UITVOERINGSBESLUIT (EU) 2021/1073 VAN DE COMMISSIE

van 28 juni 2021

tot vaststelling van technische specificaties en regels voor de uitvoering van het bij Verordening (EU) 2021/953 van het Europees Parlement en de Raad vastgestelde vertrouwenskader voor het digitaal EU-covidcertificaat

(Voor de EER relevante tekst)

DE EUROPESE COMMISSIE,

Gezien het Verdrag betreffende de werking van de Europese Unie,

Gezien Verordening (EU) 2021/953 van het Europees Parlement en de Raad van 14 juni 2021 betreffende een kader voor de afgifte, verificatie en aanvaarding van interoperabele COVID-19-vaccinatie-, test- en herstelcertificaten (digitaal EU-covidcertificaat) teneinde het vrije verkeer tijdens de COVID-19-pandemie te faciliteren ([1]), en met name artikel 9, leden 1 en 3,

Overwegende hetgeen volgt:

(1) Het bij Verordening (EU) 2021/953 vastgestelde digitale EU-covidcertificaat moet als bewijs dienen dat een persoon gevaccineerd is tegen COVID-19, negatief is getest of van COVID-19 is hersteld.

(2) Om ervoor te zorgen dat het digitale EU-covidcertificaat in de hele Unie kan worden gebruikt, moeten technische specificaties en regels worden vastgesteld voor het invullen, beveiligd afgeven en verifiëren van de digitale covidcertificaten, de beveiliging van de persoonsgegevens, het vaststellen van de gemeenschappelijke structuur van de unieke certificeringsidentificatiecode en de afgifte van een geldige, beveiligde en interoperabele barcode. Dit vertrouwenskader vormt ook de basis voor het streven naar interoperabiliteit met internationale normen en technologische systemen en zou in die zin als voorbeeld kunnen dienen voor samenwerking op mondiaal niveau.

(3) Om het digitale EU-covidcertificaat te kunnen lezen en interpreteren is er een gemeenschappelijke datastructuur nodig en moet er overeenstemming zijn over de beoogde betekenis van elk dataveld van de payload en de mogelijke waarden ervan. Om die interoperabiliteit te bevorderen, moet voor het kader van het digitale EU-covidcertificaat een gemeenschappelijke gecoördineerde datastructuur worden vastgesteld. De richtsnoeren voor dit kader zijn ontwikkeld door het bij Richtlijn 2011/24/EU van het Europees Parlement en de Raad ([2]) opgerichte e-gezondheidsnetwerk. Met deze richtsnoeren moet rekening worden gehouden bij de vaststelling van de technische specificaties inzake het formaat en het vertrouwensbeheer van het digitale EU-covidcertificaat. De datastructuur en coderingsmechanismen moeten worden gespecificeerd, evenals een transportcoderingsmechanisme in een machineleesbaar optisch formaat (QR), dat op het scherm van een mobiel apparaat kan worden weergegeven of op papier kan worden afgedrukt.

(4) Naast de technische specificaties inzake het formaat en het vertrouwensbeheer van het digitale EU-covidcertificaat moeten algemene regels voor het invullen van de certificaten worden vastgesteld zodat deze kunnen worden gebruikt voor gecodeerde waarden in de inhoud van het digitale EU-covidcertificaat. De waardereeksen waarmee die regels ten uitvoer worden gelegd, moeten regelmatig door de Commissie worden bijgewerkt en bekendgemaakt, op basis van de desbetreffende werkzaamheden van het e-gezondheidsnetwerk.

(5) Overeenkomstig Verordening (EU) 2021/953 moeten echte certificaten die het digitaal EU-covidcertificaat vormen, individueel identificeerbaar zijn door middel van een unieke certificaatidentificatiecode, aangezien het mogelijk is dat burgers meer dan één certificaat krijgen zolang Verordening (EU) 2021/953 van kracht blijft. De unieke certificaatidentificatiecode moet bestaan uit een alfanumerieke reeks en de lidstaten moeten ervoor zorgen dat die identificatiecode geen gegevens bevat waarmee een verband met andere documenten of identificatiemiddelen, zoals paspoort- of identiteitskaartnummers, kan worden gelegd, om te voorkomen dat de houder kan worden geïdentificeerd. Om ervoor te zorgen dat de certificaatidentificatiecode uniek is, moeten technische specificaties en regels voor de gemeenschappelijke structuur ervan worden vastgesteld.

([1]) PB L 211 van 15.6.2021, blz. 1.

([2]) Richtlijn 2011/24/EU van het Europees Parlement en de Raad van 9 maart 2011 betreffende de toepassing van de rechten van patiënten bij grensoverschrijdende gezondheidszorg (PB L 88 van 4.4.2011, blz. 45).

(6) De beveiliging, echtheid, geldigheid en integriteit van de certificaten die het digitaal EU-covidcertificaat vormen, alsmede de conformiteit ervan met de gegevensbeschermingswetgeving van de Unie, zijn van essentieel belang voor de aanvaarding ervan in alle lidstaten. Die doelstellingen worden bereikt door middel van het vertrouwenskader waarin de regels en infrastructuur voor de betrouwbare en beveiligde afgifte en verificatie van de digitale EU-covidcertificaten zijn vastgelegd. Het vertrouwenskader moet onder meer gebaseerd zijn op een publiekesleutelinfrastructuur met een vertrouwensketen van de gezondheidsautoriteiten of andere vertrouwensautoriteiten van de lidstaten tot de afzonderlijke entiteiten die de digitale EU-covidcertificaten afgeven. Om EU-brede interoperabiliteit te waarborgen, heeft de Commissie daarom een centraal systeem opgezet — de gateway voor digitale EU-covidcertificaten (hierna "gateway" genoemd) — waarin publieke sleutels worden opgeslagen die voor verificatie worden gebruikt. Wanneer het QR-codecertificaat wordt gescand, wordt de digitale handtekening geverifieerd met behulp van de betrokken publieke sleutel die eerder in die centrale gateway is opgeslagen. Er kunnen digitale handtekeningen worden gebruikt om de integriteit en authenticiteit van de gegevens te waarborgen. Publiekesleutelinfrastructuren (PKI's) zorgen voor vertrouwen omdat ze publieke sleutels verbinden met afgevers van certificaten. In de gateway worden meerdere PKI-certificaten gebruikt om de echtheid te verifiëren. Om tussen de lidstaten een veilige uitwisseling van data voor publiekesleutelmateriaal te waarborgen en brede interoperabiliteit mogelijk te maken, moet worden vastgelegd welke publiekesleutelcertificaten kunnen worden gebruikt en hoe deze moeten worden gegenereerd.

(7) Dit besluit maakt het mogelijk om aan de eisen van Verordening (EU) 2021/953 te voldoen op een manier die de verwerking van persoonsgegevens beperkt tot wat nodig is om het digitale EU-covidcertificaat operationeel te maken en die ertoe bijdraagt dat de finale verwerkingsverantwoordelijken het beginsel van gegevensbescherming door ontwerp eerbiedigen.

(8) Overeenkomstig Verordening (EU) 2021/953 zijn de autoriteiten of andere aangewezen instanties die verantwoordelijk zijn voor de afgifte van de certificaten, verwerkingsverantwoordelijken in de zin van artikel 4, punt 7, van Verordening (EU) 2016/679 van het Europees Parlement en de Raad ([3]) wanneer zij tijdens het afgifteproces persoonsgegevens verwerken. Afhankelijk van de wijze waarop de lidstaten het afgifteproces organiseren, kunnen er één of meer autoriteiten of aangewezen instanties zijn, bijvoorbeeld regionale gezondheidsdiensten. Overeenkomstig het subsidiariteitsbeginsel wordt die keuze overgelaten aan de lidstaten. Het zijn dan ook de lidstaten die het best in staat zijn om, wanneer er meerdere autoriteiten of andere aangewezen instanties zijn, hun respectieve verantwoordelijkheden duidelijk toe te wijzen, ongeacht of zij afzonderlijke of gezamenlijke verwerkingsverantwoordelijken zijn (zoals regionale gezondheidsdiensten die een gemeenschappelijk patiëntenportaal voor de afgifte van de certificaten opzetten). Wat betreft de verificatie van certificaten door de bevoegde autoriteiten van de lidstaat van bestemming of doorreis, of door de exploitanten van grensoverschrijdende personenvervoersdiensten die krachtens het nationale recht verplicht zijn om tijdens de COVID-19-pandemie bepaalde volksgezondheidsmaatregelen toe te passen, moeten ook deze verificateurs voldoen aan hun verplichtingen uit hoofde van de gegevensbeschermingsregels.

(9) Er worden geen persoonsgegevens verwerkt via de gateway voor digitale EU-covidcertificaten, aangezien de gateway alleen de publieke sleutels van de ondertekenende autoriteiten bevat. Die sleutels hebben betrekking op de ondertekenende autoriteiten en maken het niet mogelijk natuurlijke personen aan wie een certificaat is afgegeven, direct of indirect te heridentificeren. In haar rol als beheerder van de gateway zou de Commissie dus geen verwerkingsverantwoordelijke en evenmin een verwerker van persoonsgegevens zijn.

(10) De Europese Toezichthouder voor gegevensbescherming is geraadpleegd overeenkomstig artikel 42, lid 1, van Verordening (EU) 2018/1725 van het Europees Parlement en de Raad ([4]) en heeft op 22 juni 2021 een advies uitgebracht.

(11) Aangezien technische specificaties en regels noodzakelijk zijn voor de toepassing van Verordening (EU) 2021/953 met ingang van 1 juli 2021, is de onmiddellijke toepassing van dit besluit gerechtvaardigd.

(12) Omdat een snelle invoering van het digitale EU-covidcertificaat noodzakelijk is, moet dit besluit dus in werking treden op de dag van de bekendmaking ervan,

([3]) Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming) (PB L 119 van 4.5.2016, blz. 1).

([4]) Verordening (EU) 2018/1725 van het Europees Parlement en de Raad van 23 oktober 2018 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door de instellingen, organen en instanties van de Unie en betreffende het vrije verkeer van die gegevens, en tot intrekking van Verordening (EG) nr. 45/2001 en Besluit nr. 1247/2002/EG (PB L 295 van 21.11.2018, blz. 39).

HEEFT HET VOLGENDE BESLUIT VASTGESTELD:

Artikel 1

De technische specificaties voor het digitale EU-covidcertificaat, waarin de algemene datastructuur, de coderingsmechanismen en het transportcoderingsmechanisme in een machineleesbaar optisch formaat worden vastgesteld, zijn opgenomen in bijlage I.

Artikel 2

De regels voor het invullen van de in artikel 3, lid 1, van Verordening (EU) 2021/953 bedoelde certificaten zijn opgenomen in bijlage II bij dit besluit.

Artikel 3

De eisen inzake de gemeenschappelijke structuur van de unieke certificaatidentificatiecode zijn opgenomen in bijlage III.

Artikel 4

De governanceregels voor publiekesleutelcertificaten met betrekking tot de gateway voor digitale EU-covidcertificaten ter ondersteuning van de interoperabiliteitsaspecten van het vertrouwenskader, zijn opgenomen in bijlage IV.

Dit besluit treedt in werking op de dag van de bekendmaking ervan in het *Publicatieblad van de Europese Unie*.

Gedaan te Brussel, 28 juni 2021.

Voor de Commissie
De voorzitter
Ursula VON DER LEYEN

BIJLAGE I

FORMAAT EN VERTROUWENSBEHEER

Algemene datastructuur, coderingsmechanismen en transportcoderingsmechanisme in een machineleesbaar optisch formaat (hierna "QR" genoemd)

1. Inleiding

De technische specificaties in deze bijlage omvatten een algemene datastructuur en coderingsmechanismen voor het digitale EU-covidcertificaat (hierna "DCC" genoemd). Zij hebben ook betrekking op een transportcoderingsmechanisme in een machineleesbaar optisch formaat ("QR"), dat op het scherm van een mobiel apparaat kan worden weergegeven of dat kan worden afgedrukt. De containerindelingen van het elektronisch gezondheidscertificaat zijn in deze specificaties generiek, maar worden in dit verband gebruikt om de DCC te dragen.

2. Terminologie

Voor de toepassing van deze bijlage staat "afgevers" voor organisaties die deze specificaties gebruiken voor de afgifte van gezondheidscertificaten en "verificateurs" voor organisaties die gezondheidscertificaten als bewijs van de gezondheidsstatus aanvaarden. "Deelnemers" zijn afgevers en verificateurs. Sommige aspecten van deze bijlage moeten worden gecoördineerd tussen de deelnemers, zoals het beheer van een naamruimte en de verdeling van cryptografische sleutels. Aangenomen wordt dat een partij, hierna "secretariaat" genoemd, deze taken uitvoert.

3. Containerindeling van het elektronisch gezondheidscertificaat

De containerindeling van het elektronisch gezondheidscertificaat (*Electronic Health Certificate Container Format*, hierna "HCERT" genoemd) is ontworpen als een uniform en gestandaardiseerd vehikel voor gezondheidscertificaten van verschillende afgevers ("afgevers"). Het doel van deze specificaties is de wijze waarop deze gezondheidscertificaten worden weergegeven, gecodeerd en ondertekend te harmoniseren en daardoor de interoperabiliteit te bevorderen.

Om een door eender welke afgever afgegeven DCC te kunnen lezen en interpreteren, is er een gemeenschappelijke datastructuur nodig en moet er overeenstemming zijn over de betekenis van elk dataveld van de payload. Met het oog op die interoperabiliteit wordt een gemeenschappelijke gecoördineerde datastructuur gedefinieerd aan de hand van een "JSON"-schema dat het kader van het DCC vormt.

3.1. *Structuur van de payload*

De payload is gestructureerd en gecodeerd als een CBOR met een digitale COSE-handtekening. Dit staat algemeen bekend als een "CBOR Web Token" (CWT) en wordt gedefinieerd in RFC 8392 ([1]). De payload, zoals gedefinieerd in de volgende onderdelen, wordt getransporteerd in een hcert-claim.

De integriteit en authenticiteit van de herkomst van de payloaddata moeten door de verificateur kunnen worden geverifieerd. Om dit mechanisme mogelijk te maken, moet de afgever het CWT ondertekenen met behulp van een asymmetrische methode voor elektronische handtekeningen zoals gedefinieerd in de COSE-specificering (RFC 8152 ([2])).

3.2. *CWT-claims*

3.2.1. Overzicht van de CWT-structuur

Beschermde header

— Algoritme Handtekening (alg, label 1)

— Sleutelidentificatiecode (kid, label 4)

Payload

— Afgever (iss, claim key 1, facultatief, ISO 3166-1 alpha-2 van afgever)

— Afgegeven op (iat, claim key 6)

— Vervaltijd (exp, claim key 4)

— Gezondheidscertificaat (hcert, claim key -260)

— Digitaal EU-covidcertificaat v1 (eu_DCC_v1, claim key 1)

Handtekening

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

3.2.2. Algoritme van de handtekening

De parameter "Algoritme Handtekening" (alg) geeft aan welk algoritme wordt gebruikt voor het aanmaken van de handtekening. Het moet voldoen aan of verder gaan dan de huidige, hieronder samengevatte SOG-IS-richtsnoeren.

Er worden een primair en een secundair algoritme bepaald. Het secundaire algoritme mag alleen worden gebruikt als het primaire algoritme niet aanvaardbaar is binnen de aan de afgever opgelegde regels en voorschriften.

Om de beveiliging van het systeem te waarborgen, moeten alle implementaties het secundaire algoritme omvatten. Om deze reden moeten zowel het primaire als het secundaire algoritme worden toegepast.

De door SOG-IS vastgestelde niveaus voor de primaire en secundaire algoritmen zijn:

— Primair algoritme: Het primaire algoritme is een elliptische krommealgoritme voor digitale handtekening (ECDSA), zoals gedefinieerd in (ISO/IEC 14888—3:2006) deel 2.3, waarbij gebruik wordt gemaakt van de P-256-parameters zoals gedefinieerd in aanhangsel D (D.1.2.3) bij (FIPS PUB 186-4) in combinatie met het SHA-256-hash-algoritme zoals gedefinieerd in (ISO/IEC 10118—3:2004) functie 4.

Dit komt overeen met COSE-algoritmeparameter ES256.

— Secundair algoritme: Het secundaire algoritme is RSASSA-PSS zoals gedefinieerd in (RFC 8230 ([3])) met een modulus van 2048 bits in combinatie met het SHA-256-hash-algoritme zoals gedefinieerd in (ISO/IEC 10118—3:2004) functie 4.

Dit komt overeen met COSE-algoritmeparameter PS256.

3.2.3. Sleutelidentificatiecode

De claim "sleutelidentificatiecode" (kid) vermeldt in welk documentondertekenaarscertificaat ("Document Signer Certificate" of "DSC") de publieke sleutel zit die de verificateur moet gebruiken om de juistheid van de digitale handtekening te controleren. Het beheer van publiekesleutelcertificaten, met inbegrip van eisen inzake DSC's, wordt beschreven in bijlage IV.

De claim "sleutelidentificatiecode" (kid) wordt door verificateurs gebruikt om de juiste publieke sleutel te selecteren uit een lijst van sleutels met betrekking tot de afgever die wordt vermeld in de claim afgever (iss). Verschillende sleutels kunnen om administratieve redenen en bij het uitvoeren van sleutelrollovers parallel worden gebruikt door een afgever. De sleutelidentificatiecode is geen beveiligingskritiek veld. Om die reden kan het, indien nodig, ook in een onbeschermde header worden geplaatst. Verificateurs moeten beide opties aanvaarden. Indien beide opties voorhanden zijn, moet de sleutelidentificatiecode in de beschermde header worden gebruikt.

Door de verkorting van de identificatiecode (omdat de ruimte beperkt is) is er een kleine maar niet onbestaande kans dat de algemene lijst van DSC's die door een verificateur worden aanvaard, DSC's met dubbele kid's bevat. Daarom moet een verificateur alle DSC's met die kid controleren.

3.2.4. Afgever

De claim "afgever" (iss) is een tekenreekswaarde die eventueel de ISO 3166-1 alpha-2-landcode kan bevatten van de entiteit die het gezondheidscertificaat afgeeft. Deze claim kan door een verificateur worden gebruikt om te bepalen welke reeks DSC's moet worden gebruikt voor verificatie. De claim Key 1 wordt gebruikt om deze claim te identificeren.

3.2.5. Vervaltijd

De claim "vervaltijd" (exp) bevat een tijdstempel in het NumericDate-formaat in gehele getallen (zoals gespecificeerd in RFC 8392 ([4]), deel 2), waarin wordt aangegeven tot wanneer deze specifieke handtekening voor de payload als geldig wordt beschouwd, waarna een verificateur de payload moet afwijzen omdat deze verlopen is. De parameter "vervaltijd" heeft tot doel de geldigheidstermijn van het gezondheidscertificaat te beperken. De claim Key 4 wordt gebruikt om deze claim te identificeren.

De vervaltijd mag niet langer zijn dan de geldigheidstermijn van het DSC.

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

3.2.6. Afgegeven op

De claim “afgegeven op” (iat) bevat een tijdstempel in het NumericDate-formaat in gehele getallen (zoals gespecificeerd in RFC 8392 ([5]), deel 2), met vermelding van het tijdstip waarop het gezondheidscertificaat is aangemaakt.

De datum in het veld “afgegeven op” mag niet vallen vóór de geldigheidstermijn van het DSC.

Verificateurs kunnen aanvullende beleidslijnen toepassen om de geldigheid van het gezondheidscertificaat te beperken op basis van het tijdstip van afgifte. De claim Key 6 wordt gebruikt om deze claim te identificeren.

3.2.7. Claim “gezondheidscertificaat”

De claim “gezondheidscertificaat” (hcert) is een JSON-object (RFC 7159 ([6])) dat de informatie over de gezondheidsstatus omvat. Er kunnen verschillende soorten gezondheidscertificaten bestaan onder dezelfde claim, waarvan de DCC er één is.

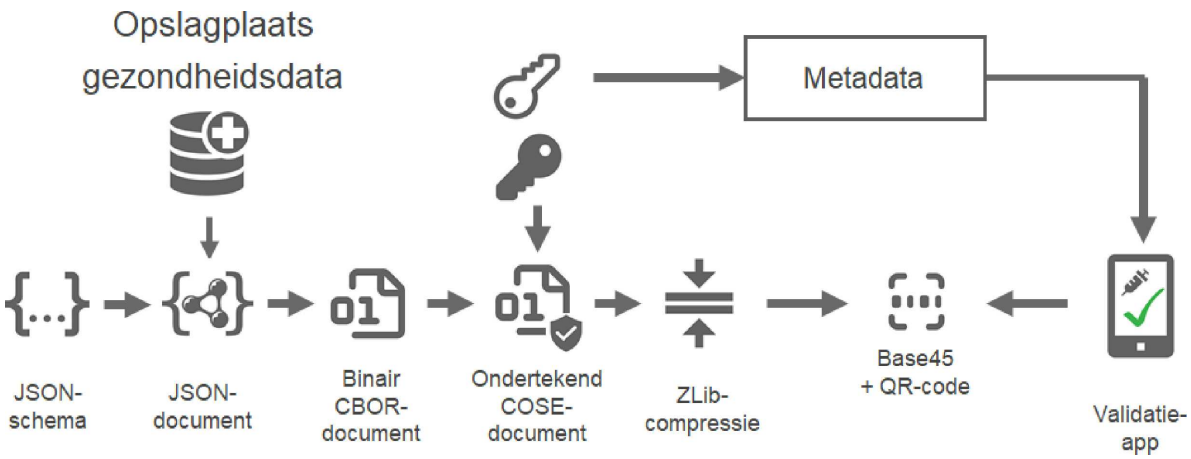
De JSON is uitsluitend bedoeld voor schematische doeleinden. Het weergaveformaat is CBOR, zoals gedefinieerd in (RFC 7049 ([7])). Applicatieontwikkelaars mogen in feite nooit het JSON-formaat decoderen of coderen naar en van het JSON-formaat, maar moeten de structuur in het geheugen gebruiken.

De te gebruiken Claim Key voor identificatie van deze claim is -260.

De strings in het JSON-object moeten worden genormaliseerd volgens Normalization Form Canonical Composition (NFC) zoals gedefinieerd in de Unicode-norm. Decodeertoepassingen moeten in deze opzichten echter ruim en robuust zijn, en de aanvaarding van elke redelijke omzetting wordt nadrukkelijk aangemoedigd. Indien tijdens het decoderen, of in latere vergelijkingsfuncties, niet-genormaliseerde data worden gevonden, moeten de implementaties zich gedragen alsof de input genormaliseerd is naar NFC.

4. Serialisatie en creatie van de DCC-payload

Als serialisatiepatroon wordt het volgende schema gebruikt:



Het proces begint met het extraheren van data, bijvoorbeeld uit een opslagplaats voor gezondheidsdata (of een externe gegevensbron), waarbij de geëxtraheerde data worden gestructureerd volgens de gedefinieerde DCC-schema’s. In dit proces kunnen de omzetting naar het gedefinieerde dataformaat en de transformatie met het oog op menselijke leesbaarheid plaatsvinden voordat de serialisatie naar CBOR begint. De acroniemen van de claims worden in elk geval vóór serialisatie en na deserialisatie toegewezen aan de weergavenamen.

Facultatieve nationale data-inhoud is niet toegestaan in certificaten die zijn afgegeven op grond van Verordening (EU) 2021/953 ([8]). De data-inhoud is beperkt tot de gedefinieerde data-elementen in de minimale dataset zoals gespecificeerd in de bijlage bij Verordening (EU) 2021/953.

([5]) rfc8392 (ietf.org)
([6]) rfc7159 (ietf.org)
([7]) rfc7049 (ietf.org)
([8]) Verordening (EU) 2021/953 van het Europees Parlement en de Raad van 14 juni 2021 betreffende een kader voor de afgifte, verificatie en aanvaarding van interoperabele COVID-19-vaccinatie-, test- en herstelcertificaten (digitaal EU-COVID-certificaat) teneinde het vrije verkeer tijdens de COVID-19-pandemie te faciliteren (PB L 211 van 15.6.2021, blz. 1).

5. **Transportcodering**

5.1. *Raw*

Voor arbitraire data-interfaces mogen de HCERT-container en de payloads ervan ongewijzigd worden overgedragen, met gebruikmaking van elk mogelijk onderliggend, veilig en betrouwbaar 8-bit-datatransport. Deze interfaces kunnen NFC (Near Field Communication), bluetooth of overdracht via een toepassingslaagprotocol omvatten, bijvoorbeeld de overdracht van een HCERT van de afgever naar het mobiele apparaat van de houder.

Als de overdracht van de HCERT van de afgever naar de houder gebaseerd is op een interface voor uitsluitend weergave (bijvoorbeeld sms, e-mail), is de transportcodering Raw uiteraard niet van toepassing.

5.2. *Barcode*

5.2.1. Compressie van de payload (CWT)

Om de grootte te verminderen en de snelheid en betrouwbaarheid van het leesproces van de HCERT te verbeteren, wordt de CWT gecomprimeerd met behulp van ZLIB (RFC 1950 ([9])) en het Deflate-compressiemechanisme in het formaat zoals gedefinieerd in RFC 1951 ([10]).

5.2.2. QR-2D-barcode

Om ervoor te zorgen dat beter kan worden gewerkt met oude apparatuur die is ontworpen voor ASCII-payloads, wordt de gecomprimeerde CWT gecodeerd als ASCII met gebruikmaking van Base45 alvorens te worden gecodeerd in een 2D-barcode.

Voor het genereren van de 2D-barcode wordt het QR-formaat gebruikt zoals gedefinieerd in (ISO/IEC 18004:2015). Een foutcorrectiepercentage van "Q" (ongeveer 25 %) wordt aanbevolen. Omdat gebruik wordt gemaakt van Base45, moet voor de QR-code alfanumerieke codering worden gebruikt (modus 2, aangegeven door de symbolen 0010).

Om verificateurs in staat te stellen het soort gecodeerde data te detecteren en het juiste decoderings- en verwerkingsschema te kiezen, moeten de met Base45 gecodeerde data (volgens deze specificatie) worden voorafgegaan door de Context-Identifier-string "HC1:". Bij toekomstige versies van deze specificatie die gevolgen hebben voor de compatibiliteit met oudere systemen, moet een nieuwe context-ID worden gedefinieerd, waarbij "HC" moet worden gevolgd door een teken uit de tekenset [1-9A-Z]. Deze tekens moeten in die volgorde worden bepaald, d.w.z. eerst [1-9] en vervolgens [A-Z].

Er wordt aanbevolen de optische code op het presentatiemedium weer te geven met een diagonaal tussen 35 mm en 60 mm, om het gebruik ervan te vergemakkelijken met lezers met vaste optische onderdelen indien het presentatiemedium op het oppervlak van de lezer moet worden geplaatst.

Indien de optische code op papier wordt gedrukt met behulp van printers met lage resolutie (< 300 dpi), moet erop worden gelet dat elk symbool (punt) van de QR-code precies vierkant worden weergegeven. Niet-proportionele schaalverkleining zal in sommige rijen of kolommen van de QR-code tot rechthoekige symbolen leiden, wat de leesbaarheid in veel gevallen zal bemoeilijken.

6. **Formaat van vertrouwenslijsten (CSCA- en DSC-lijst)**

Elke lidstaat moet een lijst van een of meer Country Signing Certificate Authorities (CSCA's) en een lijst van alle geldige Document Signer Certificates (DSC's) verstrekken en deze lijsten actueel houden.

6.1. *Vereenvoudigde CSCA/DSC*

Vanaf deze versie van de specificaties gaan de lidstaten er niet vanuit dat informatie uit de lijst van ingetrokken certificaten (Certificate Revocation List — CRL) is gebruikt of dat de gebruiksperiode van de persoonlijke sleutel door de uitvoerders is gecontroleerd.

Het primaire geldigheidsmechanisme is daarentegen de aanwezigheid van het certificaat op de meest recente versie van die certificaatlijst.

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

6.2. *eMRTD-PKI van de ICAO en trustcentra*

De lidstaten kunnen een afzonderlijke CSCA gebruiken, maar kunnen ook hun bestaande CSCA-certificaten en/of DSC's voor eMRTD indienen, en kunnen er zelfs voor kiezen deze in te kopen bij (commerciële) trustcentra en die vervolgens in te dienen. Een DSC moet echter altijd worden ondertekend door de CSCA die door die lidstaat is aangewezen.

7. **Beveiligingsoverwegingen**

Bij het ontwerpen van een regeling aan de hand van deze specificatie bepalen, analyseren en monitoren de lidstaten bepaalde beveiligingsaspecten.

Ten minste met de volgende aspecten moet rekening worden gehouden:

7.1. *Geldigheidstermijn HCERT-handtekening*

De uitgever van HCERT's moet de geldigheidsduur van de handtekening beperken door een termijn voor het verstrijken van de handtekening te specificeren. Dit houdt in dat de houder van een gezondheidscertificaat het periodiek moet vernieuwen.

De aanvaardbare geldigheidsduur kan worden bepaald op basis van praktische beperkingen. Een reiziger heeft bijvoorbeeld niet de mogelijkheid om het gezondheidscertificaat tijdens een buitenlandse reis te verlengen. Het is echter ook mogelijk dat een afgever het mogelijk acht dat de beveiliging op een of andere manier is gecompromitteerd, waardoor de afgever een DSC moet intrekken (waardoor alle gezondheidscertificaten die zijn afgegeven met gebruikmaking van de sleutel die nog binnen de geldigheidsperiode valt, ongeldig worden verklaard). De gevolgen van een dergelijke gebeurtenis kunnen worden beperkt door de sleutels van de afgever regelmatig te vernieuwen en met redelijke intervallen de vernieuwing van alle gezondheidscertificaten te eisen.

7.2. *Sleutelbeheer*

Deze specificatie is sterk afhankelijk van sterke cryptografische mechanismen om de integriteit van data en de authenticatie van de oorsprong van de data te beveiligen. Daarom is het noodzakelijk de vertrouwelijkheid van de persoonlijke sleutels te waarborgen.

De vertrouwelijkheid van cryptografische sleutels kan op verschillende manieren in het gedrang komen. Enkele voorbeelden:

— Het proces waarbij de sleutel wordt aangemaakt, kan gebreken vertonen, wat leidt tot zwakke sleutels.

— De sleutels kunnen worden onthuld door menselijke fouten.

— De sleutels kunnen worden gestolen door externe of interne daders.

— De sleutels kunnen worden berekend aan de hand van cryptoanalyse.

Om het risico op een zwak ondertekeningsalgoritme te beperken, waardoor de persoonlijke sleutels kunnen worden gecompromitteerd door cryptoanalyse, wordt met deze specificatie aanbevolen dat alle deelnemers voor noodgevallen een secundair ondertekeningsalgoritme toepassen op basis van andere parameters of een ander wiskundig probleem dan het primaire.

Wat de vermelde risico's in verband met de besturingsomgevingen van de afgevers betreft, moeten risicobeperkende maatregelen worden genomen om een doeltreffende controle te waarborgen, zodat de persoonlijke sleutels worden gegenereerd, opgeslagen en gebruikt in HSM's (Hardware Security Modules). Het gebruik van HSM's voor het ondertekenen van gezondheidscertificaten wordt nadrukkelijk aangemoedigd.

Ongeacht of een afgever besluit HSM's te gebruiken of niet, moet een schema voor sleutelrollovers worden vastgesteld waarbij de frequentie van de sleutelrollovers in verhouding staat tot de blootstelling van de sleutels aan externe netwerken, andere systemen en personeel. Een goed gekozen rolloverschema beperkt ook de risico's in verband met ten onrechte afgegeven gezondheidscertificaten, waardoor een afgever dergelijke gezondheidscertificaten in batches kan intrekken door zo nodig een sleutel in te trekken.

7.3. *Validatie van inputdata*

Deze specificaties kunnen worden gebruikt op een manier die inhoudt dat data van onbetrouwbare bronnen worden ontvangen in systemen die van missiekritische aard kunnen zijn. Om de risico's in verband met deze aanvalsvector tot een minimum te beperken, moeten alle inputvelden naar behoren worden gevalideerd op basis van datatypes, -lengtes en -inhoud. De handtekening van de afgever wordt ook geverifieerd voordat de inhoud van het HCERT wordt verwerkt. De validatie van de handtekening van de afgever houdt echter in dat eerst de beschermde header van de afgever wordt geparseerd, waarbij een potentiële aanvaller kan proberen zorgvuldig gefabriceerde informatie in te voeren die bedoeld is om de beveiliging van het systeem in gevaar te brengen.

8. **Vertrouwensbeheer**

Om de HCERT-handtekening te verifiëren, is een publieke sleutel nodig. De lidstaten maken deze publieke sleutels bekend. Uiteindelijk moet elke verificateur beschikken over een lijst van alle publieke sleutels die hij bereid is te vertrouwen (aangezien de publieke sleutel geen deel uitmaakt van het HCERT).

Het systeem bestaat uit (slechts) twee lagen; voor elke lidstaat een of meer landencertificaten waarmee telkens een of meer DSC's worden ondertekend die dagelijks worden gebruikt.

De certificaten van de lidstaten worden CSCA's genoemd (Country Signing Certificate Authority) en zijn (doorgaans) zelfondertekend. De lidstaten kunnen er meer dan één hebben (bijvoorbeeld in het geval van regionale decentralisatie). Deze CSCA-certificaten ondertekenen regelmatig de DSC's (Document Signer Certificates) die worden gebruikt voor het ondertekenen van HCERT's.

Het "secretariaat" is een functionele rol. Het verzamelt en publiceert de DSC's van de lidstaten op regelmatige tijdstippen, nadat het deze heeft geverifieerd aan de hand van de lijst van CSCA-certificaten (die met andere middelen zijn overgedragen en geverifieerd).

De daaruit voortvloeiende lijst van DSC's bevat dan de geaggregeerde reeks aanvaardbare publieke sleutels (en de bijbehorende sleutelidentificatiecodes) die verificateurs kunnen gebruiken om de handtekeningen via de HCERT's te valideren. Verificateurs moeten deze lijst regelmatig ophalen en actualiseren.

Dergelijke lidstaatspecifieke lijsten kunnen worden omgezet in het door de lidstaat vastgestelde formaat. Het bestandsformaat van deze vertrouwenslijst kan dus variëren: het kan een ondertekend JWKS zijn (JWK-setindeling volgens RFC 7517 ([11]), deel 5) of een ander formaat dat specifiek is voor de in die lidstaat gebruikte technologie.

Ter wille van de eenvoud kunnen de lidstaten zowel hun bestaande CSCA-certificaten van hun eMRTD-systemen van de ICAO indienen of, zoals aanbevolen door de WHO, een specifiek certificaat voor dit gezondheidsgebied creëren.

8.1. *De sleutelidentificatiecode*

De sleutelidentificatiecode ("key identifier" of "kid") wordt berekend bij het samenstellen van de lijst van betrouwbare publieke sleutels van DSC's en bestaat uit een afgekapte (eerste 8 bytes) SHA-256-vingerafdruk van het DSC die is gecodeerd in het DER-formaat (raw).

Verificateurs hoeven de sleutelidentificatiecode niet te berekenen op basis van het DSC en kunnen de sleutelidentificatiecode in het afgegeven gezondheidscertificaat direct matchen met de sleutelidentificatiecode op de vertrouwenslijst.

8.2. *Verschillen met het eMRTD-PKI-vertrouwensmodel van de ICAO*

Hoewel er wordt voortgebouwd op beste praktijken van het eMRTD-PKI-vertrouwensmodel van de ICAO, wordt in het belang van de snelheid een aantal vereenvoudigingen aangebracht:

— Een lidstaat kan meerdere CSCA-certificaten indienen.

— De geldigheidstermijn van het DSC (sleutelgebruik) kan eender welke lengte hebben, zolang deze de geldigheidstermijn van het CSCA-certificaat niet overschrijdt, en mag ontbreken.

— Het DSC mag beleidsidentificatiecodes (uitgebreide-sleutelgebruik) bevatten die specifiek zijn voor gezondheidscertificaten.

— De lidstaten kunnen ervoor kiezen gepubliceerde intrekkingen nooit te verifiëren, maar uitsluitend gebruik te maken van de DSC-lijsten die zij dagelijks van het secretariaat ontvangen of zelf samenstellen.

([11]) rfc7517 (ietf.org)

BIJLAGE II

REGELS VOOR HET INVULLEN VAN HET DIGITALE EU-COVIDCERTIFICAAT

De algemene regels betreffende de in deze bijlage vastgestelde waardereeksen zijn bedoeld om interoperabiliteit op semantisch niveau te waarborgen en moeten uniforme technische implementaties voor het DCC mogelijk maken. De elementen in deze bijlage mogen worden gebruikt voor de drie verschillende certificaten (vaccinatie/test/herstel), zoals vermeld in Verordening (EU) 2021/953. In deze bijlage worden alleen elementen vermeld waarvoor semantische standaardisering door middel van gecodeerde waardereeksen noodzakelijk is.

Voor de vertaling van de gecodeerde elementen in de nationale taal valt zijn de lidstaten verantwoordelijk.

Voor alle datavelden die niet in de volgende omschrijvingen van waardereeksen worden vermeld, wordt codering in UTF-8 aanbevolen (naam, testcentrum, certificaatafgever). Voor datavelden met kalenderdata (geboortedatum, vaccinatiedatum, datum van monsterneming, datum van eerste positieve testresultaat, geldigheidstermijn van het certificaat) wordt codering volgens ISO 8601 aanbevolen.

Indien om welke reden dan ook de hieronder vermelde voorkeurscodesystemen niet kunnen worden gebruikt, mogen andere internationale codesystemen worden gebruikt en moet advies worden gegeven over de wijze waarop de codes van het andere codesysteem aan het voorkeurscodesysteem kunnen worden gekoppeld. In uitzonderlijke gevallen mag als back-upmechanisme tekst (weergavenamen) worden gebruikt wanneer in de gedefinieerde waardereeksen geen geschikte code beschikbaar is.

Lidstaten die andere coderingen in hun systemen gebruiken, moeten deze codes koppelen aan de beschreven waardereeksen. De lidstaten zijn verantwoordelijk voor dergelijke koppelingen.

De waardereeksen worden regelmatig door de Commissie bijgewerkt met de steun van het e-gezondheidsnetwerk en het Gezondheidsbeveiligingscomité. De bijgewerkte waardereeksen worden gepubliceerd op de desbetreffende website van de Commissie en op de webpagina van het e-gezondheidsnetwerk. Er moet een overzicht van de wijzigingen worden gegeven.

1. **Doelziekte of -ziekteverwekker/ziekte of ziekteverwekker waarvan de houder zich heeft hersteld: COVID-19 (SARS-CoV-2 of een van de varianten daarvan)**

   Voorkeurscodesysteem: SNOMED CT.

   Te gebruiken in de certificaten 1, 2 en 3

   De geselecteerde codes verwijzen naar COVID-19 of, indien meer gedetailleerde informatie over de genetische variant van SARS-CoV-2 nodig is, naar deze varianten indien die gedetailleerde informatie om epidemiologische redenen nodig is.

   Een voorbeeld van een code die moet worden gebruikt, is SNOMED CT-code 840539006 (COVID-19).

2. **COVID-19-vaccin of -profylaxe;**

   Voorkeurscodesysteem: SNOMED CT- of ATC-classificatie.

   Te gebruiken in certificaat 1.

   Voorbeelden van codes die moeten worden gebruikt uit de voorkeurscodesystemen zijn SNOMED CT-code 1119305005 (SARS-CoV-2-antigeenvaccin), 1119349007 (SARS-CoV-2-mRNA-vaccin) of J07BX03 (COVID-19-vaccins). De waardereeks moet worden uitgebreid wanneer nieuwe vaccintypes worden ontwikkeld en in gebruik worden genomen.

3. **COVID-19-vaccin**

   Voorkeurscodesystemen (in volgorde van voorkeur):

   — Het geneesmiddelenregister van de EU voor vaccins met EU-brede vergunning (vergunningsnummers)

   — Een wereldwijd vaccinregister, zoals een register dat door de Wereldgezondheidsorganisatie zou kunnen worden opgesteld

   — Naam van het vaccin in andere gevallen. Indien de naam spaties bevat, moeten deze worden vervangen door een koppelteken (-).

Naam van de waardereeks: vaccin.

Te gebruiken in certificaat 1.

Een voorbeeld van een code uit de voorkeurscodesystemen die moet worden gebruikt is EU/1/20/1528 (Comirnaty). Een voorbeeld van de naam van het vaccin die als code moet worden gebruikt: Sputnik-V (staat voor Sputnik V).

4. **Handelsvergunninghouder of producent van het COVID-19-vaccin**

Voorkeurscodesysteem:

— Organisatiecode van het EMA (SPOR-systeem voor ISO IDMP)

— Een wereldwijd register van handelsvergunninghouders of producenten van een vaccin, zoals een register dat door de Wereldgezondheidsorganisatie zou kunnen worden opgesteld

— Naam van de organisatie in andere gevallen. Indien de naam spaties bevat, moeten deze worden vervangen door een koppelteken (-).

Te gebruiken in certificaat 1.

Een voorbeeld van een code uit het voorkeurscodesysteem die moet worden gebruikt is ORG-100001699 (AstraZeneca AB). Een voorbeeld van de naam van de organisatie die als code moet worden gebruikt: Sinovac-Biotech (staat voor Sinovac Biotech).

5. **Volgnummer in een reeks doses alsook totale aantal doses in de reeks**

Te gebruiken in certificaat 1.

Twee velden:

1) Aantal in een cyclus toegediende dosissen

2) Aantal verwachte dosissen voor een volledige cyclus (specifiek voor een persoon op het moment van toediening)

Zo zal bij 1/1 of 2/2 de cyclus als voltooid worden voorgesteld, met inbegrip van optie 1/1 voor vaccins met twee dosissen, maar waarvoor het door de lidstaat toegepaste protocol erin bestaat één dosis toe te dienen aan burgers die met COVID-19 zijn gediagnosticeerd vóór hun vaccinatie. Het totale aantal dosissen in de cyclus moet worden aangegeven op basis van de informatie die beschikbaar is op het moment dat de dosis wordt toegediend. Als voor een specifiek vaccin bijvoorbeeld een derde prik (booster) nodig is op het moment van de laatst toegediende prik, moet dit in het tweede veldnummer worden weergegeven (bijvoorbeeld 2/3, 3/3 enz.).

6. **Lidstaat of derde land waar het vaccin werd toegediend/waar de test werd uitgevoerd**

Voorkeurscodesysteem: ISO 3166-landcodes.

Te gebruiken in de certificaten 1, 2 en 3

Inhoud van de waardereeks: de volledige lijst van 2-lettercodes, beschikbaar als een in FHIR gedefinieerde waardereeks (http://hl7.org/fhir/ValueSet/iso3166-1-2)

7. **Type test**

Voorkeurscodesysteem: LOINC.

Te gebruiken in certificaten 2 en 3 indien ondersteuning voor de afgifte van herstelcertificaten op basis van andere soorten tests dan NAAT wordt ingevoerd bij een gedelegeerde handeling.

De codes in deze waardereeks verwijzen naar de testmethode en moeten worden gekozen om ten minste de NAAT-tests te scheiden van de RAT-tests als bedoeld in Verordening (EU) 2021/953.

Een voorbeeld van een code uit het voorkeurscodesysteem die moet worden gebruikt is LP217198-3 (immunoassay-sneltest).

8. **Fabrikant en handelsnaam van de gebruikte test (facultatief voor NAAT-test)**

Voorkeurscodesysteem: Lijst van het Gezondheidsbeveiligingscomité met snelle antigeentests zoals bijgehouden door het JRC (database van middelen voor in-vitrodiagnostiek en testmethoden voor COVID-19).

Te gebruiken in certificaat 2.

De inhoud van de waardereeks omvat de selectie van snelle antigeentests zoals opgenomen in de gemeenschappelijke en geactualiseerde lijst van snelle antigeentests voor COVID-19, vastgesteld op basis van Aanbeveling 2021/C 24/01 van de Raad en goedgekeurd door het Gezondheidsbeveiligingscomité. De lijst wordt door het JRC bijgehouden in de database van middelen voor in-vitrodiagnostiek en testmethoden voor COVID-19 op: https://covid-19-diagnostics.jrc.ec.europa.eu/devices/hsc-common-recognition-rat

Voor dit codesysteem moeten relevante velden, zoals de identificatiecode van het testapparaat, de naam van de test en de fabrikant worden gebruikt volgens het gestructureerde formaat van het JRC dat beschikbaar is op https://covid-19-diagnostics.jrc.ec.europa.eu/devices.

9. **Testresultaat**

Voorkeurscodesysteem: SNOMED CT.

Te gebruiken in certificaat 2.

Aan de hand van de gekozen codes moet een onderscheid kunnen worden gemaakt tussen positieve en negatieve testresultaten (al dan niet gedetecteerd). Aanvullende waarden (bijv. onbepaald) kunnen worden toegevoegd indien de gebruiksomstandigheden dit vereisen.

Voorbeelden van codes uit de voorkeurscodesystemen die moeten worden gebruikt, zijn 260415000 (niet gedetecteerd) en 260373001 (gedetecteerd).

BIJLAGE III

GEMEENSCHAPPELIJKE STRUCTUUR VAN DE UNIEKE CERTIFICAATIDENTIFICATIECODE

1. **Inleiding**

Elk digitaal EU-covidcertificaat (DCC) bevat een unieke certificeringsidentificatiecode (UCI) ter ondersteuning van de interoperabiliteit van de DCC's. De UCI kan worden gebruikt om het certificaat te verifiëren. De lidstaten zijn verantwoordelijk voor de implementatie van de UCI. De UCI is een middel om de waarheidsgetrouwheid van het certificaat te verifiëren en, indien van toepassing, te koppelen aan een registratiesysteem (bijvoorbeeld een IIS). Op basis van deze identificatiecodes moeten de lidstaten ook (op papier en digitaal) kunnen vaststellen dat personen gevaccineerd of getest zijn.

2. **Samenstelling van de unieke certificaatidentificatiecode**

De UCI volgt een gemeenschappelijke structuur en een gemeenschappelijk formaat die de menselijke en/of machinale interpretatie van informatie vergemakkelijken en kan betrekking hebben op elementen zoals de lidstaat van vaccinatie, het vaccin zelf en een lidstaatspecifieke identificatiecode. De UCI biedt de lidstaten flexibiliteit bij het opstellen ervan, met volledige inachtneming van de wetgeving inzake gegevensbescherming. De volgorde van de afzonderlijke elementen volgt een vastgestelde hiërarchie die toekomstige wijzigingen van de blokken mogelijk maakt met behoud van de structurele integriteit ervan.

De mogelijke oplossingen voor de samenstelling van de UCI vormen een spectrum waarin de twee belangrijkste onderscheidende parameters de moduleerbaarheid en de menselijke interpreteerbaarheid zijn en er één fundamenteel kenmerk is:

— Moduleerbaarheid: de mate waarin de code is samengesteld uit afzonderlijke bouwstenen die semantisch verschillende informatie bevatten;

— Menselijke interpreteerbaarheid: de mate waarin de code betekenisvol is voor of geïnterpreteerd kan worden door de menselijke lezer;

— Wereldwijd uniek; de identificatiecode van het land of de autoriteit wordt goed beheerd; en van elk land (elke autoriteit) wordt verwacht dat het zijn segment van de namespace goed beheert door nooit identificatiecodes te hergebruiken of opnieuw af te geven. De combinatie daarvan zorgt ervoor dat elke identificatiecode wereldwijd uniek is.

3. **Algemene eisen**

Met betrekking tot de UCI moet aan de volgende overkoepelende eisen worden voldaan:

1) Tekenset: alleen US-ASCII-alfanumerieke tekens in hoofdletters ("A" tot en met "Z", "0" tot en met "9") zijn toegestaan; met extra speciale tekens voor scheiding van RFC3986 ([1]) ([2]), namelijk {"/", "#", ":"};

2) Maximumlengte: ontwerpers moeten streven naar een lengte van 27-30 tekens ([3]);

3) Versieprefix: dit verwijst naar de versie van het UCI-schema. Het versieprefix is "01" voor deze versie van het document; het versieprefix bestaat uit twee cijfers;

4) Landprefix: de landcode is gespecificeerd volgens ISO 3166-1. Langere codes (bv. 3 tekens en meer (bijvoorbeeld "UNHCR") zijn gereserveerd voor toekomstig gebruik;

5) Suffix/checksum van de code:

5.1. De lidstaten moeten een checksum gebruiken wanneer het waarschijnlijk is dat verzending, (menselijke) transcriptie of andere corrupties zich kunnen voordoen (d.w.z. bij gebruik in gedrukte vorm).

5.2. De checksum mag niet worden gebruikt voor de validatie van het certificaat en maakt technisch gezien geen deel uit van de identificatiecode, maar wordt gebruikt om de integriteit van de code te verifiëren. Deze checksum moet de samenvatting volgens ISO-7812-1 (LUHN-10) ([4]) zijn van de volledige UCI in digitaal/draadformaat. De checksum wordt van de rest van de UCI gescheiden door een #-teken.

([1]) rfc3986 (ietf.org)

([2]) Velden zoals geslacht, identificatienummer van de batch/partij, vaccinatiecentrum, identificatiecode gezondheidswerker, volgende vaccinatiedatum zijn mogelijk niet nodig voor andere doeleinden dan medisch gebruik.

([3]) Voor de implementatie met QR-codes kunnen de lidstaten overwegen een extra reeks tekens met een totale lengte van 72 tekens (met inbegrip van de 27-30 van de identificatiecode zelf) te gebruiken om andere informatie over te brengen. Het is aan de lidstaten om deze informatie nader te omschrijven.

([4]) Het "Luhn mod N"-algoritme is een uitbreiding van het Luhn-algoritme (ook bekend als het mod 10-algoritme), dat voor numerieke codes werkt en bijvoorbeeld wordt gebruikt voor de berekening van de checksum van kredietkaarten. Met de extensie kan het algoritme werken met sequenties van waarden in om het even welke basis (in dit geval alfanumerieke tekens).

Er moet worden gezorgd voor compatibiliteit met oudere systemen: lidstaten die na verloop van tijd de structuur van hun identificatiecodes wijzigen (in de hoofdversie, momenteel vastgesteld op v1), zorgen ervoor dat twee identieke identificatiecodes voor hetzelfde vaccinatiecertificaat/dezelfde verklaring staan. Of, met andere woorden, de lidstaten kunnen identificatiecodes niet hergebruiken.

4. **Opties voor unieke identificatiecodes voor vaccinatiecertificaten**

De richtsnoeren van het e-gezondheidsnetwerk inzake verifieerbare vaccinatiecertificaten en basisinteroperabiliteitselementen ([5]) biedt de lidstaten en andere partijen verschillende opties die mogelijk naast elkaar kunnen bestaan. De lidstaten kunnen dergelijke verschillende opties gebruiken in verschillende versies van het UCI-schema.

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

BIJLAGE IV

BEHEER VAN PUBLIEKESLEUTELCERTIFICATEN

1. Inleiding

De beveiligde en betrouwbare uitwisseling van handtekeningsleutels voor digitale EU-covidcertificaten (DCC's) tussen de lidstaten gebeurt via de gateway voor digitale EU-covidcertificaten (DCCG), die fungeert als centraal register voor de publieke sleutels. Met de DCCG kunnen de lidstaten de publieke sleutels publiceren die overeenkomen met de persoonlijke sleutels die zij gebruiken om digitale EU-covidcertificaten te ondertekenen. De lidstaten kunnen de DCCG gebruiken om tijdig actueel publiekesleutelmateriaal op te halen. Later kan de DCCG worden uitgebreid om betrouwbare aanvullende informatie uit te wisselen die de lidstaten verstrekken, zoals validatieregels voor DCC's. Het vertrouwensmodel van het DCC-kader is een publiekesleutelinfrastructuur (Public Key Infrastructure, PKI). Elke lidstaat heeft een of meer Country Signing Certificate Authorities (CSCA's), waarvan de certificaten relatief lang blijven bestaan. De lidstaten kunnen beslissen of de CSCA gelijk is aan of verschillend is van de CSCA die voor machineleesbare reisdocumenten wordt gebruikt. De CSCA geeft publiekesleutelcertificaten af voor de nationale, tijdelijke documentondertekenaars (d.w.z. ondertekenaars voor DCC's), die Document Signer Certificates (DSC's) worden genoemd. De CSCA fungeert als een vertrouwensanker zodat de lidstaten de CSCA kunnen gebruiken om de authenticiteit en integriteit van de regelmatig veranderende DSC's te valideren. Na validatie kunnen de lidstaten hun DCC-validatietoepassingen voorzien van deze certificaten (of alleen de daarin vervatte publieke sleutels). Naast de CSCA's en DSC's vertrouwt de DCCG ook op PKI om transacties te authenticeren, data te ondertekenen, als basis voor authenticatie en als middel om de integriteit van de communicatiekanalen tussen de lidstaten en de DCCG te waarborgen.

Digitale handtekeningen kunnen worden gebruikt voor de integriteit en authenticiteit van de gegevens. Publiekesleutelinfrastructuren zorgen voor vertrouwen omdat ze publieke sleutels koppelen aan geverifieerde afgevers. Dit is noodzakelijk om andere deelnemers in staat te stellen de herkomst van de data en de identiteit van de communicatiepartner te controleren en te beslissen of deze te vertrouwen zijn. In de DCCG worden meerdere PKI-certificaten gebruikt om de authenticiteit te verifiëren. In deze bijlage wordt bepaald welke publiekesleutelcertificaten worden gebruikt en hoe deze moeten worden ontworpen om een brede interoperabiliteit tussen de lidstaten mogelijk te maken. Deze bijlage biedt meer details over de noodzakelijke publiekesleutelcertificaten en bevat richtsnoeren over certificaatmodellen en geldigheidstermijnen voor lidstaten die hun eigen CSCA willen exploiteren. Aangezien DCC's voor een bepaald tijdsbestek verifieerbaar zijn (vanaf het moment van de afgifte tot wanneer ze na een bepaalde tijd vervallen), moet een verificatiemodel worden vastgesteld voor alle handtekeningen die op de publiekesleutelcertificaten en de DCC's worden toegepast.

2. Terminologie

De volgende tabel bevat de in deze bijlage gebruikte afkortingen en terminologie.

Begrip	Definities
Certificaat	Of publiekesleutelcertificaat. Een X.509-v3-certificaat dat de publieke sleutel van een entiteit bevat
CSCA	Country Signing Certificate Authority (nationale ondertekenende certificeringsautoriteit)
DCC	Digitaal EU-covidcertificaat Een ondertekend digitaal document met vaccinatie-, test- of herstelinformatie
DCCG	Gateway voor digitale EU-covidcertificaten. Dit systeem wordt gebruikt voor de uitwisseling van DSC's tussen de lidstaten.
$DCCG_{TA}$	Het vertrouwensankercertificaat van de DCCG. De overeenkomstige persoonlijke sleutel wordt gebruikt om de lijst van alle CSCA-certificaten offline te ondertekenen.
$DCCG_{TLS}$	Het TLS-servercertificaat van de DCCG.
DSC	Document Signer Certificate (documentondertekenaarscertificaat). Het publiekesleutelcertificaat van de lidstaatautoriteit die documenten ondertekent (bijvoorbeeld een systeem dat DCC's mag ondertekenen). Dit certificaat wordt afgegeven door de CSCA van de lidstaat.
EC-DSA	Elliptische krommealgoritme voor digitale handtekening. Een cryptografisch handtekeningalgoritme op basis van elliptische krommen
Lidstaat	Lidstaat van de Europese Unie

Begrip	Definities
mTLS	Wederzijdse TLS. Het protocol inzake beveiliging op het niveau van de vervoerslaag ("Transport Layer Security Protocol") met wederzijdse authenticatie
NB	Nationale backend van een lidstaat
NB_{CSCA}	Het CSCA-certificaat van een lidstaat (kan meer dan één zijn)
NB_{TLS}	Het TLS-cliëntauthenticatiecertificaat van een nationaal backend
NB_{UP}	Het certificaat dat een nationale backend gebruikt om naar de DCCG geüploade datapakketten te ondertekenen
PKI	Publiekesleutelinfrastructuur. Vertrouwensmodel op basis van publiekesleutelcertificaten en certificeringsautoriteiten
RSA	Asymmetrisch cryptografisch algoritme op basis van ontbinding in gehele getallen dat wordt gebruikt voor digitale handtekeningen of asymmetrische versleuteling

3. **DCCG-communicatiestromen en -beveiligingsdiensten**

In dit deel wordt een overzicht gegeven van de communicatiestromen en beveiligingsdiensten in het DCCG-systeem. Hier wordt ook bepaald welke sleutels en certificaten worden gebruikt om de communicatie, de geüploade informatie, de DCC's en een ondertekende vertrouwenslijst met alle geïntroduceerde CSCA-certificaten te beschermen. De DCCG fungeert als dataknooppunt dat de uitwisseling van ondertekende datapakketten door de lidstaten mogelijk maakt.

Geüploade datapakketten worden ongewijzigd door de DCCG verstrekt, wat betekent dat de DCCG geen DSC's toevoegt of verwijdert uit de pakketten die hij ontvangt. De nationale backend (NB) van de lidstaten wordt in staat gesteld de integriteit en authenticiteit van de geüploade gegevens end-to-end te verifiëren. Daarnaast zullen nationale backends en de DCCG gebruikmaken van wederzijdse TLS-authenticatie om een beveiligde verbinding tot stand te brengen. Dit komt bovenop de handtekeningen in de uitgewisselde data.

3.1. *Authenticatie en maken van verbinding*

De DCCG maakt gebruik van Transport Layer Security (TLS) met wederzijdse authenticatie om een geauthenticeerd versleuteld kanaal tot stand te brengen tussen de nationale backend (NB) van de lidstaat en de gatewayomgeving. De DCCG beschikt derhalve over een TLS-servercertificaat, afgekort $DCCG_{TLS}$, en de nationale backends hebben een TLS-cliëntcertificaat, afgekort NB_{TLS}. De modellen voor de certificaten zijn opgenomen in deel 5. Elke nationale backend kan zijn eigen TLS-certificaat verstrekken. Dit certificaat wordt uitdrukkelijk op de whitelist geplaatst en kan dus worden afgegeven door een openbaar vertrouwde certificeringsautoriteit (bijvoorbeeld een certificeringsautoriteit die voldoet aan de basisvereisten van het CA Browser Forum), door een nationale certificeringsautoriteit of door zelfondertekening. Elke lidstaat is verantwoordelijk voor zijn nationale gegevens en voor de bescherming van de persoonlijke sleutel die wordt gebruikt om de verbinding met de DCCG tot stand te brengen. Voor de BYOC-aanpak ("bring your own certificate") is een duidelijk omschreven registratie- en identificatieprocedure nodig, evenals intrekkings- en hernieuwingsprocedures, zoals beschreven in delen *4.1*, *4.2* en *4.3*. De DCCG gebruikt een whitelist waaraan de TLS-certificaten van NB's worden toegevoegd nadat ze succesvol geregistreerd zijn. Alleen NB's die zichzelf authenticeren met een persoonlijke sleutel die overeenkomt met een certificaat op de whitelist, kunnen een beveiligde verbinding met de DCCG tot stand brengen. De DCCG zal ook een TLS-certificaat gebruiken dat de NB's in staat stelt na te gaan of zij daadwerkelijk een verbinding met de "echte" DCCG tot stand brengen en niet met een kwaadwillige entiteit die zich als DCCG voordoet. Het certificaat van de DCCG wordt na succesvolle registratie aan de NB's verstrekt. Het $DCCG_{TLS}$-certificaat wordt afgegeven door een openbaar vertrouwde CA (opgenomen in alle belangrijke browsers). Het is de verantwoordelijkheid van de lidstaten om na te gaan of hun verbinding met de DCCG beveiligd is (bijvoorbeeld door de vingerafdruk van het $DCCG_{TLS}$-certificaat van de server waarmee verbinding is gemaakt, te vergelijken met het certificaat dat na registratie werd verstrekt).

3.2. *CSCA's en validatiemodel*

De lidstaten die deelnemen aan het DCCG-kader moeten een CSCA gebruiken om de DSC's af te geven. De lidstaten kunnen meer dan één CSCA hebben (bijvoorbeeld in het geval van regionale decentralisatie). Elke lidstaat kan gebruikmaken van bestaande certificeringsautoriteiten of speciaal voor het DCC-systeem een (eventueel zelfondertekende) certificeringsautoriteit opzetten.

De lidstaten moeten hun CSCA-certificaat/-certificaten aan de DCCG-exploitant overleggen in het kader van de officiële onboardingprocedure. Na succesvolle registratie van de lidstaat (zie deel 4.*1* voor meer informatie) werkt de DCCG-exploitant een ondertekende vertrouwenslijst bij met alle CSCA-certificaten die actief zijn in het DCC-kader. De DCCG-exploitant gebruikt een specifiek asymmetrisch sleutelpaar om de vertrouwenslijst en de certificaten in een offline omgeving te ondertekenen. De persoonlijke sleutel wordt niet opgeslagen in het online DCCG-systeem, zodat een aanvaller die het onlinesysteem binnendringt de vertrouwenslijst niet in gevaar kan brengen. Het overeenkomstige vertrouwensankercertificaat $DCCG_{TA}$ wordt tijdens het onboardingproces aan de nationale backends verstrekt.

De lidstaten kunnen voor hun verificatieprocedures de vertrouwenslijst opvragen bij de DCCG. De CSCA wordt gedefinieerd als de certificeringsautoriteit die DSC's afgeeft; daarom moeten lidstaten die gebruikmaken van een meerlagige CA-hiërarchie (bijvoorbeeld basis-CA -> CSCA -> DSC's) zorgen voor de ondergeschikte certificeringsautoriteit die de DSC's afgeeft. Als een lidstaat in dat geval gebruikmaakt van een bestaande certificeringsautoriteit, zal het DCC-systeem alles boven de CSCA negeren en alleen de CSCA als vertrouwensanker toestaan (ook al is het een ondergeschikte CA). Dit is zo omdat het ICAO-model slechts precies 2 niveaus toestaat — een basis-CSCA ("root") en een eind-DSC ("leaf"), ondertekend door alleen die CSCA.

Indien een lidstaat zijn eigen CSCA exploiteert, is de lidstaat verantwoordelijk voor de beveiligde werking en het beveiligde sleutelbeheer van deze CA. De CSCA fungeert als vertrouwensanker voor DSC's, en daarom is het beschermen van de persoonlijke sleutel van de CSCA van essentieel belang voor de integriteit van de DCC-omgeving. Het verificatiemodel in de DCC-PKI volgt het shell-model, dat bepaalt dat alle certificaten bij de validatie van het certificaatpad op een bepaald tijdstip geldig moeten zijn (d.w.z. het moment van validatie van de handtekening). Daarom zijn de volgende beperkingen van toepassing:

— De CSCA geeft geen certificaten af die langer geldig zijn dan het CA-certificaat zelf;

— De ondertekenaar van het document mag geen documenten ondertekenen die langer geldig zijn dan het DSC zelf;

— De lidstaten die hun eigen CSCA exploiteren, moeten de geldigheidstermijn voor hun CSCA en alle afgegeven certificaten vaststellen en zorgen voor de vernieuwing van certificaten.

Deel 4.*2* bevat aanbevelingen voor geldigheidstermijnen.

3.3. *Integriteit en authenticiteit van geüploade data*

Nationale backends kunnen de DCCG gebruiken om digitaal ondertekende datapakketten na succesvolle wederzijdse authenticatie te uploaden en te downloaden. In het begin bevatten deze datapakketten de DSC's van de lidstaten. Het sleutelpaar dat door de nationale backend wordt gebruikt voor het digitaal ondertekenen van geüploade datapakketten in het DCCG-systeem, wordt het uploadsleutelpaar van de nationale backend genoemd en het bijbehorende publiekesleutelcertificaat wordt afgekort tot NB_{UP}-certificaat. Elke lidstaat brengt zijn eigen NB_{UP}-certificaat mee, dat zelf kan worden ondertekend of dat kan worden afgegeven door een bestaande certificeringsautoriteit, bijvoorbeeld een openbare certificeringsautoriteit (d.w.z. een certificeringsautoriteit die een certificaat afgeeft in overeenstemming met de basisvereisten van het CAB-Forum). Het NB_{UP}-certificaat is verschillend van alle andere door de lidstaat gebruikte certificaten (d.w.z. CSCA, TLS-cliënt of DSC's).

De lidstaten moeten het uploadcertificaat aan de DCCG-operator verstrekken tijdens de eerste registratieprocedure (zie deel 4.*1*voor meer informatie). Elke lidstaat is verantwoordelijk voor zijn nationale gegevens en voor de bescherming van de persoonlijke sleutel die wordt gebruikt voor het ondertekenen van de uploads.

Andere lidstaten kunnen de ondertekende datapakketten verifiëren met behulp van de door de DCCG verstrekte uploadcertificaten. De DCCG verifieert de authenticiteit en integriteit van de geüploade data aan de hand van het uploadcertificaat van de NB alvorens deze aan andere lidstaten te verstrekken.

3.4. *Eisen inzake de technische DCCG-architectuur*

Dit zijn de eisen inzake de technische DCCG-architectuur:

— De DCCG maakt gebruik van wederzijdse TLS-authenticatie om een geauthenticeerde versleutelde verbinding met de NB's tot stand te brengen. De DCCG onderhoudt daarom een whitelist van geregistreerde NB_{TLS}-cliëntcertificaten;

— De DCCG gebruikt twee digitale certificaten ($DCCG_{TLS}$ en $DCCG_{TA}$) met twee verschillende sleutelparen. De persoonlijke sleutel van het $DCCG_{TA}$-sleutelpaar wordt offline bewaard (niet op de onlinecomponenten van de DCCG);

— De DCCG onderhoudt een vertrouwenslijst van de NB_{CSCA}-certificaten die is ondertekend met de persoonlijke sleutel van de $DCCG_{TA}$;

— De gebruikte cijfers moeten voldoen aan de eisen van deel 5.*1*.

4. **Beheer van de certificatenlevenscyclus**

4.1. *Registratie van nationale backends*

De lidstaten moeten zich registreren bij de DCCG-exploitant om aan het DCCG-systeem deel te nemen. In dit deel wordt de technische en operationele procedure beschreven die moet worden gevolgd om een nationale backend te registreren.

De DCCG-exploitant en de lidstaat moeten informatie uitwisselen over technische contactpersonen voor het onboardingproces. Aangenomen wordt dat de technische contactpersonen geautoriseerd worden door hun lidstaat en dat identificatie/authenticatie via andere kanalen plaatsvindt. De authenticatie kan bijvoorbeeld worden bereikt wanneer de technische contactpersoon van een lidstaat de certificaten als met een wachtwoord versleutelde bestanden via e-mail verstrekt en het bijbehorende wachtwoord telefonisch met de DCCG-operator deelt. Ook andere door de DCCG-exploitant gedefinieerde beveiligde kanalen mogen worden gebruikt.

De lidstaat moet drie digitale certificaten verstrekken tijdens het registratie- en identificatieproces:

— Het TLS-certificaat NB_{TLS} van de lidstaat

— Het uploadcertificaat NB_{UP} van de lidstaat

— Het CSCA-certificaat/de CSCA-certificaten NB_{CSCA} van de lidstaat

Alle verstrekte certificaten moeten voldoen aan de eisen van deel 5. De DCCG-exploitant controleert of het verstrekte certificaat voldoet aan de eisen van deel 5. Na de identificatie en registratie moet de DCCG-exploitant:

— het NB_{CSCA}-certificaat/de NB_{CSCA}-certificaten toevoegen aan de vertrouwenslijst die is ondertekend met de persoonlijke sleutel die overeenstemt met de publieke sleutel van de $DCCG_{TA}$;

— het NB_{TLS}-certificaat toevoegen aan de whitelist van het TLS-eindpunt van de DCCG;

— het NB_{UP}-certificaat toevoegen aan het DCCG-systeem;

— de publiekesleutelcertificaten van de $DCCG_{TA}$ en $DCCG_{TLS}$ aan de lidstaat verstrekken.

4.2. *Certificeringsautoriteiten, geldigheidstermijnen en vernieuwing*

Indien een lidstaat zijn eigen CSCA wil exploiteren, kunnen de CSCA-certificaten zelfondertekende certificaten zijn. Zij fungeren als vertrouwensanker van de lidstaat en daarom moet de lidstaat de persoonlijke sleutel die overeenkomt met de publieke sleutel van de CSCA degelijk beschermen. Het strekt tot aanbeveling dat de lidstaten voor hun CSCA een offlinesysteem gebruiken, d.w.z. een computersysteem dat op geen enkel netwerk is aangesloten. Voor de toegang tot het systeem moet gebruik worden gemaakt van meerpersoonscontrole (bijvoorbeeld volgens het twee-paar-ogenprincipe). Na het ondertekenen van DSC's moeten operationele controles worden uitgevoerd en moet het systeem dat de persoonlijke sleutel van de CSCA bevat veilig worden opgeslagen met strenge toegangscontroles. Hardwarebeveiligingsmodules of smartcards kunnen worden gebruikt om de persoonlijke sleutel van de CSCA verder te beschermen. Digitale certificaten omvatten een geldigheidstermijn waardoor vernieuwing van de certificaten nodig is. Vernieuwing is noodzakelijk om nieuwe cryptografische sleutels te gebruiken en de omvang van de sleutels aan te passen wanneer nieuwe berekeningsmethoden of nieuwe aanvallen een bedreiging vormen voor de beveiliging van het gebruikte cryptografische algoritme. Het shell-model is van toepassing (zie deel 3.*2*).

De volgende geldigheidstermijnen worden aanbevolen, gezien de geldigheidsduur van één jaar voor digitale EU-covidcertificaten:

— CSCA: 4 jaar

— DSC: 2 jaar

— Upload: 1-2 jaar

— TLS-cliëntauthenticatie: 1-2 jaar

Voor een tijdige vernieuwing worden voor de persoonlijke sleutels de volgende gebruiksperioden aanbevolen:

— CSCA: één jaar

— DSC: zes maanden

Voor een vlotte werking moeten de lidstaten tijdig nieuwe uploadcertificaten en TLS-certificaten creëren, bijvoorbeeld één maand voor de vervaldatum. CSCA-certificaten en DSC's moeten ten minste één maand voor het einde van het gebruik van de persoonlijke sleutel worden vernieuwd (rekening houdend met de noodzakelijke operationele procedures). De lidstaten moeten geactualiseerde CSCA-, upload- en TLS-certificaten verstrekken aan de DCCG-exploitant. Verlopen certificaten worden van de whitelist en de vertrouwenslijst verwijderd.

De lidstaten en de DCCG-exploitant moeten de geldigheid van hun eigen certificaten bijhouden. Er is geen centrale entiteit die de geldigheid van het certificaat bijhoudt en de deelnemers informeert.

4.3. *Intrekking van certificaten*

In het algemeen kunnen digitale certificaten door de afgevende CA worden ingetrokken met behulp van certificaatintrekkingslijsten of een OCSP-responder (Online Certificate Status Protocol). CSCA's voor het DCC-systeem moeten certificaatintrekkingslijsten (CRL's) verstrekken. Ook als andere lidstaten deze CRL's momenteel niet gebruiken, moeten zij voor toekomstige toepassingen worden geïntegreerd. Indien een CSCA beslist geen CRL's te verstrekken, moeten de DSC's van deze CSCA worden vernieuwd zodra CRL's verplicht worden. Verificateurs dienen voor de validatie van de DSC's niet OCSP, maar CRL's te gebruiken. Het strekt tot aanbeveling dat de nationale backend de noodzakelijke validatie van uit de DCCG gedownloade DSC's uitvoert, en alleen een reeks betrouwbare en gevalideerde DSC's doorstuurt naar nationale DSC-validators. DCC-validators mogen in hun validatieproces geen intrekkingscontroles uitvoeren op DSC's. Eén reden hiervoor is dat op die manier de privacy van DCC-houders wordt beschermd door elke kans te vermijden dat het gebruik van een bepaalde DSC kan worden gecontroleerd door de bijbehorende OCSP-responder.

De lidstaten kunnen hun DSC's uit de DCCG verwijderen met behulp van hun eigen geldige upload- en TLS-certificaten. Het verwijderen van een DSC betekent dat alle DCC's die met de DSC in kwestie zijn afgegeven, ongeldig worden wanneer de lidstaten de bijgewerkte DSC-lijsten ophalen. Het is cruciaal dat persoonlijkesleutelmaterialen die overeenkomen met DSC's worden beschermd. De lidstaten moeten de DCCG-exploitant ervan in kennis stellen wanneer zij upload- of TLS-certificaten moeten intrekken, bijvoorbeeld omdat de nationale backend gecompromitteerd is. De DCCG-exploitant kan dan de vertrouwensrelatie voor het betrokken certificaat verwijderen, bijvoorbeeld door deze van de TLS-whitelist te schrappen. De DCCG-exploitant kan de uploadcertificaten uit de DCCG-databank verwijderen. Pakketten die zijn ondertekend met de persoonlijke sleutel die met dit uploadcertificaat overeenstemt, worden ongeldig wanneer nationale backends de vertrouwensrelatie van het ingetrokken uploadcertificaat verwijderen. Indien een CSCA-certificaat moet worden ingetrokken, stellen de lidstaten de DCCG-exploitant en andere lidstaten waarmee zij een vertrouwensrelatie hebben, hiervan in kennis. De DCCG-exploitant stelt dan een nieuwe vertrouwenslijst op waarin het betrokken certificaat niet meer is opgenomen. Alle door deze CSCA afgegeven DSC's worden ongeldig wanneer de lidstaten hun nationale backendvertrouwensarchief updaten. Indien het $DCCG_{TLS}$-certificaat of het $DCCG_{TA}$-certificaat moet worden ingetrokken, moeten de DCCG-exploitant en de lidstaten samenwerken om een nieuwe vertrouwde TLS-verbinding en vertrouwenslijst tot stand te brengen.

5. **Certificaatmodellen**

In dit deel worden de cryptografische eisen en richtsnoeren uiteengezet, alsmede de eisen inzake certificaatmodellen. Met betrekking tot de DCCG-certificaten worden in dit deel de certificaatmodellen gedefinieerd.

5.1. *Cryptografische eisen*

Cryptografische algoritmen en TLS-coderingssuites worden gekozen op basis van de huidige aanbeveling van het Duitse federale bureau voor informatiebeveiliging (BSI) of SOG-IS. Deze aanbevelingen zijn vergelijkbaar met die van andere instellingen en normalisatie-organisaties. De aanbevelingen staan in de technische richtsnoeren TR 02102-1 en TR 02102-2 ([1]) of SOG-IS Agreed Cryptographic Mechanisms ([2]).

5.1.1. Eisen inzake de DSC

De eisen van bijlage I, deel 3.*2.2*, zijn van toepassing. Daarom wordt ten zeerste aanbevolen dat documentondertekenaars gebruikmaken van het elliptische krommealgoritme voor digitale handtekening (ECDSA) met NIST-p-256 (zoals gedefinieerd in aanhangsel D bij FIPS PUB 186-4). Andere elliptische krommen worden niet ondersteund. Vanwege de beperkte ruimte van de DCC mogen de lidstaten geen RSA-PSS gebruiken, zelfs niet als

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

reservealgoritme. Indien lidstaten RSA-PSS gebruiken, moeten zij een modulusgrootte van 2048 of maximaal 3072 bit gebruiken. SHA-2 met een outputlengte van ≥ 256 bits wordt gebruikt als cryptografische hashfunctie (zie ISO/IEC 10118-3:2004) voor de DSC-handtekening.

5.1.2. Eisen inzake TLS-, upload- en CSCA-certificaten

Voor digitale certificaten en cryptografische handtekeningen in de context van DCCG zijn de belangrijkste eisen inzake cryptografische algoritmen en sleutellengte samengevat in de volgende tabel (vanaf 2021):

Algoritme van de handtekening	Grootte van de sleutel	Hashfunctie
EC-DSA	Min. 250 bit	SHA-2 met een outputlengte ≥ 256 bit
RSA-PSS (aanbevolen opvulling) RSA-PKCS#1 v1.5 (oude opvulling)	Min. 3000 bit RSA Modulus (N) met een publieke exponent e > 2^16	SHA-2 met een outputlengte ≥ 256 bit
DSA	Min. 3000 bit prime p, 250 bit sleutel q	SHA-2 met een outputlengte ≥ 256 bit

De aanbevolen elliptische kromme voor EC-DSA is NIST-p-256 vanwege de wijdverbreide toepassing ervan.

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

De volgende tabel bevat richtsnoeren voor het model van het NB_{CSCA}-certificaat voor het geval dat een lidstaat besluit zijn eigen CSCA voor het DCC-systeem te exploiteren.

Vetgedrukte delen zijn verplicht (moeten in het certificaat worden opgenomen), *cursieve* delen worden aanbevolen (zouden erin moeten worden opgenomen). Voor ontbrekende velden zijn geen aanbevelingen vastgesteld.

Veld	Waarde
Subject	**cn=<niet lege en unieke algemene naam>,***o=<Provider>,* **c=<lidstaat die de CSCA exploiteert>**
Key usage	**certificate signing,***CRL signing* (minimaal)
Basic Constraints	**CA = true, path length constraints = 0**

Het subject-veld mag niet leeg zijn en moet uniek zijn binnen de gespecificeerde lidstaat. De landcode (c) moet overeenkomen met de lidstaat die dit CSCA-certificaat zal gebruiken. Het certificaat moet een unieke subject key identifier (SKI) bevatten overeenkomstig RFC 5280 ([3]).

5.3. *Document Signer Certificate (DSC)*

De volgende tabel bevat richtsnoeren voor het DSC. **Vetgedrukte** delen zijn verplicht (moeten in het certificaat worden opgenomen), *cursieve* delen worden aanbevolen (zouden erin moeten worden opgenomen). Voor ontbrekende velden zijn geen aanbevelingen vastgesteld.

Veld	Waarde
Serial Number	**uniek serienummer**
Subject	**cn=<niet lege en unieke algemene naam>,***o=<Provider>,* **c=<lidstaat die de DSC gebruikt>**
Key Usage	**digital signature** (minimaal)

([3]) rfc5280 (ietf.org)

De DSC moet worden ondertekend met de persoonlijke sleutel die overeenstemt met een CSCA-certificaat dat door de lidstaat wordt gebruikt.

De volgende extensies moeten worden gebruikt:

— Het certificaat moet een Authority Key Identifier (AKI) bevatten die overeenstemt met de Subject Key Identifier (SKI) van het certificaat dat de CSCA afgeeft.

— Het certificaat moet een unieke subject key identifier bevatten (overeenkomstig RFC 5280 ([4])).

Bovendien moet het certificaat de extensie voor CRL-distributiepunten bevatten die verwijst naar de certificaatintrekkingslijst (CRL) die wordt verstrekt door de CSCA die de DSC heeft afgegeven.

De DSC kan een extensie voor uitgebreide-sleutelgebruik met nul of meer identificatiecodes voor sleutelgebruiksbeleid bevatten die de soorten HCERT's die dit certificaat mag verifiëren, beperken. Indien een of meer verificateurs aanwezig zijn, verifiëren zij het sleutelgebruik aan de hand van het opgeslagen HCERT. Hiervoor zijn de volgende extendedKeyUsage-waarden gedefinieerd:

Veld	Waarde
extendedKeyUsage	1.3.6.1.4.1.1847.2021.1.1 voor afgevers van testcertificaten
extendedKeyUsage	1.3.6.1.4.1.1847.2021.1.2 voor afgevers van vaccinatiecertificaten
extendedKeyUsage	1.3.6.1.4.1.1847.2021.1.3 voor afgevers van herstelcertificaten

Bij ontbreken van een extensie voor uitgebreide-sleutelgebruik (d.w.z. geen uitbreidingen of nuluitbreidingen), kan dit certificaat worden gebruikt om elk type HCERT te valideren. In andere documenten kunnen relevante aanvullende beleidsidentificatiecodes voor uitgebreide-sleutelgebruik worden gedefinieerd die worden gebruikt bij de validatie van HCERT's.

5.4. *Uploadcertificaten (NB_{UP})*

De volgende tabel bevat richtsnoeren voor het uploadcertificaat van nationale backends. **Vetgedrukte** delen zijn verplicht (moeten in het certificaat worden opgenomen), *cursieve* delen worden aanbevolen (zouden erin moeten worden opgenomen). Voor ontbrekende velden zijn geen aanbevelingen vastgesteld.

Veld	Waarde
Subject	**cn=<niet lege en unieke algemene naam>,***o=<Provider>,* **c=<lidstaat die dit uploadcertificaat gebruikt>**
Key Usage	**digital signature** (minimaal)

5.5. *TLS-cliëntauthenticatiecertificaat van nationale backends (NB_{TLS})*

De volgende tabel bevat richtsnoeren voor het TLS-cliëntauthenticatiecertificaat van nationale backends. **Vetgedrukte** delen zijn verplicht (moeten in het certificaat worden opgenomen), *cursieve* delen worden aanbevolen (zouden erin moeten worden opgenomen). Voor ontbrekende velden zijn geen aanbevelingen vastgesteld.

Veld	Waarde
Subject	**cn=<niet lege en unieke algemene naam>,***o=<Provider>,* **c=<lidstaat aan de NB>**
Key Usage	**digital signature** (minimaal)
Extended key usage	cliëntauthenticatie (1.3.6.1.5.5.7.3.2)

([4]) rfc5280 (ietf.org)

Het certificaat kan ook het uitgebreide-sleutelgebruik *server authentication (1.3.6.1.5.5.7.3.1)* bevatten, maar dit is niet vereist.

5.6. *Handtekeningcertificaat voor vertrouwenslijst ($DCCG_{TA}$)*

In de volgende tabel wordt het DCCG-vertrouwensankercertificaat gedefinieerd.

Veld	Waarde
Subject	**cn = Digital Green Certificate Gateway** ([5]), **o=<Provider>, c=<land>**
Key Usage	**digital signature** (minimaal)

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

In de volgende tabel wordt het DCCG-TLS-certificaat gedefinieerd.

Veld	Waarde
Subject	cn=<FQDN of IP-adres van de DCCG>, o=<Provider>, c=<land>
SubjectAltName	dNSName: <naam DCCG DNS> of iPAddress: <IP-adres DCCG>
Key Usage	**digital signature** (minimaal)
Extended key usage	server authentication (1.3.6.1.5.5.7.3.1)

Het certificaat kan ook het uitgebreide-sleutelgebruik *client authentication (1.3.6.1.5.5.7.3.2)* bevatten, maar dit is niet vereist.

Het TLS-certificaat van de DCCG wordt afgegeven door een algemeen betrouwbare certificeringsautoriteit (opgenomen in alle belangrijke browsers en besturingssystemen, volgens de basisvereisten van het CAB-forum).

([5]) De terminologie van "Digital Green Certificate" in plaats van "EU Digital COVID Certificate" is in dit verband gehandhaafd omdat dit de terminologie is die in de broncode is opgenomen en in het certificaat is gebruikt voordat de medewetgevers nieuwe terminologie hebben vastgesteld.