►**B**

KOMMISSIONENS GENNEMFØRELSESAFGØRELSE (EU) 2021/1073

af 28. juni 2021

om fastsættelse af tekniske specifikationer og regler for gennemførelsen af tillidsrammen for EU's digitale covidcertifikat som fastsat ved Europa-Parlamentets og Rådets forordning (EU) 2021/953

(EØS-relevant tekst)

(EUT L 230 af 30.6.2021, s. 32)

Ændret ved:

		Tidende		
		nr.	side	dato
►**M1**	Kommissionens gennemførelsesafgørelse (EU) 2021/2014 af 17. november 2021	L 410	180	18.11.2021
►**M2**	Kommissionens gennemførelsesafgørelse (EU) 2021/2301 af 21. december 2021	L 458	536	22.12.2021
►**M3**	Kommissionens gennemførelsesafgørelse (EU) 2022/483 af 21. marts 2022	L 98	84	25.3.2022
►**M4**	Kommissionens gennemførelsesafgørelse (EU) 2022/1516 af 8. september 2022	L 235	61	12.9.2022

▼B

KOMMISSIONENS GENNEMFØRELSESAFGØRELSE (EU) 2021/1073

af 28. juni 2021

om fastsættelse af tekniske specifikationer og regler for gennemførelsen af tillidsrammen for EU's digitale covidcertifikat som fastsat ved Europa-Parlamentets og Rådets forordning (EU) 2021/953

(EØS-relevant tekst)

Artikel 1

De tekniske specifikationer for EU's digitale covidcertifikat fastsætter den generiske datastruktur, kodningsmekanismerne og transportkodningsmekanismen i et maskinlæsbart, optisk format er fastsat i bilag I.

Artikel 2

Reglerne for udfyldelse af certifikaterne som omhandlet i artikel 3, stk. 1, i forordning (EU) 2021/953 er fastsat i bilag II til nærværende afgørelse.

Artikel 3

Kravene til den fælles struktur for den unikke certifikatidentifikator er fastsat i bilag III.

▼M1

Artikel 4

Forvaltningsreglerne for offentlige nøglecertifikater i forbindelse med portalen for EU's digitale covidcertifikat, som støtter tillidsrammens interoperabilitetsaspekter, er fastsat i bilag IV.

Artikel 5

En fælles koordineret datastruktur for de data, der skal inkluderes i certifikaterne som omhandlet i artikel 3, stk. 1, i forordning (EU) 2021/953, ved hjælp af et JSON-skema (JavaScript Object Notation), er fastsat i bilag V til nærværende afgørelse.

▼M3

Artikel 5a

Udveksling af lister over tilbagekaldte certifikater

1. Tillidsrammen for EU's digitale covidcertifikat skal muliggøre udveksling af lister over tilbagekaldte certifikater via den centrale portal for EU's digitale covidcertifikat (»portalen«) i overensstemmelse med de tekniske specifikationer i bilag I.

2. I tilfælde, hvor medlemsstaterne tilbagekalder EU's digitale covidcertifikater, kan de indsende lister over tilbagekaldte certifikater til portalen.

▼M3

3. Hvis medlemsstaterne indsender lister over tilbagekaldte certifikater, fører udstedelsesmyndighederne en liste over tilbagekaldte certifikater.

4. Hvis personoplysninger udveksles via portalen, begrænses behandlingen til det, som er nødvendigt for at støtte udvekslingen af tilbagekaldelsesoplysninger. Sådanne personoplysninger må kun anvendes til at kontrollere tilbagekaldelsesstatus for EU's digitale covidcertifikater, der er udstedt inden for rammerne af forordning (EU) 2021/953.

5. De oplysninger, der indgives til portalen, skal omfatte følgende data i overensstemmelse med de tekniske specifikationer i bilag I:

a) de pseudonymiserede unikke certifikatidentifikatorer for tilbagekaldte certifikater

b) en udløbsdato for den indsendte liste over tilbagekaldte certifikater

6. Hvis en udstedelsesmyndighed tilbagekalder EU's digitale covidcertifikater, som den har udstedt i henhold til forordning (EU) 2021/953 eller forordning (EU) 2021/954, og har til hensigt at udveksle relevante oplysninger via portalen, skal den fremsende de oplysninger, der er omhandlet i stk. 5, i form af lister over tilbagekaldte certifikater til portalen i et sikkert format i overensstemmelse med de tekniske specifikationer i bilag I.

7. Udstedelsesmyndighederne skal så vidt muligt tilvejebringe en løsning med henblik på at underrette indehavere af tilbagekaldte certifikater om deres certifikaters tilbagekaldelsesstatus og årsagen til tilbagekaldelsen på tidspunktet for tilbagekaldelsen.

8. Portalen indsamler de modtagne lister over tilbagekaldte certifikater Den stiller værktøjer til rådighed med henblik på distribution af listerne til medlemsstaterne. Den sletter automatisk listerne i overensstemmelse med de udløbsdatoer, som den indberettende myndighed har angivet for hver indsendt liste.

9. De udpegede nationale myndigheder eller officielle organer i medlemsstaterne, der behandler personoplysninger i portalen, er fælles dataansvarlige for de behandlede oplysninger. De fælles dataansvarliges forskellige ansvarsområder er som angivet i bilag VI.

10. Kommissionen er databehandler for personoplysninger, der behandles i portalen. I sin egenskab af databehandler sikrer Kommissionen på vegne af medlemsstaterne sikkerheden i forbindelse med overførsel og lagring af personoplysninger i portalen og overholder databehandlerens forpligtelser som fastsat i bilag VII.

11. Kommissionen og fælles dataansvarlige afprøver, vurderer og evaluerer regelmæssigt effektiviteten af de tekniske og organisatoriske foranstaltninger, der skal garantere sikkerheden i forbindelse med behandling af personoplysninger i portalen.

▼M3

Artikel 5b

Tredjelandes indsendelse af lister over tilbagekaldte certifikater

Tredjelande, der udsteder covid-19-certifikater, for hvilke Kommissionen har vedtaget en gennemførelsesretsakt i henhold til artikel 3, stk. 10, eller artikel 8, stk. 2, i forordning (EU) 2021/953, kan i overensstemmelse med de tekniske specifikationer, der er fastsat i bilag I, indsende lister over tilbagekaldte covid-19-certifikater omfattet af en sådan gennemførelsesretsakt, som skal behandles af Kommissionen på vegne af de fælles dataansvarlige i portalen som beskrevet i artikel 5a.

Artikel 5c

Forvaltning af behandlingen af personoplysninger i den centrale portal for EU's digitale covidcertifikat

1. De fælles dataansvarliges beslutningsproces styres af en arbejdsgruppe, der nedsættes under det udvalg, der er omhandlet i artikel 14 i forordning (EU) 2021/953.

2. De udpegede nationale myndigheder eller officielle organer i medlemsstaterne, der er fælles dataansvarlige for de personoplysninger, der behandles i portalen, skal udpege repræsentanter til den nævnte arbejdsgruppe.

▼M1

Artikel 6

Denne afgørelse træder i kraft på dagen for offentliggørelsen i *Den Europæiske Unions Tidende*.

▼B

Denne afgørelse træder i kraft på dagen for offentliggørelsen i *Den Europæiske Unions Tidende*.

▼B

BILAG I

FORMAT OG TILLIDSFORVALTNING

Generisk datastruktur, kodningsmekanismer og transportkodningsmekanisme i et maskinlæsbart, optisk format (»QR«)

1. **Indledning**

De tekniske specifikationer, der er fastsat i dette bilag, omfatter en generisk datastruktur og kodningsmekanismer for EU's digitale covidcertifikat (»DCC«). De fastsætter ligeledes en transportkodningsmekanisme i et maskinlæsbart, optisk format (»QR«), som kan vises på mobile enheders skærme eller udskrives. De i disse specifikationer fastsatte containerformater for de elektroniske sundhedscertifikater er generiske, men bruges i denne sammenhæng til at opbevare DCC'et.

2. **Terminologi**

I dette bilag forstås der ved »udstedere« organisationer, der anvender disse specifikationer ved udstedelse af sundhedscertifikater, og ved »kontrollører« organisationer, der accepterer disse certifikater som dokumentation for helbredstilstand. Ved »deltagere« forstås udstedere og kontrollører. Visse aspekter af dette bilag skal koordineres mellem deltagerne, såsom forvaltningen af et navneområde og distributionen af krypteringsnøgler. Det antages, at en part, som i det følgende benævnes »sekretariatet«, varetager disse opgaver.

3. **Containerformat for det elektroniske sundhedscertifikat**

Containerformatet for det elektroniske sundhedscertifikat (Electronic Health Certificate Container Format (»HCERT«)) er udformet, så sundhedscertifikater fra forskellige udstedere er ensartede og standardiserede. Målet med disse specifikationer er at harmonisere måden, hvorpå disse sundhedscertifikater gengives, kodes og signeres, med henblik på at fremme interoperabiliteten.

Evnen til at læse og fortolke et DCC fra en given udsteder kræver en fælles datastruktur og aftale om betydningen af hvert datafelt i nyttedataene. For at fremme denne interoperabilitet bliver der defineret en fælles koordineret datastruktur ved hjælp af et »JSON«-skema, der udgør rammen for DCC'et.

3.1. *Nyttedataenes struktur*

Nyttedataene er struktureret og kodet som en CBOR med en digital COSE-signatur. Dette er alment kendt som en »CBOR Web Token« (CWT) og er defineret i RFC 8392 ([1]). Nyttedataene som defineret i de følgende afsnit transporteres via et hcert-krav (claim).

Integriteten og ægtheden af nyttedataenes oprindelse skal kunne efterprøves af kontrollørerne. For at stille denne mekanisme til rådighed skal udstederen signere CWT'en ved hjælp af et asymmetrisk elektronisk signatursystem som defineret i COSE-specifikation (RFC 8152 ([2])).

3.2. *CWT-krav*

3.2.1. Overblik over CWT-struktur

Beskyttet header

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

▼B

— Signaturalgoritme (alg, mærkat 1)

— Nøgleidentifikator (kid, mærkat 4)

Nyttedata

— Udsteder (iss, kravnøgle 1, valgfri, udstederens ISO 3166-1 alpha-2)

— Udstedt den (iat, kravnøgle 6)

— Udløbstidspunkt (exp, kravnøgle 4)

— Sundhedscertifikat (hcert, kravnøgle -260)

— EU's digitale covidcertifikat v1 (eu_DCC_v1, kravnøgle 1)

Signatur

3.2.2. Signaturalgoritme

Parameteret signaturalgoritme (alg) angiver, hvilken algoritme der bruges til at oprette signaturen. Det skal opfylde eller overgå de nuværende SOG-IS-retningslinjer som sammenfattet nedenfor.

Der defineres en primær og en sekundær algoritme. Den sekundære algoritme bør kun bruges, hvis den primære algoritme ikke kan godkendes i henhold til de regler og forskrifter, som er pålagt udstederen.

For at sikre systemets sikkerhed vil alle implementeringer skulle medtage den sekundære algoritme. Af den årsag skal både den primære og den sekundære algoritme implementeres.

SOG-IS-værdierne for den primære og den sekundære algoritme er:

— Primær algoritme: Den primære algoritme er digital signaturalgoritme med elliptisk kurve (ECDSA) som defineret i (ISO/IEC 14888–3:2006) afsnit 2.3, der bruger P–256-parametre som defineret i tillæg D (D.1.2.3) til (FIPS PUB 186–4) i kombination med hashalgoritmen SHA–256 som defineret i (ISO/IEC 10118–3:2004) funktion 4.

Dette svarer til COSE-algoritmeparameter ES256.

— Sekundær algoritme: Den sekundære algoritme er RSASSA-PSS som defineret i (RFC 8230 ([1])) med modulo på 2048 bits i kombination med hashalgoritmen SHA–256 som defineret i (ISO/IEC
10118–3:2004) funktion 4.

Dette svarer til COSE-algoritmeparameter PS256.

3.2.3. Nøgleidentifikator

Kravet »nøgleidentifikator« (Key Identifier) (kid) angiver det dokumentsigneringscertifikat (Document Signer Certificate (DSC)), der indeholder den offentlige nøgle, som kontrolløren skal bruge til at kontrollere den digitale signaturs rigtighed med. Administration af offentlige nøglecertifikater, herunder kravene til DSC'er, er beskrevet i bilag IV.

([1]) rfc8230 (ietf.org)

▼B

Kravet »nøgleidentifikator« (kid) bruges af kontrollørerne til at vælge den korrekte offentlige nøgle fra en liste over nøgler vedrørende udstederen angivet i kravet udsteder (iss). En udsteder kan af administrative årsager og ved nøgleovergange anvende flere forskellige nøgler parallelt. Nøgleidentifikatoren er ikke et sikkerhedskritisk felt. Af den årsag kan den også placeres i en ubeskyttet header, hvis det er nødvendigt. Kontrollørerne skal acceptere begge løsninger. Hvis begge løsninger forefindes, bruges nøgleidentifikatoren i den beskyttede header.

Pga. forkortelsen af identifikatoren (af årsager relateret til begrænsning af størrelsen) kan det ikke udelukkes, at den generelle liste over DSC'er, som en kontrollør godkender, kan indeholde dobbelte forekomster af enkelte kid-krav. Af den årsag skal en kontrollør kontrollere alle DSC'er med denne kid.

3.2.4. Udsteder

Kravet »udsteder« (iss) er en strengværdi, der eventuelt kan indeholde ISO 3166-1 alpha-2-landekoden for den enhed, som udsteder sundhedscertifikatet. Dette krav kan bruges af en kontrollør til at identificere, hvilke DSC-sæt der skal bruges til kontrol. Kravnøgle 1 bruges til at identificere dette krav.

3.2.5. Udløbstidspunkt

Kravet »udløbstidspunkt« (exp) skal indeholde et tidsstempel i NumericDate-heltalsformat (som specificeret i RFC 8392 ([1]), afsnit 2), som angiver et tidspunkt indtil hvilket den pågældende signatur for nyttedataene skal betragtes som gyldig, og efter hvilket en kontrollør skal afvise nyttedataene som udløbet. Formålet med parameteret udløbstidspunkt er at sætte en grænse for sundhedscertifikatets gyldighedsperiode. Kravnøgle 4 bruges til at identificere dette krav.

Udløbstidspunktet må ikke være senere end udløbet af DSC'ens gyldighedsperiode.

3.2.6. Udstedt den

Kravet »udstedt den« (iat) skal indeholde et tidsstempel i NumericDate-heltalsformat (som specificeret i RFC 8392 ([2]), afsnit 2) og angive det tidspunkt, hvor sundhedscertifikatet blev oprettet.

Tidspunktet i feltet »udstedt den« må ikke ligge før udløbet af DSC'ens gyldighedsperiode.

Kontrollører kan anvende yderligere foranstaltninger med det formål at begrænse gyldigheden af sundhedscertifikatet baseret på tidspunktet for udstedelse. Kravnøgle 6 bruges til at identificere dette krav.

3.2.7. Kravet sundhedscertifikat

Kravet »sundhedscertifikat« (hcert) er et JSON-objekt (RFC 7159 ([3])) indeholdende oplysninger om sundhedsstatus. Der kan findes mange forskellige typer af sundhedscertifikater under samme krav, hvor DCC'et er et af dem.

JSON anvendes udelukkende til skemaformål. Gengivelsesformatet er CBOR som defineret i (RFC 7049 ([4])). Applikationsudviklere må faktisk hverken afkode eller kode til og fra JSON-formatet, men skal bruge strukturen i hukommelsen.

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

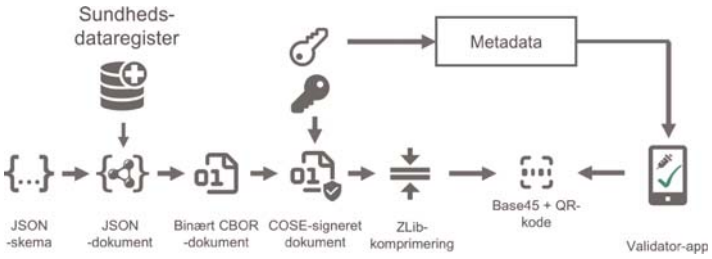
▼B

Den kravnøgle, der skal bruges til at identificere dette krav, er -260.

Strenge i JSON-objektet bør normaliseres efter Normalization Form Canonical Composition (NFC), som er defineret i Unicode-standarden. Imidlertid bør afkodningsapplikationer i den henseende være rummelige og robuste, og der tilskyndes stærkt til understøttelse af enhver rimelig typekonvertering. Hvis der i forbindelse med afkodning eller i efterfølgende sammenligningsfunktioner findes ikkenormaliserede data, bør implementeringerne behandle inputtet, som om det var normaliseret til NFC.

4. **Serialisering og oprettelse af DCC'ets nyttedata**

Som serialiseringsmønster anvendes følgende skema:



Processen starter med udtræk af data fra f.eks. et sundhedsdataregister (eller en ekstern datakilde) og strukturering af de udtrukne data ifølge de definerede DCC-skemaer. I denne proces kan konvertering til det definerede dataformat og omdannelse til for mennesker læsbare oplysninger, finde sted, før serialiseringen til CBOR starter. Kravenes akronymer skal i hvert tilfælde kobles til de viste navne før serialisering og efter deserialisering.

Valgfrit nationalt dataindhold er ikke tilladt i de certifikater, som udstedes i henhold til forordning (EU) 2021/953 ([1]). Dataindholdet er begrænset til de definerede dataelementer i det minimumsdatasæt, der er fastsat i bilaget i forordning 2021/953.

5. **Transportkodning**

5.1. *Rådata*

Hvad angår arbitrære datagrænseflader kan HCERT og dets nyttedata overføres, som de er, ved hjælp af enhver form for underliggende 8 bit sikker og pålidelig datatransport. Disse grænseflader kan omfatte Near Field Communication (NFC), bluetooth eller overførsel via en programlagsprotokol, f.eks. overførsel af et HCERT fra udstederen til en indehavers mobile enhed.

Hvis overførslen af HCERT fra udstederen til indehaveren er baseret på en grænseflade, som kun bruges til præsentation (f.eks. SMS eller e-mail), finder transportkodning af rådata naturligvis ikke anvendelse.

([1]) Europa-Parlamentets og Rådets forordning (EU) 2021/953 af 14. juni 2021 om en ramme for udstedelse, kontrol og accept af interoperable covid-19-vaccinations-, test- og restitutionscertifikater (EU's digitale covidcertifikat) for at lette fri bevægelighed under covid-19-pandemien (EUT L 211 af 15.6.2021, s. 1).

▼B

5.2. *Stregkode*

5.2.1. Komprimering af nyttedata (CWT)

For at mindske størrelsen af HCERT og øge hastigheden og pålideligheden i forbindelse med læseprocessen skal CWT komprimeres ved hjælp af ZLIB (RFC 1950 ([1])) og Deflate-komprimeringsmekanismen i det format, som er defineret i RFC 1951 ([2]).

5.2.2. QR 2D-stregkode

For bedre at kunne håndtere eksisterende udstyr, der er udformet til at fungere med ASCII-nyttedata, er den komprimerede CWT kodet som ASCII ved hjælp af Base45, før den kodes til en 2D-stregkode.

QR-formatet som defineret i (ISO/IEC 18004:2015) skal anvendes til generering af 2D-stregkoden. Der anbefales en fejlkorrektionsprocent (»Q«) på ca. 25 %. Fordi der anvendes Base45, skal QR-koden bruge alfanumerisk kode (tilstand 2, angivet med symbolerne 0010).

For at kontrollørerne skal kunne genkende den type data, der er kodet, og vælge det rigtige afkodnings- og behandlingsskema, skal Base45-kodede data (i henhold til nærværende specifikation) have den foranstillede kontekstidentifikationsstreng »HC1:«. Fremtidige versioner af denne specifikation, som påvirker bagudkompatibiliteten, skal definere en ny kontekstidentifikator, mens tegnet, som følger efter »HC«, skal tages fra tegnsættet [1-9A-Z]. Rækkefølgen er fastsat herefter, dvs. først [1-9] og dernæst [A-Z].

Det anbefales, at den optiske kode gengives på fremstillingsmediet med en diagonal størrelse på mellem 35 mm og 60 mm for at kunne bruges i aflæsningsapparater med fastmonteret optik, hvor mediet skal placeres på apparatets overflade.

Hvis den optiske kode printes på papir af printere med lav opløsning (< 300 dpi), skal der sørges for, at hvert symbol (prik) i QR-koden er helt firkantet. Ikkeforholdsmæssig skalering vil resultere i, at visse rækker eller kolonner i QR-koden har rektangulære symboler, hvilket i mange tilfælde vil gå ud over læsbarheden.

6. **Tillidslisteformat (CSCA- og DSC-lister)**

Hver medlemsstat skal udarbejde en liste over en eller flere nationalt signerende certificeringscentre (Country Signing Certification Authorities (CSCA)), og en liste over alle gyldige dokumentsigneringscertifikater (Document Signer Certificates (DSC)) og holde disse lister ajourført.

6.1. *Forenklet CSCA/DSC*

Fra og med denne version af specifikationerne kan medlemsstaterne ikke længere gå ud fra, at der anvendes oplysninger om lister over tilbagekaldte certifikater (CRL), eller at anvendelsesperioden for private nøgler kontrolleres af implementatorerne.

I stedet kontrolleres gyldigheden primært ved en validering af, at certifikatet svarer til den seneste version på certifikatlisten.

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

▼B

6.2. *ICAO eMRTD PKI og tillidscentre*

Medlemsstater kan bruge særskilte CSCA, men kan også fremsende deres eksisterende eMRTD CSCA-certifikater og/eller DSC'er og endog vælge at skaffe dem fra (kommercielle) tillidscentre og fremsende disse. Ethvert DSC skal dog altid være signeret af det CSCA, som figurerer på den pågældende medlemsstats liste.

7. **Sikkerhedshensyn**

Når de udarbejder en ordning, hvor de bruger nærværende specifikation, skal medlemsstaterne identificere, analysere og føre tilsyn med visse sikkerhedsaspekter.

Der bør som minimum tages højde for følgende aspekter:

7.1. *Gyldighedsperiode for HCERT-signatur*

Udstederen af HCERT skal begrænse gyldigheden af signaturen ved at fastsætte et tidspunkt, hvor gyldigheden udløber. Dermed pålægges indehaveren af et sundhedscertifikat at forny dette med periodiske intervaller.

Den acceptable gyldighedsperiode kan afhænge af praktiske omstændigheder. F.eks. har en rejsende ikke mulighed for at forny sit sundhedscertifikat på en oversøisk rejse. Det kan dog også hænde, at en udsteder mener, at der kan være tale om et sikkerhedsbrist, hvilket kræver, at udstederen trækker et DSC tilbage (og således gør alle de sundhedscertifikater, som er udstedt ved hjælp af denne nøgle, ugyldige, selv om gyldighedsperioden ellers ikke er udløbet). Konsekvenserne af en sådan hændelse kan begrænses ved regelmæssigt at udskifte udstedernes nøgler og kræve fornyelse af alle sundhedscertifikater med et rimeligt interval.

7.2. *Nøgleforvaltning*

Denne specifikation beror i høj grad på stærke krypteringsmekanismer, der skal sikre dataintegritet og autentificering af dataenes oprindelse. Det er derfor nødvendigt at opretholde de private nøglers fortrolighed.

Fortroligheden vedrørende krypteringsnøgler kan kompromitteres på en række forskellige måder, bl.a.:

— Genereringen af nøgler kan være mangelfuld og resultere i svage nøgler.

— Nøglerne kan blive udsat for menneskelige fejl.

— Nøglerne kan blive stjålet af eksterne eller interne gerningsmænd.

— Nøglerne kan blive regnet ud ved hjælp af kryptoanalyse.

For at afbøde risikoen for, at signeringsalgoritmen er for svag, og at private nøgler derfor kan kompromitteres ved kryptoanalyse, anbefales det i denne specifikation alle deltagere at implementere en sekundær signeringsalgoritme, der kan bruges som reserve, og som er baseret på andre parametre eller et andet matematisk problem end den primære.

Hvad angår de nævnte risici relateret til udstedernes driftsomgivelser, skal der gennemføres afbødende foranstaltninger, som skal sikre effektiv kontrol, f.eks. generering, lagring og brug af private nøgler i hardwaresikkerhedsmoduler (HSM'er). Der tilskyndes i høj grad til brug af HSM'er til signering af sundhedscertifikater.

▼B

Uanset om en udsteder vælger at bruge HSM'er eller ej, bør der lægges en plan for udskiftning af nøgler, hvor hyppigheden af udskiftningen er proportional med, hvor udsatte nøglerne er med hensyn til eksterne netværk, andre systemer og personale. En veltilrettelagt udskiftningsplan begrænser også de risici, der er forbundet med forkert udstedte sundhedscertifikater, fordi udstederen er i stand til at tilbagekalde sådanne sundhedscertifikater i portioner ved om nødvendigt at trække en nøgle tilbage.

7.3. *Validering af inputdata*

Disse specifikationer kan bruges på en måde, som indebærer modtagelse af data fra upålidelige kilder i systemer af opgavekritisk art. For at minimere den risiko, der er forbundet med denne angrebsvektor, skal alle inputfelter valideres behørigt med hensyn til datatype, længde og indhold. Før en hvilken som helst form for behandling af HCERT-indholdet finder sted, skal udstederens signatur ligeledes kontrolleres. Validering af udstederens signatur indebærer imidlertid, at udstederens beskyttede header fortolkes først, da en eventuel angriber kan forsøge at tilføre nøje udarbejdede oplysninger hertil, hvis formål er at kompromittere systemets sikkerhed.

8. **Tillidsforvaltning**

Signering af HCERT kræver, at der er en offentlig nøgle at kontrollere. Medlemsstaterne skal stille disse offentlige nøgler til rådighed. I den sidste ende skal den enkelte kontrollør have en liste over alle de offentlige nøgler, vedkommende har tillid til (eftersom den offentlige nøgle ikke er del af HCERT).

Systemet består af (kun) to lag: For hver medlemsstat et eller flere landespecifikke certifikater, som hver signerer et eller flere dokumentsigneringscertifikater, der bruges i de daglige aktiviteter.

Medlemsstaternes certifikater kaldes certifikater fra nationalt signerende certificeringscentre (Country Signing Certificate Authority (CSCA)) og er (typisk) selvsignerede certifikater. Medlemsstaterne kan have mere end et (f.eks. i tilfælde af regional decentralisering). Disse CSCA-certifikater signerer regelmæssigt de dokumentsigneringscertifikater (Document Signer Certificates (DSC)), der bruges til signering af HCERT'er.

»Sekretariatet« er en funktionel rolle. Det skal regelmæssigt aggregere og offentliggøre medlemsstaternes DSC'er efter at have verificeret disse ud fra listen over CSCA-certifikater (som er blevet overbragt og verificeret på anden vis).

Den heraf resulterende liste over DSC'er indeholder således det aggregerede sæt af godkendte offentlige nøgler (og de tilhørende nøgleidentifikatorer), som kontrollører kan bruge til at validere signaturer vedrørende HCERT'er. Kontrollørerne skal regelmæssigt hente og ajourføre denne liste.

Sådanne medlemsstatsspecifikke lister kan tilpasses det format, der passer til de nationale forhold. Filformatet for denne tillidsliste kan variere. Det kan f.eks. være et signeret JWKS (JWK set format i henhold til RFC 7517 ([1]), afsnit 5) eller ethvert andet format, der er specifikt for den teknologi, som anvendes i den pågældende medlemsstat.

For at sikre enkelthed kan medlemsstaterne både indsende deres eksisterende CSCA-certifikater fra deres ICAO eMRTD-systemer eller — som anbefalet af WHO — oprette et specielt til dette sundhedsområde.

([1]) rfc7517 (ietf.org)

▼B

8.1. *Nøgleidentifikator (Key Identifier (kid))*

Nøgleidentifikatoren (kid) beregnes, når der udarbejdes en liste over pålidelige offentlige nøgler fra DSC'er, og består af et afkortet (første 8 bytes) SHA-256-fingeraftryk fra DSC'et kodet i DER-format (raw).

Kontrollørerne behøver ikke at beregne kid'en på grundlag af DSC'et og kan direkte matche nøgleidentifikatoren i det udstedte sundhedscertifikat med kid'en på den pålidelige liste.

8.2. *Forskelle i forhold til ICAO eMRTD PKI-tillidsmodellen*

Om end den bygger på bedste praksis i ICAO eMRTD PKI-tillidsmodellen skal der foretages en række forenklinger for at øge hastigheden:

— En medlemsstat kan indsende flere forskellige CSCA-certifikater.

— DSC'ets (nøgleanvendelse) gyldighedsperiode kan fastsættes til en hvilken som helst varighed, der ikke er længere end CSCA-certifikatets gyldighedsperiode, og kan være fraværende.

— DSC'et kan indeholde politikidentifikatorer (udvidet nøgleanvendelse), som er specifikke for sundhedscertifikater.

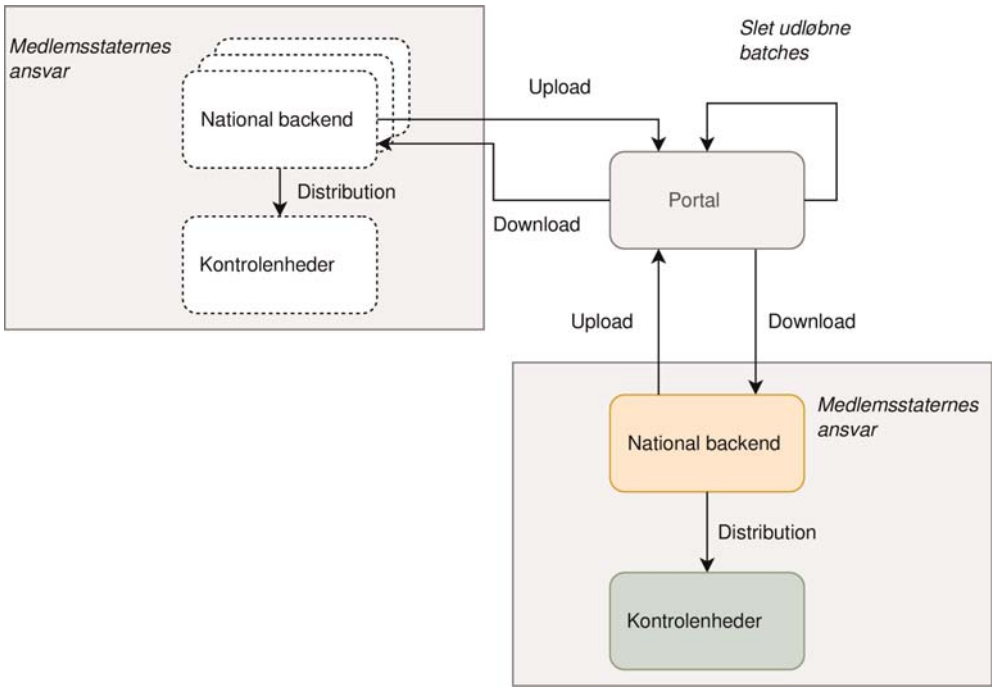
— Medlemsstaterne kan vælge ikke at foretage kontrol af offentliggjorte tilbagekaldelser og i stedet forlade sig udelukkende på de DSC-lister, de dagligt får fra sekretariatet eller selv indhenter.

▼M3

9. **Tilbagekaldelsesløsning**

9.1. *Tilvejebringelse af lister over tilbagekaldte covidcertifikater*

Portalen tilvejebringer slutpunkter og funktionaliteter til at føre og forvalte lister over tilbagekaldte certifikater:



▼M3

9.2. *Tillidsmodel*

Alle forbindelser etableres via standardtillidsmodellen for EU's digitale covidcertifikat (DCCG) ved hjælp af NB_{TLS}- og NB_{UP}-certifikater (se administration af certifikater). Alle oplysninger pakkes og uploades af CMS-meddelelser for at sikre integriteten.

9.3. *Batchudformning*

9.3.1. Batch

Hver liste over tilbagekaldte certifikater skal indeholde en eller flere indkodninger og være pakket i batches, som indeholder et sæt hashværdier og deres metadata. En batch er uforanderlig og definerer en udløbsdato, på hvilken batchen kan slettes. Udløbsdatoen for alle elementer i batchen skal være nøjagtigt den samme, hvilket betyder, at batchene skal grupperes efter udløbsdato og signeret DSC. Hver batch må maksimalt indeholde 1 000 indkodninger. Hvis en liste over tilbagekaldte certifikater indeholder mere end 1 000 indkodninger, skal der oprettes flere batches. En indkodning må kun optræde i ét batch. Batchen skal pakkes i en CMS-struktur og underskrives med det uploadende lands NB_{UP}-certifikat.

9.3.2. Batchindeks

Når der genereres en batch, tildeles den en unik identifikator af portalen og tilføjes automatisk til indekset. Batchindekset sorteres efter ændringsdato i stigende kronologisk rækkefølge.

9.3.3. Portalens funktionsmåde

Portalen behandler batches af tilbagekaldelser uden at foretage ændringer: Den kan hverken ajourføre, fjerne eller tilføje oplysninger til batchene. Batchene videresendes til samtlige autoriserede lande (se kapitel 9.6).

Portalen holder automatisk øje med batchenes udløbsdato og fjerner batches, der er udløbet. Når en batch slettes, sender portalen svaret »HTTP 410 Gone« for den slettede batchs URL. Batchen optræder derfor i batchindekset som »slettet«.

9.4. *Hashværdityper*

Listen over tilbagekaldte certifikater indeholder hashværdier, der kan repræsentere forskellige tilbagekaldelsestyper/-attributter. Disse typer eller attributter skal angives ved tilvejebringelsen af listerne over tilbagekaldte certifikater. De gængse typer er:

Type	Attribut	Hashberegning
SIGNATURE	DCC Signature	SHA256 of DCC Signature
UCI	UCI (Unique Certificate Identifier)	SHA256 of UCI
COUNTRYCODEUCI	Issuing Country Code + UCI	SHA256 of Issuing Country-Code + UCI

Det er kun de første 128 bits af de hashværdier, der er kodet som Base64-strenge, som samles i batches og bruges til identifikation af de tilbagekaldte covidcertifikater ([1]).

([1]) Se ligeledes 9.5.1.2 for de detaljerede API-beskrivelser.

▼M3

9.4.1. Hashværditype: SHA256(DCC Signature)

I dette tilfælde beregnes hashværdien ud fra bytesene for signaturen COSE_SIGN1, som kommer fra CWT. For så vidt angår RSA-signaturer vil hele signaturen blive brugt som input. Formlen for certifikater, der er signeret med ECDSA, bruger værdien r som input:

SHA256(r)

[kræves for alle nye implementeringer]

9.4.2. Hashværditype: SHA256(UCI)

I dette tilfælde beregnes hashværdien ud fra UCI-strengen, der er kodet i UTF-8 og konverteret til en byte-array.

[forældet (1), men supporteres med henblik på bagudkompatibilitet]

9.4.3. Hashværditype: SHA256(Issuing CountryCode+UCI)

I dette tilfælde er landekoden indkodet som UTF-8-streng, der er sammenkædet med UCI'en kodet med en UTF-8-streng. Dette konverteres efterfølgende til en byte-array og bruges som input til hashfunktionen.

[forældet[2], men supporteres med henblik på bagudkompatibilitet]

9.5. *API-struktur*

9.5.1. API til indkodning af tilbagekaldelser

9.5.1.1. Formål

API'en leverer indkodninger i listen over tilbagekaldte certifikater i batches, inklusiv et batchindeks.

9.5.1.2. Slutpunkter

9.5.1.2.1. Slutpunkt for download af batchliste

Slutpunkterne har en enkel struktur og returnerer en liste over batches med en lille wrapper med metadata. Batchene sorteres efter *dato* i *stigende (kronologisk)* rækkefølge:

/revocation-list

Verb: GET

Content-Type: application/json

Response: JSON Array

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

(1) Forældet betyder, at dette element ikke skal tages i betragtning i forbindelse med nye implementeringer, men at det skal supporteres for eksisterende implementeringer i en velafgrænset periode.

▼M3

Bemærkninger: Resultatet er som standard begrænset til 1 000. Hvis flaget »more« er sat til sandt, betyder det, at flere batches kan downloades. For at downloade yderligere elementer skal klienten sætte headeren If-Modified-Since til en dato, som ikke ligger før den sidst modtagne indkodning.

Svaret indeholder en JSON-array med følgende struktur:

Felt	Definition
more	Et boolesk flag, som angiver, at der findes flere batches.
batches	Array med eksisterende batches.
batchId	https://en.wikipedia.org/wiki/Universally_unique_identifier
country	Landekode ISO 3166
date	ISO 8601 Dato UTC. Dato, hvor batchen blev tilføjet eller slettet.
deleted	boolean. Sandt hvis slettet. Når flaget sættes til »deleted«, kan indkodningen endeligt fjernes fra søgeresultaterne efter syv dage.

9.5.1.2.1.1. Svarkoder

Kode	Beskrivelse
200	Alt ok.
204	Intet indhold, hvis headeren »If-Modified-Since« ikke har noget match.

Anmodningsheader

Header	Obligatorisk	Beskrivelse
If-Modified-Since	Ja	Denne header indeholder den sidste downloadede dato, så kun de nyeste resultater vises. Ved første opkald bør headeren sættes til »2021-06-01T00:00:00Z«

9.5.1.2.2. Slutpunkt for download af batch

Batchen indeholder en liste over certifikatidentifikatorer:

/revocation-list/{batchId}

Verb: GET

Accepts: application/cms

Response:CMS with Content

{

»country«: »XY«,

»expires«: »2022-11-01T00:00:00Z«,

▼**M3**

»kid«:»23S+33f=«,

»hashType«:»SIGNATURE«,

»entries«:[{

»hash«:»e2e2e2e2e2e2e2e2«

}, ..]

}

Svaret indeholder en CMS med en signatur, som skal svare til landets NB_{UP}-certifikat. Alle elementer i JSON-arrayen har følgende struktur:

Felt	Obligatorisk	Type	Definition
expires	Ja	String	Dato, hvor elementet kan fjernes. ISO8601 UTC-dato/-tid
country	Ja	String	Landekode ISO 3166
hashType	Ja	String	Hashtype brugt til indkodningerne (se Hashtyper)
entries	Ja	JSON Object Array	Se tabellen Indkodninger
kid	Ja	String	base64-kodet KID for den DSC, der er brugt til signatur af det digitale covidcertifikat. Hvis KID ikke er kendt, kan strengen 'UNKNOWN_KID' (eksklusiv ') anvendes.

Bemærk:

— Batches skal grupperes efter udløbsdato og DSC. Alle elementer skal udløbe samtidigt og være signeret med den samme nøgle.

— Udløbsdatoen er angivet i UTC-dato/-tid, fordi EU-DCC er et globalt system, og der skal anvendes en entydig tidsangivelse.

— Udløbsdatoen for et permanent tilbagekaldt digitalt covidcertifikat sættes til udløbsdatoen for den tilsvarende DSC, der er brugt til at signere covidcertifikatet, eller til udløbstidspunktet for det tilbagekaldte digitale covidcertifikat (i så tilfælde skal den anvendte NumericDate-/Epoch-tidsangivelse behandles, som om det var UTC-tid).

— National backend (*NB*) skal fjerne elementer fra listen over tilbagekaldte certifikater, når **udløbsdatoen** nås.

— *NB* kan fjerne elementer fra deres lister over tilbagekaldte certifikater i tilfælde af, at den **KID**, der er brugt til signere det digitale covidcertifikat, tilbagekaldes.

▼**M3**

9.5.1.2.2.1. Indkodninger

Felt	Obligatorisk	Type	Definition
hash	Ja	String	Første 128 bits af hashværdien SHA256 kodet som en Base64-streng

Bemærk: Indkodningsobjektet indeholder p.t. kun en hashværdi, men for at være kompatibel med fremtidige ændringer, er der valgt et objekt frem for en JSON-array.

9.5.1.2.2.2. Svarkoder

Kode	Beskrivelse
200	Alt ok.
410	Batch slettet. Batch kan slettes i den nationale backend.

9.5.1.2.2.3. Svarheader

Header	Beskrivelse
ETag	Batch ID.

9.5.1.2.3. Slutpunkt for upload af batch

Upload foretages med samme slutpunkt via verbet DELETE:

/revocation-list

Verb: POST

Accepts: application/cms

Request: CMS with Content

ContentType: application/cms

Content:

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

Batchen signeres ved hjælp af NB_{UP}-certifikatet. Portalen verificerer, at signaturen er sat af NB_{UP}-certifikatet for det pågældende *land*. Hvis signaturen ikke består tjekket, kan uploadet ikke gennemføres.

BEMÆRK: Hver batch er uforanderlig og kan ikke ændres efter upload. Den kan dog godt slettes. ID'en for hver batch lagres, og upload af en ny batch med samme ID afvises.

▼**M3**

9.5.1.2.4. Slutpunkt for sletning af batches

En batch kan slettes med samme slutpunkt via verbet DELETE:

/revocation-list

Verb: DELETE

Accepts: application/cms

ContentType: application/cms

Request: CMS with Content

Content:

{

»batchId«: »...«

}

eller — af kompatibilitetsårsager — til følgende slutpunkt med verbet POST:

/revocation-list/delete

Verb: POST

Accepts: application/cms

ContentType: application/cms

Request: CMS with Content

Content:

{

»batchId«: »...«

}

9.6. *API-beskyttelse/databeskyttelsesforordningen*

I dette afsnit præciseres foranstaltninger, som skal sikre, at implementeringen overholder bestemmelserne i forordning (EU) 2021/953 for så vidt angår behandling af personoplysninger.

9.6.1. Eksisterende autentificering

Portalen anvender p.t. NB_{TLS}-certifikatet til at autentificere de lande, der opretter forbindelse til portalen. Denne autentificering kan bruges til at fastslå identiteten på det land, der er forbundet til portalen. Denne identitet kan efterfølgende bruges til adgangskontrol.

9.6.2. Adgangskontrol

For lovligt at kunne behandle personoplysninger skal portalen indføre en mekanisme til adgangskontrol.

Portalen benytter en adgangskontrolliste kombineret med et rollebaseret sikkerhedssystem. Systemet skal indeholde to tabeller: En tabel, som beskriver hvilke roller, der kan udføre hvilke operationer med hvilke ressourcer, og en anden tabel, som beskriver, hvilke roller er tildelt hvilke brugere.

For at gennemføre de i dette dokument fastsatte kontroller kræves der tre roller, som er:

RevocationListReader

RevocationUploader

RevocationDeleter

▼**M3**

Følgende slutpunkter skal tjekke, om brugeren har rollen RevocationListReader; hvis det er tilfældet, skal der gives adgang, hvis ikke, sendes der et HTTP 403 Forbidden:

GET/revocation-list/

GET/revocation-list/{batchId}

Følgende slutpunkter skal tjekke, om brugeren har rollen RevocationUploader; hvis det er tilfældet, skal der gives adgang, hvis ikke, sendes der et HTTP 403 Forbidden:

POST/revocation-list

Følgende slutpunkter skal tjekke, om brugeren har rollen RevocationDeleter; hvis det er tilfældet, skal der gives adgang, hvis ikke, sendes der et HTTP 403 Forbidden:

DELETE/revocation-list

POST/revocation-list/delete

Portalen skal tilvejebringe en pålidelig metode, hvorved administratorer kan forvalte de roller, der er knyttet til brugerne, på en sådan måde at det reducerer risikoen for menneskelige fejl og ikke udgør en byrde for de funktionelle administratorer.

▼M1

BILAG II

REGLER FOR UDFYLDELSE AF EU'S DIGITALE COVIDCERTIFIKAT

De generelle regler vedrørende de værdisæt, der er fastsat i dette bilag, har til formål at sikre interoperabilitet på semantisk niveau og skal muliggøre ensartede tekniske implementeringer af EU's digitale covidcertifikat. Elementerne i dette bilag kan anvendes til de tre forskellige formål (vaccination/test/restitution), jf. forordning (EU) 2021/953. Kun de elementer, der kræver semantisk standardisering gennem kodede værdisæt, er opført i dette bilag.

Det er medlemsstaternes ansvar at oversætte de kodede elementer til deres nationale sprog.

For alle datafelter, der ikke er nævnt i de nedenfor beskrevne værdisæt, er kodningen beskrevet i bilag V.

Hvis de nedenstående foretrukne kodesystemer af en eller anden grund ikke kan anvendes, kan der anvendes andre internationale kodesystemer, og der bør rådgives om, hvordan koderne fra det andet kodesystem knyttes til det foretrukne kodesystem. Tekst (visningsnavne) kan undtagelsesvis anvendes som backupmekanisme, hvis der ikke findes en passende kode i de definerede værdisæt.

Medlemsstater, der anvender andre koder i deres systemer, skal knytte sådanne koder til de beskrevne værdisæt. Medlemsstaterne er ansvarlige for disse tilknytninger.

►M4 Eftersom visse værdisæt baseret på de kodesystemer, der er fastsat i nærværende bilag, såsom dem for kodning af vacciner og antigentest, ofte ændres, skal de offentliggøres og regelmæssigt ajourføres af Kommissionen med bistand fra e-sundhedsnetværket og Udvalget for Sundhedssikkerhed. ◄ De ajourførte værdisæt offentliggøres på Kommissionens relevante websted samt på e-sundhedsnetværkets websted. Der stilles en ændringshistorik til rådighed.

1. **Målsygdom eller -agens/Sygdom eller agens, som indehaveren er restitueret efter: Covid-19 (sars-CoV-2 eller en variant heraf)**

   Anvendes i certifikat 1, 2 og 3.

   Følgende kode anvendes:

Kode	Visning på skærm	Kodesystemets navn	Kodesystemets URL	Kodesystemets OID	Kodesystemets version
840539006	COVID-19	SNOMED CT	http://snomed.info/sct	2.16.840.1.113883.6.96	2021-01-31

2. **Covid-19-vaccine eller -profylakse**

   Foretrukket kodesystem: SNOMED CT-systemet eller ATC-klassifikationssystemet

   Anvendes i certifikat 1.

   Som eksempler på koder, der skal anvendes, fra de foretrukne kodesystemer, kan nævnes SNOMED CT-kode 1119305005 (sars-CoV-2-antigenvaccine), 1119349007 (sars-CoV-2-mRNA-vaccine) eller J07BX03 (covid-19-vacciner).

   Kommissionen skal med bistand fra e-sundhedsnetværket offentliggøre og regelmæssigt ajourføre et værdisæt, der fastsætter de koder, som skal bruges i henhold til de i dette afsnit fastsatte kodesystemer. Værdisættet skal udvides, når nye vaccinetyper udvikles og tages i brug.

▼M1

3. **Covid-19-vaccinelægemiddel**

Foretrukne kodesystemer (i prioriteret rækkefølge):

— EU-registret over lægemidler foretrækkes til vacciner med EU-dækkende tilladelse (tilladelsesnumre)

— Et globalt vaccineregister som det, der kunne oprettes af Verdenssundhedsorganisationen

— Vaccinelægemidlets navn i andre tilfælde. Hvis navnet indeholder mellemrumstegn, erstattes disse af en bindestreg (-).

Værdisættets navn: Vaccine.

Anvendes i certifikat 1.

Som eksempel på en kode, der skal anvendes, fra de foretrukne kodesystemer kan nævnes EU/1/20/1528 (Comirnaty). Eksempel på vaccinens navn, når det anvendes som kode: Sputnik-V (kode for Sputnik V).

Kommissionen skal med bistand fra e-sundhedsnetværket offentliggøre og regelmæssigt ajourføre et værdisæt, der fastsætter de koder, som skal bruges i henhold til de i dette afsnit fastsatte kodesystemer.

Vacciner skal kodes ved hjælp af en eksisterende kode i det offentliggjorte værdisæt, også selv om deres navne er forskellige alt efter land. Årsagen er, at der endnu ikke findes et globalt vaccineregister over alle de vacciner, der p.t. bruges. Eksempel:

— For vaccinen »COVID-19 Vaccine Moderna Intramuscular Injection«, der er navnet på Spikevax-vaccinen i Japan, anvendes koden EU/1/20/1507, da det er vaccinens navn i EU.

Hvis dette ikke er muligt eller tilrådeligt i et givet tilfælde, vil der blive tildelt en separat kode i det offentliggjorte værdisæt.

▼M4

Hvis et land, der anvender EU's digitale covidcertifikat, beslutter at udstede vaccinationscertifikater til deltagere i igangværende kliniske forsøg, skal vaccinationslægemidlet kodes således:

CT_*identifikator-for-klinisk-forsøg*

Hvis det kliniske forsøg er registreret i EU's register over kliniske forsøg (EU-CTR), skal identifikatoren for det kliniske forsøg fra dette register anvendes. I andre tilfælde kan identifikatorer fra andre registre (såsom clinicaltrials.gov eller Australian New Zealand Clinical Trials Registry) anvendes.

Identifikatoren for det kliniske forsøg skal indeholde et præfiks, der gør det muligt at finde frem til registret over kliniske forsøg (f.eks. EUCTR for EU's register over kliniske forsøg, NCT for clinicaltrials.gov, ACTRN for Australian New Zealand Clinical Trials Registry).

Når Kommissionen har modtaget vejledning fra Udvalget for Sundhedssikkerhed, Det Europæiske Center for Forebyggelse af og Kontrol med Sygdomme (ECDC) eller Det Europæiske Lægemiddelagentur (EMA) med hensyn til accept af certifikater udstedt for en covid-19-vaccine, der undergår kliniske forsøg, skal vejledningen offentliggøres enten som en del af dokumentet med værdisæt eller separat.

▼M1

4. **Indehaver af markedsføringstilladelse for covid-19-vaccine eller covid-19-vaccineproducent**

Foretrukket kodesystem:

— Organisationskode fra EMA (SPOR-systemet i overensstemmelse med ISO IDMP)

— Et globalt register over indehavere af markedsføringstilladelser for vacciner eller vaccineproducenter som det, der kunne oprettes af Verdenssundhedsorganisationen

— Organisationens navn i andre tilfælde. Hvis navnet indeholder mellemrumstegn, erstattes disse af en bindestreg (-).

Anvendes i certifikat 1.

Som eksempel på en kode, der skal anvendes, fra det foretrukne kodesystem kan nævnes ORG-100001699 (AstraZeneca AB). Eksempel på organisationens navn, når det anvendes som kode: Sinovac-Biotech (kode for Sinovac Biotech).

Kommissionen skal med bistand fra e-sundhedsnetværket offentliggøre og regelmæssigt ajourføre et værdisæt, der fastsætter de koder, som skal bruges i henhold til de i dette afsnit fastsatte kodesystemer.

Forskellige filialer inden for samme indehaver af en markedsføringstilladelse eller samme producent skal bruge en eksisterende kode i det offentliggjorte værdisæt.

For samme vaccineprodukt gælder det generelt, at det er den kode, som er knyttet til indehaveren af markedsføringstilladelsen i EU, der skal anvendes, eftersom der endnu ikke findes et internationalt aftalt register over vaccineproducenter eller indehavere af markedsføringstilladelser. Eksempler:

— For organisationen »Pfizer AG«, som er indehaver af markedsføringstilladelsen for vaccinen »Comirnaty«, der anvendes i Schweiz, anvendes koden ORG-100030215, der henviser til BioNTech Manufacturing GmbH, som er indehaver af markedsføringstilladelsen for Comirnaty i EU.

— For organisationen »Zuellig Pharma«, som er indehaver af markedsføringstilladelsen for Covid-19 Vaccine Moderna (Spikevax), der anvendes i Filippinerne, anvendes koden ORG-100031184, der henviser til Moderna Biotech Spain S.L., som er indehaver af markedsføringstilladelsen for Spikevax i EU.

Hvis dette ikke er muligt eller tilrådeligt i et givet tilfælde, vil der blive tildelt en separat kode i det offentliggjorte værdisæt.

▼M4

Hvis et land, der anvender EU's digitale covidcertifikat, beslutter at udstede vaccinationscertifikater til deltagere i igangværende kliniske forsøg, skal indehaveren af markedsføringstilladelsen eller producenten kodes ved brug af den værdi, der er angivet i værdisættet, hvis den foreligger. I andre tilfælde skal indehaveren af markedsføringstilladelsen eller producenten kodes ved brug af den regel, der er beskrevet i punkt 3 Vaccinelægemiddel (CT_*identifikator-for-klinisk-forsøg*).

▼M1

5. **Nummer i en række af doser samt det samlede antal doser i rækken**

Anvendes i certifikat 1.

To felter:

1) Nummer i en række doser af en covid-19-vaccine (N)

2) Det samlede antal doser i vaccinationsserien (C).

5.1. *Primær vaccinationsserie*

Når en person modtager doser i den primære vaccinationsserie, dvs. den vaccinationsserie, der skal give tilstrækkelig beskyttelse i en indledende fase, skal (C) afspejle det samlede antal doser i den primære vaccinationsserie, der er standard (f.eks. 1 eller 2, afhængig af den type vaccine, der er givet). Det omfatter også muligheden for at anvende en kortere serie (C=1), hvis en medlemsstats vaccinationsprotokol gør det muligt at give en enkelt dosis af en 2-dosis-vaccine til personer, der tidligere har været smittet med SARS-CoV-2. En afsluttet primær vaccinationsserie angives følgelig med N/C = 1. Eksempel:

— 1/1 angiver afslutningen af en primær vaccinationsserie med en enkelt dosis eller afslutningen af en primær serie bestående af én dosis af en 2-dosis-vaccine givet til en restitueret person i overensstemmelse med en medlemsstats vaccinationsprotokol.

— 2/2 angiver afslutningen af en primær vaccinationsserie med 2 doser.

Hvis den primære vaccinationsserie udvides, f.eks. for personer med alvorligt svækket immunforsvar eller i tilfælde, hvor det anbefalede interval mellem de primære doser ikke er blevet overholdt, skal sådanne doser indkodes som yderligere doser, jf. afsnit 5.2.

▼M2

5.2. *Boosterdoser*

Hvis personen modtager doser efter den primære vaccinationsserie, skal sådanne boosterdoser afspejles i de tilsvarende certifikater som følger:

— 2/1 angiver, at der er givet en boosterdosis efter en primær vaccinationsserie med én dosis, eller at der er givet en boosterdosis efter afslutningen af en primær serie bestående af én dosis af en todosisvaccine givet til en restitueret person i overensstemmelse med en medlemsstats vaccinationsprotokol. Derefter skal doser (X), der gives efter den første boosterdosis, angives med (2+X)/(1) > 1 (f.eks. 3/1).

— 3/3 angiver, at der er givet en boosterdosis efter en primær vaccinationsserie med 2 doser. Derefter skal doser (X), der gives efter den første boosterdosis, angives med (3+X)/(3+X) = 1 (f.eks. 4/4).

Medlemsstaterne gennemfører de kodningsregler, der er fastsat i dette afsnit, senest den 1. februar 2022.

Medlemsstaterne skal automatisk eller efter anmodning fra de berørte personer genudstede certifikater, i hvilke indgivelsen af en boosterdosis efter en primær vaccinationsserie med én dosis er kodet på en sådan måde, at den ikke kan skelnes fra afslutningen af den primære vaccinationsserie.

▼M2

I dette bilag skal henvisninger til »boosterdoser« forstås således, at de også omfatter yderligere doser, der gives for bedre at beskytte personer, der udviser utilstrækkelig immunrespons efter afslutningen af den primære vaccinationsserie, der er standard. Medlemsstaterne kan inden for den retlige ramme, der er fastsat ved forordning (EU) 2021/953, træffe foranstaltninger for at håndtere situationen med sårbare grupper, der som prioritet kan modtage yderligere doser. Hvis en medlemsstat f.eks. beslutter kun at give yderligere doser til specifikke undergrupper af befolkningen, kan den i henhold til artikel 5, stk. 1, i forordning (EU) 2021/953 vælge at udstede vaccinationscertifikater med angivelse af disse yderligere doser efter anmodning og ikke automatisk. Hvis der træffes sådanne foranstaltninger, skal medlemsstaterne underrette de pågældende personer herom og om muligheden for fortsat at kunne gøre brug af det certifikat, de modtog efter afslutning af den primære vaccinationsserie.

▼M1

6. **Medlemsstat eller tredjeland, hvor vaccinen er givet/testen er udført**

Foretrukket kodesystem: ISO 3166-landekoder.

Anvendes i certifikat 1, 2 og 3.

Værdisættets indhold: Den fuldstændige liste over koder på 2 bogstaver, der er tilgængelig som et værdisæt som defineret i FHIR (http://hl7.org/fhir/ValueSet/iso3166-1-2). Hvis vaccinen er givet, eller testen er udført af en international organisation (såsom UNHCR eller WHO), og oplysninger om landet ikke er tilgængelige, anvendes koden for organisationen. Sådanne yderligere koder offentliggøres og ajourføres regelmæssigt af Kommissionen med bistand fra e-sundhedsnetværket.

7. **Testtype**

Anvendes i certifikat 2 og certifikat 3, hvis muligheden for udstedelse af restitutionscertifikater på grundlag af andre typer test end NAAT indføres ved en delegeret retsakt.

Følgende koder anvendes:

Kode	Visning på skærm	Kodesystemets navn	Kodesystemets URL	Kodesystemets OID	Kodesystemets version
LP6464-4	Nukleinsyre-amplifikation med brug af probe	LOINC	http://loinc.org	2.16.840.1.113883.6.1	2.69
LP217198-3	Hurtig immunassay	LOINC	http://loinc.org	2.16.840.1.113883.6.1	2.69

▼M4

Koden LP217198-3 (hurtig immunassay) skal anvendes til at angive både hurtige antigentest og laboratoriebaserede antigenassays.

▼M1

8. **Testproducent og handelsbetegnelse for den anvendte test (valgfrit i forbindelse med NAAT-test)**

Anvendes i certifikat 2.

▼M4

Indholdet af værdisættet af antigentest skal omfatte udvalget af antigentest som opført på den fælles og ajourførte liste over covid-19-antigentest, der er udarbejdet på grundlag af Rådets henstilling 2021/C 24/01 og godkendt af Udvalget for Sundhedssikkerhed. Listen holdes ajour af JRC i databasen over testmetoder og udstyr til in vitro-diagnostik af covid-19, som kan tilgås på: https://covid-19-diagnostics.jrc.ec.europa.eu/devices/hsc-common-recognition-rat.

▼M1

I dette kodesystem anvendes relevante felter såsom identifikator for testanordningen, testens navn og testens producent i det strukturerede format, der findes på https://covid-19-diagnostics.jrc.ec.europa.eu/devices.

9. **Testresultat**

Anvendes i certifikat 2.

Følgende koder anvendes:

Kode	Visning på skærm	Kodesystemets navn	Kodesystemets URL	Kodesystemets OID	Kodesystemets version
260415000	Ikke påvist	SNOMED CT	http://snomed.info/sct	2.16.840.1.113883.6.96	2021-01-31
260373001	Påvist	SNOMED CT	http://snomed.info/sct	2.16.840.1.113883.6.96	2021-01-31

▼B

BILAG III

FÆLLES STRUKTUR FOR DEN UNIKKE CERTIFIKATIDENTIFIKATOR

1. **Indledning**

Hvert af EU's digitale covidcertifikater (DCC) skal indeholde en unik certifikatidentifikator (UCI), som understøtter DCC'ernes interoperabilitet. UCI'en kan anvendes til at kontrollere certifikatet. Medlemsstaterne er ansvarlige for indførelsen af UCI'en. UCI'en er et middel til at kontrollere certifikatets ægthed og, hvor det er relevant, til at knytte den til registreringssystem (f.eks. et IIS). Disse identifikatorer skal også gøre det muligt for medlemsstaterne at bekræfte (både på papir og digitalt), at enkeltpersoner er blevet vaccineret eller testet.

2. **Den unikke certifikatidentifikators sammensætning**

UCI'en skal følge en fælles struktur og et fælles format, der øger informationens læsbarhed for mennesker og/eller maskiner og kan vedrøre elementer som f.eks. den medlemsstat, hvor vaccinationen er givet, selve vaccinen og en medlemsstatsspecifik identifikator. Dette giver medlemsstaterne fleksibilitet til at udforme UCI'ens format under fuld overholdelse af databeskyttelseslovgivningen. Rækkefølgen af de separate elementer følger et defineret hierarki, der gør det muligt at foretage fremtidige ændringer af blokkene, samtidig med at deres strukturelle integritet bevares.

De mulige løsninger for UCI'ens sammensætning udgør et spektrum, hvor modularitet og læsbarhed for mennesker udgør de to vigtigste diversificeringsparametre samt et grundlæggende kendetegn:

— Modularitet: i hvilket omfang koden består af særskilte byggeklodser, der indeholder semantisk forskellige oplysninger

— Læsbarhed for mennesker: i hvilket omfang koden giver mening for eller kan læses af en menneskelig læser

— Globalt unik: Identifikatoren for landet eller certificeringscenteret forvaltes nøje, og hvert land (certificeringscenter) forventes at forvalte sit segment af navneområdet nøje ved aldrig at genanvende eller genudstede identifikatorer. Kombinationen heraf sikrer, at hver identifikator er globalt unik.

▼M1

3. **Generelle krav**

Følgende overordnede krav skal opfyldes i forbindelse med UCI'en:

1) Tegnsæt: Kun store bogstaver og alfanumeriske tegn i US-ASCII-tegnsættet (»A« til »Z« og »0« til »9«) er tilladt, suppleret med yderligere specialtegn fra RFC3986 til adskillelse af elementer ([1]): {»/«, »#«, »:«}

2) Maksimal længde: Designerne skal tilstræbe en længde på 27-30 tegn ([2])

3) Versionspræfiks: Dette angiver UCI-skemaets version. Versionspræfikset er »01« for denne version af dokumentet Versionspræfikset består af to cifre

([1]) rfc3986 (ietf.org).

([2]) Med henblik på indførelse med QR-koder kan medlemsstaterne overveje at anvende et ekstra sæt tegn med en samlet længde på 72 tegn (inklusive selve identifikatorens 27-30 tegn) til at inkludere andre oplysninger. Det er op til medlemsstaterne at definere specifikationen for disse oplysninger.

▼M1

4) Landepræfiks: Landekoden angives i overensstemmelse med ISO 3166-1. Længere koder (3 tegn og derover, f.eks. »UNHCR«) er forbeholdt fremtidig brug

5) Kodesuffiks/kontrolsum:

5.1. Medlemsstaterne kan anvende en kontrolsum, hvis der er sandsynlighed for, at overførsel, (menneskelig) transskription eller andre former for korruption kan forekomme (dvs. ved anvendelse i trykt form).

5.2. Kontrolsummen anvendes ikke til validering af certifikatet og er ikke teknisk set en del af identifikatoren, men anvendes til at kontrollere kodens integritet. Kontrolsummen opsummerer hele UCI'en i digitalt/elektronisk overførbart format i henhold til ISO-7812-1 (LUHN-10) ([1]). Kontrolsummen adskilles fra resten af UCI'en med et »#«-tegn.

Bagudkompatibiliteten skal sikres: Medlemsstater, der med tiden ændrer deres identifikatorers struktur (inden for den overordnede version, der i øjeblikket er sat til v1), skal sikre, at alle identiske identifikatorer repræsenterer det samme vaccinationscertifikat/den samme angivelse. Med andre ord kan medlemsstaterne ikke genanvende identifikatorer.

▼B

4. **Muligheder for unikke certifikatidentifikatorer for vaccinationscertifikater**

E-sundhedsnetværkets retningslinjer for kontrollerbare vaccinationscertifikater og grundlæggende interoperabilitetselementer ([2]) giver medlemsstaterne og andre parter forskellige muligheder, som kan anvendes samtidig blandt forskellige medlemsstater. Medlemsstaterne kan anvende disse forskellige muligheder i forskellige versioner af UCI-skemaet.

([1]) Luhn mod N-algoritmen er en udvidelse af Luhn-algoritmen (også kendt som mod 10-algoritmen), der fungerer for numeriske koder og anvendes f.eks. til beregning af kontrolsummen for kreditkort. Denne udvidelse gør det muligt for algoritmen at arbejde med sekvenser af værdier i enhver base (i vores tilfælde alfanumeriske tegn).

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

▼B

BILAG IV

ADMINISTRATION AF OFFENTLIGE NØGLECERTIFIKATER

1. **Indledning**

Sikker og pålidelig udveksling af signaturnøgler til EU's digitale covidcertifikater (DCC'er) mellem medlemsstaterne gennemføres via portalen for EU's digitale covidcertifikat (DCCG), der fungerer som et centralt register for de offentlige nøgler. Via DCCG kan medlemsstaterne offentliggøre de offentlige nøgler svarende til de private nøgler, der anvendes til at signere digitale covidcertifikater. De deltagende medlemsstater kan anvende DCCG til rettidigt at hente ajourført offentligt nøglemateriale. Senere kan DCCG udvides til at omfatte udveksling af pålidelige supplerende oplysninger, som medlemsstaterne stiller til rådighed, f.eks. valideringsregler for DCC'er. Tillidsmodellen for DCC-rammen er en offentlig nøgleinfrastruktur (PKI). Hver medlemsstat har et eller flere nationale signerende certificeringscentre (Country Signing Certification Authorities (CSCA)), hvis certifikater forbliver gyldige i forholdsvis lang tid. Efter medlemsstatens afgørelse kan denne CSCA være den samme eller en anden end den CSCA, der anvendes i forbindelse med maskinlæsbare rejsedokumenter. CSCA udsteder offentlige nøglecertifikater til de nationale, kortlivede dokumentunderskrivere (dvs. underskrivere af DCC'er) i form af dokumentsigneringscertifikater (Document Signer Certificates (DSC'er)). CSCA fungerer som et tillidsanker, således at de deltagende medlemsstater kan anvende CSCA's certifikat til at validere ægtheden og integriteten af de regelmæssigt skiftende DSC'er. Når de er valideret, kan medlemsstaterne videregive disse certifikater (eller blot de offentlige nøgler deri) til deres DCC-valideringsapplikationer. Ud over CSCA'er og DSC'er er DCCG også afhængig af PKI til at autentificere transaktioner og signere data som grundlag for autentificering og som et middel til at sikre integriteten af kommunikationskanalerne mellem medlemsstaterne og DCCG.

Digitale signaturer kan bruges til at opnå dataintegritet og ægthedsbekræftelse. Offentlige nøgleinfrastrukturer skaber tillid ved at knytte offentlige nøgler til bekræftede identiteter (eller udstedere). Dette er nødvendigt for at give andre deltagere mulighed for at kontrollere dataenes oprindelse og kommunikationspartnerens identitet og træffe afgørelse om tillid. I DCCG anvendes flere forskellige offentlige nøglecertifikater til kontrol af ægtheden. I dette bilag defineres det, hvilke offentlige nøglecertifikater der anvendes, og hvordan de skal udformes med henblik på bred interoperabilitet mellem medlemsstaterne. Det indeholder yderligere oplysninger om de nødvendige offentlige nøglecertifikater samt vejledning om certifikatskabeloner og gyldighedsperioder til de medlemsstater, der ønsker at drive deres egen CSCA. Da DCC'ernes ægthed skal kunne kontrolleres inden for en fastsat tidsramme (fra udstedelsen til gyldighedsperiodens udløb), er det nødvendigt at fastlægge en kontrolmodel for alle signaturer, der anvendes i de offentlige nøglecertifikater og DCC'erne.

2. **Terminologi**

Følgende tabel indeholder forkortelser og terminologi, der anvendes i dette bilag.

Udtryk/forkortelse	Definition
Certifikat	Også offentligt nøglecertifikat. Et X.509 v3-certifikat, der indeholder en enheds offentlige nøgle

▼B

Udtryk/forkortelse	Definition
CSCA	Nationalt signerende certificeringscenter (Country Signing Certification Authority)
DCC	EU's digitale covidcertifikat. Et signeret digitalt dokument, der indeholder oplysninger om vaccination, test eller restitution
DCCG	Portalen for EU's digitale covidcertifikat. Dette system anvendes til at udveksle DSC'er mellem medlemsstaterne
$DCCG_{TA}$	DCCG's tillidsanker-certifikat. Den tilsvarende private nøgle anvendes til at signere listen over alle CSCA-certifikater offline
$DCCG_{TLS}$	DCCG's TLS-servercertifikat
DSC	Dokumentsigneringscertifikat (Document Signer Certificate). Et offentligt nøglecertifikat fra en medlemsstats dokumentsigneringscenter (f.eks. et system, der har tilladelse til at signere DCC'er). Dette certifikat udstedes af medlemsstatens CSCA
EC-DSA	Digital signaturalgoritme med elliptisk kurve. En kryptografisk signaturalgoritme baseret på elliptiske kurver
Medlemsstat	En medlemsstat i Den Europæiske Union
mTLS	Gensidig transportlagsikkerhed (mutual TLS). Transportlagssikkerhedsprotokol med gensidig autentificering
NB	En medlemsstats nationale backend
NB_{CSCA}	En medlemsstats CSCA-certifikat (der kan være flere end ét)
NB_{TLS}	Certifikat til TLS-klientautentificering for en national backend
NB_{UP}	Det certifikat, som anvendes af en nationalt backend til at signere datapakker, der uploades til DCCG
PKI	Offentlig nøgleinfrastruktur (Public Key Infrastructure). Tillidsmodel baseret på offentlige nøglecertifikater og certificeringscentre
RSA	Asymmetrisk kryptografisk algoritme baseret på heltalsopløsning, der anvendes til digitale signaturer eller asymmetrisk kryptering

3. **DCCG's kommunikationsstrømme og sikkerhedstjenester**

Dette afsnit giver et overblik over kommunikationsstrømmene og sikkerhedstjenesterne i DCCG-systemet. Ligeledes defineres de nøgler og certifikater, der anvendes til at beskytte kommunikationen, de uploadede oplysninger, DCC'erne og en signeret tillidsliste, der indeholder alle onboardede CSCA-certifikater. DCCG fungerer som et dataknudepunkt, der gør det muligt for medlemsstaterne at udveksle signerede datapakker.

▼B

Uploadede datapakker leveres af DCCG i uændret stand, hvilket betyder, at DCCG ikke tilføjer eller sletter DSC'er fra de pakker, den modtager. Medlemsstaternes nationale backend (*NB*) skal være i stand til at kontrollere end-to-end-integriteten og ægtheden af de uploadede data. Dertil vil de nationale backends og DCCG ud over signaturerne i de udvekslede data anvende gensidig TLS-autentificering til at etablere en sikker forbindelse.

3.1. *Autentificering og etablering af forbindelser*

DCCG anvender transportlagsikkerhed (Transport Layer Security — TLS) med gensidig autentificering til at etablere en autentificeret krypteret kanal mellem medlemsstatens nationale backend (*NB*) og portalens miljø. DCCG har derfor et TLS-servercertifikat (benævnt $DCCG_{TLS}$), og de nationale backends har et TLS-klientcertifikat (benævnt NB_{TLS}). Certifikatskabelonerne findes i afsnit *5*. Alle nationale backends kan udstede deres eget TLS-certifikat. Dette certifikat vil blive udtrykkeligt opført på en positivliste og kan således udstedes af et offentligt pålideligt certificeringscenter (f.eks. et certificeringscenter, der følger de grundlæggende krav i CA/Browser Forum), af en national certifikatmyndighed, eller det kan være selvunderskrevet. Hver medlemsstat er ansvarlig for sine nationale data og for beskyttelsen af den private nøgle, der anvendes til at etablere forbindelsen til DCCG. »Bring your own certificate«-tilgangen kræver en veldefineret registrerings- og identifikationsproces samt procedurer for tilbagekaldelse og fornyelse som beskrevet i afsnit *4.1*, *4.2* og *4.3*. DCCG anvender en positivliste, hvor TLS-certifikater for *NB*'er tilføjes efter vellykket registrering. Kun *NB*'er, der autentificerer sig selv med en privat nøgle, der svarer til et certifikat fra positivlisten, kan etablere en sikker forbindelse til DCCG. DCCG vil også anvende et TLS-certifikat, der gør det muligt for *NB*'erne at kontrollere, at de rent faktisk etablerer forbindelse til den faktiske DCCG og ikke en ondsindet enhed, der udgiver sig for at være DCCG. DCCG's certifikat vil blive udleveret til *NB*'erne efter vellykket registrering. $DCCG_{TLS}$-certifikatet vil blive udstedt af et offentligt pålideligt certificeringscenter (inkluderet i alle større browsere). Det er medlemsstaternes ansvar at kontrollere, at deres forbindelse til DCCG er sikker (f.eks. ved at kontrollere fingeraftrykket i $DCCG_{TLS}$-certifikatet for den server, der oprettes forbindelse til, mod det fingeraftryk, der blev udleveret efter registreringen).

3.2. *Nationalt signerende certificeringscenter (CSCA) og valideringsmodel*

De medlemsstater, der deltager i DCCG-rammen, skal anvende et CSCA til at udstede DSC'er. Medlemsstaterne kan have flere end et CSCA (f.eks. i tilfælde af regional decentralisering). Hver medlemsstat kan enten anvende eksisterende certificeringscentre eller oprette et dedikeret (eventuelt selvsigneret) certificeringscenter for DCC-systemet.

Medlemsstaterne skal forelægge deres CSCA-certifikater(er) for DCCG-operatøren under den officielle onboardingprocedure. Efter vellykket registrering af medlemsstaten (se yderligere oplysninger i afsnit *4.1*) ajourfører DCCG-operatøren en signeret tillidsliste, der indeholder alle CSCA-certifikater, der er aktive inden for DCC-rammen. DCCG-operatøren vil anvende et dedikeret asymmetrisk nøglepar til at signere tillidslisten og certifikaterne i et offlinemiljø. Den private nøgle vil ikke blive lagret på DCCG-onlinesystemet, således at en eventuel sikkerhedsbrist i onlinesystemet ikke gør det muligt for en angriber at bringe tillidslisten i fare. Det tilsvarende tillidsanker-certifikat ($DCCG_{TA}$) stilles til rådighed for de nationale backends under onboardingprocessen.

▼B

Medlemsstaterne kan med henblik på deres verifikationsprocedurer hente tillidslisten fra DCCG. CSCA defineres som det certificeringscenter, der udsteder DSC'er, og medlemsstater, der anvender et hierarki med certificeringscentre i flere niveauer (f.eks. rodcertificeringscenter — > CSCA — > DSC'er), skal derfor stille det underordnede certificeringscenter, der udsteder DSC'erne, til rådighed. Hvis en medlemsstat anvender et eksisterende certificeringscenter, vil DCC-systemet i dette tilfælde ignorere alt over CSCA-niveauet og kun opføre CSCA på positivlisten som tillidsanker (selv om det er en underordnet certificeringscenter). Ligesom i ICAO-modellen giver dette kun mulighed for to niveauer — et »rod«-CSCA og et »blad«-DSC, der kun er signeret af dette CSCA.

Hvis en medlemsstat driver sit eget CSCA, er medlemsstaten ansvarlig for dette certificeringscenters sikre drift og nøgleadministration. CSCA fungerer som tillidsanker for DSC'er, og beskyttelsen af CSCA's private nøgle er derfor afgørende for DCC-miljøets integritet. Verifikationsmodellen i PKI'en for DCC'erne er shell-modellen, hvori det hedder, at alle certifikater ved valideringen af certifikatstien skal være gyldige på et givet tidspunkt (dvs. på tidspunktet for signaturvalideringen). Der gælder derfor følgende begrænsninger:

— CSCA må ikke udstede certifikater, der er gyldige i længere tid end certificeringscenterets eget certifikat.

— Dokumentunderskriveren må ikke signere dokumenter, der er gyldige i længere tid end dokumentunderskrivercertifikatet (DSC).

— Medlemsstater, der driver deres eget CSCA, skal fastsætte gyldighedsperioder for deres CSCA og alle udstedte certifikater, og de skal sørge for fornyelse af certifikater.

Anbefalinger vedrørende gyldighedsperioder kan ses i afsnit *4.2*.

3.3. *De uploadede datas integritet og ægthed*

De nationale backends kan bruge DCCG til at uploade og downloade digitalt signerede datapakker efter vellykket gensidig autentificering. I begyndelsen indeholder disse datapakker medlemsstaternes DSC'er. Det nøglepar, der anvendes af den nationale backend til digital signatur af datapakker ved upload til DCCG-systemet, kaldes den nationale backends uploadsignaturnøglepar, og det tilsvarende offentlige nøglecertifikat benævnes NB_{UP}-certifikatet. Hver medlemsstat har sit eget NB_{UP}-certifikat, som kan være selvsigneret eller udstedt af et eksisterende certificeringscenter, såsom et offentligt certificeringscenter (dvs. et certificeringscenter, der udsteder certifikater i overensstemmelse med CA/Browser Forums basiskrav). NB_{UP}-certifikatet skal være forskelligt fra alle andre certifikater, der anvendes af medlemsstaten (dvs. CSCA-certifikater, TLS-klient-certifikater og DSC'er).

Medlemsstaterne skal udlevere uploadcertifikatet til DCCG-operatøren under den indledende registreringsprocedure (se yderligere oplysninger i afsnit *4.1*). Hver medlemsstat er ansvarlig for sine nationale data og for beskyttelsen af den private nøgle, der anvendes til signatur ved upload.

Andre medlemsstater kan kontrollere de signerede datapakker ved hjælp af uploadcertifikaterne fra DCCG. DCCG kontrollerer ægtheden og integriteten af de uploadede data mod *NB*'s uploadcertifikat, inden dataene stilles til rådighed for andre medlemsstater.

▼B

3.4. *Krav til den tekniske DCCG-arkitektur*

Kravene til den tekniske DCCG-arkitektur er som følger:

— DCCG anvender gensidig TLS-autentificering til at etablere en autentificeret krypteret forbindelse til *NB*'erne. DCCG fører derfor en positivliste over registrerede NB_{TLS}-klientcertifikater

— DCCG anvender to digitale certifikater ($DCCG_{TLS}$ og $DCCG_{TA}$) med to særskilte nøglepar. Den private nøgle i nøgleparret for $DCCG_{TA}$ opbevares offline (ikke på DCCG's onlinekomponenter)

— DCCG fører en tillidsliste over de NB_{CSCA}-certifikater, der er underskrevet med den private $DCCG_{TA}$-nøgle.

— Krypteringen, der anvendes, skal opfylde kravene i afsnit *5.1*.

4. **Administration af certifikaters livscyklus**

4.1. *Registrering af nationale backends*

Medlemsstaterne skal registrere sig hos DCCG-operatøren for at deltage i DCCG-systemet. I dette afsnit beskrives den tekniske og operationelle procedure, der skal følges ved registrering af en national backend.

DCCG-operatøren og medlemsstaten skal udveksle oplysninger om tekniske kontaktpersoner i forbindelse med onboardingprocessen. Det antages, at de tekniske kontaktpersoner er legitimeret af deres medlemsstater, og at identifikation/autentificering heraf foretages via andre kanaler. Autentificeringen kan f.eks. gennemføres ved, at en medlemsstats tekniske kontakt leverer certifikaterne som password-krypterede filer via e-mail og deler det tilknyttede password med DCCG-operatøren via telefon. Der kan også anvendes andre sikre kanaler, som DCCG-operatøren har defineret.

Medlemsstaten skal indgive tre digitale certifikater under registrerings- og identifikationsprocessen:

— Medlemsstatens TLS-certifikat (NB_{TLS})

— Medlemsstatens uploadcertifikat (NB_{UP})

— Medlemsstatens CSCA-certifikat(er) (NB_{CSCA}).

Alle indgivne certifikater skal opfylde de krav, der er fastsat i afsnit *5*. DCCG-operatøren skal kontrollere, at de indgivne certifikater opfylder kravene i afsnit *5*. Efter identifikationen og registreringen skal DCCG-operatøren:

— tilføje NB_{CSCA}-certifikatet eller -certifikaterne til den tillidsliste, der er underskrevet med den private nøgle, som svarer til den offentlige nøgle i $DCCG_{TA}$

— tilføje NB_{TLS}-certifikatet til positivlisten for slutpunktet for $DCCG_{TLS}$

— tilføje NB_{UP}-certifikatet til DCCG-systemet

— stille de offentlige $DCCG_{TA}$- og $DCCG_{TLS}$-nøglecertifikater til rådighed for medlemsstaten.

▼B

4.2. *Certificeringscentre, gyldighedsperioder og fornyelse*

En medlemsstats CSCA-certifikater kan være selvsignerede, såfremt medlemsstaten ønsker at drive sit eget CSCA. Det fungerer som medlemsstatens tillidsanker, og derfor skal medlemsstaten indføre kraftig beskyttelse af den private nøgle, der svarer til CSCA's offentlige nøgle. Det anbefales, at medlemsstaterne anvender et offlinesystem til deres CSCA, dvs. et computersystem, der ikke er tilsluttet noget netværk. Der skal anvendes flerpersonskontrol til at få adgang til systemet (f.eks. efter »fire øjne«-princippet). Efter signering af DSC'er skal der anvendes operationelle kontroller, og det system, der ligger inde med den private CSCA-nøgle, skal opbevares sikkert med strenge adgangskontroller. Hardwaresikkerhedsmoduler eller chipkort kan anvendes til at beskytte den private CSCA-nøgle yderligere. Digitale certifikater indeholder en gyldighedsperiode, der gør det nødvendigt at forny dem. Certifikaterne skal fornyes for at anvende nye kryptografiske nøgler og tilpasse nøglestørrelserne i tilfælde af, at stigende computerkraft eller nye former for angreb truer sikkerheden af den anvendte kryptografiske algoritme. Shell-modellen anvendes (se afsnit *3.2*).

Følgende gyldighedsperioder anbefales i betragtning af de digitale covid-certifikaters gyldighedsperiode på ét år:

— CSCA: 4 år

— DSC: 2 år

— Upload: 1-2 år

— Autentificering af TLS-klient: 1-2 år

Med henblik på en rettidig fornyelse anbefales følgende anvendelsesperioder for de private nøgler:

— CSCA: 1 år

— DSC: 6 måneder

Medlemsstaterne skal oprette nye uploadcertifikater og TLS-certifikater rettidigt, f.eks. en måned før udløbet, for at forhindre problemer med driften. CSCA-certifikater og DSC'er bør fornyes mindst en måned, inden anvendelsen af den private nøgle ophører (under hensyntagen til de påkrævede operationelle procedurer). Medlemsstaterne skal levere ajourførte CSCA-, upload- og TLS-certifikater til DCCG-operatøren. Udløbne certifikater fjernes fra positivlisten og tillidslisten.

Medlemsstaterne og DCCG-operatøren skal føre tilsyn med gyldigheden af deres egne certifikater. Der er ingen central enhed, der fører tilsyn med certifikaternes gyldighed eller underretter deltagerne herom.

▼B

4.3. *Tilbagekaldelse af certifikater*

Generelt kan digitale certifikater tilbagekaldes af deres udstedende certificeringscenter ved hjælp af certifikattilbagekaldelseslister eller en Online Certificate Status Protocol Responder (OCSP). CSCA'erne for DCC-systemet bør stille lister over certifikattilbagekaldelser (CRL'er) til rådighed. Selv hvis disse CRL'er i øjeblikket ikke anvendes af andre medlemsstater, bør de integreres med henblik på fremtidig anvendelse. Hvis et CSCA beslutter ikke at stille CRL'er til rådighed, skal dette CSCA's DSC'er fornyes, når CRL'erne bliver obligatoriske. Kontrollører bør ikke anvende OCSP til validering af DSC'er og bør i stedet anvende CRL'er. Det anbefales, at den nationale backend udfører den nødvendige validering af DSC'er, der downloades fra DCCG, og kun fremsender et sæt pålidelige og validerede DSC'er til de nationale DCC-validatorer. DCC-validatorerne bør i deres valideringsproces ikke udføre tilbagekaldelseskontrol af DSC'er. En af grundene hertil er at beskytte DCC-indehavernes privatliv ved at undgå enhver risiko for, at anvendelsen af en bestemt DSC overvåges af dens tilknyttede OCSP Responder.

Medlemsstaterne kan selv fjerne deres DSC'er fra DCCG ved hjælp af gyldige upload- og TLS-certifikater. Fjernelsen af en DSC indebærer, at alle DCC'er, der er udstedt med denne DSC, bliver ugyldige, når medlemsstaterne henter de ajourførte DSC-lister. Beskyttelsen af DSC'ers tilsvarende private nøglemateriale er af afgørende betydning. Medlemsstaterne skal underrette DCCG-operatøren, når upload- eller TLS-certifikater skal tilbagekaldes, f.eks. hvis der opstår en sikkerhedsbrist i den nationale backend. DCCG-operatøren kan derefter fjerne tilliden til det berørte certifikat, f.eks. ved at fjerne det fra TLS-positivlisten. DCCG-operatøren kan fjerne uploadcertifikaterne fra DCCG-databasen. Pakker, der er signeret med disse uploadcertifikaters tilsvarende private nøgle, bliver ugyldige, når de nationale backends fjerner tilliden til det tilbagekaldte uploadcertifikat. Hvis et CSCA-certifikat skal tilbagekaldes, underretter medlemsstaterne DCCG-operatøren og de andre medlemsstater, som de har et tillidsforhold til. DCCG-operatøren vil derefter udstede en ny tillidsliste, hvori det pågældende certifikat ikke længere er indeholdt. Alle DSC'er udstedt af denne CSCA bliver ugyldige, når medlemsstaterne ajourfører tillidslageret i deres nationale backend. Hvis $DCCG_{TLS}$- eller $DCCG_{TA}$-certifikatet skal tilbagekaldes, skal DCCG-operatøren og medlemsstaterne samarbejde om at oprette en ny pålidelig TLS-forbindelse og tillidsliste.

5. **Certifikatskabeloner**

Dette afsnit indeholder kryptografiske krav og kryptografisk vejledning samt krav til certifikatskabeloner. Certifikatskabelonerne for DCCG-certifikaterne defineres i dette afsnit.

5.1. *Kryptografiske krav*

Kryptografiske algoritmer og TLS-kryptering skal vælges på grundlag af de gældende anbefalinger fra det tyske forbundskontor for informationssikkerhed (BSI) eller SOG-IS. Disse anbefalinger og anbefalingerne fra andre institutioner og standardiseringsorganisationer ligner hinanden. Anbefalingerne findes i de tekniske retningslinjer TR 02102-1 og TR 02102-2 ([1]) eller *SOG-IS Agreed Cryptographic Mechanisms* ([2]).

([1]) BSI - Tekniske retningslinjer TR-02102 (bund.de)
([2]) SOG-IS - Dokumentation (sogis.eu)

▼B

5.1.1. Krav til DSC

Kravene i bilag I, afsnit *3.2.2*, finder anvendelse. Det anbefales derfor kraftigt, at dokumentunderskrivere anvender den digitale signaturalgoritme med elliptisk kurve (EC-DSA) NIST-p-256 (som defineret i tillæg D til FIPS PUB 186-4). Andre elliptiske kurver understøttes ikke. På grund af DCC's pladsbegrænsninger bør medlemsstaterne ikke anvende RSA-PSS, selv om den er tilladt som reservealgoritme. Hvis medlemsstaterne anvender RSA-PSS, bør modulo være på 2048 eller højst 3072 bit. SHA-2 med en outputlængde på ≥ 256 bit skal anvendes som kryptografisk hashfunktion (se ISO/IEC 10118-3:2004) for DSC-signaturen.

5.1.2. Krav til TLS-, upload- og CSCA-certifikater

For digitale certifikater og kryptografiske signaturer i DCCG-sammenhæng er de vigtigste krav til kryptografiske algoritmer og nøglelængde opsummeret i følgende tabel (pr. 2021):

Signaturalgoritme	Nøglestørrelse	Hashfunktion
EC-DSA	Min. 250 bit	SHA-2 med en outputlængde på ≥ 256 bit
RSA-PSS (udfyldning anbefalet) RSA-PKCS#1 v1.5 (nedarvet udfyldning)	RSA modulo (N) på min. 3000 bit med offentlig eksponent e > 2^16	SHA-2 med en outputlængde på ≥ 256 bit
DSA	Primtal p på min. 3000 bit, nøgle q på 250 bit	SHA-2 med en outputlængde på ≥ 256 bit

Den anbefalede elliptiske kurve til EC-DSA er NIST-p-256 på grund af dens udbredte anvendelse.

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

Nedenstående tabel giver vejledning vedrørende skabelonen for NB_{CSCA}-certifikatet, hvis en medlemsstat beslutter at drive sin egen CSCA til DCC-systemet.

Angivelser med **fed skrift** er påkrævede (skal indgå i certifikatet), og angivelser med *kursiv* anbefales (bør indgå i certifikatet). For tomme felter er der ikke defineret nogen anbefalinger.

Felt	Værdi
Emne	**cn=<unikt fællesnavn, der ikke må være tomt>,***o*=<*Udbyder*>,**c=<medlemsstat, der driver pågældende CSCA>**
Nøgleanvendelse	**certifikatsignatur,***CRL-signatur* (som minimum)
Basisbegrænsninger	**CA = sand, stilængdebegrænsninger = 0**

Feltet for emnets navn må ikke være tomt, og navnet skal være unikt inden for den angivne medlemsstat. Landekoden (c) skal svare til den medlemsstat, der skal anvende dette CSCA-certifikat. Certifikatet skal indeholde en unik identifikator til emnenøgle (SKI) i henhold til RFC 5280 ([1]).

([1]) rfc5280 (ietf.org)

▼B

5.3. *Dokumentsigneringscertifikat (DSC)*

Følgende tabel indeholder vejledning om DSC. Angivelser med **fed skrift** er påkrævede (skal indgå i certifikatet), og angivelser med *kursiv* anbefales (bør indgå i certifikatet). For tomme felter er der ikke defineret nogen anbefalinger.

Felt	Værdi
Serienummer	**unikt serienummer**
Emne	**cn=<unikt fællesnavn, der ikke må være tomt>,***o*=<*Udbyder*>,**c=<medlemsstat, der anvender dette DSC>**
Nøgleanvendelse	**digital signatur** (som minimum)

DSC'et skal signeres med en privat nøgle, der svarer til et CSCA-certifikat, som anvendes af medlemsstaten.

Følgende udvidelser skal anvendes:

— Certifikatet skal indeholde en nøgleidentifikator (Authority Key Identifier — AKI), der svarer til identifikatoren for emnenøglen (Subject Key Identifier — SKI) i det udstedende CSCA-certifikat

— Certifikatet bør indeholde en unik identifikator til emnenøgle (SKI) i overensstemmelse med RFC 5280 ([1]).

Certifikatet bør desuden indeholde CRL-distributionspunktudvidelsen med henvisning til listen over tilbagekaldte certifikater (CRL), som stilles til rådighed af det CSCA, der udstedte DSC'en.

DSC'en kan indeholde en udvidet nøgleanvendelsesudvidelse med nul eller flere nøglepolitikidentifikatorer, som begrænser antallet af HCERT-typer, som dette certifikat har lov til at kontrollere. Hvis der findes en eller flere, kontrollerer kontrollørerne nøgleanvendelsen i forhold til den lagrede HCERT. Med henblik herpå defineres følgende værdier for udvidet nøgleanvendelse:

Felt	Værdi
extendedKeyUsage	1.3.6.1.4.1.1847.2021.1.1 for udstedere i forbindelse med test
extendedKeyUsage	1.3.6.1.4.1.1847.2021.1.2 for udstedere i forbindelse med vaccine
extendedKeyUsage	1.3.6.1.4.1.1847.2021.1.3 for udstedere i forbindelse med restitution

Hvis der ikke foreligger nogen nøgleanvendelsesudvidelse (dvs. ingen udvidelser eller udvidelser med værdien nul), kan dette certifikat anvendes til at validere enhver type HCERT. Andre dokumenter kan definere relevante yderligere udvidelser til identifikatorer for nøgleanvendelsespolitik, der anvendes i forbindelse med validering af HCERT'er.

5.4. *Uploadcertifikater (NB_{UP})*

Nedenstående tabel indeholder vejledning om den nationale backends uploadcertifikat. Angivelser med **fed skrift** er påkrævede (skal indgå i certifikatet), og angivelser med *kursiv* anbefales (bør indgå i certifikatet). For tomme felter er der ikke defineret nogen anbefalinger.

([1]) rfc5280 (ietf.org)

▼B

Felt	Værdi
Emne	**cn=<unikt fællesnavn, der ikke må være tomt>,***o*=<*Udbyder*>,**c=<medlemsstat, der anvender dette uploadcertifikat>**
Nøgleanvendelse	**digital signatur** (som minimum)

5.5. *TLS-klientautentificering for den nationale backend (NB_{TLS})*

Nedenstående tabel indeholder vejledning om den nationale backends certifikat til TLS-klientautentificering. Angivelser med **fed skrift** er påkrævede (skal indgå i certifikatet), og angivelser med *kursiv* anbefales (bør indgå i certifikatet). For tomme felter er der ikke defineret nogen anbefalinger.

Felt	Værdi
Emne	**cn=<unikt fællesnavn, der ikke må være tomt>,***o*=<*Udbyder*>,**c=<*NB*'ens medlemsstat>**
Nøgleanvendelse	**digital signatur** (som minimum)
Udvidet nøgleanvendelse	klientautentificering (1.3.6.1.5.5.7.3.2)

Certifikatet kan også indeholde *serverautentificeringen for den udvidede nøgleanvendelse (1.3.6.1.5.5.7.3.1)*, men dette er ikke påkrævet.

5.6. *Certifikat for signatur af tillidslisten ($DCCG_{TA}$)*

Følgende tabel definerer DCCG's tillidsanker-certifikat.

Felt	Værdi
Emne	**cn = portal for det digitale grønne certifikat** ([1])**, o = <udbyder>, c = <land>**
Nøgleanvendelse	**digital signatur** (som minimum)

5.7. *DCCG's TLS-servercertifikater ($DCCG_{TLS}$)*

Følgende tabel definerer DCCG's TLS-certifikat.

Felt	Værdi
Emne	CN = < FQDN eller DCCG's IP-adresse>, o = <udbyder>, c = <land>
SubjectAltName	dNSName: <navn på DCCG's DNS> eller iPAddress: <DCCG's IP-adresse>
Nøgleanvendelse	**digital signatur** (som minimum)
Udvidet nøgleanvendelse	serverautentificering(1.3.6.1.5.5.7.3.1)

([1]) Udtrykket »digitalt grønt certifikat« er bibeholdt i stedet for »EU's digitale covidcertifikat« i denne sammenhæng, fordi det er den terminologi, der er blevet fast indkodet og anvendt i certifikatet, inden medlovgiverne traf afgørelse om ny terminologi.

▼B

Certifikatet kan også indeholde *klientautentificeringen for den udvidede nøgleanvendelse (1.3.6.1.5.5.7.3.2)*, men dette er ikke påkrævet.

DCCG's TLS-certifikat skal udstedes af et offentligt pålideligt certificeringscenter (som er inkluderet i alle større browsere og operativsystemer og følger de grundlæggende krav i CA/Browser Forum)

▼M1

BILAG V

JAVASCRIPT OBJECT NOTATION (JSON)-SKEMA

1. **Indledning**

I dette bilag fastsættes den tekniske datastruktur for EU's digitale covidcertifikater, gengivet som et JSON-skema. Dokumentet indeholder specifikke instruktioner vedrørende de enkelte datafelter.

2. **JSON-skema — placering og versioner**

Det autoritative officielle JSON-skema for EU's digitale covidcertifikat er tilgængeligt på https://github.com/ehn-dcc-development/ehn-dcc-schema. Andre placeringer er ikke autoritative, men kan bruges til forberedelse af kommende revisioner.

Som standard vises den aktuelle version, der er fastsat i dette bilag og bruges af alle lande, under den angivne URL.

Den kommende version, der skal understøttes af alle lande inden en bestemt dato, er vist under den anførte URL version tagging og beskrevet mere specifikt i Readme-filen.

▼M3

3. **Fælles strukturer og generelle krav**

EU's digitale covidcertifikater udstedes ikke, hvis ikke alle datafelter grundet manglende oplysninger kan udfyldes korrekt i overensstemmelse med nærværende specifikation. **Dette påvirker ikke medlemsstaternes forpligtelse til at udstede digitale covidcertifikater.**

Oplysningerne i alle felter kan udfyldes ved anvendelse af det fulde sæt UNICODE 13.0-tegn kodet i UTF-8, medmindre der er specifikke begrænsninger af værdisættene eller et smallere sæt tegn.

Den fælles struktur skal være som følger:

»JSON«:{

»ver«:<oplysninger om version>,

»nam«:{

<oplysninger om navn>

},

»dob«:<fødselsdato>,

»v« eller »t« eller »r«: [

{<oplysninger om vaccinedosis, test eller restitution, én indkodning>}

]

}

Detaljerede oplysninger om individuelle grupper og felter følger i nedenstående afsnit.

Hvis reglerne foreskriver, at et felt skal springes over, betyder det, at indholdet skal være tomt, og at hverken feltets navn eller værdi må optræde i indholdet.

▼M3

3.1. *Version*

Oplysninger om version skal fremgå. Versioneringen følger Semantic Versioning (semver: https://semver.org). Den version, der bruges, skal det være en af de offentliggjorte versioner (nuværende eller tidligere offentliggjort version). Se afsnit JSON Schema location for yderligere oplysninger.

Felt-ID	Feltnavn	Instrukser
ver	Version af skema	Skal svare til identifikatoren for den version af skemaet, der anvendes til udarbejdelse af EU's digitale covidcertifikat. Eksempel: »ver«:»1.3.0«

3.2. *Personens navn og fødselsdato*

Personens navn er personens fulde officielle navn, der svarer til det navn, der fremgår af rejsedokumenter. Strukturens identifikator er *nam*. Præcis 1 (ét) navn skal angives.

Felt-ID	Feltnavn	Instrukser
nam/fn	Efternavn(e)	Indehavers efternavn(e). Hvis indehaveren ikke har noget efternavn, men har et fornavn, springes feltet over. I alle andre tilfælde skal der angives præcis 1 (ét) ikketomt felt, indeholdende alle efternavne. I tilfælde af flere efternavne skal disse adskilles med mellemrum. Kombinerede navne, herunder med bindestreger eller lignende tegn, skal imidlertid ikke ændres. Eksempler: »fn«:»Musterfrau-Gößinger« »fn«:»Musterfrau-Gößinger Müller«
nam/fnt	Standardiseret/standardiserede efternavn(e)	Indehaverens efternavn(e) translittereret efter samme regel som den, der er brugt til indehaverens maskinlæsbare rejsedokumenter (såsom de regler, der er fastsat i ICAO-dokument 9303, del 3). Hvis indehaveren ikke har noget efternavn, men har et fornavn, springes feltet over. I alle andre tilfælde skal der angives præcis 1 (ét) ikketomt felt, udelukkende indeholdende tegnene A-Z og <. Maksimal længde: 80 tegn (jf. ICAO-specifikation 9303). Eksempler: »fnt«:»MUSTERFRAU<GOESSINGER« »fnt«:»MUSTERFRAU<GOESSINGER<MUELLER«
nam/gn	Fornavn(e)	Fornavn(e) på indehaveren. Hvis indehaveren ikke har noget fornavn, men har et efternavn, springes feltet over. I alle andre tilfælde skal der angives præcis 1 (ét) ikketomt felt, indeholdende alle fornavne. I tilfælde af flere fornavne skal disse adskilles med mellemrum. Eksempel: »gn«:»Isolde Erika«

▼M3

Felt-ID	Feltnavn	Instrukser
nam/gnt	Standardiseret/standardiserede fornavn(e)	Indehaverens fornavn(e) translittereret efter samme regel som den, der er brugt til indehaverens maskinlæsbare rejsedokumenter (såsom de regler, der er fastsat i ICAO-dokument 9303, del 3). Hvis indehaveren ikke har noget fornavn, men har et efternavn, springes feltet over. I alle andre tilfælde skal der angives præcis 1 (ét) ikketomt felt, udelukkende indeholdende tegnene A-Z og <. Maksimal længde: 80 tegn. Eksempel: »gnt«:»ISOLDE<ERIKA«
dob	Fødselsdato	Fødselsdato på indehaveren af EU's digitale covidcertifikat. Fuldstændig eller delvis dato uden klokkeslæt, begrænset til intervallet fra 1900-01-01 til 2099-12-31. Præcis 1 (ét) ikketomt felt skal angives, hvis den fuldstændige eller delvise fødselsdato er kendt. Hvis fødselsdatoen ikke er kendt, heller ikke delvist, skal feltet udfyldes med en tom streng »«. Dette bør stemme overens med oplysningerne i rejsedokumenterne. Et af de følgende ISO 8601-formater skal anvendes, hvis fødselsdatoen er kendt. Andre muligheder understøttes ikke. ÅÅÅÅ-MM-DD ÅÅÅÅ-MM ÅÅÅÅ (Kontrolapplikationen kan vise manglende dele af fødselsdatoen ved at anvende XX-reglen ligesom i maskinlæsbare rejsedokumenter, f.eks. 1990-XX-XX.) Eksempler: »dob«:»1979-04-14« »dob«:»1901-08« »dob«:»1939« »dob«:»«

3.3. *Grupper for oplysninger, der er specifikke for certifikattypen*

JSON-skemaet understøtter tre grupper af indkodninger, der omfatter oplysninger, som er specifikke for certifikattypen. Hvert digitalt covidcertifikat skal indeholde præcis 1 (én) gruppe. Tomme grupper er ikke tilladt.

Gruppeidentifikator	Gruppens navn	Indkodninger
v	Vaccinationsgruppe	Skal, hvis den findes, indeholde præcis 1 (én) indkodning, der præcis beskriver 1 (én) vaccinedosis (én dosis).
t	Testgruppe	Skal, hvis den findes, indeholde præcis 1 (én) indkodning, der præcis beskriver 1 (ét) et testresultat.
r	Restitutionsgruppe	Skal, hvis den findes, indeholde præcis 1 (én) indkodning, der beskriver 1 (én) oplysning om restitution.

▼M1

4. **Oplysninger, der er specifikke for diverse certifikattyper**

4.1. *Vaccinationscertifikat*

Vaccinationsgruppen skal, hvis den findes, indeholde præcis 1 (én) indkodning, der præcis beskriver én vaccination (én dosis). Alle elementer i vaccinationsgruppen er obligatoriske, og tomme værdier understøttes ikke.

▼**M1**

Felt-ID	Feltnavn	Vejledning
v/tg	Målsygdom eller -agens: Covid-19 (sars-CoV eller en variant heraf)	En kodet værdi fra værdisættet disease-agent-targeted.json. Denne værdi indkodes som 840539006, der er koden for covid-19 fra SNOMED CT (GPS). Præcis 1 (ét) ikketomt felt skal angives. Eksempel: "tg": "840539006"
v/vp	Covid-19-vaccine eller -profylakse	Type af anvendt vaccine eller profylakse. En kodet værdi fra værdisættet vaccine-prophylaxis.json. Værdisættet stammer fra portalen for EU's digitale covidcertifikat. Præcis 1 (ét) ikketomt felt skal angives. Eksempel: "vp": "1119349007" (en SARS-CoV-2 mRNA-vaccine)
v/mp	Covid-19-vaccineprodukt	Lægemiddel anvendt til denne specifikke vaccinedosis. ►**M4** En kodet værdi fra værdisættet vaccine-medicinal-product.json. Eller en kodet værdi, der henviser til et klinisk forsøg, og som følger reglen i punkt 3 i bilag II. ◄ Værdisættet stammer fra portalen for EU's digitale covidcertifikat. Præcis 1 (ét) ikke tomt felt skal angives. Eksempel: "mp": "EU/1/20/1528" (Comirnaty)
v/ma	Indehaver af markedsføringstilladelse for covid-19-vaccine eller covid-19-vaccineproducent	Indehaver af markedsføringstilladelse eller producent, hvis der ikke er nogen indehaver af markedsføringstilladelse. ►**M4** En kodet værdi fra værdisættet vaccine-mah-manf.json. Eller en kodet værdi, der henviser til et klinisk forsøg, og som følger reglen i punkt 4 i bilag II. ◄ Værdisættet stammer fra portalen for EU's digitale covidcertifikat. Præcis 1 (ét) ikke tomt felt skal angives. Eksempel: "ma": "ORG-100030215" (Biontech Manufacturing GmbH)
v/dn	Nummer i en række af doser	Sekvensnummer (positivt heltal) på den dosis, der gives ved vaccinationen. 1 for den første dosis, 2 for anden dosis etc. Mere specifikke regler findes i bilag II, afsnit 5. Præcis 1 (ét) ikketomt felt skal angives. Eksempler: "dn": "1" (første dosis) "dn": "2" (anden dosis) "dn": "3" (tredje dosis)
v/sd	Det samlede antal doser i serien.	Det samlede antal doser (positivt heltal) i vaccinationsserien. Mere specifikke regler findes i bilag II, afsnit 5. Præcis 1 (ét) ikketomt felt skal angives. Eksempler: "sd": "1" (i tilfælde af en primær vaccinationsserie med 1 dosis) "sd": "2" (i tilfælde af en primær vaccinationsserie med 2 doser eller en yderligere dosis efter en primær vaccinationsserie med 1 dosis) "sd": "3 "(f.eks. i tilfælde af en yderligere dosis efter en primær vaccinationsserie med 2 doser)

▼**M1**

Felt-ID	Feltnavn	Vejledning
v/dt	Vaccinationsdato	Datoen, hvor den beskrevne dosis er givet, i formatet ÅÅÅÅ-MM-DD (fuldstændig dato uden klokkeslæt). Andre formater understøttes ikke. Præcis 1 (ét) ikketomt felt skal angives. Eksempel: "dt": "2021-03-28"
v/co	Medlemsstat eller tredjeland, hvor vaccinen er givet	Land udtrykt som en ISO3166-kode på 2 bogstaver (ANBEFALET) eller en henvisning til en international organisation, der er ansvarlig for vaccinationen (såsom UNHCR eller WHO). En kodet værdi fra værdisættet country-2-codes.json. Værdisættet stammer fra portalen for EU's digitale covidcertifikat. Præcis 1 (ét) felt skal angives. Eksempel: "co": "CZ" "co": "UNHCR"
v/is	Udsteder af certifikat	Navn på den organisation, der har udstedt certifikatet. Identifikatorer er tilladt som del af navnet, men det anbefales ikke at bruge dem særskilt uden navnet som tekst. Maksimalt 80 UTF-8-tegn. Præcis 1 (ét) ikketomt felt skal angives. Eksempel: "is": "Den Tjekkiske Republiks Sundhedsministerium" "is": "Vaccinationscenter Syd 3"
v/ci	Unik certifikatidentifikator	Unik certifikatidentifikator som beskrevet på https://ec.europa.eu/health/sites/default/files/ehealth/docs/vaccination-proof_interoperability-guidelines_en.pdf. Det er valgfrit at medtage kontrolsummen. Præfikset "URN:UVCI:" kan tilføjes. Præcis 1 (ét) ikketomt felt skal angives. Eksempler: "ci": "URN:UVCI:01:NL:187/37512422923" "ci": "URN:UVCI:01:AT:10807843F94AEE0EE5093FBC254BD813#B"

4.2. *Testcertifikat*

Testgruppen skal, hvis den findes, indeholde præcis 1 (én) indkodning, der præcis beskriver ét testresultat.

Felt-ID	Feltnavn	Vejledning
t/tg	Målsygdom eller -agens: Covid-19 (sars-CoV eller en variant heraf)	En kodet værdi fra værdisættet disease-agent-targeted.json. Denne værdi indkodes som 840539006, der er koden for COVID-19 fra SNOMED CT (GPS). Præcis 1 (ét) ikke tomt felt skal angives. Eksempel: "tg": "840539006"
t/tt	Testtype	Type anvendt test, baseret på det materiale, der testes. En kodet værdi fra værdisættet test-type.json (baseret på LOINC). Værdier uden for værdisættet er ikke tilladt. Præcis 1 (ét) ikke tomt felt skal angives. Eksempel: "tt": "LP6464-4" (Nukleinsyre-amplifikation med brug af probe) "tt": "LP217198-3" (Hurtig immunassay)

▼M1

Felt-ID	Feltnavn	Vejledning
t/nm	Testnavn (kun test med nukleinsyre-amplifikation)	Navn på den anvendte test med nukleinsyre-amplifikation (NAAT). Navnet bør indeholde navnet på testproducenten og testens handelsbetegnelse, adskilt med komma. For NAAT: Dette felt er valgfrit. ►M4 For antigentest: Dette felt skal ikke anvendes, da navnet på testen tilvejebringes indirekte via identifikatoren for testanordningen (t/ma). ◄ Når det foreligger, skal feltet ikke være tomt. Eksempel: "nm": "ELITechGroup, SARS-CoV-2 ELITe MGB® Kit"
▼M4 **t/ma**	Identifikator for testanordning (kun antigentest)	Identifikator fra JRC-databasen for anordning til brug ved antigentest. Værdisæt (HSC's fælles liste): — Alle antigentest på HSC's fælles liste (menneskeligt læsbar). — https://covid-19-diagnostics.jrc.ec.europa.eu/devices/hsc-common-recognition-rat (maskinlæsbar, værdier for feltet id_device inkluderet på listen udgør værdisættet). I EU-/EØS-landene skal udstedere kun udstede certifikater for test, der er knyttet til et aktuelt gyldigt værdisæt. Værdisættet ajourføres hver 24. time. Værdier uden for værdisættet kan bruges i certifikater udstedt af tredjelande, men identifikatorerne skal stamme fra JRC-databasen. Brug af andre identifikatorer såsom dem, der kommer direkte fra testproducenterne, er ikke tilladt. Kontrolapplikationen skal opfange værdier, der ikke stammer fra det ajourførte værdisæt, og behandle certifikater indeholdende disse værdier som ugyldige. Hvis en identifikator fjernes fra værdisættet, kan certifikater indeholdende denne identifikator godkendes i en periode på maksimalt 72 timer efter, at denne identifikator er blevet fjernet. Værdisættet stammer fra portalen for EU's digitale covidcertifikat. For antigentest: Præcis 1 (ét) ikketomt felt skal angives. For NAAT: Feltet skal ikke anvendes, heller ikke selv om identifikatoren for NAAT-testen er tilgængelig i JRC-databasen. Eksempel: »ma«: »344« (SD BIOSENSOR Inc, STANDARD F COVID-19 Ag FIA)
▼M1 **t/sc**	Dato og klokkeslæt for prøveudtagning	Den dato og det klokkeslæt, hvor prøven blev udtaget. Klokkeslættet skal indeholde oplysninger om tidszone. Værdien skal ikke angive det klokkeslæt, hvor testresultatet blev genereret. Præcis 1 (ét) ikke tomt felt skal angives. Et af følgende ISO 8601-formater skal anvendes. Andre muligheder understøttes ikke. ÅÅÅÅ-MM-DDTtt:mm:ssZ ÅÅÅÅ-MM-DDTtt:mm:ss[+-]tt

▼**M1**

Felt-ID	Feltnavn	Vejledning
		ÅÅÅÅ-MM-DDTtt:mm:ss[+-]ttmm ÅÅÅÅ-MM-DDTtt:mm:ss[+-]tt:mm Eksempler: "sc": "2021-08-20T10:03:12Z" (UTC-tid) "sc": "2021-08-20T12:03:12+02" (CEST) "sc": "2021-08-20T12:03:12+0200" (CEST) "sc": "2021-08-20T12:03:12+02:00" (CEST)
t/tr	Testresultat	Resultatet af testen. En kodet værdi fra værdisættet test-result.json (baseret på SNOMED CT, GPS). Præcis 1 (ét) ikke tomt felt skal angives. Eksempel: "tr": "260415000" (Ikke påvist)
t/tc	Testcenter eller -facilitet	Navn på den aktør, der har foretaget testen. Identifikatorer er tilladt som del af navnet, men det anbefales ikke at bruge dem særskilt uden navnet som tekst. Maksimalt 80 UTF-8-tegn. Eventuelle ekstra tegn bør trunkeres. Navnet er ikke beregnet til automatisk verifikation. For NAAT-test: Præcis 1 (ét) ikketomt felt skal angives. ►**M4** For antigentest: Dette felt er valgfrit. Hvis det foreligger, skal feltet ikke være tomt. ◄ Eksempel: "tc": "Testcenter vest 245"
t/co	Medlemsstat eller tredjeland, hvor testen er udført	Land udtrykt som en ISO3166-kode på 2 bogstaver (ANBEFALET) eller en henvisning til en international organisation, der er ansvarlig for udførelse af testen (såsom UNHCR eller WHO). Dette skal være en kodet værdi fra værdisættet country-2-codes.json. Værdisættet stammer fra portalen for EU's digitale covidcertifikat. Præcis 1 (ét) felt skal angives. Eksempler: "co": "CZ" "co": "UNHCR"
t/is	Udsteder af certifikat	Navn på organisation, der har udstedt certifikatet. Identifikatorer er tilladt som del af navnet, men det anbefales ikke at bruge dem særskilt uden navnet som tekst. Maksimalt 80 UTF-8-tegn. Præcis 1 (ét) ikke tomt felt skal angives. Eksempler: "is": "Den Tjekkiske Republiks Sundhedsministerium" "is": "Sundhedsmyndigheden for den nordvestlige region"

▼M1

Felt-ID	Feltnavn	Vejledning
t/ci	Unik certifikatidentifikator	Unik certifikatidentifikator som beskrevet på vaccination-proof_interoperability-guidelines_en.pdf (europa.eu). Det er valgfrit at medtage kontrolsummen. Præfikset »URN:UVCI:« kan tilføjes. Præcis 1 (ét) ikke tomt felt skal angives. Eksempler: "ci": "URN:UVCI:01:NL:187/37512422923 " "ci": "URN:UVCI:01:AT:10807843F94AEE0EE5093FBC254BD813#B"

4.3. *Restitutionscertifikat*

Restitutionsgruppen skal, hvis den findes, indeholde præcis 1 (én) indkodning, der præcis beskriver en oplysning om restitution. Alle elementer i restitutionsgruppen er obligatoriske, og tomme værdier understøttes ikke.

Felt-ID	Feltnavn	Vejledning
r/tg	Sygdom eller agens, som indehaveren er restitueret efter: Covid-19 (sars-CoV-2 eller en variant heraf)	En kodet værdi fra værdisættet disease-agent-targeted.json. Denne værdi indkodes som 840539006, der er koden for covid-19 fra SNOMED CT (GPS). Præcis 1 (ét) ikke tomt felt skal angives. Eksempel: "tg": "840539006"
r/fr	Dato for indehaverens første positive ►M4 ——— ◄-testresultat	Datoen, hvor en prøve til en ►M4 ——— ◄-test, der har givet et positivt resultat, blev udtaget, i formatet ÅÅÅÅ-MM-DD (fuldstændig dato uden klokkeslæt). Andre formater understøttes ikke. Præcis 1 (ét) ikke tomt felt skal angives. Eksempel: "fr": "2021-05-18"
r/co	Medlemsstat eller tredjeland, hvor testen er udført	Land udtrykt som en ISO3166-kode på 2 bogstaver (ANBEFALET) eller en henvisning til en international organisation, der er ansvarlig for udførelse af testen (såsom UNHCR eller WHO). Dette skal være en kodet værdi fra værdisættet country-2-codes.json. Værdisættet stammer fra portalen for EU's digitale covidcertifikat. Præcis 1 (ét) felt skal angives. Eksempler: "co": "CZ" "co": "UNHCR"
r/is	Udsteder af certifikat	Navn på organisation, der har udstedt certifikatet. Identifikatorer er tilladt som del af navnet, men det anbefales ikke at bruge dem særskilt uden navnet som tekst. Maksimalt 80 UTF-8-tegn. Præcis 1 (ét) ikke tomt felt skal angives. Eksempel: "is": "Den Tjekkiske Republiks Sundhedsministerium" "is": "Det centrale universitetshospital"

▼**M1**

Felt-ID	Feltnavn	Vejledning
r/df	Certifikat gyldigt fra	Den første dato fra hvilken certifikatet betragtes som gyldigt. Datoen må ikke ligge før den dato, der er beregnet som r/fr + 11 dage. Datoen skal angives i formatet ÅÅÅÅ-MM-DD (fuldstændig dato uden klokkeslæt). Andre formater understøttes ikke. Præcis 1 (ét) ikke tomt felt skal angives. Eksempel: "df": "2021-05-29"
r/du	Certifikat gyldigt indtil	Den sidste dato på hvilken certifikatet betragtes som gyldigt, fastsat af certifikatudstederen. Datoen må ikke ligge efter den dato, der er beregnet som r/fr + 180 dage. Datoen skal angives i formatet ÅÅÅÅ-MM-DD (fuldstændig dato uden klokkeslæt). Andre formater understøttes ikke. Præcis 1 (ét) ikke tomt felt skal angives. Eksempel: "du": "2021-11-14"
r/ci	Unik certifikatidentifikator	Unik certifikatidentifikator (UVCI) som beskrevet på vaccination-proof_interoperability-guidelines_en.pdf (europa.eu) Det er valgfrit at medtage kontrolsummen. Præfikset "URN:UVCI:" kan tilføjes. Præcis 1 (ét) ikke tomt felt skal angives. Eksempler: "ci": "URN:UVCI:01:NL:187/37512422923" "ci": »URN:UVCI:01:AT:10807843F94AEE0EE5093FBC254BD813#B«

▼M3

BILAG VI

MEDLEMSSTATERNES ANSVAR SOM FÆLLES DATAANSVARLIGE FOR PORTALEN FOR EU'S DIGITALE COVIDCERTIFIKAT FOR SÅ VIDT ANGÅR UDVEKSLING AF LISTER OVER TILBAGEKALDTE CERTIFIKATER

AFSNIT 1

Underafsnit 1

Ansvarsfordeling

(1) De fælles dataansvarlige behandler personoplysninger via tillidsrammens portal i overensstemmelse med de tekniske specifikationer, der er fastsat i bilag I.

(2) Medlemsstaternes udstedende myndigheder forbliver de eneste dataansvarlige for indsamling, anvendelse, offentliggørelse og enhver anden form for behandling af tilbagekaldelsesoplysninger uden for portalen, herunder for den procedure, der fører til tilbagekaldelse af et certifikat.

(3) Hver dataansvarlig er ansvarlig for at behandle personoplysninger i tillidsrammens portal i overensstemmelse med artikel 5, 24 og 26 i den generelle forordning om databeskyttelse.

(4) Hver dataansvarlig opretter et kontaktpunkt med en funktionel mailboks, som anvendes til kommunikation mellem selve de fælles dataansvarlige og mellem de fælles dataansvarlige og databehandleren.

(5) En midlertidig undergruppe oprettet i overensstemmelse med artikel 14 i forordning (EU) 2021/953 skal have til opgave at undersøge alle spørgsmål, der opstår i forbindelse med udveksling af listerne over tilbagekaldte certifikater, og det fælles dataansvar for dertil knyttet behandling af personoplysninger, og at lette koordinerede instrukser til Kommissionen som databehandler. De fælles dataansvarliges beslutningsproces styres af denne arbejdsgruppe og af den forretningsorden, som gruppen vedtager. Grundlæggende gælder det, at en fælles dataansvarligs manglende deltagelse i et møde i denne arbejdsgruppe, som er meddelt mindst syv (7) dage før den skriftlige mødeindkaldelse, er ensbetydende med stiltiende enighed med resultaterne af dette møde i arbejdsgruppen. Enhver af de fælles dataansvarlige kan indkalde til møde i arbejdsgruppen.

(6) Instrukser til databehandleren sendes af et af de fælles dataansvarliges kontaktpunkter efter aftale med de øvrige fælles dataansvarlige, jf. arbejdsgruppens beslutningsproces som beskrevet i ovenstående punkt 5. Den fælles dataansvarlige, som udsteder instrukser, skal fremlægge disse for databehandleren på skrift og informere alle andre fælles dataansvarlige herom. Hvis det pågældende spørgsmål er så tilstrækkeligt tidskritisk, at det ikke er muligt at holde et møde i den arbejdsgruppe, der er omhandlet i ovenstående punkt 5, kan der alligevel udstedes en instruks, som dog kan annulleres af arbejdsgruppen. Denne instruks bør gives skriftligt, og alle de andre fælles dataansvarlige bør i den forbindelse informeres herom.

(7) Den arbejdsgruppe, der er nedsat i overensstemmelse med punkt 5, udelukker ikke den enkelte fælles dataansvarliges individuelle kompetence til at informere sin kompetente tilsynsmyndighed i overensstemmelse med artikel 33 og 24 i den generelle forordning om databeskyttelse. En sådan meddelelse kræver ikke de øvrige fælles dataansvarliges samtykke.

▼M3

(8) Kun personer med tilladelse fra de udpegede nationale myndigheder eller officielle organer må tilgå de personoplysninger, der udveksles i tillidsrammens portal.

(9) Hver udstedende myndighed fører en fortegnelse over behandlingsaktiviteter under dens ansvarsområde. Det fælles dataansvar kan angives i fortegnelsen.

Underafsnit 2

Ansvar og roller i forbindelse med behandling af anmodninger fra og information af registrerede

(1) Hver dataansvarlig skal i sin rolle som udstedende myndighed over for fysiske personer, hvis certifikat(er), den har tilbagekaldt, (»de registrerede«) fremlægge oplysninger om den pågældende tilbagekaldelse og om behandling af deres personoplysninger i portalen for EU's digitale covidcertifikat med henblik på at støtte udvekslingen af lister over tilbagekaldte certifikater, jf. artikel 14 i den generelle forordning om databeskyttelse, medmindre dette viser sig at være umuligt eller vil indebære en uforholdsmæssig stor indsats.

(2) Hver dataansvarlig fungerer som kontaktpunkt for fysiske personer, hvis certifikater, den har tilbagekaldt, og behandler anmodninger vedrørende udøvelsen af registreredes rettigheder i overensstemmelse med den generelle forordning om databeskyttelse. Hvis en fælles dataansvarlig modtager en anmodning fra en registreret vedrørende et certifikat, der er udstedt af en anden fælles dataansvarlig, informerer den den registrerede om den ansvarlige fælles dataansvarliges identitet og kontaktoplysninger. De fælles dataansvarlige bistår efter anmodning fra en fælles dataansvarlig hinanden med behandlingen af registreredes anmodninger, og de svarer hinanden hurtigst muligt og under alle omstændigheder senest 1 måned efter at have modtaget en anmodning om bistand. Hvis en anmodning vedrører data indsendt af et tredjeland, skal den dataansvarlige, som modtager anmodningen, behandle anmodningen og informere den registrerede om identitet og kontaktoplysninger på tredjelandets udstedende myndighed.

(3) Hver dataansvarlig stiller indholdet af dette bilag, herunder de ordninger, der er fastlagt i punkt 1 og 2, til rådighed for de registrerede.

AFSNIT 2

Håndtering af sikkerhedsrelaterede hændelser, herunder brud på persondatasikkerheden

(1) De fælles dataansvarlige bistår hinanden med identifikation og håndtering af eventuelle sikkerhedsrelaterede hændelser, herunder brud på persondatasikkerheden, i forbindelse med behandlingen i portalen for EU's digitale covidcertifikat.

(2) De fælles dataansvarlige underretter især hinanden om følgende:

a) enhver potentiel eller reel risiko i forhold til adgangen til, fortroligheden for og/eller integriteten af de personoplysninger, der er genstand for behandling i tillidsrammens portal

b) ethvert brud på persondatasikkerheden, de sandsynlige konsekvenser af bruddet på persondatabeskyttelsen og en vurdering af risikoen for fysiske personers rettigheder og frihedsrettigheder samt alle foranstaltninger, der træffes for at håndtere bruddet på persondatasikkerheden og begrænse risikoen for fysiske personers rettigheder og frihedsrettigheder

▼M3

c) enhver overtrædelse af de tekniske og/eller organisatoriske sikkerhedsforanstaltninger for behandlingsaktiviteterne i tillidsrammens portal.

(3) De fælles dataansvarlige anmelder, i overensstemmelse med artikel 33 og 34 i den generelle forordning om databeskyttelse eller efter anmeldelse fra Kommissionen, ethvert brud på persondatasikkerheden i forbindelse med behandlingsaktiviteterne i tillidsrammens portal til Kommissionen, til de kompetente tilsynsmyndigheder og, for så vidt det er påkrævet, til de registrerede.

(4) Hver udstedende myndighed for systemet for tidlig varsling og reaktion gennemfører passende tekniske og organisatoriske foranstaltninger, der har til formål at:

a) garantere og sikre tilgængelighed, integritet og fortrolighed af de fælles behandlede personoplysninger

b) beskytte personoplysninger i dens besiddelse mod uautoriseret eller ulovlig behandling, tab, anvendelse, offentliggørelse eller erhvervelse af eller adgang dertil

c) sikre, at adgangen til personoplysninger ikke offentliggøres eller gives til andre end modtagerne eller behandlerne.

AFSNIT 3

Konsekvensanalyse vedrørende databeskyttelse

(1) Hvis en dataansvarlig, for at overholde sine forpligtelser i henhold til artikel 35 og 36 i forordning (EU) 2016/679, har brug for oplysninger fra en anden dataansvarlig, sender førstnævnte dataansvarlige en specifik anmodning til den fællespostkasse, der er omhandlet i afsnit 1, underafsnit 1, punkt 4. Sidstnævnte gør sit bedste for at tilvejebringe de pågældende oplysninger.

▼M3

BILAG VII

KOMMISSIONENS ANSVAR SOM FÆLLES DATABEHANDLER FOR PORTALEN FOR EU'S DIGITALE COVIDCERTIFIKAT FOR SÅ VIDT ANGÅR STØTTE AF UDVEKSLINGEN AF LISTER OVER TILBAGEKALDTE CERTIFIKATER

Kommissionen skal:

(1) på vegne af medlemsstaterne etablere og sikre en sikker og pålidelig kommunikationsinfrastruktur, som støtter udvekslingen af de lister over tilbagekaldte certifikater, der indsendes til portalen for EU's digitale covidcertifikat.

(2) For at opfylde sine forpligtelser som databehandler for tillidsrammens portal kan Kommissionen inddrage tredjeparter som underdatabehandlere; Kommissionen skal underrette de fælles dataansvarlige om påtænkte ændringer vedrørende tilføjelse eller udskiftning af andre underdatabehandlere, således at de dataansvarlige får mulighed for i fællesskab at gøre indsigelse mod de pågældende ændringer. Kommissionen sikrer, at der gælder samme databeskyttelsesforpligtelser for disse underdatabehandlere som fastsat i denne afgørelse

(3) behandle personoplysningerne udelukkende efter dokumenterede instrukser fra de dataansvarlige, medmindre det kræves i henhold til EU-retten eller medlemsstaternes nationale ret; i så fald underretter Kommissionen de fælles dataansvarlige om dette retlige krav, inden oplysningerne behandles, medmindre den pågældende ret forbyder en sådan underretning af hensyn til væsentlige samfundsinteresser.

Kommissionens behandling indebærer følgende:

a) at autentificere nationale backend-servere på grundlag af nationale backend-servercertifikater

b) at modtage de data omhandlet i afgørelsens artikel 5a, stk. 3, der uploades af de nationale backend-servere, ved at stille en applikationsprogrammeringsgrænseflade til rådighed, som gør det muligt for nationale backend-servere at uploade de relevante data

c) at lagre data i portalen for EU's digitale covidcertifikat

d) at stille dataene til rådighed, så de kan downloades af de nationale backend-servere

e) at slette data efter deres udløbsdato eller efter instruks fra den dataansvarlige, der har indsendt dem

f) at slette eventuelle resterende data, efter at tjenesterne er ophørt, medmindre EU-retten eller medlemsstaternes nationale ret foreskriver opbevaring af personoplysningerne.

(4) træffe alle avancerede organisatoriske, fysiske og logiske sikkerhedsforanstaltninger for at vedligeholde portalen for EU's digitale covidcertifikat. Kommissionen skal med henblik herpå:

a) udpege en enhed, der er ansvarlig for sikkerhedsstyring på niveauet for portalen for EU's digitale covidcertifikat, kommunikere enhedens kontaktoplysninger til de fælles dataansvarlige og sikre, at enheden kan reagere på sikkerhedstrusler

▼M3

b) påtage sig ansvaret for sikkerheden ved portalen for EU's digitale covidcertifikat, herunder foretage regelmæssige test, evalueringer og vurderinger af sikkerhedsforanstaltningerne

c) sikre, at alle, der får adgang til portalen for EU's digitale covidcertifikat, er underlagt kontraktlig, professionel eller lovbestemt tavshedspligt

(5) træffe alle nødvendige sikkerhedsforanstaltninger til at undgå at kompromittere driften af de nationale backend-servere. Kommissionen skal til dette formål fastlægge specifikke procedurer i tilknytning til forbindelsen fra backend-serverne til portalen for EU's digitale covidcertifikat. Dette omfatter:

a) risikovurderingsprocedure — til identificering og vurdering af mulige trusler mod systemet

b) audit- og kontrolprocedure til:

i. kontrol af overensstemmelse mellem de gennemførte sikkerhedsforanstaltninger og sikkerhedspolitik i anvendelse

ii. regelmæssig kontrol af integriteten af systemfiler, sikkerhedsparametre og udstedte tilladelser

iii. overvågning med henblik på afsløring af brud på sikkerheden og indtrængen

iv. gennemførelse af ændringer for at begrænse eksisterende sikkerhedsproblemer

v. fastsættelse af betingelser, under hvilke der gives tilladelse, herunder på anmodning fra dataansvarlige, og bidrage til udførelsen af uafhængige audit, herunder inspektioner, og gennemgang af sikkerhedsforanstaltninger på vilkår, der er i overensstemmelse med protokol (nr. 7) til TEUF vedrørende Den Europæiske Unions privilegier og immuniteter

c) ændring af kontrolproceduren til dokumentation og måling af virkningen af en ændring, før den gennemføres, og underretning af de fælles dataansvarlige om ændringer, der kan påvirke kommunikationen med og/eller sikkerheden i deres infrastrukturer

d) fastlæggelse af en vedligeholdelses- og reparationsprocedure til præcisering af bestemmelser og betingelser, som skal overholdes ved vedligeholdelse og/eller reparation af udstyr

e) fastlæggelse af en procedure for sikkerhedsrelaterede hændelser til fastlæggelse af rapporterings- og eskaleringsordningen, omgående underretning af de berørte dataansvarlige, så de kan underrette de nationale datatilsynsmyndigheder om brud på persondatasikkerheden og fastlæggelse af en disciplinær proces til håndtering af brud på sikkerheden

(6) træffe avancerede fysiske og/eller logiske sikkerhedsforanstaltninger for de faciliteter, som opbevarer udstyret til portalen for EU's digitale covidcertifikat, og for kontrollen af adgangen til logiske data og sikkerhed. Kommissionen skal med henblik herpå:

a) håndhæve den fysiske sikkerhed for at oprette særlige sikkerhedsområder og muliggøre afsløring af brud

▼**M3**

b) kontrollere adgang til faciliteterne og vedligeholde et besøgsregister med henblik på sporing

c) sikre, at eksterne personer med adgang til området ledsages af behørigt bemyndigede medarbejdere

d) sikre, at udstyr ikke kan tilføjes, erstattes eller fjernes uden forudgående godkendelse fra de udpegede ansvarlige organer

e) kontrollere adgang fra og til de nationale backend-servere til tillidsrammens portal

f) sikre, at alle, der har adgang til portalen for EU's digitale covidcertifikat, identificeres og autentificeres

g) gennemgå godkendelsesrettighederne i forbindelse med adgang til portalen for EU's digitale covidcertifikat, i tilfælde af at et brud på sikkerheden har betydning for denne infrastruktur

h) fastholde integriteten i de oplysninger, der overføres via portalen for EU's digitale covidcertifikat

i) gennemføre tekniske og organisatoriske sikkerhedsforanstaltninger for at forhindre uautoriseret adgang til personoplysninger

j) om nødvendigt gennemføre foranstaltninger for at blokere uautoriseret adgang til portalen for EU's digitale covidcertifikat fra de udstedende myndigheders domæne (dvs. blokere en lokation/IP-adresse)

(7) træffe foranstaltninger til beskyttelse af sit domæne, herunder fjerne forbindelser, hvis der er væsentlig afvigelse fra principper og koncepter for kvalitet og sikkerhed

(8) opstille en risikostyringsplan i forbindelse med sit ansvarsområde

(9) overvåge — i realtid — udførelsen af alle servicekomponenter af sine tjenester i tillidsrammens portal, udarbejde regelmæssige statistikker og føre registre

(10) yde støtte til alle tjenester i tillidsrammens portal på engelsk 24/7 via telefon, e-mail eller webportal og modtage opkald fra autoriserede personer: koordinatorer af portalen for EU's digitale covidcertifikat og deres respektive helpdeske, projektledere og udpegede personer fra Kommissionen.

(11) bistå de fælles dataansvarlige, i den udstrækning det er muligt og ved hjælp af passende tekniske og organisatoriske foranstaltninger, jf. artikel 12 i forordning (EU) 2018/1725, med opfyldelse af den dataansvarliges forpligtelse til at besvare anmodninger om udøvelse af de registreredes rettigheder som fastlagt i kapitel III i den generelle forordning om databeskyttelse

▼**M3**

(12) yde støtte til de fælles dataansvarlige ved at levere oplysninger vedrørende portalen for EU's digitale covidcertifikat for at gennemføre forpligtelserne i henhold til artikel 32, 33, 34, 35 og 36 i den generelle forordning om databeskyttelse

(13) sikre, at oplysninger, der behandles inden for portalen for EU's digitale covidcertifikat, er uforståelige for alle, der ikke har tilladelse til at tilgå faciliteten

(14) træffe alle relevante foranstaltninger for at forhindre, at operatører af den portalen for EU's digitale covidcertifikat har uautoriseret adgang til overførte oplysninger

(15) træffe foranstaltninger for at fremme interoperabiliteten og kommunikationen mellem de udpegede dataansvarlige for portalen for EU's digitale covidcertifikat

(16) føre en fortegnelse over de behandlingsaktiviteter, der foretages på vegne af de fælles dataansvarlige, i overensstemmelse med artikel 31, stk. 2, i forordning (EU) 2018/1725.