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)

EUROPA-KOMMISSIONEN HAR —

under henvisning til traktaten om Den Europæiske Unions funktionsmåde,

under henvisning til Europa-Parlamentets og Rådets forordning (EU) 2021/953 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 ([1]), særlig artikel 9, stk. 1 og 3, og

ud fra følgende betragtninger:

(1) I forordning (EU) 2021/953 fastsættes EU's digitale covidcertifikat, der skal tjene som dokumentation for, at en person har modtaget en covid-19-vaccine, har et negativt testresultat eller er kommet sig over sygdommen.

(2) For at EU's digitale covidcertifikat kan blive operationelt i hele Unionen, er det nødvendigt at fastsætte tekniske specifikationer og regler for udfyldelse, sikker udstedelse og kontrol af de digitale covidcertifikater samt sikre beskyttelsen af personoplysninger, fastsætte den fælles struktur for den unikke certifikatidentifikator og udstede en gyldig, sikker og interoperabel stregkode. Denne tillidsramme fastsætter også præmisserne for at forsøge at sikre interoperabilitet med internationale standarder og teknologiske systemer og kan som sådan udgøre en model for samarbejde på globalt niveau.

(3) Evnen til at læse og fortolke EU's digitale covidcertifikat kræver en fælles datastruktur og aftale om den tilsigtede mening med hvert datafelt i nyttedataene og dets mulige værdier. For at fremme en sådan interoperabilitet er det nødvendigt at definere en fælles koordineret datastruktur for rammen for EU's digitale covidcertifikat. Retningslinjerne for denne ramme er blevet udviklet af det e-sundhedsnetværk, der er etableret på grundlag af Europa-Parlamentets og Rådets direktiv 2011/24/EU ([2]). Disse retningslinjer bør tages i betragtning, når der fastsættes tekniske specifikationer for formatet og tillidsforvaltningen vedrørende EU's digitale covidcertifikat. Der bør fastsættes en datastruktur og kodningsmekanismer såvel som en transportkodningsmekanisme i et maskinlæsbart, optisk format (QR), som kan vises på mobile enheders skærme eller udskrives på et stykke papir.

(4) Ud over de tekniske specifikationer for EU's digitale covidcertifikats format og tillidsforvaltningen heraf bør der fastsættes generelle regler for udfyldelse af certifikaterne, der kan bruges til kodede værdier i indholdet af EU's digitale covidcertifikat. De værdier, der skal bruges til gennemførelse af disse regler, bør ajourføres regelmæssigt og offentliggøres af Kommissionen, idet der trækkes på det relevante arbejde i e-sundhedsnetværket.

(5) Ifølge forordning (EU) 2021/953 bør ægte certifikater, der udgør EU's digitale covidcertifikat, være individuelt identificerbare ved hjælp af en unik certifikatidentifikator, idet der tages hensyn til, at indehavere kan få udstedt mere end ét certifikat i den tid, forordning (EU) 2021/953 er i kraft. Den unikke certifikatidentifikator skal bestå af en alfanumerisk streng, og medlemsstaterne bør sikre, at den ikke indeholder data, der knytter den til andre dokumenter eller identifikatorer såsom pas- eller identitetskortnumre for at forhindre identifikation af indehaveren. For at sikre, at certifikatidentifikatoren er unik, bør der fastsættes tekniske specifikationer og regler for den fælles struktur herfor.

([1]) EUT L 211 af 15.6.2021, s. 1.

([2]) Europa-Parlamentets og Rådets direktiv 2011/24/EU af 9. marts 2011 om patientrettigheder i forbindelse med grænseoverskridende sundhedsydelser (EUT L 88 af 4.4.2011, s. 45).

(6) Sikkerheden, ægtheden, gyldigheden og integriteten af de certifikater, der udgør EU's digitale covidcertifikat, og deres overholdelse af Unionens databeskyttelsesret er afgørende for deres accept i alle medlemsstater. Disse målsætninger nås ved den tillidsramme, som fastsætter reglerne og infrastrukturen for den pålidelige og sikre udstedelse og verifikation af EU's digitale covidcertifikater. Tillidsrammen bør bl.a. baseres på en offentlig nøgleinfrastruktur med en tillidskæde fra medlemsstaternes sundhedsmyndigheder eller andre betroede myndigheder til de enkelte enheder, der udsteder EU's digitale covidcertifikater. Kommissionen har — med henblik på at sikre et EU-dækkende interoperabilitetssystem — derfor etableret et centralt system, portalen for EU's digitale covidcertifikat (»portalen«), der lagrer offentlige nøgler, som bruges til verifikation. Når certifikatets QR-kode scannes, verificeres den digitale signatur ved hjælp af den relevante offentlige nøgle, der tidligere er lagret i denne centrale portal. Digitale signaturer kan bruges til at sikre dataintegritet og -autenticitet. Offentlige nøgleinfrastrukturer skaber tillid ved at knytte offentlige nøgler til certifikatudstedere. I portalen anvendes flere forskellige offentlige nøglecertifikater til verifikation af ægtheden. For at sørge for sikker dataudveksling for det offentlige nøglemateriale mellem medlemsstaterne og muliggøre bred interoperabilitet er det nødvendigt at fastsætte, hvilke offentlige nøglecertifikater der må bruges, og hvordan de genereres.

(7) Nærværende afgørelse gør det muligt at gøre kravene i forordning (EU) 2021/953 operationelle på en måde, der minimerer behandlingen af personoplysninger til det, der er nødvendigt for at gøre EU's digitale covidcertifikat operationelt, og bidrager til en gennemførelse, hvor det sidste kontrolled respekterer en skræddersyet databeskyttelse.

(8) I overensstemmelse med forordning (EU) 2021/953 betragtes myndigheder eller de andre udpegede organer med ansvar for udstedelsen af certifikater som værende dataansvarlige, jf. definitionen i artikel 4, nr. 7), i Europa-Parlamentets og Rådets forordning (EU) 2016/679 ([3]), idet de i forbindelse med udstedelsesprocessen behandler personoplysninger. Afhængig af, hvordan medlemsstaterne organiserer udstedelsesprocessen, kan der være en eller flere myndigheder eller udpegede organer, f.eks. regionale sundhedstjenester. I overensstemmelse med nærhedsprincippet er dette op til medlemsstaterne. Medlemsstaterne er derfor dem, der bedst kan sikre, at ansvaret, i tilfælde hvor der er flere forskellige myndigheder eller andre udpegede organer, er klart fordelt, uafhængigt af om de er særskilte eller fælles dataansvarlige (heriblandt regionale sundhedstjenester, der etablerer en fælles patientportal til udstedelse af certifikater). Hvad angår den verifikation af certifikater, de kompetente myndigheder i bestemmelses- eller transitmedlemsstaten eller operatører af grænseoverskridende passagertransport foretager i henhold til national lovgivning for at gennemføre visse offentlige sundhedsforanstaltninger i forbindelse med covid-19-pandemien, skal disse kontrollører opfylde deres forpligtelser under databeskyttelsesreglerne.

(9) Ingen behandling af personoplysninger finder sted via portalen for EU's digitale covidcertifikat, idet portalen kun indeholder de signerende myndigheders offentlige nøgler. Disse nøgler vedrører de signerende myndigheder og tillader hverken direkte eller indirekte reidentifikation af en fysisk person, som et certifikat er udstedt til. I sin rolle som forvalter af portalen bør det derfor ikke være Kommissionens rolle at kontrollere eller behandle personoplysninger.

(10) Den Europæiske Tilsynsførende for Databeskyttelse er hørt i overensstemmelse med artikel 42, stk. 1, i Europa-Parlamentets og Rådets forordning (EU) 2018/1725 ([4]) og afgav udtalelse den 22. juni 2021.

(11) Eftersom de tekniske specifikationer og regler er nødvendige for at kunne anvende forordning (EU) 2021/953 fra den 1. juli 2021, er den øjeblikkelige anvendelse af nærværende afgørelse begrundet.

(12) Set i lyset af behovet for hurtig gennemførelse af EU's digitale covidcertifikat bør denne afgørelse derfor træde i kraft dagen efter dens offentliggørelse —

([3]) Europa-Parlamentets og Rådets forordning (EU) 2016/679 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger og om ophævelse af direktiv 95/46/EF (generel forordning om databeskyttelse) (EUT L 119 af 4.5.2016, s. 1).

([4]) Europa-Parlamentets og Rådets forordning (EU) 2018/1725 af 23. oktober 2018 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger i Unionens institutioner, organer, kontorer og agenturer og om fri udveksling af sådanne oplysninger og om ophævelse af forordning (EF) nr. 45/2001 og afgørelse nr. 1247/2002/EF (EUT L 295 af 21.11.2018, s. 39).

VEDTAGET DENNE AFGØRELSE:

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.

Artikel 4

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

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

Udfærdiget i Bruxelles, den 28. juni 2021.

På Kommissionens vegne
Ursula VON DER LEYEN
Formand

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

— 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

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

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 ([3])) 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.

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

3.2.6. Udstedt den

Kravet »udstedt den« (iat) skal indeholde et tidsstempel i NumericDate-heltalsformat (som specificeret i RFC 8392 ([5]), 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 ([6])) indeholdende oplysninger om sundhedsstatus. Der kan findes mange forskellige typer af sundhedscertifikater under samme krav, hvor DCC'et er et af dem.

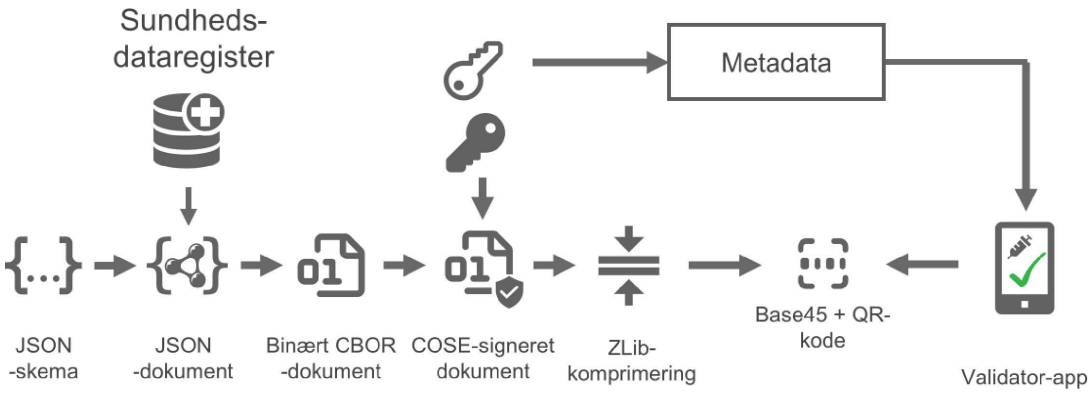
JSON anvendes udelukkende til skemaformål. Gengivelsesformatet er CBOR som defineret i (RFC 7049 ([7])). Applikationsudviklere må faktisk hverken afkode eller kode til og fra JSON-formatet, men skal bruge strukturen i hukommelsen.

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 ([8]). Dataindholdet er begrænset til de definerede dataelementer i det minimumsdatasæt, der er fastsat i bilaget i forordning 2021/953.

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

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.

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 ([9])) og Deflate-komprimeringsmekanismen i det format, som er defineret i RFC 1951 ([10]).

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.

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

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.

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 ([11]), 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.

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.

([11]) rfc7517 (ietf.org)

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 DCC'et. 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, anbefales det at kode dem i UTF-8 (navn, testcenter, certifikatudsteder). Det anbefales at kode datafelter med kalenderdatoer (fødselsdato, vaccinationsdato, dato for prøveudtagning, dato for første positive testresultat, certifikatets gyldighedsdatoer) i henhold til ISO 8601.

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

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

Værdisættene ajourføres regelmæssigt af Kommissionen med støtte fra e-sundhedsnetværket og Udvalget for Sundhedssikkerhed. De ajourførte værdisæt offentliggøres på Kommissionens relevante websted samt på e-sundhedsnetværkets websted. Der bør 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)**

   Foretrukket kodesystem: SNOMED CT.

   Anvendes i certifikat 1, 2 og 3.

   De udvalgte koder skal henvise til covid-19 eller de enkelte genetiske varianter af sars-CoV-2, hvis der af epidemiologiske årsager er behov for mere detaljerede oplysninger om disse varianter.

   Som eksempel på en kode, der bør anvendes, kan nævnes SNOMED CT-kode 840539006 (covid-19).

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

   Foretrukket kodesystem: SNOMED CT-systemet eller ATC-klassifikationssystemet

   Anvendes i certifikat 1.

   Som eksempler på koder, der bør 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). Værdisættet bør udvides, når der udvikles og tages nye vaccinetyper i brug.

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, bør disse erstattes af en bindestreg (-).

Værdisættets navn: Vaccine.

Anvendes i certifikat 1.

Som eksempel på en kode, der bør 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).

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, bør disse erstattes af en bindestreg (-).

Anvendes i certifikat 1.

Som eksempel på en kode, der bør 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).

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

Anvendes i certifikat 1.

To felter:

(1) Antal modtagne doser i en cyklus

(2) Antal forventede doser for en fuldendt cyklus (specifikt for den pågældende person på det tidspunkt, hvor dosen modtages)

For eksempel vil 1/1 eller 2/2 fremstå som fuldendt, herunder muligheden for at angive 1/1 for vacciner, der gives i to doser, men for hvilke medlemsstatens fremgangsmåde er at give én dosis til borgere, der er blevet diagnosticeret med covid-19 inden vaccinationen. Det samlede antal doser i rækken bør angives i henhold til de oplysninger, der foreligger på det tidspunkt, hvor dosen modtages. Hvis en specifik vaccine f.eks. kræver en tredje dosis (booster-dosis) på tidspunktet for den senest modtagne dosis, skal nummeret i andet felt afspejle dette (f.eks. 2/3, 3/3 osv.).

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)

7. **Testtype**

Foretrukket kodesystem: LOINC.

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

Koderne i dette værdisæt skal henvise til testmetoden og som minimum gøre forskel mellem NAAT-test og RAT-test som udtrykt i forordning (EU) 2021/953.

Som eksempel på en kode, der bør anvendes, fra det foretrukne kodesystem kan nævnes LP217198-3 (hurtig immunassay).

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

Foretrukket kodesystem: HSC's liste over hurtige antigentest, som holdes ajour af JRC (database over testmetoder og udstyr til in vitro-diagnostik af covid-19).

Anvendes i certifikat 2.

Indholdet af værdisættet af hurtige antigentest skal omfatte udvalget af hurtige antigentest som opført på den fælles og ajourførte liste over hurtige 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 database 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

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**

Foretrukket kodesystem: SNOMED CT.

Anvendes i certifikat 2.

De udvalgte koder skal gøre det muligt at skelne mellem positive og negative testresultater (påvist eller ikke påvist). Der kan tilføjes yderligere værdier (f.eks. ikke fastslået), hvis dette er nødvendigt i brugstilfældene.

Som eksempler på koder, der bør anvendes, fra det foretrukne kodesystem kan nævnes 260415000 (ikke påvist) og 260373001 (påvist).

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.

3. Generelle krav

Følgende overordnede krav bør 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]): {»/", »#", »:«}

(2) Maksimal længde: designerne bør tilstræbe en længde på 27-30 tegn ([3])

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

(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 bør 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 må ikke anvendes til validering af certifikatet og er ikke teknisk set en del af identifikatoren, men anvendes til at kontrollere kodens integritet. Denne kontrolsum bør opsummere hele UCI'en i digitalt/elektronisk overførbart format i henhold til ISO-7812-1 (LUHN-10) ([4]). Kontrolsummen adskilles fra resten af UCI'en med et »#"-tegn.

([1]) rfc3986 (ietf.org)

([2]) Felter til f.eks. køn, batch-/partinummer, administrationscenter, identifikation af sundhedsprofessionel eller næste vaccinationsdato er ikke nødvendigvis nødvendige til andre formål end medicinske formål.

([3]) 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.

([4]) 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).

Bagudkompatibiliteten bør 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.

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

E-sundhedsnetværkets retningslinjer for kontrollerbare vaccinationscertifikater og grundlæggende interoperabilitetselementer ([5]) 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.

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

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
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

Udtryk/forkortelse	Definition
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.

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.

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 dokumentunderskriver-certifikatet (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.

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.

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 covidcertifikaters 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.

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]).

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

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

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 ([3]).

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)

([3]) rfc5280 (ietf.org)

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 ([4]).

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.

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)

([4]) rfc5280 (ietf.org)

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** ([5])**, 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)

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)

([5]) 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.