►B

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)

(EUT L 230, 30.6.2021, s. 32)

Ändrad genom:

		Officiella tidningen		
		nr	sida	datum
►M1	Kommissionens genomförandebeslut (EU) 2021/2014 av den 17 november 2021	L 410	180	18.11.2021
►M2	Kommissionens genomförandebeslut (EU) 2021/2301 av den 21 december 2021	L 458	536	22.12.2021
►M3	Kommissionens genomförandebeslut (EU) 2022/483 av den 21 mars 2022	L 98	84	25.3.2022
►M4	Kommissionens genomförandebeslut (EU) 2022/1516 av den 8 september 2022	L 235	61	12.9.2022

▼B

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)

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.

▼M1

Artikel 4

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

Artikel 5

En gemensam samordnad datastruktur för de data som ska ingå i de intyg som avses i artikel 3.1 i förordning (EU) 2021/953, med användning av ett JSON-schema (*JavaScript Object Notation schema*), fastställs i bilaga V till detta beslut.

▼M3

Artikel 5a

Utbyte av förteckningar över återkallade intyg

1. Tillitsramverket för EU:s digitala covidintyg ska möjliggöra utbyte av förteckningar över återkallade intyg via den centrala nätslussen för EU:s digitala covidintyg (*nätslussen*) i enlighet med de tekniska specifikationerna i bilaga I.

2. När medlemsstaterna återkallar EU:s digitala covidintyg får de lämna in förteckningar över återkallade intyg till nätslussen.

▼M3

3. När medlemsstaterna lämnar in förteckningar över återkallade intyg ska de utfärdande myndigheterna föra en förteckning över återkallade intyg.

4. När personuppgifter utbyts via nätslussen ska behandlingen begränsas till syftet att stödja utbytet av information om återkallande. Sådana personuppgifter får endast användas för att kontrollera återkallandestatusen för EU:s digitala covidintyg som utfärdats inom ramen för förordning (EU) 2021/953.

5. Den information som lämnas till nätslussen ska omfatta följande uppgifter i enlighet med de tekniska specifikationerna i bilaga I:

a) Pseudonymiserade unika identifierare för intyg för återkallade intyg.

b) Sista giltighetsdatum för den inlämnade förteckningen över återkallade intyg.

6. Om en utfärdande myndighet återkallar EU:s digitala covidintyg som den har utfärdat i enlighet med förordning (EU) 2021/953 eller förordning (EU) 2021/954 och avser att utbyta relevant information via nätslussen ska den överföra den information som avses i punkt 5 i form av förteckningar över återkallade intyg till nätslussen i ett säkert format i enlighet med de tekniska specifikationerna i bilaga I.

7. De utfärdande myndigheterna ska i möjligaste mån tillhandahålla en lösning för att informera innehavarna av återkallade intyg om att deras intyg har återkallats och om skälet till återkallandet vid tidpunkten för återkallandet.

8. Nätslussen ska samla in de förteckningar över återkallade intyg som inkommit. Den ska tillhandahålla verktyg för att skicka ut förteckningarna till medlemsstaterna. Den ska automatiskt radera förteckningarna i enlighet med de sista giltighetsdatum som anges för varje inlämnad förteckning av den myndighet som lämnar in den.

9. De utsedda nationella myndigheter eller officiella organ i medlemsstaterna som behandlar personuppgifter i nätslussen ska vara gemensamt personuppgiftsansvariga för de uppgifter som behandlas. De gemensamt personuppgiftsansvarigas respektive ansvarsområden ska fördelas i enlighet med bilaga VI.

10. Kommissionen ska vara personuppgiftsbiträde för de personuppgifter som behandlas i nätslussen. I egenskap av personuppgiftsbiträde på medlemsstaternas vägnar ska kommissionen säkerställa säkerheten vid överföring och lagring av personuppgifter inom nätslussen och fullgöra personuppgiftsbiträdets skyldigheter enligt bilaga VII.

11. Ändamålsenligheten hos de tekniska och organisatoriska åtgärderna för att säkerställa säkerheten vid behandling av personuppgifter inom nätslussen ska regelbundet testas, bedömas och utvärderas av kommissionen och de gemensamt personuppgiftsansvariga.

▼M3

Artikel 5b

Tredjeländers inlämning av förteckningar över återkallade intyg

Tredjeländer som utfärdar covid-19-intyg för vilka kommissionen har antagit en genomförandeakt i enlighet med artikel 3.10 eller 8.2 i förordning (EU) 2021/953 får lämna in förteckningar över återkallade covid-19-intyg som omfattas av en sådan genomförandeakt, så att dessa kan behandlas av kommissionen, på de gemensamt personuppgiftsansvarigas vägnar, i den nätsluss som avses i artikel 5a, i enlighet med de tekniska specifikationerna i bilaga I.

Artikel 5c

Styrning av behandlingen av personuppgifter i den centrala nätslussen för EU:s digitala covidintyg

1. Beslutsprocessen för de gemensamt personuppgiftsansvariga ska styras av en arbetsgrupp som inrättats inom ramen för den kommitté som avses i artikel 14 i förordning (EU) 2021/953.

2. De utsedda nationella myndigheter eller officiella organ i medlemsstaterna som behandlar personuppgifter i nätslussen i egenskap av gemensamt personuppgiftsansvariga ska utse företrädare till den gruppen.

▼M1

Artikel 6

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

▼B

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

▼B

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)

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

▼B

— 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

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 ([1])) 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.

([1]) rfc8230 (ietf.org).

▼B

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 ([1]), 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.

3.2.6 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 ([2]), 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 ([3])) 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 ([4])). Applikationsutvecklare får i praktiken aldrig avkoda, eller koda till och från JSON-formatet utan ska använda in memory-strukturen.

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

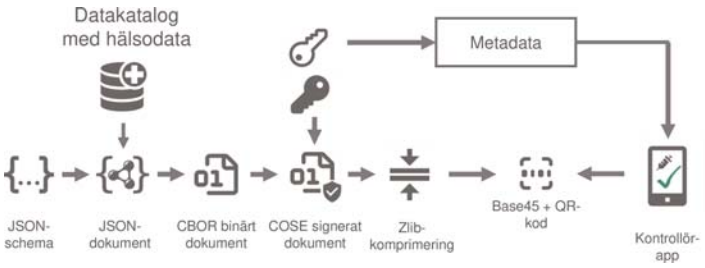
▼B

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 Unicodestandarden. 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 ([1]). Datainnehållet är begränsat till de definierade dataelementen i de minimidataset som anges i bilagan till förordning 2021/953.

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.

([1]) 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).

▼B

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 ([1])) och komprimeringsmekanismen Deflate i det format som definieras i RFC 1951 ([2]).

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.

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

▼B

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.

▼B

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 ([1]), 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.

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

▼B

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.

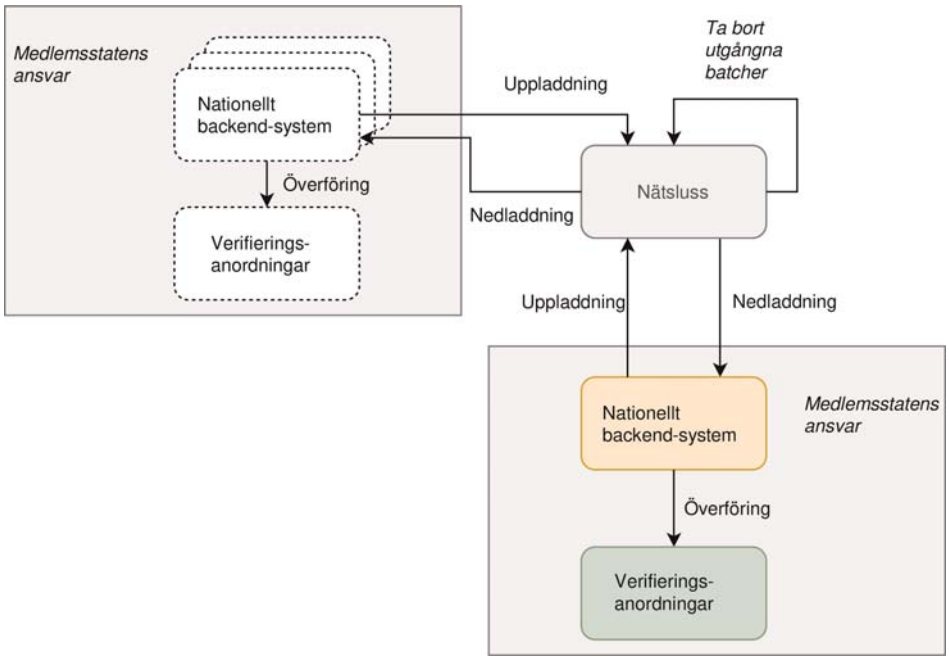
— Medlemsstaterna kan välja att aldrig göra någon kontroll av offentliggjorda återkallanden, utan i stället helt förlita sig på de DSC-förteckningar som de dagligen får från sekretariatet eller själva sammanställer.

▼M3

9. **Systemlösning för återkallande**

9.1 *Tillhandahållande av förteckningar (DRL) över återkallade digitala covidintyg (DCC)*

Nätslussen (gateway) ska ge tillgång till ändpunkter (endpoints) och funktionalitet för att lagra och hantera återkallandeförteckningarna:



▼M3

9.2 *Tillitsmodell*

Alla anslutningar skapas av den standardiserade tillitsmodellen för nätslussen (DCCG) genom NB_{TLS}- och NB_{UP}-certifikaten (se hantering av certifikat). All information packas och laddas upp med CMS-meddelanden för att säkerställa integriteten.

9.3 *Utformning av batcher*

9.3.1 Batch

Varje återkallandeförteckning ska innehålla en eller flera poster och ska packas i batcher som innehåller en uppsättning hashvärden (hashes) och tillhörande metadata. En batch är oföränderlig och har ett utgångsdatum som anger när batchen kan raderas. Alla element i batchen måste ha exakt samma utgångsdatum, vilket innebär att batcherna måste grupperas efter utgångsdatum och efter signerande DSC. Varje batch får innehålla högst 1 000 poster. Om återkallandeförteckningen består av fler än 1 000 poster ska flera batcher skapas. Varje post får förekomma i högst en batch. Batchen ska packas i en CMS-struktur och signeras med det uppladdande landets NB_{up}-certifikat.

9.3.2 Batchindex

När en batch skapas ska den tilldelas ett unikt ID av nätslussen och automatiskt läggas till i indexet. Indexet över batcher ordnas efter ändringsdatum, i stigande kronologisk ordning.

9.3.3 Nätslussens funktion

Nätslussen behandlar återkallandebatcher utan att göra några ändringar: den kan varken uppdatera, ta bort eller lägga till någon information i batcherna. Batcherna vidarebefordras till alla godkända länder (se kapitel 9.6).

Nätslussen övervakar batchernas utgångsdatum och tar bort utgångna batcher. Efter att batchen har raderats sänder nätslussen tillbaka svaret ”HTTP 410 Gone” för den raderade batchens URL. Batchen anges därför i batchindexet som ”deleted”.

9.4 *Hashtyper*

Återkallandeförteckningen innehåller hashvärden som kan representera olika återkallandetyper/-attribut. Dessa typer eller attribut ska anges vid tillhandahållandet av återkallandeförteckningarna. Följande typer används för närvarande:

Typ	Attribut	Beräkning av hashvärden
SIGNATURE	DCC Signature	SHA256 of DCC Signature
UCI	UCI (Unique Certificate Identifier)	SHA256 of UCI
COUNTRYCODEUCI	Issuing Country Code + UCI	SHA256 of Issuing Country-Code + UCI

Bara de första 128 bits av hashvärdena, kodade som base64-strängar, läggs in i batcherna och används för att identifiera ett återkallat DCC ([1]).

([1]) Se även de detaljerade API-beskrivningarna i avsnitt 9.5.1.2.

▼**M3**

9.4.1 Hashtyp: SHA256(DCC-signatur)

I detta fall beräknas hashvärdet på grundval av samtliga byte för COSE_SIGN1-signaturen från CWT. För RSA-signaturer kommer hela signaturen att användas som indata. Formeln för EC-DSA-signerade certifikat använder r-värdet som indata:

SHA256(r)

[krävs för alla nya tillämpningar]

9.4.2 Hashtyp: SHA256(UCI)

I detta fall beräknas hashvärdet på grundval av den UCI-sträng som är kodad i UTF-8 och konverterad till en bytesträng (byte array).

[föråldrad ([1]), men stöds för bakåtkompatibilitet]

9.4.3 Hashtyp: SHA256(Issuing CountryCode+UCI)

I detta fall landskod kodad som en UTF-8-sträng, konkatenerad med UCI kodad som en UTF-8-sträng. Detta konverteras sedan till en bytesträng och används som indata till hashfunktionen.

[föråldrad[2], men stöds för bakåtkompatibilitet]

9.5 *API-struktur*

9.5.1 API för tillhandahållande av återkallandepost

9.5.1.1 Syfte

API tillhandahåller posterna i återkallandeförteckningen i batcher som inkluderar ett batchindex.

9.5.1.2 Ändpunkter

9.5.1.2.1 Ändpunkt för nedladdning av batchlista

Ändpunkterna har en enkel utformning och returnerar en batchlista tillsammans med en liten wrapper som innehåller metadata. Batcherna sorteras efter *datum* i *stigande (kronologisk)* ordning:

/revocation-list

Verb: GET

Content-Type: application/json

Response: JSON Array

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

([1]) Föråldrad innebär att denna funktion inte ska användas för nya tillämpningar men ska stödjas för befintliga tillämpningar under en väldefinierad tidsperiod.

▼M3

Anmärkning: Resultatet begränsas automatiskt till 1 000. Om flaggan ”more” är satt till ”true” anger svaret att fler batcher kan laddas ned. För att ladda ned fler element måste klienten sätta headern If-Modified-Since till ett datum som är lika med eller senare än datumet för den senast mottagna posten.

Svaret innehåller en JSON-sträng (array) med följande struktur:

Fält	Definition
more	Boolesk flagga som anger att det finns fler batcher.
batches	Sträng med befintliga batcher.
batchId	https://en.wikipedia.org/wiki/Universally_unique_identifier
country	Landskod enligt ISO 3166.
date	UTC-datum enligt ISO 8601. Datum då batchen lades till eller raderades.
deleted	boolean. ”True” innebär radering. När flaggan för radering är satt kan posten slutligen tas bort från sökresultaten efter 7 dagar.

9.5.1.2.1.1 Svarskoder

Kod	Beskrivning
200	Alla ok.
204	Inget innehåll om headern ”If-Modified-Since” inte har något matchande värde.

Header för begäran

Header	Obligatoriskt	Beskrivning
If-Modified-Since	Ja	Den här headern innehåller datum för senaste nedladdning för att man ska få enbart de senaste resultaten. Vid den första begäran ska headern sättas till ”2021–06–01T00:00:00Z”

9.5.1.2.2 Ändpunkt för nedladdning av batcher

Batcherna innehåller en lista med identifierare för certifikat:

/revocation-list/{batchId}

Verb: GET

Accepts: application/cms

Response:CMS with Content

{

”country”: ”XY”,

”expires”: ”2022–11–01T00:00:00Z”,

▼**M3**

”kid”:‘23S+33f=’,

‘hashType’:‘SIGNATURE’,

”entries”:[{

”hash”:‘e2e2e2e2e2e2e2e2’

}, ..]

}

Svaret innehåller en CMS med en signatur som måste överensstämma med landets NB_{UP}-certifikat. Alla element i JSON-strängen innehåller följande struktur:

Fält	Obligatoriskt	Typ	Definition
expires	Ja	String	Datum då elementet kan tas bort. UTC-datum/tid enligt ISO 8601
country	Ja	String	Landskod enligt ISO 3166.
hashType	Ja	String	Hashtyp för de tillhandahållna posterna (se hashtyper)
entries	Ja	JSON Object Array	Se tabell Poster
kid	Ja	String	base64-kodad KID för det DSC som används för att signera DCC. Om KID är okänd kan strängen 'UNKNOWN_KID' (utan') användas.

Anmärkningar:

— Batcherna ska grupperas efter utgångsdatum och DSC – alla element ska upphöra att gälla samtidigt och ha signerats med samma nyckel.

— Utgångsdatum är ett datum/en tidpunkt i UTC eftersom EU-DCC är ett globalt system och en otvetydig tidsangivelse måste användas.

— Utgångsdatum för ett permanent återkallat DCC ska fastställas till utgångsdatumet för motsvarande DSC som används för att signera DCC eller till den tidpunkt då det återkallade DCC upphör att gälla (Expiration Time; de använda NumericDate/epoch-tiderna ska då betraktas som om de avser UTC-tidszonen).

— Det nationella backend-systemet (NB) ska ta bort element från sin återkallandeförteckning när **utgångsdatumet** infaller.

— *Anm.:* får ta bort element från sin återkallandeförteckning om den **kid** som använts för att signera DCC återkallas.

▼M3

9.5.1.2.2.1 Poster

Fält	Obligatoriskt	Typ	Definition
hash	Ja	String	De första 128 bits av SHA256-hashen kodade som en base64-sträng

Anmärkning: Objektet ”entries” innehåller för närvarande bara ett hashvärde, men för att säkra kompatibilitet med framtida ändringar valdes ett objekt i stället för en json-sträng.

9.5.1.2.2.2 Svarskoder

Kod	Beskrivning
200	Alla ok.
410	Batchen saknas. Batchen kan raderas i det nationella backend-systemet.

9.5.1.2.2.3 Header för svar

Header	Beskrivning
ETag	Batchens ID

9.5.1.2.3 Ändpunkt för uppladdning av batcher

Uppladdningen görs via samma ändpunkt med verbet POST:

/revocation-list

Verb: POST

Accepts: application/cms

Request: CMS with Content

ContentType: application/cms

Content:

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

Batchen ska signeras med hjälp av NB_{UP} -certifikatet. Nätslussen ska verifiera att signaturen har angetts med hjälp av NB_{UP} för det berörda landet (*country*). Om signaturen inte godkänns ska uppladdningen inte göras.

ANMÄRKNING: Varje batch är oföränderlig och kan inte ändras efter uppladdning. Den kan dock raderas. ID för varje raderad batch lagras, och en uppladdning av en ny batch med samma ID avvisas.

▼**M3**

9.5.1.2.4 Ändpunkt för radering av batcher

En batch kan raderas via samma ändpunkt med verbet DELETE:

/revocation-list

Verb: DELETE

Accepts: application/cms

ContentType: application/cms

Request: CMS with Content

Content:

{

”batchId”: ”...”

}

eller, av kompatibilitetsskäl, till följande ändpunkt med verbet POST:

/revocation-list/delete

Verb: POST

Accepts: application/cms

ContentType: application/cms

Request: CMS with Content

Content:

{

”batchId”: ”...”

}

9.6 *API-skydd – GDPR*

I detta avsnitt anges åtgärder för att tillämpningen ska följa bestämmelserna i förordning (EU) 2021/953 när det gäller behandling av personuppgifter.

9.6.1 Befintlig autentisering

Nätslussen använder för närvarande NB_{TLS}-certifikatet för att autentisera de länder som ansluter till nätslussen. Denna autentisering kan användas för att fastställa identiteten för det land som är anslutet till nätslussen. Denna identitet kan sedan användas för att genomföra åtkomstkontroll.

9.6.2 Åtkomstkontroll

För att lagligen kunna behandla personuppgifter ska nätslussen använda en mekanism för åtkomstkontroll.

Nätslussen tillämpar en åtkomstkontrollista i kombination med rollbaserad säkerhet (Role Based Security). I det systemet ska två tabeller underhållas – en tabell som beskriver vilka roller (Roles) som kan tillämpa specifika operationer på specifika resurser och en annan tabell som beskriver vilka roller som tilldelas specifika användare (Users).

För att göra de kontroller som krävs enligt detta dokument krävs tre roller, nämligen

RevocationListReader

RevocationUploader

RevocationDeleter

▼**M3**

Följande ändpunkter ska kontrollera om användaren har rollen RevocationListReader; om så är fallet ska åtkomst beviljas, om inte ska HTTP 403 Forbidden returneras:

GET /revocation-list/

GET /revocation-list/{batchId}

Följande ändpunkter ska kontrollera om användaren har rollen RevocationUploader; om så är fallet ska åtkomst beviljas, om inte ska HTTP 403 Forbidden returneras:

POST /revocation-list

Följande ändpunkter ska kontrollera om användaren har rollen RevocationDeleter; om så är fallet ska åtkomst beviljas, om inte ska HTTP 403 Forbidden returneras:

DELETE /revocation-list

POST /revocation-list/delete

Nätslussen ska också tillhandahålla en tillförlitlig metod som gör det möjligt för administratörerna att hantera de roller som är kopplade till användarna på ett sådant sätt att risken för mänskliga fel reduceras samtidigt som de funktionella administratörerna inte belastas.

▼M1

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 av EU:s digitala covidintyg. 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 översättningen av kodade element till det nationella språket.

För alla datafält som inte nämns i beskrivningarna av värdeset nedan beskrivs kodningen i bilaga V.

Om de nedan angivna förespråkade kodningssystemen av någon anledning inte kan användas får andra internationella kodningssystem användas, och det ska 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 ska sammanpassa dessa koder med de värdeset som beskrivs. Medlemsstaterna har ansvaret för all sådan sammanpassning.

►M4 Mot bakgrund av de täta ändringarna av några värdeset som baseras på de kodningssystem som föreskrivs i denna bilaga, såsom de värdeset som avser kodning av vaccin och antigentester, ska dessa offentliggöras och regelbundet uppdateras av kommissionen med stöd av nätverket för e-hälsa och hälsosäkerhetskommittén. ◄ Uppdaterade värdeset ska offentliggöras på kommissionens berörda 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)**

   Ska användas i intyg 1, 2 och 3.

   Följande koder ska användas:

Kod	Visas (*display*)	Kodsystem namn	Kodsystem URL	Kodsystem OID	Kodsystem version
840539006	COVID-19	SNOMED CT	http://snomed.info/sct	2.16.840.1.113883.6.96	2021-01-31

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

   Förespråkat kodningssystem: SNOMED CT eller ATC-klassificering

   Ska användas i intyg 1.

   Exempel på koder som ska 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).

   Ett värdeset som anger de koder som ska användas i enlighet med det kodningssystem som fastställs i detta avsnitt ska offentliggöras och regelbundet uppdateras av kommissionen med stöd av nätverket för e-hälsa. Detta värdeset ska utvidgas när nya vaccintyper utvecklas och börjar användas.

▼M1

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 ska dessa ersättas med bindestreck (-).

Namn på berört värdeset: Vaccin.

Ska användas i intyg 1.

Ett exempel på en kod som ska 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).

Ett värdeset som anger de koder som ska användas i enlighet med det kodningssystem som fastställs i detta avsnitt ska offentliggöras och regelbundet uppdateras av kommissionen med stöd av nätverket för e-hälsa.

Vaccin ska kodas med användning av en befintlig kod från det värdeset som offentliggjorts, även om vaccinet har olika namn i olika länder. Anledningen är att det fortfarande inte finns något globalt vaccinregister som omfattar alla vaccin som används i dagsläget. Exempel:

— För vaccinet ”COVID-19 Vaccine Moderna Intramuscular Injection”, som är benämningen på Spikevax i Japan, ska koden EU/1/20/1507 användas, eftersom detta är vaccinets namn i EU.

Om detta inte är möjligt eller tillrådligt i ett enskilt fall kommer en separat kod att tillhandahållas i det värdeset som offentliggörs.

▼M4

Om ett land som använder EU:s digitala covidintyg beslutar att utfärda vaccinationsintyg åt deltagare i kliniska prövningar under pågående kliniska prövningar ska vaccinläkemedlet kodas enligt mönstret

CT_*clinical-trial-identifier* (CT_*identifierare-för-klinisk-prövning*)

Om den kliniska prövningen har registrerats i EU:s register över kliniska prövningar (EU-CTR) ska den kliniska prövningens identifierare från det registret användas. I andra fall får identifierare från andra register (såsom clinicaltrials.gov eller Australian New Zealand Clinical Trials Registry) användas.

Den kliniska prövningens identifierare ska innehålla ett prefix som gör det möjligt att identifiera registret över kliniska prövningar (såsom EUCTR för EU:s register över kliniska prövningar, NCT för clinicaltrials.gov och ACTRN för Australian New Zealand Clinical Trials Registry).

I de fall då kommissionen har fått riktlinjer från hälsosäkerhetskommittén, Europeiska centrumet för förebyggande och kontroll av sjukdomar (ECDC) eller Europeiska läkemedelsmyndigheten (EMA) med avseende på godtagandet av intyg som utfärdats för ett covid-19-vaccin som genomgår kliniska prövningar, ska dessa riktlinjer offentliggöras, antingen som en del av dokumentet med värdeset eller separat.

▼M1

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 ska dessa ersättas med bindestreck (-).

Ska användas i intyg 1.

Ett exempel på en kod som ska 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).

Ett värdeset som anger de koder som ska användas i enlighet med det kodningssystem som fastställs i detta avsnitt ska offentliggöras och regelbundet uppdateras av kommissionen med stöd av nätverket för e-hälsa.

Olika filialer av samma innehavare av ett godkännande för försäljning eller av samma tillverkare ska använda en befintlig kod från det värdeset som offentliggjorts.

Generellt ska den kod som avser innehavaren av ett godkännande för försäljning inom EU användas för samma vaccinprodukt, eftersom det ännu inte finns något internationellt godkänt register över vaccintillverkare eller innehavare av godkännande för försäljning. Exempel:

— För organisationen ”Pfizer AG”, som är innehavare av ett godkännande för försäljning för vaccinet ”Comirnaty” som används i Schweiz, ska koden ORG-100030215, som avser BioNTech Manufacturing GmbH, användas, eftersom det är innehavaren av godkännandet för försäljning i EU.

— För organisationen ”Zuellig Pharma”, som är innehavare av ett godkännande för försäljning för vaccinet Covid-19 Vaccine Moderna (Spikevax) som används i Filippinerna, ska koden ORG-100031184, som avser Moderna Biotech Spain S.L. användas, eftersom det är innehavaren av godkännandet för försäljning av Spikewax i EU.

Om detta inte är möjligt eller tillrådligt i ett enskilt fall kommer en separat kod att tillhandahållas i det värdeset som offentliggörs.

▼M4

Om ett land som använder EU:s digitala covidintyg beslutar att utfärda vaccinationsintyg åt deltagare i kliniska prövningar under pågående kliniska prövningar ska innehavare av godkännande för försäljning av vaccin eller tillverkare kodas med användning av det värde som anges i berört värdeset, om tillgängligt. I andra fall ska innehavare av godkännande för försäljning av vaccin eller vaccintillverkare kodas enligt den regel som beskrivs i avsnitt 3 Covid-19-vaccinläkemedel (CT_*identifierare-för-klinisk-prövning*).

▼M1

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

Ska användas i intyg 1.

Två fält:

(1) Nummer i en serie doser av ett Covid-19-vaccin:

(2) Totalt antal doser i vaccinationsserien (C).

5.1 *Primär vaccinationsserie*

När en person får doser som ingår i den primära vaccinationsserien, dvs. den vaccinationsserie som är avsedd att ge tillräckligt skydd i en inledande fas, ska (C) återspegla det totala antalet doser i den primära standardvaccinationsserien (dvs. 1 eller 2, beroende på vilken typ av vaccin som administreras). Detta innefattar alternativet att använda en kortare serie (C=1) i de fall då det vaccinationsprotokoll som tillämpas av en medlemsstat omfattar administrering av en enda dos av ett 2-dosvaccin till personer som tidigare varit smittade av SARS-CoV-2. En slutförd primär vaccinationsserie ska därför anges med N/C = 1. Exempel:

— 1/1 betecknar slutförandet av en primär vaccinationsserie som omfattar ett 1-dosvaccin, eller slutförandet av en primär vaccinationsserie som omfattar en dos av ett 2-dosvaccin som administreras till en tillfrisknad person i enlighet med det vaccinationsprotokoll som tillämpas av en medlemsstat.

— 2/2 betecknar slutförandet av en primär vaccinationsserie med ett 2-dosvaccin.

I de fall då den primära vaccinationsserien utvidgas, exempelvis för personer med kraftigt försvagat immunförsvar eller då det rekommenderade intervallet mellan de primära doserna inte har iakttagits, ska alla sådana doser kodas som ytterligare doser som omfattas av avsnitt 5.2.

▼M2

5.2 *Påfyllnadsdoser*

I de fall då en person erhåller doser efter primärvaccinationsserien ska sådana påfyllnadsdoser återspeglas i de motsvarande intygen enligt följande:

— 2/1 betecknar administrering av en påfyllnadsdos efter primärvaccination med ett 1-dosvaccin, eller administrering av en påfyllnadsdos efter slutförandet av en primärvaccinationsserie som omfattar en dos av ett 2-dosvaccin som administreras till en tillfrisknad person i enlighet med det vaccinationsprotokoll som tillämpas av en medlemsstat. Därefter ska doser (X) som administreras efter den första påfyllnadsdosen anges med (2+X)/(1) > 1 (t.ex. 3/1).

— 3/3 betecknar administrering av en påfyllnadsdos efter slutförandet av en primärvaccinationsserie med ett 2-dosvaccin. Därefter ska doser (X) som administreras efter den första påfyllnadsdosen anges med (3+X)/(3+X) = 1 (t.ex. 4/4).

Medlemsstaterna ska tillämpa de regler för kodning som anges i detta avsnitt senast den 1 februari 2022.

Medlemsstaterna ska, automatiskt eller på begäran av de personer som berörs, återutfärda intyg i vilka administreringen av en påfyllnadsdos efter primärvaccination med ett 1-dosvaccin kodats på ett sådant sätt att den inte kan särskiljas från slutförandet av en primärvaccinationsserie.

▼M2

Vid tillämpningen av denna bilaga bör hänvisningar till ”påfyllnadsdoser” tolkas som att de även omfattar extradoser som getts för att bättre skydda individer som uppvisar otillräckliga immunsvar efter en avslutad normal primärvaccinationsserie. Inom den rättsliga ram som fastställs genom förordning (EU) 2021/953 får medlemsstaterna vidta åtgärder för att hantera situationen för utsatta grupper som kan prioriteras för extradoser. Om en medlemsstat exempelvis beslutar att administrera extradoser endast till specifika undergrupper av befolkningen kan den, i enlighet med artikel 5.1 i förordning (EU) 2021/953, välja att utfärda vaccinationsintyg som anger att sådana extradoser administrerats endast på begäran och inte automatiskt. När sådana åtgärder vidtas ska medlemsstaterna underrätta de berörda personerna om detta och även om att de får fortsätta att utnyttja det intyg de fick efter slutförandet av den normala primärvaccinationsserien.

▼M1

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). Om vaccinationen eller testet utfördes av en internationell organisation (t.ex. UNHCR eller WHO) och ingen landsinformation finns tillgänglig, ska en kod för organisationen användas. Sådana kompletterande koder ska offentliggöras och regelbundet uppdateras av kommissionen med stöd av nätverket för e-hälsa.

7. **Typ av test**

Ska användas i intyg 2, och i intyg 3 om stöd för utfärdandet av intyg på tillfrisknande baserat på andra typer av tester än NAAT införs genom en delegerad akt.

Följande koder ska användas.

Kod	Visas (*display*)	Kodsystem namn	Kodsystem URL	Kodsystem OID	Kodsystem version
LP6464-4	Nukleinsyraamplifiering med probpåvisande	LOINC	http://loinc.org	2.16.840.1.113883.6.1	2.69
LP217198-3	Snabbimmunanalys	LOINC	http://loinc.org	2.16.840.1.113883.6.1	2.69

▼M4

Koden LP217198-3 (snabbimmunanalys) ska användas för angivelse av både antigentester i form av snabbtester och laboratoriebaserade antigentester.

▼M1

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

Ska användas i intyg 2.

▼M4

Innehållet i detta värdeset ska innefatta det urval av antigentester som finns förtecknade i den gemensamma och uppdaterade förteckningen över antigentest för covid-19, upprättad 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.

▼M1

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

9. **Testresultat**

Ska användas i intyg 2.

Följande koder ska användas:

Kod	Visas (*display*)	Kodsystem namn	Kodsystem URL	Kodsystem OID	Kodsystem version
260415000	Ej påvisat	SNOMED CT	http://snomed.info/sct	2.16.840.1.113883.6.96	2021-01-31
260373001	Påvisat	SNOMED CT	http://snomed.info/sct	2.16.840.1.113883.6.96	2021-01-31

▼B

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.

▼M1

3. **Allmänna krav**

Följande övergripande krav ska 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]), nämligen {'/','#',':'}.

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

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

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

([2]) För implementering med QR-koder kan medlemsstaterna överväga att använda 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.

▼M1

(4) Landprefix: 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 kan 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 ska vara ISO-7812-1 (LUHN-10) ([1]) -sammanfattningen av hela UCI i digitalt format/trådtransportformat (*wire transport format*). Checksumman separeras från resten av UCI med ett ”#”-tecken.

Kompatibiliteten bakåt ska säkerställas: medlemsstater som efter hand 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.

▼B

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

Riktlinjerna från nätverket för e-hälsa avseende kontrollerbara vaccinationsintyg och grundläggande interoperabilitetselement ([2]) 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.

([1]) 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).

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

▼B

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.

▼B

Term	Definition
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.
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.

▼B

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.

▼B

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.

▼B

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.

▼B

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.

▼B

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]).

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

▼B

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 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 ([1]).

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

▼B

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)

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) ([1]).

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.

([1]) rfc5280 (ietf.org)

▼B

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)

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** [1]**, 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)

[1] 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.

▼B

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).

▼M1

BILAGA V

JSON-SCHEMA (*JAVASCRIPT OBJECT NOTATION SCHEMA*)

1. **Inledning**

I bilagan fastställs den tekniska datastrukturen för EU:s digitala covidintyg (*EUDCC*), representerad som ett JSON-schema. Dokumentet innehåller specifika instruktioner för de enskilda datafälten.

2. **JSON-schema – lokalisering och versioner**

Det enda autentiska officiella JSON-schemat för EUDCC offentliggörs på: https://github.com/ehn-dcc-development/ehn-dcc-schema. Scheman på andra platser är inte autentiska, men kan användas vid förberedelse av kommande ändringar.

Som standard visas den aktuella versionen enligt denna bilaga som stöds av alla länder och som för närvarande används för att generera intyg under angivet URL.

Nästa version, som senast ett fastställt datum ska stödjas av alla länder, visas under angivet URL genom versionstaggning som beskrivs mer detaljerat i Readme-filen.

▼M3

3. **Gemensamma strukturer och allmänna krav**

EU:s digitala covidintyg får inte utfärdas om inte alla datafält kan fyllas i korrekt i enlighet med denna specifikation på grund av att information saknas. **Detta ska inte förstås som att det påverkar medlemsstaternas skyldighet att utfärda EU:s digitala covidintyg.**

Informationen i alla fält får tillhandahållas med hjälp av den fullständiga teckenuppsättningen UNICODE 13.0 som kodas med användning av UTF-8, om inte tillhandahållandet är specifikt begränsat till värdeset eller snävare teckenuppsättningar.

Den gemensamma strukturen ska vara följande:

"JSON":{

"ver":<information om version>,

"nam":{

<information om personens namn>

},

"dob":<födelsedatum>,

"v" eller "t" eller "r":[

{<information om vaccinationsdos eller test eller tillfrisknande, en post>}

]

}

Detaljerad information om individuella grupper och fält finns i de följande avsnitten.

Om reglerna anger att ett fält ska hoppas över innebär detta att det ska lämnas tomt och att varken fältets namn eller dess värde får ingå.

▼M3

3.1. *Version*

Information om versionen ska tillhandahållas. Versionshanteringen följer Semantic Versioning (semver: https://semver.org). Versionen ska vara en av de versioner som släppts officiellt (nuvarande version eller en av de äldre versioner som släppts officiellt). Se avsnittet JSON-schema – lokalisering för mer detaljer.

Fältets id	Fältets namn	Instruktioner
ver	Schemaversion	Ska motsvara identifieraren för den schemaversion som används för att producera EUDCC. Exempel: "ver":"1.3.0"

3.2. *Personens namn och födelsedatum*

Personens namn ska vara det fullständiga officiella namnet på personen, som är identiskt med det namn som anges i resehandlingar. Strukturens identifierare är *nam*. Exakt 1 (ett) personnamn ska tillhandahållas.

Fältets id	Fältets namn	Instruktioner
nam/fn	Efternamn (ett eller flera)	Innehavarens efternamn (ett eller flera) Om innehavaren inte har några efternamn men har ett förnamn ska detta fält hoppas över. I samtliga andra fall ska exakt 1 (ett) icke-tomt fält tillhandahållas, där alla efternamn inkluderats. Om det finns flera efternamn ska dessa separeras med mellanslag. Kombinationsnamn där bindestreck eller liknande tecken ingår ska dock vara oförändrade. Exempel: "fn":"Musterfrau-Gößinger" "fn":"Musterfrau-Gößinger Müller"
nam/fnt	Standardiserade efternamn (ett eller flera)	Innehavarens efternamn som translittererats enligt samma konvention som i innehavarens maskinläsbara resehandlingar (såsom de regler som fastställs i Icao Doc 9303 Part 3). Om innehavaren inte har några efternamn men har ett förnamn ska detta fält hoppas över. I samtliga andra fall ska exakt 1 (ett) icke-tomt fält tillhandahållas, där alla förnamn inkluderats, och endast tecknen A-Z och < får användas. Maximal längd: 80 tecken (enligt specifikationen i Icao 9303). Exempel: "fnt":"MUSTERFRAU<GOESSINGER" "fnt":"MUSTERFRAU<GOESSINGER<MUELLER"
nam/gn	Förnamn (ett eller flera)	Innehavarens förnamn (ett eller flera). Om innehavaren inte har några förnamn men har ett efternamn ska detta fält hoppas över. I samtliga andra fall ska exakt 1 (ett) icke-tomt fält tillhandahållas, där alla förnamn inkluderats. Om det finns flera förnamn ska dessa separeras med mellanslag. Exempel: "gn":"Isolde Erika"

▼M3

Fältets id	Fältets namn	Instruktioner
nam/gnt	Standardiserade förnamn (ett eller flera)	Innehavarens förnamn som translitterererats enligt samma konvention som i innehavarens maskinläsbara resehandlingar (såsom de regler som fastställs i Icao Doc 9303 Part 3). Om innehavaren inte har några förnamn men har ett efternamn ska detta fält hoppas över. I samtliga andra fall ska exakt 1 (ett) icke-tomt fält tillhandahållas, där alla förnamn inkluderats, och endast tecknen A-Z och < får användas. Maximal längd: 80 tecken. Exempel: "gnt":"ISOLDE<ERIKA"
dob	Födelsedatum	DCC-innehavarens födelsedatum. Fullständigt eller partiellt datum men ej tid, begränsat till intervallet 1900-01-01–2099-12-31. Exakt 1 (ett) icke-tomt fält ska tillhandahållas om det fullständiga eller partiella födelsedatumet är känt. Om födelsedatumet inte är känt ens partiellt ska fältet innehålla en tom sträng "". Detta bör vara identiskt med den information som tillhandahålls i resehandlingar. Ett av följande ISO 8601-format ska användas om information om födelsedatum finns tillgänglig. Andra alternativ stöds inte. YYYY-MM-DD YYYY-MM YYYY (Verifieringsappen kan visa att delar av födelsedatumet saknas med hjälp av den XX-konvention som används i maskinläsbara resehandlingar, t.ex. 1990-XX-XX.) Exempel: "dob":"1979-04-14" "dob":"1901–08" "dob":"1939" "dob":""

3.3. *Grupper för information som är specifik för intygstypen*

JSON-schemat stöder tre grupper av poster som omfattar information som är specifik för intygstypen. Varje EUDCC ska innehålla exakt 1 (en) grupp. Tomma grupper är inte tillåtna.

Gruppidentifierare	Gruppnamn	Poster
v	Vaccinationsgrupp	Ska, i förekommande fall, innehålla exakt 1 (en) post som beskriver exakt 1 (en) vaccinationsdos (en dos).
t	Testgrupp	Ska, i förekommande fall, innehålla exakt 1 (en) post som beskriver exakt 1 (ett) testresultat.
r	Tillfrisknandegrupp	Ska, i förekommande fall, innehålla exakt 1 (en) post som beskriver exakt 1 (en) utsaga om tillfrisknande.

▼M1

4. **Information som är specifik för intygstypen**

4.1 *Vaccinationsintyg*

Vaccinationsgrupp, i förekommande fall, ska innehålla exakt 1 (en) post som exakt beskriver en vaccinationshändelse (en dos). Alla element av vaccinationsgruppen är obligatoriska, tomma värden stöds inte.

▼**M1**

Fältets id	Fältets namn	Anvisningar
v/tg	Sjukdom eller smittämne Covid-19 (SARS-CoV-2 eller en av dess varianter)	Ett kodat värde från värdeset disease-agent-targeted.json. Detta värdeset har den enda posten 840539006, som är koden för covid-19 från SNOMED CT (GPS). Exakt 1 (ett) icke-tomt fält ska tillhandahållas. Exempel: ”tg”: ”840539006”
v/vp	Covid-19-vaccin eller covid-19-profylax	Typ av vaccin eller profylax som använts. Ett kodat värde från värdeset vaccine-prophylaxis.json. Detta värdeset distribueras från EUDCC-nätslussen. Exakt 1 (ett) icke-tomt fält ska tillhandahållas. Exempel: ”vp”: ”1119349007” (ett SARS-CoV-2 mRNA-vaccin)
v/mp	Covid-19-vaccinprodukt	Läkemedel som använts för denna specifika vaccinationsdos. ►**M4** Ett kodat värde från värdeset vaccine-medicinal-product.json. Eller ett kodat värde som avser en klinisk prövning och som följer den regel som fastställs i avsnitt 3 i bilaga II. ◄ Detta värdeset distribueras från EUDCC-nätslussen. Exakt 1 (ett) icke-tomt fält ska tillhandahållas. Exempel: ”mp”: ”EU/1/20/1528” (Comirnaty)
v/ma	Innehavare av godkännande för försäljning av covid-19-vaccin eller covid-19-vaccintillverkare	Innehavaren av godkännandet för försäljning eller tillverkaren om ingen innehavare av ett godkännande för försäljning finns att tillgå. ►**M4** Ett kodat värde från värdeset vaccine-mah-manf.json. Eller ett kodat värde som avser en klinisk prövning och som följer den regel som fastställs i avsnitt 4 i bilaga II. ◄ Detta värdeset distribueras från EUDCC-nätslussen. Exakt 1 (ett) icke-tomt fält ska tillhandahållas. Exempel: ”ma”: ”ORG-100030215” (Biontech Manufacturing GmbH)
v/dn	Nummer i en serie doser	Ordningsnummer (positivt heltal) för den dos som gavs genom denna specifika vaccinationshändelse. 1 för den första dosen, 2 för den andra dosen etc. Mer specifika regler finns i avsnitt 5 i bilaga II. Exakt 1 (ett) icke-tomt fält ska tillhandahållas. Exempel: ”dn”: ”1” (första dosen) ”dn”: ”2” (andra dosen) ”dn”: ”3” (tredje dosen)
v/sd	Totalt antal doser i serien	Totalt antal doser (positivt heltal) i vaccinationsserien. Mer specifika regler finns i avsnitt 5 i bilaga II. Exakt 1 (ett) icke-tomt fält ska tillhandahållas. Exempel: ”sd”: ”1” (vid en primär vaccinationsserie med 1-dosvaccin) ”sd”: ”2” (vid en primär vaccinationsserie med 2-dosvaccin eller vid en ytterligare dos efter en primär vaccinationsserie med 1-dosvaccin) ”sd”: ”3” (t.ex. vid ytterligare doser efter en primär vaccinationsserie med 2-dosvaccin)

▼M1

Fältets id	Fältets namn	Anvisningar
v/dt	Vaccinationsdatum	Det datum då den beskrivna dosen gavs, i formatet ÅÅÅÅ-MM-DD (fullständigt datum men ej tid). Andra format stöds inte. Exakt 1 (ett) icke-tomt fält ska tillhandahållas. Exempel: ”dt”: ”2021-03-28”
v/co	Medlemsstat eller tredjeland där vaccinet administrerades	Land uttryckt som en ISO3166-tvåbokstavskod (REKOMMENDERAS) eller en hänvisning till en internationell organisation som ansvarat för vaccinationshändelsen (såsom UNHCR eller WHO). Ett kodat värde från värdeset country-2-codes.json. Detta värdeset distribueras från EUDCC-nätslussen. Exakt 1 (ett) fält ska tillhandahållas. Exempel: ”co”: ”CZ” ”co”: ”UNHCR”
v/is	Utfärdare av intyget	Namn på den organisation som utfärdat intyget. Identifierare tillåts som del av namnet, men det rekommenderas att identifierare inte används separat utan namnet som text. Högst 80 UTF-8-tecken. Exakt 1 (ett) icke-tomt fält ska tillhandahållas. Exempel: ”is”: ”Republiken Tjeckiens hälsoministerium” ”is”: ”Vaccinationscentrum söder distrikt 3”
v/ci	Unik identifierare för intyget	Unik identifierare för intyget (UVCI) i enlighet med https://ec.europa.eu/health/sites/default/files/ehealth/docs/vaccination-proof_interoperability-guidelines_en.pdf. Inkludering av checksumman är frivillig. Prefixet ”URN:UVCI:” får läggas till. Exakt 1 (ett) icke-tomt fält ska tillhandahållas. Exempel: ”ci”: ”URN:UVCI:01:NL:187/37512422923” ”ci”: ”URN:UVCI:01:AT:10807843F94AEE0EE5093FBC254BD813#B”

4.2 *Testintyg*

Testgruppen ska, i förekommande fall, innehålla exakt 1 (en) post som exakt beskriver 1 (ett) testresultat.

Fältets id	Fältets namn	Anvisningar
t/tg	Sjukdom eller smittämne Covid-19 (SARS-CoV-2 eller en av dess varianter)	Ett kodat värde från värdeset disease-agent-targeted.json. Detta värdeset har den enda posten 840539006, som är koden för covid-19 från SNOMED CT (GPS). Exakt 1 (ett) icke-tomt fält ska tillhandahållas. Exempel: ”tg”: ”840539006”
t/tt	Typ av test	Den typ av test som använts, baserat på det material som testet omfattar. Ett kodat värde från värdeset test-type.json (baserat på LOINC). Värden utanför detta värdeset tillåts inte. Exakt 1 (ett) icke-tomt fält ska tillhandahållas. Exempel: ”tt”: ”LP6464-4” (nukleinsyraamplifiering med probpåvisande) ”tt”: ”LP217198-3” (Snabbimmunanalys)

▼M1

Fältets id	Fältets namn	Anvisningar
t/nm	Testnamn (endast nukleinsyraamplifieringstester)	Namnet på det nukleinsyraamplifieringstest (NAAT) som använts. Namnet bör innefatta namnet på tillverkaren av testet och testets varubeteckning, separerat med komma. För NAAT: fältet är frivilligt. ►M4 För antigentest: fältet ska inte användas, eftersom namnet på testet tillhandahålls indirekt genom testutrustningens identifierare (t/ma). ◄ När fältet tillhandahålls får det inte vara tomt. Exempel: ”nm”: ”ELITechGroup, SARS-CoV-2 ELITe MGB® Kit”
▼M4 **t/ma**	Testutrustningens identifierare (endast för antigentester)	Identifierare för utrustning för antigentest från JRC:s databas. Värdeset (gemensam förteckning från HSC). — Alla antigentester i den gemensamma förteckningen från HSC (läsbart för människor). — https://covid-19-diagnostics.jrc.ec.europa.eu/devices/hsc-common-recognition-rat (maskinläsbart, värden i fältet id_device som finns med i förteckningen utgör detta värdeset). I EU- och EES-länder ska utfärdaren endast utfärda intyg för tester som tillhör det värdeset som för närvarande är giltigt. Detta värdeset ska uppdateras var 24:e timme. Värden utanför detta värdeset får användas i intyg som utfärdas av tredjeländer, men identifierarna ska fortfarande vara från JRC:s databas. Användning av andra identifierare, såsom de som tillhandahålls av testtillverkarna, är inte tillåten. Verifierarna ska upptäcka värden som inte tillhör detta uppdaterade värdeset och visa intyg med sådana värden som ogiltiga. Om en identifierare avlägsnas från ett värdeset får de intyg där denna identifierare ingår godtas i högst 72 timmar från tidpunkten för avlägsnandet. Detta värdeset distribueras från EUDCC-nätslussen. För antigentest: Exakt 1 (ett) icke-tomt fält ska tillhandahållas. För NAAT: Fältet ska inte användas, även om NAA-testidentifieraren finns tillgänglig i JRC-databasen. Exempel: ”ma”: ”344”(SD BIOSENSOR Inc, STANDARD F COVID-19 Ag FIA)
▼M1 **t/sc**	Datum och tid för provtagningen	Datum och tid då provtagningen skedde. Tiden ska innefatta information om tidszonen. Värdet ska inte avse den tidpunkt då testresultatet producerades. Exakt 1 (ett) icke-tomt fält ska tillhandahållas. Ett av följande ISO 8601-format ska användas. Andra alternativ stöds inte. YYYY-MM-DDThh:mm:ssZ YYYY-MM-DDThh:mm:ss[+-]hh

▼**M1**

Fältets id	Fältets namn	Anvisningar
		YYYY-MM-DDThh:mm:ss[+-]hhmm YYYY-MM-DDThh:mm:ss[+-]hh:mm Exempel: ”sc”: ”2021-08-20T10:03:12Z” (UTC-tid) ”sc”: ”2021-08-20T12:03:12+02” (CEST-tid) ”sc”: ”2021-08-20T12:03:12+0200” (CEST-tid) ”sc”: ”2021-08-20T12:03:12+02:00” (CEST-tid)
t/tr	Testresultat	Testresultatet Ett kodat värde från värdeset test-result.json (baserat på SNOMED CT, GPS). Exakt 1 (ett) icke-tomt fält ska tillhandahållas. Exempel: ”tr”: ”260415000” (Ej påvisat)
t/tc	Provtagningsstation	Namn på den aktör som utförde testet. Identifierare tillåts som del av namnet, men det rekommenderas att identifierare inte används separat utan namnet som text. Högst 80 UTF-8-tecken. Eventuella extra tecken bör trunkeras. Namnet är inte utformat för automatiserad kontroll. För NAAT-tester: Exakt 1 (ett) icke-tomt fält ska tillhandahållas. ►**M4** För antigentest: fältet är frivilligt. Får inte vara tomt om det tillhandahålls. ◄ Exempel: ”tc”: ”Test centre west region 245”
t/co	Medlemsstat eller tredjeland där testningen utfördes	Land uttryckt som en ISO3166-tvåbokstavskod (REKOMMENDERAS) eller en hänvisning till en internationell organisation som ansvarat för utförandet av testningen (såsom UNHCR eller WHO). Ett kodat värde från värdeset country-2-codes.json. Detta värdeset distribueras från EUDCC-nätslussen. Exakt 1 (ett) fält ska tillhandahållas. Exempel: ”co”: ”CZ” ”co”: ”UNHCR”
t/is	Utfärdare av intyget	Namn på den organisation som utfärdat intyget. Identifierare tillåts som del av namnet, men det rekommenderas att identifierare inte används separat utan namnet som text. Högst 80 UTF-8-tecken. Exakt 1 (ett) icke-tomt fält ska tillhandahållas. Exempel: ”is”: ”Republiken Tjeckiens hälsoministerium” ”is”: ”Nordvästra regionens hälsomyndighet”

▼M1

Fältets id	Fältets namn	Anvisningar
t/ci	Unik identifierare för intyget	Unik identifierare för intyget (UVCI) i enlighet med vaccination-proof_interoperability-guidelines_en.pdf (europa.eu). Inkludering av checksumman är frivillig. Prefixet ”URN:UVCI:” får läggas till. Exakt 1 (ett) icke-tomt fält ska tillhandahållas. Exempel: ”ci”: ”URN:UVCI:01:NL:187/37512422923” ”ci”: ”URN:UVCI:01:AT:10807843F94AEE0EE5093FBC254BD813#B”

4.3 *Intyg om tillfrisknande*

Tillfrisknandegruppen ska, i förekommande fall, innehålla exakt 1 (en) post som exakt beskriver en utsaga om tillfrisknande. Alla element av tillfrisknandegruppen är obligatoriska, tomma värden stöds inte.

Fältets id	Fältets namn	Anvisningar
r/tg	Sjukdom eller smittämne som innehavaren har tillfrisknat från: Covid-19 (SARS-CoV-2 eller en av dess varianter)	Ett kodat värde från värdeset disease-agent-targeted.json. Detta värdeset har den enda posten 840539006, som är koden för covid-19 från SNOMED CT (GPS). Exakt 1 (ett) icke-tomt fält ska tillhandahållas. Exempel: ”tg”: ”840539006”
r/fr	Datum för innehavarens första positiva ►M4 ——— ◄-testresultat	Det datum då provtagningen gjordes för det ►M4 ——— ◄-testresultat som gav ett positivt resultat, i formatet ÅÅÅÅ-MM-DD (fullständigt datum utan tid). Andra format stöds inte. Exakt 1 (ett) icke-tomt fält ska tillhandahållas. Exempel: ”fr”: ”2021-05-18”
r/co	Medlemsstat eller tredjeland där testningen utfördes	Land uttryckt som en ISO3166-tvåbokstavskod (REKOMMENDERAS) eller en hänvisning till en internationell organisation som ansvarat för utförandet av testningen (såsom UNHCR eller WHO). Ett kodat värde från värdeset country-2-codes.json. Detta värdeset distribueras från EUDCC-nätslussen. Exakt 1 (ett) fält ska tillhandahållas. Exempel: ”co”: ”CZ” ”co”: ”UNHCR”
r/is	Utfärdare av intyget	Namn på den organisation som utfärdat intyget. Identifierare tillåts som del av namnet, men det rekommenderas att identifierare inte används separat utan namnet som text. Högst 80 UTF-8-tecken. Exakt 1 (ett) icke-tomt fält ska tillhandahållas. Exempel: ”is”: ”Republiken Tjeckiens hälsoministerium” ”is”: ”Centrala universitetssjukhuset”

▼**M1**

Fältets id	Fältets namn	Anvisningar
r/df	Intyget giltigt från och med	Det datum från och med vilket intyget är giltigt. Detta datum får inte föregå det datum som beräknas som r/fr + 11 days. Datumet ska tillhandahållas i formatet ÅÅÅÅ-MM-DD (fullständigt datum utan tiden). Andra format stöds inte. Exakt 1 (ett) icke-tomt fält ska tillhandahållas. Exempel: ”df”: ”2021-05-29”
r/du	Intyget giltigt till och med	Det sista datum då intyget anses giltigt, fastställt av utfärdaren av intyget. Detta datum får inte vara senare än det datum som beräknas som r/fr + 180 days. Datumet ska tillhandahållas i formatet ÅÅÅÅ-MM-DD (fullständigt datum utan tiden). Andra format stöds inte. Exakt 1 (ett) icke-tomt fält ska tillhandahållas. Exempel: ”du”: ”2021-11-14”
r/ci	Unik identifierare för intyget	Unik identifierare för intyget (UVCI) i enlighet med vaccination-proof_interoperability-guidelines_en.pdf (europa.eu). Inkludering av checksumman är frivillig. Prefixet ”URN:UVCI:” får läggas till. Exakt 1 (ett) icke-tomt fält ska tillhandahållas. Exempel: ”ci”: ”URN:UVCI:01:NL:187/37512422923” ”ci”: ”URN:UVCI:01:AT:10807843F94AEE0EE5093FBC254BD813#B”

▼M3

BILAGA VI

MEDLEMSSTATERNAS ANSVAR SOM GEMENSAMT PERSONUPPGIFTSANSVARIGA FÖR NÄTSLUSSEN FÖR EU:S DIGITALA COVIDINTYG AVSEENDE UTBYTE AV FÖRTECKNINGAR ÖVER ÅTERKALLANDEN AV EU:S DIGITALA COVIDINTYG

AVSNITT 1

Underavsnitt 1

Ansvarsfördelning

(1) De gemensamt personuppgiftsansvariga ska behandla personuppgifter via tillitsramverkets nätsluss i enlighet med de tekniska specifikationerna i bilaga I.

(2) Medlemsstaternas utfärdande myndigheter förblir den enda personuppgiftsansvariga för insamlingen, användningen, utlämnandet och all annan behandling av uppgifter utanför nätslussen, inbegripet förfarandet som leder till återkallande av ett intyg.

(3) Varje personuppgiftsansvarig ska ansvara för behandlingen av personuppgifter i tillitsramverkets nätsluss i enlighet med artiklarna 5, 24 och 26 i den allmänna dataskyddsförordningen.

(4) Varje personuppgiftsansvarig ska inrätta en kontaktpunkt med en funktionsbrevlåda för kommunikationen mellan de gemensamt personuppgiftsansvariga och mellan de gemensamt personuppgiftsansvariga och personuppgiftsbiträdet.

(5) En arbetsgrupp som inrättas av den kommitté som avses i artikel 14 i förordning (EU) 2021/953 ska ha i uppdrag att fatta beslut i alla frågor som uppstår i samband med utbytet av förteckningar över återkallade intyg och det gemensamma personuppgiftsansvaret för den tillhörande behandlingen av personuppgifter samt för att underlätta samordnade instruktioner till kommissionen i dess egenskap av personuppgiftsbiträde. Beslutsprocessen för de gemensamt personuppgiftsansvariga styrs av arbetsgruppen och den arbetsordning som den ska anta. Grundregeln är att om någon av de gemensamt personuppgiftsansvariga inte deltar i ett arbetsgruppsmöte som har meddelats skriftligen minst sju (7) dagar innan det sammankallas, så innebär detta ett underförstått godkännande av resultatet av detta möte. Vem som helst av de gemensamt personuppgiftsansvariga kan sammankalla ett möte i arbetsgruppen.

(6) Instruktioner till personuppgiftsbiträdet ska skickas via någon av de gemensamt personuppgiftsansvarigas kontaktpunkter, i samförstånd med övriga gemensamt personuppgiftsansvariga och i enlighet med den beslutsprocess för arbetsgruppen som beskrivs i punkt 5 ovan. Den gemensamt personuppgiftsansvariga som tillhandahåller instruktionen bör lämna dem skriftligen till personuppgiftsbiträdet och informera alla andra gemensamt personuppgiftsansvariga om detta. Om den aktuella frågan är så tidskritisk att det inte är möjligt att behandla den vid ett möte i den arbetsgrupp som avses i punkt 5 ovan kan en instruktion ändå ges, men den kan upphävas av arbetsgruppen. Denna instruktion bör ges skriftligen, och alla andra gemensamt personuppgiftsansvariga bör informeras om detta när instruktionen ges.

(7) Den arbetsgrupp som inrättats enligt punkt 5 påverkar inte någon av de gemensamt personuppgiftsansvarigas enskilda befogenhet att informera sin behöriga tillsynsmyndighet i enlighet med artiklarna 33 och 24 i den allmänna dataskyddsförordningen. En sådan anmälan kräver inte samtycke från någon av de andra gemensamt personuppgiftsansvariga.

▼M3

(8) Inom ramen för tillitsramverkets nätsluss får endast personer som bemyndigats av de utsedda nationella myndigheterna eller officiella organen ha åtkomst till de personuppgifter som utbyts.

(9) Varje utfärdande myndighet ska föra ett register över all behandling som utförts under dess ansvar. Gemensamt personuppgiftsansvar får anges i registret.

Underavsnitt 2

Ansvarsområden och roller vid hantering av begäranden från och information till registrerade

(1) Varje personuppgiftsansvarig ska i sin egenskap av utfärdande myndighet förse fysiska personer vars intyg den har återkallat (*de registrerade*) med information om återkallandet och behandlingen av deras personuppgifter i nätslussen för EU:s digitala covidintyg avseende utbytet av förteckningar över återkallande, i enlighet med artikel 14 i den allmänna dataskyddsförordningen, såvida detta inte visar sig vara omöjligt eller skulle innebära en oproportionell ansträngning.

(2) Varje personuppgiftsansvarig ska fungera som kontaktpunkt för fysiska personer vars intyg den har återkallat och ska behandla begäranden från de registrerade eller deras företrädare när de utövar sina rättigheter i enlighet med den allmänna dataskyddsförordningen. Om en gemensamt personuppgiftsansvarig tar emot en begäran från en registrerad som avser ett intyg som utfärdats av en annan gemensamt personuppgiftsansvarig ska den informera den registrerade om denna gemensamt personuppgiftsansvarigas identitet och kontaktuppgifter. Om en annan gemensamt personuppgiftsansvarig begär bistånd med hanteringen av registrerades förfrågningar ska de gemensamt personuppgiftsansvariga bistå varandra och svara varandra utan onödigt dröjsmål, senast inom en månad från mottagandet av en begäran om bistånd. Om en begäran avser uppgifter som lämnats in av ett tredjeland ska den personuppgiftsansvariga som tar emot begäran behandla den och informera den registrerade om identitet och kontaktuppgifter för den utfärdande myndigheten i tredjelandet.

(3) Varje personuppgiftsansvarig ska ge de registrerade tillgång till innehållet i denna bilaga, inbegripet de arrangemang som fastställs i punkterna 1 och 2.

AVSNITT 2

Hantering av säkerhetsincidenter, inbegripet personuppgiftsincidenter

(1) De gemensamt personuppgiftsansvariga ska bistå varandra i identifiering och hantering av alla säkerhetsincidenter, inbegripet personuppgiftsincidenter, som har koppling till behandlingen i nätslussen för EU:s digitala covidintyg.

(2) De gemensamt personuppgiftsansvariga ska särskilt underrätta varandra om följande:

a) Varje potentiell eller faktisk risk för tillgängligheten till samt sekretessen och/eller integriteten hos de personuppgifter som behandlas i tillitsramverkets nätsluss.

b) Varje personuppgiftsincident, de sannolika konsekvenserna av personuppgiftsincidenten och bedömningen av risken för fysiska personers rättigheter och friheter samt alla åtgärder som vidtagits för att åtgärda personuppgiftsincidenten och minska risken för fysiska personers rättigheter och friheter.

▼M3

c) Varje överträdelse av tekniska och/eller organisatoriska skyddsåtgärder avseende behandlingen i tillitsramverkets nätsluss.

(3) De gemensamt personuppgiftsansvariga ska anmäla alla personuppgiftsincidenter som är relaterade till behandlingen i tillitsramverkets nätsluss till kommissionen, till behöriga tillsynsmyndigheter och, när så krävs, till registrerade i enlighet med artiklarna 33 och 34 i den allmänna dataskyddsförordningen eller efter meddelande från kommissionen.

(4) Varje utfärdande myndighet ska genomföra lämpliga tekniska och organisatoriska åtgärder för att

a) säkerställa och skydda tillgängligheten, integriteten och sekretessen hos de personuppgifter som behandlas gemensamt,

b) skydda mot obehörig eller olaglig behandling, förlust, användning, utlämnande eller förvärv av eller åtkomst till personuppgifter som den innehar,

c) säkerställa att tillgången till personuppgifterna inte utlämnas till eller tillåts för någon annan än mottagaren eller personuppgiftsbiträdet.

AVSNITT 3

Konsekvensbedömning avseende dataskydd

(1) Om en personuppgiftsansvarig behöver information från en annan personuppgiftsansvarig för att kunna uppfylla sina skyldigheter enligt artiklarna 35 och 36 i förordning (EU) 2016/679 ska en särskild begäran skickas till den funktionsbrevlåda som avses i avsnitt 1 underavsnitt 1.4. Den andra personuppgiftsansvariga ska göra sitt yttersta för att tillhandahålla sådan information.

▼M3

BILAGA VII

KOMMISSIONENS ANSVAR SOM PERSONUPPGIFTSBITRÄDE FÖR NÄTSLUSSEN FÖR EU:S DIGITALA COVIDINTYG FÖR ATT STÖDJA UTBYTET AV FÖRTECKNINGAR ÖVER ÅTERKALLANDEN

Kommissionen ska göra följande:

(1) För medlemsstaternas räkning inrätta och säkerställa en säker och tillförlitlig kommunikationsinfrastruktur som stöder utbytet av de förteckningar över återkallanden som lämnas via nätslussen för EU:s digitala covidintyg.

(2) Kommissionen får, för att fullgöra sina skyldigheter som personuppgiftsbiträde för tillitsramverkets nätsluss gentemot medlemsstaterna, anlita tredje parter som underleverantörer. Kommissionen ska informera de gemensamt personuppgiftsansvariga om alla planerade ändringar som rör tillägg av nya eller utbyte av befintliga underleverantörer, och därigenom ge de personuppgiftsansvariga möjlighet att gemensamt invända mot sådana ändringar. Kommissionen ska säkerställa att dataskyddsskyldigheterna i detta beslut även tillämpas på dessa underleverantörer.

(3) Endast behandla personuppgifter på grundval av dokumenterade instruktioner från de personuppgiftsansvariga, såvida inte behandlingen krävs enligt unionsrätten eller en medlemsstats nationella rätt. I sådant fall ska kommissionen informera de gemensamt personuppgiftsansvariga om det rättsliga kravet innan någon behandling av uppgifterna sker, såvida det inte är förbjudet att lämna sådana uppgifter med hänvisning till ett viktigt allmänintresse enligt denna rätt.

Kommissionens behandling omfattar följande:

a) Autentisering av nationella backendservrar, baserat på certifikat för nationella backendservrar.

b) Mottagande av de uppgifter som avses i artikel 5a.3 i beslutet och som laddas upp av nationella backendservrar genom tillhandahållande av ett programmeringsgränssnitt som möjliggör att nationella backendservrar kan ladda upp de relevanta uppgifterna.

c) Lagring av uppgifter i nätslussen för EU:s digitala covidintyg.

d) Tillgängliggörande av uppgifterna för nedladdning av nationella backendservrar.

e) Radering av uppgifterna på deras utgångsdatum eller efter instruktion av den personuppgiftsansvariga som lämnat in dem.

f) När tillhandahållandet av tjänsten har avslutats, radering av alla kvarvarande uppgifter såvida inte lagring av personuppgifterna krävs enligt unionsrätten eller medlemsstaternas nationella rätt.

(4) Vidta alla de bästa tillgängliga organisatoriska, fysiska och logiska säkerhetsåtgärder som krävs för att upprätthålla nätslussen för EU:s digitala covidintyg. Kommissionen ska i detta syfte

a) utse en enhet som ansvarar för säkerhetsförvaltningen av nätslussen för EU:s digitala covidintyg, informera de gemensamt personuppgiftsansvariga om enhetens kontaktuppgifter och säkerställa att den kan hantera säkerhetshot,

▼M3

b) ta ansvaret för säkerheten hos nätslussen för EU:s digitala covidintyg, bland annat genom att regelbundet utföra tester, utvärderingar och bedömningar av säkerhetsåtgärderna,

c) säkerställa att alla personer som beviljas åtkomst till nätslussen för EU:s digitala covidintyg omfattas av avtalsenlig, yrkesmässig eller lagstadgad tystnadsplikt.

(5) Vidta alla nödvändiga säkerhetsåtgärder så att de nationella backendservrarna fungerar smidigt. Kommissionen ska därför införa särskilda förfaranden för anslutning från backendservrarna till nätslussen för EU:s digitala covidintyg. Detta omfattar följande:

a) Ett riskbedömningsförfarande för att identifiera och utvärdera potentiella hot mot systemet.

b) Ett revisions- och granskningsförfarande för att

i. kontrollera sambandet mellan de genomförda säkerhetsåtgärderna och den tillämpliga säkerhetspolicyn,

ii. regelbundet kontrollera systemfilernas, säkerhetsparametrarnas och de beviljade tillståndens integritet,

iii. övervaka att säkerhetsöverträdelser och intrång upptäcks,

iv. genomföra ändringar för att minska befintliga säkerhetsbrister,

v. fastställa villkoren för att tillåta, även på begäran av personuppgiftsansvariga, och bidra till oberoende revisioner, inbegripet inspektioner, och översyner av säkerhetsåtgärder, på villkor som följer protokoll nr 7 till EUF-fördraget om Europeiska unionens immunitet och privilegier.

c) Ändring av kontrollförfarandet för att dokumentera och mäta effekten av en ändring innan den genomförs och hålla de gemensamt personuppgiftsansvariga informerade om samtliga ändringar som kan påverka kommunikationen med och/eller säkerheten i deras infrastrukturer.

d) Inrättande av ett underhålls- och reparationsförfarande för att fastställa de regler och villkor som ska följas vid underhåll och/eller reparation av utrustning.

e) Inrättande av ett förfarande för säkerhetsincidenter för att fastställa ett rapporterings- och eskaleringssystem, information utan dröjsmål till personuppgiftsansvariga som berörs, så att de vid behov även kan informera de nationella dataskyddsmyndigheterna om personuppgiftsincidenter, och fastställande av ett disciplinärt förfarande för att åtgärda dessa.

(6) Vidta bästa tillgängliga fysiska och/eller logiska säkerhetsåtgärder för de anläggningar där utrustningen för nätslussen för EU:s digitala covidintyg finns och för kontroller av åtkomst till logiska data och säkert tillträde. Kommissionen ska i detta syfte göra följande:

a) Införa fysiska säkerhetsåtgärder för att upprätta tydliga säkerhetsperimetrar och möjliggöra att överträdelser upptäcks.

▼M3

b) Kontrollera tillträdet till anläggningar och upprätthålla ett besöksregister för spårning.

c) Säkerställa att externa personer som beviljas tillträde till lokaler åtföljs av vederbörligen bemyndigad personal.

d) Säkerställa att utrustning inte kan läggas till, ersättas eller avlägsnas utan förhandstillstånd från utsedda ansvariga organ.

e) Kontrollera ömsesidig åtkomst mellan de nationella backendservrarna och tillitsramverkets nätsluss.

f) Säkerställa att personer som får åtkomst till nätslussen för EU:s digitala covidintyg identifieras och autentiseras.

g) Se över de tillståndsrättigheter som gäller åtkomst till nätslussen för EU:s digitala covidintyg vid säkerhetsöverträdelser som påverkar denna infrastruktur.

h) Bevara integriteten hos den information som överförs via nätslussen för EU:s digitala covidintyg.

i) Vidta tekniska och organisatoriska säkerhetsåtgärder för att förhindra obehörig åtkomst till personuppgifter.

j) Vid behov vidta åtgärder för att blockera obehörig åtkomst till nätslussen för EU:s digitala covidintyg från de utfärdande myndigheternas domän (dvs. blockera en plats/IP-adress).

(7) Vidta åtgärder för att skydda sin domän, inklusive genom frånkoppling, vid betydande avvikelser från principerna och koncepten för kvalitet eller säkerhet.

(8) Upprätthålla en riskhanteringsplan för sitt ansvarsområde.

(9) Övervaka – i realtid – prestandan för alla tjänstekomponenter i sina tjänster i tillitsramverkets nätsluss, ta fram regelbunden statistik och upprätthålla register.

(10) Ge stöd för alla tjänster i tillitsramverkets nätsluss dygnet runt och året runt på engelska via telefon, e-post eller webbportalen och godta samtal från godkända personer som ringer upp: samordnarna för nätslussen för EU:s digitala covidintyg och deras respektive hjälpcentraler, projektansvariga och utsedda personer från kommissionen.

(11) Bistå de gemensamt personuppgiftsansvariga med lämpliga tekniska och organisatoriska åtgärder, när detta är möjligt i enlighet med artikel 12 i förordning (EU) 2018/1725, i syfte att fullgöra den personuppgiftsansvarigas skyldighet att besvara begäran om utövande av den registrerades rättigheter enligt kapitel III i den allmänna dataskyddsförordningen.

▼**M3**

(12) Stödja de gemensamt personuppgiftsansvariga genom att tillhandahålla information om nätslussen för EU:s digitala covidintyg i syfte att fullgöra skyldigheterna enligt artiklarna 32, 33, 34, 35 och 36 i den allmänna dataskyddsförordningen.

(13) Säkerställa att de uppgifter som behandlas i nätslussen för EU:s digitala covidintyg är oläsbara för personer som inte är behöriga att få tillgång till den.

(14) Vidta alla relevanta åtgärder för att förhindra att operatörerna av nätslussen för EU:s digitala covidintyg får obehörig tillgång till överförda uppgifter.

(15) Vidta åtgärder för att underlätta interoperabiliteten och kommunikationen mellan de utsedda personuppgiftsansvariga för nätslussen för EU:s digitala covidintyg.

(16) Föra ett register över behandling som utförts för de gemensamt personuppgiftsansvarigas räkning i enlighet med artikel 31.2 i förordning (EU) 2018/1725.