KOMISJONI RAKENDUSOTSUS (EL) 2021/1073,

28. juuni 2021,

millega kehtestatakse ELi digitaalse COVID-tõendi usaldusraamistiku (mis loodi Euroopa Parlamendi ja nõukogu määrusega (EL) 2021/953) kasutuselevõtu tehnilised spetsifikatsioonid ja normid

(EMPs kohaldatav tekst)

EUROOPA KOMISJON,

võttes arvesse Euroopa Liidu toimimise lepingut,

võttes arvesse Euroopa Parlamendi ja nõukogu määrust (EL) 2021/953, millega kehtestatakse koostalitlusvõimeliste COVID-19 vaktsineerimis-, testimis- ja läbipõdemistõendite (ELi digitaalne COVID-tõend) väljaandmise, kontrollimise ja aktsepteerimise raamistik, et hõlbustada vaba liikumist COVID-19 pandeemia ajal, ([1]) eriti selle artikli 9 lõikeid 1 ja 3,

ning arvestades järgmist:

(1) Määrusega (EL) 2021/953 kehtestatakse ELi digitaalne COVID-tõend, mille eesmärk on tõendada, et isik on COVID-19 vastu vaktsineeritud, tal on olemas negatiivne testitulemus või ta on nakkuse läbi põdenud.

(2) Selleks et ELi digitaalne COVID-tõend toimiks kõikjal liidus, tuleb kehtestada tehnilised spetsifikatsioonid ja normid, mis käsitlevad digitaalsete COVID-tõendite andmetega täitmist, turvalist väljastamist ja kontrolli, isikuandmete kaitse tagamist, tõendi kordumatu tunnuse ühtse struktuuri kehtestamist ning kehtiva, turvalise ja koostalitlusvõimelise vöötkoodi väljastamist. Selline usaldusraamistik loob muu hulgas aluse püüdele tagada koostalitlusvõime rahvusvaheliste standardite ja tehnoloogiliste süsteemidega ning võiks seeläbi olla eeskujuks üleilmsele koostööle.

(3) Selleks et ELi digitaalset COVID-tõendit oleks võimaliku lugeda ja tõlgendada, on vaja ühtset andmestruktuuri ning kokkulepet lasti kõigi andmeväljade kavandatud tähenduse ja nende võimalike väärtuste kohta. Et sellist koostalitlusvõimet soodustada, tuleb määratleda ühtne kooskõlastatud andmestruktuur, mille raames ELi digitaalne COVID-tõend toimib. Nimetatud raamistiku suunised töötas välja Euroopa Parlamendi ja nõukogu direktiivi 2011/24/EL ([2]) alusel loodud e-tervise võrgustik. Nende suunistega tuleks arvestada, koostades tehnilised spetsifikatsioonid, milles on sätestatud ELi digitaalse COVID-tõendi vorming ja selle usaldusteenuste haldus. Kehtestada tuleks andmestruktuuri spetsifikatsioon ja kodeerimismehhanismid, samuti kodeerimismehhanism andmete edastamiseks masinloetavas optilises vormingus (QR-kood), mida saab kuvada mobiilseadme ekraanil või trükkida paberile.

(4) Lisaks ELi digitaalse COVID-tõendi vormingu ja usaldusteenuste halduse tehnilistele spetsifikatsioonidele tuleks kehtestada üldised normid tõendite andmetega täitmise kohta, et kasutada neid ELi digitaalse COVID-tõendi sisu kodeeritud väärtuste puhul. Komisjon peaks nimetatud normide kohaseid väärtuste kogumeid e-tervise võrgustiku tööle tuginedes korrapäraselt uuendama ja avalikustama.

(5) Vastavalt määrusele (EL) 2021/953 peaks iga ELi digitaalse COVID-tõendi koosseisu kuuluv ehtne tõend olema tõendi kordumatu tunnuse abil eraldi tuvastatav, kuna kodanikele võib määruse (EL) 2021/953 jõusoleku jooksul olla väljastatud rohkem kui üks tõend. Tõendi kordumatu tunnus peab koosnema tärgistringist ja liikmesriigid peaksid tagama, et see ei sisalda andmeid, mis seostaksid seda teiste dokumentide või tunnustega, nagu passi või isikutunnistuse numbrid, et takistada võimalust omanik kindlaks teha. Selleks et tagada tõendi tunnuse kordumatus, tuleks kehtestada selle ühtse struktuuri tehnilised spetsifikatsioonid ja normid.

([1]) ELT L 211, 15.6.2021, lk 1.

([2]) Euroopa Parlamendi ja nõukogu 9. märtsi 2011. aasta direktiiv 2011/24/EL patsiendiõiguste kohaldamise kohta piiriüleses tervishoius (ELT L 88, 4.4.2011, lk 45).

(6) Et ELi digitaalse COVID-tõendi moodustavaid tõendeid aktsepteeritaks kõigis liikmesriikides, on keskse tähtsusega nende turvalisus, ehtsus, kehtivus ja terviklus ning kooskõla liidu andmekaitsealaste õigusaktidega. See eesmärk saavutatakse usaldusraamistikuga, millega nähakse ette reeglid ja taristu ELi digitaalse COVID-tõendi usaldusväärseks ja turvaliseks väljastamiseks ja kontrolliks. Usaldusraamistik peaks muu hulgas põhinema avaliku võtme taristul, mille usaldusahel ulatub liikmesriikide tervishoiuasutustest või muudest usaldusväärsetest asutustest ELi digitaalseid COVID-tõendeid väljastavate üksusteni. Eesmärgiga tagada üleeuroopaline koostalitlusvõime süsteem on komisjon niisiis loonud kesksüsteemi (ELi digitaalse COVID-tõendi lüüs, edaspidi „lüüs"), kus säilitatakse kontrolliks kasutatavaid avalikke võtmeid. QR-koodi skaneerimisel kontrollitakse digiallkirja asjaomase avaliku võtmega, mis on eelnevalt nimetatud kesklüüsi salvestatud. Digiallkirju saab kasutada andmete tervikluse ja ehtsuse tagamiseks. Avalike võtmete ja tõendite väljastajate sidumisega loovad avaliku võtme taristud usaldusväärsuse. Lüüs kasutab autentimiseks mitut digitaalsertifikaati. Selleks et tagada avalike võtmete andmete turvaline vahetamine liikmesriikide vahel ja võimaldada laialdast koostalitlusvõimet, tuleb ette näha see, milliseid digitaalsertifikaate tohib kasutada ja kuidas need tuleks genereerida.

(7) Käesolev otsus võimaldab määruse (EL) 2021/953 nõudeid rakendada viisil, millega vähendatakse isikuandmete töötlemist ELi digitaalse COVID-tõendi toimimiseks vajaliku miinimumini ja mis aitab vastutavatel lõpptöötlejatel neid kohaldada lõimitud andmekaitse põhimõtet järgides.

(8) Määruse (EL) 2021/953 kohaselt on tõendite väljastamise eest vastutavad ametiasutused või muud määratud asutused väljastamise kestel isikuandmete töötleja rolli täites Euroopa Parlamendi ja nõukogu määruse (EL) 2016/679 ([3]) artikli 4 lõikes 7 osutatud vastutavad töötlejad. Sõltuvalt sellest, kuidas liikmesriigid väljastamise korraldavad, võib ametiasutusi või määratud asutusi olla üks või rohkem (näiteks piirkondlikud tervishoiuteenistused). Kooskõlas subsidiaarsuse põhimõttega otsustavad selle üle liikmesriigid. Seega suudavad liikmesriigid kõige paremini tagada, et kui ametiasutusi või muid määratud asutusi on mitu, on neist igaühe vastutus selgelt määratletud sõltumata sellest, kas vastutavad töötlejad on eraldiseisvad või kaasvastutavad (sealhulgas juhul kui piirkondlikud tervishoiuteenistused loovad tõendite väljastamiseks ühise patsiendiportaali). Lisaks sellele peavad seoses tõendite kontrollimisega andmekaitse-eeskirjadest neile tulenevaid kohustusi täitma siht- või transiitliikmesriigi pädevad asutused või piiriülese reisijateveo teenuse osutajad, kes peavad riigisisese õiguse kohaselt rakendama COVID-19 pandeemia ajal teatavaid rahvatervisealaseid meetmeid.

(9) Isikuandmeid ei töödelda ELi digitaalse COVID-tõendi lüüsi kaudu, kuna see sisaldab ainult allkirjastavate asutuste avalikke võtmeid. Need võtmed on seotud allkirjastavate asutustega ja ei võimalda otse ega kaudselt taastuvastada füüsilist isikut, kellele tõend on väljastatud. Komisjon kui lüüsi haldaja ei peaks seega olema ei isikuandmete vastutav ega volitatud töötleja.

(10) Vastavalt Euroopa Parlamendi ja nõukogu määruse (EL) 2018/1725 ([4]) artikli 42 lõikele 1 konsulteeriti Euroopa Andmekaitseinspektoriga, kes esitas oma arvamuse 22. juunil 2021.

(11) Kuna tehnilised spetsifikatsioonid ja normid on vajalikud määruse (EL) 2021/953 kohaldamise alustamiseks 1. juulil 2021, on õigustatud, et käesolev otsus on viivitamata kohaldatav.

(12) Arvestades niisiis vajadust võtta ELi digitaalne COVID-tõend kiiresti kasutusele, peaks käesolev otsus jõustuma selle avaldamise päeval,

([3]) Euroopa Parlamendi ja nõukogu 27. aprilli 2016. aasta määrus (EL) 2016/679 füüsiliste isikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise ning direktiivi 95/46/EÜ kehtetuks tunnistamise kohta (isikuandmete kaitse üldmäärus) (ELT L 119, 4.5.2016, lk 1).

([4]) Euroopa Parlamendi ja nõukogu 23. oktoobri 2018. aasta määrus (EL) 2018/1725, mis käsitleb füüsiliste isikute kaitset isikuandmete töötlemisel liidu institutsioonides, organites ja asutustes ning isikuandmete vaba liikumist, ning millega tunnistatakse kehtetuks määrus (EÜ) nr 45/2001 ja otsus nr 1247/2002/EÜ (ELT L 295, 21.11.2018, lk 39).

ON VASTU VÕTNUD KÄESOLEVA OTSUSE:

Artikkel 1

I lisas on esitatud ELi digitaalse COVID-tõendi tehnilised spetsifikatsioonid, millega kehtestatakse üldine andmestruktuur, kodeerimismehhanismid ja kodeerimismehhanism andmete edastamiseks masinloetavas optilises vormingus.

Artikkel 2

Käesoleva otsuse II lisas on esitatud nõuded määruse (EL) 2021/953 artikli 3 lõikes 1 osutatud tõendite andmetega täitmise kohta.

Artikkel 3

III lisas on esitatud normid, millega kehtestatakse tõendi kordumatu tunnuse ühtne struktuur.

Artikkel 4

IV lisas on esitatud eeskirjad, mida kohaldatakse digitaalsertifikaatide haldamise suhtes seoses ELi digitaalse COVID-tõendi lüüsi usaldusraamistiku koostalitlusvõimet toetavate aspektidega.

Käesolev otsus jõustub *Euroopa Liidu Teatajas* avaldamise päeval.

Brüssel, 28. juuni 2021

Komisjoni nimel
president
Ursula VON DER LEYEN

I LISA

VORMING JA USALDUSTEENUSTE HALDUS

Üldine andmestruktuur, kodeerimismehhanismid ja kodeerimismehhanism andmete edastamiseks masinloetavas optilises vormingus (edaspidi „QR-kood“))

1. Sissejuhatus

Käesolevas lisas esitatud tehnilised spetsifikatsioonid hõlmavad ELi digitaalse COVID-tõendi üldist andmestruktuuri ja kodeerimismehhanisme. Samuti on sellega kindlaks määratud kodeerimissüsteem andmete edastamiseks masinloetavas optilises vormingus (edaspidi „QR-kood“), mida saab kuvada mobiilseadme ekraanil või trükkida paberile. Käesolevates spetsifikatsioonides on elektroonilise tervisetõendi puhul käibel konteinerite argivormingud, mida selles kontekstis kasutatakse ELi digitaalse COVID-tõendi kanduritena.

2. Terminoloogia

Käesolevas lisas tähendab „väljastajad“ organisatsioone, kes kasutavad nimetatud spetsifikatsioone tervisetõendite väljastamiseks, ja „kontrollijad“ organisatsioone, kes aktsepteerivad tervisetõendeid tõendina tervisliku seisundi kohta. „Osalejad“ tähendab väljastajaid ja kontrollijaid. Osalejad peavad omavahel kooskõlastama teatavaid käesolevas lisas esitatud aspekte, nagu nimeruumi haldamine ja krüptovõtmete jaotamine. Eelduste kohaselt täidab neid ülesandeid konkreetne üksus (edaspidi „sekretariaat“).

3. Elektroonilise tervisetõendi konteineri vorming

Elektroonilise tervisetõendi konteineri vorming (Electronic Health Certificate Container Format, edaspidi „HCERT“) on välja töötatud selleks, et anda tervisetõendite eri väljastajate (edaspidi „väljastajad“) käsutusse ühetaoline ja standarditud vahend nende edastamiseks. Spetsifikatsioonide eesmärk on lihtsustada nende tõendite esitamist, kodeerimist ja allkirjastamist, et suurendada koostalitlusvõimet.

Selleks et ELi digitaalset COVID-tõendit saaks lugeda ja tõlgendada kõik väljastajad, on vaja ühtset andmestruktuuri ning kokkulepet lasti kõigi andmeväljade tähenduse kohta. Sellise koostalitlusvõime suurendamiseks määratletakse ühine ühtne andmestruktuur, kasutades ELi digitaalse COVID-tõendi raamistikuna JSON-skeemi.

3.1. *Lasti ülesehitus*

Last ehitatakse üles ja kodeeritakse CBOR-kujul COSE-vormingus digiallkirjaga. Selle üldnimetus on „CBOR Web Token“ (edaspidi „CWT“), mis on määratletud dokumendis RFC 8392 ([1]). Järgmistes lõikudes määratletud lasti transporditakse hcert väitena.

Kontrollijal peab olema võimalik kontrollida lasti terviklust ja ehtsust. Selle mehhanismi kättesaadavaks tegemiseks peab väljastaja CWT allkirjastama, kasutades asümmeetrilist e-allkirja süsteemi, nagu see on määratletud COSE spetsifikatsioonis RFC 8152 ([2]).

3.2. *CWT väited*

3.2.1. Ülevaade CWT struktuurist

Kaitstud päis

— Allkirja algoritm (alg, märgend 1)

— Võtmeidentifikaator (kid, märgend 4)

Last

— Väljastaja (iss, väitevõti 1, ei ole kohustuslik, väljastaja ISO 3166-1 alpha-2)

— Väljastusaeg (iat, väitevõti 6)

— Aegumisaeg (exp, väitevõti 4)

— Tervisetõend (hcert, väitevõti −260)

— ELi digitaalne COVID-tõend v1 (eu_DCC_v1, väitevõti 1)

Allkiri

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

3.2.2. Allkirja algoritm

Parameeter „allkirja algoritm“ (alg) näitab seda, millist algoritmi allkirja loomiseks kasutatakse. See peab vastama järgmistes lõikudes lühidalt kokku võetud kehtivate SOG-IS suuniste nõuetele või neid ületama.

Määratletakse üks primaarne ja üks sekundaarne algoritm. Sekundaarset algoritmi tuleks kasutada ainult juhul, kui primaarne algoritm ei ole väljastajale kehtestatud eeskirjade kohaselt aktsepteeritav.

Süsteemi turvalisuse tagamiseks peavad kõik rakendused hõlmama sekundaarset algoritmi. Sel põhjusel tuleb kasutusele võtta nii primaarne kui ka sekundaarne algoritm.

SOG-ISiga on kehtestatud primaarsete ja sekundaarsete algoritmide jaoks järgmised tasemed.

— Primaarne algoritm: primaarne algoritm on standardi (ISO/IEC 14888–3:2006) jaotises 2.3 määratletud elliptiliste kõverate digiallkirja algoritm (Elliptic Curve Digital Signature Algorithm, ECDSA), kasutades standardi (FIPS PUB 186–4) D lisas (D.1.2.3) määratletud P–256 parameetreid koos standardi (ISO/IEC 10118–3:2004) funktsioonis 4 määratletud SHA–256 räsialgoritmiga.

See vastab COSE algoritmi parameetrile ES256.

— Sekundaarne algoritm: sekundaarne algoritm on dokumendis RFC 8230 ([3]) määratletud RSASSA-PSS koos 2048 bitise mooduliga kombinatsioonis standardi (ISO/IEC 10118–3:2004) funktsioonis 4 määratletud SHA–256 räsialgoritmiga.

See vastab COSE algoritmi parameetrile PS256.

3.2.3. Võtmeidentifikaator

Väide „võtmeidentifikaator“ (kid) näitab dokumendi allkirjastaja sertifikaati (DSC), mis sisaldab avalikku võtit, mida kontrollija peab kasutama digiallkirja õigsuse kontrollimiseks. Digitaalsertifikaatide haldust, sealhulgas DSCdele esitatavaid nõudeid, on kirjeldatud IV lisas.

Kontrollijad kasutavad väidet „võtmeidentifikaator“ (kid) selleks, et valida väljastaja (iss) väitega seotud väljastajale kuuluvate võtmete loetelust õige avalik võti. Halduslikel põhjustel ja võtmete asendamise (rollover) korral võib väljastaja kasutada paralleelselt mitut võtit. Võtmeidentifikaator ei ole turvalisuse seisukohast kriitiline väli. Seetõttu võidakse see paigutada ka kaitsmata päisesse. Kontrollijad peavad aktsepteerima mõlemat varianti. Kui olemas on mõlemad, tuleb kasutada kaitstud päises olevat võtmeidentifikaatorit.

Kuna identifikaatorit on lühendatud (piiratud ruumi tõttu), on väike, kuid siiski eksisteeriv võimalus, et kontrollija poolt heaks kiidetud dokumendi allkirjastaja sertifikaatide (Document Signer Certificates, edaspidi „DSC“) üldises loetelus leidub DSCsid, millel on sama kid. Sel põhjusel peab kontrollija kontrollima kõiki DSCsid, milles on asjaomane kid.

3.2.4. Väljastaja

Väide „väljastaja“ (iss) on string, mis võib valikuliselt sisaldada tervisetõendit väljastava üksuse ISO 3166-1 alpha-2 riigikoodi. Kontrollija saab seda väidet kasutada, et teha kindlaks, millist DSCde kogumit kontrolliks kasutada. Selle väite identifitseerimiseks kasutatakse väitevõtit 1.

3.2.5. Aegumisaeg

Väide „aegumisaeg“ (exp) peab sisaldama täisarvuna esitatud ajatemplit NumericDate-vormingus (vastavalt dokumendi RFC 8392 ([4]) jaotisele 2), mis näitab, kui kaua tuleb lasti seda konkreetset allkirja pidada kehtivaks (aeg, mille möödumisel peab kontrollija lasti tagasi lükkama kui aegunu). Aegumisparameetri eesmärk on piiritleda periood, mille jooksul tervisetõend kehtib. Selle väite identifitseerimiseks kasutatakse väitevõtit 4.

Aegumisaeg ei tohi ületada DSC kehtivusaega.

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

3.2.6. Väljastusaeg

Väide „väljastusaeg“ (iat) peab sisaldama täisarvuna esitatud ajatemplit NumericDate-vormingus (vastavalt dokumendi RFC 8392 ([5]) jaotisele 2), mis näitab aega, kui tervisetõend loodi.

Välja „väljastusaeg“ väärtus ei tohi olla varasem kui DSC kehtivusaja algus.

Kontrollijad võivad kohaldada täiendavaid tegevuspõhimõtteid, et piirata tervisetõendi kehtivust väljastamisaja alusel. Selle väite identifitseerimiseks kasutatakse väitevõtit 6.

3.2.7. Väide „tervisetõend“

Väide „tervisetõend“ (hcert) on dokumendi RFC 7159 ([6]) kohane JSON-vormingus objekt, mis sisaldab teavet tervisliku seisundi kohta. Üks ja sama väide võib hõlmata mitut tervisetõendit, millest üks on digitaalne COVID-tõend.

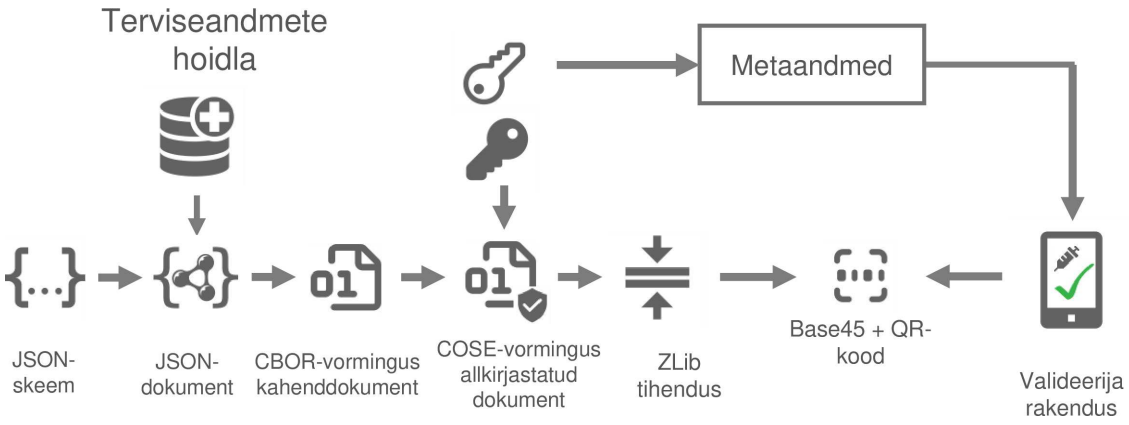
JSON on mõeldud pelgalt skeemi määratlusena. Edastamisvorming on dokumendis RFC 7049 ([7]) määratletud CBOR. Rakenduste arendajad ei pruugi tegelikkuses JSON-vormingus esitatud andmeid üldse dekodeerida ega kodeerida – selle asemel kasutavad nad mälus olevat struktuuri.

Selle väite identifitseerimiseks tuleb kasutada väitevõtit –260.

JSON-vormingus objektide stringid tuleks normaliseerida vastavalt Unicode standardis määratletud NFC-le (Normalization Form Canonical Composition). Samas peaksid dekodeerimisrakendused olema neis aspektides sallivad ja töökindlad ning tungivalt soovitatakse aktsepteerida kõiki teisendusviise. Kui dekodeerimisel või järgnevate võrdlusfunktsioonide kestel leitakse normaliseerimata andmeid, peaksid rakendused käituma nii, nagu oleks sisend NFC järgi normaliseeritud.

4. DCC lasti jadastamine ja loomine

Jadastamismallina kasutatakse järgmist skeemi.



Protsess algab andmete ekstraheerimisega (näiteks terviseandmete hoidlast või mõnest välisest andmeallikast), struktureerides ekstraheeritud andmed digitaalse COVID-tõendi jaoks määratletud skeemide kohaselt. Selle protsessi käigus võib teisendamine kindlaksmääratud andmevormingusse ja inimloetavaks muutmine toimuda enne CBOR-vormingusse jadastamise algust. Igal juhul toimub enne jadastamist ja pärast objektimist väite akronüümide vastandamine kuvatavatele nimedele.

Määruse (EL) 2021/953 ([8]) kohaselt väljastatud tõendites ei ole lubatud riiklik valikuline andmesisu. Andmesisu on piiratud määruse 2021/953 lisas loetletud miinimumandmete kindlaksmääratud andmeelementidega.

([5]) rfc8392 (ietf.org)
([6]) rfc7159 (ietf.org)
([7]) rfc7049 (ietf.org)
([8]) Euroopa Parlamendi ja nõukogu 14. juuni 2021. aasta määrus (EL) 2021/953, millega kehtestatakse koostalitlusvõimeliste COVID-19 vaktsineerimis-, testimis- ja läbipõdemistõendite (ELi digitaalne COVID-tõend) väljaandmise, kontrollimise ja aktsepteerimise raamistik, et hõlbustada vaba liikumist COVID-19 pandeemia ajal (ELT L 211, 15.6.2021, lk 1).

5. **Kodeerimissüsteem andmete edastamiseks**

5.1. *Toorkodeering*

Eri andmeliideste puhul võib HCERTi konteineri ja selle lastid edastada muutmata kujul, kasutades ükskõik millist olemasolevat 8-bitist, turvalist ja usaldusväärset andmeedastust. Nende liideste hulgas võivad olla lähiväljaside (NFC), Bluetooth või edastus rakenduskihi protokolli kaudu, näiteks kui väljastaja edastab HCERTi selle omaja mobiilseadmesse.

Kui väljastaja edastab HCERTi selle omajale ainult kuvamiskihti sisaldava liidese kaudu (näiteks SMSi või e-kirjaga), ei ole toorkodeering loomulikult kohaldatav.

5.2. *Vöötkood*

5.2.1. Lasti (CWT) tihendus

Et vähendada HCERTi mahtu ning suurendada selle lugemisprotsessi kiirust ja usaldusväärsust, kasutatakse CWT tihendamisel ZLIB-vormingut (RFC 1950 ([9])) ja Deflate tihendusmehhanismi dokumendis (RFC 1951 ([10])) määratletud vormingus.

5.2.2. QR 2D vöötkood

ASCII lastidega toimivate pärandseadmete paremaks haldamiseks kodeeritakse tihendatud CWT enne 2D vöötkoodiks kodeerimist Base45 koodi kasutades ASCIIsse.

2D vöötkoodi genereerimiseks kasutatakse standardis (ISO/IEC 18004:2015) määratletud QR-vormingut. Soovituslik veaparandustase on Q (umbes 25 %). Tulenevalt Base45 kasutamisest tuleb QR-koodis kasutada tärkkoodi (Mode 2, mida näitavad sümbolid 0010).

Selleks et kontrollijad saaksid kindlaks teha kodeeritud andmete liigi ning valida kohase dekodeerimis- ja töötlusskeemi, lisatakse Base45ga kodeeritud andmete (käesoleva spetsifikatsiooni kohaselt) ette kontekstituvastusstring „HC1:“. Selle spetsifikatsiooni tulevastes tagasiühilduvust mõjutavates versioonides määratletakse uus kontekstiidentifikaator, milles ühendile „HC“ järgnev tärk valitakse tärgistikust [1–9A–Z]. Sammud tehakse seda järjestust järgides, st kõigepealt [1–9] ja seejärel [A–Z].

Soovitatav on ilmestada koodi optiline kujutis esitusmeediumis diagonaali pikkusega 35 mm kuni 60 mm, et seda saaks kasutada liikumatu optikaga lugemisseadmetes, kui esitusmeedium peab asuma lugemisseadme pinnal.

Kui koodi optiline kujutis trükitakse paberile, kasutades väikese eraldusvõimega (< 300 dpi) printerit, tuleb hoolitseda selle eest, et kõik QR-koodi sümbolid (punktid) oleksid täpselt ruudukujulised. Kui mastabeerimine on ebavõrdeline, on mõnede QR-koodi ridade või veergude sümbolid ristkülikukujulised, mis halvendab paljudel juhtudel loetavust.

6. **Usaldusloetelu vorming (CSCA sertifikaatide ja DSCde loetelu)**

Kõik liikmesriigid peavad esitama loetelu ühe või mitme riikliku allkirjastamise sertimiskeskuse (Country Signing Certification Authority, edaspidi „CSCA“) ja loetelu kõigi kehtivate dokumentide allkirjastaja sertifikaatide (Document Signer Certificate, edaspidi „DSC“) kohta ning neid loetelusid ajakohastama.

6.1. *Lihtsustatud CSCA/DSC*

Alates spetsifikatsioonide sellest versioonist ei eelda liikmesriigid, et kasutatakse ükskõik millise tühistatud sertifikaatide loendi (Certificate Revocation List, edaspidi „CRL“) teavet või et teostajad kontrollivad privaatvõtme kasutamisperioodi.

Selle asemel on esmane meetod kehtivuse kontrolliks sertifikaadi olemasolu kõnealuse sertifikaatide loetelu uusimas versioonis.

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

6.2. *Rahvusvahelise Tsiviillennunduse Organisatsiooni (ICAO) elektrooniliselt masinloetavate reisidokumentide (eMRTD) avaliku võtme taristu (PKI) ja usalduskeskused*

Liikmesriigid võivad kasutada eraldi CSCAd, kuid võivad samuti esitada oma kehtivad elektrooniliselt masinloetavate reisidokumentide (edaspidi „eMRTD“) CSCA-sertifikaadid ja/või DSCd; neil on isegi võimalus otsustada hankida need (äriühingutest) usalduskeskustelt ja need esitada. Samas peab kõik DSCd allkirjastama asjaomase liikmesriigi poolt teatatud CSCA.

7. **Turvakaalutlused**

Kui liikmesriigid töötavad välja käesolevat spetsifikatsiooni kasutavat skeemi, peavad nad teatavad turvalisusega seotud aspektid määratlema ning neid analüüsima ja jälgima.

Minimaalselt tuleks arvesse võtta järgmisi aspekte.

7.1. *HCERTi allkirja kehtivusaeg*

HCERTide väljastaja peab piirama allkirja kehtivusaega, määrates kindlaks selle aegumisaja. Seega peab tervisetõendi omaja seda korrapäraste ajavahemike järel uuendama.

Vastuvõetava kehtivusaja võivad ära määrata praktilised asjaolud. Näiteks reisijal ei pruugi olla võimalust uuendada tervisetõendit välisreisi kestel. Teisalt aga võib näiteks juhtuda nii, et väljastaja peab võimalikuks mõnd turvariket, mistõttu väljastaja peab DSC tühistama (muutes kehtetuks kõik seda võtit kasutades väljastatud tervisetõendid, ehkki võtme kehtivusaeg ei ole lõppenud). Sellise juhtumi mõju võib vähendada sellega, et korrapäraselt asendatakse väljastaja võtmeid ja nõutakse, et kõiki tervisetõendeid mõistlike ajavahemike järel uuendataks.

7.2. *Võtmehaldus*

See spetsifikatsioon kasutab andmete tervikluse tagamiseks ja andmete päritolu autentimiseks ennekõike tugevaid krüptograafiamehhanisme. Seega on vaja säilitada privaatvõtmete konfidentsiaalsus.

Krüptovõtmete konfidentsiaalsust on võimalik rikkuda mitmel eri viisil, näiteks:

— võtme genereerimisprotsessis võib tekkida viga, mistõttu võtmed on nõrgad;

— võtmed võidakse avalikustada inimliku eksimuse tõttu;

— organisatsiooni kuuluv või selle väline isik võib võtmed varastada;

— võtmed võidakse välja arvutada krüptoanalüüsi kasutades.

Leevendamaks riski, et allkirjastamise algoritm osutub nõrgaks, mistõttu privaatvõtmeid on võimalik murda krüptoanalüüsiga, soovitatakse käesolevas spetsifikatsioonis kõigil osalejatel rakendada sekundaarne allkirjastamise algoritm (varuvariant), mis tugineb muudele parameetritele või teistsugusele matemaatilisele probleemile kui primaarne algoritm.

Seoses nimetatud riskidega, mis on seotud väljastajate tegevuskeskkonnaga, tuleb tulemusliku kontrolli eesmärgil rakendada selliseid leevendusmeetmeid nagu privaatvõtmete genereerimine, säilitamine ja kasutamine füüsilistes turvamoodulites (edaspidi „HSM“). Tungivalt soovitatakse HSMe kasutada tervisetõendite allkirjastamiseks.

Sõltumata sellest, kas väljastaja otsustab HSMe kasutada või mitte, tuleks kehtestada võtmete asendamise ajakava, mille kohaselt võtmete asendamissagedus on võrdeline sellega, kui kaitsetud on võtmed väliste võrkude, muude süsteemide ja personali suhtes. Samuti piirab hästi valitud asendamise ajakava riske, mis on seotud ekslikult väljastatud tervisetõenditega, võimaldades väljastajal sellised tõendid vajaduse korral võtme tühistamisega ühekorraga kehtetuks muuta.

7.3. *Sisendandmete valideerimine*

Neid spetsifikatsioone saab kasutada nii, et ebausaldusväärsetest allikatest andmeid võetakse vastu süsteemides, mis võivad oma loomult olla missioonikriitilised. Selle ründevektoriga seonduvate riskide minimeerimiseks tuleb kõik andmeväljad andmeliikide, pikkuste ja sisu põhjal nõuetekohaselt valideerida. Enne HCERTi sisu mistahes töötlemist tuleb samuti kontrollida väljastaja allkirja. Samas eeldab väljastaja allkirja valideerimine väljastaja kaitstud päise (Protected Issuer Header) eelnevat parsimist ja selle käigus võib võimalik ründaja teha katset sisestada hoolikalt meisterdatud teavet, mille eesmärk on õõnestada süsteemi turvalisust.

8. **Usaldusteenuste haldus**

HCERTi allkirja kontrolliks on vaja avalikku võtit. Liikmesriigid avalikustavad sellised avalikud võtmed. Põhimõtteliselt peab igal kontrollijal olema loetelu kõigi avalike võtmete kohta, mida ta on nõus usaldama (kuna avalik võti ei ole HCERTi osa).

Süsteemil on (ainult) kaks kihti: iga liikmesriigi kohta on üks või mitu riigi tasandi sertifikaati, millega allkirjastatakse üks või rohkem igapäevaste toimingute juures kasutatavatest dokumentide allkirjastaja sertifikaatidest.

Liikmesriikide sertifikaate nimetatakse riiklike allkirjastamise sertimiskeskuste (CSCA) sertifikaatideks ja tegu on (tavaliselt) iseallkirjastatud sertifikaatidega. Liikmesriikidel võib neid olla rohkem kui üks (näiteks piirkondliku detsentraliseerituse korral). Selliste CSCA-sertifikaatidega allkirjastatakse korrapäraselt dokumentide allkirjastaja sertifikaate (DSC), mida kasutatakse HCERTide allkirjastamiseks.

Sekretariaat täidab talitluslikku rolli. Ta koondab ja avaldab korrapäraselt liikmesriikide DSCsid, olles neid eelnevalt kontrollinud CSCA-sertifikaatide loetelust (mis on edastatud ja mida on kontrollitud muude vahenditega).

Selle põhjal moodustuv DSCde loetelu koondab aktsepteeritavaid avalikke võtmeid (ja neile vastavaid võtmeindikaatoreid), mida kontrollijad võivad kasutada HCERTide allkirjade valideerimiseks. Kontrollijad peavad selle loetelu võtma ja seda korrapäraselt ajakohastama.

Selliste liikmesriigispetsiifiliste loetelude vormingut võib kohandada riiklike olude järgi. Seega võib selle usaldusloetelu failivorming varieeruda: näiteks võib see olla allkirjastatud JWKS (dokumendi RFC 7517 ([11]) jaotise 5 kohane JWK set-vorming) või mis tahes muu asjaomases liikmesriigis kasutatavale tehnoloogiale iseloomulik vorming.

Lihtsuse tagamiseks võivad liikmesriigid niihästi esitada oma ICAO eMRTD süsteemide kehtivad CSCA-sertifikaadid või – nagu soovitab WHO – luua sertifikaadi spetsiaalselt selle tervishoiuvaldkonna jaoks.

8.1. *Võtmeidentifikaator (kid)*

Võtmeidentifikaator (kid) arvutatakse DSCde usaldusväärsete avalike võtmete loetelu koostamisel ja see koosneb DER-(toor)vormingusse kodeeritud DSC kärbitud (esimesed 8 baiti) SHA-256 sõrmejäljest.

Kontrollijad ei pea võtmeidentifikaatorit DSC põhjal arvutama ja saavad väljastatud tervisetõendi võtmeidentifikaatorit kohe kõrvutada usaldusloetelus oleva võtmeindikaatoriga.

8.2. *Erinevus ICAO eMRTD PKI usaldusmudelist*

Ehkki spetsifikatsioonid järgivad ICAO eMRTD PKI usaldusmudeli häid tavasid, tehakse neis kiiruse eesmärgil mitu lihtsustust:

— liikmesriik võib esitada mitu CSCA-sertifikaati;

— DSC (võtme kasutamise) kehtivusajaks võib seada mis tahes aja, mis ei ületa CSCA-sertifikaadi kehtivusaega, ja see võib puududa;

— DSCd võivad sisaldada tervisetõendite-spetsiifilisi otstarbe tunnuseid (võtmekasutuslaiend);

— liikmesriigid võivad otsustada, et nad ei kontrolli mitte kunagi avaldatud tühistamisi, vaid tuginevad pelgalt sellistele DSCde loeteludele, mille nad iga päev sekretariaadilt saavad või ise koostavad.

([11]) rfc7517 (ietf.org)

II LISA

NORMID ELi DIGITAALSE COVID-TÕENDI ANDMETEGA TÄITMISE KOHTA

Käesoleva lisaga kehtestatud väärtuste kogumite eesmärk on tagada semantilise tasandi koostalitlusvõime ja need peavad võimaldama digitaalse COVID-tõendi tehnilisi rakendusi. Vastavalt määruses (EL) 2021/953 sätestatule võib käesolevas lisas esitatud elemente kasutada kõigi kolme eri olukorra (vaktsineerimine/testimine/läbipõdemine) puhul. Käesolevas lisas on loetletud ainult elemendid, mis vajavad semantilist standardimist kodeeritud väärtuskogumitega.

Kodeeritud elementide riigikeelde tõlkimise eest vastutavad liikmesriigid.

Kõigi selliste andmeväljade puhul, mida ei ole järgmistes väärtuste kogumites nimetatud, soovitatakse kasutada UTF-8-süsteemi (nimi, testimiskeskus, tõendi väljastaja). Andmeväljad, mis sisaldavad kuupäevi (sünnikuupäev, vaktsineerimise kuupäev, esimese positiivse tulemuse andnud testi kuupäev, tõendi kehtivuse kuupäevad), soovitatakse kodeerida ISO 8601 kohaselt.

Kui ükskõik millisel põhjusel ei saa kasutada allpool loetletud eelistatud koodisüsteeme, võib kasutada muid rahvusvahelisi koodisüsteeme ja koostada tuleks juhised selle kohta, kuidas vastendada teise koodisüsteemi koodid eelistatud koodisüsteemiga. Kui kindlaksmääratud väärtuste kogumites ei ole olemas sobilikku koodi, võib erandjuhtudel kasutada teksti (kuvatavad nimed).

Liikmesriigid, kes kasutavad oma süsteemides teistsugust kodeerimist, peaksid oma koodid vastendama kirjeldatud väärtuste kogumitega. Igasuguse sellise vastendamise eest vastutavad liikmesriigid.

Komisjon, keda abistavad e-tervise võrgustik ja terviseohutuse komitee, ajakohastab väärtuste kogumeid korrapäraselt. Ajakohastatud väärtuste kogumid avaldatakse komisjoni vastaval veebisaidil, samuti e-tervise võrgustiku veebilehel. Esitada tuleks ülevaade tehtud muudatustest.

1. **Haigus või haigustekitaja, mille suhtes testiti/Haigus või haigustekitaja, millest tõendi omaja on tervenenud: COVID-19 (SARS-CoV-2 või üks selle variantidest)**

   Eelistatud koodisüsteem: SNOMED CT.

   Kasutatakse tõendite nr 1, 2 ja 3 puhul.

   Valitud koodid tähistavad COVID-19 või juhul, kui on vaja üksikasjalikumat teavet SARS-CoV-2 konkreetse geneetilise variandi kohta, seda varianti, kui see üksikasjalik teave on vajalik epidemioloogilistel põhjustel.

   Näide koodi kohta, mida tuleks kasutada: SNOMED CT kood 840539006 (COVID-19).

2. **COVID-19 vaktsiin või profülaktika**

   Eelistatud koodisüsteem: SNOMED CT või anatoomiline, terapeutiline ja keemiline (ATC) klassifikatsioon.

   Kasutatakse tõendi nr 1 puhul.

   Näide eelistatud koodisüsteemidest pärinevate koodide kohta, mida tuleks kasutada: SNOMED CT kood 1119305005 (SARS-CoV-2 antikehade põhine vaktsiin), 1119349007 (SARS-CoV-2 mRNA vaktsiin), J07BX03 (COVID-19 vaktsiinid). Uute vaktsiiniliikide väljatöötamise ja kasutuselevõtu korral tuleks väärtuste kogumit laiendada.

3. **COVID-19 vastu vaktsineerimiseks kasutatud ravim**

   Eelistatud koodisüsteemid (eelistuse järjekorras):

   — liidu ravimiregister – kogu ELis kehtivat müügiluba omavad vaktsiinid (loa number);

   — üleilmne vaktsiinide register, mille võib luua Maailma Terviseorganisatsioon;

   — muudel juhtudel vaktsineerimiseks kasutatud ravimi nimetus. Kui nimetus sisaldab tühikud, tuleks need asendada sidekriipsudega.

Väärtuste kogumi nimi: vaktsiin.

Kasutatakse tõendi nr 1 puhul.

Näide eelistatud koodisüsteemidest pärineva koodi kohta, mida tuleks kasutada: EU/1/20/1528 (Comirnaty). Näide koodina kasutatava vaktsiini nimetuse kohta: Sputnik-V (tähistab vaktsiini Sputnik V).

4. **COVID-19 vaktsiini müügiloa hoidja või tootja**

Eelistatud koodisüsteem:

— Euroopa Ravimiameti antud organisatsiooni kood (ISO ravimite identifitseerimise standardite kohane süsteem SPOR);

— üleilmne vaktsiinide müügiloa hoidjate või tootjate register, mille võib luua Maailma Terviseorganisatsioon;

— muudel juhtudel organisatsiooni nimi. Kui nimetus sisaldab tühikud, tuleks need asendada sidekriipsudega.

Kasutatakse tõendi nr 1 puhul.

Näide eelistatud koodisüsteemidest pärineva koodi kohta, mida tuleks kasutada: ORG-100001699 (AstraZeneca AB). Näide koodina kasutatava vaktsiini nimetuse kohta: Sinovac-Biotech (tähistab vaktsiini Sinovac Biotech).

5. **Järjekorranumber mitme vaktsiinidoosi korral ning dooside koguarv vaktsiiniseerias**

Kasutatakse tõendi nr 1 puhul.

Kaks välja:

(1) tsükli käigus manustatud doosi järjekorranumber;

(2) täieliku vaktsineerimistsükli dooside eeldatav arv (konkreetse isiku puhul manustamise hetkel).

Näiteks 1/1 ja 2/2 tähendab, et tsükkel on lõpetatud; see hõlmab valikut 1/1 juhul, kui vaktsiinil on kaks doosi, aga kui liikmesriigi rakendatava korra kohaselt manustatakse seda üks doos isikutele, kellel on enne vaktsineerimist diagnoositud COVID-19. Tsükli dooside koguarv tuleks märkida vastavalt teabele, mis on doosi manustamise ajal olemas. Näiteks juhul kui konkreetse vaktsiini viimase annuse manustamise ajal on teada, et vaja läheb kolmandat (võimendavat) annust, kajastub see teises väljale märgitud arvus (näiteks 2/3, 3/3 jne).

6. **Liikmesriik või kolmas riik, kus vaktsiin manustati/test tehti**

Eelistatud koodisüsteem: ISO 3166 riigikoodid.

Kasutatakse tõendite nr 1, 2 ja 3 puhul.

Väärtuste kogumi sisu: täielik kahetäheliste koodide loetelu, mis on FIHRi spetsifikatsiooni kohase väärtuste kogumine kättesaadav aadressil (http://hl7.org/fhir/ValueSet/iso3166-1-2).

7. **Testi liik**

Eelistatud koodisüsteem: LOINC.

Kasutatakse tõendi nr 2 puhul ja juhul kui delegeeritud õigusaktiga hakatakse toetama selliste läbipõdemistõendite väljastamist, mis tuginevad muud liiki testidele kui nukleiinhappe amplifitseerimise test, tõendi nr 3 puhul.

Selle väärtuste kogumi koodid tähistavad testimismeetodeid ja need tuleb valida vähemalt selleks, et teha vahel nukleiinhappe amplifitseerimise testidel ja antigeeni kiirtestidel, nagu on sätestatud määruses (EL) 2021/953.

Näide eelistatud koodisüsteemidest pärineva koodi kohta, mida tuleks kasutada: LP217198-3 (immuunkromatograafiline kiirtest).

8. **Kasutatud testi tootja ja kaubanduslik nimetus (nukleiinhappe amplifitseerimise testi puhul ei ole kohustuslik)**

Eelistatud koodisüsteem: terviseohutuse komitee koostatud ja Teadusuuringute Ühiskeskuse hallatav loetelu antigeeni testide kohta (COVID-19 *in vitro* diagnostika meditsiiniseadmete ja testimismeetodite andmebaas).

Kasutatakse tõendi nr 2 puhul.

Väärtuste kogumi sisu hõlmab antigeeni kiirtestide valikut, mis on loetletud COVID-19 antigeeni kiirtestide ajakohastatud ühisloetelus, mis loodi nõukogu soovituse 2021/C 24/01 alusel ja mille on heaks kiitnud terviseohutuse komitee. Loetelu haldab Teadusuuringute Ühiskeskus ja see asub COVID-19 *in vitro* diagnostika meditsiiniseadmete ja testimismeetodite andmebaasis aadressil https://covid-19-diagnostics.jrc.ec.europa.eu/devices/hsc-common-recognition-rat.

Selle koodisüsteemi puhul kasutatakse asjakohaseid välju (testimisseadme tunnus, testi ja tootja nimi) vastavalt Teadusuuringute Ühiskeskuse struktureeritud vormingule, mis on esitatud aadressil https://covid-19-diagnostics.jrc.ec.europa.eu/devices.

9. **Testitulemus**

Eelistatud koodisüsteem: SNOMED CT.

Kasutatakse tõendi nr 2 puhul.

Valitud kood peab võimaldama vahetegemist positiivsel ja negatiivsel testitulemusel („nakkus tuvastati“ või „nakkust ei tuvastatud“). Kui kasutusjuhtumitest tulenevalt on vaja täiendavaid väärtusi (näiteks „määratlemata“), võib need lisada.

Näide eelistatud koodisüsteemidest pärinevate koodide kohta, mida tuleks kasutada: 260415000 („nakkust ei tuvastatud“) ja 260373001 („nakkus tuvastati“).

III LISA

TÕENDI KORDUMATU TUNNUSE ÜHTNE STRUKTUUR

1. **Sissejuhatus**

Igal ELi digitaalsel COVID-tõendil on tõendi kordumatu tunnus, mis toetab selliste tõendite koostalitlusvõimet. Tõendi kordumatut tunnust saab kasutada tõendi kontrolliks. Tõendi kordumatu tunnuse kasutuselevõtu eest vastutavad liikmesriigid. Tõendi kordumatu tunnus on vahend, millega kontrollida tõendi õigsust ja vajaduse korral siduda see registreerimissüsteemiga (näiteks immuniseerimise infosüsteemiga). Samuti võimaldavad need tunnused liikmesriikidel veenduda (paberkandja alusel ja digitaalselt), et isik on vaktsineeritud või teda on testitud.

2. **Tõendi kordumatu tunnuse ülesehitus**

Tõendi kordumatu tunnus järgib ühtset struktuuri ja vormingut, mis hõlbustavad teabe tõlgendamist inimeste poolt ja/või masinaga, ning see võib puudutada selliseid elemente nagu vaktsineerimise liikmesriik, vaktsiin ise ja liikmesriigi konkreetne tunnus. See tagab liikmesriikidele paindlikkuse selle vormistamisel täielikus kooskõlas normidega isikuandmete kaitse kohta. Eri elementide järjestus vastab kindlale hierarhiale, mis võimaldab plokke tulevikus muuta, säilitades samal ajal selle struktuurse terviklikkuse.

Tõendi kordumatu tunnuse ülesehituse võimalikud lahendused moodustavad spektri, millel on kaks peamist muutuvat parameetrit – modulaarsus ja inimesepoolne tõlgendatavus – ning üks keskne omadus.

— Modulaarsus: millisel määral koosneb kood eri moodulitest, mis sisaldavad semantiliselt erinevat teavet;

— inimesepoolne tõlgendatavus: millisel määral kood on seda lugeva inimese jaoks mõistetav või tema poolt tõlgendatav;

— üleilmselt kordumatu; riigi või asutuse tunnust hallatakse hoolikalt; igalt riigilt (asutuselt) oodatakse, et ta haldab nimeruumi talle kuuluvat segmenti hoolikalt, see tähendab ei taaskasuta tunnuseid ega väljasta neid uuesti. Selline kombinatsioon tagab, et iga tunnus on ainuke omataoline maailmas.

3. **Üldnõuded**

Tõendi kordumatu tunnus peaks vastama järgmistele üldnõuetele.

(1) Märgistik: lubatud on ainult US-ASCII kohased suured tärgid (A–Z, 0–9); eraldamiseks võidakse kasutada dokumendi RFC3986 [1] [2] kohaseid täiendavaid erimärke („/“, „#“, „:“).

(2) Maksimumpikkus: projekteerijad peaksid seadma eesmärgiks pikkuse 27–30 märki; [3]

(3) Versiooni eesliide: näitab tõendi kordumatu tunnuse skeemi versiooni. Dokumendi käesoleva versiooni eesliide on „01“; eesliide koosneb kahest numbrist.

(4) Riigi eesliide: riigikoodid on esitatud standardis ISO 3166-1. Pikemad koodid (st kolm märki ja rohkem, nagu näiteks „UNHCR“) jäetakse kasutamiseks tulevikus.

(5) Koodi järelliide/kontrollsumma.

5.1. Liikmesriigid peaksid kasutama kontrollsummat juhul, kui on tõenäoline, et tunnus edastatakse, kirjutatakse ümber (inimese poolt) või see muul viisil laostub (st juhul kui seda kasutatakse väljatrüki kujul).

5.2. Kontrollsummat ei tohi kasutada tõendi valideerimiseks ja tehniliselt ei moodusta see osa tunnusest, vaid seda kasutatakse koodi tervikluse kontrolliks. Kontrollsumma peaks olema standardi ISO-7812-1 (LUHN–10) [4] kohane kogu tõendi kordumatu tunnuse digitaalses/sidevahendi kaudu edastatavas vormingus kokkuvõte. Kontrollsumma on tõendi kordumatu tunnuse ülejäänud osast eraldatud märgiga „#“.

---

[1] rfc3986 (ietf.org)

[2] Selliseid välju nagu sugu, partii number, manustamiskeskus, tervishoiutöötaja tunnus või järgmise vaktsineerimise kuupäev ei pruugi olla vaja muul otstarbel kui kasutamiseks meditsiinilistel eesmärkidel.

[3] QR-koodide kasutuselevõtu korral võivad liikmesriigid kaaluda võimalust kasutada lisamärke kogupikkusega kuni 72 märki (sealhulgas tunnuse enese 27–30 märki), et edastada muud teavet. Selle, millise teabega on tegu, määravad kindlaks liikmesriigid ise.

[4] Luhn'i mod N algoritm on laiendatud Luhn'i algoritm (mida nimetatakse ka mod 10 algoritmiks), mis toimib numbrikoodide puhul ja mida kasutatakse näiteks krediitkaartide kontrollsumma arvutamiseks. Laiendus võimaldab algoritmil toimida ükskõik millise väärtuste jada puhul (siinsel juhul tähtedega).

Tagada tuleks tagasiühilduvus: liikmesriigid, kes muudavad aja jooksul oma tunnuste struktuuri (põhiversiooni piires, milleks on praegu v1), peavad tagama, et mis tahes kaks identset tunnust tähistavad ühte ja sama vaktsineerimistõendit/-kinnitust. Teisisõnu ei saa liikmesriigid tunnuseid taaskasutada.

4. **Vaktsineerimistõendite kordumatute tunnuste variandid**

E-tervise võrgustiku suunistes kontrollitavate vaktsineerimistõendite ja nende põhiliste koostalitlusvõime elementide kohta ([5]) on esitatud eri võimalused, mida liikmesriigid ja muud osalised saavad kasutada ning mis võivad liikmesriikides samal ajal käibel olla. Liikmesriigid saavad sellised eri variandid kasutusele võtta tõendi kordumatu tunnuse skeemi eri versioonis.

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

IV LISA

DIGITAALSERTIFIKAATIDE HALDUS

1. **Sissejuhatus**

ELi digitaalsete COVID-tõendite (digital COVID certificates, edaspidi „DCC“) signeerimisvõtmete turvaline ja usaldusväärne vahetamine liikmesriikide vahel toimub ELi digitaalse COVID-tõendi lüüsi kaudu (Digital COVID Certificate Gateway, edaspidi „DCCG“), mis toimib avalike võtmete keskse hoidlana. DCCG annab liikmesriikidele võimaluse avaldada avalikud võtmed, mis vastavad nende poolt DCCde allkirjastamiseks kasutatavatele privaatvõtmetele. DCCG-le tuginevad liikmesriigid võivad selle vahendusel hankida kiiresti uusimat avalike võtmete materjali. Hiljem saab DCCGd laiendada, et vahetada liikmesriikide esitatavat usaldusväärset lisateavet, nagu DCCde valideerimisreeglid. COVID-tõendite raamistiku usaldusmudel on avaliku võtme taristu (edaspidi „PKI“). Igal liikmesriigil on üks või mitu riiklikku allkirjastamise sertimiskeskust (Country Signing Certification Authority, edaspidi „CSCA“), kelle sertifikaadid on küllaltki pika kehtivusajaga. Vastavalt liikmesriigi otsusele võib CSCA olla sama nagu masinloetavate reisidokumentide puhul kasutatav CSCA või sellest erineda. CSCA väljastab digitaalsertifikaate riiklikele ja lühiajalistele dokumentide allkirjastajatele (st DCCde allkirjastajatele), mida nimetatakse dokumentide allkirjastaja sertifikaatideks (Document Signer Certificates, edaspidi „DSC“). CSCA toimib ankurvõtmena, nii et sellele tuginevad liikmesriigid saavad kasutada CSCA-sertifikaati korrapäraselt muutuvate DSCde ehtsuse ja tervikluse valideerimiseks. Pärast valideerimist saavad liikmesriigid kasutada nimetatud sertifikaate (või pelgalt neis sisalduvaid avalikke võtmeid) omaenese rakendustes DCCde valideerimiseks. Lisaks CSCAdele ja DSCdele tugineb DCCG tehingute autentimisel ja andmete allkirjastamisel ka PKI-le kui autentimise alusele ja vahendile, millega tagada liikmesriikide ja lüüsi vaheliste sidekanalite terviklus.

Andmete tervikluse ja ehtsuse saavutamiseks saab kasutada digiallkirju. Avalike võtmete ja kontrollitud identiteetide (või väljastajate) sidumisega loovad avaliku võtme taristud usaldusväärsuse. Seda on vaja, et muud osalised saaksid kontrollida andmete päritolu ja sidepartneri identiteeti ning teha usaldamisega seotud otsuseid. DCCG kasutab ehtsuse kinnitamiseks mitut digitaalsertifikaati. Käesolevas lisas määratakse kindlaks, milliseid digitaalsertifikaate kasutatakse ja kuidas need välja töötada, et tagada liikmesriikides nende laialdane koostalitlusvõime. Selles on esitatud üksikasjalikum teave vajalike digitaalsertifikaatide kohta ning antud suuniseid sertifikaadimallide ja kehtivusaja kohta liikmesriikides, kes soovivad käitada omaenese CSCAd. Kuna DCCsid saab kontrollida konkreetse ajavahemiku vältel (alates väljastamisest, aeguvad teatud aja jooksul), on vaja kindlaks määrata kontrollimudel kõigi digitaalsertifikaatidele ja DCCdele lisatavate allkirjade jaoks.

2. **Terminoloogia**

Järgmises tabelis on esitatud käesolevas lisas kasutatud lühendid ja terminid.

Termin	Määratlus
Sertifikaat	Teise nimega digitaalsertifikaat. X.509 v3 sertifikaat, mis sisaldab avaliku üksuse avalikku võtit
CSCA	Riiklik allkirjastamise sertimiskeskus
DCC	ELi digitaalne COVID-tõend Allkirjastatud digitaalne dokument, mis sisaldab teavet vaktsineerimise, testimise või läbipõdemise kohta
DCCG	ELi digitaalse COVID-tõendi lüüs. Süsteem, mida kasutatakse DSCde vahetamiseks liikmesriikide vahel
$DCCG_{TA}$	DCCG ankurvõtme sertifikaat. Sellele vastavat privaatvõtit kasutatakse kõigi CSCA-sertifikaatide allkirjastamiseks vallasrežiimis
$DCCG_{TLS}$	DCCG TLSi serveri sertifikaat
DSC	Dokumendi allkirjastaja sertifikaat. Digitaalsertifikaat, mis kuulub liikmesriigi dokumentide allkirjastajale (näiteks süsteemile, millel on luba DCCsid allkirjastada). Selle sertifikaadi väljastab liikmesriigi CSCA
EC-DSA	Elliptiliste kõverate digiallkirja algoritm. Elliptilistel kõveratel põhinev krüptoalgoritm allkirjastamiseks
Liikmesriik	ELi liikmesriik

Termin	Määratlus
mTLS	Vastastikune TLS. Transpordikihi turbeprotokoll, mis kasutab vastastikust autentimist
NB	Liikmesriigi tagateenistus
NB_{CSCA}	Liikmesriigi CSCA-sertifikaat (võib olla rohkem kui üks)
NB_{TLS}	Riikliku tagateenistuse TLS-kliendi autentimissertifikaat
NB_{UP}	Sertifikaat, mida riiklik tagateenistus kasutab DCCGsse üleslaaditavate andmepakettide allkirjastamiseks
PKI	Avaliku võtme taristu. Digitaalsertifikaatidele ja sertimiskeskustele tuginev usaldusmudel
RSA	Asümmeetriline krüptoalgoritm, mis põhineb täisarvu tegurdusel ja mida kasutatakse digiallkirjadeks või asümmeetrilises krüptograafias

3. **DCCG andmevood ja turvateenused**

Selles punktis antakse ülevaade DCCG süsteemi andmevoogudest ja turvateenustest. Samuti määratletakse selles võtmed ja sertifikaadid, mida kasutatakse, et kaitsta sidet, üleslaaditud teavet, DCCsid ja allkirjastatud usaldusloetelu kõigist kaasatud CSCA-sertifikaatidest. DCCG toimib andmekeskusena, mis võimaldab liikmesriikidel vahetada allkirjastatud andmepakette.

DCCG pakub üleslaaditud andmepakette nende algkujul, mis tähendab, et DCCG ei lisa talle saabunud pakettidele DSCsid ega kustuta sealt neid. Liikmesriikide tagateenistusel on võimalik kontrollida üleslaaditud andmete läbivat terviklust ja ehtsust. Lisaks sellele kasutavad riiklikud tagateenistused ja DCCG vastastikust TLS-autentimist turvalise ühenduse loomiseks. See lisandub vahetatud andmetes leiduvatele allkirjadele.

3.1. *Autentimine ja ühenduse loomine*

DCCG kasutab transpordikihi vastastikuse autentimisega turvet (TLS), et luua liikmesriigi tagateenistuse ja lüüsikeskkonna vahele autenditud ja krüpteeritud kanal. Seega on DCCG-l TLS-serveri sertifikaat (lühivormis „$DCCG_{TLS}$“) ja riiklikel tagateenistustel on TLS-kliendi sertifikaat (lühivormis „NB_{TLS}“). Sertifikaatide mallid on esitatud *punktis 5*. Kõik riiklikud tagateenistused võivad esitada oma TLS-sertifikaadi. See sertifikaat kantakse ühemõtteliselt valgesse nimekirja ja seega võib selle väljastada avalikult usaldatav sertimiskeskus (näiteks sertimiskeskus, kes järgib CA/Browser Forumi põhinõudeid), riiklik sertimiskeskus või see võib olla ise allkirjastatud. Iga liikmesriik vastutab oma riiklike andmete ja DCCGga ühenduse loomiseks kasutatud privaatvõtme kaitse eest. Nn oma sertifikaadi (bring your own certificate) lähenemisviisiks on vaja täpselt määratletud registreerimis- ja identimisprotsessi, samuti tühistamis- ja uuendamismenetlusi, nagu kirjeldatud *punktides 4.1, 4.2* ja *4.3*. DCCG kasutab valget nimekirja, kuhu NBde TLS-sertifikaadid lisatakse pärast nende edukat registreerimist. Turvalise ühenduse DCCGga saavad luua ainult need NBd, kes autendivad ennast privaatvõtmega, mis vastab valgesse nimekirja kuuluvale sertifikaadile. Ka DCCG kasutab TLS-sertifikaati, mis võimaldab NBdel kontrollida, et nad loovad tõepoolest ühenduse tegeliku DCCGga, mitte mõne DCCGd teeskleva pahatahtliku üksusega. DCCG sertifikaat antakse NBdele pärast edukat registreerimist. $DCCG_{TLS}$ sertifikaadi väljastab avalikult usaldatav sertimiskeskus (sealhulgas kõigi peamiste brauserite jaoks). Selle eest, et ühendus DCCGga on turvaline, vastutavad liikmesriigid (näiteks võivad nad võrrelda ühendusserveri $DCCG_{TLS}$ sertifikaadi sõrmejälge sellega, mis edastati pärast registreerimist).

3.2. *Riiklikud allkirjastamise sertimiskeskused ja valideerimismudel*

DCCG raamistikus osalevad liikmesriigid peavad DSCde väljastamiseks kasutama CSCAd. Liikmesriikidel võib olla rohkem kui üks CSCA (näiteks piirkondliku detsentraliseerituse korral). Iga liikmesriik võib kas kasutada olemasolevaid sertimiskeskusi või luua spetsiaalse (võimaluse korral iseallkirjastatud) sertimiskeskuse DCC-süsteemi jaoks.

Ametliku kaasamisprotsessi käigus peavad liikmesriigid esitama oma CSCA-sertifikaadi(d) DCCG käitajale. Pärast liikmesriigi edukat registreerimist (*täpsemat teavet vt punkt 4.1*) uuendab DCCG käitaja allkirjastatud usaldusloetelu, mis sisaldab kõiki DCC raamistikus aktiivseid CSCA-sertifikaate. DCCG käitaja kasutab spetsiaalset asümmeetrilist võtmepaari, et usaldusloetelu ja sertifikaadid vallaskeskkonnas allkirjastada. Privaatvõtit ei säilitata DCCG sidussüsteemis, nii et sidussüsteemi rikkumine ei anna ründajale võimalust rikkuda usaldusloetelu. Sellele vastav ankurvõtme sertifikaat ($DCCG_{TA}$) antakse riiklike tagateenistuste käsutusse kaasamisprotsessi käigus.

Liikmesriigid saavad usaldusloetelu oma kontrollimenetluste jaoks DCCG-lt. CSCA on määratletud kui DSCsid väljastav sertimiskeskus ja seega peavad liikmesriigid, kes kasutavad mitmetasandilist sertimiskeskuste hierarhiat (näiteks juursertimiskeskus -> CSCA -> DSCd), esitama DSCsid väljastava alamsertimiskeskuse. Sellisel juhul, see tähendab kui liikmesriik kasutab olemasolevat sertimiskeskust, eirab DCC-süsteem kõike, mis on CSCAst ülalpool, ja paneb valgesse nimekirja ankurvõtmena ainult CSCA (hoolimata sellest, et tegu on alamsertimiskeskusega). See tuleneb asjaolust, et ICAO mudel võimaldab ainult täpselt kaht tasandit – nn juur ehk CSCA ja nn leht ehk DSC, mis on allkirjastatud just selle CSCA poolt.

Juhul kui liikmesriik käitab omaenese CSCAd, vastutab selle sertimiskeskuse turvalise toimimise ja võtmehalduse eest liikmesriik. CSCA toimib DSCde ankurvõtmena ja seega on CSCA privaatvõtme kaitse DCC keskkonna tervikluse seisukohalt keskse tähtsusega. DCC PKI kontrollimudel on kestmudel (shell model), mis deklareerib, et kõik sertifitseerimisahela valideerimiseks kasutatavad sertifikaadid peavad kehtima teataval ajal (st allkirja valideerimise ajal). Seega kehtivad järgmised piirangud:

— CSCA ei väljasta sertifikaate, mille kehtivusaeg on pikem kui sertimiskeskuse enese sertifikaat;

— dokumentide allkirjastaja ei allkirjasta dokumente, mille kehtivusaeg on pikem kui DSC enda oma;

— omaenese CSCAd käitavad liikmesriigid peavad kindlaks määrama oma CSCA ja kõigi väljastatud tõendite kehtivusaja ning kandma hoolt sertifikaatide uuendamise eest.

Punktis4.2 on esitatud soovitused kehtivusaegade kohta.

3.3. *Üleslaaditud andmete terviklus ja ehtsus*

Riiklikud tagateenistused saavad DCCGd pärast edukat vastastikust autentimist kasutada selleks, et laadida üles ja alla digitaalselt allkirjastatud andmepakette. Alguses sisaldavad need andmepaketid liikmesriikide DSCsid. Võtmepaari, mida riiklik tagateenistus kasutab DCCG süsteemi üles laaditud andmepakettidele digiallkirjastamiseks, nimetatakse riikliku tagateenistuse üleslaadimisallkirja võtmepaariks ja selle vastava digitaalsertifikaadi lühivorm on NB_{UP}-sertifikaat. Iga liikmesriik kasutab omaenese isiklikku NB_{UP}-sertifikaati, mis võib olla iseallkirjastatud või mille võib olla väljastanud olemasolev sertimiskeskus, näiteks riiklik sertimiskeskus (st vastavalt CA/Browser Forumi põhinõuetele sertifikaate väljastav sertimiskeskus). NB_{UP}-sertifikaat erineb kõigist liikmesriigi kasutatavatest sertifikaatidest (st CSCA, TLSi klient või DSCd).

Liikmesriigid peavad üleslaadimissertifikaadi DCCG käitajale esitama algse registreerimismenetluse käigus (*üksikasjalikum teave vt punkt 4.1*). Iga liikmesriik vastutab oma riiklike andmete eest ja peab kaitsma üleslaaditud andmete allkirjastamiseks kasutatavat privaatvõtit.

Teised liikmesriigid saavad allkirjastatud andmepakette kontrollida, kasutades DCCG poolt nende käsutusse antud üleslaadimissertifikaate. Enne üleslaaditud andmete edastamist teistele liikmesriikidele kontrollib DCCG selle ehtsust ja terviklust NB üleslaadimissertifikaadi abil.

3.4. *DCCG tehnilisele arhitektuurile esitatavad nõuded*

DCCG tehnilise arhitektuuri suhtes kehtivad järgmised nõuded.

— DCCG kasutab vastastikust TLS-autentimist, et luua NBdega autenditud ja krüpteeritud ühendus. Seega peab DCCG registreeritud NB_{TLS} kliendisertifikaatide valget nimekirja;

— DCCG kasutab kaht elektroonilist sertifikaati ($DCCG_{TLS}$ ja $DCCG_{TA}$), millel on kaks eri võtmepaari. $DCCG_{TA}$ võtmepaari privaatvõtit hoitakse vallaskeskkonnas (mitte DCCG siduselementides);

— DCCG peab NB_{CSCA}-sertifikaatide usaldusloetelu, mis on allkirjastatud $DCCG_{TA}$ privaatvõtmega;

— kasutatavad šifrid peavad vastama *punkti 5.1* nõuetele.

4. **Sertifikaatide elutsükli haldus**

4.1. *Riiklike tagateenistuste registreerimine*

Liikmesriigid peavad DCCG süsteemis osaleva käitaja DCCG juures registreerima. Käesolevas punktis on kirjeldatud tehnilisi toiminguid ja töökorda, mida tuleb järgida riikliku tagateenistuse registreerimiseks.

DCCG käitaja ja liikmesriigid peavad kaasamisprotsessi eesmärgil vahetama teavet tehniliste kontaktisikute kohta. Eeldatakse, et tehnilised kontaktisikud on nende liikmesriigi poolt õiguspäraseks tunnistatud ja identimine/autentimine toimub muude kanalite kaudu. Näiteks võib autentimine toimuda nii, et liikmesriigi tehniline kontaktisik esitab sertifikaadid salasõnaga krüpteeritud failidena e-postiga ja annab vastava salasõna DCCG käitajale telefonitsi. Samuti võib kasutada muid DCCG käitaja poolt kindlaksmääratud turvalisi kanaleid.

Registreerimise ja identimise käigus peab liikmesriik esitama kolm elektroonilist sertifikaati:

— liikmesriigi TLS-sertifikaat NB_{TLS};

— liikmesriigi üleslaadimissertifikaat NB_{UP};

— liikmesriigi CSCA-sertifikaat/sertifikaadid NB_{CSCA}.

Kõik esitatud sertifikaadid peavad vastama *punktis 5* esitatud nõuetele. DCCG käitaja kontrollib, et esitatud sertifikaat vastab *punktis 5* esitatud nõuetele. Pärast identimist ja registreerimist teeb DCCG käitaja järgmist.

— Lisab NB_{CSCA} sertifikaadi(d) usaldusloetellu, mis on allkirjastatud privaatvõtmega, mis vastab $DCCG_{TA}$ avalikule võtmele;

— lisab NB_{TLS} sertifikaadi DCCG TLS otspunktide valgesse nimekirja;

— lisab NB_{UP} sertifikaadi DCCG süsteemi;

— annab liikmesriigi käsutusse $DCCG_{TA}$ ja $DCCG_{TLS}$ digitaalsertifikaadi.

4.2. *Sertimiskeskused, kehtivusajad ja uuendamine*

Juhul kui liikmesriik soovib kasutada omaenese CSCAd, võivad CSCA-sertifikaadid olla iseallkirjastatud sertifikaadid. Need toimivad liikmesriigi ankurvõtmena ja seega peab liikmesriik CSCA-sertifikaadi avalikule võtmele vastavat privaatvõtit kindlalt kaitsma. Liikmesriigil soovitatakse oma CSCA jaoks kasutada vallassüsteemi, st arvutisüsteemi, mis ei ole ühendatud ühtegi võrku. Süsteemile juurdepääsuks tuleb kasutada mitut inimest nõudvat korda (näiteks järgides nn nelja silma põhimõtet). Pärast DSCde allkirjastamist kohaldatakse toimimiskontrolli, CSCA privaatvõtit sisaldavat süsteemi hoitakse turvaliselt ja juurdepääsu sellele kontrollitakse rangelt. CSCA privaatvõtme täiendavaks kaitseks võib kasutada füüsilisi turvamooduleid või kiipkaarte. Elektroonilistel sertifikaatidel on kehtivusaeg, mis sunnib sertifikaati uuendama. Uuendamist on vaja, et kasutada värskeid krüptovõtmeid ja kohandada võtmete pikkust, kui kasutatava krüptoalgoritmi turvalisust ohustavad uued edusammud andmetöötluse vallas või uued ründed. Kasutatakse kestmudelit (vt *punkt 3.2*).

Arvestades digitaalsete COVID-tõendite aastast kehtivust, soovitatakse järgmisi kehtivusaegu:

— CSCA: 4 aastat;

— DSC: 2 aastat;

— üleslaadimine: 1–2 aastat;

— TLS-kliendi autentimine: 1–2 aastat.

Õigeaegseks uuendamiseks soovitatakse privaatvõtmete puhul järgmisi kasutusaegu:

— CSCA: 1 aasta;

— DSC: 6 kuud.

Selleks et võimaldada sujuvat toimimist, peavad liikmesriigid looma uued üleslaadimissertifikaadid ja TLS-sertifikaadid õigeaegselt, näiteks kuu aega enne nende aegumist. CSCA sertifikaate ja DSCsid tuleks uuendada vähemalt kuu aega enne privaatvõtme kehtivuse lõppu (võttes arvesse vajalikke korralduslikke meetmeid). Liikmesriigid peavad esitama uuendatud CSCA, üleslaadimis- ja TLS-sertifikaadid DCCG käitajale. Aegunud sertifikaadid eemaldatakse valgest nimekirjast ja usaldusloetelust.

Liikmesriigid ja DCCG käitaja peavad ise jälgima oma sertifikaatide kehtivust. Puudub keskne üksus, kes peaks arvet sertifikaatide kehtivuse üle ja osalisi teavitaks.

4.3. *Sertifikaatide tühistamine*

Üldiselt saab elektroonilise sertifikaadi tühistada selle väljastanud sertimiskeskus, kasutades tühistatud sertifikaatide loendit või OCSP kehtivuskinnitusi. DCC süsteemi CSCAd peaksid esitama tühistatud sertifikaatide loendi. Isegi kui teised liikmesriigid neid tühistatud sertifikaatide loendeid praegu ei kasuta, tuleks need integreerida tulevaseks kasutuseks. Juhul kui CSCA otsustab tühistatud sertifikaatide loendeid mitte esitada, tuleb kõnealuse CSCA DSCsid uuendada, kui tühistatud sertifikaatide loendid muutuvad kohustuslikuks. Kontrollijad ei peaks DSCde valideerimiseks kasutama mitte OCSP kehtivuskinnitusi, vaid tühistatud sertifikaatide loendeid. On soovitatav, et riiklik tagateenistus tegeleb DCC lüüsist alla laaditud DSCde vajaliku valideerimisega ja edastab riiklikele DCC valideerijatele ainult usaldusväärsete ja valideeritud DSCde kogumi. DCC valideerijad ei peaks oma valideerimisprotsessi käigus tegelema DSC kehtivuse kontrolliga. Selle üks põhjus on kaitsta DCC omajate privaatsust, vältides mis tahes võimalust, et ühe konkreetse DSC kasutamist saaks jälgida sellega seotud OCSP kehtivuskinnituse kaudu.

Liikmesriigid saavad oma DSCd kehtivat üleslaadimis- ja TLS-sertifikaati kasutades DCCGst ise eemaldada. DSC eemaldamine tähendab, et kui liikmesriigid laadivad alla DSCde uuendatud loetelu, muutuvad kõik selle DSCga väljastatud DCCd kehtetuks. DSCdele vastava privaatvõtme materjali kaitse on eluliselt tähtis. Kui liikmesriigid peavad üleslaadimis- või TLS-sertifikaate uuendama, näiteks riikliku tagateenistuse rikkumise tõttu, peavad nad DCCG käitajat sellest teavitama. Siis saab DCCG käitaja mõjutatud sertifikaadilt usalduse ära võtta, näiteks eemaldades selle TLSi valgest nimekirjast. DCCG käitaja võib üleslaadimissertifikaadid DCCG andmebaasist eemaldada. Sellele üleslaadimissertifikaadile vastava privaatvõtmega allkirjastatud paketid kaotavad kehtivuse, kui riiklikud tagateenistused usalduse tühistatud sertifikaadilt ära võtavad. Juhul kui tühistada tuleb CSCA-sertifikaat, teavitavad liikmesriigid DCCG käitajat, samuti teisi liikmesriike, kellega neil on usaldussuhted. DCCG käitaja väljastab uue usaldusloetelu, milles asjaomast sertifikaati enam ei ole. Kõik selle CSCA väljastatud DSCd kaotavad kehtivuse, kui liikmesriigid oma tagateenistuse usaldusväärsete sertifikaatide ladu uuendavad. Juhul kui on vaja tühistada $DCCG_{TLS}$ sertifikaat või $DCCG_{TA}$ sertifikaat, peavad DCCG käitaja ja liikmesriik tegema koostööd, et luua uus usaldatav TLS-ühendus ja usaldusloetelu.

5. **Sertifikaatide mallid**

Selles punktis on esitatud nõuded ja suunised krüptograafia kohta, samuti teatavatele mallidele esitatavad nõuded. DCCG sertifikaatide kohta on käesolevas punktis määratletud sertifikaatide mallid.

5.1. *Krüptograafilised nõuded*

Krüptoalgoritmid ja TLSi šifrikomplektid võib valida vastavalt Saksamaa Infoturbe Liiduameti (BSI) või SOG-ISi soovitustele. Need soovitused on sarnased muude institutsioonide ja standardiorganisatsioonide soovitustega. Soovitused on esitatud tehnilistes suunistes TR 02102-1 ja TR 02102-2 ([1]) või SOG-ISi dokumendis „Agreed Cryptographic Mechanisms“ ([2]).

5.1.1. Nõuded DSC-le

Kehtivad *I lisa punktis 3.2.2* esitatud nõudeid. Seega soovitatakse tungivalt, et dokumentide allkirjastajad kasutaksid elliptiliste kõverate digiallkirja algoritmi ja NIST-p-256 (nagu on kirjeldatud standardi (FIPS PUB 186–4) D lisas). Teistele elliptilistele kõveratele puudub tugi. DCC ruumipiirangute tõttu ei peaks liikmesriigid kasutama RSA-PSSi,

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

ehkki see on lubatud kui algoritmi varuvariant. Juhul kui liikmesriik kasutab RSA-PSSi, peaks mooduli suurus olema 2048 või kõige enam 3072 bitti. DSC allkirja krüptograafilise räsifunktsiooni jaoks tuleb kasutada SHA-2, mille väljund on ≥ 256 bitti (vt ISO/IEC 10118-3:2004).

5.1.2. Nõuded seoses TLS-, üleslaadimis- ja CSCA-sertifikaatidega

DCCG kontekstis on peamised nõuded, mis esitatakse krüptoalgoritmidele ja võtmete pikkusele elektrooniliste sertifikaatide ja krüpteeritud allkirjade puhul, kokku võetud järgmises tabelis (2021. aasta seisuga).

Allkirja algoritm	Võtme pikkus	Räsifunktsioon
EC-DSA	Vähemalt 250 bitti	SHA-2, mille väljund on ≥ 256 bitti
RSA-PSS (soovituslik täidis) RSA-PKCS#1 v1.5 (pärandtäidis)	Vähemalt 3000 bitine RSA-moodul (N), mille avalik eksponent e > 2^16	SHA-2, mille väljund on ≥ 256 bitti
DSA	Vähemalt 3000 bitti algarv p, 250 bitti võti q	SHA-2, mille väljund on ≥ 256 bitti

EC-DSA soovituslik elliptiline kõver on NIST-p-256 tulenevalt selle laialdasest kasutusest.

5.2. *CSCA sertifikaat (NB_{CSCA})*

Järgmises tabelis antakse suuniseid NB_{CSCA} sertifikaadi malli kohta, kui liikmesriik otsustab DCC süsteemi jaoks käitada omaenese CSCAd.

Rasvases kirjas kanded on kohustuslikud (peavad sertifikaadis olema), *kaldkirjas* kanded on soovituslikud (peaksid seal olema). Puuduvate väljade kohta ei ole soovitusi antud.

Väli	Väärtus
Subjekt	**cn=<mittetühi ja kordumatu üldnimi>,***o=<pakkuja>*,**c=<CSCAd käitav liikmesriik>**
Võtme kasutamise eesmärk	**Sertifikaatide allkirjastamine,***tühistatud sertifikaatide loendi allkirjastamine* (miinimum)
Põhipiirangud	**CA = true, raja pikkuse piirang = 0**

Subjekti nimi peab olema mittetühi ja nimetatud liikmesriigis kordumatu. Riigikood (c) peab langema kokku seda CSCA-sertifikaati kasutava liikmesriigiga. Sertifikaat peab sisaldama dokumendi RFC 5280 ([3]) kohast subjekti võtme identifikaatorit.

5.3. *Dokumendi allkirjastaja sertifikaat (DSC)*

Järgmises tabelis on esitatud suunised DSC kohta. **Rasvases kirjas** kanded on kohustuslikud (peavad sertifikaadis olema), *kaldkirjas* kanded on soovituslikud (peaksid seal olema). Puuduvate väljade kohta ei ole soovitusi antud.

Väli	Väärtus
Sarjanumber	**Kordumatu sarjanumber**
Subjekt	**cn=<mittetühi ja kordumatu üldnimi>,***o=<pakkuja>*, **c=<asjaomast DSCd kasutav liikmesriik>**
Võtme kasutamise eesmärk	**Digiallkiri** (miinimum)

([3]) rfc5280 (ietf.org)

DSC peab olema allkirjastatud privaatvõtmega, mis vastab liikmesriigi poolt kasutatavale CSCA-sertifikaadile.

Kasutada tuleb järgmisi laiendeid:

— sertifikaat peab sisaldama asutuse võtme identifikaatorit, mis vastab väljastava CSCA-sertifikaadi subjekti võtme identifikaatorile;

— sertifikaat peaks sisaldama kordumatut subjekti võtme identifikaatorit (kooskõlas dokumendiga RFC 5280) ([4]).

Lisaks sellele peaks sertifikaat sisaldama tühistatud sertifikaatide loendi väljastamispunkti laiendit, mis viitab tühistatud sertifikaatide loendile, mille on esitanud DSC väljastanud CSCA.

DSC võib sisaldada laiendatud võtmekasutuslaiendit, milles on null või rohkem võtmekasutuse otstarbe tunnust, mis piiravad seda, millist liiki HCERTe asjaomane sertifikaat tohib kontrollida. Kui neid on üks või rohkem, võrdlevad kontrollijad võtit selle kontrolliks salvestatud HCERTiga. Selle jaoks on määratletud järgmised extendedKeyUsage väärtused.

Väli	Väärtus
extendedKeyUsage	1.3.6.1.4.1.1847.2021.1.1 testimistõendite väljastajatele
extendedKeyUsage	1.3.6.1.4.1.1847.2021.1.2 vaktsineerimistõendite väljastajatele
extendedKeyUsage	1.3.6.1.4.1.1847.2021.1.3 paranemistõendite väljastajatele

Juhul kui võtmekasutuslaiend puudub (st puuduv laiend või null laiendit), võib asjaomast sertifikaati kasutada ükskõik mis liiki HCERTi valideerimiseks. Muudes dokumentides võidakse määratleda võtmekasutuslaiendis asjakohased täiendavad otstarbe tunnused, mida kasutatakse HCERTide valideerimiseks.

5.4. *Üleslaadimissertifikaadid (NBUP)*

Järgmises tabelis on esitatud suunised riikliku tagateenistuse üleslaadimissertifikaadi kohta. **Rasvases kirjas** kanded on kohustuslikud (peavad sertifikaadis olema), *kaldkirjas* kanded on soovituslikud (peaksid seal olema). Puuduvate väljade kohta ei ole soovitusi antud.

Väli	Väärtus
Subjekt	**cn=<mittetühi ja kordumatu üldnimi>,***o=<pakkuja>,* **c=<asjaomast üleslaadimissertifikaati kasutav liikmesriik>**
Võtme kasutamise eesmärk	**Digiallkiri** (miinimum)

5.5. *Riikliku tagateenistuse TLS-kliendi autentimine (NB_{TLS})*

Järgmises tabelis on esitatud suunised riikliku tagateenistuse TLS-kliendi autentimissertifikaadi kohta. **Rasvases kirjas** kanded on kohustuslikud (peavad sertifikaadis olema), *kaldkirjas* kanded on soovituslikud (peaksid seal olema). Puuduvate väljade kohta ei ole soovitusi antud.

Väli	Väärtus
Subjekt	**cn=<mittetühi ja kordumatu üldnimi>,***o=<pakkuja>,* **c=<NB liikmesriik>**
Võtme kasutamise eesmärk	**Digiallkiri** (miinimum)
Võtmekasutuslaiend	**Kliendi autentimine (1.3.6.1.5.5.7.3.2)**

([4]) rfc5280 (ietf.org)

Samuti võib sertifikaat sisaldada võtmekasutuslaiendit *serveri autentimine (1.3.6.1.5.5.7.3.1)*, kuid see ei ole nõutav.

5.6. *Usaldusloetelu allkirjastamise sertifikaat ($DCCG_{TA}$)*

DCCG ankurvõtme sertifikaat on määratletud järgmises tabelis.

Väli	Väärtus
Subjekt	**cn = Rohelise digitõendi lüüs,** ([5])**o=<pakkuja>, c=<riik>**
Võtme kasutamise eesmärk	**Digiallkiri** (miinimum)

5.7. *DCCG TLS serveri sertifikaadid ($DCCG_{TLS}$)*

DCCG TLS-sertifikaat on määratletud järgmises tabelis.

Väli	Väärtus
Subjekt	cn=<DCCG täisdomeeninimi või IP-aadress>, o=<pakkuja>, c= <riik>
SubjectAltName	dNSName: <DCCG DNS-nimi> või iPAddress: <DCCG IP-aadress>
Võtme kasutamise eesmärk	**Digiallkiri** (miinimum)
Võtmekasutuslaiend	**Serveri autentimine (1.3.6.1.5.5.7.3.1)**

Samuti võib sertifikaat sisaldada võtmekasutuslaiendit *kliendi autentimine (1.3.6.1.5.5.7.3.2)*, kuid see ei ole nõutav.

DCCG TLS-sertifikaadi väljastab avalikult usaldatav sertimiskeskus (sealhulgas kõigi peamiste brauserite ja operatsioonisüsteemide jaoks järgides CA/Browser Forumi põhinõudeid).

([5]) Käesolevas kontekstis on jätkatud termini „roheline digitõend“ kasutamist termini „ELi digitaalne COVID-tõend“ asemel, kuna see on termin, mis on tõendisse püsikodeeritud ja selles kasutusele võetud enne, kui kaasseadusandjad otsustasid kasutada uut terminit.