KOMISSION TÄYTÄNTÖÖNPANOPÄÄTÖS (EU) 2021/1073,

annettu 28 päivänä kesäkuuta 2021,

Euroopan parlamentin ja neuvoston asetuksella (EU) 2021/953 vahvistetun EU:n digitaalisen koronatodistuksen luottamuskehyksen täytäntöönpanoa koskevista teknisistä eritelmistä ja säännöistä

(ETA:n kannalta merkityksellinen teksti)

EUROOPAN KOMISSIO, joka

ottaa huomioon Euroopan unionin toiminnasta tehdyn sopimuksen,

ottaa huomioon kehyksestä covid-19-tautiin liittyvien yhteentoimivien rokotusta, testausta ja taudista parantumista koskevien todistusten (EU:n digitaalinen koronatodistus) myöntämiseksi, todentamiseksi ja hyväksymiseksi helpottamaan henkilöiden vapaata liikkuvuutta covid-19-pandemian aikana 14 päivänä kesäkuuta 2021 annetun Euroopan parlamentin ja neuvoston asetuksen (EU) 2021/953 ([1]) ja erityisesti sen 9 artiklan 1 ja 3 kohdan,

sekä katsoo seuraavaa:

(1) Asetuksessa (EU) 2021/953 vahvistetaan EU:n digitaalinen koronatodistus, jonka on tarkoitus toimia todisteena siitä, että henkilö on saanut covid-19-rokotteen tai negatiivisen testituloksen tai on toipunut taudista.

(2) Jotta EU:n digitaalinen koronatodistus saataisiin käyttöön kaikkialla unionissa, on tarpeen vahvistaa tekniset eritelmät ja säännöt, joiden avulla voidaan täyttää, turvallisesti myöntää ja todentaa digitaaliset koronatodistukset, varmistaa henkilötietojen tietoturva, määritellä yksilöllisen todistustunnuksen yhteinen rakenne ja antaa pätevä, suojattu ja yhteentoimiva viivakoodi. Tämä luottamuskehys luo myös edellytykset pyrkimykselle varmistaa yhteentoimivuus kansainvälisten standardien ja teknologisten järjestelmien kanssa, ja se voisi siten toimia mallina maailmanlaajuiselle yhteistyölle.

(3) Kyky lukea ja tulkita EU:n digitaalista koronatodistusta edellyttää yhteistä tietorakennetta ja yhteisymmärrystä hyötykuorman kunkin tietokentän tarkoitetusta merkityksestä ja mahdollisista arvoista. Tällaisen yhteentoimivuuden helpottamiseksi EU:n digitaalisen koronatodistuksen kehykselle on tarpeellista määritellä yhteinen koordinoitu tietorakenne. Tätä kehystä koskevat suuntaviivat on laatinut Euroopan parlamentin ja neuvoston direktiivin 2011/24/EU ([2]) nojalla perustettu sähköisten terveyspalvelujen verkosto. Nämä suuntaviivat olisi otettava huomioon laadittaessa teknisiä eritelmiä, joissa vahvistetaan EU:n digitaalisen koronatodistuksen muoto ja luottamuksen hallinta. Olisi määriteltävä tietorakenteen eritelmä ja koodausmekanismit sekä siirtokoodausmekanismi koneellisesti luettavassa optisessa muodossa (’QR’), joka voidaan näyttää mobiililaitteen kuvaruudulla tai tulostaa paperille.

(4) EU:n digitaalisen koronatodistuksen muotoa ja luottamuksen hallintaa koskevien teknisten eritelmien lisäksi olisi vahvistettava yleiset säännöt varmenteiden täyttämistä varten, jotta niitä voidaan käyttää EU:n digitaalisen koronatodistuksen sisällön koodattuina arvoina. Komission olisi säännöllisesti päivitettävä ja julkaistava arvojoukot, joilla nämä säännöt pannaan täytäntöön, hyödyntäen sähköisten terveyspalvelujen verkoston asiaa koskevaa työtä.

(5) Asetuksen (EU) 2021/953 mukaan EU:n digitaalisen koronatodistuksen muodostavat aidot todistukset olisi voitava tunnistaa yksilöivästi yksilöllisen todistustunnuksen avulla, kun otetaan huomioon, että kansalaisille voidaan asetuksen (EU) 2021/953 voimassaoloaikana myöntää useampi kuin yksi todistus. Yksilöllisen todistustunnuksen olisi koostuttava aakkosnumeerisesta jonosta, ja jäsenvaltioiden olisi varmistettava, ettei se sisällä mitään tietoja, jotka linkittävät sen muihin asiakirjoihin tai tunnisteisiin, kuten passin tai henkilökortin numeroihin, jotta estetään todistuksen haltijan tunnistaminen. Sen varmistamiseksi, että todistustunnus on yksilöllinen, olisi vahvistettava tekniset eritelmät ja säännöt sen yhteistä rakennetta varten.

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

([2]) Euroopan parlamentin ja neuvoston direktiivi 2011/24/EU, annettu 9 päivänä maaliskuuta 2011, potilaiden oikeuksien soveltamisesta rajatylittävässä terveydenhuollossa (EUVL L 88, 4.4.2011, s. 45).

(6) EU:n digitaalisen koronatodistuksen muodostavien todistusten turvallisuus, aitous, pätevyys ja eheys sekä se, että ne ovat unionin tietosuojalainsäädännön mukaisia, ovat keskeisen tärkeitä niiden hyväksymiselle kaikissa jäsenvaltioissa. Nämä tavoitteet saavutetaan luottamuskehyksellä, jossa vahvistetaan säännöt ja infrastruktuuri EU:n digitaalisten koronatodistusten luotettavaa ja suojattua myöntämistä ja todentamista varten. Luottamuskehyksen olisi perustuttava muun muassa julkisen avaimen infrastruktuuriin, jossa luottamusketju ulottuu jäsenvaltioiden terveysviranomaisista tai muista luotetuista viranomaisista EU:n digitaalisia koronatodistuksia myöntäviin yksittäisiin tahoihin. Sen vuoksi komissio on EU:n laajuisen yhteentoimivuusjärjestelmän varmistamiseksi perustanut keskusjärjestelmän – EU:n digitaalisen koronatodistuksen yhdyskäytävän, jäljempänä 'yhdyskäytävä' – johon todentamiseen käytettävät julkiset avaimet tallennetaan. Kun QR-koodivarmenne skannataan, digitaalinen allekirjoitus todennetaan käyttämällä asiaankuuluvaa julkista avainta, joka on aiemmin tallennettu kyseiseen keskusyhdyskäytävään. Digitaalisia allekirjoituksia voidaan käyttää tietojen eheyden ja aitouden varmistamiseen. Julkisen avaimen infrastruktuurit luovat luottamusta sitomalla julkiset avaimet varmenteiden myöntäjiin. Yhdyskäytävässä todentamiseen käytetään useita julkisen avaimen varmenteita. Jotta voidaan varmistaa julkisen avaimen aineiston suojattu vaihto jäsenvaltioiden välillä ja mahdollistaa laaja yhteentoimivuus, on tarpeen vahvistaa käytettävät julkisen avaimen varmenteet ja säätää, miten ne olisi tuotettava.

(7) Tämän päätöksen ansiosta asetuksen (EU) 2021/953 vaatimuksia voidaan soveltaa siten, että henkilötietojen käsittely rajoitetaan siihen, mikä on tarpeen EU:n digitaalisen koronatodistuksen käyttämiseksi. Päätös edistää myös lopullisten rekisterinpitäjien suorittamaa täytäntöönpanoa, jossa noudatetaan sisäänrakennettua tietosuojaa.

(8) Asetuksen (EU) 2021/953 mukaan todistusten myöntämisestä vastaavia viranomaisia tai muita nimettyjä elimiä pidetään Euroopan parlamentin ja neuvoston asetuksen (EU) 2016/679 ([3]) 4 artiklan 7 alakohdassa tarkoitettuina rekisterinpitäjinä, kun ne käsittelevät henkilötietoja myöntämisprosessin aikana. Riippuen siitä, miten jäsenvaltiot järjestävät myöntämismenettelyn, viranomaisia tai nimettyjä elimiä voi olla yksi tai useampi; niitä voivat olla esimerkiksi alueelliset terveydenhuoltoyksiköt. Toissijaisuusperiaatteen mukaisesti tämä on jäsenvaltioiden päätettävissä. Jäsenvaltioilla on siten parhaat edellytykset varmistaa, että jos viranomaisia tai muita nimettyjä elimiä on useita, niiden vastuualueet jaetaan selkeästi riippumatta siitä, ovatko ne erillisiä vai yhteisiä rekisterinpitäjiä (mukaan lukien alueelliset terveydenhuoltoyksiköt, jotka perustavat yhteisen potilasportaalin todistusten myöntämistä varten). Samoin silloin, kun todistuksia todentavat määrä- tai kauttakulkujäsenvaltion toimivaltaiset viranomaiset tai rajatylittävien henkilöliikennepalvelujen tarjoajat, jotka ovat kansallisen lainsäädännön nojalla velvollisia panemaan täytäntöön tiettyjä kansanterveystoimenpiteitä covid-19-pandemian aikana, näiden todentajien on noudatettava tietosuojasääntöjen mukaisia velvoitteitaan.

(9) Henkilötietoja ei käsitellä EU:n digitaalisen koronatodistuksen yhdyskäytävän kautta, koska yhdyskäytävä sisältää ainoastaan allekirjoittavien viranomaisten julkiset avaimet. Nämä avaimet liittyvät allekirjoittaviin viranomaisiin, eivätkä ne mahdollista varmenteen saaneen luonnollisen henkilön tunnistamista suoraan tai välillisesti. Komission ei siis pitäisi olla henkilötietojen rekisterinpitäjä eikä käsittelijä, kun se toimii yhdysväylän hallinnoijana.

(10) Euroopan tietosuojavaltuutettua on kuultu Euroopan parlamentin ja neuvoston asetuksen (EU) 2018/1725 ([4]) 42 artiklan 1 kohdan mukaisesti, ja hän antoi lausuntonsa 22 päivänä kesäkuuta 2021.

(11) Koska tekniset eritelmät ja säännöt ovat tarpeen asetuksen (EU) 2021/953 soveltamiseksi 1 päivästä heinäkuuta 2021, tämän päätöksen välitön soveltaminen on perusteltua.

(12) Koska EU:n digitaalinen koronatodistus on siten otettava käyttöön nopeasti, tämän päätöksen olisi tultava voimaan päivänä, jona se julkaistaan,

([3]) Euroopan parlamentin ja neuvoston asetus (EU) 2016/679, annettu 27 päivänä huhtikuuta 2016, luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta ja direktiivin 95/46/EY kumoamisesta (yleinen tietosuoja-asetus) (EUVL L 119, 4.5.2016, s. 1).

([4]) Euroopan parlamentin ja neuvoston asetus (EU) 2018/1725, annettu 23 päivänä lokakuuta 2018, luonnollisten henkilöiden suojelusta unionin toimielinten, elinten ja laitosten suorittamassa henkilötietojen käsittelyssä ja näiden tietojen vapaasta liikkuvuudesta sekä asetuksen (EY) N:o 45/2001 ja päätöksen N:o 1247/2002/EY kumoamisesta (EUVL L 295, 21.11.2018, s. 39).

ON HYVÄKSYNYT TÄMÄN PÄÄTÖKSEN:

1 artikla

EU:n digitaalisen koronatodistuksen tekniset eritelmät, joissa vahvistetaan yleinen tietorakenne, koodausmekanismit ja siirtokoodausmekanismi koneellisesti luettavassa optisessa muodossa, esitetään liitteessä I.

2 artikla

Asetuksen (EU) 2021/953 3 artiklan 1 kohdassa tarkoitettujen todistusten täyttämistä koskevat säännöt esitetään tämän päätöksen liitteessä II.

3 artikla

Yksilöllisen todistustunnuksen yhteistä rakennetta koskevat vaatimukset esitetään liitteessä III.

4 artikla

Hallinnointisäännöt, joita sovelletaan julkisen avaimen varmenteisiin luottamuskehyksen yhteentoimivuusnäkökohtia tukevan EU:n digitaalisen koronatodistuksen yhdyskäytävän yhteydessä, esitetään liitteessä IV.

Tämä päätös tulee voimaan sinä päivänä, jona se julkaistaan *Euroopan unionin virallisessa lehdessä*.

Tehty Brysselissä 28 päivänä kesäkuuta 2021.

Komission puolesta
Puheenjohtaja
Ursula VON DER LEYEN

LIITE I

MUOTO JA LUOTTAMUKSEN HALLINTA

Yleinen tietorakenne, koodausmekanismit ja siirtokoodausmekanismi koneellisesti luettavassa optisessa muodossa (jäljempänä 'QR')

1. Johdanto

Tässä liitteessä vahvistetut tekniset eritelmät sisältävät EU:n digitaalisen koronatodistuksen yleisen tietorakenteen ja koodausmekanismit. Niissä määritellään myös siirtokoodausmekanismi koneellisesti luettavassa optisessa muodossa ('QR'), joka voidaan näyttää mobiililaitteen kuvaruudulla tai tulostaa. Näissä eritelmissä kuvatut sähköisen terveystodistuksen säilömuodot ovat yleisiä, mutta tässä yhteydessä niitä käytetään digitaalisen koronatodistuksen esittämiseen.

2. Terminologia

Tässä liitteessä 'myöntäjillä' tarkoitetaan organisaatioita, jotka käyttävät näitä eritelmiä terveystodistusten myöntämiseen, ja 'todentajilla' organisaatioita, jotka hyväksyvät terveystodistukset todisteena terveydentilasta. 'Osallistujilla' tarkoitetaan myöntäjiä ja todentajia. Osallistujien on koordinoitava joitakin tässä liitteessä esitettyjä näkökohtia, kuten nimitilan hallinnointia ja salausavainten jakelua. Oletetaan, että nämä tehtävät suorittaa osapuoli, jota kutsutaan jäljempänä 'sihteeristöksi'.

3. Sähköisen terveystodistuksen säilömuoto

Sähköisen terveystodistuksen säilömuoto (Electronic Health Certificate Container Format, HCERT) on suunniteltu siten, että se tarjoaa yhtenäisen ja standardoidun välineen eri myöntäjien terveystodistuksille. Näiden eritelmien tavoitteena on yhdenmukaistaa kyseisten terveystodistusten esitystapaa, koodausta ja allekirjoittamista yhteentoimivuuden helpottamiseksi.

Kyky lukea ja tulkita minkä tahansa myöntäjän myöntämää digitaalista koronatodistusta edellyttää yhteistä tietorakennetta ja yhteisymmärrystä hyötykuorman kunkin tietokentän merkityksestä. Yhteentoimivuuden helpottamiseksi yhteinen koordinoitu tietorakenne määritellään käyttämällä JSON-muotoa, joka muodostaa digitaalisen koronatodistuksen kehyksen.

3.1 *Hyötykuorman rakenne*

Hyötykuorma on jäsennelty ja koodattu tiiviiksi binääriobjektiesitykseksi (Concise Binary Object Representation, CBOR), jossa käytetään COSE-muotoista (CBOR Object Signing and Encryption) digitaalista allekirjoitusta. Tämä tunnetaan yleisesti nimellä "CBOR Web Token" (CWT), ja se määritellään standardissa RFC 8392 ([1]). Seuraavissa kohdissa määritelty hyötykuorma siirretään hcert-väitteessä.

Todentajan on voitava todentaa hyötykuorman tietojen eheys ja aitous. Tämän mekanismin tarjoamiseksi myöntäjän on allekirjoitettava CWT käyttäen COSE-spesifikaatiossa (RFC 8152 ([2])) määriteltyä epäsymmetristä sähköistä allekirjoitusjärjestelmää.

3.2 *CWT-väitteet*

3.2.1 Yhteenveto CWT-rakenteesta

Suojattu otsikko

— Allekirjoitusalgoritmi (alg, tunniste 1)

— Avaimen tunniste (kid, tunniste 4)

Hyötykuorma

— Myöntäjä (iss, väiteavain 1, valinnainen, myöntäjän ISO 3166–1 alpha-2-koodi)

— Myönnetty (iat, väiteavain 6)

— Voimassaolon päättymisajankohta (exp, väiteavain 4)

— Terveystodistus (hcert, väiteavain -260)

— EU:n digitaalinen koronatodistus v1 (eu_DCC_v1, väiteavain 1)

Allekirjoitus

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

3.2.2 Allekirjoitusalgoritmi (Signature Algorithm)

Allekirjoitusalgoritmin (alg) parametri osoittaa, mitä algoritmia käytetään allekirjoituksen luomiseen. Sen on täytettävä tai ylitettävä nykyisten SOG-IS-suuntaviivojen vaatimukset, jotka esitetään tiivistetysti seuraavissa kohdissa.

Määritellään yksi ensisijainen ja yksi toissijainen algoritmi. Toissijaista algoritmia olisi käytettävä vain, jos ensisijainen algoritmi ei ole hyväksyttävissä myöntäjälle asetettujen sääntöjen ja määräysten mukaisesti.

Järjestelmän turvallisuuden varmistamiseksi kaikkiin toteutuksiin on sisällyttävä toissijainen algoritmi. Tästä syystä on otettava käyttöön sekä ensisijainen että toissijainen algoritmi.

Ensisijaisten ja toissijaisten algoritmien SOG-IS-tasot ovat seuraavat:

— Ensisijainen algoritmi: Ensisijainen algoritmi on ECDSA (Elliptic Curve Digital Signature Algorithm), sellaisena kuin se on määritelty standardin (ISO/IEC 14888–3:2006) 2.3 kohdassa, käyttäen standardin (FIPS PUB 186–4) lisäyksessä D (D.1.2.3) määriteltyjä P-256-parametreja yhdessä standardin (ISO/IEC 10118–3:2004) funktiossa 4 määritellyn SHA-256-hajautusalgoritmin kanssa.

Tämä vastaa COSE-algoritmin parametria ES256.

— Toissijainen algoritmi: Toissijainen algoritmi on RSASSA-PSS, sellaisena kuin se on määritelty standardissa (RFC 8230 ([3])) 2048-bitin moduluksella, yhdessä standardin (ISO/IEC 10118–3:2004) funktiossa 4 määritellyn SHA-256-hajautusalgoritmin kanssa.

Tämä vastaa COSE-algoritmin parametria PS256.

3.2.3 Avaimen tunniste (Key Identifier)

Avaimen tunnistetta (kid) koskeva väite näyttää asiakirjan allekirjoittajan varmenteen (Document Signer Certificate, DSC). Se sisältää julkisen avaimen, jota todentajan on käytettävä digitaalisen allekirjoituksen oikeellisuuden tarkistamiseen. Julkisen avaimen varmenteiden hallinnointi, mukaan lukien DSC-varmenteita koskevat vaatimukset, kuvataan liitteessä IV.

Todentajat käyttävät avaimen tunnistetta (kid) koskevaa väitettä oikean julkisen avaimen valitsemiseen myöntäjään liittyvästä avainluettelosta, joka ilmoitetaan myöntäjää (Issuer, iss) koskevassa väitteessä. Myöntäjä voi käyttää samanaikaisesti useita avaimia hallinnollisista syistä ja uusiessaan avaimia. Avaimen tunniste ei ole turvallisuuden kannalta kriittinen kenttä. Tästä syystä se voidaan tarvittaessa sijoittaa suojaamattomaan otsikkoon. Todentajien on hyväksyttävä molemmat vaihtoehdot. Jos molemmat vaihtoehdot ovat mahdollisia, avaimen tunniste on sijoitettava suojattuun otsikkoon.

Koska tunnistetta on lyhennetty (kokorajoituksiin liittyvistä syistä), on olemassa pieni mutta nollaa suurempi mahdollisuus, että todentajan hyväksymä yleinen DSC-luettelo voi sisältää DSC-varmenteita, joissa on sama kid. Tästä syystä todentajan on tarkistettava kaikki DSC-varmenteet, joissa on kyseinen kid.

3.2.4 Myöntäjä (Issuer)

Myöntäjää (iss) koskeva väite on merkkijonoarvo, jossa voi valinnaisesti olla terveystodistuksen myöntävän tahon ISO 3166–1 alpha-2 -maakoodi. Todentaja voi käyttää tätä väitettä määrittääkseen, mitä DSC-varmenteita todentamisessa käytetään. Tämän väitteen yksilöimiseen käytetään väiteavainta 1.

3.2.5 Voimassaolon päättymisajankohta (Expiration Time)

Voimassaolon päättymisajankohtaa (exp) koskevassa väitteessä on oltava NumericDate-kokonaislukumuodossa oleva aikaleima (siten kuin se on määritelty standardin RFC 8392 ([4]) 2 kohdassa), josta käy ilmi, kuinka kauan kyseisen hyötykuorman allekirjoituksen on katsottava olevan voimassa, minkä jälkeen todentajan on hylättävä hyötykuorma vanhentuneena. Voimassaolon päättymistä koskevan parametrin tarkoituksena on rajoittaa terveystodistuksen voimassaoloaikaa. Tämän väitteen yksilöimiseen käytetään väiteavainta 4.

Voimassaolon päättymisajankohta ei saa ylittää DSC-varmenteen voimassaoloaikaa.

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

3.2.6 Myönnetty (Issued At)

Myönnetty (iat) -väitteessä on oltava NumericDate-kokonaislukumuodossa oleva aikaleima (siten kuin se on määritelty standardin RFC 8392 ([5]) 2 kohdassa), josta käy ilmi terveystodistuksen laatimisajankohta.

Myönnetty-kentän arvo ei saa olla aikaisempi kuin DSC-varmenteen voimassaoloaika.

Todentajat voivat soveltaa muita toimintaperiaatteita terveystodistuksen voimassaolon rajoittamiseksi myöntämisajankohdan perusteella. Tämän väitteen yksilöimiseen käytetään väiteavainta 6.

3.2.7 Terveystodistusta koskeva väite (Health Certificate Claim)

Terveystodistusta (hcert) koskeva väite on standardin (RFC 7159 ([6])) mukainen JSON-objekti, joka sisältää terveydentilaa koskevat tiedot. Saman väitteen nojalla voi olla olemassa useita erityyppisiä terveystodistuksia, joista digitaalinen koronatodistus on yksi.

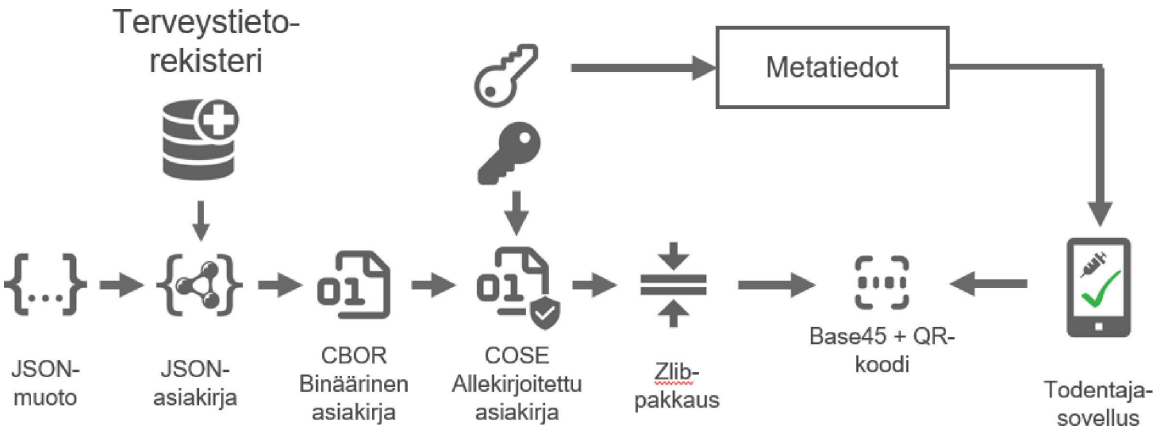
JSON on tarkoitettu yksinomaan rakenteen määrittelyyn. Esitysmuoto on CBOR, siten kuin se on määritelty standardissa (RFC 7049 ([7])). Sovelluskehittäjät eivät välttämättä koskaan pura koodia JSON-muodosta tai koodaa sitä JNOS-muotoon, vaan käyttävät muistissa olevaa rakennetta.

Tämän väitteen yksilöimiseen käytetään väiteavainta -260.

JSON-objektin merkkijonot olisi normalisoitava Unicode-standardissa määritellyn NFC-muodon (Normalization Form Canonical Composition) mukaisesti. Koodauksenpurkusovellusten olisi kuitenkin oltava tässä suhteessa sallivia ja vakaita, ja kaikkien kohtuudella odotettavissa olevien muuntamistyyppien hyväksymistä suositellaan voimakkaasti. Jos koodin purkamisen aikana tai myöhemmissä vertailutoiminnoissa havaitaan normalisoimattomia tietoja, toteutusten olisi toimittava ikään kuin syöte olisi normalisoitu NFC-muotoon.

4. **Digitaalisen koronatodistuksen hyötykuorman sarjoittaminen ja luominen**

Sarjoitusmallina käytetään seuraavaa skeemaa:



Prosessi alkaa tietojen keräämisestä esimerkiksi terveystietorekisteristä (tai jostain ulkoisesta tietolähteestä), jolloin kerätyt tiedot jäsennetään digitaalisen koronatodistuksen määriteltyjen rakenteiden mukaisesti. Tässä prosessissa muuntaminen määriteltyyn tietomuotoon ja muuttaminen ihmisluettavaan muotoon voi tapahtua ennen kuin sarjoittaminen CBOR-muotoon alkaa. Väitteiden lyhenteet on joka tapauksessa yhdistettävä näyttönimeen ennen sarjoittamista ja sarjoituksen poistamisen jälkeen.

Valinnaista kansallista tietosisältöä ei sallita asetuksen (EU) 2021/953 ([8]) mukaisesti myönnetyissä todistuksissa. Tietosisältö rajoittuu asetuksen (EU) 2021/953 liitteessä täsmennettyjen vähimmäistietojoukkojen määriteltyihin tietoelementteihin.

([5]) rfc8392 (ietf.org)
([6]) rfc7159 (ietf.org)
([7]) rfc7049 (ietf.org)
([8]) Euroopan parlamentin ja neuvoston asetus (EU) 2021/953, annettu 14 päivänä kesäkuuta 2021, kehyksestä covid-19-tautiin liittyvien yhteentoimivien rokotusta, testausta ja taudista parantumista koskevien todistusten (EU:n digitaalinen koronatodistus) myöntämiseksi, todentamiseksi ja hyväksymiseksi helpottamaan henkilöiden vapaata liikkuvuutta covid-19-pandemian aikana (EUVL L 211, 15.6.2021, s. 1).

5. **Siirtokoodaus**

5.1 *Raaka*

Satunnaisissa tietoliitännöissä HCERT-säilö ja sen hyötykuormat voidaan siirtää sellaisinaan käyttäen mitä tahansa pohjana olevaa 8-bittistä, turvallista ja luotettavaa tiedonsiirtoa. Näihin liitäntöihin voi sisältyä lähitiedonsiirto (Near-Field Communication, NFC), Bluetooth tai siirto sovelluskerroksen protokollan kautta, esimerkiksi HCERT:n siirtäminen myöntäjältä haltijan mobiililaitteeseen.

Jos HCERT:n siirtäminen myöntäjältä haltijalle perustuu pelkän esitystapakerroksen sisältävään rajapintaan (esim. tekstiviesti, sähköposti), raakaa siirtokoodausta ei tietenkään voida soveltaa.

5.2 *Viivakoodi*

5.2.1 Hyötykuorman (CWT) pakkaaminen

HCERT:n koon pienentämiseksi ja lukuprosessin nopeuden ja luotettavuuden parantamiseksi CWT pakataan ZLIB:llä (RFC 1950 ([9])) ja Deflate-pakkausmenetelmällä standardissa RFC 1951 ([10]) määritellyssä muodossa.

5.2.2 QR 2D -viivakoodi

Jotta voidaan hallita paremmin vanhoja laitteita, jotka on suunniteltu toimimaan ASCII-hyötykuormilla, pakattu CWT koodataan ASCII-muotoon käyttäen Base45-koodausta ennen kuin se koodataan 2D-viivakoodiksi.

2D-viivakoodin luomisessa käytetään standardissa (ISO/IEC 18004:2015) määriteltyä QR-formaattia. Virheenkorjaustasoksi suositellaan Q (noin 25 prosenttia). Koska käytetään Base45:a, QR-koodissa on käytettävä aakkosnumeerista koodausta (Mode 2, ilmaistaan symboleilla 0010).

Jotta todentajat pystyvät havaitsemaan koodattujen tietojen tyypin ja valitsemaan oikean koodinpurku- ja käsittelymenetelmän, (tämän eritelmän mukaisesti) Base45-koodatuille tiedoille on annettava etuliitteeksi kontekstitunnisterivi ”HC1:”. Tämän eritelmän tulevissa versioissa, jotka vaikuttavat yhteensopivuuteen taaksepäin, määritellään uusi kontekstitunniste, jossa ”HC”:tä seuraava merkki valitaan merkkijoukosta [1–9A-Z]. Lisäykset tehdään edellä olevassa järjestyksessä, eli ensin [1–9] ja sitten [A-Z].

Suositellaan, että optinen koodi renderoidaan esitysvälineessä siten, että sen läpimitta on 35–60 mm, jotta se soveltuu lukulaitteille, joissa on kiinteä optiikka ja joissa esitysväline on sijoitettava lukulaitteen pinnalle.

Jos optinen koodi painetaan paperille käyttäen matalaresoluutioisia (< 300 dpi) tulostimia, on huolehdittava siitä, että QR-koodin jokainen symboli (piste) on täsmälleen neliö. Ei-suhteellinen skaalaus johtaa siihen, että QR-koodin joillakin riveillä tai joissakin sarakkeissa on suorakulmaisia symboleja, mikä vaikeuttaa luettavuutta monissa tapauksissa.

6. **Luottamusluettelon muoto (CSCA- ja DSC-luettelo)**

Kunkin jäsenvaltion on toimitettava luettelo yhdestä tai useammasta kansallisesta juurivarmentajasta (Country Signing Certificate Authority, CSCA) ja luettelo kaikista voimassa olevista asiakirjan allekirjoittajan varmenteista (Document Signing Certificate, DSC) ja pidettävä luettelot ajan tasalla.

6.1 *Yksinkertaistettu CSCA/DSC*

Eritelmän tästä versiosta alkaen jäsenvaltiot eivät saa olettaa, että mitään varmenteiden sulkulistaa (Certificate Revocation List, CRL) koskevia tietoja käytetään tai että todentajat tarkistavat yksityisen avaimen käyttöajan.

Sen sijaan ensisijainen voimassaolon tarkistusmekanismi on se, että varmenne on merkitty kyseisen varmenneluettelon viimeisimpään versioon.

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

6.2 *ICAOn eMRTD-matkustusasiakirjan PKI ja luottamuskeskukset*

Jäsenvaltiot voivat käyttää erillistä CSCA-varmennetta, mutta ne voivat myös toimittaa olemassa olevat sirullisen koneluettavan matkustusasiakirjan (eMRTD) CSCA- ja/tai DSC-varmenteet, ja ne voivat jopa hankkia varmenteet (kaupallisilta) luottamuskeskuksilta ja toimittaa ne. Kyseisen jäsenvaltion ilmoittaman CSCA:n on kuitenkin aina allekirjoitettava kaikki DSC-varmenteet.

7. **Turvallisuusnäkökohdat**

Suunnitellessaan järjestelmää, jossa käytetään tätä eritelmää, jäsenvaltioiden on määriteltävä ja analysoitava tietyt turvallisuusnäkökohdat ja seurattava niitä.

Huomioon olisi otettava vähintään seuraavat seikat:

7.1 *HCERT:n allekirjoituksen voimassaoloaika*

HCERT:n myöntäjän on rajoitettava allekirjoituksen voimassaoloaikaa määrittämällä allekirjoituksen voimassaolon päättymisajankohta. Tämä edellyttää, että terveystodistuksen haltija uusii sen säännöllisin väliajoin.

Hyväksyttävä voimassaoloaika voidaan määritellä käytännön rajoitteiden perusteella. Esimerkiksi matkustajalla ei välttämättä ole mahdollisuutta uusia terveystodistusta ulkomaanmatkan aikana. Voi kuitenkin käydä myös niin, että myöntäjä näkee mahdollisuuden jonkinlaiseen turvallisuuden vaarantumiseen, mikä edellyttää, että myöntäjä peruuttaa DSC-varmenteen (mikä mitätöi kaikki kyseisellä avaimella myönnetyt terveystodistukset, vaikka todistusten voimassaoloaika ei ole vielä kulunut umpeen). Tällaisen tapahtuman seurauksia voidaan rajoittaa ottamalla säännöllisesti käyttöön uusia myöntäjän avaimia ja edellyttämällä kaikkien terveystodistusten uusimista kohtuullisin määräajoin.

7.2 *Avainten hallinta*

Tämä eritelmä perustuu suurelta osin vahvoihin salausmekanismeihin tietojen eheyden ja tietojen alkuperän todentamisen turvaamiseksi. Sen vuoksi on tarpeen säilyttää yksityisten avainten luottamuksellisuus.

Salausavainten luottamuksellisuus voi vaarantua useilla eri tavoilla, esimerkiksi seuraavasti:

— Avainten luomisprosessi voi olla virheellinen, mikä johtaa heikkoihin avaimiin.

— Avaimet voivat paljastua inhimillisen erehdyksen vuoksi.

— Ulkopuoliset tai sisäiset tunkeutujat voivat varastaa avaimet.

— Avaimet voidaan laskea kryptoanalyysilla.

Jotta voidaan vähentää riskiä, että allekirjoitusalgoritmi osoittautuu heikoksi ja mahdollistaa yksityisten avaimien vaarantumisen kryptoanalyysin avulla, tässä eritelmässä suositellaan, että kaikki osallistujat ottavat käyttöön varalla olevan toissijaisen allekirjoitusalgoritmin, joka perustuu erilaisiin parametreihin tai erilaiseen matemaattiseen ongelmaan kuin ensisijainen algoritmi.

Edellä mainittujen myöntäjien toimintaympäristöön liittyvien riskien osalta on toteutettava lieventäviä toimenpiteitä tehokkaan valvonnan varmistamiseksi, kuten yksityisten avainten luominen, tallentaminen ja käyttö laitteistoturva-moduuleissa (Hardware Security Module, HSM). HSM-laitteiden käyttö terveystodistusten allekirjoittamisessa on erittäin suositeltavaa.

Riippumatta siitä, päättääkö myöntäjä käyttää HSM-laitteita vai ei, olisi laadittava avainten uusimisaikataulu, jossa avainten uusimistiheys on oikeassa suhteessa avainten altistumiseen ulkoisille verkoille, muille järjestelmille ja henkilöstölle. Hyvin valittu uusimisaikataulu rajoittaa myös virheellisesti myönnettyihin terveystodistuksiin liittyviä riskejä ja antaa myöntäjälle mahdollisuuden peruuttaa tällaiset terveystodistukset tarvittaessa erissä kumoamalla avaimen.

7.3 *Syöttötietojen validointi*

Näitä eritelmiä voidaan käyttää tavalla, jossa tietoja vastaanotetaan epäluotetuista lähteistä järjestelmiin, jotka voivat olla tehtävän kannalta kriittisiä. Tähän hyökkäysvektoriin liittyvien riskien minimoimiseksi kaikki syöttökentät on validoitava asianmukaisesti tietotyyppien, pituuksien ja sisällön suhteen. Myös myöntäjän allekirjoitus on tarkistettava ennen HCERT:n sisällön käsittelyä. Myöntäjän allekirjoituksen validointi edellyttää kuitenkin, että ensin jäsennetään suojattu myöntäjän otsikko, johon mahdollinen hyökkääjä voi yrittää syöttää taitavasti suunniteltuja tietoja järjestelmän turvallisuuden vaarantamiseksi.

8. **Luottamuksen hallinta**

HCERT:n allekirjoituksen todentaminen edellyttää julkista avainta. Jäsenvaltioiden on asetettava nämä julkiset avaimet saataville. Viime kädessä jokaisella todentajalla on oltava luettelo kaikista julkisista avaimista, joihin se on halukas luottamaan (koska julkinen avain ei ole osa HCERT:ä).

Järjestelmä koostuu (vain) kahdesta kerroksesta: kunkin jäsenvaltion osalta yksi tai useampi maakohtainen varmenne, jolla kullakin allekirjoitetaan yksi tai useampi päivittäisessä toiminnassa käytettävä asiakirjan allekirjoittajan varmenne.

Jäsenvaltioiden varmenteita kutsutaan CSCA-varmenteiksi (Country Signing Certificate Authority), ja ne ovat (tyypillisesti) itse allekirjoitettuja. Jäsenvaltioilla voi olla niitä useampi kuin yksi (esimerkiksi jos hallinto on hajautettu alueellisesti). Näillä CSCA-varmenteilla allekirjoitetaan tavallisesti HCERT-todistusten allekirjoittamiseen käytettävät asiakirjan allekirjoittajan varmenteet (DSC).

”Sihteeristöllä” on toiminnallinen tehtävä. Se kokoaa ja julkaisee säännöllisesti jäsenvaltioiden DSC-varmenteet tarkastettuaan ne suhteessa CSCA-varmenteiden luetteloon (joka on toimitettu ja todennettu muulla tavoin).

Tuloksena saatavassa DSC-varmenneluettelossa on esitettävä kootut hyväksyttävät julkiset avaimet (ja vastaavat kid-tunnisteet), joita todentajat voivat käyttää validoidakseen HCERT-todistusten allekirjoitukset. Todentajien on haettava luettelo ja päivitettävä se säännöllisesti.

Näiden jäsenvaltiokohtaisten luettelojen muotoa voidaan mukauttaa kunkin jäsenvaltion kansallisten olosuhteiden mukaan. Tämän luottamusluettelon tiedostomuoto voi vaihdella; se voi olla esimerkiksi allekirjoitettu JWKS (standardin RFC 7517 ([11]) 5 jakson mukainen JWK Set -muoto) tai mikä tahansa muu kyseisessä jäsenvaltiossa käytetylle teknologialle ominainen muoto.

Yksinkertaisuuden vuoksi jäsenvaltiot voivat toimittaa olemassa olevat CSCA-varmenteensa ICAOn eMRTD-järjestelmistä tai luoda WHO:n suosituksen mukaisesti nimenomaan tätä terveydenhuollon toimialuetta koskevan varmenteen.

8.1 *Avaimen tunniste (kid)*

Avaimen tunniste (kid) lasketaan, kun laaditaan luotettujen julkisten avainten luettelo DSC-varmenteista, ja se koostuu DER-(raaka)muodossa koodatun DSC-varmenteen katkaistusta (ensimmäiset 8 bittiä) SHA-256-sormenjäljestä.

Todentajien ei tarvitse laskea kid-tunnistetta DSC-varmenteen perusteella, vaan ne voivat suoraan verrata myönnetyssä terveystodistuksessa käytettyä avaimen tunnistetta luottamusluettelossa olevaan kid-tunnisteeseen.

8.2 *Erot ICAOn eMRTD:n PKI-luottamusmalliin*

Nämä eritelmät perustuvat ICAOn eMRTD-matkustusasiakirjan PKI-luottamusmallia koskeviin parhaisiin käytäntöihin, mutta nopeuden vuoksi niihin on tehty joitain yksinkertaistuksia:

— Jäsenvaltio voi toimittaa useita CSCA-varmenteita.

— DSC-varmenteen (avaimen käytön) voimassaoloaika voi olla mikä tahansa aika, joka ei ylitä CSCA-varmenteen voimassaoloaikaa, tai se voidaan jättää pois.

— DSC-varmenne voi sisältää erityisesti terveystodistuksiin liittyviä käyttökäytäntöjen tunnisteita (laajennettu avaimen käyttö).

— Jäsenvaltiot voivat päättää olla tarkistamatta julkaistuja peruutuksia, vaan ne voivat sen sijaan käyttää pelkkiä DSC-luetteloja, jotka ne saavat päivittäin sihteeristöltä tai kokoavat itsensä.

([11]) rfc7517 (ietf.org)

LIITE II

EU:N DIGITAALISEN KORONATODISTUKSEN TÄYTTÖOHJEET

Tässä liitteessä vahvistetuilla arvojoukkoja koskevilla yleisillä säännöillä pyritään varmistamaan yhteentoimivuus semanttisella tasolla ja mahdollistetaan digitaalisen koronatodistuksen yhdenmukainen tekninen toteutus. Tässä liitteessä olevia elementtejä voidaan käyttää asetuksen (EU) 2021/953 mukaisissa kolmessa eri tilanteessa (rokotus/testaus/taudista parantuminen). Tässä liitteessä luetellaan ainoastaan elementit, jotka edellyttävät semanttista standardointia koodattujen arvojoukkojen avulla.

Koodattujen elementtien kääntäminen kansalliselle kielelle on jäsenvaltioiden vastuulla.

Koodaamista UTF-8-merkkijärjestelmällä suositellaan kaikissa tietokentissä, joita ei mainita seuraavissa arvojoukkojen kuvauksissa (nimi, testauskeskus, todistuksen myöntäjä). Kalenteripäiviä sisältävät tietokentät (syntymäaika, rokotuspäivä, testinäytteen ottopäivä, ensimmäisen positiivisen testituloksen päivämäärä, todistuksen voimassaolopäivät) suositellaan koodattavaksi ISO 8601 -standardin mukaisesti.

Jos jäljempänä lueteltuja suositeltavia koodijärjestelmiä ei jostain syystä voida käyttää, voidaan käyttää muita kansainvälisiä koodijärjestelmiä ja antaa ohjeita siitä, miten muiden koodijärjestelmien koodit vastaavat suositeltavaa koodijärjestelmää. Tekstiä (näyttönimiä) voidaan poikkeustapauksissa käyttää varamekanismina, jos määritellyissä arvojoukoissa ei ole saatavilla sopivaa koodia.

Jäsenvaltioiden, jotka käyttävät järjestelmissään muita koodeja, olisi määritettävä, kuinka nämä koodit liittyvät kuvattuihin arvojoukkoihin. Jäsenvaltiot vastaavat tällaisista määrityksistä.

Komissio päivittää arvojoukkoja säännöllisesti sähköisten terveyspalvelujen verkoston ja terveysturvakomitean tuella. Päivitetyt arvojoukot julkaistaan asiaa koskevalla komission verkkosivustolla sekä sähköisten terveyspalvelujen verkoston verkkosivustolla. Muutoshistoria olisi esitettävä.

1. **Kyseessä oleva tauti tai taudinaiheuttaja / Tauti tai taudinaiheuttaja, josta todistuksen haltija on parantunut: covid-19 (SARS-CoV-2 tai jokin sen muunnoksista)**

   Suositeltava koodijärjestelmä: SNOMED CT.

   Käytetään todistuksissa 1, 2 ja 3.

   Valituissa koodeissa on viitattava covid-19:ään tai, jos tarvitaan tarkempia tietoja SARS-CoV-2-viruksen geneettisestä muunnoksesta, näihin muunnoksiin, jos tällaisia yksityiskohtaisia tietoja tarvitaan epidemiologisista syistä.

   Esimerkki koodista, jota olisi käytettävä, on SNOMED CT -koodi 840539006 (covid-19).

2. **Covid-19-rokote tai -estolääkitys**

   Suositeltava koodijärjestelmä: SNOMED CT tai ATC-luokitus.

   Käytetään todistuksessa 1.

   Esimerkkejä suositeltavien koodijärjestelmien koodeista, joita olisi käytettävä, ovat SNOMED CT -koodi 1119305005 (SARS-CoV-2-antigeenirokote), 1119349007 (SARS-CoV-2-mRNA-rokote) tai J07BX03 (covid-19-rokotteet). Arvojoukkoa olisi laajennettava, kun uusia rokotetyyppejä kehitetään ja otetaan käyttöön.

3. **Covid-19-rokotevalmiste**

   Suositeltavat koodijärjestelmät (suosituimmuusjärjestyksessä):

   — Unionin lääkerekisteri rokotteille, joilla on EU:n laajuinen myyntilupa (lupien numerot)

   — Maailmanlaajuinen rokoterekisteri, jonka Maailman terveysjärjestö voisi perustaa

   — Muissa tapauksissa rokotevalmisteen nimi. Jos nimi sisältää välilyöntejä, ne olisi korvattava yhdysmerkillä (-).

Arvojoukon nimi: Rokote.

Käytetään todistuksessa 1.

Esimerkki suositeltavien koodijärjestelmien koodista, jota olisi käytettävä, on EU/1/20/1528 (Comirnaty). Esimerkki koodina käytettävästä rokotteen nimestä: Sputnik-V (rokotteesta Sputnik V).

4. **Covid-19-rokotteen myyntiluvan haltija tai valmistaja**

Suositeltava koodijärjestelmä:

— EMA:n antama organisaation koodi (ISO IDMP-standardien mukainen SPOR-tietokanta)

— Rokotteen myyntiluvan haltijoiden tai valmistajien maailmanlaajuinen rekisteri, jonka Maailman terveysjärjestö voisi perustaa

— Muissa tapauksissa organisaation nimi. Jos nimi sisältää välilyöntejä, ne olisi korvattava yhdysmerkillä (-).

Käytetään todistuksessa 1.

Esimerkki suositeltavan koodijärjestelmän koodista, jota olisi käytettävä, on ORG-100001699 (AstraZeneca AB). Esimerkki koodina käytettävästä organisaation nimestä: Sinovac-Biotech (organisaatiosta Sinovac Biotech).

5. **Annosnumero rokotussarjassa ja sarjarokotteen annosten kokonaismäärä**

Käytetään todistuksessa 1.

Kaksi kenttää:

(1) Sarjassa annetun annoksen annosnumero

(2) Odotettu annosmäärä koko sarjassa (henkilökohtainen annoksen antamishetkellä)

Esimerkiksi 1/1, 2/2 esittää loppuun saatettua rokotussarjaa; siihen sisältyy vaihtoehto 1/1 rokotteille, joita annetaan kaksi annosta, mutta joiden osalta jäsenvaltion käytäntönä on antaa yksi annos kansalaisille, joilla on diagnosoitu covid-19-tauti ennen rokottamista. Sarjaan sisältyvien annosten kokonaismäärä olisi ilmoitettava annoksen antamishetkellä saatavilla olleiden tietojen mukaisesti. Jos esimerkiksi tietystä rokotteesta on annettava kolmas annos (tehosteannos) viimeksi annetun annoksen antamishetkellä saatavilla olevien tietojen mukaan, tämän on käytävä ilmi toisen kentän numerosta (esimerkiksi 2/3, 3/3 jne.).

6. **Jäsenvaltio tai kolmas maa, jossa rokote annettiin / testi tehtiin**

Suositeltava koodijärjestelmä: ISO 3166 -maakoodit.

Käytetään todistuksissa 1, 2 ja 3.

Arvojoukon sisältö: täydellinen luettelo 2-kirjaimista koodeista, jotka ovat saatavilla FHIR-standardissa määriteltynä arvojoukkona (http://hl7.org/fhir/ValueSet/iso3166-1-2)

7. **Testin tyyppi**

Suositeltava koodijärjestelmä: LOINC.

Käytetään todistuksessa 2 sekä todistuksessa 3, jos delegoidulla säädöksellä otetaan käyttöön tuki taudista parantumista koskevien todistusten myöntämiselle muiden testityyppien kuin NAAT-testin perusteella.

Tämän arvojoukon koodeissa on viitattava testimenetelmään, ja ne on valittava vähintään erottamaan NAAT-testit RAT-testeistä asetuksessa (EU) 2021/953 esitetyllä tavalla.

Esimerkki suositeltavan koodijärjestelmän koodista, jota olisi käytettävä, on LP217198-3 (Nopea immuunimääritys).

8. **Käytetyn testin valmistaja ja myyntinimike (NAAT-testin osalta valinnainen)**

Suositeltava koodijärjestelmä: Terveysturvakomitean laatima ja JRC:n ylläpitämä antigeenipikatestien luettelo (Covid-19-taudin in vitro -diagnostiikkaan tarkoitettujen laitteiden ja testimenetelmien tietokanta).

Käytetään todistuksessa 2.

Arvojoukon sisällön muodostaa antigeenipikatestien valikoima, joka on lueteltu neuvoston suosituksen 2021/C 24/01 perusteella laaditussa ja terveysturvakomitean hyväksymässä covid-19-antigeenipikatestien yhteisessä päivitetyssä luettelossa. JRC ylläpitää luetteloa covid-19-taudin in vitro -diagnostiikkaan tarkoitettujen laitteiden ja testimenetelmien tietokannassa, joka on saatavilla osoitteessa: https://covid-19-diagnostics.jrc.ec.europa.eu/devices/hsc-common-recognition-rat

Tässä koodijärjestelmässä on käytettävä asianmukaisia kenttiä, kuten testilaitteen tunniste, testin nimi ja valmistaja, käyttäen JRC:n jäsenneltyä muotoa, joka on saatavilla osoitteessa https://covid-19-diagnostics.jrc.ec.europa.eu/devices.

9. **Testin tulos**

Suositeltava koodijärjestelmä: SNOMED CT.

Käytetään todistuksessa 2.

Valittujen koodien avulla on voitava erottaa positiiviset ja negatiiviset testitulokset (havaittu tai ei-havaittu). Muita arvoja (kuten määrittelemätön) voidaan lisätä, jos käyttötapaukset sitä edellyttävät.

Esimerkkejä suositeltavien koodijärjestelmien koodeista, joita olisi käytettävä, ovat 260415000 (Ei-havaittu) ja 260373001 (Havaittu).

LIITE III

YKSILÖLLISEN TODISTUSTUNNUKSEN YHTEINEN RAKENNE

1. **Johdanto**

Jokaisella EU:n digitaalisella koronatodistuksella on oltava yksilöllinen todistustunnus (Unique Certificate Identifier, UCI), joka tukee digitaalisten koronatodistusten yhteentoimivuutta. UCI-tunnistetta voidaan käyttää todistuksen todentamiseen. Jäsenvaltiot vastaavat UCI-tunnisteen täytäntöönpanosta. UCI-tunniste on keino tarkistaa todistuksen todenmukaisuus ja tarvittaessa linkittää se rekisteröintijärjestelmään (esim. IIS-rokotustietojärjestelmään). Näiden tunnisteiden on myös mahdollistettava jäsenvaltioiden (paperiset ja digitaaliset) vakuutukset siitä, että henkilöt on rokotettu tai testattu.

2. **Yksilöllisen todistustunnuksen sisältö**

UCI-tunnisteen on noudatettava yhteistä rakennetta ja muotoa, joilla helpotetaan ihmisen tekemää ja/tai koneellista tietojen tulkintaa, ja se voi liittyä esimerkiksi rokotusjäsenvaltioon, itse rokotteeseen ja jäsenvaltiokohtaiseen tunnisteeseen. Sillä varmistetaan, että jäsenvaltiot voivat muotoilla sen joustavasti tietosuojalainsäädäntöä täysimääräisesti noudattaen. Erillisten osien järjestys noudattaa määriteltyä hierarkiaa, joka mahdollistaa lohkojen myöhemmät muutokset säilyttäen samalla niiden rakenteellisen eheyden.

UCI-tunnisteen muodostamista koskevat mahdolliset ratkaisut muodostavat jatkumon, jossa modulaarisuus ja ihmisen tulkittavissa oleminen ovat kaksi tärkeintä vaihtelevaa parametria ja jossa on yksi perusominaisuus:

— Modulaarisuus: se, missä määrin koodi koostuu erillisistä rakenneosista, jotka sisältävät semanttisesti erilaisia tietoja

— Ihmisen tulkittavissa oleminen: se, missä määrin koodi on merkityksellinen sitä lukevalle ihmiselle tai tämän tulkittavissa

— Globaalisti ainutlaatuinen; maan tai viranomaisen tunnistetta hallinnoidaan hyvin, ja kunkin maan (viranomaisen) odotetaan hallinnoivan omaa nimiavaruuden segmenttiään hyvin siten, ettei tunnisteita koskaan kierrätetä tai annetaan uudelleen. Näiden yhdistelmällä varmistetaan, että jokainen tunniste on globaalisti ainulaatuinen.

3. **Yleiset vaatimukset**

UCI-tunnisteiden olisi täytettävä seuraavat yleiset vaatimukset:

(1) Merkistö: ainoastaan isot aakkosnumeeriset US-ASCII-merkit (A–Z, 0–9) ovat sallittuja; lisäksi standardista RFC3986 ([1]) ([2]), erottamiseksi voidaan käyttää erikoismerkkejä, kuten {'/','#',':'};

(2) Enimmäispituus: suunnittelijoiden olisi pyrittävä tavoittelemaan 27–30 merkin pituutta ([3]);

(3) Version etuliite: tällä viitataan UCI-rakenteen versioon. Asiakirjan tämän version etuliite on '01'; version etuliite koostuu kahdesta numerosta;

(4) Maan etuliite: maakoodi määritellään standardissa ISO 3166–1. Pidemmät koodit (esim. kolme merkkiä ja enemmän (esimerkiksi 'UNHCR')) varataan myöhempään käyttöön;

(5) Koodin jälkiliite / tarkistussumma:

5.1 Jäsenvaltioiden olisi käytettävä tarkistussummaa, kun on todennäköistä, että tunniste voidaan siirtää tai kopioida (ihmisen toimesta) tai siihen voidaan puuttua muulla tavoin (eli kun tunnistetta käytetään tulosteena).

5.2 Tarkistussummaa ei saa käyttää todistuksen validoimiseen, eikä se ole teknisesti osa tunnistetta, vaan sitä käytetään koodin eheyden todentamiseen. Tarkistussumman olisi oltava ISO-7812-1 (LUHN-10) ([4]) -kooste koko UCI-tunnisteesta digitaalisessa/langallisessa siirtomuodossa. Tarkistussumma erotetaan muusta UCI-tunnisteesta merkillä '#'.

([1]) rfc3986 (ietf.org)

([2]) Sukupuolen, erän numeron, rokotuskeskuksen, terveydenhuollon ammattihenkilön tunnistetietojen ja seuraavan rokotuspäivän kaltaisia kenttiä ei välttämättä tarvita muihin tarkoituksiin kuin lääketieteelliseen käyttöön.

([3]) Kun käytetään QR-koodeja, jäsenvaltiot voivat harkita lisämerkkien käyttöä yhteensä 72 merkkiin saakka (mukaan lukien itse tunnisteen 27–30 merkkiä) muiden tietojen välittämiseksi. Jäsenvaltiot voivat itse määritellä nämä tiedot.

([4]) Luhn mod N -algoritmi on laajennus Luhn-algoritmiin (tunnetaan myös nimellä mod 10 -algoritmi), joka toimii numeeristen koodien kanssa ja jota käytetään esimerkiksi luottokorttien tarkistussumman laskemiseen. Laajennuksen ansiosta algoritmi voi toimia arvosekvenssien kanssa millä tahansa pohjalla (tässä tapauksessa kirjainten).

Yhteensopivuus taaksepäin olisi varmistettava: jäsenvaltioiden, jotka ajan mittaan muuttavat tunnisteidensa rakennetta (pääversiossa, joka on tällä hetkellä v1), on varmistettava, että kaksi samanlaista tunnistetta vastaavat samaa rokotustodistusta/-vakuutusta. Toisin sanoen jäsenvaltiot eivät voi kierrättää tunnisteita.

4. **Rokotustodistusten yksilöllisten todistustunnusten vaihtoehdot**

Sähköisen terveydenhuollon verkoston laatimissa todennettavissa olevia rokotustodistuksia ja yhteentoimivuuden perustekijöitä koskevissa suuntaviivoissa ([5]) esitetään jäsenvaltioille ja muille osapuolille erilaisia vaihtoehtoja, joita voidaan soveltaa samanaikaisesti eri jäsenvaltioissa. Jäsenvaltiot voivat käyttää tällaisia eri vaihtoehtoja UCI-rakenteen eri versioissa.

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

LIITE IV

JULKISEN AVAIMEN VARMENTEEN HALLINNOINTI

1. Johdanto

EU:n digitaalisten koronatodistusten allekirjoitusavainten suojattu ja luotettava vaihto jäsenvaltioiden välillä toteutetaan EU:n digitaalisen koronatodistuksen yhdyskäytävän (DCCG) kautta. Se toimii julkisten avainten keskusrekisterinä. Yhdyskäytävän avulla jäsenvaltiot voivat julkaista julkiset avaimet, jotka vastaavat niitä yksityisiä avaimia, joita ne käyttävät digitaalisten koronatodistusten allekirjoittamiseen. Luottavat jäsenvaltiot voivat käyttää yhdyskäytävää ajantasaisen julkisen avaimen aineiston hakemiseen oikea-aikaisesti. Myöhemmässä vaiheessa yhdyskäytävä voidaan laajentaa jäsenvaltioiden toimittamien luotettavien lisätietojen vaihtoon. Ne voivat liittyä esimerkiksi digitaalisten koronatodistusten validointisääntöihin. Digitaalisten koronatodistusten kehyksen luottamusmallina on julkisen avaimen infrastruktuuri (PKI). Kukin jäsenvaltion pitää yllä yhtä tai useampaa kansallista juurivarmentajaa (CSCA), jonka varmenteet ovat suhteellisen pitkäikäisiä. Jäsenvaltion päätöksestä CSCA voi olla sama tai eri kuin koneluettavia matkustusasiakirjoja varten käytetty CSCA. CSCA myöntää julkisen avaimen varmenteita kansallisille, lyhytikäisille asiakirjan allekirjoittajille (eli digitaalisten koronatodistusten allekirjoittajille). Niitä kutsutaan nimellä asiakirjan allekirjoittajan varmenteet (DSC). CSCA toimii luottamusankkurina, jonka avulla luottavat jäsenvaltiot voivat käyttää CSCA-varmennetta säännöllisesti muuttuvien DSC-varmenteiden aitouden ja eheyden varmentamiseen. Kun varmenteet on validoitu, jäsenvaltiot voivat antaa niitä (tai vain niihin sisältyviä julkisia avaimia) digitaalisten koronatodistusten validointia koskeville hakemuksille. CSCA- ja DSC-varmenteiden lisäksi digitaalisten koronatodistusten yhdyskäytävä tukeutuu myös PKI-järjestelmään transaktioiden todentamisessa, tietojen allekirjoittamisessa, todentamisen perustana sekä keinona varmistaa jäsenvaltioiden ja yhdyskäytävän välisten tiedonsiirtokanavien eheys.

Digitaalisia allekirjoituksia voidaan käyttää tietojen eheyden ja aitouden saavuttamiseksi. Julkisen avaimen infrastruktuurit luovat luottamusta sitomalla julkiset avaimet todennettuihin henkilöllisyyksiin (tai myöntäjiin). Tämä on tarpeen, jotta muut osallistujat voivat tarkistaa tiedon alkuperän ja viestintäkumppanin henkilöllisyyden ja päättää luottamuksesta. Yhdyskäytävässä todentamiseen käytetään useita julkisen avaimen varmenteita. Tässä liitteessä määritellään, mitä julkisen avaimen varmenteita käytetään ja miten ne on suunniteltava laajan yhteentoimivuuden mahdollistamiseksi jäsenvaltioiden kesken. Siinä annetaan tarkempia tietoja tarvittavista julkisen avaimen varmenteista ja annetaan ohjeita varmenteiden malleista ja voimassaoloajoista niille jäsenvaltioille, jotka haluavat käyttää omaa CSCA:aan. Koska digitaalisten koronatodistusten on oltava todennettavissa määrätyn ajan (myöntämisestä voimassaolon päättymiseen), on tarpeen määritellä todentamismalli kaikille julkisen avaimen varmenteissa ja digitaalisissa koronatodistuksissa käytetyille allekirjoituksille.

2. Terminologia

Seuraavassa taulukossa esitetään tässä liitteessä käytetyt lyhenteet ja termit.

Termi	Määritelmä
Varmenne	Eli julkisen avaimen varmenne. X.509 v3 -varmenne, joka sisältää yksikön julkisen avaimen
CSCA	Country Signing Certificate Authority; kansallinen juurivarmentaja
DCC	EU Digital COVID Certificate; EU:n digitaalinen koronatodistus. Allekirjoitettu digitaalinen asiakirja, joka sisältää tietoja rokotuksesta, testauksesta tai taudista parantumisesta
DCCG	EU Digital COVID Certificate Gateway. EU:n digitaalisen koronatodistuksen yhdyskäytävä. Tätä järjestelmää käytetään DSC-varmenteiden vaihtoon jäsenvaltioiden välillä
$DCCG_{TA}$	DCCG:n luottamusankkurin varmenne. Vastaavaa yksityistä avainta käytetään kaikkien CSCA-varmenteiden luettelon allekirjoittamiseen verkon ulkopuolella
$DCCG_{TLS}$	DCCG:n TLS-palvelinvarmenne
DSC	Document Signer Certificate; asiakirjan allekirjoittajan varmenne. Jäsenvaltion asiakirjojen allekirjoittajaviranomaisen (esimerkiksi järjestelmä, jolla on lupa allekirjoittaa digitaalisia koronatodistuksia) julkisen avaimen varmenne. Tämän varmenteen myöntää jäsenvaltion CSCA
EC-DSA	Elliptic Curve Digital Signature Algorithm; elliptisen käyrän digitaalinen allekirjoitusalgoritmi. Elliptisiin käyriin perustuva kryptografinen allekirjoitusalgoritmi
Jäsenvaltio	Euroopan unionin jäsenvaltio

Termi	Määritelmä
mTLS	Keskinäinen TLS. Transport Layer Security (TLS) -protokolla, johon sisältyy molemminpuolinen todentaminen
NB	National Backend; jäsenvaltion kansallinen taustajärjestelmä
NB_{CSCA}	Jäsenvaltion CSCA-varmenne (voi olla useampia kuin yksi)
NB_{TLS}	Kansallisen taustajärjestelmän TLS-asiakkaan todennusvarmenne
NB_{UP}	Varmenne, jota kansallinen taustajärjestelmä käyttää DCCG:hen ladattavien datapakettien allekirjoittamiseen
PKI	Public Key Infrastructure; julkisen avaimen järjestelmä. Julkisen avaimen varmenteisiin ja varmenneviranomaisiin perustuva luottamusmalli
RSA	Epäsymmetrinen salausalgoritmi, joka perustuu kokonaislukujen tekijöihin jakamiseen ja jota käytetään digitaalisissa allekirjoituksissa tai epäsymmetrisessä salauksessa

3. **DCCG:n tietoliikennevirrat ja turvallisuuspalvelut**

Tässä jaksossa esitetään yleiskatsaus DCCG-järjestelmän tietoliikennevirroista ja turvallisuuspalveluista. Siinä määritellään myös, mitä avaimia ja varmenteita käytetään suojaamaan tietoliikenne, ladatut tiedot, digitaaliset koronatodistukset ja allekirjoitettu luottamusluettelo, joka sisältää kaikki käyttöön otetut CSCA-varmenteet. DCCG toimii tietokeskuksena, joka mahdollistaa allekirjoitettujen datapakettien vaihdon jäsenvaltioille.

DCCG toimittaa järjestelmään ladatut datapaketit ”sellaisinaan”, eli DCCG ei lisää tai poista DSC-varmenteita vastaanottamistaan paketeista. Jäsenvaltioiden kansallisten taustajärjestelmien on voitava tarkistaa ladattujen tietojen eheys ja aitous päästä päähän. Tämän lisäksi kansalliset taustajärjestelmät ja DCCG käyttävät keskinäistä TLS-todennusta suojatun yhteyden luomiseksi. Tämä tehdään tietojenvaihdon allekirjoitusten lisäksi.

3.1 *Todentaminen ja yhteyden luominen*

DCCG:ssä käytetään TLS-salausprotokollaa ja molemminpuolista todentamista todennetun salatun kanavan luomiseen jäsenvaltion kansallisen taustajärjestelmän ja yhdyskäytäväympäristön välille. DCCG:llä on näin ollen TLS-palvelinvarmenne ($DCCG_{TLS}$) ja kansallisilla taustajärjestelmillä TLS-asiakasvarmenne (NB_{TLS}). Varmenteiden mallit esitetään *jaksossa 5*. Kukin kansallinen taustajärjestelmä voi antaa oman TLS-varmenteensa. Tämä varmenne lisätään hyväksyttyjen varmenteiden valkoiselle listalle, ja sen voi siten myöntää julkisesti luotettu varmenneviranomainen (esimerkiksi varmenneviranomainen, joka noudattaa CA Browser Forumin perusvaatimuksia) tai kansallinen varmenneviranomainen tai se voi olla itse allekirjoitettu. Kukin jäsenvaltio on vastuussa kansallisista tiedoistaan ja sen yksityisen avaimen suojaamisesta, jota käytetään yhteyden luomiseen DCCG:hen. ”Tuo oma varmenteesi” -toimintatapa edellyttää tarkasti määriteltyä rekisteröinti- ja tunnistusprosessia sekä *4.1, 4.2 ja 4.3 kohdassa* selostettuja peruuttamis- ja uusimismenettelyjä. DCCG käyttää valkoista listaa, johon kansallisten taustajärjestelmien TLS-varmenteet lisätään niiden onnistuneen rekisteröinnin jälkeen. Ainoastaan sellaiset kansalliset taustajärjestelmät, jotka todentavat itsensä valkoiseen listaan sisältyvää varmennetta vastaavalla yksityisellä avaimella, voivat luoda suojatun yhteyden DCCG:hen. DCCG käyttää myös TLS-varmennetta, jonka avulla kansalliset taustajärjestelmät voivat tarkistaa, että ne todella muodostavat yhteyden ”todelliseen” DCCG:hen eivätkä johonkin DCCG:nä esiintyvään pahantahtoiseen tahoon. DCCG:n varmenne toimitetaan kansalliselle taustajärjestelmälle onnistuneen rekisteröinnin jälkeen. $DCCG_{TLS}$-varmenne saadaan julkisesti luotetulta varmenneviranomaiselta (sisältyy kaikkiin tärkeimpiin selaimiin). Jäsenvaltioiden vastuulla on varmistaa, että niiden yhteys DCCG:hen on suojattu (esim. vertaamalla yhteydessä olevan palvelimen $DCCG_{TLS}$- varmenteen sormenjälkeä rekisteröinnin jälkeen annettuun sormenjälkeen).

3.2 *Kansalliset juurivarmentajat ja validointimalli*

DCCG-kehykseen osallistuvien jäsenvaltioiden on käytettävä CSCA:a DSC-varmenteiden myöntämiseen. Jäsenvaltioilla voi olla useampi kuin yksi CSCA (esimerkiksi jos hallinto on hajautettu alueellisesti). Kukin jäsenvaltio voi joko käyttää olemassa olevia varmenneviranomaisia tai perustaa DCC-järjestelmää varten oman (mahdollisesti itse allekirjoitetun) varmenneviranomaisen.

Jäsenvaltioiden on esitettävä CSCA-varmenteensa DCCG-operaattorille virallisen liittymismenettelyn aikana. Kun jäsenvaltio on rekisteröity onnistuneesti (*ks. lisätietoja kohdassa 4.1*), DCCG-operaattori päivittää allekirjoitetun luottamusluettelon, joka sisältää kaikki DCC-järjestelmän aktiiviset CSCA-varmenteet. DCCG-operaattori käyttää erityistä epäsymmetristä avainparia luottamusluettelon ja varmenteiden allekirjoittamiseen verkon ulkopuolella. Yksityistä avainta ei tallenneta DCCG:n verkkojärjestelmään, joten verkkojärjestelmän vaarantuminen ei anna hyökkääjälle mahdollisuutta vaarantaa luottamusluetteloa. Vastaava luottamusankkurin varmenne $DCCG_{TA}$ annetaan kansallisille taustajärjestelmille liittymisprosessin aikana.

Jäsenvaltiot voivat hakea luottamusluettelon DCCG:stä todentamismenettelyjään varten. CSCA:lla tarkoitetaan DSC-varmenteita myöntävää varmenneviranomaista. Jäsenvaltioiden, jotka käyttävät monitasoista CA-hierarkiaa (esim. juuri-CA -> CSCA -> DSC), on ilmoitettava DSC-varmenteita myöntävä alemman tason varmenneviranomainen. Jos tässä tapauksessa jäsenvaltio käyttää olemassa olevaa varmenneviranomaista, DCC-järjestelmä jättää huomiotta kaiken CSCA:n yläpuolella olevan ja lisää valkoiselle listalle luottamusankkuriksi ainoastaan CSCA:n (vaikka se olisikin alemman tason varmenneviranomainen). ICAOn mallin tavoin tämä sallii täsmälleen kaksi tasoa – 'juuritason' CSCA:n ja 'lehtitason' DSC:n, jonka allekirjoittaa ainoastaan kyseinen CSCA.

Jos jäsenvaltio operoi omaa CSCA:taan, se vastaa kyseisen varmenneviranomaisen turvallisesta toiminnasta ja avainhallinnosta. CSCA toimii DSC-varmenteiden luottamusankkurina, minkä vuoksi CSCA:n yksityisen avaimen suojaaminen on olennaisen tärkeää DCC-ympäristön eheyden kannalta. DCC-järjestelmän PKI:n todennusmalli on kuorimalli, jonka mukaan kaikkien varmennepolun validoinnissa käytettävien varmenteiden on oltava voimassa tiettynä ajankohtana (eli allekirjoituksen validointihetkellä). Sen vuoksi sovelletaan seuraavia rajoituksia:

— CSCA ei saa myöntää varmenteita, jotka ovat voimassa pidempään kuin itse CA-varmenne;

— Asiakirjan allekirjoittaja ei saa allekirjoittaa asiakirjoja, jotka ovat voimassa pidempään kuin itse DSC-varmenne;

— Jäsenvaltioiden, jotka operoivat omaa CSCA:taan, on määriteltävä CSCA:n ja kaikkien myönnettyjen todistusten voimassaoloajat, ja niiden on huolehdittava varmenteiden uusimisesta.

Kohdassa 4.2 esitetään voimassaoloaikaa koskevia suosituksia.

3.3 *Ladattujen tietojen eheys ja aitous*

Kansalliset taustajärjestelmät voivat käyttää DCCG:tä digitaalisesti allekirjoitettujen datapakettien lataamiseen järjestelmästä ja järjestelmään onnistuneen molemminpuolisen todentamisen jälkeen. Alussa nämä datapaketit sisältävät jäsenvaltioiden DSC-varmenteet. Avainparia, jota kansallinen taustajärjestelmä käyttää DCCG-järjestelmään ladattujen datapakettien digitaaliseen allekirjoitukseen, kutsutaan kansallisen taustajärjestelmän latauksen allekirjoitusavainpariksi, ja vastaava julkisen avaimen varmenne on lyhyesti NB_{UP}-varmenne. Kukin jäsenvaltio ottaa käyttöön oman NB_{UP}-varmenteensa, joka voi olla itse allekirjoitettu tai jonka myöntää olemassa oleva varmenneviranomainen, kuten julkinen varmenneviranomainen (eli varmenneviranomainen, joka myöntää varmenteita CA Browser Forumin perusvaatimusten mukaisesti). NB_{UP}-varmenteen on erottava kaikista muista jäsenvaltion käyttämistä varmenteista (eli CSCA-, TLS-asiakas- tai DSC-varmenteista).

Jäsenvaltioiden on toimitettava latausvarmenne DCCG-operaattorille ensimmäisen rekisteröintimenettelyn aikana (*lisätietoja 4.1 kohdassa*). Kukin jäsenvaltio on vastuussa kansallisista tiedoistaan, ja kunkin jäsenvaltion on suojattava yksityinen avain, jota käytetään latausten allekirjoittamiseen.

Muut jäsenvaltiot voivat todentaa allekirjoitetut datapaketit DCCG:n toimittamien latausvarmenteiden avulla. DCCG todentaa ladattujen tietojen aitouden ja eheyden kansallisen taustajärjestelmän latausvarmenteen avulla ennen niiden toimittamista muille jäsenvaltioille.

3.4 *DCCG:n teknistä rakennetta koskevat vaatimukset*

DCCG:n teknistä rakennetta koskevat vaatimukset ovat seuraavat:

— DCCG käyttää keskinäistä TLS-todennusta luodakseen todennetun salatun yhteyden kansallisiin taustajärjestelmiin. Sen vuoksi DCCG ylläpitää valkoista listaa rekisteröidyistä NB_{TLS}-asiakasvarmenteista;

— DCCG käyttää kahta digitaalista varmennetta ($DCCG_{TLS}$ ja $DCCG_{TA}$), joissa on kaksi erillistä avainparia. $DCCG_{TA}$-avainparin yksityinen avain säilytetään verkon ulkopuolella (ei DCCG:n verkkoelementeissä);

— DCCG ylläpitää NB_{CSCA}-varmenteiden luottamusluetteloa, joka on allekirjoitettu $DCCG_{TA}$-varmenteen yksityisellä avaimella;

— Käytettävien salausten on täytettävä *5.1 kohdassa* esitetyt vaatimukset.

4. **Varmenteen elinkaaren hallinta**

4.1 *Kansallisten taustajärjestelmien rekisteröinti*

Jäsenvaltioiden on rekisteröidyttävä DCCG-operaattorille voidakseen osallistua DCCG-järjestelmään. Tässä jaksossa kuvataan tekniset ja toiminnalliset menettelyt, joita on noudatettava kansallisen taustajärjestelmän rekisteröimiseksi.

DCCG-operaattorin ja jäsenvaltion on vaihdettava tietoja teknisistä yhteyshenkilöistä liittymisprosessia varten. Oletetaan, että tekniset yhteyshenkilöt ovat jäsenvaltionsa laillisesti hyväksymiä ja että henkilöllisyyden todistaminen/todentaminen tapahtuu muiden kanavien kautta. Todentaminen voidaan toteuttaa esimerkiksi siten, että jäsenvaltion tekninen yhteyshenkilö toimittaa varmenteet sähköpostitse salasanalla salattuina tiedostoina ja jakaa vastaavan salasanan DCCG-operaattorin kanssa puhelimitse. Myös muita DCCG-operaattorin määrittelemiä suojattuja kanavia voidaan käyttää.

Jäsenvaltion on annettava rekisteröinti- ja tunnistamisprosessin aikana kolme digitaalista varmennetta:

— Jäsenvaltion TLS-varmenne NB_{TLS}

— Jäsenvaltion latausvarmenne NB_{UP}

— Jäsenvaltion CSCA-varmenne(-varmenteet) NB_{CSCA}

Kaikkien toimitettujen varmenteiden on oltava *5 jaksossa* määriteltyjen vaatimusten mukaisia. DCCG-operaattori tarkistaa, että annettu varmenne on *5 jakson* vaatimusten mukainen. Tunnistamisen ja rekisteröinnin jälkeen DCCG-operaattori

— lisää NB_{CSCA}-varmenteen(-varmenteet) luottamusluetteloon, joka on allekirjoitettu $DCCG_{TA}$:n julkista avainta vastaavalla yksityisellä avaimella;

— lisää NB_{TLS}-varmenteen DCCG:n TLS-päätepisteen valkoiseen listaan;

— lisää NB_{UP}-varmenteen DCCG-järjestelmään;

— toimittaa julkisen avaimen $DCCG_{TA}$- ja $DCCG_{TLS}$-varmenteen jäsenvaltiolle.

4.2 *Varmenneviranomaiset, voimassaoloajat ja uusiminen*

Jos jäsenvaltio haluaa käyttää omaa CSCA:aan, CSCA-varmenteet voivat olla itse allekirjoitettuja. Ne toimivat jäsenvaltion luottamusankkurina, ja siksi jäsenvaltion on suojattava vahvasti CSCA-varmenteen julkista avainta vastaava yksityinen avain. On suositeltavaa, että jäsenvaltiot käyttävät CSCA:aan offline-järjestelmää eli tietokonejärjestelmää, jota ei ole liitetty mihinkään verkkoon. Järjestelmään pääsemiseksi on käytettävä usean henkilön suorittamaa valvontaa (esimerkiksi kahden käsittelijän periaatteen mukaisesti). DSC-varmenteiden allekirjoittamisen jälkeen on sovellettava operatiivisia valvontatoimia, ja järjestelmä, jossa yksityistä CSCA-avainta pidetään, on tallennettava turvallisesti siten, että käyttöoikeuksia valvotaan tiukasti. CSCA:n yksityisen avaimen suojaamiseen voidaan käyttää myös laitteistoturvamoduuleja tai älykortteja. Digitaalisilla varmenteilla on voimassaoloaika, joka pakottaa uusimaan varmenteet. Uusiminen on tarpeen, jotta voidaan käyttää uusia salausavaimia ja mukauttaa avainkokoja laskentatehon parantuessa tai kun uudet hyökkäykset uhkaavat käytettävän salausalgoritmin turvallisuutta. Käytetään kuorimallia (ks. *3.2 kohta*).

Digitaalisten koronatodistusten yhden vuoden voimassaoloaika huomioon ottaen suositellaan seuraavia voimassaoloaikoja:

— CSCA: 4 vuotta

— DSC: 2 vuotta

— Lataus: 1–2 vuotta

— TLS-asiakkaan todentaminen: 1–2 vuotta

Jotta uusiminen tapahtuisi hyvissä ajoin, yksityisille avaimille suositellaan seuraavia käyttöaikoja:

— CSCA: 1 vuosi

— DSC: 6 kuukautta

Jotta toiminta olisi sujuvaa, jäsenvaltioiden on luotava uusia latausvarmenteita ja TLS-varmenteita hyvissä ajoin, esimerkiksi kuukausi ennen niiden voimassaolon päättymistä. CSCA- ja DSC-varmenteet olisi uusittava vähintään kuukausi ennen yksityisen avaimen käytön päättymistä (ottaen huomioon tarvittavat operatiiviset menettelyt). Jäsenvaltioiden on toimitettava päivitetyt CSCA-, lataus- ja TLS-varmenteet DCCG-operaattorille. Vanhentuneet varmenteet poistetaan valkoisesta listasta ja luottamusluettelosta.

Jäsenvaltioiden ja DCCG-operaattorin on seurattava omien varmenteidensa voimassaoloa. Ei ole keskustahoa, joka pitää kirjaa varmenteiden voimassaolosta ja ilmoittaa siitä osallistujille.

4.3 *Varmenteiden peruuttaminen*

Yleisesti ottaen digitaaliset varmenteet myöntänyt varmenneviranomainen voi peruuttaa varmenteet käyttämällä varmenteiden sulkulistoja tai verkossa olevaa varmenteen statusprotokollaa (Online Certificate Status Protocol Responder, OCSP). DCC-järjestelmän CSCA:iden olisi toimitettava varmenteiden sulkulistat. Vaikka muut jäsenvaltiot eivät tällä hetkellä käytä näitä sulkulistoja, ne olisi integroitava tuleviin sovelluksiin. Jos CSCA päättää olla toimittamatta varmenteiden sulkulistoja, kyseisen CSCA:n DSC-varmenteet on uusittava, kun sulkulistoista tulee pakollisia. Todentajien ei pitäisi käyttää OCSP:tä DSC-varmenteiden validointiin, vaan niiden olisi käytettävä varmenteiden sulkulistoja. On suositeltavaa, että kansallinen taustajärjestelmä suorittaa DCCG-yhdyskäytävästä ladattujen DSC-varmenteiden tarvittavan validoinnin ja toimittaa edelleen kansallisille DCC-validoijille ainoastaan luotetun ja validoidun joukon DSC-varmenteita. DCC-validoijien ei pitäisi tehdä DSC-varmenteiden peruutuksia koskevia tarkastuksia validointiprosessissaan. Yksi syy tähän on digitaalisten koronatodistusten haltijoiden yksityisyyden suojaaminen välttämällä mahdollisuus, että OCSP-vastaaja voi valvoa tietyn DSC-varmenteen käyttöä.

Jäsenvaltiot voivat itse poistaa DSC-varmenteensa DCCG:stä käyttämällä voimassa olevia lataus- ja TLS-varmenteita. DSC-varmenteen poistaminen tarkoittaa, että kaikista kyseisellä DSC-varmenteella myönnetyistä digitaalisista koronatodistuksista tulee pätemättömiä, kun jäsenvaltiot hakevat päivitetyt DSC-luettelot. DSC-varmenteita vastaavan yksityisen avainaineiston suojaaminen on ratkaisevan tärkeää. Jäsenvaltioiden on ilmoitettava DCCG-operaattorille, jos niiden on peruutettava lataus- tai TLS-varmenteita esimerkiksi kansallisen taustajärjestelmän vaarantumisen vuoksi. DCCG-operaattori voi tämän jälkeen poistaa kyseessä olevaa varmennetta koskevan luottamuksen esimerkiksi poistamalla sen TLS:n valkoisesta listasta. DCCG-operaattori voi poistaa latausvarmenteen DCCG-tietokannasta. Tätä latausvarmennetta vastaavalla yksityisellä avaimella allekirjoitetuista paketeista tulee pätemättömiä, kun kansalliset taustajärjestelmät poistavat peruutetun latausvarmenteen luottamuksen. Jos CSCA-varmenne on peruutettava, jäsenvaltioiden on ilmoitettava asiasta DCCG-operaattorille ja muille jäsenvaltioille, joihin niillä on luottamussuhteita. DCCG-operaattori julkaisee uuden luottamusluettelon, johon kyseessä oleva varmenne ei enää sisälly. Kaikista tämän CSCA:n myöntämistä DSC-varmenteista tulee pätemättömiä, kun jäsenvaltiot päivittävät kansallisen taustajärjestelmänsä luottamussäilön. Jos $DCCG_{TLS}$-varmenne tai $DCCG_{TA}$-varmenne on peruutettava, DCCG-operaattorin ja jäsenvaltioiden on tehtävä yhteistyötä uuden luotetun TLS-yhteyden ja luottamusluettelon luomiseksi.

5. **Varmenteiden mallit**

Tässä jaksossa esitetään salausvaatimukset ja -ohjeet sekä varmenteiden malleja koskevat vaatimukset. DCCG-varmenteiden osalta tässä jaksossa määritellään varmenteiden mallit.

5.1 *Salausvaatimukset*

Salausalgoritmit ja TLS-salausohjelmat valitaan Saksan liittovaltion tietoturvaviraston (BSI) tai SOG-IS:n nykyisen suosituksen perusteella. Nämä suositukset sekä muiden elinten ja standardointiorganisaatioiden suositukset ovat samankaltaisia. Suositukset löytyvät teknisistä ohjeista TR 02102–1 ja TR 02102–2 ([1]) tai SOG-IS:n asiakirjasta *Agreed Cryptographic Mechanisms* ([2]).

5.1.1 DSC-varmennetta koskevat vaatimukset

Sovelletaan *liitteessä I olevassa 3.2.2 kohdassa* säädettyjä vaatimuksia. Siksi on erittäin suositeltavaa, että asiakirjan allekirjoittajat käyttävät elliptisen käyrän digitaalista allekirjoitusalgoritmia (ECDSA) NIST-p-256-käyrällä (siten kuin se on määritelty standardin FIPS PUB 186–4 lisäyksessä D). Muita elliptisiä käyriä ei tueta. Digitaaliseen koronatodistukseen liittyvien tilarajoitusten vuoksi jäsenvaltioiden ei pitäisi käyttää RSA-PSS-allekirjoitusme-

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

netelmää, vaikka se olisikin sallittu vara-algoritmina. Jos jäsenvaltiot käyttävät RSA-PSS-menetelmää, niiden olisi käytettävä moduluskokoa 2048 tai enintään 3072 bittiä. SHA-2-algoritimia, jonka tuloksen pituus ≥ 256 bittiä, on käytettävä DSC-allekirjoituksen salauksen tiivistefunktiona (ks. ISO/IEC 10118–3:2004).

5.1.2 TLS-, lataus- ja CSCA-varmennetta koskevat vaatimukset

DCCG:n yhteydessä käytettävien digitaalisten varmenteiden ja salattujen allekirjoitusten osalta salausalgoritmeja ja avaimen pituutta koskevat keskeiset vaatimukset esitetään tiivistetysti seuraavassa taulukossa (vuodesta 2021 alkaen):

Allekirjoitusalgoritmi	Avaimen koko	Tiivistefunktio
EC-DSA	Vähintään 250 bittiä	SHA-2; tiivisteen pituus ≥ 256 bittiä
RSA-PSS (suositeltu täyte) RSA-PKCS#1 v1.5 (vanha täyte)	Vähintään 3000 bitin RSA Modulus (N) julkisella eksponentilla e > 2^16	SHA-2; tiivisteen pituus ≥ 256 bittiä
DSA	Vähintään 3000 bitin alkuluku p, 250 bitin avain q	SHA-2; tiivisteen pituus ≥ 256 bittiä

EC-DSA:n suositeltava elliptinen käyrä on NIST-p-256 sen laajan käytön vuoksi.

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

Seuraavassa taulukossa annetaan ohjeita NB_{CSCA}-varmenteen mallista, jos jäsenvaltio päättää käyttää omaa CSCA:aan DCC-järjestelmää varten.

Lihavoidut merkinnät ovat pakollisia (niiden on sisällyttävä varmenteeseen), *kursivoidut* merkinnät ovat suositeltavia (niiden olisi sisällyttävä varmenteeseen). Puuttuvia kenttiä varten ei ole määritelty suosituksia.

Kenttä	Arvo
Subject	**cn=<ei-tyhjä ja yksilöivä yleisnimi>,***o=<Tarjoaja>*,**c=<CSCA:ta käyttävä jäsenvaltio>**
Key usage	**certificate signing,***CRL signing* (vähintään)
Basic Constraints	**CA = true, path length constraints = 0**

Aiheen nimen on oltava ei-tyhjä ja yksilöivä kyseisessä jäsenvaltiossa. Maakoodin c on vastattava sitä jäsenvaltiota, joka käyttää tätä CSCA-varmennetta. Varmenteessa on oltava standardin RFC 5280 ([3]) mukainen yksilöivä aihe-avaimen tunniste (Subject Key Identifier, SKI).

5.3 *Asiakirjan allekirjoittajan varmenne (DSC)*

Seuraavassa taulukossa annetaan DSC-varmennetta koskevia ohjeita. **Lihavoidut** merkinnät ovat pakollisia (niiden on sisällyttävä varmenteeseen), *kursivoidut* merkinnät ovat suositeltavia (niiden olisi sisällyttävä varmenteeseen). Puuttuvia kenttiä varten ei ole määritelty suosituksia.

Kenttä	Arvo
Serial Number	**unique serial number**
Subject	**cn=<ei-tyhjä ja yksilöivä yleisnimi>,***o=<Tarjoaja>*,**c=<tätä DSC:tä käyttävä jäsenvaltio>**
Key Usage	**digital signature** (vähintään)

([3]) rfc5280 (ietf.org)

DSC-varmenne on allekirjoitettava jäsenvaltion käyttämää CSCA-varmennetta vastaavalla yksityisellä avaimella.

Seuraavia laajennuksia on käytettävä:

— Varmenteessa on oltava viranomaisen avaimen tunniste (Authority Key Identifier, AKI), joka vastaa myöntävän CSCA-varmenteen aihe-avaimen tunnistetta (SKI).

— Varmenteessa olisi oltava yksilöivä aihe-avaimen tunniste (standardin RFC 5280 ([4]) mukaisesti).

Varmenteen olisi lisäksi sisällettävä CRL-jakelupisteen laajennus, joka viittaa DSC-varmenteen myöntäneen CSCA:n toimittamaan varmenteiden sulkulistaan (CRL).

DSC voi sisältää laajennettua avaimen käyttöä koskevan laajennuksen, jossa on nolla tai useampia avaimen käyttökäytäntöjen tunnisteita, jotka rajoittavat niitä HCERT-tyyppejä, joita tällä varmenteella saa todentaa. Jos tunnisteita on yksi tai useampi, todentajien on todennettava avaimen käyttö suhteessa tallennettuun HCERT-todistukseen. Tätä varten määritellään seuraavat extendedKeyUsage-arvot:

Kenttä	Arvo
extendedKeyUsage	1.3.6.1.4.1.1847.2021.1.1 Testaustodistusten myöntäjille
extendedKeyUsage	1.3.6.1.4.1.1847.2021.1.2 Rokotustodistusten myöntäjille
extendedKeyUsage	1.3.6.1.4.1.1847.2021.1.3 Parantumistodistusten myöntäjille

Jos avaimen käytön laajennuksia ei ole (eli ei laajennuksia tai nolla laajennusta), tätä varmennetta voidaan käyttää minkä tahansa tyyppisen HCERT-todistuksen validoimiseen. Muissa asiakirjoissa voidaan määritellä HCERT-todistusten validoinnissa käytettäviä asiaankuuluvia laajennettujen avaimen käyttökäytäntöjen tunnisteita.

5.4 *Latausvarmenteet (NB_{UP})*

Seuraavassa taulukossa annetaan kansallisen taustajärjestelmän latausvarmennetta koskevia ohjeita. **Lihavoidut** merkinnät ovat pakollisia (niiden on sisällyttävä varmenteeseen), *kursivoidut* merkinnät ovat suositeltavia (niiden olisi sisällyttävä varmenteeseen). Puuttuvia kenttiä varten ei ole määritelty suosituksia.

Kenttä	Arvo
Subject	**cn=<ei-tyhjä ja yksilöivä yleisnimi>,***o=<Tarjoaja>*,**c=<tätä latausvarmennetta käyttävä jäsenvaltio>**
Key Usage	**digital signature** (vähintään)

5.5 *Kansallisen taustajärjestelmän TLS-asiakkaan todentaminen (NB_{TLS})*

Seuraavassa taulukossa annetaan kansallisen taustajärjestelmän TLS-asiakkaan todentamisvarmennetta koskevia ohjeita. **Lihavoidut** merkinnät ovat pakollisia (niiden on sisällyttävä varmenteeseen), *kursivoidut* merkinnät ovat suositeltavia (niiden olisi sisällyttävä varmenteeseen). Puuttuvia kenttiä varten ei ole määritelty suosituksia.

Kenttä	Arvo
Subject	**cn=<ei-tyhjä ja yksilöivä yleisnimi>,***o=<Tarjoaja>*, **c=<taustajärjestelmän jäsenvaltio>**
Key Usage	**digital signature** (vähintään)
Extended key usage	client authentication (1.3.6.1.5.5.7.3.2)

([4]) rfc5280 (ietf.org)

Varmenne voi sisältää myös *palvelimen todentamista (1.3.6.1.5.5.7.3.1)* koskevan laajennetun avaimen käytön, mutta sitä ei vaadita.

5.6 *Luottamusluettelon allekirjoitusvarmenne ($DCCG_{TA}$)*

Seuraavassa taulukossa määritellään DCCG:n luottamusankkurin varmenne.

Kenttä	Arvo
Subject	**cn = Digital Green Certificate Gateway** ([5])**, o=<Tarjoaja>, c=<maa>**
Key Usage	**digital signature** (vähintään)

5.7 *DCCG:n TLS-palvelinvarmenteet ($DCCG_{TLS}$)*

Seuraavassa taulukossa määritellään DCCG:n TLS-palvelinvarmenne.

Kenttä	Arvo
Subject	cn=<DCCG:n FQDN tai IP-osoite>, o=<Tarjoaja>, c= <maa>
SubjectAltName	dNSName: <DCCG:n DNS-nimi> tai iPAddress: <DCCG:n IP-osoite>
Key Usage	**digital signature** (vähintään)
Extended Key usage	server authentication (1.3.6.1.5.5.7.3.1)

Varmenne voi sisältää myös *asiakkaan todentamista (1.3.6.1.5.5.7.3.2)* koskevan laajennetun avaimen käytön, mutta sitä ei vaadita.

DCCG:n TLS-varmenteen myöntää julkisesti luotettu varmenneviranomainen (sisältyy kaikkiin tärkeimpiin selaimiin ja käyttöjärjestelmiin CA Browser Forumin perusvaatimusten mukaisesti).

([5]) Tässä yhteydessä käytetään edelleen ilmausta ”digitaalinen vihreä todistuta” ilmauksen ”EU:n digitaalinen koronatodistus” sijasta, koska tämä terminologia on kovakoodattu ja otettu käyttöön todistuksessa ennen kuin lainsäätäjät päättivät uudesta terminologiasta.