eines Mitgliedstaats
NB_{CSCA}	CSCA-Zertifikat eines Mitgliedstaats (eines oder mehrere Zertifikate)
NB_{TLS}	das TLS-Client-Authentifizierungszertifikat eines nationalen Back-Ends
NB_{UP}	Zertifikat, das von einem nationalen Back-End für die Signatur von Datenpaketen genutzt wird, die zum DCCG hochgeladen werden
PKI	Public-Key-Infrastruktur: Vertrauensmodell auf der Grundlage von Public-Key-Zertifikaten und Zertifizierungsstellen
RSA	asymmetrischer Verschlüsselungsalgorithmus, der auf der Faktorisierung ganzer Zahlen beruht und für digitale Signaturen oder die asymmetrische Verschlüsselung genutzt wird

3. **DCCG-Kommunikationswege und -Sicherheitsdienste**

Dieser Abschnitt gibt einen Überblick über die Kommunikationswege und Sicherheitsdienste innerhalb des DCCG-Systems. Zudem ist festgelegt, welche Schlüssel und Zertifikate für den Schutz der Kommunikation, der hochgeladenen Informationen, der DCC und einer signierten Vertrauensliste, die alle aufgenommenen CSCA-Zertifikate enthält, verwendet werden. Das DCCG dient als Datenplattform für den Austausch signierter Datenpakete zwischen den Mitgliedstaaten.

▼B

Die hochgeladenen Datenpakete werden vom DCCG im „Ist-Zustand“ bereitgestellt, d. h. das DCCG ergänzt oder entfernt keine Daten aus den eingegangenen Paketen. Das nationale Back-End (NB) der Mitgliedstaaten muss in der Lage sein, die Integrität und Authentizität der hochgeladenen Daten für den gesamten Kommunikationsweg (von Ende zu Ende) zu überprüfen. Zudem nutzen die nationalen Back-Ends und das DCCG die gegenseitige TLS-Authentifizierung für die Herstellung einer sicheren Verbindung. Dies ergänzt die Signatur der ausgetauschten Daten.

3.1. *Authentifizierung und Herstellung der Verbindung*

Das DCCG nutzt Transportschichtsicherheit (Transport Layer Security, TLS) mit gegenseitiger Authentifizierung, um einen authentifizierten verschlüsselten Kanal zwischen dem nationalen Back-End (NB) des Mitgliedstaats und der Gateway-Umgebung herzustellen. Das DCCG verfügt daher über ein TLS-Serverzertifikat (Abkürzung $DCCG_{TLS}$) und die nationalen Back-Ends über ein TLS-Client-Zertifikat (Abkürzung NB_{TLS}). Vorlagen für die Zertifikate finden sich in *Abschnitt 5*. Jedes nationale Back-End kann sein eigenes TLS-Zertifikat bereitstellen. Dieses Zertifikat wird ausdrücklich in eine weiße Liste aufgenommen und kann daher von einer öffentlich als vertrauenswürdig anerkannten Zertifizierungsstelle (z. B. einer Zertifizierungsstelle, die die Mindestanforderungen (Baseline Requirements) des CA/Browser-Forums erfüllt) oder einer nationalen Zertifizierungsstelle ausgestellt oder selbstsigniert sein. Jeder Mitgliedstaat ist für seine nationalen Daten verantwortlich und muss den privaten Schlüssel für die Herstellung der Verbindung mit dem DCCG schützen. Für die Vorgehensweise nach dem Prinzip „bring your own certificate“ sind ein gut definiertes Registrierungs- und Identifizierungsverfahren sowie die in den *Abschnitten 4.1, 4.2* und *4.3* beschriebenen Widerrufs- und Erneuerungsverfahren erforderlich. Das DCCG nutzt eine weiße Liste, in die die TLS-Zertifikate der NB nach ihrer erfolgreichen Registrierung aufgenommen werden. Eine sichere Verbindung mit dem DCCG können nur NB herstellen, die sich mit einem privaten Schlüssel authentisieren, der einem Zertifikat aus der weißen Liste entspricht. Zudem nutzt das DCCG ein TLS-Zertifikat, das es den NB ermöglicht zu überprüfen, dass sie tatsächlich eine Verbindung mit dem „echten“ DCCG herstellen und nicht mit einer Stelle, die sich mit bösartiger Absicht als DCCG ausgibt. Das Zertifikat des DCCG wird den NB nach erfolgreicher Registrierung bereitgestellt. Das $DCCG_{TLS}$-Zertifikat wird von einer öffentlich als vertrauenswürdig anerkannten Zertifizierungsstelle (in allen gebräuchlichen Browsern enthalten) ausgestellt. Die Mitgliedstaaten sind dafür verantwortlich zu überprüfen, dass ihre Verbindung mit dem DCCG sicher ist (z. B. durch Abgleich des Fingerabdrucks des $DCCG_{TLS}$-Zertifikats des Servers, mit dem sie verbunden sind, mit dem nach der Registrierung bereitgestellten Fingerabdruck).

3.2. *Country Signing CA und Validierungsmodell*

Mitgliedstaaten, die am DCCG-Rahmen teilnehmen, müssen für die Ausstellung von DSC eine Country Signing CA (Länder-Signatur-Zertifizierungsstelle) nutzen. Die Mitgliedstaaten können über mehr als eine CSCA verfügen, z. B. bei Dezentralisierung auf regionaler Ebene. Jeder Mitgliedstaat kann entweder bestehende Zertifizierungsstellen nutzen oder eine spezielle (möglicherweise selbstsignierte) Zertifizierungsstelle für das DCC-System einrichten.

Die Mitgliedstaaten müssen dem DCCG-Betreiber ihr(e) CSCA-Zertifikat(e) während des offiziellen Aufnahmeverfahrens (Onboarding) vorlegen. Nach erfolgreicher Registrierung des Mitgliedstaats (*weitere Einzelheiten in Abschnitt 4.1*) aktualisiert der DCCG-Betreiber eine signierte Vertrauensliste, die alle aktiven CSCA-Zertifikate im DCC-Rahmen enthält. Der DCCG-Betreiber nutzt ein spezielles asymmetrisches Schlüsselpaar, um die Vertrauensliste und die Zertifikate in einer Offline-Umgebung zu signieren. Der private Schlüssel wird nicht im Online-DCCG-System gespeichert, damit die Vertrauensliste bei einem Angriff auf das Online-System nicht beeinflusst werden kann. Das entsprechende Vertrauensanker-Zertifikat $DCCG_{TA}$ wird den nationalen Back-Ends während des Aufnahmeverfahrens bereitgestellt.

▼B

Die Mitgliedstaaten können die Vertrauensliste für ihre Überprüfungsverfahren vom DCCG abrufen. Die CSCA ist die Zertifizierungsstelle, die DSC ausstellt, sodass Mitgliedstaaten, die eine CA-Hierarchie mit mehreren Ebenen nutzen (z. B. Root CA -> CSCA -> DSC) die untergeordnete Zertifizierungsstelle angeben müssen, die die DSC ausstellt. In diesem Fall ignoriert das DCC-System alle der CSCA übergeordneten Stellen, falls der Mitgliedstaat eine bestehende Zertifizierungsstelle nutzt, und nimmt nur die CSCA als Vertrauensanker in die weiße Liste auf (obwohl es sich dabei um eine untergeordnete Zertifizierungsstelle handelt). Das ICAO-Modell lässt nämlich nur genau zwei Ebenen zu — eine „Stamm"-Zertifizierungsstelle („root CSCA") und ein untergeordnetes DSC („leaf DSC"), das von eben dieser Zertifizierungsstelle signiert wird.

Wenn ein Mitgliedstaat seine eigene CSCA betreibt, ist er für einen sicheren Betrieb und ein sicheres Management der Schlüssel dieser CA verantwortlich. Die CSCA dient als Vertrauensanker für DSC, sodass der Schutz des privaten Schlüssels der CSCA für die Integrität der DCC-Umgebung von entscheidender Bedeutung ist. Als Überprüfungsmodell der DCC-PKI dient das Schalenmodell, wonach alle Zertifikate bei der Validierung des Pfads zu einem bestimmten Zeitpunkt (d. h. bei Validierung der Signatur) gültig sein müssen. Daher gelten folgende Beschränkungen:

— Die CSCA darf keine Zertifikate ausstellen, die länger gültig sind als das CA-Zertifikat selbst;

— der Dokumentensignierer darf keine Dokumente signieren, die länger gültig sind als das DSC selbst;

— Mitgliedstaaten, die ihre eigene CSCA betreiben, müssen Gültigkeitszeiträume für ihre CSCA und alle ausgestellten Zertifikate festlegen und die Erneuerung der Zertifikate sicherstellen.

Abschnitt 4.2 enthält Empfehlungen zu Gültigkeitszeiträumen.

3.3. *Integrität und Authentizität der hochgeladenen Daten*

Die nationalen Back-Ends können das DCCG nach erfolgreicher gegenseitiger Authentifizierung nutzen, um digital signierte Datenpakete hoch- und herunterzuladen. Zu Beginn enthalten diese Datenpakete die DSC der Mitgliedstaaten. Das vom nationalen Back-End für die digitale Signatur hochgeladener Datenpakete im DCCG-System genutzte Schlüsselpaar wird als „national backend upload signature key pair" bezeichnet und das entsprechende Public-Key-Zertifikat erhält die Abkürzung NB_{UP}-Zertifikat. Jeder Mitgliedstaat stellt sein eigenes NB_{UP}-Zertifikat bereit, das selbstsigniert ist oder von einer bestehenden Zertifizierungsstelle wie z. B. einer öffentlichen Zertifizierungsstelle ausgestellt wurde (d. h. von einer Zertifizierungsstelle, die Zertifikate im Einklang mit den Baseline Requirements des CAB-Forums ausstellt). Das NB_{UP}-Zertifikat muss sich von allen anderen von dem Mitgliedstaat genutzten Zertifikaten (d. h. CSCA-, TLS-Client-Zertifikate oder DSC) unterscheiden.

Der Mitgliedstaat muss dem DCCG-Betreiber das Upload-Zertifikat während des anfänglichen Registrierungsverfahrens bereitstellen (*weitere Einzelheiten in Abschnitt 4.1*). Jeder Mitgliedstaat ist für die nationalen Daten sowie für den Schutz des beim Hochladen für die Signatur verwendeten privaten Schlüssels verantwortlich.

Andere Mitgliedstaaten können die signierten Datenpakete mithilfe der vom DCCG bereitgestellten Upload-Zertifikate überprüfen. Das DCCG überprüft die Authentizität und Integrität der hochgeladenen Daten anhand des NB-Upload-Zertifikats, bevor sie anderen Mitgliedstaaten bereitgestellt werden.

▼B

3.4. *Anforderungen an die technische DCCG-Architektur*

Die technische DCCG-Architektur muss folgende Anforderungen erfüllen:

— Das DCCG stellt mithilfe der gegenseitigen TLS-Authentifizierung eine authentifizierte verschlüsselte Verbindung mit den NB her. Das DCCG führt daher eine weiße Liste registrierter NB_{TLS}-Client-Zertifikate;

— das DCCG nutzt zwei digitale Zertifikate ($DCCG_{TLS}$ und $DCCG_{TA}$) mit zwei unterschiedlichen Schlüsselpaaren. Der private Schlüssel des $DCCG_{TA}$-Schlüsselpaares wird offline (nicht in den Online-Komponenten des DCCG) gespeichert;

— das DCCG führt eine Vertrauensliste der NB_{CSCA}-Zertifikate, die mit dem privaten Schlüssel des $DCCG_{TA}$-Schlüsselpaares signiert ist;

— die Chiffren müssen den Anforderungen aus *Abschnitt 5.1* entsprechen.

4. **Lebenszyklusmanagement von Zertifikaten**

4.1. *Registrierung der nationalen Back-Ends*

Die Mitgliedstaaten müssen sich beim DCCG-Betreiber registrieren, um am DCCG-System teilzunehmen. In diesem Abschnitt ist das technische und betriebliche Verfahren beschrieben, das bei der Registrierung eines nationalen Back-Ends anzuwenden ist.

Der DCCG-Betreiber und der Mitgliedstaat müssen Informationen über technische Kontaktpersonen für das Aufnahmeverfahren austauschen. Dabei wird angenommen, dass die technischen Kontaktpersonen von ihren Mitgliedstaaten legitimiert sind und die Identifizierung/Authentifizierung über andere Kanäle erfolgt. Zur Authentifizierung könnte die technische Kontaktperson eines Mitgliedstaats die Zertifikate z. B. als passwortgeschützte Dateien per E-Mail bereitstellen und dem DCCG-Betreiber das entsprechende Passwort per Telefon mitteilen. Zudem können weitere vom DCCG-Betreiber genannte sichere Kanäle genutzt werden.

Die Mitgliedstaaten müssen während des Registrierungs- und Identifizierungsverfahrens drei digitale Zertifikate bereitstellen:

— das TLS-Zertifikat NB_{TLS} des Mitgliedstaats

— das Upload-Zertifikat NB_{UP} des Mitgliedstaats

— das/die CSCA-Zertifikat(e) NB_{CSCA} des Mitgliedstaats

Alle bereitgestellten Zertifikate müssen die Anforderungen aus *Abschnitt 5* erfüllen. Der DCCG-Betreiber überprüft, ob die bereitgestellten Zertifikate den Anforderungen aus *Abschnitt 5* entsprechen. Nach der Identifizierung und Registrierung trifft der DCCG-Betreiber folgende Maßnahmen:

— Er nimmt das/die NB_{CSCA}-Zertifikat(e) in die Vertrauensliste auf, die mit dem privaten Schlüssel signiert ist, die dem öffentlichen Schlüssel des $DCCG_{TA}$-Schlüsselpaares entspricht;

— er nimmt das NB_{TLS}-Zertifikat in die weiße Liste des DCCG-TLS-Endpunkts auf;

— er nimmt das NB_{UP}-Zertifikat in das DCCG-System auf;

— er stellt dem Mitgliedstaat die Public-Key-Zertifikate $DCCG_{TA}$ und $DCCG_{TLS}$ bereit.

▼B

4.2. *Zertifizierungsstellen, Gültigkeitszeiträume und Erneuerung*

Wenn ein Mitgliedstaat seine eigene CSCA betreiben will, können die CSCA-Zertifikate selbstsigniert sein. Da sie als Vertrauensanker des Mitgliedstaats dienen, muss der Mitgliedstaat den privaten Schlüssel, der dem öffentlichen Schlüssel des CSCA-Zertifikats entspricht, gut schützen. Es wird empfohlen, für die CSCA der Mitgliedstaaten ein Offline-System zu nutzen, d. h. ein Computersystem, das mit keinem Netz verbunden ist. Die Zugangskontrolle muss durch mehrere Personen erfolgen (z. B. nach dem Vier-Augen-Prinzip). Wenn die DSC signiert sind, sind betriebliche Kontrollen durchzuführen, und das System, in dem der private CSCA-Schlüssel gespeichert wird, ist unter Anwendung strenger Zugangskontrollen sicher zu verwahren. Zusätzlich kann der private CSCA-Schlüssel durch Hardware-Sicherheitsmodule oder Smart Cards geschützt werden. Digitale Zertifikate sind mit einem Gültigkeitszeitraum verbunden, der eine Erneuerung erforderlich macht. Die Erneuerung ist erforderlich, um neue kryptografische Schlüssel zu verwenden und die Schlüssellängen anzupassen, wenn die Sicherheit des verwendeten Verschlüsselungsalgorithmus aufgrund aktueller Entwicklungen in der Computertechnik oder neuer Angriffe gefährdet ist. Dabei wird ein Schalenmodell angewandt (siehe *Abschnitt 3.2*).

Angesichts des einjährigen Gültigkeitszeitraums digitaler COVID-Zertifikate werden folgende Gültigkeitszeiträume empfohlen:

— CSCA: 4 Jahre

— DSC: 2 Jahre

— Upload: 1 bis 2 Jahre

— TLS-Client-Authentifizierung: 1 bis 2 Jahre

Im Interesse einer rechtzeitigen Erneuerung werden für private Schlüssel folgende Nutzungszeiträume empfohlen:

— CSCA-Zertifikat: 1 Jahr

— DSC: 6 Monate

Die Mitgliedstaaten müssen rechtzeitig, z. B. einen Monat vor dem Verfall, neue Upload-Zertifikate und TLS-Zertifikate generieren, um einen unterbrechungsfreien Betrieb zu gewährleisten. CSCA-Zertifikate und DSC sollten (angesichts der erforderlichen betrieblichen Verfahren) spätestens einen Monat vor dem Ende der Nutzung des privaten Schlüssels erneuert werden. Die Mitgliedstaaten müssen dem DCCG-Betreiber aktualisierte CSCA-, Upload- und TLS-Zertifikate bereitstellen. Verfallene Zertifikate werden aus der weißen Liste und der Vertrauensliste gestrichen.

Die Mitgliedstaaten und der DCCG-Betreiber müssen die Gültigkeit ihrer eigenen Zertifikate im Blick behalten. Es gibt keine zentrale Stelle, die die Gültigkeit der Zertifikate überwacht und die Teilnehmer informiert.

▼B

4.3. *Widerruf von Zertifikaten*

Digitale Zertifikate können grundsätzlich von der ausstellenden CA anhand von Zertifikatsperrlisten oder eines Online Certificate Status Protocol Responder (OCSP) widerrufen werden. Die CSCA des DCC-Systems sollten Zertifikatsperrlisten (CRL) bereitstellen. Auch wenn diese CRL gegenwärtig von anderen Mitgliedstaaten nicht genutzt werden, sollten sie für künftige Anwendungen integriert werden. Entscheidet sich eine CSCA, keine CRL bereitzustellen, müssen die DSC dieser CSCA erneuert werden, sobald CRL vorgeschrieben sind. Überprüfer sollten für die Validierung der DSC keine OCSP verwenden, sondern CRL. Es wird empfohlen, dass das nationale Back-End die erforderliche Validierung der vom DCCG heruntergeladenen DSC vornimmt, und den nationalen DCC-Validatoren nur vertrauenswürdige und validierte DSC weiterleitet. Die DCC-Validatoren sollten in ihrem Validierungsverfahren die DSC nicht auf Widerruf überprüfen. Dies dient unter anderem dem Schutz der Daten der DCC-Inhaber, da jede Möglichkeit ausgeschlossen werden soll, dass die Nutzung eines speziellen DSC von dem damit verbundenen OCSP-Responder überwacht werden kann.

Die Mitgliedstaaten können ihre DSC mithilfe gültiger Upload- und TLS-Zertifikate selbst aus dem DCCG entfernen. Wird ein DSC entfernt, werden alle mit diesem DSC ausgestellten DCC ungültig, wenn die Mitgliedstaaten die aktualisierten DSC-Listen erhalten. Der Schutz des den DSC entsprechenden privaten Schlüssel-Materials ist von entscheidender Bedeutung. Die Mitgliedstaaten müssen den DCCG-Betreiber informieren, wenn sie Upload- oder TLS-Zertifikate z. B. aufgrund einer Beeinträchtigung des nationalen Back-Ends widerrufen müssen. Der DCCG-Betreiber kann dann das Vertrauen für das betreffende Zertifikat beenden, z. B. durch Streichen aus der weißen Liste der TLS-Zertifikate. Der DCCG-Betreiber kann die Upload-Zertifikate aus der DCCG-Datenbank entfernen. Pakete, die mit dem privaten Schlüssel signiert wurden, der diesem Upload-Zertifikat entspricht, werden ungültig, wenn nationale Back-Ends das Vertrauen für das widerrufene Upload-Zertifikat beenden. Muss ein CSCA-Zertifikat widerrufen werden, informieren die Mitgliedstaaten den DCCG-Betreiber und die anderen Mitgliedstaaten, mit denen ein Vertrauensverhältnis besteht. Der DCCG-Betreiber erstellt eine neue Vertrauensliste, die das Zertifikat nicht mehr enthält. Alle von dieser CSCA ausgestellten DSC werden ungültig, wenn die Mitgliedstaaten den Truststore ihres nationalen Back-Ends aktualisieren. Muss das $DCCG_{TLS}$-Zertifikat oder das $DCCG_{TA}$-Zertifikat widerrufen werden, müssen der DCCG-Betreiber und die Mitgliedstaaten zusammenarbeiten, um eine neue vertrauenswürdige TLS-Verbindung herzustellen und eine neue Vertrauensliste zu erstellen.

5. **Vorlagen für Zertifikate**

Dieser Abschnitt enthält Anforderungen und Leitlinien zur Verschlüsselung sowie Anforderungen an Vorlagen für Zertifikate. Für die DCCG-Zertifikate werden die Vorlagen der Zertifikate in diesem Abschnitt festgelegt.

5.1. *Anforderungen an die Verschlüsselung*

Verschlüsselungsalgorithmen und TLS-Chiffrensammlungen sind auf der Grundlage der aktuellen Empfehlung des deutschen Bundesamts für Sicherheit in der Informationstechnik (BSI) oder der Gruppe hoher Beamter für die Sicherheit der Informationssysteme (SOG-IS) auszuwählen. Diese Empfehlungen und die Empfehlungen anderer Einrichtungen und Normungsorganisationen sind einander ähnlich. Die Empfehlungen sind in den Technischen Richtlinien TR 02102-1 und TR 02102-2 ([1]) oder den SOG-IS Agreed Cryptographic Mechanisms ([2]) festgelegt.

([1]) BSI - Technical Guidelines TR-02102 (bund.de)
([2]) SOG-IS - Supporting documents (sogis.eu)

▼B

5.1.1. Anforderungen an das DSC

Es gelten die Anforderungen aus *Anhang I Abschnitt 3.2.2*. Den Dokumentensignierern wird daher dringend empfohlen, den Elliptic Curve Digital Signature Algorithm (ECDSA) mit NIST-p-256 (gemäß Anlage D von FIPS PUB 186-4) zu nutzen. Andere elliptische Kurven werden nicht unterstützt. Aufgrund von Platzbeschränkungen der DCC sollten die Mitgliedstaaten RSA-PSS nicht nutzen, auch wenn das Verfahren als Backup-Algorithmus zulässig ist. Wenn Mitgliedstaaten RSA-PSS verwenden, sollten sie eine Modulgröße von 2048 oder maximal 3072 Bit nutzen. Als kryptografische Hash-Funktion für die DSC-Signatur ist SHA-2 mit einer Ausgabelänge von ≥ 256 Bit zu verwenden (siehe ISO/IEC 10118-3:2004).

5.1.2. Anforderungen in Bezug auf TLS-, Upload- und CSCA-Zertifikate

Die folgende Tabelle enthält die wichtigsten Anforderungen an Verschlüsselungsalgorithmen und die Schlüssellängen für digitale Zertifikate und kryptografische Signaturen im Zusammenhang mit dem DCCG (Stand 2021):

Signaturalgorithmus	Schlüssellänge	Hash-Funktion
EC-DSA	mindestens 250 Bit	SHA-2 mit einer Ausgabelänge ≥ 256 Bit
RSA-PSS (empfohlenes Padding) RSA-PKCS#1 v1.5 (Legacy-Padding)	RSA-Modul (N) mit mindestens 3000 Bit und einem öffentlichen Exponenten e > 2^16	SHA-2 mit einer Ausgabelänge ≥ 256 Bit
DSA	Primzahl p mit mindestens 3000 Bit, Schlüssel q mit mindestens 250 Bit	SHA-2 mit einer Ausgabelänge ≥ 256 Bit

Als elliptische Kurve wird für EC-DSA aufgrund der breiten Verwendung NIST-p-256 empfohlen.

5.2. *CSCA-Zertifikat (NB_{CSCA})*

Die folgende Tabelle enthält Anleitungen zur Vorlage für NB_{CSCA}-Zertifikate, wenn ein Mitgliedstaat sich im Zusammenhang mit dem DCC-System für den Betrieb seiner eigenen CSCA entscheidet.

Fettgedruckte Einträge sind obligatorisch (sie müssen in das Zertifikat aufgenommen werden), Einträge in *Kursivschrift* werden empfohlen (sie sollten aufgenommen werden). Für nicht angegebene Felder gibt es keine Empfehlungen.

Feld	Wert
Subjekt	**cn=<nicht leer und eindeutige gebräuchliche Bezeichnung>,** *o=<bereitgestellt durch>,* **c=<Mitgliedstaat, der die CSCA betreibt>**
Schlüsselverwendung	**Signieren von Zertifikaten,** *CRL signing* (mindestens)
Grundlegende Beschränkungen	**CA = true, path length constraints = 0**

Der Name des Subjekts darf nicht leer sein und muss innerhalb des jeweiligen Mitgliedstaats eindeutig sein. Der Ländercode (c) muss dem Mitgliedstaat entsprechen, der dieses CSCA-Zertifikat nutzt. Das Zertifikat muss eine eindeutige Subjekt-Schlüsselkennung (Subject Key Identifier) gemäß RFC 5280 ([1]) enthalten.

([1]) rfc5280 (ietf.org)

▼B

5.3. *Document-Signer-Zertifikat DSC*

Die folgende Tabelle enthält Anleitungen zum DSC. **Fettgedruckte** Einträge sind obligatorisch (sie müssen in das Zertifikat aufgenommen werden), Einträge in *Kursivschrift* werden empfohlen (sie sollten aufgenommen werden). Für nicht angegebene Felder gibt es keine Empfehlungen.

Feld	Wert
Seriennummer	**eindeutige Seriennummer**
Subjekt	**cn=<nicht leer und eindeutige gebräuchliche Bezeichnung>**, *o=<bereitgestellt durch>,* **c=<Mitgliedstaat, der dieses DSC nutzt>**
Schlüsselverwendung	**digitale Signatur** (mindestens)

Das DSC muss mit dem privaten Schlüssel signiert sein, der einem von dem Mitgliedstaat verwendeten CSCA-Zertifikat entspricht.

Dabei sind folgende Erweiterungen zu nutzen:

— Das Zertifikat muss die Schlüsselkennung einer Zertifizierungsstelle (Authority Key Identifier, AKI) enthalten, die der Subjekt-Schlüsselkennung (Subject Key Identifier, SKI) des Zertifikats der ausstellenden CSCA entspricht.

— Das Zertifikat sollte eine eindeutige SKI (gemäß RFC 5280 ([1])) enthalten.

Zudem sollte das Zertifikat die CRL-Verteilerpunkterweiterung enthalten, die auf die Zertifikatsperrliste (CRL) verweist, die von der CSCA, die das DSC ausgestellt hat, bereitgestellt wird.

Das DSC kann eine erweiterte Schlüsselverwendungserweiterung mit null oder mehr Kennungen für die Schlüsselverwendungsvorgaben (Key Usage Policy Identifiers) enthalten, mit denen die Arten von HCERT, die das Zertifikat verifizieren kann, eingeschränkt werden. Ist mindestens eine solche Kennung vorhanden, müssen die Überprüfer die Schlüsselverwendung mit den gespeicherten HCERT abgleichen. Für die erweiterte Schlüsselverwendung werden folgende Werte (extendedKeyUsage values) festgelegt:

Feld	Wert
extendedKeyUsage	1.3.6.1.4.1.1847.2021.1.1 für Aussteller in Bezug auf Tests
extendedKeyUsage	1.3.6.1.4.1.1847.2021.1.2 für Aussteller in Bezug auf Impfungen
extendedKeyUsage	1.3.6.1.4.1.1847.2021.1.3 für Aussteller in Bezug auf Genesung

Ist keine Schlüsselverwendungserweiterung vorhanden (d. h. keine Erweiterungen oder Null-Erweiterung), kann dieses Zertifikat zur Validierung aller Arten von HCERT verwendet werden. In weiteren Unterlagen können zusätzliche relevante Extended Key Usage Policy Identifiers für die Validierung von HCERT bestimmt werden.

5.4. *Upload-Zertifikate (NBUP)*

Die folgende Tabelle enthält Anleitungen für das Upload-Zertifikat des nationalen Back-Ends. **Fettgedruckte** Einträge sind obligatorisch (sie müssen in das Zertifikat aufgenommen werden), Einträge in *Kursivschrift* werden empfohlen (sie sollten aufgenommen werden). Für nicht angegebene Felder gibt es keine Empfehlungen.

([1]) rfc5280 (ietf.org)

▼B

Feld	Wert
Subjekt	**cn=<nicht leer und eindeutige gebräuchliche Bezeichnung>**, *o=<bereitgestellt durch>*, **c=<Mitgliedstaat, der dieses Upload-Zertifikat nutzt>**
Schlüsselverwendung	**digitale Signatur** (mindestens)

5.5. *TLS-Client-Authentifizierung des nationalen Back-Ends (NB_{TLS})*

Die folgende Tabelle enthält Anleitungen für das TLS-Client-Authentifizierungszertifikat des nationalen Back-Ends. **Fettgedruckte** Einträge sind obligatorisch (sie müssen in das Zertifikat aufgenommen werden), Einträge in *Kursivschrift* werden empfohlen (sie sollten aufgenommen werden). Für nicht angegebene Felder gibt es keine Empfehlungen.

Feld	Wert
Subjekt	**cn=<nicht leer und eindeutige gebräuchliche Bezeichnung>**, *o=<bereitgestellt durch>*, **c=<Mitgliedstaat des NB>**
Schlüsselverwendung	**digitale Signatur** (mindestens)
erweiterte Schlüsselverwendung	Client-Authentifizierung (1.3.6.1.5.5.7.3.2)

Das Zertifikat kann auch die erweiterte Schlüsselverwendung *Server-Authentifizierung (1.3.6.1.5.5.7.3.1)* umfassen; dies ist jedoch nicht erforderlich.

5.6. *Zertifikat für die Signatur der Vertrauensliste ($DCCG_{TA}$)*

In der folgenden Tabelle ist das Zertifikat für den DCCG-Vertrauensanker festgelegt.

Feld	Wert
Subjekt	**cn = Gateway für das digitale grüne Zertifikat** ([1])**, o=<bereitgestellt durch>, c=<Land>**
Schlüsselverwendung	**digitale Signatur** (mindestens)

5.7. *DCCG-TLS-Server-Zertifikate ($DCCG_{TLS}$)*

In der folgenden Tabelle ist das DCCG-TLS-Zertifikat festgelegt.

Feld	Wert
Subjekt	cn=<FQDN oder IP-Adresse des DCCG>, o=<bereitgestellt durch>, c= <Land>
SubjectAltName	dNSName: <DCCG DNS-Name> oder IP-Adresse: <DCCG IP-Adresse>
Schlüsselverwendung	**digitale Signatur** (mindestens)
erweiterte Schlüsselverwendung	Server-Authentifizierung (1.3.6.1.5.5.7.3.1)

([1]) Der Begriff „digitales grünes Zertifikat“ anstelle von „digitales COVID-Zertifikat der EU“ wurde in diesem Zusammenhang beibehalten, da dieser Begriff fest kodiert und in das Zertifikat aufgenommen wurde, bevor die beiden Gesetzgebungsorgane über eine neue Terminologie entschieden haben.

▼B

Das Zertifikat kann auch die erweiterte Schlüsselverwendung *Client-Authentifizierung (1.3.6.1.5.5.7.3.2)* umfassen; dies ist jedoch nicht erforderlich.

Das TLS-Zertifikat des DCCG ist von einer öffentlich als vertrauenswürdig anerkannten Zertifizierungsstelle (in allen gebräuchlichen Browsern und Betriebssystemen enthalten, entsprechend den Baseline Requirements des CAB-Forums) auszustellen.

▼M1

ANHANG V

JAVASCRIPT OBJECT NOTATION (JSON)-SCHEMA

1. **Einleitung**

In diesem Anhang wird die technische Datenstruktur für digitale COVID-Zertifikate der EU (EUDCC) festgelegt, dargestellt als JSON-Schema. Das Dokument enthält spezifische Hinweise zu den einzelnen Datenfeldern.

2. **Lokalisierung des JSON-Schemas und Versionen**

Das einzige maßgebliche JSON-Schema für EUDCC ist abrufbar unter https://github.com/ehn-dcc-development/ehn-dcc-schema. An anderer Stelle verfügbare Schemata sind nicht maßgeblich, können jedoch für die Vorbereitung künftiger Überarbeitungen genutzt werden.

Standardmäßig wird unter der angegebenen URL die aktuelle Version angezeigt, die in diesem Anhang beschrieben und von allen Ländern, die derzeit Zertifikate ausstellen, unterstützt wird.

Die anstehende nächste Version, die bis zu einem festgelegten Datum von allen Ländern unterstützt werden soll, wird unter der angegebenen URL mittels Version Tagging angezeigt; eine nähere Beschreibung dazu findet sich in der Readme-Datei.

▼M3

3. **Gemeinsame Strukturen und allgemeine Anforderungen**

Ein digitales COVID-Zertifikat der EU darf nicht ausgestellt werden, wenn aufgrund fehlender Informationen nicht alle Datenfelder entsprechend dieser Spezifikation korrekt gefüllt werden können. **Die Pflicht der Mitgliedstaaten zur Ausstellung digitaler COVID-Zertifikate der EU bleibt hiervon unberührt.**

In allen Feldern können Informationen unter Verwendung des vollständigen Zeichensatzes UNICODE 13.0 im Format UTF-8 eingegeben werden, sofern keine besonderen Beschränkungen auf Wertesätze oder begrenztere Zeichensätze gelten.

Die gemeinsame Struktur stellt sich wie folgt dar:

„JSON“:{

„ver“:<Versionsinformationen>,

„nam“:{

<Informationen zum Namen der Person>

},

„dob“:<Geburtsdatum>,

„v“ or „t“ or „r“:[

{<Informationen zu Impfdosis, Test oder Genesung, ein Eintrag>}

]

}

Nähere Informationen zu einzelnen Gruppen und Feldern finden sich in den nachfolgenden Abschnitten.

Ist nach den Regeln ein Feld zu überspringen, bedeutet dies, dass sein Inhalt leer sein muss und es weder die Bezeichnung noch den Wert des Feldes aufweisen darf.

▼M3

3.1. *Version*

Informationen zur Version sind anzugeben. Die Versionierung erfolgt nach dem Konzept der semantischen Versionierung (semver: https://semver.org). Bei der genutzten Version muss es sich um eine der offiziell freigegebenen Versionen (die aktuelle oder eine ältere offiziell freigegebene Version) handeln. Siehe Abschnitt „Lokalisierung des JSON-Schemas“ für weitere Einzelheiten.

Feldkennung	Feldbezeichnung	Erläuterungen
ver	Schemaversion	Muss der Kennung der für die Erstellung des EUDCC verwendeten Schemaversion entsprechen. Beispiel: „ver“:„1.3.0“

3.2. *Name und Geburtsdatum der Person*

Der Name der Person ist ihr amtlicher vollständiger Name, der dem in Reisedokumenten eingetragenen Namen entspricht. Die Kennung der Struktur ist *nam*. Es ist genau 1 (ein) Personenname anzugeben.

Feldkennung	Feldbezeichnung	Erläuterungen
nam/fn	Nachname(n)	Nachname(n) des Inhabers. Hat der Inhaber keine Nachnamen, aber einen Vornamen, so ist das Feld zu überspringen. In allen anderen Fällen muss genau 1 (ein) nicht leeres Feld vorhanden sein, das alle Nachnamen enthält. Im Fall mehrerer Nachnamen sind diese durch ein Leerzeichen voneinander zu trennen. Zusammengesetzte Namen mit Bindestrichen oder ähnlichen Zeichen müssen jedoch unverändert bleiben. Beispiele: „fn“:„Musterfrau-Gößinger“ „fn“:„Musterfrau-Gößinger Müller“
nam/fnt	Standardisierte(r) Nachname(n)	Nachname(n) des Inhabers, der/die nach derselben Konvention transliteriert wurde(n) wie in den maschinenlesbaren Reisedokumenten des Inhabers (zum Beispiel nach den von der ICAO in ihrem Dokument 9303 Teil 3 festgelegten Regeln). Hat der Inhaber keine Nachnamen, aber einen Vornamen, so ist das Feld zu überspringen. In allen anderen Fällen muss genau 1 (ein) nicht leeres Feld vorhanden sein, das nur die Zeichen A-Z und < enthält. Maximale Länge: 80 Zeichen (gemäß der ICAO-Spezifikation im Dokument 9303). Beispiele: „fnt“:„MUSTERFRAU<GOESSINGER“ „fnt“:„MUSTERFRAU<GOESSINGER<MUELLER“
nam/gn	Vorname(n)	Vorname(n) des Inhabers. Hat der Inhaber keine Vornamen, aber einen Nachnamen, so ist das Feld zu überspringen. In allen anderen Fällen muss genau 1 (ein) nicht leeres Feld vorhanden sein, das alle Vornamen enthält. Im Fall mehrerer Vornamen sind diese durch ein Leerzeichen voneinander zu trennen. Beispiel: „gn“:„Isolde Erika“

▼M3

Feldkennung	Feldbezeichnung	Erläuterungen
nam/gnt	Standardisierte(r) Vorname(n)	Vorname(n) des Inhabers, der/die nach derselben Konvention transliteriert wurde(n) wie in den maschinenlesbaren Reisedokumenten des Inhabers (zum Beispiel nach den von der ICAO in ihrem Dokument 9303 Teil 3 festgelegten Regeln). Hat der Inhaber keine Vornamen, aber einen Nachnamen, so ist das Feld zu überspringen. In allen anderen Fällen muss genau 1 (ein) nicht leeres Feld vorhanden sein, das nur die Zeichen A-Z und < enthält. Maximale Länge: 80 Zeichen. Beispiel: „gnt":„ISOLDE<ERIKA"
dob	Geburtsdatum	Geburtsdatum des Inhabers des digitalen COVID-Zertifikats der EU. Vollständiges Datum oder Teildatum ohne Uhrzeit, beschränkt auf den Bereich von 1900-01-01 bis 2099-12-31. Wenn das Geburtsdatum vollständig oder teilweise bekannt ist, muss genau 1 (ein) nicht leeres Feld vorhanden sein. Wenn das Geburtsdatum auch nicht teilweise bekannt ist, muss das Feld auf eine leere Zeichenfolge „" gesetzt werden. Dies sollte mit den Angaben in den Reisedokumenten übereinstimmen. Wenn Informationen zum Geburtsdatum vorliegen, ist eines der nachstehenden ISO-8601-Formate zu verwenden. Andere Optionen werden nicht unterstützt. YYYY-MM-DD YYYY-MM YYYY (Die Prüf-App kann unter Verwendung der XX-Konvention, die in maschinenlesbaren Reisedokumenten verwendet wird, fehlende Teile des Geburtsdatums anzeigen, z. B. 1990-XX-XX.) Beispiele: „dob":„1979-04-14" „dob":„1901-08" „dob": „1939" „dob":

3.3. *Gruppen für spezifische Informationen je nach Zertifikatstyp*

Das JSON-Schema unterstützt drei Gruppen von Einträgen mit spezifischen Informationen je nach Zertifikatstyp. Jedes EUDCC muss genau 1 (eine) Gruppe enthalten. Leere Gruppen sind nicht zulässig.

Gruppenkennung	Bezeichnung der Gruppe	Einträge
v	Gruppe Impfung	Sie muss, falls vorhanden, genau 1 (einen) Eintrag enthalten, der genau 1 (eine) Impfdosis (eine Dosis) beschreibt.
t	Gruppe Test	Sie muss, falls vorhanden, genau 1 (einen) Eintrag enthalten, der genau 1 (ein) Testergebnis beschreibt.
r	Gruppe Genesung	Sie muss, falls vorhanden, genau 1 (einen) Eintrag enthalten, der genau 1 (eine) Genesungsbestätigung beschreibt.

▼M1

4. **Spezifische Informationen je nach Zertifikatstyp**

4.1. *Impfzertifikat*

Die Gruppe Impfung, falls vorhanden, muss genau 1 (einen) Eintrag enthalten, der genau 1 (ein) Impfereignis (eine Dosis) beschreibt. Alle Elemente der Gruppe Impfung sind obligatorisch, Leerwerte werden nicht unterstützt.

▼**M1**

Feldkennung	Feldbezeichnung	Hinweise
v/tg	Zielkrankheit oder -erreger: COVID-19 (SARS-CoV-2 oder eine seiner Varianten)	Ein codierter Wert aus dem Wertesatz disease-agent-targeted.json. Dieser Wertesatz hat einen einzigen Eintrag 840539006, bei dem es sich um den Code für COVID-19 aus SNOMED CT (GPS) handelt. Es muss genau 1 (ein) nicht leeres Feld vorhanden sein. Beispiel: "tg": "840539006"
v/vp	COVID-19-Impfstoff oder -Prophylaxe	Art des verwendeten Impfstoffs oder der angewandten Prophylaxe. Ein codierter Wert aus dem Wertesatz vaccine-prophylaxis.json. Der Wertesatz wird über das EUDCC-Gateway verteilt. Es muss genau 1 (ein) nicht leeres Feld vorhanden sein. Beispiel: "vp": "1119349007" (ein SARS-CoV-2-mRNA-Impfstoff)
v/mp	COVID-19-Impfstoff	Für diese spezifische Impfdosis verwendetes Arzneimittel. ►**M4** Ein codierter Wert aus dem Wertesatz vaccine-medicinal-product.json. Oder ein codierter Wert, der sich auf eine klinische Prüfung bezieht und der in Anhang II Abschnitt 3 festgelegten Regel entspricht. ◄ Der Wertesatz wird über das EUDCC-Gateway verteilt. Es muss genau 1 (ein) nicht leeres Feld vorhanden sein. Beispiel: "mp": "EU/1/20/1528" (Comirnaty)
v/ma	Zulassungsinhaber oder Hersteller des COVID-19-Impfstoffs	Zulassungsinhaber oder Hersteller, wenn kein Zulassungsinhaber vorhanden. ►**M4** Ein codierter Wert aus dem Wertesatz vaccine-mah-manf.json. Oder ein codierter Wert, der sich auf eine klinische Prüfung bezieht und der in Anhang II Abschnitt 4 festgelegten Regel entspricht. ◄ Der Wertesatz wird über das EUDCC-Gateway verteilt. Es muss genau 1 (ein) nicht leeres Feld vorhanden sein. Beispiel: "ma": "ORG-100030215" (BioNTech Manufacturing GmbH)
v/dn	Nummer der Dosis in einer Impfserie	Sequenznummer (positive ganze Zahl) der bei diesem Impfereignis verabreichten Dosis. 1 für die erste Dosis, 2 für die zweite Dosis usw. Weitere spezifische Regeln finden sich in Anhang II Abschnitt 5. Es muss genau 1 (ein) nicht leeres Feld vorhanden sein. Beispiele: "dn": "1" (erste Dosis) "dn": "2" (zweite Dosis) "dn": "3" (dritte Dosis)
v/sd	Gesamtzahl der Dosen der Impfserie	Gesamtzahl der Dosen (positive ganze Zahl) der Impfserie. Weitere spezifische Regeln finden sich in Anhang II Abschnitt 5. Es muss genau 1 (ein) nicht leeres Feld vorhanden sein. Beispiele: "sd": "1" (im Fall einer ersten Impfserie mit einem nur in einer Dosis zu verabreichenden Impfstoff) "sd": "2" (im Fall einer ersten Impfserie mit einem in zwei Dosen zu verabreichenden Impfstoff oder im Fall einer zusätzlichen Dosis nach einer ersten Impfserie mit einem nur in einer Dosis zu verabreichenden Impfstoff) "sd": "3" (z. B. im Fall zusätzlicher Dosen nach einer ersten Impfserie mit einem in zwei Dosen zu verabreichenden Impfstoff)

▼**M1**

Feldkennung	Feldbezeichnung	Hinweise
v/dt	Datum der Impfung	Datum der Verabreichung der beschriebenen Dosis im Format YYYY-MM-DD (vollständiges Datum ohne Uhrzeit). Andere Formate werden nicht unterstützt. Es muss genau 1 (ein) nicht leeres Feld vorhanden sein. Beispiel: "dt": "2021-03-28"
v/co	Mitgliedstaat oder Drittland, in dem der Impfstoff verabreicht wurde	Angabe des Landes im Format eines 2-Buchstaben-Codes nach ISO 3166 (EMPFOHLEN) oder Verweis auf eine internationale Organisation mit Zuständigkeit für das Impfereignis (z. B. UNHCR oder WHO). Ein codierter Wert aus dem Wertesatz country-2-codes.json. Der Wertesatz wird über das EUDCC-Gateway verteilt. Es muss genau 1 (ein) Feld vorhanden sein. Beispiel: "co": "CZ" "co": "UNHCR"
v/is	Zertifikataussteller	Bezeichnung der Organisation, die das Zertifikat ausgestellt hat. Kennungen sind als Teil der Bezeichnung zulässig; ihre Verwendung allein ohne die Bezeichnung in Textform wird jedoch nicht empfohlen. Maximal 80 UTF-8-Zeichen. Es muss genau 1 (ein) nicht leeres Feld vorhanden sein. Beispiel: "is": "Gesundheitsministerium der Tschechischen Republik" "is": "Impfzentrum Bezirk Süd 3"
v/ci	Eindeutige Zertifikatkennung	Eindeutige Zertifikatkennung (UVCI) gemäß der Festlegung in https://ec.europa.eu/health/sites/default/files/ehealth/docs/vaccination-proof_interoperability-guidelines_en.pdf Die Aufnahme der Prüfsumme ist fakultativ. Das Präfix "URN:UVCI:" kann hinzugefügt werden. Es muss genau 1 (ein) nicht leeres Feld vorhanden sein. Beispiele: "ci": "URN:UVCI:01:NL:187/37512422923" "ci": "URN:UVCI:01:AT:10807843F94AEE0EE5093FBC254BD813#B"

4.2. *Testzertifikat*

Die Gruppe Test, falls vorhanden, muss genau 1 (einen) Eintrag enthalten,
der genau 1 (ein) Testergebnis beschreibt.

Feldkennung	Feldbezeichnung	Hinweise
t/tg	Zielkrankheit oder -erreger: COVID-19 (SARS-CoV-2 oder eine seiner Varianten)	Ein codierter Wert aus dem Wertesatz disease-agent-targeted.json. Dieser Wertesatz hat einen einzigen Eintrag 840539006, bei dem es sich um den Code für COVID-19 aus SNOMED CT (GPS) handelt. Es muss genau 1 (ein) nicht leeres Feld vorhanden sein. Beispiel: "tg": "840539006"
t/tt	Art des Tests	Art des verwendeten Tests, basierend auf dem Zielmaterial des Tests. Ein codierter Wert aus dem Wertesatz test-type.json (basierend auf LOINC). Werte außerhalb des Wertesatzes sind nicht zulässig. Es muss genau 1 (ein) nicht leeres Feld vorhanden sein. Beispiel: "tt": "LP6464-4" (Nukleinsäure-Amplifikation mit Sondennachweis) "tt": "LP217198-3" (Schnell-Immunoassay)

▼M1

Feldkennung	Feldbezeichnung	Hinweise
t/nm	Bezeichnung des Tests (nur Nukleinsäure-Amplifikationstests)	Bezeichnung des verwendeten Nukleinsäure-Amplifikationstests (NAAT). Die Bezeichnung sollte den Namen des Testherstellers und die Handelsbezeichnung des Tests umfassen, getrennt durch ein Komma. Bei NAAT: Das Feld ist fakultativ. ►M4 Bei Antigentest: Das Feld darf nicht genutzt werden, da die Bezeichnung des Tests indirekt über die Kennung des Testgeräts (t/ma) eingesetzt wird. ◄ Wenn vorhanden, darf das Feld nicht leer sein. Beispiel: "nm": "ELITechGroup, SARS-CoV-2 ELITe MGB® Kit"

▼M4

t/ma	Kennung des Testgeräts (nur Antigentests)	Kennung des Testgeräts für Antigentests aus der JRC-Datenbank. Wertesatz (gemeinsame Liste des Gesundheitssicherheitsausschusses): — Alle Antigentests in der gemeinsamen Liste des Gesundheitssicherheitsausschusses (vom Menschen lesbares Format). — https://covid-19-diagnostics.jrc.ec.europa.eu/devices/hsc-common-recognition-rat (maschinenlesbar, Werte des Felds id_device in der Liste des Wertesatzes enthalten). In den EU/EWR-Ländern dürfen Aussteller nur Zertifikate für Tests ausstellen, die im derzeit gültigen Wertesatz enthalten sind. Der Wertesatz wird alle 24 Stunden aktualisiert. Werte außerhalb des Wertesatzes dürfen in von Drittländern ausgestellten Zertifikaten verwendet werden, doch auch dann müssen die Kennungen aus der JRC-Datenbank stammen. Die Verwendung anderer Kennungen, zum Beispiel der direkt von den Testherstellern gelieferten Kennungen, ist nicht zulässig. Prüf-Apps müssen Werte erkennen, die nicht im aktuellen Wertesatz enthalten sind und Zertifikate mit solchen Werten als ungültig anzeigen. Wenn eine Kennung aus dem Wertesatz entfernt wird, dürfen Zertifikate, die diese enthalten, noch höchstens 72 Stunden nach dem Datum der Entfernung akzeptiert werden. Der Wertesatz wird über das EUDCC-Gateway verteilt. Bei Antigentest: Es muss genau 1 (ein) nicht leeres Feld vorhanden sein. Bei NAAT: Das Feld darf nicht genutzt werden, selbst wenn die NAAT-Kennung in der JRC-Datenbank verfügbar ist. Beispiel: „ma“: „344“ (SD BIOSENSOR Inc, STANDARD F COVID-19 Ag FIA);

▼M1

t/sc	Datum und Uhrzeit der Probenahme	Datum und Uhrzeit der Entnahme der Probe. Die Uhrzeit muss Informationen zur Zeitzone umfassen. Der Wert darf nicht die Uhrzeit bezeichnen, zu der das Testergebnis erzielt wurde. Es muss genau 1 (ein) nicht leeres Feld vorhanden sein. Zu verwenden ist eines der nachstehenden ISO-8601-Formate. Andere Optionen werden nicht unterstützt. YYYY-MM-DDThh:mm:ssZ YYYY-MM-DDThh:mm:ss[+-]hh

▼**M1**

Feldkennung	Feldbezeichnung	Hinweise
		YYYY-MM-DDThh:mm:ss[+-]hhmm YYYY-MM-DDThh:mm:ss[+-]hh:mm Beispiele: "sc": "2021-08-20T10:03:12Z" (Uhrzeit UTC) "sc": "2021-08-20T12:03:12+02" (Uhrzeit MESZ) "sc": "2021-08-20T12:03:12+0200" (Uhrzeit MESZ) "sc": "2021-08-20T12:03:12+02:00" (Uhrzeit MESZ)
t/tr	Testergebnis	Ergebnis des Tests. Ein codierter Wert aus dem Wertesatz test-result.json (basierend auf SNOMED CT, GPS). Es muss genau 1 (ein) nicht leeres Feld vorhanden sein. Beispiel: "tr": "260415000" (Nicht nachgewiesen)
t/tc	Testzentrum oder -einrichtung	Bezeichnung des Akteurs, der den Test durchgeführt hat. Kennungen sind als Teil der Bezeichnung zulässig; ihre Verwendung allein ohne die Bezeichnung in Textform wird jedoch nicht empfohlen. Maximal 80 UTF-8-Zeichen. Etwaige zusätzliche Zeichen sollten verkürzt werden. Die Bezeichnung ist nicht für die automatische Verifizierung konzipiert. Bei NAAT: Es muss genau 1 (ein) nicht leeres Feld vorhanden sein. ►**M4** Bei Antigentest: Das Feld ist fakultativ. Wenn vorhanden, darf das Feld nicht leer sein; ◄ Beispiel: "tc": "Testzentrum West Region 245"
t/co	Mitgliedstaat oder Drittland, in dem der Test durchgeführt wurde	Angabe des Landes im Format eines 2-Buchstaben-Codes nach ISO 3166 (EMPFOHLEN) oder Verweis auf eine internationale Organisation mit Zuständigkeit für die Durchführung des Tests (z. B. UNHCR oder WHO). Ein codierter Wert aus dem Wertesatz country-2-codes.json. Der Wertesatz wird über das EUDCC-Gateway verteilt. Es muss genau 1 (ein) Feld vorhanden sein. Beispiele: "co": "CZ" "co": "UNHCR"
t/is	Zertifikataussteller	Bezeichnung der Organisation, die das Zertifikat ausgestellt hat. Kennungen sind als Teil der Bezeichnung zulässig; ihre Verwendung allein ohne die Bezeichnung in Textform wird jedoch nicht empfohlen. Maximal 80 UTF-8-Zeichen. Es muss genau 1 (ein) nicht leeres Feld vorhanden sein. Beispiele: "is": "Gesundheitsministerium der Tschechischen Republik" "is": "Gesundheitsbehörde Region Nord-West"

▼**M1**

Feldkennung	Feldbezeichnung	Hinweise
t/ci	Eindeutige Zertifikatkennung	Eindeutige Zertifikatkennung (UVCI) gemäß der Festlegung in vaccination-proof_interoperability-guidelines_en.pdf (europa.eu) Die Aufnahme der Prüfsumme ist fakultativ. Das Präfix "URN:UVCI:" kann hinzugefügt werden. Es muss genau 1 (ein) nicht leeres Feld vorhanden sein. Beispiele: "ci": "URN:UVCI:01:NL:187/37512422923" "ci": "URN:UVCI:01:AT:10807843F94AEE0EE5093FBC254BD813#B"

4.3. *Genesungszertifikat*

Die Gruppe Genesung, falls vorhanden, muss genau 1 (einen) Eintrag enthalten, der genau 1 (eine) Genesungsbestätigung beschreibt. Alle Elemente der Gruppe Genesung sind obligatorisch, Leerwerte werden nicht unterstützt.

Feldkennung	Feldbezeichnung	Hinweise
r/tg	Krankheit oder Erreger, von der bzw. dem der Inhaber genesen ist: COVID-19 (SARS-CoV-2 oder eine seiner Varianten)	Ein codierter Wert aus dem Wertesatz disease-agent-targeted.json. Dieser Wertesatz hat einen einzigen Eintrag 840539006, bei dem es sich um den Code für COVID-19 aus SNOMED CT (GPS) handelt. Es muss genau 1 (ein) nicht leeres Feld vorhanden sein. Beispiel: "tg": "840539006"
r/fr	Datum des ersten positiven ►**M4** ——— ◄-Testergebnisses des Inhabers	Datum der Entnahme einer Probe für den ►**M4** ——— ◄, bei dem ein positives Testergebnis erzielt wurde, im Format YYYY-MM-DD (vollständiges Datum ohne Uhrzeit). Andere Formate werden nicht unterstützt. Es muss genau 1 (ein) nicht leeres Feld vorhanden sein. Beispiel: "fr": "2021-05-18"
r/co	Mitgliedstaat oder Drittland, in dem der Test durchgeführt wurde	Angabe des Landes im Format eines 2-Buchstaben-Codes nach ISO 3166 (EMPFOHLEN) oder Verweis auf eine internationale Organisation mit Zuständigkeit für die Durchführung des Tests (z. B. UNHCR oder WHO). Ein codierter Wert aus dem Wertesatz country-2-codes.json. Der Wertesatz wird über das EUDCC-Gateway verteilt. Es muss genau 1 (ein) Feld vorhanden sein. Beispiele: "co": "CZ" "co": "UNHCR"
r/is	Zertifikataussteller	Bezeichnung der Organisation, die das Zertifikat ausgestellt hat. Kennungen sind als Teil der Bezeichnung zulässig; ihre Verwendung allein ohne die Bezeichnung in Textform wird jedoch nicht empfohlen. Maximal 80 UTF-8-Zeichen. Es muss genau 1 (ein) nicht leeres Feld vorhanden sein. Beispiel: "is": "Gesundheitsministerium der Tschechischen Republik" "is": "Zentrales Universitätskrankenhaus"

▼**M1**

Feldkennung	Feldbezeichnung	Hinweise
r/df	Zertifikat gültig ab	Erstes Datum, an dem das Zertifikat als gültig gilt. Das Datum darf nicht vor dem als r/fr + 11 days berechneten Datum liegen. Das Datum ist im Format YYYY-MM-DD anzugeben (vollständiges Datum ohne Uhrzeit). Andere Formate werden nicht unterstützt. Es muss genau 1 (ein) nicht leeres Feld vorhanden sein. Beispiel: "df": "2021-05-29"
r/du	Zertifikat gültig bis	Letztes Datum, an dem das Zertifikat als gültig gilt, zugewiesen vom Zertifikataussteller. Das Datum darf nicht nach dem als r/fr + 180 days berechneten Datum liegen. Das Datum ist im Format YYYY-MM-DD anzugeben (vollständiges Datum ohne Uhrzeit). Andere Formate werden nicht unterstützt. Es muss genau 1 (ein) nicht leeres Feld vorhanden sein. Beispiel: "du": "2021-11-14"
r/ci	Eindeutige Zertifikatkennung	Eindeutige Zertifikatkennung (UVCI) gemäß der Festlegung in vaccination-proof_interoperability-guidelines_en.pdf (europa.eu) Die Aufnahme der Prüfsumme ist fakultativ. Das Präfix "URN:UVCI:" kann hinzugefügt werden. Es muss genau 1 (ein) nicht leeres Feld vorhanden sein. Beispiele: "ci": "URN:UVCI:01:NL:187/37512422923" "ci": "URN:UV-CI:01:AT:10807843F94AEE0EE5093FBC254BD813#B"

▼M3

ANHANG VI

ZUSTÄNDIGKEITEN DER MITGLIEDSTAATEN FÜR DEN AUSTAUSCH VON EUDCC-WIDERRUFSLISTEN ALS GEMEINSAM VERANTWORTLICHE FÜR DAS GATEWAY FÜR DAS DIGITALE COVID-ZERTIFIKAT DER EU

ABSCHNITT 1

Unterabschnitt 1

Aufteilung der Zuständigkeiten

(1) Die gemeinsam Verantwortlichen verarbeiten personenbezogene Daten über das Gateway im Einklang mit den technischen Spezifikationen aus Anhang I.

(2) Die für die Ausstellung zuständigen Behörden der Mitgliedstaaten bleiben weiterhin alleine verantwortlich für die Erhebung, Nutzung, Offenlegung und jede sonstige Verarbeitung von Widerrufsinformationen außerhalb des Gateways, einschließlich des Verfahrens für den Widerruf von Zertifikaten.

(3) Jeder Verantwortliche ist dafür verantwortlich, dass die Verarbeitung personenbezogener Daten im Gateway des Vertrauensrahmens im Einklang mit den Artikeln 5, 24 und 26 der Datenschutz-Grundverordnung erfolgt.

(4) Jeder Verantwortliche richtet eine Anlaufstelle mit einer Funktions-Mailbox ein, die der Kommunikation zwischen den gemeinsam Verantwortlichen sowie zwischen den gemeinsam Verantwortlichen und dem Auftragsverarbeiter dient.

(5) Eine von dem in Artikel 14 der Verordnung (EU) 2021/953 genannten Ausschuss eingesetzte Arbeitsgruppe wird damit beauftragt, über alle Fragen zu entscheiden, die sich in Bezug auf den Austausch von Widerrufslisten und die gemeinsame Verantwortlichkeit für die Verarbeitung der personenbezogenen Daten ergeben können, und an der Erstellung koordinierter Weisungen für die Kommission als Auftragsverarbeiterin mitzuwirken. Der Entscheidungsprozess der gemeinsam Verantwortlichen wird von dieser Arbeitsgruppe und der von ihr zu verabschiedenden Verfahrensordnung geregelt. Grundsätzlich führt die Nichtteilnahme eines der gemeinsam Verantwortlichen an einer Sitzung dieser Arbeitsgruppe, die mindestens sieben (7) Tage vor ihrer Einberufung schriftlich angekündigt wurde, zur stillschweigenden Zustimmung zu den Ergebnissen dieser Sitzung der Arbeitsgruppe. Jeder der gemeinsam Verantwortlichen kann eine Sitzung dieser Arbeitsgruppe einberufen.

(6) Weisungen an die Auftragsverarbeiterin werden im Einvernehmen mit den anderen gemeinsam Verantwortlichen gemäß dem unter Nummer 5 beschriebenen Entscheidungsprozess der Arbeitsgruppe von einer der Anlaufstellen der gemeinsam Verantwortlichen übermittelt. Der gemeinsam Verantwortliche, der die Weisung erteilt, übermittelt sie der Auftragsverarbeiterin schriftlich und informiert alle anderen gemeinsam Verantwortlichen darüber. Ist die betreffende Angelegenheit so zeitkritisch, dass eine Sitzung der Arbeitsgruppe gemäß Nummer 5 nicht mehr einberufen werden kann, so kann dennoch eine Weisung erteilt werden, die jedoch von der Arbeitsgruppe zurückgenommen werden kann. Diese Weisung sollte schriftlich erteilt werden, und alle anderen gemeinsam Verantwortlichen sollten zum Zeitpunkt der Erteilung der Anweisung darüber informiert werden.

(7) Durch die Einrichtung der Arbeitsgruppe gemäß Nummer 5 wird die Zuständigkeit eines gemeinsam Verantwortlichen nicht berührt, seine zuständige Aufsichtsbehörde gemäß den Artikeln 33 und 24 der Datenschutz-Grundverordnung zu unterrichten. Für diese Unterrichtung ist keine Zustimmung eines anderen gemeinsam Verantwortlichen erforderlich.

▼M3

(8) Im Rahmen des Gateways des Vertrauensrahmens dürfen nur Personen, die von den benannten nationalen Behörden oder amtlichen Stellen dazu ermächtigt wurden, auf die ausgetauschten personenbezogenen Daten von Nutzern zugreifen.

(9) Jede ausstellende Behörde führt ein Verzeichnis aller Verarbeitungstätigkeiten, die ihrer Zuständigkeit unterliegen. Der Status als gemeinsam Verantwortlicher kann in dem Verzeichnis angegeben werden.

Unterabschnitt 2

Zuständigkeiten und Funktionen bei der Bearbeitung von Anfragen/Anträgen und der Unterrichtung betroffener Personen

(1) In seiner Rolle als ausstellende Behörde informiert jeder Verantwortliche natürliche Personen, deren Zertifikat(e) er widerrufen hat, (im Folgenden die „betroffenen Personen“) über diesen Widerruf und die Verarbeitung ihrer personenbezogenen Daten im Gateway für das digitale COVID-Zertifikat der EU zur Unterstützung des Austauschs von Widerrufslisten gemäß Artikel 14 der Datenschutz-Grundverordnung, außer wenn sich dies als unmöglich erweist oder mit einem unverhältnismäßigen Aufwand verbunden wäre.

(2) Jeder Verantwortliche dient als Anlaufstelle für natürliche Personen, deren Zertifikat er widerrufen hat, und bearbeitet die von betroffenen Personen oder ihren Vertretern gestellten Anfragen/Anträge im Zusammenhang mit der Ausübung ihrer Rechte im Einklang mit der Datenschutz-Grundverordnung. Erhält ein gemeinsam Verantwortlicher eine Anfrage/einen Antrag einer betroffenen Person in Bezug auf ein Zertifikat, das von einem anderen gemeinsam Verantwortlichen ausgestellt wurde, teilt er der betroffenen Person die Identität und die Kontaktdaten dieses zuständigen gemeinsam Verantwortlichen mit. Auf Anfrage eines anderen gemeinsam Verantwortlichen unterstützen sich die gemeinsam Verantwortlichen gegenseitig bei der Bearbeitung von Anfragen/Anträgen betroffener Personen und antworten einander unverzüglich, spätestens jedoch innerhalb von 1 Monat nach Eingang eines Amtshilfeersuchens. Geht bei einem Verantwortlichen eine Anfrage/ein Antrag zu von einem Drittland übermittelten Daten ein, so bearbeitet der Verantwortliche die Anfrage/den Antrag und teilt der betroffenen Person die Identität und die Kontaktdaten der ausstellenden Behörde des Drittlands mit.

(3) Jeder Verantwortliche stellt den betroffenen Personen den Inhalt dieses Anhangs einschließlich der Bestimmungen der Nummern 1 und 2 zur Verfügung.

ABSCHNITT 2

Management von Sicherheitsvorfällen, einschließlich Verletzungen des Schutzes personenbezogener Daten

(1) Die gemeinsam Verantwortlichen unterstützen einander bei der Ermittlung und Behandlung von Sicherheitsvorfällen im Zusammenhang mit der Verarbeitung im Gateway für das digitale COVID-Zertifikat der EU, einschließlich Verletzungen des Schutzes personenbezogener Daten.

(2) Insbesondere teilen die gemeinsam Verantwortlichen einander Folgendes mit:

a) potenzielle oder tatsächliche Risiken für die Verfügbarkeit, Vertraulichkeit und/oder Integrität der personenbezogenen Daten, die im Gateway des Vertrauensrahmens verarbeitet werden;

b) jede Verletzung des Schutzes personenbezogener Daten, die wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten und die Bewertung der Risiken für die Rechte und Freiheiten natürlicher Personen sowie alle Maßnahmen, die ergriffen wurden, um gegen die Verletzung des Schutzes personenbezogener Daten vorzugehen und das Risiko für die Rechte und Freiheiten natürlicher Personen zu mindern;

▼M3

c) jeden Verstoß gegen die technischen und/oder organisatorischen Vorkehrungen für die Verarbeitungsvorgänge im Gateway des Vertrauensrahmens.

(3) Die gemeinsam Verantwortlichen unterrichten die Kommission, die zuständigen Aufsichtsbehörden und, falls erforderlich, die betroffenen Personen im Einklang mit den Artikeln 33 und 34 der Datenschutz-Grundverordnung oder nach Mitteilung der Kommission über alle Verletzungen des Schutzes personenbezogener Daten im Zusammenhang mit der Verarbeitung im Gateway des Vertrauensrahmens.

(4) Jede ausstellende Behörde trifft geeignete technische und organisatorische Maßnahmen, um

a) die Verfügbarkeit, Integrität und Vertraulichkeit der gemeinsam verarbeiteten personenbezogenen Daten zu gewährleisten und zu schützen;

b) alle in ihrem Besitz befindlichen personenbezogenen Daten vor jeglicher unbefugten oder unrechtmäßigen Form der Verarbeitung, des Verlusts, der Verwendung, der Offenlegung, des Erwerbs oder Zugriffs zu schützen;

c) zu gewährleisten, dass der Zugriff auf die personenbezogenen Daten nicht an andere Personen als die Empfänger oder Auftragsverarbeiter weitergegeben oder gewährt wird.

ABSCHNITT 3

Datenschutzfolgenabschätzung

(1) Benötigt ein Verantwortlicher zur Erfüllung seiner Pflichten nach den Artikeln 35 und 36 der Verordnung (EU) 2016/679 Informationen von einem anderen Verantwortlichen, so übermittelt er eine besondere Anfrage an die in Abschnitt 1 Unterabschnitt 1 Nummer 4 genannte Funktions-Mailbox. Letzterer bemüht sich nach besten Kräften, diese Informationen zur Verfügung zu stellen.

▼M3

ANHANG VII

ZUSTÄNDIGKEITEN DER KOMMISSION FÜR DIE UNTERSTÜTZUNG DES AUSTAUSCHS VON EUDCC-WIDERRUFSLISTEN ALS AUFTRAGSVERARBEITERIN FÜR DAS GATEWAY FÜR DAS DIGITALE COVID-ZERTIFIKAT DER EU

Die Kommission

(1) schafft und gewährleistet im Auftrag der Mitgliedstaaten eine sichere und zuverlässige Kommunikationsinfrastruktur, die den Austausch der an das Gateway für das digitale COVID-Zertifikat der EU übermittelten Widerrufslisten unterstützt;

(2) kann Dritte als Unterauftragsverarbeiter beauftragen, um ihren Verpflichtungen als Auftragsverarbeiterin im Gateway des Vertrauensrahmens für die Mitgliedstaaten nachzukommen; die Kommission informiert die gemeinsam Verantwortlichen über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder die Ersetzung anderer Unterauftragsverarbeiter, wodurch die Verantwortlichen die Möglichkeit erhalten, gemeinsam gegen derartige Änderungen Einspruch zu erheben. Die Kommission stellt sicher, dass dieselben Datenschutzverpflichtungen, die in diesem Beschluss festgelegt sind, auch für diese Unterauftragsverarbeiter gelten;

(3) verarbeitet personenbezogene Daten nur auf dokumentierte Weisung der Verantwortlichen, es sei denn, dass eine Verarbeitung nach Unionsrecht oder nationalem Recht erfolgen muss; in einem solchen Fall teilt die Kommission den gemeinsam Verantwortlichen diese rechtliche Anforderung vor der Durchführung der Verarbeitungstätigkeit mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet;

verarbeitet die Daten wie folgt:

a) Authentifizierung nationaler Back-End-Server auf der Grundlage nationaler Back-End-Server-Zertifikate;

b) Empfang der in Artikel 5a Absatz 3 des Durchführungsbeschlusses genannten Daten von nationalen Back-End-Servern über eine von ihr bereitgestellte Anwendungsprogrammierschnittstelle, die es nationalen Back-End-Servern ermöglicht, die betreffenden Daten hochzuladen;

c) Speicherung der Daten im Gateway für das digitale COVID-Zertifikat der EU;

d) Bereitstellung der Daten zum Herunterladen durch nationale Back-End-Server;

e) Löschung der Daten an ihrem Ablaufdatum oder auf Anweisung des Verantwortlichen, der sie übermittelt hat;

f) Löschung aller verbleibenden Daten nach Beendigung der Leistung, es sei denn, das Unionsrecht oder das Recht der Mitgliedstaaten schreibt eine Speicherung der personenbezogenen Daten vor;

(4) trifft alle organisatorischen, physischen und logischen Sicherheitsmaßnahmen auf der Grundlage des aktuellen Stands der Technik, um das Gateway für das digitale COVID-Zertifikat der EU zu erhalten. Zu diesem Zweck wird die Kommission

a) eine für das Sicherheitsmanagement beim Gateway für das digitale COVID-Zertifikat der EU zuständige Stelle benennen, den gemeinsam Verantwortlichen deren Kontaktdaten mitteilen und deren Verfügbarkeit zur Reaktion auf Sicherheitsbedrohungen gewährleisten;

▼M3

b) die Verantwortung für die Sicherheit des Gateways für das digitale COVID-Zertifikat der EU übernehmen, einschließlich regelmäßiger Prüfungen, Beurteilungen und Bewertungen der Sicherheitsmaßnahmen;

c) sicherstellen, dass alle Personen, denen der Zugriff auf das Gateway für das digitale COVID-Zertifikat der EU gewährt wird, vertraglichen, beruflichen oder gesetzlichen Vertraulichkeitsverpflichtungen unterliegen;

(5) trifft alle erforderlichen Sicherheitsmaßnahmen, damit das reibungslose Funktionieren der nationalen Back-End-Server nicht beeinträchtigt wird. Zu diesem Zweck richtet die Kommission besondere Verfahren für den Anschluss der Back-End-Server an das Gateway für das digitale COVID-Zertifikat der EU ein. Dies umfasst:

a) ein Verfahren zur Risikobewertung, um potenzielle Bedrohungen des Systems zu ermitteln und abzuschätzen;

b) ein Audit- und Überprüfungsverfahren

i) zur Überprüfung der Übereinstimmung der umgesetzten Sicherheitsmaßnahmen mit den geltenden Sicherheitsvorgaben;

ii) zur regelmäßigen Kontrolle der Integrität der Systemdateien, der Sicherheitsparameter und der erteilten Genehmigungen;

iii) zur Überwachung zwecks Feststellung von Sicherheitsverstößen und von unbefugtem Eindringen;

iv) zur Umsetzung von Änderungen zur Behebung bestehender Sicherheitslücken und

v) zur Festlegung der Bedingungen, unter denen — auch auf Anfrage der Verantwortlichen — unabhängige Audits einschließlich Inspektionen sowie Überprüfungen von Sicherheitsmaßnahmen im Einklang mit den Bedingungen des Protokolls (Nr. 7) zum AEUV über die Vorrechte und Befreiungen der Europäischen Union durchgeführt werden können und die Mitwirkung an diesen Audits und Überprüfungen zulässig ist;

c) ein Änderungskontrollverfahren, um die Auswirkungen einer Änderung vor ihrer Umsetzung zu dokumentieren und abzuschätzen und die gemeinsam Verantwortlichen über alle Änderungen auf dem Laufenden zu halten, die sich auf die Kommunikation mit ihren Infrastrukturen und/oder deren Sicherheit auswirken können;

d) die Festlegung eines Wartungs- und Reparaturverfahrens mit Regeln und Bedingungen für die Wartung und/oder Reparatur von Ausrüstungen;

e) die Festlegung eines Verfahrens in Bezug auf Sicherheitsvorfälle zur Festlegung des Melde- und Eskalationsprogramms, zur unverzüglichen Unterrichtung der Verantwortlichen über jegliche Verletzung des Schutzes personenbezogener Daten, unter anderem, damit diese die nationalen Datenschutzaufsichtsbehörden informieren können, sowie zur Festlegung eines Disziplinarverfahrens, um gegen Sicherheitsverletzungen vorzugehen;

(6) ergreift physische und/oder logische Sicherheitsmaßnahmen auf der Grundlage des aktuellen Stands der Technik für die Einrichtungen, in denen die Ausrüstung für das Gateway für das digitale COVID-Zertifikat der EU untergebracht ist, und für die Kontrollen der logischen Daten und der Zugriffssicherheit. Zu diesem Zweck wird die Kommission

a) die physische Sicherheit durchsetzen, um abgegrenzte Sicherheitsbereiche einzurichten und das Erkennen von Verstößen zu ermöglichen;

▼M3

b) den Zugang zu den Einrichtungen kontrollieren und ein Besucherregister für Rückverfolgungszwecke führen;

c) sicherstellen, dass die externen Personen, denen Zugang zu den Räumlichkeiten gewährt wird, von entsprechend bevollmächtigten Mitarbeitern begleitet werden;

d) sicherstellen, dass Ausrüstungen nicht ohne Vorabgenehmigung durch die benannten zuständigen Stellen hinzugefügt, ersetzt oder entfernt werden können;

e) den beiderseitigen Zugriff auf nationale Back-End-Server und das Gateway des Vertrauensrahmens kontrollieren;

f) sicherstellen, dass Personen, die Zugriff auf das Gateway für das digitale COVID-Zertifikat der EU haben, identifiziert und authentifiziert werden;

g) die Rechte für den Zugriff auf das Gateway für das digitale COVID-Zertifikat der EU überprüfen, falls eine Sicherheitsverletzung in Bezug auf diese Infrastruktur eintritt;

h) die Integrität der über das Gateway für das digitale COVID-Zertifikat der EU übermittelten Informationen wahren;

i) technische und organisatorische Sicherheitsmaßnahmen umsetzen, um unbefugten Zugriff auf personenbezogene Daten zu verhindern;

j) bei Bedarf Maßnahmen zur Verhinderung des unbefugten Zugriffs auf das Gateway für das digitale COVID-Zertifikat der EU von der Netzdomäne der nationalen Behörden aus ergreifen (d. h. Sperrung eines Standorts/einer IP-Adresse);

(7) ergreift Maßnahmen zum Schutz ihrer Netzdomäne, einschließlich der Trennung von Anschlüssen, im Falle einer erheblichen Abweichung von den Qualitäts- oder Sicherheitsgrundsätzen und -konzepten;

(8) führt einen Risikomanagementplan in Bezug auf ihren Zuständigkeitsbereich;

(9) überwacht — in Echtzeit — die Leistung aller Dienstkomponenten ihrer Dienste für das Gateway des Vertrauensrahmens, erstellt regelmäßige Statistiken und führt Aufzeichnungen;

(10) leistet Unterstützung für alle Dienste des Gateways des Vertrauensrahmens in englischer Sprache rund um die Uhr über Telefon, E-Mail oder das Web-Portal und nimmt Anrufe von autorisierten Anrufern entgegen: von den Koordinatoren des Gateways für das digitale COVID-Zertifikat der EU und ihren jeweiligen Helpdesks, von Projektbeauftragten und benannten Mitarbeitern der Kommission;

(11) unterstützt, soweit dies gemäß Artikel 12 der Verordnung (EU) 2018/1725 möglich ist, die gemeinsam Verantwortlichen durch geeignete technische und organisatorische Maßnahmen bei der Erfüllung von deren Verpflichtung zur Bearbeitung von Anfragen/Anträgen in Bezug auf die Ausübung der Rechte der betroffenen Person gemäß Kapitel III der Datenschutz-Grundverordnung;

▼**M3**

(12) unterstützt die gemeinsam Verantwortlichen durch die Bereitstellung von Informationen über das Gateway für das digitale COVID-Zertifikat der EU dabei, den Verpflichtungen gemäß den Artikeln 32, 33, 34, 35 und 36 der Datenschutz-Grundverordnung nachzukommen;

(13) stellt sicher, dass die im Gateway für das digitale COVID-Zertifikat der EU verarbeiteten Daten für Personen, die nicht zugriffsbefugt sind, unverständlich sind;

(14) ergreift alle erforderlichen Maßnahmen, damit die Betreiber des Gateways für das digitale COVID-Zertifikat der EU keinen unbefugten Zugriff auf übermittelte Daten haben;

(15) ergreift Maßnahmen, um die Interoperabilität und die Kommunikation zwischen den benannten Verantwortlichen des Gateways für das digitale COVID-Zertifikat der EU zu erleichtern;

(16) führt gemäß Artikel 31 Absatz 2 der Verordnung (EU) 2018/1725 ein Verzeichnis aller im Auftrag der gemeinsam Verantwortlichen durchgeführten Verarbeitungsvorgänge.