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)

DIE EUROPÄISCHE KOMMISSION —

gestützt auf den Vertrag über die Arbeitsweise der Europäischen Union,

gestützt auf die Verordnung (EU) 2021/953 des Europäischen Parlaments und des Rates 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 ([1]), insbesondere auf Artikel 9 Absätze 1 und 3,

in Erwägung nachstehender Gründe:

(1) Das digitale COVID-Zertifikat der EU soll gemäß der Verordnung (EU) 2021/953 als Nachweis dafür dienen, dass eine Person gegen COVID-19 geimpft wurde, ein negatives Testergebnis erhalten hat oder von einer Infektion genesen ist.

(2) Damit das digitale COVID-Zertifikat der EU in der gesamten Union verwendet werden kann, ist es erforderlich, technische Spezifikationen und Vorschriften festzulegen, um die digitalen COVID-Zertifikate zu füllen, auf sichere Weise auszustellen und zu überprüfen, den Schutz personenbezogener Daten zu gewährleisten, die gemeinsame Struktur der eindeutigen Zertifikatkennung sicherzustellen und einen gültigen, sicheren und interoperablen Strichcode zu erstellen. Dieser Vertrauensrahmen schafft auch die erforderlichen Voraussetzungen, um die Interoperabilität mit internationalen Standards und technologischen Systemen zu gewährleisten, und könnte somit als Vorbild für die Zusammenarbeit auf globaler Ebene dienen.

(3) Damit das digitale COVID-Zertifikat der EU gelesen und verarbeitet werden kann, bedarf es einer gemeinsamen Datenstruktur und einer Einigung auf die beabsichtigte Bedeutung der einzelnen Nutzdatenfelder und ihrer möglichen Werte. Zur Förderung dieser Interoperabilität muss eine gemeinsame, koordinierte Datenstruktur für den Rahmen des digitalen COVID-Zertifikats der EU festgelegt werden. Die Leitlinien für diesen Rahmen wurden vom Netzwerk für elektronische Gesundheitsdienste entwickelt, das auf der Grundlage der Richtlinie 2011/24/EU des Europäischen Parlaments und des Rates ([2]) eingerichtet wurde. Bei der Festlegung der technischen Spezifikationen für das Format und das Vertrauensmanagement für das digitale COVID-Zertifikat der EU sollten diese Leitlinien berücksichtigt werden. Es sollten eine Spezifikation der Datenstruktur und Verschlüsselungsmechanismen sowie ein Transportverschlüsselungsmechanismus in einem maschinenlesbaren optischen Format (QR) festgelegt werden, das auf dem Bildschirm eines mobilen Geräts angezeigt oder auf Papier ausgedruckt werden kann.

(4) Zusätzlich zu den technischen Spezifikationen für das Format und das Vertrauensmanagement für das digitale COVID-Zertifikat der EU sollten allgemeine Regelungen für das Füllen der Zertifikate festgelegt werden, die auf verschlüsselte Inhalte des digitalen COVID-Zertifikats der EU angewandt werden. Die Wertesätze zur Umsetzung dieser Regelungen sollten von der Kommission auf der Grundlage der einschlägigen Arbeiten des Netzwerks für elektronische Gesundheitsdienste regelmäßig aktualisiert und veröffentlicht werden.

(5) Gemäß der Verordnung (EU) 2021/953 müssen echte Zertifikate, aus denen sich das digitale COVID-Zertifikat der EU zusammensetzt, mittels einer eindeutigen Zertifikatkennung einzeln identifiziert werden können, da es sein kann, dass Bürgerinnen und Bürgern mehr als ein Zertifikat ausgestellt wird, solange die Verordnung (EU) 2021/953 in Kraft ist. Die eindeutige Zertifikatkennung muss aus einer alphanumerischen Zeichenfolge bestehen, und die Mitgliedstaaten sollten sicherstellen, dass sie keine Daten enthält, die sie mit anderen Dokumenten oder Kennungen wie Pass- oder Personalausweisnummern verknüpft, damit eine Identifizierung des Inhabers verhindert wird. Um die Eindeutigkeit der Zertifikatkennung zu gewährleisten, sollten für deren gemeinsame Struktur technische Spezifikationen und Vorschriften festgelegt werden.

([1]) ABl. L 211 vom 15.6.2021, S. 1.

([2]) Richtlinie 2011/24/EU des Europäischen Parlaments und des Rates vom 9. März 2011 über die Ausübung der Patientenrechte in der grenzüberschreitenden Gesundheitsversorgung (ABl. L 88 vom 4.4.2011, S. 45).

(6) Die Sicherheit, Authentizität, Gültigkeit und Integrität der Zertifikate, aus denen das digitale COVID-Zertifikat der EU besteht, sowie ihre Übereinstimmung mit dem Datenschutzrecht der Union sind unverzichtbare Voraussetzungen für die Akzeptanz in allen Mitgliedstaaten. Diese Ziele werden durch den Vertrauensrahmen erreicht, der die Regeln sowie die Infrastruktur für die zuverlässige und sichere Ausstellung und Überprüfung der digitalen COVID-Zertifikate der EU enthält. Der Vertrauensrahmen sollte sich unter anderem auf eine Public-Key-Infrastruktur stützen, wobei die Vertrauenskette von den Gesundheitsbehörden oder anderen vertrauenswürdigen Stellen der Mitgliedstaaten bis hin zu den einzelnen Stellen, die die digitalen COVID-Zertifikate der EU ausstellen, reichen sollte. Zur Gewährleistung eines EU-weit interoperablen Systems hat die Kommission deshalb ein zentrales System — das „EU Digital COVID Certificate Gateway" (im Folgenden „Gateway") — eingerichtet, in dem die für die Überprüfung verwendeten öffentlichen Schlüssel gespeichert werden. Beim Scannen des QR-Codes des Zertifikats wird die digitale Signatur mithilfe des entsprechenden öffentlichen Schlüssels, der zuvor in diesem zentralen Gateway gespeichert wurde, überprüft. Digitale Signaturen können verwendet werden, um die Integrität und Authentizität der Daten zu gewährleisten. Public-Key-Infrastrukturen stellen durch die Zuordnung öffentlicher Schlüssel zu den Zertifikatausstellern Vertrauen her. Im Gateway wird die Authentizität mithilfe mehrerer Public-Key-Zertifikate gewährleistet. Um zwischen den Mitgliedstaaten einen sicheren Datenaustausch für das öffentliche Schlüsselmaterial zu gewährleisten und eine umfassende Interoperabilität zu ermöglichen, muss festgelegt werden, welche Public-Key-Zertifikate verwendet werden dürfen und wie sie generiert werden sollen.

(7) Dieser Beschluss ermöglicht es, die Anforderungen der Verordnung (EU) 2021/953 so umzusetzen, dass die Verarbeitung personenbezogener Daten auf das für die Verwendung des digitalen COVID-Zertifikats der EU notwendige Maß beschränkt wird und durch konstruktive Maßnahmen sichergestellt wird, dass die Umsetzung durch die für die Verarbeitung Verantwortlichen im Einklang mit dem Datenschutz erfolgt.

(8) Gemäß der Verordnung (EU) 2021/953 sind die Behörden oder anderen benannten Stellen, die für die Zertifikatausstellung zuständig sind, Verantwortliche im Sinne von Artikel 4 Absatz 7 der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates ([3]), wenn sie während des Ausstellungsvorgangs personenbezogene Daten verarbeiten. Je nachdem, wie die Mitgliedstaaten diesen Vorgang gestalten, können eine oder mehrere Behörden oder benannte Stellen, z. B. regionale Gesundheitsdienste, beteiligt sein. Im Einklang mit dem Subsidiaritätsprinzip bleibt diese Entscheidung den Mitgliedstaaten überlassen. Deshalb sind bei Beteiligung mehrerer Behörden oder anderer benannter Stellen die Mitgliedstaaten am ehesten in der Lage, für eine klare Aufgabenzuweisung zu sorgen, unabhängig davon, ob es sich um eigenständige oder gemeinsam Verantwortliche handelt (u. a. regionale Gesundheitsdienste, die für die Ausstellung der Zertifikate ein gemeinsames Patientenportal einrichten). Auch bei der Überprüfung der Zertifikate durch die zuständigen Behörden des Bestimmungs- oder Transitmitgliedstaats oder die grenzüberschreitend tätigen Personenverkehrsdienstleister, die nach nationalem Recht verpflichtet sind, bestimmte Maßnahmen im Bereich der öffentlichen Gesundheit während der COVID-19-Pandemie durchzuführen, müssen die betreffenden Überprüfer ihren datenschutzrechtlichen Verpflichtungen nachkommen.

(9) Das „EU Digital COVID Certificate Gateway" verarbeitet keine personenbezogenen Daten, da es lediglich die öffentlichen Schlüssel der signierenden Stellen enthält. Diese Schlüssel beziehen sich auf die signierenden Stellen und ermöglichen weder eine direkte noch indirekte Identifizierung natürlicher Personen, denen ein Zertifikat ausgestellt wurde. Als Verwalterin des Gateways sollte die Kommission somit weder Verantwortliche noch Auftragsverarbeiterin personenbezogener Daten sein.

(10) Der Europäische Datenschutzbeauftragte wurde gemäß Artikel 42 Absatz 1 der Verordnung (EU) 2018/1725 des Europäischen Parlaments und des Rates ([4]) angehört und hat am 22. Juni 2021 eine Stellungnahme abgegeben.

(11) Da für die Anwendung der Verordnung (EU) 2021/953 ab dem 1. Juli 2021 technische Spezifikationen und Vorschriften benötigt werden, ist die sofortige Anwendung dieses Beschlusses gerechtfertigt.

(12) In Anbetracht der Notwendigkeit, das digitale COVID-Zertifikat der EU rasch umzusetzen, sollte daher dieser Beschluss am Tag seiner Veröffentlichung in Kraft treten —

([3]) Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (ABl. L 119 vom 4.5.2016, S. 1).

([4]) Verordnung (EU) 2018/1725 des Europäischen Parlaments und des Rates vom 23. Oktober 2018 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe, Einrichtungen und sonstigen Stellen der Union, zum freien Datenverkehr und zur Aufhebung der Verordnung (EG) Nr. 45/2001 und des Beschlusses Nr. 1247/2002/EG (ABl. L 295 vom 21.11.2018, S. 39).

HAT FOLGENDEN BESCHLUSS ERLASSEN:

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.

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 aufgeführt.

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

Brüssel, den 28. Juni 2021

Für die Kommission
Die Präsidentin
Ursula VON DER LEYEN

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

— 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

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

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 ([3])) 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.

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 ([4]), 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]) rfc8230 (ietf.org)
([4]) rfc8392 (ietf.org)

3.2.6. Ausgestellt am

Die Anforderung „Ausgestellt am“ (iat) muss einen Zeitstempel im ganzzahligen NumericDate-Format (gemäß RFC 8392 ([5]), 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 ([6])), das die Angaben zum Gesundheitsstatus enthält. Für dieselbe Anforderung kann es mehrere verschiedene Arten von Gesundheitszertifikaten geben, von denen das DCC eines ist.

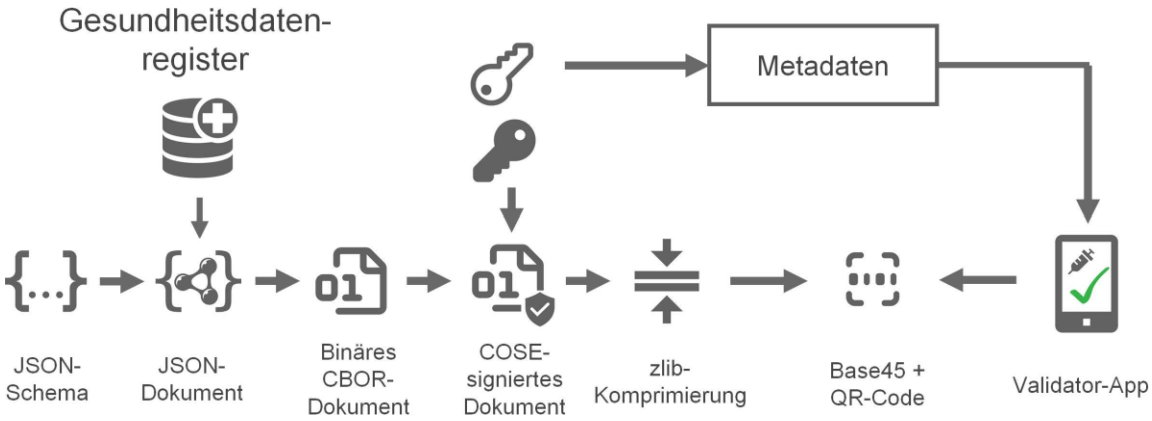
Die JSON dient rein schematischen Zwecken. Das Darstellungsformat ist CBOR gemäß der Spezifikation in (RFC 7049 ([7])). In der Praxis ent- oder verschlüsseln Anwendungsentwickler möglicherweise nie aus dem bzw. in das JSON-Format, sondern verwenden lediglich die In-Memory-Struktur.

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 ([8]) 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]) rfc8392 (ietf.org)
([6]) rfc7159 (ietf.org)
([7]) rfc7049 (ietf.org)
([8]) 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).

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.

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 ([9])) und des Deflate-Kompressionsverfahrens in das in (RFC 1951 ([10])) 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.

([9]) rfc1950 (ietf.org)
([10]) rfc1951 (ietf.org)

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.

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 ([11]), 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.

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.

([11]) rfc7517 (ietf.org)

ANHANG II

VORSCHRIFTEN FÜR DAS FÜLLEN DES DIGITALEN COVID-ZERTIFIKATS DER EU

Die allgemeinen Vorschriften bezüglich der in diesem Anhang festgelegten Wertesätze sollen die Interoperabilität auf semantischer Ebene gewährleisten und eine einheitliche technische Umsetzung des DCC ermöglichen. 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 verschlüsselter Wertesätze semantisch standardisiert werden müssen.

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

Für alle Datenfelder, die nicht in den folgenden Beschreibungen der Wertesätze aufgeführt sind, wird eine UTF-8-Verschlüsselung empfohlen (Name, Testzentrum, Zertifikatausssteller). Datenfelder mit Kalenderdaten (Geburtsdatum, Impfdatum, Datum der Probenahme, Datum des ersten positiven Testergebnisses, Gültigkeitsdaten des Zertifikats) sollten gemäß ISO 8601 verschlüsselt werden.

Sind aus einem Grund die nachstehenden bevorzugten Verschlüsselungssysteme nicht anwendbar, so können andere internationale Verschlüsselungssysteme verwendet werden, wobei Hinweise zur Umwandlung der Codes des anderen Systems in das bevorzugte Verschlüsselungssystem gegeben werden sollten. Ist in den festgelegten Wertesätzen kein geeigneter Code enthalten, so kann in Ausnahmefällen auch Text (Anzeigennamen) als Sicherungsmechanismus verwendet werden.

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

Die Wertesätze werden von der Kommission mit Unterstützung des Netzwerks für elektronische Gesundheitsdienste und des Gesundheitssicherheitsausschusses regelmäßig aktualisiert. Die aktualisierten Wertesätze werden auf der einschlägigen Website der Kommission sowie auf der Website des Netzwerks für elektronische Gesundheitsdienste veröffentlicht. Alle Änderungen sollten dokumentiert werden.

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

   Bevorzugtes Codesystem: SNOMED CT.

   Zu verwenden in Zertifikat 1, 2 und 3.

   Die gewählten Codes müssen auf COVID-19 oder, falls aus epidemiologischen Gründen genauere Informationen über die genetische Variante von SARS-CoV-2 benötigt werden, auf diese Varianten verweisen.

   Zu verwenden ist beispielsweise der SNOMED-CT-Code 840539006 (COVID-19).

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

   Bevorzugtes Codesystem: SNOMED CT oder ATC-Klassifikation.

   Zu verwenden in Zertifikat 1.

   Beispiele aus den bevorzugten Codesystemen: SNOMED CT 1119305005 (SARS-CoV-2-Antigen-Impfstoff), 1119349007 (SARS-CoV-2-mRNA-Impfstoff) oder J07BX03 (COVID-19-Impfstoffe). Sobald neue Arten von Impfstoffen entwickelt und verwendet werden, sollte der Wertesatz erweitert werden.

3. **COVID-19-Impfstoff**

   Bevorzugte Codesysteme (in der Reihenfolge ihrer Präferenz):

   — EU-Arzneimittelregister für Impfstoffe mit unionsweiter Zulassung (Zulassungsnummern)

   — Globales Impfstoffregister, wie es die Weltgesundheitsorganisation einrichten könnte

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

Name des Wertesatzes: Impfstoff.

Zu verwenden in Zertifikat 1.

Beispiel aus den bevorzugten Codesystemen: EU/1/20/1528 (Comirnaty). Beispiel für die Code-Bezeichnung eines Impfstoffes: Sputnik-V (für Sputnik V).

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

Bevorzugtes Codesystem:

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

— Globales Zulassungsinhaber-/Hersteller-Register, wie es die Weltgesundheitsorganisation einrichten könnte

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

Zu verwenden in Zertifikat 1.

Beispiel aus dem bevorzugten Codesystem: ORG-100001699 (AstraZeneca AB). Beispiel für die Code-Bezeichnung einer Organisation: Sinovac-Biotech (für Sinovac Biotech).

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

Zu verwenden in Zertifikat 1.

Zwei Felder:

(1) Anzahl der in einem Zyklus verabreichten Dosen

(2) Anzahl der für einen vollständigen Zyklus zu erwartenden Dosen (bezogen auf eine Person zum Zeitpunkt der Verabreichung).

Beispielsweise stehen 1/1, 2/2 für einen vollständigen Zyklus, wobei 1/1 auch für Impfstoffe mit zwei Dosen steht, wenn das Protokoll des Mitgliedstaats die Verabreichung nur einer Dosis für Personen vorsieht, bei denen vor der Impfung COVID-19 festgestellt wurde. Die Gesamtzahl der Dosen einer Serie sollte nach Maßgabe der zum Zeitpunkt der Verabreichung der Dosis verfügbaren Informationen angegeben werden. Wird beispielsweise für einen bestimmten Impfstoff zum Zeitpunkt der letzten verabreichten Impfung eine dritte Dosis (Auffrischung) für notwendig erachtet, so muss dies aus der zweiten Zahl des Feldes hervorgehen (z. B. 2/3, 3/3 usw.).

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)

7. **Art des Tests**

Bevorzugtes Codesystem: LOINC.

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

Die Codes in diesem Wertesatz müssen auf das Testverfahren verweisen und sind mindestens so zu wählen, dass die NAAT-Tests von den Antigen-Schnelltests gemäß der Verordnung (EU) 2021/953 unterschieden werden.

Beispiel aus dem bevorzugten Codesystem: LP217198-3 (Rapid immunoassay).

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

Bevorzugtes Codesystem: Liste der Antigen-Schnelltests des Gesundheitssicherheitsausschusses, die von der Gemeinsamen Forschungsstelle (JRC) geführt wird (Datenbank für In-vitro-Diagnostika und Testmethoden für COVID-19).

Zu verwenden in Zertifikat 2.

Der Wertesatz muss alle Antigen-Schnelltests enthalten, die in der aktuellen gemeinsamen Liste der COVID-19-Antigen-Schnelltests, die gemäß der Empfehlung 2021/C 24/01 des Rates erstellt und vom Gesundheitssicherheitsausschuss gebilligt wurde, aufgeführt sind. 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

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**

Bevorzugtes Codesystem: SNOMED CT.

In Zertifikat 2 zu verwenden.

Die gewählten Codes müssen eine Unterscheidung zwischen positivem und negativem Testergebnis (nachgewiesen oder nicht nachgewiesen) ermöglichen. Weitere Werte (z. B. unbestimmt) können hinzugefügt werden, wenn die Anwendungsfälle dies erfordern.

Beispiele aus dem bevorzugten Codesystem: 260415000 (nicht nachgewiesen) und 260373001 (nachgewiesen).

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.

3. **Allgemeine Anforderungen**

Die UCI sollten folgenden generellen 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], [2] verwendet werden: {„/“, „#“, “:“};

(2) Maximale Länge: bei der Programmierung sollte eine Länge von 27-30 Zeichen möglichst nicht überschritten werden [3];

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

(4) Länderpräfix: Das Länderkürzel ist in ISO 3166-1 festgelegt. Längere Kürzel (drei Zeichen und mehr (z. B. „UNHCR“) sind künftigen Verwendungen vorbehalten;

(5) Code-Suffix/Prüfsumme:

5.1. Die Mitgliedstaaten sollten 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 sollte die gesamte nach ISO-7812-1 (LUHN-10) [4] zusammengefasste UCI in digitalem Übertragungsformat sein. Die Prüfsumme wird durch das Zeichen „#“ von der übrigen UCI getrennt.

---

[1] rfc3986 (ietf.org)

[2] Felder wie Geschlecht, Chargen-/Losnummer, Impfzentrum, Identifizierungsdaten der Gesundheitsfachkraft, nächster Impftermin werden eventuell nur zu medizinischen Zwecken benötigt.

[3] 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.

[4] Der Luhn-Mod-N-Algorithmus ist eine Erweiterung des Luhn-Algorithmus (auch als „Modulo-10-Algorithmus“ bezeichnet), der für numerische Schlüssel 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.

Die Rückwärts-Kompatibilität sollte sichergestellt werden: Die Mitgliedstaaten, die im Laufe 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.

4. **UCI-Optionen bei Impfzertifikaten**

Die EHN-Leitlinien zu überprüfbaren Impfzertifikaten und grundlegenden Elementen der Interoperabilität ([5]) 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.

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

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
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

Begriff	Begriffsbestimmung
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.

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.

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.

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.

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.

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.

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 Back-up-Algorithmus

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

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 ([3]) enthalten.

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)

([3]) rfc5280 (ietf.org)

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 ([4])) 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.

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)

([4]) rfc5280 (ietf.org)

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** ([5])**, 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)

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.

([5]) 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.