KOMMISJONENS GJENNOMFØRINGSBESLUTNING (EU) 2021/1073 **2022/EØS/83/36**

av 28. juni 2021

om fastsettelse av tekniske spesifikasjoner og regler for gjennomføringen av tillitsrammen for EUs digitale covid-sertifikat fastsatt ved europaparlaments- og rådsforordning (EU) 2021/953(*)

EUROPAKOMMISJONEN HAR

under henvisning til traktaten om Den europeiske unions virkemåte,

under henvisning til europaparlaments- og rådsforordning (EU) 2021/953 om en ramme for utstedelse, kontroll og godtakelse av interoperable covid-19-sertifikater for vaksinasjon, testing og restitusjon (EUs digitale covid-sertifikat) for å lette fri bevegelighet under covid-19-pandemien([1]), særlig artikkel 9 nr. 1 og 3,

ut fra følgende betraktninger:

1) I forordning (EU) 2021/953 fastsettes EUs digitale covid-sertifikat, som har som formål å dokumentere at en person har fått en covid-19-vaksine, har fått et negativt testresultat eller har blitt frisk etter infeksjonen.

2) For at EUs digitale covid-sertifikat skal kunne brukes i hele Unionen, må det fastsettes tekniske spesifikasjoner og regler for utfylling og sikker utstedelse og kontroll av de digitale covid-sertifikatene, og for å sikre vernet av personopplysninger, fastsette en felles struktur for den unike sertifikatidentifikatoren og utstede en gyldig, sikker og interoperabel strekkode. Denne tillitsrammen fastsetter også premissene for å sikre interoperabilitet med internasjonale standarder og teknologiske systemer, og kan dermed utgjøre en modell for samarbeid på globalt plan.

3) Evnen til å lese og tolke EUs digitale covid-sertifikat krever en felles datastruktur og enighet om den tilsiktede betydningen av hvert datafelt i nyttedataene og dets mulige verdier. For å fremme en slik interoperabilitet er det nødvendig å definere en felles samordnet datastruktur for rammen for EUs digitale covid-sertifikat. Retningslinjene for denne rammen er utarbeidet av nettverket for e-helsetjenester, som er opprettet på grunnlag av europaparlaments- og rådsdirektiv 2011/24/EU([2]). Det bør tas hensyn til disse retningslinjene ved fastsettelsen av de tekniske spesifikasjonene som angir formatet for og tillitsforvaltningen i forbindelse med EUs digitale covid-sertifikat. Det bør fastsettes en datastruktur og kodingsmekanismer samt en mekanisme for transportkoding i et maskinleselig optisk format (QR), som kan vises på skjermen til en mobil enhet eller skrives ut på papir.

4) I tillegg til de tekniske spesifikasjonene for formatet for og tillitsforvaltningen av EUs digitale covid-sertifikat bør det fastsettes alminnelige regler for utfylling av sertifikatene, slik at de kan brukes for kodede verdier i EUs digitale covid-sertifikat. De verdisettene som skal brukes for å gjennomføre disse reglene, bør regelmessig oppdateres og offentliggjøres av Kommisjonen, på grunnlag av det relevante arbeidet i nettverket for e-helsetjenester.

5) I henhold til forordning (EU) 2021/953 skal autentiske sertifikater som inngår i det digitale covid-sertifikatet for EU, kunne identifiseres enkeltvis ved hjelp av en unik sertifikatidentifikator, idet det tas hensyn til at borgere kan få utstedt mer enn ett sertifikat i det tidsrommet forordning (EU) 2021/953 er i kraft. Den unike sertifikatidentifikatoren skal bestå av en alfanumerisk streng, og medlemsstatene bør sikre at den ikke inneholder data som knytter den til andre dokumenter eller identifikatorer, for eksempel passnummer eller ID-kortnummer, for å hindre at innehaveren kan identifiseres. For å sikre at sertifikatidentifikatoren er unik, bør det fastsettes tekniske spesifikasjoner og regler for den felles strukturen for denne.

(*) Denne unionsrettsakten, kunngjort i EUT L 230 av 30.6.2021, s. 32, er omhandlet i EØS-komiteens beslutning nr. 188/2021 av 30. juni 2021 om endring av EØS-avtalens vedlegg V (Fri bevegelighet for arbeidstakere) og vedlegg VIII (Etableringsrett), ennå ikke kunngjort.

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

([2]) Europaparlaments- og rådsdirektiv 2011/24/EU av 9. mars 2011 om anvendelse av pasientrettigheter ved helsetjenester over landegrensene (EUT L 88 av 4.4.2011, s. 45).

6) Sikkerheten, autentisiteten, gyldigheten og integriteten til de sertifikatene som inngår i EUs digitale covid-sertifikat, og deres samsvar med Unionens personvernregelverk, er avgjørende for at de skal kunne godtas i alle medlemsstater. Disse målene nås gjennom tillitsrammen med regler og infrastruktur for pålitelig og sikker utstedelse og kontroll av EUs digitale covid-sertifikater. Tillitsrammen bør blant annet baseres på en infrastruktur for offentlige nøkler (PKI (Public Key Infrastructure)) med en tillitskjede fra medlemsstatenes helsemyndigheter eller andre betrodde myndigheter til de enkelte enhetene som utsteder EUs digitale covid-sertifikater. For å sikre et interoperabilitetssystem for hele EU har Kommisjonen derfor opprettet et sentralt system – portalen for EUs digitale covid-sertifikat («portalen») – som lagrer offentlige nøkler som brukes til kontrollen. Når QR-kodesertifikatet skannes, kontrolleres den digitale signaturen ved hjelp av den relevante offentlige nøkkelen, som tidligere er lagret i den sentrale portalen. Digitale signaturer kan benyttes for å sikre dataenes integritet og autentisitet. Infrastrukturer for offentlige nøkler skaper tillit gjennom å kople offentlige nøkler til sertifikatutstedere. I portalen brukes flere offentlig-nøkkel-sertifikater for å kontrollere autentisiteten. For å sikre en sikker datautveksling av offentlig-nøkkel-materiale mellom medlemsstatene og muliggjøre bred interoperabilitet er det nødvendig å fastsette hvilke offentlig-nøkkel-sertifikater som kan brukes, og hvordan de bør genereres.

7) Denne beslutningen gjør det mulig å iverksette kravene i forordning (EU) 2021/953 på en måte som minimerer behandlingen av personopplysninger til det som er nødvendig for at EUs digitale covid-sertifikat skal kunne tas i bruk, og bidrar til at de behandlingsansvarlige som foretar den siste kontrollen, respekterer det innebygde personvernet.

8) I samsvar med forordning (EU) 2021/953 anses myndighetene eller andre utpekte organer som har ansvar for å utstede sertifikatene, som behandlingsansvarlige nevnt i artikkel 4 nr. 7 i europaparlaments- og rådsforordning (EU) 2016/679([3]) ettersom de behandler personopplysninger i forbindelse med utstedelsesprosessen. Avhengig av hvordan medlemsstatene organiserer utstedelsesprosessen, kan det være en eller flere myndigheter eller et eller flere utpekte organer, for eksempel regionale helsetjenester. I samsvar med nærhetsprinsippet er dette opp til medlemsstatene. Det er derfor medlemsstatene som best kan sikre at dersom det finnes flere myndigheter eller andre utpekte organer, så er deres respektive ansvarsområder klart fordelt, uavhengig av om de er atskilte eller felles behandlingsansvarlige (herunder regionale helsetjenester som oppretter en felles pasientportal for utstedelse av sertifikatene). Når det gjelder den kontrollen av sertifikater som foretas av vedkommende myndigheter i bestemmelsesstaten eller transittmedlemsstaten eller av operatører av persontransporttjenester over landegrensene som i henhold til nasjonal rett er forpliktet til å gjennomføre visse folkehelsetiltak under covid-19-pandemien, skal disse kontrollørene oppfylle sine forpliktelser i henhold til personvernreglene.

9) Det foretas ingen behandling av personopplysninger gjennom portalen for EUs digitale covid-sertifikat, ettersom portalen bare inneholder de signerende myndighetenes offentlige nøkler. Disse nøklene gjelder de signerende myndighetene og tillater verken direkte eller indirekte gjenidentifisering av en fysisk person som sertifikatet er utstedt til. I sin rolle som forvalter av portalen bør Kommisjonen derfor verken være behandlingsansvarlig eller databehandler i forbindelse med personopplysninger.

10) EUs datatilsyn er blitt rådspurt i samsvar med artikkel 42 nr. 1 i europaparlaments- og rådsforordning (EU) 2018/1725([4]) og avga uttalelse 22. juni 2021.

11) Ettersom tekniske spesifikasjoner og regler er nødvendige for at forordning (EU) 2021/953 skal kunne anvendes fra 1. juli 2021, er det berettiget at denne beslutningen får anvendelse umiddelbart.

12) I lys av behovet for en rask innføring av EUs digitale covid-sertifikat bør denne beslutningen tre i kraft den dagen den kunngjøres.

([3]) Europaparlaments- og rådsforordning (EU) 2016/679 av 27. april 2016 om vern av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger samt om oppheving av direktiv 95/46/EF (generell personvernforordning) (EUT L 119 av 4.5.2016, s. 1).

([4]) Europaparlaments- og rådsforordning (EU) 2018/1725 av 23. oktober 2018 om vern av fysiske personer i forbindelse med behandling av personopplysninger i Unionens institusjoner, organer, kontorer og byråer og om fri utveksling av slike opplysninger samt om oppheving av forordning (EF) nr. 45/2001 og beslutning nr. 1247/2002/EF (EUT L 295 av 21.11.2018, s. 39).

TRUFFET DENNE BESLUTNINGEN:

Artikkel 1

De tekniske spesifikasjonene for EUs digitale covid-sertifikat, som fastsetter den generiske datastrukturen, kodingsmekanismene og mekanismen for transportkoding i et maskinleselig optisk format, er fastsatt i vedlegg I.

Artikkel 2

Reglene for utfylling av sertifikatene omhandlet i artikkel 3 nr. 1 i forordning (EU) 2021/953 er fastsatt i vedlegg II til denne beslutningen.

Artikkel 3

Kravene til den felles strukturen for den unike sertifikatidentifikatoren er fastsatt i vedlegg III.

Artikkel 4

Reglene for forvaltning av offentlig-nøkkel-sertifikater i forbindelse med portalen for EUs digitale covid-sertifikat, som støtter tillitsrammens interoperabilitetsaspekter, er fastsatt i vedlegg IV.

Denne beslutningen trer i kraft den dagen den kunngjøres i *Den europeiske unions tidende*.

Utferdiget i Brussel 28. juni 2021.

For Kommisjonen

Ursula VON DER LEYEN

President

VEDLEGG I

FORMAT OG TILLITSFORVALTNING

Generisk datastruktur, kodingsmekanismer og mekanisme for transportkoding i et maskinleselig optisk format (heretter kalt «QR»)

1. **Innledning**

De tekniske spesifikasjonene som er fastsatt i dette vedlegget, omfatter en generisk datastruktur og kodingsmekanismer for EUs digitale covid-sertifikat (heretter kalt «DCC»). De fastsetter også en mekanisme for transportkoding i et maskinleselig optisk format («QR»), som kan vises på skjermen til en mobil enhet eller skrives ut. Beholderformatene for det elektroniske helsesertifikatet som er fastsatt i disse spesifikasjonene, er generiske, men brukes i denne forbindelsen til å oppbevare DCC-et.

2. **Terminologi**

I dette vedlegget menes med «utstedere» organisasjoner som bruker disse spesifikasjonene for å utstede helsesertifikater, og med «kontrollører» organisasjoner som godtar helsesertifikater som dokumentasjon for helsestatus. Med «deltakere» menes utstedere og kontrollører. Visse aspekter som fastsettes i dette vedlegget må samordnes mellom deltakerne, for eksempel forvaltningen av et navneområde og utdelingen av kryptonøkler. Det antas at en part, heretter kalt «sekretariatet», utfører disse oppgavene.

3. **Beholderformat for det elektroniske helsesertifikatet**

Beholderformatet for det elektroniske helsesertifikatet (Electronic Health Certificate Container Format («HCERT»)) er utformet slik at helsesertifikater fra forskjellige utstedere er ensartede og standardiserte. Formålet med disse spesifikasjonene er å harmonisere den måten disse helsesertifikatene representeres, kodes og signeres på, med sikte på å fremme interoperabilitet.

Evnen til å lese og tolke et DCC som er utstedt av en utsteder, krever en felles datastruktur og enighet om betydningen av hvert datafelt i nyttedataene. For å fremme slik interoperabilitet defineres en felles samordnet datastruktur ved hjelp av et «JSON»-skjema som utgjør rammen for DCC-et.

3.1. *Nyttedataenes struktur*

Nyttedataene struktureres og kodes som en CBOR med en digital COSE-signatur. Dette kalles ofte «CBOR Web Token» (heretter kalt «CWT») og er definert i RFC 8392([1]). Nyttedataene som defineres i de følgende avsnittene, overføres i et HCERT-krav.

Kontrolløren må kunne kontrollere integriteten og autentisiteten til nyttedataenes opprinnelse. For å stille denne mekanismen til rådighet må utstederen signere CWT ved hjelp av et asymmetrisk elektronisk signatursystem som definert i COSE-spesifikasjonen (RFC 8152([2])).

3.2. *CWT-krav*

3.2.1. Oversikt over CWT-strukturen

Beskyttet konvolutt (Protected Header)

— Signaturalgoritme (Signature Algorithm) (alg, etikett1)

— Nøkkelidentifikator (Key Identifier) (kid, etikett 4)

Nyttedata (Payload)

— Utsteder (Issuer) (iss, kravnøkkel 1, valgfritt, utsteders ISO 3166-1 alpha-2)

— Utstedt den (Issued At) (iat, kravnøkkel 6)

— Utløpsdato (Expiration Time) (exp, kravnøkkel 4)

— Helsesertifikat (Health Certificate) (hcert, kravnøkkel -260)

— EUs digitale covid-sertifikat, versjon 1 (EU Digital COVID Certificate v1) (eu_DCC_v1, kravnøkkel 1)

Signatur

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

3.2.2. Signaturalgoritme

Parameteren for signaturalgoritme (alg) angir hvilken algoritme som brukes for å opprette signaturen. Den skal oppfylle eller overstige de nåværende SOG-IS-retningslinjene som sammenfattes nedenfor.

En primær og en sekundær algoritme defineres. Sekundæralgoritmen bør brukes bare dersom den primære algoritmen ikke kan godtas i henhold til de reglene og forskriftene som utstederen er pålagt.

For å garantere systemets sikkerhet må all utføring omfatte den sekundære algoritmen. Av den grunn må både den primære og den sekundære algoritmen utføres.

SOG-IS-verdiene for den primære og den sekundære algoritmen er følgende:

— Primær algoritme: Den primære algoritmen er digital signaturalgoritme for elliptisk kurve (Elliptic Curve Digital Signature Algorithm (ECDSA)) som definert i (ISO/IEC 14888–3: 2006) avsnitt 2.3, som bruker P-256-parametrene som definert i tillegg D (D.1.2.3) til (FIPS PUB 186–4) kombinert med hash-algoritmen SHA-256 som definert i (ISO/IEC 10118–3: 2004) funksjon 4.

Dette tilsvarer COSE-algoritmeparameter ES256.

— Sekundær algoritme: Den sekundære algoritmen er RSASSA-PSS som definert i (RFC 8230([3])) med en modul på 2048 bit kombinert med hash-algoritmen SHA-256 som definert i (ISO/IEC 10118–3: 2004) funksjon 4.

Dette tilsvarer COSE-algoritmeparameter PS256.

3.2.3. Nøkkelidentifikator

Kravet «nøkkelidentifikator» (Key Identifier) (kid) angir det dokumentsigneringssertifikatet (Document Signer Certificate, (DSC)) som inneholder den offentlige nøkkelen som kontrolløren skal bruke for å kontrollere den digitale signaturen. Forvaltning av offentlig-nøkkel-sertifikater, herunder krav til DSC-er, beskrives i vedlegg IV.

Kontrollørene bruker kravet «nøkkelidentifikator» (kid) for å velge riktig offentlig nøkkel fra en liste over nøkler som er tilordnet utstederen som angis i kravet «utsteder» (iss). En utsteder kan av administrative årsaker og ved nøkkelutskiftinger bruke flere forskjellige nøkler parallelt. Nøkkelidentifikatoren er ikke et sikkerhetskritisk felt. Den kan derfor om nødvendig også plasseres i en ubeskyttet konvolutt. Kontrollørene må godta begge alternativer. Dersom begge alternativene foreligger, skal nøkkelidentifikatoren i den beskyttede konvolutten brukes.

Ettersom identifikatoren forkortes (for å begrense størrelsen), kan det ikke utelukkes at den samlede listen over DSC-er som en kontrollør godtar, kan inneholde DSC-er med samme kid. En kontrollør må derfor kontrollere alle DSC-er med denne kid-en.

3.2.4. Utsteder

Kravet «utsteder» (iss) er en strengverdi som eventuelt kan inneholde ISO 3166-1 alfa-2-landkoden for den enheten som utsteder helsesertifikatet. En kontrollør kan bruke dette kravet for å identifisere hvilket sett av DSC-er som skal brukes til kontrollen. Kravnøkkel 1 brukes for å identifisere dette kravet.

3.2.5. Utløpsdato

Kravet «utløpsdato» (exp) skal ha et tidsstempel i numerisk datoformat med heltall («integer NumericDate format», som spesifisert i RFC 8392([4]) avsnitt 2), som angir til hvilken dato den aktuelle signaturen for nyttedataene skal anses som gyldig, og etter hvilken kontrolløren må avvise nyttedataene fordi de har utløpt. Formålet med parameteren utløpsdato er å fastsette en grense for helsesertifikatets gyldighetsperiode. Kravnøkkel 4 brukes for å identifisere dette kravet.

Utløpsdatoen skal ikke være senere enn utløpet av DSC-ets gyldighetsperiode.

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

3.2.6. Utstedt den

Kravet «utstedt den» (iat) skal inneholde et tidsstempel i numerisk datoformat med heltall («integer NumericDate format», som spesifisert i RFC 8392([5]) avsnitt 2), som angir tidspunktet da helsesertifikatet ble utstedt.

Datoen i feltet «utstedt den» skal ikke være før DSC-ets gyldighetsperiode.

Kontrollørene kan anvende ytterligere tiltak for å begrense helsesertifikatets gyldighet på grunnlag av utstedelses-tidspunktet. Kravnøkkel 6 brukes for å identifisere dette kravet.

3.2.7. Kravet «helsesertifikat»

Kravet «helsesertifikat» (hcert) er et JSON-objekt (RFC 7159 ([6])) som inneholder opplysninger om helsestatus. Det kan finnes flere forskjellige typer helsesertifikat under samme krav, og DCC-et er et av dem.

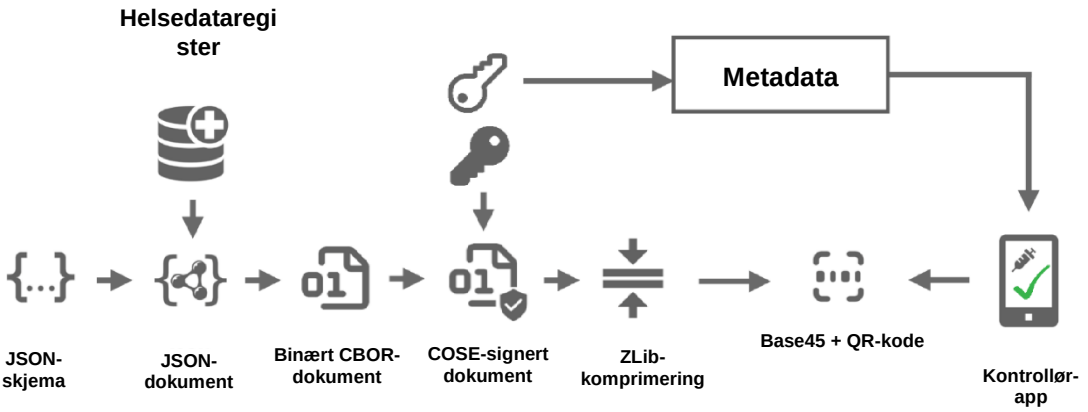
JSON er bare beregnet på bruk i skjemaer. Representasjonsformatet er CBOR, som definert i (RFC 7049([7])). Applikasjonsutviklere kan i praksis verken avkode eller kode til og fra JSON-formatet, men skal bruke minnestrukturen.

Den kravnøkkelen som skal brukes for å identifisere dette kravet, er -260.

Strenger i JSON-objektet bør normaliseres i samsvar med «Normalization Form Canonical Composition» (NFC) som er definert i Unicode-standarden. Avkodingsapplikasjoner bør imidlertid være romslige og robuste med hensyn til disse aspektene, og det oppfordres på det sterkeste til at enhver rimelig typekonvertering godtas. Dersom det i forbindelse med avkoding eller i etterfølgende sammenligningsfunksjoner blir funnet ikke-normaliserte data, bør utføringene skje som når inndata er normalisert til NFC.

4. **Serialisering og opprettelse av DCC-ets nyttedata**

Som serialiseringsmønster brukes følgende skjema:



Prosessen starter med at data utledes, for eksempel fra et helsedataregister (eller en ekstern datakilde), og de utledede dataene struktureres i samsvar med de definerte DCC-skjemaene. I denne prosessen kan konverteringen til det definerte dataformatet og omdanningen til et format som kan leses av mennesker, finne sted før serialiseringen til CBOR starter. Kravenes akronymer skal i hvert tilfelle koples til visningsnavnene før serialisering og etter avserialisering.

Valgfritt nasjonalt datainnhold er ikke tillatt i sertifikater utstedt i henhold til forordning (EU) 2021/953([8]). Datainnholdet er begrenset til de definerte dataelementene i det minstesettet av data som er angitt i vedlegget til forordning (EU) 2021/953.

([5]) rfc8392 (ietf.org)
([6]) rfc7159 (ietf.org)
([7]) rfc7049 (ietf.org)
([8]) Europaparlaments- og rådsforordning (EU) 2021/953 om en ramme for utstedelse, kontroll og godtakelse av interoperable covid-19-sertifikater for vaksinasjon, testing og restitusjon (EUs digitale covid-sertifikat) for å lette fri bevegelighet under covid-19-pandemien (EUT L 211 av 15.6.2021, s. 1).

5. **Transportkoding**

5.1. *Rådata*

I forbindelse med arbitrære datagrensesnitt kan HCERT og dets nyttedata overføres som de er, ved hjelp av enhver form for underliggende 8-bits sikker og pålitelig datatransport. Disse grensesnittene kan omfatte NFC (Near-Field Communication), Bluetooth eller overføring via en applikasjonslagsprotokoll, for eksempel overføring av et HCERT fra utstederen til en innehavers mobile enhet.

Dersom overføringen av HCERT fra utstederen til innehaveren er basert på et grensesnitt som bare brukes til presentasjon (for eksempel SMS, e-post), anvendes selvsagt ikke transportkoding av rådata.

5.2. *Strekkode*

5.2.1. Komprimering av nyttedata (CWT)

For å redusere størrelsen av HCERT og øke hastigheten og påliteligheten i forbindelse med leseprosessen skal CWT komprimeres ved hjelp av ZLIB (RFC 1950([9])) og «Deflate»-komprimeringsmekanismen i det formatet som er definert i RFC 1951([10]).

5.2.2. QR 2D-strekkode

For bedre å kunne håndtere eksisterende utstyr som er utformet for bruk av ASCII-nyttedata, kodes komprimert CWT som ASCII ved hjelp av Base45 før den kodes til en 2D-strekkode.

QR-formatet som definert i (ISO/IEC 18004:2015) skal brukes for å generere 2D-strekkoden. En feilkorrigeringsprosent «Q» (ca. 25 %) anbefales. Ettersom Base45 brukes, må QR-koden bruke alfanumerisk koding (modus 2, angitt med symbolene 0010).

For at kontrollørene skal kunne gjenkjenne den typen data som er kodet, og velge riktig avkodings- og behandlingssystem, skal Base45-kodede data (i henhold til denne spesifikasjonen) ha den foranstilte kontekst-identifikatorstrengen «HC1:». Framtidige versjoner av denne spesifikasjonen som påvirker bakoverkompatibilitet, skal definere en ny kontekstidentifikator, mens tegnet etter «HC» skal tas fra tegnsettet [1–9A–Z]. Rekkefølgen er fastsatt i samsvar med dette, dvs. først [1–9] og deretter [A–Z].

Det anbefales at den optiske koden gjengis på visningsmediet med en diagonal størrelse på mellom 35 mm og 60 mm for å kunne brukes i lesere med fastmontert optikk, der visningsmediet skal plasseres på leserens overflate.

Dersom den optiske koden trykkes på papir ved hjelp av skrivere med lav oppløsning (<300 dpi), må det påses at hvert symbol (prikk) i QR-koden vises som et nøyaktig kvadrat. Dersom skaleringen ikke er proporsjonal, vil noen rader eller kolonner i QR få rektangulære symboler, noe som i mange tilfeller vil gå ut over lesbarheten.

6. **Format for tillitslister (CSCA- og DSC-lister)**

Hver medlemsstat skal framlegge en liste over en eller flere nasjonale signerende sertifiseringsmyndigheter (Country Signing Certification Authorities (CSCA)) og en liste over alle gyldige dokumentsigneringssertifikater (Document Signer Certificates (DSC)), og skal oppdatere disse listene.

6.1. *Forenklet CSCA/DSC*

Fra og med denne versjonen av spesifikasjonene skal medlemsstatene ikke anta at det brukes opplysninger fra lister over tilbakekalte sertifikater (CRL-er), eller at bruksperioden for privat nøkkel blir kontrollert av kontrollørene.

I stedet kontrolleres gyldigheten primært gjennom en validering av at sertifikatet finnes i den seneste versjonen av denne sertifikatlisten.

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

6.2. *ICAO-PKI for maskinlesbare reisedokumenter (eMRTD) og tillitssentre (Trust Centers)*

Medlemsstatene kan bruke en egen CSCA – men kan også oversende sine eksisterende eMRTD CSCA-sertifikater og/eller DSC-er, og de kan velge å anskaffe disse fra (kommersielle) tillitssentre – og oversende disse. Eventuelle DSC-er må imidlertid alltid signeres av den CSCA-en som den berørte medlemsstaten har meddelt.

7. **Sikkerhetshensyn**

Når medlemsstatene utformer et system basert på denne spesifikasjonen, skal de identifisere, analysere og overvåke visse sikkerhetsaspekter.

Det bør tas hensyn til minst følgende aspekter:

7.1. *Gyldighetsperiode for HCERT-signaturen*

Utstederen av HCERT skal begrense signaturens gyldighetsperiode ved å angi et tidspunkt da gyldigheten utløper. Det innebærer at innehaveren av et helsesertifikat regelmessig må fornye det.

Den akseptable gyldighetsperioden kan fastsettes på grunnlag av praktiske begrensninger. Det kan for eksempel hende at en reisende ikke har mulighet til å fornye helsesertifikatet på en utenlandsreise. Det kan imidlertid også hende at en utsteder anser at det kan foreligge en viss sikkerhetsrisiko som krever at utstederen trekker tilbake et DSC (noe som innebærer at alle helsesertifikater som er utstedt ved bruk av denne nøkkelen, blir ugyldige selv om gyldighetsperioden ikke er utløpt). Konsekvensene av en slik hendelse kan begrenses ved regelmessig å skifte ut utstedernøkler og kreve fornyelse av alle helsesertifikater, med rimelige intervaller.

7.2. *Nøkkelforvaltning*

Denne spesifikasjonen bygger i høy grad på sterke krypteringsmekanismer for å sikre dataintegritet og autentisering av dataenes opprinnelse. Det er derfor nødvendig å behandle de private nøklene fortrolig.

For kryptonøkler kan fortroligheten kompromitteres på en rekke ulike måter, for eksempel følgende:

— Genereringen av nøkler kan være mangelfull og resultere i svake nøkler.

— Nøklene kan bli ubeskyttet på grunn av menneskelig feil.

— Nøklene kan bli stjålet av eksterne eller interne gjerningspersoner.

— Nøklene kan beregnes ved hjelp av kryptoanalyse.

For å redusere risikoen for at signeringsalgoritmen er for svak, slik at de private nøklene kan kompromitteres gjennom kryptoanalyse, anbefaler denne spesifikasjonen at alle deltakere innfører en sekundær signaturalgoritme som kan brukes som reserve, og som er basert på andre parametrer eller et annet matematisk problem enn den primære.

Når det gjelder de nevnte risikoene knyttet til utstedernes driftsmiljø, skal det gjennomføres risikoreduserende tiltak som sikrer effektiv kontroll, for eksempel generering, lagring og bruk av private nøkler i maskinvaresikkerhetsmoduler (HSM-er). Det oppfordres på det sterkeste til å bruke HSM-er for å signere helsesertifikater.

Uansett om en utsteder beslutter å bruke HSM-er eller ikke, bør det fastsettes en nøkkelutskiftingsplan der hyppigheten av nøkkelutskiftingene står i forhold til nøklenes eksponering mot eksterne nett, andre systemer og personale. En velvalgt utskiftingsplan begrenser også risikoene som er knyttet til feilaktig utstedte helsesertifikater, ettersom den gjør det mulig for en utsteder å tilbakekalle slike helsesertifikater gruppevis ved å trekke tilbake en nøkkel, dersom det er nødvendig.

7.3. *Validering av inndata*

Disse spesifikasjonene kan brukes på en måte som innebærer at data fra upålitelige kilder mottas av systemer av oppgavekritisk art. For å redusere risikoene som er knyttet til denne angrepsvektoren, må alle inndatafelter valideres på behørig måte med hensyn til datatype, lengde og innhold. Utstedersignaturen skal også kontrolleres før HCERT-innholdet behandles. Valideringen av utstedersignaturen innebærer imidlertid at utstederens beskyttede konvolutt (Protected Issuer Header) analyseres først, og en mulig angriper kan forsøke å legge inn informasjon som er nøye utformet med sikte på å kompromittere systemets sikkerhet.

8. **Tillitsforvaltning**

For å kontrollere HCERT-signaturen kreves en offentlig nøkkel. Medlemsstatene skal gjøre disse offentlige nøklene tilgjengelige. I siste instans må hver kontrollør ha en liste over alle offentlige nøkler som den velger å ha tillit til (ettersom den offentlige nøkkelen ikke er en del av HCERT).

Systemet består av (bare) to lag: For hver medlemsstat skal det finnes et eller flere landsspesifikke sertifikater, som hvert for seg signerer et eller flere dokumentsigneringssertifikater som brukes i den daglige virksomheten.

Medlemsstatens sertifikater kalles CSCA-sertifikater (Country Signing Certificate Authority certificates) og er (vanligvis) egensignerte sertifikater. Medlemsstatene kan ha flere enn ett (for eksempel ved regional desentralisering). Disse CSCA-sertifikatene signerer regelmessig de dokumentsigneringssertifikatene (DSC-ene) som brukes for å signere HCERT-er.

«Sekretariatet» er en funksjonell rolle. Det skal regelmessig samle og offentliggjøre medlemsstatenes DSC-er etter å ha kontrollert dem mot listen over CSCA-sertifikater (som er overført og kontrollert på annen måte).

Den resulterende listen over DSC-er inneholder det aggregerte settet av akseptable offentlige nøkler (og tilhørende kid) som kontrollører kan bruke for å validere signaturene i forbindelse med HCERT-ene. Kontrollørene må regelmessig hente og oppdatere denne listen.

Slike medlemsstatsspesifikke lister kan tilpasses det formatet som er egnet for de nasjonale forholdene. Filformatet for denne tillitslisten kan variere, og kan for eksempel være et signert JWKS (JWK-Set-format i samsvar med RFC 7517([11]), avsnitt 5), eller et annet format som er spesifikt for den teknologien som brukes i den berørte medlemsstaten.

For å sikre enkelhet kan medlemsstatene enten oversende sine eksisterende CSCA-sertifikater fra sine ICAO eMRTD-systemer eller, som anbefalt av WHO, opprette et eget sertifikat for dette helseområdet.

8.1. *Nøkkelidentifikatoren (Key Identifier, (kid))*

Nøkkelidentifikatoren (kid) beregnes når det utarbeides en liste over pålitelige offentlige nøkler fra DSC-er, og består av et trunkert (første 8 byte) SHA-256-fingeravtrykk fra DSC-et som er kodet i DER-format (råformat).

Kontrollørene trenger ikke å beregne kid på grunnlag av DSC-et, men kan direkte kople nøkkelidentifikatoren i det utstedte helsesertifikatet til tilsvarende kid på tillitslisten.

8.2. *Forskjeller sammenlignet med ICAO eMRTD PKI-tillitsmodellen*

Beste praksis fra ICAO eMRTD PKI-tillitsmodellen er brukt som mønster, men en rekke forenklinger skal foretas for å øke hastigheten:

— En medlemsstat kan sende inn flere CSCA-sertifikater.

— Gyldighetsperioden for DSC-et (nøkkelbruk) kan fastsettes til en hvilken som helst varighet som ikke overskrider CSCA-sertifikatets gyldighetsperiode, og kan utelates.

— DSC-et kan inneholde politikkidentifikatorer (utvidet nøkkelbruk) som er spesifikke for helsesertifikater.

— Medlemsstatene kan velge å aldri foreta kontroll av offentliggjorte tilbakekallinger, men i stedet utelukkende støtte seg til de DSC-listene som de daglig får fra sekretariatet eller selv sammenstiller.

———

([11]) rfc7517 (ietf.org)

VEDLEGG II

REGLER FOR UTFYLLING AV EUs DIGITALE COVID-SERTIFIKAT

De alminnelige reglene for verdisettene fastsatt i dette vedlegget har som mål å sikre interoperabilitet på semantisk nivå og skal muliggjøre ensartet teknisk gjennomføring for DCC. Elementene i dette vedlegget kan brukes for de tre ulike situasjonene (vaksinasjon/testing/restitusjon), som fastsatt i forordning (EU) 2021/953. Bare de elementene som krever semantisk standardisering gjennom kodede verdisett, er oppført i dette vedlegget.

Medlemsstatene har ansvar for å oversette de kodede elementene til det nasjonale språket.

For alle datafelter som ikke er nevnt i beskrivelsene av verdisett nedenfor, anbefales koding i UTF-8 (navn, testsenter, sertifikatutsteder). Det anbefales at datafelter som inneholder kalenderdatoer (fødselsdato, vaksinasjonsdato, testdato, dato for første positive testresultat, sertifikatets gyldighetsdatoer), kodes i henhold til ISO 8601.

Dersom de foretrukne kodesystemene angitt nedenfor av en eller annen grunn ikke kan benyttes, kan andre internasjonale kodesystemer benyttes, og det bør gis råd om hvordan kodene fra det andre kodesystemet skal knyttes til det foretrukne kodesystemet. Tekst (visningsnavn) kan unntaksvis brukes som reserveløsning når det ikke finnes en egnet kode i de definerte verdisettene.

Medlemsstater som bruker andre koder i sine systemer, bør knytte slike koder til de beskrevne verdisettene. Medlemsstatene er ansvarlige for slike tilknytninger.

Kommisjonen skal regelmessig oppdatere verdisettene med støtte fra nettverket for e-helsetjenester og Helsesikkerhetskomiteen. De oppdaterte verdisettene skal offentliggjøres på Kommisjonens relevante nettsted samt på nettsiden til nettverket for e-helsetjenester. En endringshistorikk bør framlegges.

1. **Aktuell sykdom eller aktuelt smittestoff / Sykdom eller smittestoff som innehaveren er friskmeldt etter å ha hatt Covid-19 (SARS-CoV-2 eller en variant av dette)**

   Foretrukket kodesystem: SNOMED CT.

   Skal brukes i sertifikat 1, 2 og 3.

   De valgte kodene skal vise til covid-19 eller, dersom det er behov for mer detaljerte opplysninger om den genetiske varianten av SARS-CoV-2, til disse variantene dersom det av epidemiologiske årsaker er behov for slike detaljerte opplysninger.

   Et eksempel på en kode som bør brukes, er SNOMED CT-koden 840539006 (covid-19).

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

   Foretrukket kodesystem: SNOMED CT eller ATC-klassifisering.

   Skal brukes i sertifikat 1.

   Eksempler på koder som skal brukes fra de foretrukne kodesystemene, er SNOMED CT-koden 1119305005 (SARS-CoV-2-antigenvaksine), 1119349007 (SARS-CoV-2-mRNA-vaksine) eller J07BX03 (covid-19-vaksiner). Verdisettet bør utvides når nye vaksinetyper utvikles og tas i bruk.

3. **Covid-19-vaksinelegemiddel**

   Foretrukne kodesystemer (i prioritert rekkefølge):

   — Unionens register over legemidler for vaksiner med EU-godkjenning (godkjenningsnumre)

   — Et globalt vaksineregister, for eksempel et register som kan opprettes av Verdens helseorganisasjon.

   — Vaksinelegemiddelets navn i andre tilfeller. Dersom navnet omfatter blanktegn, skal disse erstattes med en bindestrek (-).

Verdisettets navn: Vaksine.

Skal brukes i sertifikat 1.

Et eksempel på en kode som bør brukes, fra de foretrukne kodesystemene, er EU/1/20/1528 (Comirnaty). Et eksempel på vaksinenavnet som skal brukes som kode: Sputnik-V (står for Sputnik V).

4. **Innehaver av markedsføringstillatelse for covid-19-vaksinen eller covid-19-vaksineprodusent**

Foretrukket kodesystem:

— Organisasjonskode fra EMA (SPOR-system for ISO IDMP)

— Et globalt register over innehavere av markedsføringstillatelser for vaksiner eller vaksineprodusenter, for eksempel et register som kan opprettes av Verdens helseorganisasjon.

— Organisasjonens navn i andre tilfeller. Dersom navnet omfatter blanktegn, skal disse erstattes med en bindestrek (-).

Skal brukes i sertifikat 1.

Eksempel på en kode som bør brukes, fra det foretrukne kodesystemet, er ORG-100001699 (AstraZeneca AB). Et eksempel på organisasjonsnavnet som skal brukes som kode: Sinovac-Biotech (står for Sinovac Biotech).

5. **Nummer i en serie av doser og samlet antall doser i serien**

Skal brukes i sertifikat 1.

To felter:

1) Nummer på dose som tilføres i en syklus.

2) Antall forventede doser i en hel syklus (spesifikt for en person på det tidspunktet dosen mottas)

For eksempel angir 1/1, 2/2 at syklusen er fullført, inkludert alternativet 1/1 for vaksiner som omfatter to doser, men der det i henhold til protokollen som medlemsstaten anvender, skal gis én dose til borgere som er diagnostisert med covid-19 før vaksinasjonen. Samlet antall doser i serien skal angis i henhold til de opplysningene som er tilgjengelige på det tidspunktet dosen tilføres. Dersom en bestemt vaksine for eksempel krever en tredje dose (påfyllingsdose) på tidspunktet for den siste tilførte dosen, skal det andre nummeret i feltet gjenspeile dette (for eksempel 2/3, 3/3 osv.).

6. **Navn på medlemsstaten eller tredjelandet der vaksinen ble gitt / testen ble utført**

Foretrukket kodesystem: Landkoder i henhold til ISO 3166.

Skal brukes i sertifikat 1, 2 og 3.

Verdisettets innhold: Den fullstendige listen over koder med to bokstaver, som er tilgjengelig som et verdisett definert i FHIR (http://hl7.org/fhir/ValueSet/iso3166-1-2).

7. **Testtype**

Foretrukket kodesystem: LOINC.

Skal brukes i sertifikat 2, og i sertifikat 3 dersom en delegert rettsakt innebærer at utstedelsen av restitusjonssertifikater som er basert på andre typer tester enn NAAT, støttes.

Kodene i dette verdisettet skal vise til testmetoden og skal minst skille mellom NAAT-tester og RAT-tester, som angitt i forordning (EU) 2021/953.

Et eksempel på en kode som bør brukes, fra det foretrukne kodesystemet, er LP217198-3 (hurtig immunologisk analyse).

8. **Den benyttede testens produsent og handelsnavn (valgfritt i forbindelse med NAAT-test)**

Foretrukket kodesystem: Helsesikkerhetskomiteens (HSCs) liste over antigen-hurtigtester, som føres av Det felles forskningssenter (FFS) (database for utstyr til in vitro-diagnostikk og testmetoder for covid-19).

Skal brukes i sertifikat 2.

Datasettets innhold skal omfatte utvalget av antigen-hurtigtester som er oppført på den felles og oppdaterte listen over covid-19-antigen-hurtigtester som er fastsatt på grunnlag av rådsrekommandasjon 2021/C 24/01 og godkjent av Helsesikkerhetskomiteen. Listen føres av FFS i databasen for utstyr til in vitro-diagnostikk og testmetoder for covid-19: https://covid-19-diagnostics.jrc.ec.europa.eu/devices/hsc-common-recognition-rat

I dette kodesystemet benyttes de relevante feltene, for eksempel identifikatoren for testutstyret, testens navn og produsentens navn, i samsvar med FFSs strukturerte format, som finnes på https://covid-19-diagnostics.jrc.ec.europa.eu/devices.

9. **Testresultat**

Foretrukket kodesystem: SNOMED CT.

Skal brukes i sertifikat 2.

De valgte kodene skal gjøre det mulig å skille mellom positive og negative testresultater (påvist eller ikke påvist). Ytterligere verdier (f.eks. ikke-fastsatt) kan legges til dersom det er nødvendig i brukstilfellene.

Eksempler på koder som bør brukes, fra det foretrukne kodesystemet, er 260415000 (Ikke påvist) og 260373001 (Påvist).

———

VEDLEGG III

FELLES STRUKTUR FOR DEN UNIKE SERTIFIKATIDENTIFIKATOREN

1. **Innledning**

Hvert av EUs digitale covid-sertifikater (DCC-er) skal inneholde en unik sertifikatidentifikator (Unique Certificate Identifier (UCI)), som støtter DCC-enes interoperabilitet. UCI-en kan brukes for å kontrollere sertifikatet. Medlemsstatene skal være ansvarlige for innføringen av UCI-en. UCI-en er et middel til å kontrollere sertifikatets ekthet og, når det er relevant, til å opprette kopling til et registreringssystem (f.eks. et IIS (Immunisation Information System)). Disse identifikatorene skal også gjøre det mulig for medlemsstatene å bekrefte (på papir og digitalt) at enkeltpersoner har blitt vaksinert eller testet.

2. **Den unike sertifikatidentifikatorens oppbygning**

UCI-en skal følge en felles struktur og et felles format som gjør det lettere for mennesker og/eller maskiner å tolke informasjonen, og kan omfatte elementer som for eksempel vaksinasjonsmedlemsstaten, selve vaksinen og en medlemsstatsspesifikk identifikator. Dette gir medlemsstatene mulighet til å være fleksible når de utformer UCI-ens format, i fullt samsvar med personvernregelverket. De enkelte elementenes rekkefølge er basert på et definert hierarki som gjør det mulig å foreta framtidige endringer av blokkene, samtidig som deres strukturelle integritet opprettholdes.

De mulige løsningene for oppbygningen av UCI-en utgjør et spektrum der modularitet og mulighet for menneskelig tolkning er de to viktigste diversifiseringsparametrene og et grunnleggende kjennetegn:

— Modularitet: i hvilken grad koden består av atskilte byggesteiner som inneholder semantisk forskjellige opplysninger

— Mulighet for menneskelig tolkning: I hvilken grad koden er meningsfull eller kan tolkes av det mennesket som leser den

— Globalt unik: Identifikatoren for landet eller myndigheten forvaltes på en god måte, og det forventes at hvert land (hver myndighet) forvalter sitt segment av navneområdet nøye ved aldri å gjenbruke eller gjenutstede identifikatorer. Kombinasjonen av dette sikrer at hver identifikator er globalt unik.

3. **Generelle krav**

Følgende overordnede krav bør oppfylles i forbindelse med UCI-en:

1) Tegnsett: Bare store bokstaver og alfanumeriske tegn i US-ASCII-tegnsettet («A» til «Z» og «0» til «9») er tillatt, supplert med ytterligere spesialtegn fra RFC3986([1]) ([2]) for å atskille elementer, dvs. {«/», «#»,«:»}.

2) Maksimal lengde: Utviklerne bør helst ikke overskride en lengde på 27–30 tegn([3]).

3) Versjonsprefiks: Dette viser til versjonen av UCI-skjemaet. Versjonsprefikset er «01» for denne versjonen av dokumentet. Versjonsprefikset består av to sifre.

4) Landprefiks: Landkoden angis i samsvar med ISO 3166-1. Lengre koder (dvs. med tre eller flere tegn (for eksempel «UNHCR») er forbeholdt framtidig bruk.

5) Kodesuffiks/kontrollsum:

5.1. Medlemsstatene bør bruke en kontrollsum når det er sannsynlig at overføring, transkripsjon (foretatt av mennesker) eller andre uønskede endringer kan forekomme (dvs. ved anvendelse i trykt form).).

5.2. Kontrollsummen skal ikke brukes for å validere sertifikatet, og er ikke teknisk sett en del av identifikatoren, men brukes for å kontrollere kodens integritet. Denne kontrollsummen bør oppsummere hele UCI-en i digitalt/elektronisk overførbart format i henhold til ISO-7812-1 (LUHN-10)([4]). Kontrollsummen skilles fra resten av UCI-en med tegnet #.

([1]) rfc3986 (ietf.org)

([2]) Felter til f.eks. kjønn, produksjons-/partinummer, vaksinasjonssenter, identifisering av helsepersonell eller neste vaksinasjonsdato kan eventuelt være nødvendige bare for medisinske formål.

([3]) For utføring med QR-koder kan medlemsstatene vurdere å bruke et tilleggssett av tegn opp til en samlet lengde på 72 tegn (inkludert de 27–30 tegnene for selve identifikatoren), som kan brukes til andre opplysninger. Medlemsstatene skal selv definere spesifikasjonen for disse opplysningene.

([4]) Luhn mod N-algoritmen er en utvidelse av Luhn-algoritmen (også kjent som mod 10-algoritmen), som fungerer for numeriske koder og brukes for eksempel for å beregne kontrollsummen for kredittkort. Utvidelsen gjør det mulig for algoritmen å arbeide med sekvenser av verdier (i vårt tilfelle alfanumeriske tegn) i enhver base.

Bakoverkompatibilitet bør sikres: Medlemsstater som over tid endrer strukturen på sine identifikatorer (i hovedversjonen, som for tiden er v1), må sikre at to identifikatorer som er identiske, representerer det samme vaksinasjonssertifikatet / den samme vaksinasjonsbekreftelsen. Med andre ord kan medlemsstatene ikke gjenbruke identifikatorer.

4. **Alternativer til unike sertifikatidentifikatorer for vaksinasjonssertifikater**

«Guidelines on Verifiable Vaccination Certificates – Basic Interoperability Elements»([5]) fra nettverket for e-helsetjenester omhandler ulike alternativer som er tilgjengelige for medlemsstatene og andre parter, og som kan anvendes samtidig av ulike medlemsstater. Medlemsstatene kan benytte slike ulike alternativer i ulike versjoner av UCI-skjemaet.

———

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

VEDLEGG IV

FORVALTNING AV OFFENTLIG-NØKKEL-SERTIFIKATER

1. **Innledning**

Sikker og pålitelig utveksling av signaturnøkler for EUs digitale covid-sertifikater (DCC-er) mellom medlemsstatene gjennomføres via portalen for EUs digitale covid-sertifikat (DCCG), som fungerer som et sentralt datalager for de offentlige nøklene. Gjennom DCCG kan medlemsstatene offentliggjøre de offentlige nøklene som motsvarer de private nøklene som brukes for å signere digitale covid-sertifikater. Deltakende medlemsstater kan bruke DCCG for raskt å hente oppdaterte opplysninger om offentlige nøkler. Senere kan DCCG utvides til å omfatte utveksling av pålitelige tilleggsopplysninger som medlemsstatene stiller til rådighet, for eksempel valideringsregler for DCC-er. Tillitsmodellen for DCC-rammen er en infrastruktur for offentlige nøkler (PKI). Hver medlemsstat har en eller flere nasjonale signerende sertifiseringsmyndigheter (Country Signing Certification Authorities (CSCA)), hvis sertifikater har forholdsvis lang gyldighet. Som følge av medlemsstatens beslutning kan denne CSCA-en være den samme eller en annen enn den CSCA-en som benyttes i forbindelse med maskinleselige reisedokumenter. CSCA-en utsteder offentlig-nøkkel-sertifikater til de nasjonale, kortvarige dokumentsunderskriverne (dvs. de som underskriver DCC-er), som kalles dokumentsigneringssertifikater (Document Signer Certificates (DSC-er)). CSCA-en fungerer som et tillitsanker slik at deltakende medlemsstater kan bruke CSCA-sertifikatet for å validere de regelmessig endrede DSC-enes autentisitet og integritet. Når disse sertifikatene er validert, kan medlemsstatene overføre dem (eller bare de offentlige nøklene de inneholder) til sine DCC-valideringsapplikasjoner. I tillegg til CSCA-er og DSC-er benytter DCCG også PKI for å autentisere transaksjoner, signere data som grunnlag for autentisering og sikre integriteten til kommunikasjonskanalene mellom medlemsstatene og DCCG.

Digitale signaturer kan brukes for å oppnå dataintegritet og -autentisitet. Infrastrukturer for offentlige nøkler skaper tillit gjennom å kople offentlige nøkler til kontrollerte identiteter (eller utstedere). Dette er nødvendig for at andre deltakere skal kunne kontrollere dataenes opprinnelse og kommunikasjonspartnerens identitet og treffe beslutning om tillit. I DCCG brukes flere offentlig-nøkkel-sertifikater for å kontrollere autentisiteten. I dette vedlegget fastsettes hvilke offentlig-nøkkel-sertifikater som skal brukes, og hvordan de skal utformes for å muliggjøre bred interoperabilitet mellom medlemsstatene. Det inneholder nærmere opplysninger om de nødvendige offentlig-nøkkel-sertifikatene, og det gir veiledning om sertifikatmaler og gyldighetsperioder for medlemsstater som ønsker å drive sin egen CSCA. Ettersom DCC-er skal kunne kontrolleres innenfor en fastsatt tidsramme (fra utstedelsen til gyldighetsperiodens utløp), er det nødvendig å fastsette en kontrollmodell for alle signaturer som anvendes i offentlig-nøkkel-sertifikatene og DCC-ene.

2. **Terminologi**

Tabellen nedenfor inneholder forkortelser og terminologi som brukes i dette vedlegget.

Begrep	Definisjon
Sertifikat	Eller offentlig-nøkkel-sertifikat. Et X.509 v3-sertifikat som inneholder en enhets offentlige nøkkel
CSCA	Nasjonal signerende sertifiseringsmyndighet
DCC	EUs digitale covid-sertifikat Et signert digitalt dokument med opplysninger om vaksinasjon, testing eller restitusjon
DCCG	Portalen for EUs digitale covid-sertifikat. Dette systemet brukes for å utveksle DSC-er mellom medlemsstatene
$DCCG_{TA}$	DCCGs tillitsankersertifikat. Den motsvarende private nøkkelen brukes for å signere listen over alle CSCA-sertifikater uten bruk av internett
$DCCG_{TLS}$	DCCGs TLS-serversertifikat
DSC	Dokumentsigneringssertifikat. Offentlig-nøkkel-sertifikatet for en medlemsstats dokumentsigneringsmyndighet (for eksempel et system som har tillatelse til å signere DCC-er). Dette sertifikatet utstedes av medlemsstatens CSCA
EC-DSA	Digital signaturalgoritme for elliptisk kurve (Elliptic Curve Digital Signature Algorithm) En kryptografisk signaturalgoritme basert på elliptiske kurver
Medlemsstat	Medlemsstat i Den europeiske union

Begrep	Definisjon
mTLS	Gjensidig TLS. Transportlagssikkerhetsprotokoll med gjensidig autentisering
NB	En medlemsstats nasjonale «backend»
NB_{CSCA}	En medlemsstats CSCA-sertifikat (kan være flere enn ett)
NB_{TLS}	TLS-klientautentiseringssertifikatet for en nasjonal «backend»
NB_{UP}	Sertifikatet som en nasjonal «backend» bruker for å signere datapakker som er lastet opp til DCCG
PKI	Infrastruktur for offentlige nøkler (Public Key Infrastructure) Tillitsmodell basert på offentlig-nøkkel-sertifikater og sertifiseringsmyndigheter
RSA	Asymmetrisk krypteringsalgoritme basert på heltallsfaktorisering, som benyttes for digitale signaturer eller asymmetrisk kryptering

3. DCCGs kommunikasjonsstrømmer og sikkerhetstjenester

Dette avsnittet gir en oversikt over kommunikasjonsstrømmene og sikkerhetstjenestene i DCCG-systemet. Det fastsetter også hvilke nøkler og sertifikater som brukes for å beskytte kommunikasjonen, opplastede opplysninger, DCC-ene og en signert tillitsliste som omfatter alle de CSCA-sertifikatene som inngår. DCCG fungerer som en dataplattform som gjør det mulig for medlemsstatene å utveksle signerte datapakker.

De opplastede datapakkene leveres av DCCG i uendret stand, som betyr at DCCG ikke tilføyer eller sletter DSC-er fra de pakkene den mottar. Medlemsstatenes nasjonale backend (NB) skal kunne kontrollere de opplastede dataenes integritet og autentisitet fra begynnelse til slutt. I tillegg til dette vil nasjonale «backends» og DCCG benytte gjensidig TLS-autentisering for å opprette en sikker forbindelse. Dette kommer i tillegg til signaturene i de utvekslede dataene.

3.1. *Autentisering og opprettelse av forbindelse*

DCCG bruker transportlagsikkerhet (TLS) med gjensidig autentisering for å opprette en autentisert kryptert kanal mellom medlemsstatens nasjonale «backends» (NB) og portalmiljøet. DCCG har derfor et TLS-serversertifikat, forkortet $DCCG_{TLS}$, og nasjonale «backends» har et TLS-klientsertifikat – forkortet NB_{TLS}. Sertifikatmaler er angitt i *avsnitt 5*. Alle nasjonale «backends» kan utstede sitt eget TLS-sertifikat. Dette sertifikatet vil bli uttrykkelig hvitlistet og kan dermed utstedes av en offentlig betrodd sertifiseringsmyndighet (for eksempel en sertifiseringsmyndighet som følger CAB-forumets basiskrav) eller en nasjonal sertifiseringsmyndighet, eller det kan være egensignert. Hver medlemsstat er ansvarlig for sine nasjonale data og for å beskytte den private nøkkelen som brukes for å opprette forbindelsen til DCCG. Tilnærmingen basert på å «ta med sitt eget sertifikat» krever en veldefinert registrerings- og identifikasjonsprosess samt prosedyrer for tilbakekalling og fornyelse som beskrevet i *avsnitt 4.1, 4.2* og *4.3*. DCCG bruker en hvitliste der TLS-sertifikater for NB-er tilføyes etter gjennomført registrering. Bare NB-er som autentiserer seg med en privat nøkkel som motsvarer et sertifikat fra hvitlisten, kan opprette en sikker forbindelse til DCCG. DCCG vil også bruke et TLS-sertifikat som gjør det mulig for NB-ene å kontrollere at de faktisk oppretter en forbindelse til den ekte DCCG-en, og ikke til en ondsinnet enhet som utgir seg for å være DCCG. DCCGs sertifikat vil bli utstedt til NB-ene etter gjennomført registrering. $DCCG_{TLS}$-sertifikatet vil bli utstedt av en offentlig betrodd sertifiseringsmyndighet (CA) (inngår i alle større nettlesere). Medlemsstatene har ansvar for å kontrollere at deres forbindelse til DCCG-en er sikker (for eksempel ved å kontrollere fingeravtrykket i $DCCG_{TLS}$-sertifikatet for den serveren som det opprettes forbindelse til, mot fingeravtrykket etter registreringen).

3.2. *Nasjonal signerende sertifiseringsmyndighet (CSCA) og valideringsmodell*

Medlemsstater som deltar i DCCG-rammen, må benytte en CSCA for å utstede DSC-er. Medlemsstatene kan ha flere enn én CSCA, for eksempel ved regional desentralisering. Hver medlemsstat kan enten benytte eksisterende sertifiseringsmyndigheter eller opprette en egen (eventuelt egensignert) sertifiseringsmyndighet for DCC-systemet.

Medlemsstatene må framlegge sine CSCA-sertifikater for DCCG-operatøren i forbindelse med den offisielle «onboarding»-prosedyren. Når registreringen av medlemsstaten er gjennomført (nærmere opplysninger finnes i *avsnitt 4.1*), vil DCCG-operatøren oppdatere en signert tillitsliste som omfatter alle CSCA-sertifikater som er aktive innenfor DCC-rammen. DCCG-operatøren vil bruke et eget nøkkelpar for å signere tillitslisten og sertifikatene i et offline-miljø. Den private nøkkelen vil ikke bli lagret i det nettbaserte DCCG-systemet, slik at en eventuell sikkerhetsbrist i det nettbaserte systemet ikke gjør det mulig for en angriper å kompromittere tillitslisten. Det tilsvarende tillitsanker-sertifikatet $DCCG_{TA}$ vil bli stilt til rådighet for nasjonale «backends» i forbindelse med «onboarding»-prosessen.

Medlemsstatene kan hente tillitslisten fra DCCG for kontrollformål. CSCA er definert som den sertifiseringsmyndigheten som utsteder DSC-er, og medlemsstater som benytter et CA-hierarki med flere nivåer (for eksempel rot-CA -> CSCA -> DSC-er), må derfor stille den underordnede sertifiseringsmyndigheten som utsteder DSC-er, til rådighet. Dersom en medlemsstat benytter en eksisterende sertifiseringsmyndighet, vil DCC-systemet ignorere alt over CSCA-nivået og hvitliste bare CSCA-en som tillitsanker (selv om den er en underordnet CA). Dette skyldes at ICAO-modellen tillater bare to nivåer – en rot-CSCA og et underordnet («leaf») DSC som signeres av bare denne CSCA-en.

Dersom en medlemsstat driver sin egen CSCA, er medlemsstaten ansvarlig for en sikker drift og nøkkelforvaltning for denne CA-en. CSCA fungerer som tillitsanker for DSC-er, og det er derfor avgjørende for DCC-miljøets integritet at CSCAs private nøkkel beskyttes. Kontrollmodellen i DCC PKI er skallmodellen, som angir at alle sertifikater som omfattes av valideringen av sertifikatstien må være gyldige på et gitt tidspunkt (dvs. tidspunktet for validering av signaturen). Derfor gjelder følgende begrensninger:

— CSCA skal ikke utstede sertifikater som har lengre gyldighet enn sertifiseringsmyndighetens eget sertifikat (CA-sertifikatet).

— Dokumentunderskriveren skal ikke signere dokumenter som har lengre gyldighet enn DSC-et.

— Medlemsstater som driver sin egen CSCA, må fastsette gyldighetsperioder for sine CSCA-er og alle utstedte sertifikater, og de må sikre at sertifikatene fornyes.

Avsnitt 4.2 inneholder anbefalinger om gyldighetsperioder.

3.3. *De opplastede dataenes integritet og autentisitet*

Nasjonale «backends» kan bruke DCCG til opp- og nedlasting av digitalt signerte datapakker etter gjennomført gjensidig autentisering. I begynnelsen inneholder disse datapakkene medlemsstatenes DSC-er. Det nøkkelparet som brukes av nasjonal «backend» for den digitale signaturen av datapakker som lastes opp i DCCG-systemet, kalles nasjonal «backends» nøkkelpar for opplastingssignatur, og det motsvarende offentlig-nøkkel-sertifikatet kalles NB_{UP}-sertifikatet. Hver medlemsstat har sitt eget NB_{UP}-sertifikat, som kan være egensignert eller utstedt av en eksisterende sertifiseringsmyndighet, for eksempel en offentlig sertifiseringsmyndighet (dvs. en sertifiseringsmyndighet som utsteder sertifikater i samsvar med CAB-forumets basiskrav). NB_{UP}-sertifikatet skal være forskjellig fra andre sertifikater som brukes av medlemsstaten (dvs. CSCA-sertifikater, TLS-klientsertifikater og DSC-er).

Medlemsstatene må framlegge opplastingssertifikatet for DCCG-operatøren i forbindelse med den innledende registreringsprosedyren (nærmere opplysninger finnes i *avsnitt 4.1*). Hver medlemsstat er ansvarlig for sine nasjonale data, og den må beskytte den private nøkkelen som brukes for å signere opplastingene.

Andre medlemsstater kan kontrollere de signerte datapakkene ved hjelp av opplastingssertifikatene fra DCCG. DCCG kontrollerer de opplastede dataenes autentisitet og integritet mot NB-opplastingssertifikatet før dataene stilles til rådighet for andre medlemsstater.

3.4. *Krav til den tekniske DCCG-arkitekturen*

For den tekniske DCCG-arkitekturen gjelder følgende krav:

— DCCG bruker gjensidig TLS-autentisering for å opprette en autentisert kryptert forbindelse til NB-ene. DCCG fører derfor en hvitliste over registrerte NB_{TLS}-klientsertifikater.

— DCCG bruker to digitale sertifikater ($DCCG_{TLS}$ og $DCCG_{TA}$) med to forskjellige nøkkelpar. Den private nøkkelen for $DCCG_{TA}$-nøkkelparet oppbevares offline (ikke på de nettbaserte komponentene for DCCG).

— DCCG fører en tillitsliste over NB_{CSCA}-sertifikater som er signert med den private nøkkelen for $DCCG_{TA}$.

— Krypteringen som benyttes, skal oppfylle kravene i *avsnitt 5.1*.

4. **Livssyklusforvaltning av sertifikater**

4.1. *Registrering av nasjonale «backends»*

Medlemsstatene må registrere seg hos DCCG-operatøren for å delta i DCCG-systemet. I dette avsnittet beskrives den tekniske og operasjonelle prosedyren som skal følges for å registrere en nasjonal «backend».

DCCG-operatøren og medlemsstaten må utveksle opplysninger om tekniske kontaktpersoner i forbindelse med «onboarding»-prosessen. Det antas at de tekniske kontaktpersonene er legitimert av sine medlemsstater, og at identifiseringen/autentiseringen foretas via andre kanaler. Autentiseringen kan for eksempel gjennomføres ved at en medlemsstats tekniske kontakt sender sertifikatene som passordkrypterte filer via e-post og gir DCCG-operatøren det tilsvarende passordet per telefon. Det kan også brukes andre sikre kanaler som DCCG-operatøren fastsetter.

Medlemsstaten må inngi tre digitale sertifikater i forbindelse med registrerings- og identifiseringsprosessen:

— Medlemsstatens TLS-sertifikat NB_{TLS}

— Medlemsstatens opplastingssertifikat NB_{UP}

— Medlemsstatens CSCA-sertifikat(er) NB_{CSCA}

Alle inngitte sertifikater skal oppfylle kravene i *avsnitt 5*. DCCG-operatøren vil kontrollere at det inngitte sertifikatet oppfyller kravene i *avsnitt 5*. Etter identifisering og registrering skal DCCG-operatøren

— tilføye NB_{CSCA}-sertifikatet eller -sertifikatene på tillitslisten som er signert med den private nøkkelen som motsvarer den offentlige nøkkelen for $DCCG_{TA}$,

— tilføye NB_{TLS}-sertifikatet på hvitlisten for sluttpunktet for DCCG TLS,

— tilføye NB_{UP}-sertifikatet til DCCG-systemet,

— stille offentlig-nøkkel-sertifikatet for $DCCG_{TA}$ og $DCCG_{TLS}$ til rådighet for medlemsstaten.

4.2. *Sertifiseringsmyndigheter, gyldighetsperioder og fornyelse*

Dersom en medlemsstat ønsker å drive sin egen CSCA, kan CSCA-sertifikatene være egensignerte sertifikater. De fungerer som tillitsanker for medlemsstaten, og medlemsstaten må derfor ha en sterk beskyttelse for den private nøkkelen som motsvarer CSCA-sertifikatets offentlige nøkkel. Det anbefales at medlemsstatene bruker et offline-system for sine CSCA-er, dvs. et datasystem som ikke er koplet til noe nettverk. Det skal foretas flerpersonskontroll for å gi tilgang til systemet (f.eks. etter prinsippet om fire øyne). Etter signering av DSC-er skal det foretas operasjonell kontroll, og det systemet som oppbevarer den private CSCA-nøkkelen, skal lagres på en sikker måte med strenge tilgangskontroller. Maskinvaresikkerhetsmoduler eller smartkort kan brukes for å beskytte den private CSCA-nøkkelen ytterligere. I digitale sertifikater angis en gyldighetsperiode som gjør det nødvendig å fornye dem. Fornyelse er nødvendig for å ta i bruk nye kryptonøkler og for å tilpasse nøklenes størrelse når datateknikken videreutvikles eller nye angrep truer sikkerheten for den krypteringsalgoritmen som brukes. Skallmodellen benyttes (se *avsnitt 3.2*).

Følgende gyldighetsperioder anbefales i betraktning av de digitale covid-sertifikatenes gyldighetsperiode på ett år:

— CSCA: 4 år

— DSC: 2 år

— Opplasting: 1–2 år

— TLS-klientautentisering: 1–2 år

For at fornyelsen skal skje i rett tid, anbefales følgende bruksperioder for de private nøklene:

— CSCA: 1 år

— DSC: 6 måneder

Medlemsstatene skal opprette nye opplastingssertifikater og TLS-sertifikater i god tid, f.eks. en måned før bruken av den private nøkkelen opphører, for å unngå driftsproblemer. CSCA-sertifikater og DSC-er bør fornyes minst en måned før bruken av den private nøkkelen opphører (i betraktning av de nødvendige operasjonelle prosedyrene). Medlemsstatene må levere oppdaterte CSCA-, opplastings- og TLS-sertifikater til DCCG-operatøren. Utløpte sertifikater skal fjernes fra hvitlisten og tillitslisten.

Medlemsstatene og DCCG-operatøren må følge med på gyldigheten av sine egne sertifikater. Det finnes ingen sentral enhet som registrerer sertifikatenes gyldighetstid eller opplyser deltakerne om den.

4.3. *Tilbakekalling av sertifikater*

Generelt kan digitale sertifikater tilbakekalles av de utstedende sertifiseringsmyndighetene ved hjelp av lister over tilbakekalte sertifikater eller en OCSP (Online Certificate Status Protocol Responder). CSCA-ene for DCC-systemet bør stille lister over tilbakekalte sertifikater (CRL-er) til rådighet. Selv om disse CRL-ene for tiden ikke brukes av andre medlemsstater, bør de integreres med sikte på framtidig bruk. Dersom en CSCA beslutter ikke å stille CRL-er til rådighet, må denne CSCA-ens DSC-er fornyes når CRL-ene blir obligatoriske. Kontrollørene bør ikke bruke OCSP for å validere DSC-er, og bør bruke CRL-er. Det anbefales at nasjonal «backend» foretar den nødvendige valideringen av DSC-er som lastes ned fra DCC-portalen, og bare videresender et sett av pålitelige og validerte DSC-er til nasjonale DCC-kontrollører. DCC-kontrollører bør ikke foreta tilbakekallingskontroll av DSC i valideringsprosessen. Dette skyldes blant annet behovet for å beskytte DCC-innehavernes data ved å unngå enhver risiko for at bruken av et bestemt DSC kan bli overvåket av dens tilknyttede OCSP-responderen.

Medlemsstatene kan selv fjerne sine DSC-er fra DCCG ved hjelp av gyldige opplastings- og TLS-sertifikater. Fjerning av et DSC innebærer at alle DCC-er som er utstedt med dette DSC-et, vil bli ugyldige når medlemsstatene henter de oppdaterte DSC-listene. Det er svært viktig å beskytte privat-nøkkel-materialet som motsvarer DSC-ene. Medlemsstatene må informere DCCG-operatøren når de må tilbakekalle opplastings- eller TLS-sertifikater, for eksempel fordi nasjonal «backend» kompromitteres. DCCG-operatøren kan deretter fjerne tillitsstatusen til det berørte sertifikatet, for eksempel ved å fjerne det fra TLS-hvitlisten. DCCG-operatøren kan fjerne opplastingssertifikatene fra DCCG-databasen. Pakker som er signert med den private nøkkelen som motsvarer dette opplastingssertifikatet, vil bli ugyldige når nasjonale «backends» fjerner tillitsstatusen til det tilbakekalte opplastingssertifikatet. Dersom et CSCA-sertifikat må tilbakekalles, skal medlemsstatene informere DCCG-operatøren og de andre medlemsstatene som de har et tillitsforhold til. DCCG-operatøren vil utstede en ny tillitsliste som ikke inneholder det berørte sertifikatet. Alle DSC-er som utstedes av denne CSCA-en, vil bli ugyldige når medlemsstatene oppdaterer tillitslageret for sine nasjonale «backends». Dersom $DCCG_{TLS}$-sertifikatet eller $DCCG_{TA}$-sertifikatet må tilbakekalles, skal DCCG-operatøren og medlemsstatene samarbeide for å opprette en ny pålitelig TLS-forbindelse og tillitsliste.

5. **Sertifikatmaler**

I dette avsnittet fastsettes kryptografiske krav og retningslinjer samt krav til sertifikatmaler. Sertifikatmalene for DCCG-sertifikatene fastsettes i dette avsnittet.

5.1. *Kryptografiske krav*

Krypteringsalgoritmer og TLS-krypteringsprogrammer skal velges på grunnlag av den gjeldende anbefalingen fra det tyske føderale kontoret for informasjonssikkerhet (BSI) eller SOG-IS. Disse anbefalingene ligner anbefalingene fra andre institusjoner og standardiseringsorganisasjoner. Anbefalingene finnes i de tekniske retningslinjene TR 02102-1 og TR 02102-2([1]) eller i SOG-IS Agreed Cryptographic Mechanisms([2]).

5.1.1. Krav til DSC

Kravene i *vedlegg I avsnitt 3.2.2* får anvendelse. Det anbefales derfor på det sterkeste at dokumentunderskriverne bruker den digitale signaturalgoritmen for elliptisk kurve (ECDSA) med NIST-p-256 (som definert i tillegg D til FIPS PUB 186-4). Andre elliptiske kurver støttes ikke. På grunn av plassbegrensninger i DCC bør medlemsstatene ikke bruke

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

RSA-PSS, selv om den er tillatt som reservealgoritme. Dersom medlemsstatene bruker RSA-PSS, bør de bruke en modulstørrelse på 2048 eller høyst 3072 bit. SHA-2 med en utdatalengde på ≥ 256 bit skal brukes som kryptografisk hash-funksjon (se ISO/IEC 10118-3:2004) for DSC-signaturen.

5.1.2. Krav til TLS-, opplastings- og CSCA-sertifikater

For digitale sertifikater og kryptografiske signaturer i DCCG-sammenheng er de viktigste kravene til krypteringsalgoritmer og nøkkellengde sammenfattet i tabellen nedenfor (per 2021):

Signaturalgoritme	Nøkkelstørrelse	Hash-funksjon
EC-DSA	Minst 250 bit	SHA-2 med en utdatalengde på ≥ 256 bit
RSA-PSS (anbefalt utfylling) RSA-PKCS#1 v1.5 (eksisterende utfylling)	RSA-modul (N) med minst 3000 bit og en offentlig eksponent e >2^16	SHA-2 med en utdatalengde på ≥ 256 bit
DSA	Primtall p med minst 3000 bit, nøkkel q med minst 250 bit	SHA-2 med en utdatalengde på ≥ 256 bit

Den anbefalte elliptiske kurven for EC-DSA er NIST-p-256 på grunn av dens utbredte anvendelse.

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

Tabellen nedenfor gir veiledning om NB_{CSCA}-sertifikatet i tilfeller der en medlemsstat beslutter å drive sin egen CSCA for DCC-systemet.

En angivelse i **fet** skrift er obligatorisk (må inngå i sertifikatet), mens en angivelse i *kursiv* er anbefalt (bør inngå). For tomme felter er det ikke fastsatt anbefalinger.

Felt	Verdi
Emne	**cn=<unikt emnenavn som ikke kan være tomt>,** *o=<Tilbyder>*, **c=<medlemsstat som driver CSCA>**
Nøkkelbruk	**sertifikatsignering,** *CRL-signering* (minst)
Hovedbegrensninger	**CA = true, path length constraints = 0**

Feltet for emnets navn kan ikke være tomt, og navnet skal være unikt innenfor den angitte medlemsstaten. Landkoden (c) må være landkoden for den medlemsstaten som skal bruke CSCA-sertifikatet. Sertifikatet skal inneholde en unik nøkkelidentifikator for emne (SKI) i samsvar med RFC 5280([3]).

5.3. *Dokumentsigneringssertifikat (DSC)*

I tabellen nedenfor gis veiledning om DSC-et. En angivelse i **fet** skrift er obligatorisk (må inngå i sertifikatet), mens en angivelse i *kursiv* er anbefalt (bør inngå). For tomme felter er det ikke fastsatt anbefalinger.

Felt	Verdi
Serienummer	**unikt serienummer**
Emne	**cn=<unikt emnenavn som ikke kan være tomt>,** *o=<Tilbyder>*, **c=<medlemsstat som bruker dette DSC-et>**
Nøkkelbruk	**digital signatur** (minst)

([3]) rfc5280 (ietf.org)

DSC-et må signeres med den private nøkkelen som motsvarer et CSCA-sertifikat som brukes av medlemsstaten.

Følgende utvidelser skal anvendes:

— Sertifikatet må inneholde en nøkkelidentifikator for instans (AKI) som svarer til nøkkelidentifikatoren for emne (SKI) for det utstedende CSCA-sertifikatet

— Sertifikatet bør inneholde en unik nøkkelidentifikator for emne (SKI) (i samsvar med RFC 5280([4])).

Sertifikatet bør i tillegg inneholde den CRL-distribusjonspunktutvidelsen som viser til den listen over tilbakekalte sertifikater (CRL) som stilles til rådighet av CSCA-en som utstedte DSC-et.

DSC-et kan inneholde en utvidet nøkkelbruksutvidelse med null eller flere identifikatorer for nøkkelretningslinjer som avgrenser hvilke HCERT-typer dette sertifikatet har rett til å kontrollere. Dersom det finnes en eller flere slike, skal kontrollørene kontrollere nøkkelbruken mot det lagrede HCERT-et. Følgende verdier for utvidet nøkkelbruk fastsettes for dette formålet:

Felt	Verdi
extendedKeyUsage	1.3.6.1.4.1.1847.2021.1.1 for utstedere i forbindelse med testing
extendedKeyUsage	1.3.6.1.4.1.1847.2021.1.2 for utstedere i forbindelse med vaksinasjon
extendedKeyUsage	1.3.6.1.4.1.1847.2021.1.3 for utstedere i forbindelse med restitusjon

Dersom det ikke foreligger noen nøkkelbruksutvidelse (dvs. ingen utvidelser eller utvidelser med verdien null), kan dette sertifikatet brukes for å validere alle typer HCERT. Andre dokumenter kan definere relevante ytterligere utvidelser for identifikatorer for nøkkelretningslinjer som brukes ved validering av HCERT-er.

5.4. *Opplastingssertifikater (NBUP)*

Tabellen nedenfor inneholder veiledning for opplastingssertifikatet for nasjonal «backend». En angivelse i **fet** skrift er obligatorisk (må inngå i sertifikatet), mens en angivelse i *kursiv* er anbefalt (bør inngå). For tomme felter er det ikke fastsatt anbefalinger.

Felt	Verdi
Emne	**cn=<unikt emnenavn som ikke kan være tomt>**, *o=<Tilbyder>*, **c=<medlemsstat som bruker dette opplastingssertifikatet>**
Nøkkelbruk	**digital signatur** (minst)

5.5. *TLS-klientautentisering for en nasjonal «backend» (NB_{TLS})*

Tabellen nedenfor gir veiledning om TLS-klientautentiseringssertifikatet for nasjonal «backend». En angivelse i **fet** skrift er obligatorisk (må inngå i sertifikatet), mens en angivelse i *kursiv* er anbefalt (bør inngå). For tomme felter er det ikke fastsatt anbefalinger.

Felt	Verdi
Emne	**cn=<unikt emnenavn som ikke kan være tomt>**, *o=<Tilbyder>*,**c=<NB-ens medlemsstat>**
Nøkkelbruk	**digital signatur** (minst)
Utvidet nøkkelbruk	**Klientautentisering (1.3.6.1.5.5.7.3.2)**

([4]) rfc5280 (ietf.org)

Sertifikatet kan også inneholde den utvidede nøkkelbruken *serverautentisering (1.3.6.1.5.5.7.3.1)*, men det er ikke påkrevd.

5.6. *Sertifikat for signatur på tillitslisten ($DCCG_{TA}$)*

I tabellen nedenfor defineres DCCGs tillitsankersertifikat.

Felt	Verdi
Emne	**cn = Portal for det grønne digitale sertifikatet**([5])**, o=<Tilbyder>, c=<land>**
Nøkkelbruk	**digital signatur** (minst)

5.7. *DCCGs TLS-serversertifikater ($DCCG_{TLS}$)*

I tabellen nedenfor defineres DCCGs TLS-sertifikat.

Felt	Verdi
Emne	**cn=<FQDN eller IP-adresse for DCCG>, o=<Tilbyder>, c=<land>**
SubjectAltName	**dNSName:<DCCG DNS-navn> eller IP-adresse:<DCCG IP-adresse>**
Nøkkelbruk	**digital signatur** (minst)
Utvidet nøkkelbruk	**serverautentisering (1.3.6.1.5.5.7.3.1**)

Sertifikatet kan også inneholde den utvidede nøkkelbruken *klientautentisering (1.3.6.1.5.5.7.3.2)*, men det er ikke påkrevd.

DCCGs TLS-sertifikat skal utstedes av en offentlig betrodd sertifiseringsmyndighet (inngår i alle større nettlesere og operativsystemer, i samsvar med CAB-forumets retningslinjer).

([5]) Begrepet «digitalt grønt sertifikat» er beholdt i stedet for «EUs digitale covid-sertifikat» i denne sammenhengen, ettersom det har blitt fast innkodet og brukt i sertifikatet før medregelgiverne besluttet å endre terminologien.