KOMMISSIONENS GENOMFÖRANDEBESLUT (EU) 2021/1073

av den 28 juni 2021

om fastställande av tekniska specifikationer och regler för genomförandet av och tillitsramverket för EU:s digitala covidintyg som infördes genom Europaparlamentets och rådets förordning (EU) 2021/953

(Text av betydelse för EES)

EUROPEISKA KOMMISSIONEN HAR ANTAGIT DETTA BESLUT

med beaktande av fördraget om Europeiska unionens funktionssätt,

med beaktande av Europaparlamentets och rådets förordning (EU) 2021/953 om en ram för utfärdande, kontroll och godtagande av interoperabla intyg om vaccination mot, testning för och tillfrisknande från covid-19 (EU:s digitala covidintyg) för att underlätta fri rörlighet under covid-19-pandemin ([1]), särskilt artikel 9.1 och 9.3, och

av följande skäl:

(1) I förordning (EU) 2021/953 fastställs EU:s digitala covidintyg, som har till syfte att styrka att en person har fått ett covid-19-vaccin, ett negativt testresultat eller återhämtat sig från infektion.

(2) För att EU:s digitala covidintyg ska kunna användas i hela unionen är det nödvändigt att fastställa tekniska specifikationer och regler för ifyllande och ett säkert utfärdande och säker kontroll av de digitala covidintygen och för att säkerställa skyddet av personuppgifter, fastställa den gemensamma strukturen för den unika identifieraren för intyg och utfärda en giltig, säker och interoperabel streckkod. Detta tillitsramverk omfattar också premisserna för strävan att säkerställa interoperabilitet med internationella standarder och tekniska system och skulle därmed kunna ge en modell för samarbete på global nivå.

(3) Förmågan att läsa och tolka EU:s digitala covidintyg förutsätter en gemensam datastruktur och enighet om den avsedda meningen för varje datafält i nyttolasten och om dess möjliga värden. För att främja sådan interoperabilitet är det nödvändigt att fastställa en gemensam samordnad datastruktur för ramen för EU:s digitala covidintyg. Riktlinjerna för denna ram har tagits fram av nätverket för e-hälsa som inrättades på grundval av Europaparlamentets och rådets direktiv 2011/24/EU ([2]). Dessa riktlinjer bör beaktas vid fastställandet av de tekniska specifikationerna för formatet och tillitshanteringen för EU:s digitala covidintyg. Datastrukturen och kodningsmekanismerna bör specificeras, liksom en transportkodningsmekanism i maskinläsbart optiskt format (QR), som kan visas på skärmen till en mobilenhet eller skrivas ut på papper.

(4) Vid sidan av de tekniska specifikationerna avseende format och tillitshantering för EU:s digitala covidintyg bör allmänna regler för utformningen av intyget fastställas så att de kan användas för kodade värden i innehållet i EU:s digitala covidintyg. De värdeset som genomför dessa regler bör regelbundet uppdateras och offentliggöras av kommissionen, baserat på relevant arbete i nätverket för e-hälsa.

(5) I enlighet med förordning (EU) 2021/953 bör äkta intyg som ingår i EU:s digitala covidintyg kunna identifieras individuellt med hjälp av en unik identifierare för intyg, där hänsyn även tas till att en innehavare kan få mer än ett intyg utfärdat under den tid som förordning (EU) 2021/953 är i kraft. Den unika identifieraren för intyg kommer att bestå av en alfanumerisk sträng, och medlemsstaterna bör se till att den inte innehåller några uppgifter som kopplar den till andra handlingar eller identifierare, såsom pass eller id-kortsnummer, för att förhindra direkt identifiering av innehavaren. För att säkerställa att identifieraren är unik bör tekniska specifikationer och regler fastställas för en gemensam struktur för denna.

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

([2]) Europaparlamentets och rådets direktiv 2011/24/EU av den 9 mars 2011 om tillämpningen av patienträttigheter vid gränsöverskridande hälso- och sjukvård (EUT L 88, 4.4.2011, s. 45).

(6) Säkerheten, äktheten, giltigheten och integriteten hos de intyg som utgör EU:s digitala covidintyg, och intygens överensstämmelse med unionsrätten på dataskyddsområdet är avgörande för att de ska kunna godtas i alla medlemsstater. Dessa mål uppnås genom ett tillitsramverk som omfattar regler och infrastruktur som gör att EU:s digitala covidintyg kan utfärdas och kontrolleras på ett tillförlitligt och säkert sätt. Tillitsramverket bör bland annat bygga på en infrastruktur för kryptering med öppen nyckel med en tillitskedja från medlemsstaternas hälsomyndigheter eller andra betrodda myndigheter till de enskilda enheter som utfärdar EU:s digitala covidintyg. För att säkerställa ett EU-täckande interoperabilitetssystem har kommissionen därför byggt upp ett centralt system – nätslussen för EU:s digitala covidintyg (nedan kallad *nätslussen*) – som förvarar de öppna nycklar som används för kontrollen. När QR-kodintyget skannas kontrolleras den digitala signaturen med hjälp av berörd öppen nyckel, som i förväg lagrats i den centrala nätslussen. Digitala signaturer kan användas för att säkerställa uppgifternas integritet och äkthet. Infrastrukturer med öppna nycklar upprättar tillit genom att koppla öppna nycklar till utfärdare av intyg. I nätslussen används flera certifikat för öppen nyckel för äktheten. För att säkerställa ett säkert datautbyte för öppet nyckelmaterial mellan medlemsstater och möjliggöra en bred interoperabilitet är det nödvändigt att fastställa vilka certifikat för öppen nyckel som får användas och föreskriva hur dessa bör genereras.

(7) Detta beslut gör det möjligt att göra kraven i förordning 2021/953 operativa på ett sätt som minimerar behandlingen av personuppgifter till vad som är nödvändigt för att göra EU:s digitala covidintyg operativt och bidrar till att de slutliga personuppgiftansvarigas implementerande är förenligt med inbyggt dataskydd.

(8) I enlighet med förordning (EU) 2021/953 ska myndigheter eller andra utsedda organ som ansvarar för att utfärda intygen anses vara personuppgiftsansvariga enligt artikel 4.7 i Europaparlamentets och rådets förordning (EU) 2016/679 ([3]) i sin uppgift att behandla personuppgifter inom ramen för utfärdandeförfarandet. Beroende på hur medlemsstaterna organiserar utfärdandeförfarandet kan det finnas en eller flera myndigheter eller ett eller flera utsedda organ, exempelvis regionala hälso- och sjukvårdstjänster. I enlighet med subsidiaritetsprincipen är det medlemsstaterna själva som får välja. Därmed är medlemsstaterna bäst lämpade att, i de fall då det finns flera myndigheter eller andra utsedda organ, säkerställa att deras respektive ansvarsområden är tydligt fördelade, oberoende av om de är separat eller gemensamt personuppgiftsansvariga (inbegripet regionala hälso- och sjukvårdstjänster som inrättar en gemensam patientportal för utfärdande av intygen). När det gäller den kontroll av intyg som görs av den behöriga myndigheten i destinations- eller transitmedlemsstaten, eller av de gränsöverskridande persontrafikföretag som enligt nationell rätt är ålagda att genomföra vissa folkhälsoåtgärder under covid-19-pandemin, måste dessa kontrollörer uppfylla sina skyldigheter enligt dataskyddsreglerna.

(9) Det görs ingen behandling av personuppgifter via nätslussen för EU:s digitala covidintyg, eftersom nätslussen endast innehåller de öppna nycklarna för signerande myndigheter. Dessa nycklar relaterar till de signerande myndigheterna och tillåter varken direkt eller indirekt återidentifiering av en fysisk person för vilken ett intyg utfärdats. I sin roll som förvaltare av nätslussen bör kommissionen alltså varken vara personuppgiftsansvarig eller personuppgiftsbiträde.

(10) Europeiska datatillsynsmannen har hörts i enlighet med artikel 42.1 i Europaparlamentets och rådets förordning (EU) 2018/1725 ([4]) och avgav ett yttrande den 22 juni 2021.

(11) Mot bakgrund av att tekniska specifikationer och regler är nödvändiga för tillämpningen av förordning (EU) 2021/953 från och med den 1 juli 2021 är det motiverat att detta beslut börjar tillämpas omedelbart.

(12) Mot bakgrund av behovet av ett snabbt införande av EU:s digitala covidintyg bör därför detta beslut träda i kraft samma dag som det offentliggörs.

([3]) Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning) (EUT L 119, 4.5.2016, s. 1).

([4]) Europaparlamentets och rådets förordning (EU) 2018/1725 av den 23 oktober 2018 om skydd för fysiska personer med avseende på behandling av personuppgifter som utförs av unionens institutioner, organ och byråer och om det fria flödet av sådana uppgifter samt om upphävande av förordning (EG) nr 45/2001 och beslut nr 1247/2002/EG (EUT L 295, 21.11.2018, s. 39).

HÄRIGENOM FÖRESKRIVS FÖLJANDE.

Artikel 1

De tekniska specifikationerna för EU:s digitala covidintyg, som fastställer den generiska datastrukturen, kodningsmekanismerna och transportkodningsmekanismen i maskinläsbart optiskt format fastställs i bilaga I.

Artikel 2

Reglerna för ifyllande av intygen enligt artikel 3.1 i förordning (EU) 2021/953 fastställs i bilaga II till detta beslut.

Artikel 3

Kraven för den gemensamma strukturen för den unika identifieraren för intygen fastställs i bilaga III.

Artikel 4

De styrningsregler som i samband med ska tillämpas på certifikat för öppen nyckel, i samband med nätslussen, vilka stöder tillitsramverkets interoperalitetsaspekter, fastställs i bilaga IV.

Detta beslut träder i kraft samma dag som det offentliggörs i *Europeiska unionens officiella tidning*.

Utfärdat i Bryssel den 28 juni 2021.

På kommissionens vägnar
Ursula VON DER LEYEN
Ordförande

BILAGA I

FORMAT OCH TILLITSFÖRVALTNING

Generisk datastruktur, kodningsmekanismer och transportkodningsmekanism i maskinläsbart optiskt format (nedan kallat QR)

1. Inledning

De tekniska specifikationer som fastställs i denna bilaga omfattar en generisk datastruktur och kodningsmekanism för EU:s digitala covidintyg (nedan kallat *intyget* eller *DCC*). De specificerar också en transportkodningsmekanism i maskinläsbart optiskt format (nedan kallad *QR*), som kan visas på skärmen till en mobilenhet eller skrivas ut på papper. Behållarformat för det elektroniska hälsointyget enligt dessa specfikationer är generiska, men används i detta sammanhang för att bära intyget.

2. Terminologi

I denna bilaga avser ”utfärdare” organisationer som använder dessa specifikationer för att utfärda hälsointyg och ”kontrollörer” avser organisationer som godtar hälsointyg som bevis på hälsostatus. ”Deltagare” avser utfärdare och kontrollörer. Vissa aspekter som fastställs i denna bilaga måste samordnas mellan deltagarna, såsom förvaltningen av en namnrymd och distributionen av krypteringsnycklar. Det antas att en part, som nedan kallas *sekretariatet*, utför dessa uppgifter.

3. HCERT (Electronic Health Certificate Container Format)

Behållarformatet för det elektroniska hälsointyget (Electronic Health Certificate Container Format, *HCERT*) är utformat för att ge en enhetlig och standardiserad form åt hälsointyg från olika utfärdare (nedan kallad *utfärdare*). Syftet med dessa specifikationer är att harmonisera hur dessa hälsointyg presenteras, kodas och signeras med målet att främja interoperabilitet.

Förmågan att läsa och tolka intyg som utfärdats av olika utfärdare förutsätter en gemensam datastruktur och enighet om betydelsen av varje datafält i nyttolasten. För att främja sådan interoperabilitet definieras en gemensam samordnad datastruktur genom användningen av ett ”JSON-schema” som utgör ramen för intyget.

3.1 *Nyttolastens struktur*

Nyttolasten struktureras och kodas som en CBOR med en digital COSE-signatur. Den brukar betecknas som ”CBOR Web Token” (nedan kallat *CWT*), och definieras i RFC 8392 ([1]). Nyttolasten, enligt definitionen i avsnitten nedan, transporteras i ett hcert (claim).

Integriteten och äktheten för nyttolastens ursprung måste kunna kontrolleras av kontrollören. För att tillhandahålla denna mekanism måste utfärdaren signera CWT med användning av ett asymmetriskt schema för elektroniska signaturer enligt definitionen i COSE-specifikationen (RFC 8152 ([2])).

3.2 *CWT-claim*

3.2.1 Överblick av CWT-strukturen

Skyddad headerk (Protected Header)

— Signaturalgoritm (Signature Algorithm) (alg, label 1)

— Nyckelidentifierare (Key Identifier) (kid, label 4)

Nyttolast (Payload)

— Utfärdare (Issuer) (iss, claim key 1, optional, ISO 3166-1 alpha-2 of issuer)

— Plats för utfärdandet (Issued At) (iat, claim key 6)

— Sista giltighetsdag (Expiration Time) (exp, claim key 4)

— Hälsointyg (Health Certificate) (hcert, claim key -260)

— EU:s digitala covidintyg, version 1 (EU Digital COVID Certificate v1) (eu_DCC_v1, claim key 1)

Signatur

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

3.2.2 Signaturalgoritm

Signaturalgoritmparametern (alg) anger vilken algoritm som använts för att skapa signaturen. Den måste minst uppfylla de nuvarande SOG-IS-riktlinjerna, som sammanfattas nedan.

En primär och en sekundär algoritm definieras. Den sekundära algoritmen bör endast användas om den primära algoritmen inte är godtagbar inom ramen för de regler och bestämmelser som gäller för utfärdaren.

För att säkerställa systemsäkerheten måste all implementering inbegripa den sekundära algoritmen. Därför måste både den primära och den sekundära algoritmen implementeras.

De fastställda SOG-IS-nivåerna för de primära och sekundära algoritmerna är:

— Primär algoritm: Den primära algoritmen är ECDSA (Elliptic Curve Digital Signature Algorithm) enligt definitionen i (ISO/IEC 14888-3:2006) avsnitt 2.3, med användning av de P-256-parametrar som definieras i tillägg D (D.1.2.3) i (FIPS PUB 186-4) i kombination med SHA-256-hashalgoritmen enligt definitionen i (ISO/IEC 10118-3:2004) funktion 4.

Detta motsvarar COSE-algoritmparameter ES256.

— Sekundär algoritm: Den sekundära algoritmen är RSASSA-PSS enligt definitionen i (RFC 8230 [3]) med en modul på 2048 bit i kombination med SHA-256-hashalgoritmen enligt definitionen i (ISO/IEC 10118-3:2004) funktion 4.

Detta motsvarar COSE-algoritmparameter PS256.

3.2.3 Key Identifier (nyckelidentifierare)

Claim nyckelidentifierare (kid) anger det certifikat för dokumentsignatär (Document Signer Certificate, DSC) som innehåller den öppna nyckel som ska användas av kontrollören för att kontrollera att den digitala signaturen är korrekt. Styrningen avseende certifikat för öppen nyckel, inklusive kraven för DSC, beskrivs i bilaga IV.

Kontrollörerna använder claim nyckelidentifieraren (kid) för att välja korrekt öppen nyckel från en lista med nycklar som hänför sig till den utfärdare som anges i kravet utfärdare (iss). Flera nycklar kan användas parallellt av en utfärdare, av administrativa skäl och vid nyckel-rollover. Nyckelidentifierare är inte ett säkerhetskritiskt fält. Därför får den också placeras i en oskyddad header om så krävs. Kontrollörer måste godta båda alternativen. Om båda alternativen förekommer måste nyckelidentifieraren i den skyddade headern användas.

I och med att identifieraren förkortats (för att begränsa storleken) finns det en marginell men inte obefintlig risk för att den övergripande DSC-förteckning som godtas av kontrollören kan innehålla DSC:er som har samma kid. Därför måste en kontrollör kontrollera alla DSC som har denna kid.

3.2.4 Utfärdare

Claim utfärdare (iss) är ett strängvärde som får (valfritt) innehålla ISO 3166-1 alpha-2-landskoden för den enhet som utfärdar hälsointyget. Denna claim kan användas av kontrollören för att identifiera vilket DSC-set som ska användas för kontrollen. Claim Key 1 används för att identifiera denna claim.

3.2.5 Sista giltighetsdag (Expiration Time)

Claim sista giltighetsdag (exp) ska omfatta en tidsstämpel i numeriskt datumformat med heltal (integer NumericDate format) (såsom anges i RFC 8392 [4], avsnitt 2) som anger hur länge just denna signatur avseende nyttolasten ska anses giltig, varefter en kontrollör måste avvisa nyttolasten såsom utgången. Syftet med parametern för sista giltighetsdag är att se till att hälsointygens giltighetstid begränsas. Claim Key 4 används för att identifiera denna claim.

Sista giltighetsdag får inte innebära att giltighetstiden för DSC överskrids.

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

3.2.6 Plats för utfärdandet (Issued At)

Claim Issued At (iat) ska omfatta en tidsstämpel i numeriskt datumformat i heltal (integer NumericDate format) (såsom anges i RFC 8392 ([5]), avsnitt 2) som anger den tidpunkt då hälsointyget skapades.

Fältet Issued At får inte föregå intygets giltighetsperiod.

Kontrollörerna får tillämpa ytterligare policyer för att begränsa giltigheten för hälsointyget baserat på tidpunkten för utfärdandet. Claim Key 6 används för att identifiera denna claim.

3.2.7 Claim hälsointyg (Health Certificate Claim)

Claim hälsointyg (hcert) är ett JSON-objekt (RFC 7159 ([6])) som innehåller informationen om hälsostatus. Flera olika typer av hälsointyg kan existera inom ramen för samma claim, där DCC är ett sådant.

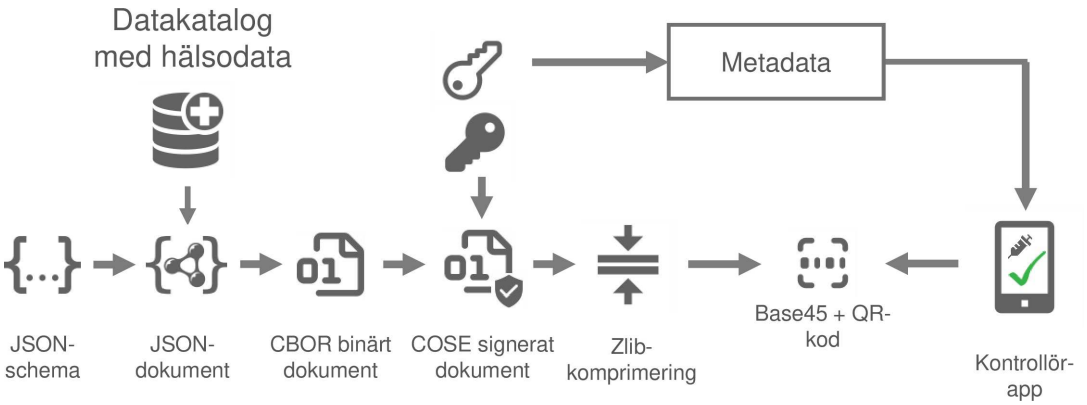
JSON är enbart för schemasyften. Representationsformatet är CBOR, enligt definitionen i (RFC 7049 ([7])). Applikationsutvecklare får i praktiken aldrig avkoda, eller koda till och från JSON-formatet utan ska använda in memory-strukturen.

Den Claim Key som ska användas för att identifiera detta krav är –260.

Strängar i JSON-objektet bör normaliseras i enlighet med NFC (Normalization Form Canonical Composition) som definieras i Unicode-standarden. Avkodningsapplikationer bör dock vara tillåtande och robusta när det gäller dessa aspekter, och det uppmuntras starkt att all rimlig typkonvertering ska godtas. Om icke-normaliserade data hittas vid avkodning, eller i efterföljande jämförelsefunktioner, bör implementeringen ske såsom när input är normaliserat till NFC.

4. Serialisering och skapande av DCC-nyttolast

Som serialiseringsmönster används följande system:



Processen inleds med extrahering av data, exempelvis från en datakatalog för hälsouppgifter (Health Data Repository) (eller en extern datakälla), och extraherade data struktureras i enlighet med definierade DCC-scheman. I denna process kan konverteringen till det fastställda dataformatet och omvandling för mänsklig läsbarhet ske innan serialiseringen till CBOR inleds. Akronymerna för en claim ska i varje enskilt fall sammanpassas med displaynamnen före serialisering och efter deserialisering.

Frivilligt nationellt datainnehåll är inte tillåtet i intyg som utfärdas i enlighet med förordning (EU) 2021/953 ([8]). Datainnehållet är begränsat till de definierade dataelementen i de minimidataset som anges i bilagan till förordning 2021/953.

([5]) rfc8392 (ietf.org).
([6]) rfc7159 (ietf.org).
([7]) rfc7049 (ietf.org).
([8]) Europaparlamentets och rådets förordning (EU) 2021/953 av den 14 juni 2021 om en ram för utfärdande, kontroll och godtagande av interoperabla intyg om vaccination mot, testning för och tillfrisknande från covid-19 (EU:s digitala covidintyg) för att underlätta fri rörlighet under covid-19-pandemin (EUT L 211, 15.6.2021, s. 1).

5. **Transportkodning (Transport Encodings)**

5.1 *Rå (Raw)*

För arbiträra datagränssnitt får HCERT-behållaren och dess nyttolaster överföras i befintlig form (as-is), med användning av valfri underliggande säker och tillförlitlig datatransport på 8 bitar. Dessa gränssnitt kan omfatta NFC (Near-Field Communication), bluetooth eller överföring via ett applikationsskiktsprotokoll, exempelvis överföring av en HCERT från utfärdaren till innehavarens mobilenhet.

Om överföringen av en HCERT från utfärdaren till innehavaren baseras på ett presentation-only-gränssnitt (exempelvis sms eller e-post) är det självklart inte tillämpligt med rå transportkodning.

5.2 *Streckkod*

5.2.1 Payload (CWT) Compression (komprimering av nyttolast)

För att minska storleken och öka hastigheten och tillförlitligheten i läsningsprocessen för HCERT, ska CWT komprimeras med användning av ZLIB (RFC 1950 ([9])) och komprimeringsmekanismen Deflate i det format som definieras i RFC 1951 ([10]).

5.2.2 QR 2D-streckkod

För att bättre hantera befintlig utrustning som utformats för användning av ASCII-nyttolast, kodas komprimerad CWT som ASCII med användning av Base45 innan den kodas in i en 2D-streckkod.

QR-formatet enligt definitionen i (ISO/IEC 18004:2015) ska användas för generering av 2D-streckkoden. En felkorrigeringsfrekvens på "Q" (omkring 25 %) rekommenderas. Eftersom Base45 används måste QR-koden använda alfanumerisk kodning (Mode 2, indikeras med symbolerna 0010).

För att kontrollörerna ska kunna upptäcka den typ av data som inkodats och välja korrekt avkodnings- och bearbetningssystem ska Base45-kodade data (enligt denna specifikation) förses med prefixet "HC1" som Context Identifier-sträng: Framtida versioner av denna specifikation, vilka påverkar kompatibiliteten bakåt, ska definiera en ny Context Identifier, medan det tecken som följer på "HC" ska tas från teckenuppsättningen [1–9A–Z]. Den inkrementella ordningen fastställs vara i denna ordning, alltså först [1–9] och sedan [A–Z].

Det rekommenderas att den optiska koden visas på presentationsmediet med en diagonal storlek på 35–60 mm med tanke på läsare med fast optik där presentationsmediet måste placeras på en yta framför läsaren.

Om den optiska koden trycks på papper med användning av en skrivare med låg upplösning (< 300 dpi), bör man bemöda sig om att varje symbol (prick) i QR-koden visas som en exakt kvadrat. En icke-proportionell skala kommer att resultera i att vissa rader eller kolumner i QR-koden har rektangulära symboler, vilket i många fall kommer att hämma läsbarheten.

6. **Format för tillitsförteckningar (CSCA- och DSC-förteckningar)**

Varje medlemsstat måste tillhandahålla en förteckning med en eller flera CSCA (Country Signing Certificate Authorities) och en förteckning med alla giltiga DSC (Document Signer Certificates), och hålla dessa förteckningar uppdaterade.

6.1 *Förenklat CSCA/DSC*

Från och med denna version av specifikationerna ska medlemsstaterna inte anta att någon CRL-information (Certificate Revocation List) används, eller att Private Key Usage Period (användningsperiod för privat nyckel) kontrolleras av implementerarna.

I stället utgörs den primära giltighetsmekanismen av det faktum att certifikatet finns med i den senaste versionen av denna certifikatförteckning.

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

6.2 *Icao eMRTD PKI och tillitscentrum (Trust Centers)*

Medlemsstaterna får använda en separat CSCA – men de får också inkomma med sina befintliga eMRTD CSCA-certifikat och/eller DSC:er, och de får till och med välja att upphandla dessa från (kommersiella) tillitscentrum – och inkomma med dessa. Varje DSC måste dock alltid signeras av den CSCA som den berörda medlemsstaten meddelat.

7. **Säkerhetsöverväganden**

Vid utformningen av ett system baserat på denna specifikation ska medlemsstaterna identifiera, analysera och övervaka vissa säkerhetsaspekter.

Som ett minimum bör följande aspekter beaktas:

7.1 *HCERT-signaturens giltighetstid*

Utfärdaren av HCERT ska begränsa signaturens giltighetsperiod genom att specificera en förfallotidpunkt för signaturen. Därmed måste innehavaren av ett hälsointyg förnya det med jämna mellanrum.

Den godtagbara giltighetsperioden kan avgöras av praktiska begränsningar. Det kan exempelvis hända att en resenär inte har möjlighet att förnya hälsointyget under en utlandsresa. Det kan också hända att utfärdaren undersöker en eventuell säkerhetskompromettering av något slag, som innebär att utfärdaren måste dra in ett DSC (vilket innebär att alla hälsointyg som utfärdats med den nyckeln blir ogiltiga även om gilitighetsperioden inte har löpt ut). Konsekvenserna av en sådan händelse kan begränsas genom att utfärdarnycklar regelbundet ändras och krav på att alla hälsointyg förnyas, med rimliga intervall.

7.2 *Nyckelförvaltning*

Denna specifikation bygger i hög grad på starka krypteringsmekanismer för att säkra dataintegriteten och autentisering av dataursprung. Det är därför nödvändigt att bevara konfidentialiteten för privata nycklar.

För krypteringsnycklar kan konfidentialiteten komprometteras på ett antal olika sätt, exempelvis följande:

— Processen för generering av nycklar kan vara bristfällig, vilket resulterar i svaga nycklar.

— Nycklarna kan vara exponerade till följd av mänskliga misstag.

— Nycklarna kan stjälas av externa eller interna gärningsmän.

— Nycklarna kan beräknas med hjälp av kryptoanalys.

För att begränsa riskerna för att signaturalgoritmen ska befinnas vara svag, så att de privata nycklarna kan komprometteras genom kryptoanalys, rekommenderas i denna specifikation att alla deltagare inför en sekundär reservsignaturalgoritm (secondary fallback signature algorithm) som baseras på andra parametrar eller ett annat matematiskt problem än den primära.

När det gäller de nämnda risker som rör utfärdarens driftsmiljö ska riskreducerande åtgärder vidtas för att säkerställa en effektiv kontroll – exempelvis att privata nycklar genereras, lagras och används i säkerhetsmoduler i maskinvara (Hardware Security Modules, HSM). Användning av HSM för signering av hälsointyg uppmuntras starkt.

Oavsett om en utfärdare beslutar att använda HSM eller inte bör ett system för nyckel-rollover fastställas där frekvensen för nyckel-rollover frekvens står i proportion till nycklarnas exponering för externa nät, andra system och personal. Ett välvalt system för nyckel-rollover begränsar också de risker som är förbundna med felaktigt utfärdade hälsointyg, eftersom det gör det möjligt för utfärdaren att återkalla sådana hälsointyg i omgångar (batch), genom att vid behov dra tillbaka en nyckel.

7.3 *Kontroll av indata*

Dessa specifikationer kan användas på ett sätt som innebär att data tas emot från ej tillförlitliga källor till system som kan vara av uppdragskritisk art. För att minimera riskerna förbundna med denna angreppsvektor måste alla indatafält valideras korrekt enligt datatyp, längd och innehåll. Utfärdarsignaturen bör också kontrolleras innan HCERT-innehållet behandlas. Valideringen av utfärdarsignaturen innebär dock att man först gör en parsning av Protected Issuer Header, där en potentiell angripare kan försöka injicera information som utformats omsorgsfullt för att kompromettera systemsäkerheten.

8. **Tillitsförvaltning**

För HCERT-signaturen krävs en öppen nyckel för kontroll. Medlemsstaterna ska göra dessa öppna nycklar tillgängliga. I slutändan måste varje kontrollör ha en förteckning över alla öppna nycklar som den är villig att lita på (eftersom den öppna nyckeln inte ingår i HCERT).

Systemet består av (endast) två skikt. För varje medlemsstat ska det på landsnivå finnas ett eller flera certifikat som vart och ett signerar ett eller flera DSC som används i den dagliga verksamheten.

Medlemsstatscertifikaten benämns CSCA-certifikat (Country Signing Certificate Authorities) och är (normalt) självsignerade certifikat. Medlemsstater får ha mer än ett sådant (exempelvis vid regional decentralisering). Dessa CSCA-certifikat signerar regelbundet DCS:er (Document Signing Certificates) som används för att signera HCERT:er.

”Sekretariatet” är en funktionell uppgift. Det ska regelbundet sammanställa och offentliggöra medlemsstaternas DSC:er efter att ha kontrollerat dessa mot förteckningen över CSCA-certifikat (som har överförts och verifierats på andra sätt).

Den förteckning över DSC-certifikat som upprättas på detta sätt ska sedan tillhandahålla den aggregerade uppsättningen godtagbara öppna nycklar (med motsvarande kid) som kontrollörerna kan använda för att validera signaturerna avseende HCERT. Kontrollörerna måste regelbundet hämta och uppdatera denna förteckning.

Formatet på sådana medlemsstatsspecifika förteckningar får anpassas till de egna nationella förhållandena. Därmed kan filformatet för denna tillitsförteckning variera. Den kan exempelvis vara en signerad JWKS (JWK set format per RFC 7517 ([11]), avsnitt 5) eller ett annat format som är specifikt för den teknik som används i den berörda medlemsstaten.

För enkelhetens skull får medlemsstaterna inkomma med både sina befintliga CSCA-certifikat från sina Icao eMRTD-system eller, såsom rekommenderas av WHO, skapa ett särskilt sådant för just detta hälsoområde.

8.1 *Nyckelidentifierare (Key Identifier, kid)*

Nyckelidentifieraren (kid) beräknas vid framtagandet av förteckningen över betrodda öppna nycklar från DSC:er och består av ett trunkerat (första 8 byte) SHA-256-fingeravtryck för DSC inkodat i DER-format (råformat).

Kontrollörerna behöver inte beräkna kid baserat på en DSC utan kan direkt matcha kid i utfärdade hälsointyg mot rätt kid i tillitsförteckningen.

8.2 *Skillnader jämfört med Icao eMRTD PKI-tillitsmodellen*

Bästa praxis från Icao eMRTD PKI-tillitsmodellen har använts som mönster, men ett antal förenklingar ska göras för att öka hastigheten:

— En medlemsstat får inkomma med flera CSCA-certifikat.

— DSC-giltighetstiden (nyckelanvändning, key usage) får fastställas till vilken period som helst men får inte innebära att CSCA-certifikatets giltighetstid överskrids och den får saknas.

— DSC får innehålla policyidentifierare (Extended Key Usage) som är specifika för hälsointyg.

— Medlemsstaterna kan välja att aldrig göra någon kontroll av offentliggjorda återkallanden, utan i stället helt förlita sig på de DSC-förteckningar som de dagligen får från sekretariatet eller själva sammanställer.

([11]) rfc7517 (ietf.org).

BILAGA II

REGLER FÖR IFYLLANDET AV EU:S DIGITALA COVIDINTYG

De allmänna reglerna för de värdeset som fastställs i denna bilaga syftar till att säkerställa interoperabilitet på en semantisk nivå och ska möjliggöra enhetlig teknisk implementering för DCC. Element som finns i denna bilaga får användas för tre olika situationer (vaccination/testning/tillfrisknande) i enlighet med förordning (EU) 2021/953. Endast de element där det är nödvändigt med en semantisk standardisering genom kodade värdeset förtecknas i denna bilaga.

Det är medlemsstaterna som ansvarar för översättning av kodade element till det nationella språket.

För alla datafält som inte nämns i nedanstående beskrivningar av värdeset rekommenderas kodning i UTF-8 (namn, testcentrum, utfärdare av intyget). För datafält som innehåller kalenderdatum (födelsedatum, vaccinationsdatum, datum för provtagning, datum för första positiva testresultat, giltighetsdatum för intyg) rekommenderas kodning enligt ISO 8601.

Om de nedan angivna förespråkade kodningssystemen av någon anledning inte kan användas får andra internationella kodningssystem användas, och det bör finnas råd för hur koderna från det andra kodningssystemet ska sammanpassas med det förespråkade kodningssystemet. Text (display names) får användas i exceptionella fall som reservmekanism när ingen lämplig kod finns tillgänglig inom fastställda värdeset.

Medlemsstater som använder annan kodning i sina system bör sammanpassa sådana koder med de värdeset som beskrivs. Medlemsstaterna har ansvaret för sådan sammanpassning.

Dessa värdeset ska regelbundet uppdateras av kommissionen med stöd av nätverket för e-hälsa och hälsosäkerhetskommittén. Uppdaterade värdeset ska offentliggöras på kommissionens relevanta webbplats samt på webbsidan för nätverket för e-hälsa. En historik över ändringar ska tillhandahållas.

1. **Sjukdom eller smittämne / Sjukdom eller smittämne som innehavaren har tillfrisknat från: Covid-19 (SARS-CoV-2 eller en av dess varianter)**

   Förespråkat kodningssystem: SNOMED CT.

   Ska användas i intyg 1, 2 och 3.

   De valda koderna ska avse covid-19 eller, om det behövs mer detaljerad information om den genetiska varianten av SARS-CoV-2, dessa varianter om sådan detaljerad information behövs av epidemiologiska skäl.

   Ett exempel på en kod som bör användas är SNOMED CT-koden 840539006 (covid-19).

2. **Covid-19-vaccin eller covid-19-profylax**

   Förespråkat kodningssystem: SNOMED CT eller ATC-klassificering

   Ska användas i intyg 1.

   Exempel på koder som bör användas från de förespråkade kodningssystemen är SNOMED CT-kod 1119305005 (SARS-CoV-2 antigenvaccin), 1119349007 (SARS-CoV-2 mRNA-vaccin) eller J07BX03 (covid-19-vaccin). Detta värdeset bör utvidgas när nya vaccintyper utvecklas och börjar användas.

3. **Covid-19-vaccinläkemedel**

   Förespråkade kodningssystem (i prioriteringsordning):

   — Unionens register över vaccinläkemedel med EU-godkännande (godkännandenummer).

   — Ett globalt vaccinregister av det slag som skulle kunna upprättas av Världshälsoorganisationen.

   — Namnet på vaccinläkemedlet i andra fall. Om namnet innehåller icke-svärtande tecken bör dessa ersättas med bindestreck (-).

Namn på berört värdeset: Vaccin.

Ska användas i intyg 1.

Ett exempel på en kod som bör användas från det förespråkade kodningssystemet är EU/1/20/1528 (Comirnaty). Ett exempel på ett namn på vaccin som används som kod: Sputnik-V (står för Sputnik V).

4. **Innehavare av godkännande för försäljning av covid-19-vaccin eller covid-19-vaccintillverkare**

Förespråkat kodningssystem:

— Organisationskod från EMA (SPOR-system för ISO IDMP).

— Ett globalt register över innehavare av ett godkännande för försäljning eller vaccintillverkare, av det slag som skulle kunna upprättas av Världshälsoorganisationen.

— Organisationens namn i andra fall. Om namnet innehåller icke-svärtande tecken bör dessa ersättas med bindestreck (-).

Ska användas i intyg 1.

Exempel på en kod som bör användas från det förespråkade kodningssystemet är ORG-100001699 (AstraZeneca AB). Ett exempel på ett organisationsnamn som används som kod: Sinovac-Biotech (står för Sinovac Biotech).

5. **Nummer i en serie doser och det totala antalet doser i serien**

Ska användas i intyg 1.

Två fält:

1) Numret för den dos som administreras i en cykel.

2) Antal förväntade doser i en komplett cykel (specifikt för en person vid tidpunkten för administrerandet).

Exempelvis kommer 1/1, 2/2 att anges som komplett, inbegripet alternativet 1/1 för vaccin som omfattar två doser men där det protokoll som tillämpas av medlemsstaten innebär att endast en dos ges till medborgare som diagnostiserats med covid-19 före vaccinationen. Det totala antalet doser i serien bör anges enligt den information som finns tillgänglig vid den tidpunkt då dosen administreras. Om exempelvis ett visst vaccin förutsätter en tredje dos (påfyllnadsdos) vid tidpunkten för den sista administrerade dosen, bör det andra numret i fältet reflektera detta (t.ex. 2/3, 3/3 etc).

6. **Medlemsstat eller tredjeland där vaccinet administrerades / testningen utfördes**

Förespråkat kodningssystem: ISO 3166 landskoder.

Ska användas i intyg 1, 2 och 3.

Innehåll i detta värdeset: den kompletta förteckningen över tvåbokstavskoder, som finns tillgänglig som ett värdeset definierat i FHIR (http://hl7.org/fhir/ValueSet/iso3166-1-2).

7. **Typ av test**

Förespråkat kodningssystem: LOINC.

Ska användas i intyg 2, och i intyg 3 om en delegerad akt innebär att utfärdandet av intyg på tillfrisknande baserat på andra typer av tester än NAAT stöds.

Koderna i detta värdeset ska avse testmetoden och ska väljas för att åtminstone skilja mellan NAAT-tester och RAT-tester, såsom anges i förordning (EU) 2021/953.

Ett exempel på en kod som bör användas från det förespråkade kodningssystemet är LP217198-3 (Rapid immunoassay).

8. **Tillverkare och handelsbeteckning för det test som används (frivilligt för NAAT-test)**

Förespråkat kodningssystem: Förteckningen från HSC för antigentest i form av snabbtest (Rapid Antigen Tests) som upprätthålls av JRC (databas över testmetoder och produkter för in vitro-diagnostik av covid-19, COVID-19 In Vitro Diagnostic Devices and Test Methods Database).

Ska användas i intyg 2.

Innehållet i detta värdeset ska innefatta det urval av antigentester i form av snabbtest som finns förtecknade i den gemensamma och uppdaterade förteckningen över antigentest för covid-19 i form av snabbtest, inrättad på grundval av rådets rekommendation 2021/C 24/01 och godkänd av hälsosäkerhetskommittén. Förteckningen upprätthålls av JRC i databasen över testmetoder och produkter för in vitro-diagnostik av covid-19 på: https://covid-19-diagnostics.jrc.ec.europa.eu/devices/hsc-common-recognition-rat.

För detta kodsystem ska de relevanta fälten, såsom testutrustningens identifierare, testets namn och tillverkare, användas, i enlighet med JRC:s strukturerade format som finns tillgängligt på https://covid-19-diagnostics.jrc.ec.europa.eu/devices.

9. **Testresultat**

Förespråkat kodningssystem: SNOMED CT.

Ska användas i intyg 2.

De valda koderna ska göra det möjligt att skilja mellan positiva och negativa testresultat (påvisade eller ej påvisade). Ytterligare värden (såsom ej fastställt) får läggas till om det behövs för användarfallen.

Exempel på koder som bör användas från det förespråkade kodningssystemet är 260415000 (Ej påvisat) och 260373001 (Påvisat).

BILAGA III

GEMENSAM STRUKTUR FÖR INTYGETS UNIKA IDENTIFIERARE

1. Inledning

Alla EU:s digitala covidintyg (DCC) ska vara försedda med en unik identifierare för intyget (unique certificate identifier, UCI) som stöder intygens interoperabilitet. Identifieraren kan användas för att kontrollera intyget. Det är medlemsstaterna som ansvarar för implementeringen av denna identifierare. Identifieraren är ett sätt att kontrollera intygets sanningsenlighet och, om tillämpligt, att länka till ett registreringssystem (exempelvis ett IIS). Dessa identifierare ska också möjliggöra försäkringar (på papper eller digitalt) från medlemsstaterna om att individer har vaccinerats eller testats.

2. Uppbyggnaden av den unika identifieraren för intyg

Den unika identifieraren ska ha en gemensam struktur och ett gemensamt format som underlättar mänsklig och/eller maskinell tolkningsbarhet för informationen och får omfatta sådana element som vaccinationsmedlemsstaten, själva vaccinet och en specifik medlemsstatsspecifik identifierare. Den säkerställer flexibilitet för medlemsstaterna vad gäller formatering, i full enlighet med dataskyddslagstiftningen. De separata elementens ordning följer en fastställd hierarki som kan möjliggöra framtida ändringar av blocken samtidigt som den strukturella integriteten upprätthålls.

De möjliga lösningarna för den unika identifierarens uppbyggnad bildar ett spektrum där modularitet och möjlighet till mänsklig tolkning är de två viktigaste diversifierande parametrarna och en grundläggande egenskap:

— Modularitet: den grad till vilken koden består av distinkta byggstenar som innehåller semantiskt olika uppgifter.

— Möjlighet till mänsklig tolkning: den grad till vilken koden är meningsfull och kan tolkas av en mänsklig läsare.

— Globalt unik; lands- eller myndighetsidentifieraren är välförvaltad, och varje land (myndighet) förväntas förvalta sitt segment av namnrymden väl genom att aldrig återvinna eller återutfärda identifierare. Denna kombination säkerställer att varje identifierare är globalt unik.

3. Allmänna krav

Följande övergripande krav bör uppfyllas i förhållande till UCI:

1) Charset: endast US-ASCII-alfanumeriska tecken (”A”–”Z”, ”0”–”9”) i versaler tillåts, med ytterligare specialtecken för separering från RFC3986 ([1]) ([2]), nämligen {’/’,’#’,’:’};

2) Maximal längd: utformarna bör sikta på en längd av 27–30 tecken ([3]).

3) Versionprefix: detta avser versionen av UCI-systemet. Versionprefixet är ”01” för denna version av dokumentet, och versionprefixet består av två siffror.

4) Landsprefix: landskoden specificeras i ISO 3166-1. Längre koder (dvs. med 3 eller flera tecken (exempelvis ”UNHCR”) reserveras för framtida användning.

5) Kodsuffix / checksumma

   5.1 Medlemsstaterna bör använda en checksumma när det är troligt att överföring, (mänsklig) transkribering eller annan korruption kan inträffa (alltså vid användning av utskriven version).

   5.2 Man ska inte förlita sig på checksumman för validering av intyget och den ingår tekniskt sett inte i identifieraren utan används för att kontrollera kodens integritet. Denna checksumma bör vara ISO-7812-1 (LUHN-10)-sammanfattningen ([4]) av hela UCI i digitalt format/trådtransportformat (wire transport format). Checksumman separeras från resten av UCI med ett ”#”-tecken.

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

([2]) Det är möjligt att sådana fält som kön, partinummer, vaccinationscentrum, identifierare för vårdpersonal eller nästa vaccinationsdatum inte behövs för andra syften än medicinsk användning.

([3]) För implementering med QR-koder kan medlemsstaterna överväga en extra uppsättning tecken upp till en total längd av 72 tecken (inbegripet de 27–30 tecknen för själva identifieraren) som kan användas för annan information. Det är medlemsstaterna själva som fastställer vad den informationen ska innehålla.

([4]) Luhn mod N-algoritmen är ett tillägg till Luhn-algoritmen (även kallad mod 10-algoritmen) som fungerar för numeriska koder och används för exempelvis beräkning av checksumman för kreditkort. Tillägget innebär att algoritmen kan arbeta med sekvenser av värden i vilken bas som helst (i vårt fall alfatecken).

Kompatibiliteten bakåt bör säkerställas: medlemsstater som över tid ändrar strukturen på sina identifierare (inom ramen för huvudversionen, som för närvarande är v1) måste säkerställa att två identifierare som är identiska med varandra representerar samma vaccinationsintyg/vaccinationsförsäkran. Eller med andra ord, medlemsstaterna får inte återvinna identifierare.

4. **Alternativ för unika certifikatidentifierare för vaccinationsintyg**

Riktlinjerna från nätverket för e-hälsa avseende kontrollerbara vaccinationsintyg och grundläggande interoperabilitetselement ([5]) omfattar olika alternativ som är tillgängliga för medlemsstaterna och andra parter som kan samexistera mellan olika medlemsstater. Medlemsstaterna får använda sådana olika alternativ i en annan version av UCI-systemet.

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

BILAGA IV

STYRNING AV CERTIFIERINGEN AV ÖPPNA NYCKLAR (PUBLIC KEY CERTIFICATE GOVERNANCE)

1. Inledning

Ett säkert och tillitsbaserat utbyte av signaturnycklar för EU:s digitala covidintyg (DCC) mellan medlemsstater görs av DCGG (nätslussen för EU:s digitala covidintyg) som fungerar som central datakatalog för öppna nycklar. Med DCCG har medlemsstaterna befogenhet att offentliggöra de öppna nycklar som motsvarar de privata nycklar som de använder för att signera digitala covidcertifikat. Deltagande medlemsstater kan använda DCCG för att snabbt hämta uppdaterat material om öppna nycklar. Senare kan DCCG utvidgas till att omfatta ett utbyte av kompletterande tillförlitlig information som tillhandahålls av medlemsstaterna, såsom valideringsregler för DCC. Tillitsmodellen för DCC-ramen är en PKI (infrastruktur med öppna nycklar). Varje medlemsstat har en eller flera CSCA (Country Signing Certificate Authority), vars certifikat har relativt lång giltighet. Till följd av medlemsstatens beslut kan CSCA vara samma CSCA som används för maskinläsbara resehandlingar eller en annan CSCA. CSCA utfärdar certifikat för öppna nycklar åt de nationella, kortlivade, dokumentsignatärerna (Document Signers) (som alltså signerar DCC); dessa certifikat benämns DSC (Document Signer Certificates). CSCA fungerar som ett tillitsankare (trust anchor) så att deltagande medlemsstater kan använda CSCA-certifikatet för att validera de regelbundet ändrade DSC:ernas äkthet och integritet. Efter valideringen kan medlemsstaterna tillhandahålla dessa certifikat (eller bara de öppna nycklar som de innehåller) åt sina DCC-valideringstillämpningar. Vid sidan av CSCA och DSC förlitar sig DCCG också på PKI för att autentisera transaktioner, signera data, som grundval för autentisering och som ett sätt att säkerställa integriteten för kommunikationskanalerna mellan medlemsstaterna och DCCG.

Digitala signaturer kan användas för att uppnå dataintegritet och uppgifternas äkthet. PKI upprättar tillit genom att koppla öppna nycklar till utfärdare av intyg. Detta är nödvändigt för att andra deltagare ska kunna kontrollera uppgifternas ursprung och kommunikationspartnerns identitet och besluta om tillit. I DCCG används flera olika certifikat för öppen nyckel för äkthet. I denna bilaga fastställs vilka certifikat för öppen nyckel som används och hur dessa ska utformas för att möjliggöra en bred interoperabilitet mellan medlemsstaterna. Där tillhandahålls fler detaljer om de nödvändiga certifikaten för öppna nycklar och ges vägledning om certifikatmallar och giltighetsperioder för medlemsstater som vill driva egna CSCA. Eftersom DCC:er ska vara möjliga att kontrollera under en fastställd tidsperiod (som inleds vid utfärdandet och löper ut efter viss tid) är det nödvändigt att fastställa en kontrollmodell för alla signaturer som används för certifikat för öppen nyckel och DCC.

2. Terminologi

Följande tabell innehåller förkortningar och terminologi som används i denna bilaga.

Term	Definition
Certifikat	Eller certifikat för öppen nyckel. Ett X.509 v3-certifikat som innehåller den öppna nyckeln för en enhet.
CSCA	Country Signing Certificate Authority
DCC	EU:s digitala covidintyg (EU Digital COVID Certificate). Ett signerat digitalt dokument som innehåller uppgifter om vaccination, testning eller tillfrisknande.
DCCG	EU:s digitala nätsluss för covidintyg (EU Digital COVID Certificate Gateway). Detta system används för utbyte av DSC mellan medlemsstater.
$DCCG_{TA}$	Tillitsankarcertifikat (Trust Anchor certificate) för DCCG. Motsvarande privata nyckel används för att signera förteckningen över alla CSCA-certifikat offline.
$DCCG_{TLS}$	TLS-servercertifikat (TLS server certificate) för DCCG.
DSC	DSC (Document Signer Certificate). Certifikat för öppen nyckel för en medlemsstats myndighet för signering av dokument (document signing authority) (exempelvis ett system som har rätt att signera DCC). Detta certifikat utfärdas av medlemsstatens CSCA.
EC-DSA	Elliptic Curve Digital Signature Algorithm. En krypteringsalgoritm för signaturer som baseras på elliptiska kurvor.
Medlemsstat	Medlemsstat i Europeiska unionen.

Term	Definition
mTLS	Ömsesidig TLS (Mutual TLS). Transport Layer Security Protocol med ömsesidig autentisering.
Anm.:	En medlemsstats nationella backend-system.
NB_{CSCA}	CSCA-certifikat för en medlemsstat (kan finnas mer än ett).
NB_{TLS}	TLS-klientautentiseringscertifikat (TLS client authentication certificate) för ett nationellt backend-system.
NB_{UP}	Det certifikat som ett nationellt backend-system använder för att signera datapaket som laddas upp till DCCG.
PKI	Public Key Infrastructure (infrastruktur för kryptering med öppen nyckel). Tillitsmodell baserad på certifikat för öppen nyckel och certifikatmyndigheter.
RSA	Asymmetrisk krypteringsalgoritm baserad på heltalsfaktorisering som används för digitala signaturer eller asymmetrisk kryptering.

3. **Kommunikationsflöden och säkerhetstjänster för DCCG**

Detta avsnitt innehåller en översikt över kommunikationsflödena och säkerhetstjänsterna i DCCG-systemet. Där fastställs också vilka nycklar och certifikat som används för att skydda kommunikationen, den uppladdade informationen, DCC:erna och en signerad tillitsförteckning som omfattar alla CSCA-certifikat som ingår. DCGG fungerar som en datahubb som möjliggör ett utbyte av signerade datapaket för medlemsstaterna.

Uppladdade datapaket tillhandahålls av DCCG ”i befintligt skick” (as is), vilket innebär att DCCG inte lägger till eller tar bort några DSC från paket som de tar emot. Medlemsstaternas nationella backend-system (NB) ska kunna kontrollera att integriteten och äktheten för uppladdade data är obruten. Vid sidan av detta kommer nationella backend-system och DCCG att använda ömsesidig TLS-autentisiering för att upprätta en säker anslutning. Detta är ett komplement till signaturerna i de data som utbyts.

3.1 *Autentisering och upprättande av anslutning*

DCCG använder TLS (Transport Layer Security) med ömsesidig autentisering för att upprätta en autentiserad krypterad kanal mellan medlemsstaternas nationella backend-system (NB) och nätslussmiljön. Därför har DCCG ett TLS-servercertifikat, förkortat till $DCCG_{TLS}$, och nationella backend-system har ett TLS-klientcertifikat – förkortat NB_{TLS}. Certifikatmallar tillhandahålls i *avsnitt 5*. Varje nationellt backend-system kan tillhandahålla sitt eget TLS-certifikat. Detta certifikat kommer uttryckligen att vitlistas och får därmed utfärdas av en offentligt betrodd certifikatmyndighet (t.ex. en certifikatmyndighet som följer baslinjekraven från CA Browser Forum), av en nationell certifikatmyndighet eller kan vara självsignerat. Varje medlemsstat ansvarar för sina nationella data och skyddet av den privata nyckel som används för att upprätta anslutningen till DCCG. Tillvägagångssättet baserat på att man ”tar med sitt eget certifikat” förutsätter en väldefinierad registrerings- och identifieringsprocess samt förfaranden för återkallande och förnyande enligt beskrivningen i *avsnitt 4.1*, *4.2* och *4.3*. DCCG använder en vitlistning där TLS-certifikaten för nationella backends läggs till när registreringen har genomförts. Endast nationella backends som autentiserar sig själva med en privat nyckel som motsvarar ett certifikat från vitlistan kan upprätta en säker anslutning till DCCG. DCCG kommer också att använda ett TLS-certifikat som gör det möjligt för nationella backends att verifiera att de faktiskt upprättar en anslutning till den ”riktiga” DCCG:n och inte till någon illvillig enhet som utger sig för att vara DCCG. Certifikatet för DCCG kommer att tillhandahållas åt nationella backend-system när registreringen genomförts. $DCCG_{TLS}$-certifikatet kommer att utfärdas från en offentligt betrodd CA (ingår i alla vanliga webbläsare). Det är medlemsstaternas ansvar att kontrollera att deras anslutning till DCCG är säker (exempelvis genom att kontrollera fingeravtrycket för $DCCG_{TLS}$-certifikatet för den anslutna servern mot det som tillhandahölls efter registreringen).

3.2 *CSCA och valideringsmodell*

Medlemsstater som deltar i DCCG-ramen måste använda en CSCA för att utfärda DSC:er. Medlemsstater får ha mer än en CSCA (exempelvis vid regional decentralisering). Varje medlemsstat kan antingen använda befintliga certifikatmyndigheter eller inrätta en särskild (eventuellt självsignerad) certifikatmyndighet för DCC-systemet.

Medlemsstaterna måste lägga fram sina CSCA-certifikat (ett eller flera) för DCCG-operatören under det officiella förfarandet för onboarding. Efter genomförd registrering av medlemsstaten (*se avsnitt 4.1 för ytterligare detaljer*), kommer DCCG-operatören att uppdatera en signerad tillitsförteckning som omfattar alla CSCA-certifikat som är aktiva i DCC-ramen. DCCG-operatören kommer att använda ett särskilt asymmetriskt nyckelpar för att signera tillitsförteckningen och certifikaten i en offlinemiljö. Den privata nyckeln kommer inte att lagras i online-DCCG-systemet, så att inte tillitsförteckningen komprometteras av en angripare om onlinesystemet komprometteras. Motsvarande $DCCG_{TA}$-tillitsankarcertifikat kommer att tillhandahållas åt nationella backend-system under förfarandet för onboarding.

Medlemsstaterna kan erhålla tillitsförteckningen från DCGG för sina kontrollförfaranden. CSCA definieras som den certifikatmyndighet som utfärdar DSC, och därför måste medlemsstater som använder CA-hierarki med flera nivåer (multi-tier) (t.ex. Root CA -> CSCA -> DSC) tillhandahålla den underordnade certifikatmyndighet som utfärdar DSC. I sådana fall gäller att om en medlemsstat använder en befintlig certifikatmyndighet så kommer DSS-systemet att ignorera allt som är över CSCA och endast vitlista CSCA:n som tillitsankare (även om den är en underordnad CA). Detta beror på att Icao-modellen endast tillåter exakt 2 nivåer - en ”root”-CSCA och en ”leaf”-DSC som signerats av just denna CSCA.

Om en medlemsstat driver sin egen CSCA är medlemsstaten ansvarig för en säker drift och nyckelförvaltning för denna CA. CSCA fungerar som tillitsankare för DSC:er och därför är det mycket viktigt för DCC-miljöns integritet att den privata nyckeln för CSCA skyddas. Kontrollmodellen i DCC PKI är skalmodellen, som anger att alla certifikat i certifikatkedjevalideringen (certificate path validation) måste vara giltiga en given tidpunkt (dvs. vid tidpunkten för valideringen av signaturen). Därför gäller följande begränsningar:

— CSCA får inte utfärda certifikat som har längre giltighet än själva CA-certifikatet.

— Dokumentsignatären får inte som har längre giltighet än själva DSC.

— Medlemsstater som driver sin egen CSCA måste fastställa giltighetsperioderna för sina CSCA och alla utfärdade certifikat, och de måste ta hand om förnyanden av certifikat.

Avsnitt 4.2 omfattar rekommendationer om giltighetsperioder.

3.3 *Integritet och äkthet för uppladdade data*

Nationella backend-system kan använda DCCG för uppladdning och nerladdning av digitalt signerade datapaket efter framgångsrik ömsesidig autentisering. Först innehåller dessa datapaket medlemsstaternas DSC. Det nyckelpar som används av ett nationellt backend-system för den digitala signaturen för datapaket som laddats upp i DCCG-systemet betecknas ”national backend upload signature key pair” och motsvarande certifikat för öppen nyckel förkortas till NB_{UP}-certifikat. Varje medlemsstat tar med sitt eget NB_{UP}-certifikat, som kan vara självsignerat, eller utfärdat av en befintlig certifikatmyndighet, såsom en offentlig certifikatmyndighet (t.ex. en certifikatmyndighet som utfärdar certifikat i enlighet med CAB-Forums baslinjekrav. NB_{UP}-certifikatet ska skilja sig från andra certifikat som används av medlemsstaten (t.ex. CSCA, TLS client eller DSC).

Medlemsstaterna måste förse DCCG-operatören med uppladdningscertifikatet under det ursprungliga registreringsförfarandet (*se avsnitt 4.1 för mer detaljer*). Varje medlemsstat ansvarar för sina nationella data och måste skydda den privata nyckel som används för att signera uppladdningarna.

Andra medlemsstater kan verifiera de signerade datapaketen med hjälp av de uppladdningscertifikat som tillhandahålls av DCCG. DCCG kontrollerar äktheten och integriteten för uppladdade data med NB-uppladdningscertifikat innan dessa tillhandahålls åt andra medlemsstater.

3.4 *Krav på den tekniska DCCG-arkitekturen*

För den tekniska DCCG-arkitekturen gäller följande krav:

— DCCG använder ömsesidig TLS-autentisering för att upprätta en autentiserad krypterad anslutning till NBs. Därför upprätthåller DCCG en vitlista över registrerade NB_{TLS}-klientcertifikat.

— DCCG använder två digitala certifikat ($DCCG_{TLS}$ och $DCCG_{TA}$) med två distinkta nyckelpar. Den privata nyckeln för $DCCG_{TA}$-nyckelparet upprätthålls offline (inte på onlinekomponenterna för DCCG).

— DCCG upprätthåller en tillitsförteckning över NB_{CSCA}-certifikat som signerats med den privata nyckeln för $DCCG_{TA}$.

— De chiffer som används måste uppfylla kraven i *avsnitt 5.1*.

4. Livscykelförvaltning av certifikat (Certificate Lifecycle Management)

4.1 *Registrering av nationella backend-system*

Medlemsstaterna måste registrera sig hos DCCG-operatören för att delta i DCCG-systemet. I detta avsnitt beskrivs det tekniska och operativa förfarande som måste följas för registrering av ett nationellt backend-system.

DCCG-operatören och medlemsstaten måste utbyta information om tekniska kontaktpersoner för förfarandet för onboarding. Det förutsätts att de tekniska kontaktpersonerna har legitimerats av sina medlemsstater och att identifieringen/autentiseringen utförs via andra kanaler. Exempelvis kan autentisering uppnås när en medlemsstats tekniska kontakt tillhandahåller certifikaten som lösenordskrypterade filer via e-post och meddelar DCCG-operatören motsvarande lösenord per telefon. Även andra säkra kanaler som fastställs av DCCG-operatören får användas.

Medlemsstaterna måste tillhandahålla tre digitala certifikat under registrerings- och identifieringsprocessen:

— Medlemsstatens TLS-certifikat NB_{TLS}.

— Medlemsstatens uppladdningscertifikat NB_{UP}.

— Medlemsstatens CSCA-certifikat (ett eller flera) NB_{CSCA}.

Alla certifikat som tillhandahålls måste uppfylla de krav som fastställs i *avsnitt 5*. DCCG-operatören kommer att kontrollera att det certifikat som tillhandahålls uppfyller kraven i *avsnitt 5*. Efter identifiering och registrering ska DCCG-operatören göra följande:

— Lägga till NB_{CSCA}-certifikatet (ett eller flera) i tillitsförteckningen signerat med den privata nyckel som motsvarar den öppna nyckeln för $DCCG_{TA}$.

— Lägga till NB_{TLS}-certifikatet i vitlistan för DCCG TLS-ändpunkten.

— Lägga till NB_{UP}-certifikatet i DCCG-systemet.

— Tillhandahålla certifikatet för öppen nyckel för $DCCG_{TA}$ och $DCCG_{TLS}$ åt medlemsstaten.

4.2 *Certifikatmyndigheter, giltighetstider och förnyande*

Om en medlemsstat vill driva sin egen CSCA får CSCA-certifikaten vara självsignerade certifikat. De fungerar som tillitsankare för medlemsstaten och därför måste medlemsstaten ha ett starkt skydd för den privata nyckel som motsvarar den öppna nyckeln för CSCA-certifikatet. Det rekommenderas att medlemsstaterna använder ett offlinesystem för sina CSCA, t.ex. ett datorsystem som inte är anslutet till något nätverk. Flerpersonskontroll ska användas för åtkomst till systemet (t.ex. enligt principen om fyra ögon). Efter signering av DSC ska operativa kontroller tillämpas och det system som förvarar den privata CSCA-nyckeln ska lagras på ett säkert sätt med stark åtkomstkontroll. Säkerhetsmoduler i maskinvara (Hardware Security Modules) eller smartkort kan användas för att ytterligare skydda den privata nyckeln för CSCA. Digitala certifikat innehåller en giltighetsperiod som säkerställer förnyande av certifikaten. Det krävs ett förnyande för användning av färska krypteringsnycklar och för att anpassa nyckelstorlekarna vid nya förbättringar av datortekniken eller nya angrepp som hotar säkerheten för den krypteringsalgoritm som används. Det är skalmodellen som ska tillämpas (se *avsnitt 3.2*).

Följande giltighetsperioder rekommenderas, med tanke på de digitala covidintygens giltighetstid på ett år.

— CSCA: 4 år.

— DSC: 2 år.

— Uppladdning: 1–2 år.

— TLS-klientautentisering (TLS Client authentication): 1–2 år.

För förnyande i rätt tid rekommenderas följande användningsperioder för de privata nycklarna:

— CSCA: 1 år.

— DSC: 6 månader.

Medlemsstaterna måste skapa nya uppladdningscertifikat och TLS-certifikat i rätt tid, t.ex. en månad innan giltighetstiden löper ut, för att möjliggöra en smidig drift. CSCA-certifikat och DSC bör förnyas minst en månad innan användningen av den privata nyckeln upphör (med tanke på de nödvändiga operativa förfarandena). Medlemsstaterna måste tillhandahålla uppdaterade CSCA-certifikat och uppladdnings- och TLS-certifikat åt DCCG-operatören. Certifikat som är utgångna ska tas bort från vitlistan och tillitsförteckningen.

Medlemsstaterna och DCCG-operatören måste hålla reda på giltigheten för sina egna certifikat. Det finns inte någon central enhet som registrerar certifikatens giltighet och underrättar deltagarna.

4.3 *Återkallande av certifikat*

Generellt kan digitala certifikat återkallas av sin utfärdande CA med användning av certifikatåterkallandelistor (CRL) eller OCSP (Online Certificate Status Protocol Responder). CSCA:er för DCC-systemet bör tillhandahålla CRL. Även om dessa CRL för tillfället inte används av andra medlemsstater bör de integreras för framtida tillämpningar. Ifall en CSCA beslutar att inte tillhandahålla några CRL måste denna CSCA:s DSC:er förnyas när det blir obligatoriskt med CRL. Kontrollörer bör inte använda OCSP för validering av DSC utan bör använda CRL. Det rekommenderas att nationella backend-system utför den nödvändiga valideringen av DSC:er som laddats ner från DCC-nätslussen och endast vidarebefordrar en uppsättning betrodda och validerade DSC till nationella DCC-validerare. DCC-validerare bör inte utföra någon återkallandekontroll av DSC i sin valideringsprocess. Ett skäl till detta är att skydda DCC-innehavares integritet genom att undanröja risken för att användningen av en viss DCS skulle kunna övervakas av dess därmed förbundna OCSP.

Medlemsstaterna kan själva ta bort sina DSC från DCCG med hjälp av giltiga uppladdnings- och TLS-certifikat. Borttagandet av en DSC innebär att alla DCC:er som utfärdats med denna DSC kommer att bli ogiltiga när medlemsstaterna hämtar de uppdaterade DSC-förteckningarna. Det är mycket viktigt att skydda det privata nyckelmaterial som motsvarar DSC:erna. Medlemsstaterna måste informera DCCG-operatören när de måste återkalla uppladdnings- eller TLS-certifikat, på grund av att exempelvis ett nationellt backend-system komprometterats. DCCG-operatören kan sedan ta bort tillitsstatusen för det berörda certifikatet, exempelvis genom att ta bort det från TLS-vitlistan. DCCG-operatören kan ta bort de uppladdade certifikaten från DCCG-databasen. Paket som signerats med den privata nyckel som motsvarar detta uppladdningscertifikat kommer att bli ogiltiga när nationella backend-system tar bort tillitsstatusen för det återkallade uppladdningscertifikatet. Om ett CSCA-certifikat måste återkallas ska medlemsstaterna underrätta DCCG-operatöreren och andra medlemsstater som de har tillitsförhållanden till. DCCG-operatören kommer att utfärda en ny tillitsförteckning där det berörda certifikatet inte längre finns med. Alla DSC som utfärdas av denna CSCA kommer att bli ogiltiga när medlemsstaterna uppdaterar sin truststore avseende nationella backend-system. Om $DCCG_{TLS}$-certifikatet eller $DCCG_{TA}$-certifikatet måste återkallas ska DCCG-operatören och medlemsstaterna samarbeta för att upprätta en ny tillförlitlig TLS-anslutning och tillitsförteckning.

5. **Certifikatmallar**

I detta avsnitt fastställs krypteringskrav, riktlinjer och krav för certifikatmallar. För DCCG-certifikaten fastställer detta avsnitt certifikatmallarna.

5.1 *Krypteringskrav*

Krypteringsalgoritmer och TLS-chiffersviter ska väljas baserat på de nuvarande rekommendationerna från det tyska förbundsorganet för informationssäkerhet (BSI) eller SOG-IS. Dessa rekommendationer och rekommendationerna från andra institutioner och standardiseringsorganisationer liknar varandra. Rekommendationerna finns i de tekniska riktlinjerna TR 02102-1 och TR 02102-2 ([1]) eller SOG-IS Agreed Cryptographic Mechanisms ([2]).

5.1.1 Krav för DSC

De krav som anges i *bilaga I, avsnitt 3.2.2* ska tillämpas. Därför rekommenderas det starkt att dokumentsignatärer använder ECDSA (Elliptic Curve Digital Signature Algorithm) med NIST-p-256 (enligt definitionen i tillägg D till FIPS PUB 186-4). Andra elliptiska kurvor stöds inte. På grund av det begränsade utrymmet på det digitala covidintyget bör medlemsstaterna inte använda RSA-PSS, även om det är tillåtet som reservalgoritm. Om

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

medlemsstaterna använder RSA-PSS bör de använda en modulstorlek på 2048 eller högst 3072 bitar. SHA-2 med en outputlängd på ≥ 256 bitar ska användas som kryptografisk hashfunktion (se ISO/IEC 10118-3:2004) för DSC-signaturen.

5.1.2 Krav för TLS-, uppladdnings- och CSCA-certifikat

För digitala intyg och kryptografiska signaturer i DCCG-sammanhang sammanfattas huvudkraven för krypteringsalgoritmer och nyckellängd i följande tabell (från och med 2021):

Signaturalgoritm	Nyckelstorlek	Hashfunktion
EC-DSA.	Min. 250 bitar.	SHA-2 med en outputlängd på ≥ 256 bitar.
RSA-PSS (rekommenderad padding) RSA-PKCS#1 v1.5 (legacy padding).	Min. 3000 Bit RSA Modulus (N) med en öppen exponent på e > 2^16.	SHA-2 med en outputlängd på ≥ 256 bitar.
DSA	Min. 3000 Bit prime p, 250 Bit key q.	SHA-2 med en outputlängd på ≥ 256 bitar.

Den rekommenderade elliptiska kurvan för EC-DSA är NIST-p-256 på grund av dess omfattande användning.

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

Följande tabell innehåller riktlinjer för NB_{CSCA}-certifikatmallen om en medlemsstat beslutar att driva sin egen CSCA för DCC-systemet.

Poster i **fetstil** är obligatoriska (måste finnas på intyget), poster i *kursiverad stil* är rekommenderade (bör inkluderas). För utelämnade fält finns inga fastställda rekommendationer.

Fält	Värde
Område	**cn=<ej tomt och unikt gemensamt namn>,***o=<Tillhandahållare>,* **c=<Medlemsstat som driver CSCA>**
Nyckelanvändning	**signering av certifikat,***CRL-signering* (som minimum)
Grundläggande begränsningar	**CA = true, path length constraints = 0**

Områdesnamnet måste vara ifyllt och unikt inom den angivna medlemsstaten. Landskoden (c) måste matcha den medlemsstat som kommer att använda detta CSCA-certifikat. Certifikatet måste innehålla en unik områdesnyckelidentifierare (SKI) i enlighet med RFC 5280 ([3]).

5.3 *DSC (Document Signer Certificate)*

Följande tabell innehåller riktlinjer för DSC. Poster i **fetstil** är obligatoriska (måste inkluderas i certifikatet), poster i *kursiverad stil* är rekommenderade (bör inkluderas). För utelämnade fält finns inga fastställda rekommendationer.

Fält	Värde
Serienummer	**unikt serienummer**
Område	**cn=<ej tomt och unikt gemensamt namn>,***o=<Tillhandahållare>,* **c=<Medlemsstat som driver CSCA>**
Nyckelanvändning	**digital signatur** (som minimum)

([3]) rfc5280 (ietf.org).

DSC måste signeras med den privata nyckel som motsvarar ett CSCA-certifikat som används av medlemsstaten.

Följande tillägg ska användas:

— Certifikatet måste innehålla en AKI (Authority Key Identifier) som matchar SKI (Subject Key Identifier) för det utfärdande CSCA-certifikatet.

— Certifikatet bör innehålla en unik SKI (i enlighet med RFC 5280) ([4]).

Certifikatet bör också innehålla det CRL-distributionspunktstillägg (CRL distribution point extension) som pekar på den certifikatåterkallandelista (certificate revocation list, CRL) som tillhandahålls av den CSCA som utfärdade DSC.

DSC får innehålla ett utvidgat nyckelanvändningstillägg (key usage extension) med noll eller fler identifierare för nyckelanvändningspolicy (key usage policy identifiers) som avgränsar vilka typer av HCERT som detta certifikat har rätt att kontrollera. Om det finns ett eller flera sådana ska kontrollörerna kontrollera nyckelanvändningen mot lagrad HCERT. Följande värden för extendedKeyUsage fastställs för detta:

Fält	Värde
extendedKeyUsage	1.3.6.1.4.1.1847.2021.1.1 för utfärdare vad gäller tester (Test Issuers)
extendedKeyUsage	1.3.6.1.4.1.1847.2021.1.2 för utfärdare vad gäller vaccination (Vaccination Issuers)
extendedKeyUsage	1.3.6.1.4.1.1847.2021.1.3 för utfärdare vad gäller tillfrisknande (Recovery Issuers)

I avsaknad av något nyckelanvändningstillägg (dvs. inga tillägg eller noll tillägg) kan detta certifikat användas för att validera alla typer av HCERT. Andra dokument kan definiera relevanta ytterligare identifierare för utökad nyckelanvändningspolicy som används med validering av HCERT.

5.4 *Uppladdningscertifikat (Upload Certificates) (NBUP)*

Följande tabell innehåller riktlinjer för NBUP. Poster i **fetstil** är obligatoriska (måste inkluderas i certifikatet), poster i *kursiverad stil* är rekommenderade (bör inkluderas). För utelämnade fält finns inga fastställda rekommendationer.

Fält	Värde
Område	**cn=<ej tomt och unikt gemensamt namn>**, *o=<Tillhandahållare>*,**c=<Medlemsstat som använder detta uppladdningscertifikat>**
Nyckelanvändning	**digital signatur** (som minimum)

5.5 *National Backend TLS Client Authentication (NB_{TLS})*

Följande tabell innehåller riktlinjer för *Anm.:* TLS-klientautentiseringscertifikatet. Poster i **fetstil** är obligatoriska (måste inkluderas i certifikatet), poster i *kursiverad stil* är rekommenderade (bör inkluderas). För utelämnade fält finns inga fastställda rekommendationer.

Fält	Värde
Område	**cn=<ej tomt och unikt gemensamt namn>**, *o=<Tillhandahållare>*,**c=<Medlemsstat på NB>**
Nyckelanvändning	**digital signatur** (som minimum)
Utökad nyckelanvändning	kundautentisering (1.3.6.1.5.5.7.3.2)

([4]) rfc5280 (ietf.org)

Certifikatet får också innehålla *serverautentiseringen (1.3.6.1.5.5.7.3.1)* för den utökade nyckelanvändningen, men det är inget krav.

5.6 *Trust list signature certificate ($DCCG_{TA}$)*

I följande tabell definieras DCCG tillitsankar-certifikatet.

Fält	Värde
Område	**cn = Nätsluss för det digitala gröna intyget** ([5]), **o=<Tillhandahållare>, c=<land>**
Nyckelanvändning	**digital signatur** (som minimum)

5.7 *DCCG TLS-servercertifikat ($DCCG_{TLS}$)*

I följande tabell definieras DCCG TLS-certifikatet.

Fält	Värde
Område	cn=<FQDN eller IP-adress för DCCG>, o=<Tillhandahållare>, c= <land>
SubjectAltName	dNSName: <DCCG DNS-namn> eller IP-adress: <DCCG IP-adress>
Nyckelanvändning	**digital signatur** (som minimum)
Utökad nyckelanvändning	serverautentisering (1.3.6.1.5.5.7.3.1)

Certifikatet får också innehålla *klientautentiseringen (1.3.6.1.5.5.7.3.2)* för den utökade nyckelanvändningen, men det är inget krav.

DCCG:s TLS-certifikat ska utfärdas av en offentligt betrodd certifikatmyndighet (inkluderad i alla vanliga webbläsare och operativsystem, i enlighet med baslinjekraven från CAB Forum).

([5]) Termen ”digitalt grönt intyg” (Digital Green Certificate) i stället för ”EU:s digitala covidintyg” har behållits i detta sammanhang eftersom denna terminologi hårdkodades och användes i intyget innan medlagstiftarna beslutade om en ny terminologi.