KOMISIJAS ĪSTENOŠANAS LĒMUMS (ES) 2021/1073

(2021. gada 28. jūnijs),

ar ko nosaka tehniskās specifikācijas un noteikumus ar Eiropas Parlamenta un Padomes Regulu (ES) 2021/953 izveidotā ES digitālā Covid sertifikāta uzticamības satvara īstenošanai

(Dokuments attiecas uz EEZ)

EIROPAS KOMISIJA,

ņemot vērā Līgumu par Eiropas Savienības darbību,

ņemot vērā Eiropas Parlamenta un Padomes Regulu (ES) 2021/953 par sadarbspējīgu Covid-19 vakcinācijas, testa un pārslimošanas sertifikātu (ES digitālais Covid sertifikāts) izdošanas, verifikācijas un akceptēšanas satvaru nolūkā atvieglot brīvu pārvietošanos Covid-19 pandēmijas laikā ([1]), un jo īpaši tās 9. panta 1. un 3. punktu,

tā kā:

(1) Regulā (ES) 2021/953 ir noteikts ES digitālais Covid sertifikāts, kura mērķis ir pierādīt, ka persona ir saņēmusi Covid-19 vakcīnu, negatīvu testa rezultātu vai šo infekciju pārslimojusi.

(2) Lai ES digitālais Covid sertifikāts varētu darboties visā Savienībā, ir jānosaka tehniskās specifikācijas un noteikumi, lai digitālos Covid sertifikātus varētu aizpildīt, droši izdot un verificēt, nodrošinātu persondatu aizsardzību, noteiktu unikālā sertifikāta identifikatora kopīgo struktūru un izdotu derīgu, drošu un sadarbspējīgu svītrkodu. Minētais uzticamības satvars ietver arī priekšnoteikumus, kuru mērķis ir nodrošināt sadarbspēju ar starptautiskajiem standartiem un tehnoloģiskām sistēmām, un pats par sevi varētu noderēt par paraugu sadarbībai pasaules līmenī.

(3) Lai varētu nolasīt un interpretēt ES digitālo Covid sertifikātu, ir vajadzīga kopīga datu struktūra un ir jāvienojas par to, ko katrs pamatdatu lauks nozīmēs un kādas ir tā iespējamās vērtības. Lai šādu sadarbspēju veicinātu, ES digitālā Covid sertifikāta satvaram ir jānosaka vienota saskaņota datu struktūra. Satvara pamatnostādnes ir izstrādājis e-veselības tīkls, kas izveidots uz Eiropas Parlamenta un Padomes Direktīvas 2011/24/ES ([2]) pamata. Minētās pamatnostādnes būtu jāņem vērā, kad tiek noteiktas tehniskās specifikācijas, kurās paredz ES digitālā Covid sertifikāta formātu un uzticamības pārvaldību. Datu struktūras specifikācija un kodēšanas mehānismi, kā arī pārneses kodēšanas mehānismi ir jānosaka mašīnlasāmā optiskā formātā (*QR*), ko var attēlot uz mobilās ierīces ekrāna vai izdrukāt uz papīra.

(4) Papildus ES digitālā Covid sertifikāta formāta un uzticamības pārvaldības tehniskajām specifikācijām būtu jānosaka vispārīgi noteikumi par sertifikātu aizpildīšanu, ko izmanto, lai ES digitālajā Covid sertifikātā ievadītu kodētas vērtības. Komisijai, pamatojoties uz e-veselības tīkla veikto darbu, būtu regulāri jāatjaunina un jāpublicē minēto noteikumu īstenošanas vērtību kopas.

(5) Saskaņā ar Regulu (ES) 2021/953 autentiskajiem sertifikātiem, kas veido ES digitālo Covid sertifikātu, jābūt individuāli identificējamiem ar unikālu sertifikāta identifikatoru, ņemot vērā to, ka Regulas (ES) 2021/953 spēkā esības laikā iedzīvotājiem varētu tikt izdots vairāk nekā viens sertifikāts. Unikālo sertifikāta identifikatoru veidos burtciparu virknes, un dalībvalstīm būtu jānodrošina, ka tas nesatur tādus datus, kas to var sasaistīt ar citiem dokumentiem vai identifikatoriem, piemēram, ar pases vai personas apliecības numuru, lai nepieļautu to, ka sertifikāta turētāju var identificēt. Lai nodrošinātu, ka sertifikāta identifikators ir unikāls, būtu jānosaka tā kopīgās struktūras tehniskās specifikācijas un noteikumi.

([1]) OV L 211, 15.6.2021., 1. lpp.

([2]) Eiropas Parlamenta un Padomes Direktīva 2011/24/ES (2011. gada 9. marts) par pacientu tiesību piemērošanu pārrobežu veselības aprūpē (OV L 88, 4.4.2011., 45. lpp.).

(6) ES digitālo Covid sertifikātu veidojošo sertifikātu drošība, autentiskums, derīgums, nedalāmība un atbilstība Savienības datu aizsardzības tiesību aktiem ir būtiska, lai sertifikāti tiktu akceptēti visās dalībvalstīs. Minēto mērķu izpildi nodrošina ar uzticamības satvaru, kas paredz noteikumus un infrastruktūru attiecībā uz ES digitālo Covid sertifikātu uzticamu un drošu izdošanu un verifikāciju. Cita starpā uzticamības satvara pamatā vajadzētu būt publisko atslēgu infrastruktūrai ar uzticamības ķēdi no dalībvalstu veselības aizsardzības iestādēm vai citām uzticamības iestādēm līdz atsevišķajām struktūrām, kas izdod ES digitālos Covid sertifikātus. Tāpēc, lai nodrošinātu ES mēroga sadarbspējas sistēmu, Komisija ir izveidojusi centrālu sistēmu – ES digitālā Covid sertifikāta vārteju ("vārteja") –, kurā tiek uzglabātas publiskās atslēgas, ko izmanto verifikācijā. Kad QR koda sertifikāts tiek noskenēts, digitālais paraksts tiek verificēts, izmantojot attiecīgo publisko atslēgu, kas tiek uzglabāta centrālajā vārtejā. Digitālos parakstus var izmantot, lai nodrošinātu datu integritāti un autentiskumu. Publisko atslēgu infrastruktūras ir uzticamas, jo publiskās atslēgas tiek piesaistītas sertifikātu izdevējiem. Vārtejā autentificēšanai tiek izmantoti vairāki publisko atslēgu sertifikāti. Lai starp dalībvalstīm nodrošinātu publisko atslēgu materiāla drošu datu apmaiņu un plašu sadarbspēju, ir jānosaka izmantojamie publisko atslēgu sertifikāti un tas, kā tie būtu jāģenerē.

(7) Ar šo lēmumu Regulas (ES) 2021/953 prasības var darboties tā, lai persondatu apstrādi samazinātu līdz minimālajam līmenim, kāds vajadzīgs, lai ES digitālais Covid sertifikāts darbotos, un sekmētu to, ka galīgie pārziņi veic īstenošanu, ievērojot datu aizsardzību integrēti.

(8) Saskaņā ar Regulu (ES) 2021/953 iestādes vai citas izraudzītās struktūras, kas ir atbildīgas par sertifikātu izdošanu un kas izdošanas procesā veic persondatu apstrādi, ir pārziņi, kas minēti Eiropas Parlamenta un Padomes Regulas (ES) 2016/679 ([3]) 4. panta 7. punktā. Atkarībā no tā, kā dalībvalstis organizē izdošanas procesu, var būt viena vai vairākas iestādes vai izraudzītās struktūras, piemēram, reģionāli veselības dienesti. Ievērojot subsidiaritātes principu, to dalībvalstis izvēlas pašas. Tādējādi dalībvalstis ir vislabākajā pozīcijā, lai, ja tajās ir vairākas iestādes vai citas norīkotās struktūras, nodrošinātu, ka to atbildības jomas ir skaidri nošķirtas neatkarīgi no tā, vai tās ir atsevišķi vai kopīgi pārziņi (piemēram, reģionālie veselības dienesti, kas sertifikātu izdošanai izveidojuši kopīgu portālu pacientiem). Tāpat attiecībā uz sertifikātu verifikāciju, ko veic galamērķa vai tranzīta dalībvalsts kompetentā iestāde vai pārrobežu pasažieru pārvadājumu pakalpojumu sniedzēji, kam saskaņā ar valsts tiesību aktiem Covid-19 pandēmijas laikā ir jāveic konkrēti sabiedriskās veselības aizsardzības pasākumi, tādiem verificētājiem ir jāievēro pienākumi, kas noteikti datu aizsardzības noteikumos.

(9) Ar ES digitālā Covid sertifikāta vārtejas starpniecību netiek veikta persondatu apstrāde, jo vārtejā ir tikai sertifikāta parakstītājiestāžu publiskās atslēgas. Minētās atslēgas ir saistītas ar parakstītājiestādēm, un ar tām nevar ne tieši, ne netieši identificēt fizisko personu, kurai izdots sertifikāts. Veicot vārtejas pārvaldību, Komisijai nav jābūt ne pārzinim, ne persondatu apstrādātājam.

(10) Notika apspriešanās ar Eiropas Datu aizsardzības uzraudzītāju saskaņā ar Eiropas Parlamenta un Padomes Regulas (ES) 2018/1725 ([4]) 42. panta 1. punktu, un tas ir sniedzis atzinumu 2021. gada 22. jūnijā.

(11) Ņemot vērā, ka tehniskās specifikācijas un noteikumi ir vajadzīgi, lai Regulu (ES) 2021/953 varētu piemērot no 2021. gada 1. jūlija, šo lēmumu ir pamats piemērot nekavējoties.

(12) Tāpēc, ņemot vērā nepieciešamību ES digitālā Covid sertifikāta ieviest ātri, šim lēmumam būtu jāstājas spēkā tā publicēšanas dienā,

([3]) Eiropas Parlamenta un Padomes Regula (ES) 2016/679 (2016. gada 27. aprīlis) par fizisku personu aizsardzību attiecībā uz personas datu apstrādi un šādu datu brīvu apriti un ar ko atceļ Direktīvu 95/46/EK (Vispārīgā datu aizsardzības regula) (OV L 119, 4.5.2016., 1. lpp.).

([4]) Eiropas Parlamenta un Padomes Regula (ES) 2018/1725 (2018. gada 23. oktobris) par fizisku personu aizsardzību attiecībā uz personas datu apstrādi Savienības iestādēs, struktūrās, birojos un aģentūrās un par šādu datu brīvu apriti un ar ko atceļ Regulu (EK) Nr. 45/2001 un Lēmumu Nr. 1247/2002/EK (OV L 295, 21.11.2018., 39. lpp.).

IR PIEŅĒMUSI ŠO LĒMUMU.

1. pants

ES digitālā Covid sertifikāta tehniskās specifikācijas, kurās noteikta vispārīgo datu struktūra, kodēšanas mehānismi un koda pārneses mehānisms mašīnlasāmā optiskā formātā, ir noteikti I pielikumā.

2. pants

Noteikumi par sertifikātu aizpildīšanu, kas minēti Regulas (ES) 2021/953 3. panta 1. punktā, ir izklāstīti šā lēmuma II pielikumā.

3. pants

Prasības par unikālā sertifikāta identifikatora kopīgo struktūru ir izklāstītas III pielikumā.

4. pants

Pārvaldības noteikumi, ko piemēro publiskās atslēgas sertifikātiem saistībā ar ES digitālā Covid sertifikāta vārteju, kura atbalsta uzticamības satvara sadarbspējas aspektus, ir izklāstīti IV pielikumā.

Šis lēmums stājas spēkā dienā, kad to publicē *Eiropas Savienības Oficiālajā Vēstnesī*.

Briselē, 2021. gada 28. jūnijā

Komisijas vārdā –
priekšsēdētāja
Ursula VON DER LEYEN

I PIELIKUMS

FORMĀTS UN UZTICAMĪBAS PĀRVALDĪBA

Vispārīga datu struktūra, kodēšanas mehānismi un koda pārneses mehānisms mašīnlasāmā optiskā formātā (QR)

1. Ievads

Šajā pielikumā izklāstītās tehniskās specifikācijas ietver vispārīgu datu struktūru un kodēšanas mehānismus ES digitālajam Covid sertifikātam (*DCC*). Tajās noteikti arī pārneses kodēšanas mehānismi mašīnlasāmā optiskā formātā (*QR*), ko var attēlot uz mobilās ierīces ekrāna vai izdrukāt uz papīra. Šo specifikāciju elektronisko veselības sertifikātu saturošie formāti ir vispārīgi, bet šajā kontekstā tos izmanto *DCC* pārnesei.

2. Terminoloģija

Šajā pielikumā apzīmējums "izdevēji" attiecas uz organizācijām, kas veselības sertifikātu izdošanai izmanto šīs specifikācijas, un apzīmējums "verificētāji" attiecas uz organizācijām, kas veselības sertifikātus akceptē kā veselības stāvokļa apliecinājumu. "Dalībnieki" ir izdevēji un verificētāji. Daži šajā pielikumā iekļautie aspekti dalībniekiem ir jāsaskaņo, piemēram, nosaukumu telpas pārvaldība un šifrēšanas atslēgu izplatīšana. Tiek pieņemts, ka šos uzdevumus veic kāda puse, ko turpmāk sauc par "sekretariātu".

3. Elektronisko veselības sertifikātu saturošais formāts

Elektronisko veselības sertifikātu saturošais formāts (*HCERT*) ir paredzēts tam, lai nodrošinātu vienotu un standartizētu nesēju veselības sertifikātiem, ko izdevuši dažādi izdevēji ("izdevēji"). Šo specifikāciju mērķis ir harmonizēt to, kā šos veselības sertifikātus attēlo, kodē un paraksta, lai atvieglotu sadarbspēju.

Lai varētu nolasīt un interpretēt jebkura izdevēja izdotu *DCC*, ir vajadzīga vienota datu struktūra un vienošanās par pamatdatu katra datu lauka nozīmīgumu. Sadarbspējas atvieglošanai vienota saskaņotā datu struktūra ir noteikta, izmantojot "JSON" shēmu, kas veido *DCC* struktūru.

3.1. *Pamatdatu struktūra*

Pamatdati ir strukturēti un kodēti kā *CBOR* ar *COSE* digitālo parakstu. To parasti dēvē par "*CBOR* tīmekļa marķieri" (*CWT*), un tas ir definēts *RFC 8392* ([1]). Pamatdatus, kas definēti nākamajās iedaļās, pārnes kā hcert pieprasījumu.

Verificētājam ir jāspēj pārliecināties par pamatdatu izcelsmes integritāti un autentiskumu. Šā mehānisma nodrošināšanai izdevējam ir jāparaksta *CWT*, izmantojot asimetriska elektroniskā paraksta shēmu, kas definēta *COSE* specifikācijā (*RFC 8152* ([2])).

3.2. *CWT pieprasījumi*

3.2.1. CWT struktūras pārskats

Aizsargāta galvene

— Paraksta algoritms (alg, iezīme 1)

— Atslēgas identifikators (kid, iezīme 4)

Pamatdati

— Izdevējs (iss, pieprasījuma atslēga 1, fakultatīvs, izdevēja ISO 3166-1 alpha-2)

— Izdošanas laiks (iat, pieprasījuma atslēga 6)

— Derīguma laiks (exp, pieprasījuma atslēga 4)

— Veselības sertifikāts (hcert, pieprasījuma atslēga -260)

— ES digitālais Covid sertifikāts v1 (eu_DCC_v1, pieprasījuma atslēga 1)

Paraksts

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

3.2.2. Paraksta algoritms

Paraksta algoritma (alg) parametrs norāda paraksta izveidošanai izmantoto algoritmu. Tam ir jāatbilst pašreizējām *SOG-IS* pamatnostādnēm, kas izklāstītas turpmāk, vai jāpārsniedz tās.

Ir definēts viens primārais un viens sekundārais algoritms. Sekundārais algoritms būtu jāizmanto tikai tad, ja primārais algoritms nav pieņemams atbilstoši izdevējam piemērotajiem noteikumiem.

Lai nodrošinātu sistēmas aizsardzību, visos izpildījumos jāiekļauj sekundārais algoritms. Tāpēc ir jāievieš gan primārais, gan sekundārais algoritms.

SOG-IS noteiktie līmeņi primārajam un sekundārajam algoritmam:

— primārais algoritms: primārais algoritms ir eliptiskās līknes digitālā paraksta algoritms (*ECDSA*), kas definēts standarta ISO/IEC 14888–3:2006 2.3. iedaļā, izmantojot P–256 parametrus, kas definēti publikācijas "FIPS PUB 186–4" D (D.1.2.3) papildinājumā, kopā ar SHA–256 kontrolsummas algoritmu, kas definēts standarta ISO/IEC 10118–3:2004 4. funkcijā.

Tas atbilst *COSE* algoritma parametram ES256.

— sekundārais algoritms: sekundārais algoritms ir *RSASSA-PSS*, kas definēts *RFC 8230* ([3]), ar 2048 bitu moduli kopā ar SHA–256 kontrolsummas algoritmu, kas definēts standarta ISO/IEC 10118–3:2004 4. funkcijā.

Tas atbilst *COSE* algoritma parametram PS256.

3.2.3. Atslēgas identifikators

Atslēgas identifikatora (kid) prasījumā norāda dokumenta parakstītāja sertifikātu (*DSC*), kuram ir publiskā atslēga, kas verificētājam jāizmanto, lai pārbaudītu digitālā paraksta pareizību. Publiskās atslēgas sertifikātu pārvaldība, tostarp prasības attiecībā uz *DSC*, ir aprakstītas IV pielikumā.

Atslēgas identifikatora (kid) pieprasījumu verificētāji izmanto, lai atlasītu pareizo publisko atslēgu no atslēgu saraksta, kas attiecas uz izdevēja (iss) pieprasījumā norādīto izdevēju. Administratīvu iemeslu dēļ un atslēgu pārņemšanā izdevējs vienlaikus var izmantot vairākas atslēgas. Atslēgas identifikators nav drošībai būtisks lauks. Tāpēc, ja vajadzīgs, to var ievietot neaizsargātā galvenē. Verificētājiem ir jāpieņem abas iespējas. Ja ir izmantotas abas iespējas, jāizmanto aizsargātajā galvenē ievietotais atslēgas identifikators.

Saistībā ar identifikatora saīsināšanu (izmēra ierobežojuma dēļ) pastāv ļoti maza iespējamība, ka kopējā verificētāja akceptēto *DSC* sarakstā var būt *DSC* ar dubultiem kid. Tāpēc validētājam ir jāpārbauda visi *DSC* ar attiecīgo kid.

3.2.4. Izdevējs

Izdevēja (iss) pieprasījums ir vērtība, kas fakultatīvi var saturēt ISO 3166-1 alpha-2 veselības sertifikāta izdevējstruktūras valsts kodu. Verificētājs šo pieprasījumu var izmantot, lai noteiktu, kura *DSC* kopa jāizmanto verifikācijai. Šā pieprasījuma identificēšanai izmanto pieprasījuma atslēgu 1.

3.2.5. Derīguma laiks

Derīguma laika (exp) pieprasījums satur laika zīmogu, kurš ir vesela skaitļa *NumericDate* formātā (kā noteikts *RFC 8392* ([4]), 2. iedaļā) un kurš norāda, cik ilgi konkrētais paraksts attiecībā uz pamatdatiem ir uzskatāms par derīgu; pēc minētā laika verificētājam pamatdati ir jānoraida. Derīguma parametra nolūks ir ierobežot veselības sertifikāta derīguma periodu. Šā pieprasījuma identificēšanai izmanto pieprasījuma atslēgu 4.

Derīguma laiks nedrīkst pārsniegt *DSC* derīguma periodu.

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

3.2.6. Izdošanas laiks

Izdošanas laika (iat) pieprasījums satur laika zīmogu, kurš ir vesela skaitļa *NumericDate* formātā (kā noteikts *RFC 8392* ([5]), 2. iedaļā) un kurš norāda veselības sertifikāta izveidošanas laiku.

Izdošanas laika laukā norādītais laiks nedrīkst būt pirms *DSC* derīguma perioda sākuma.

Verificētāji drīkst piemērot papildu noteikumus, kuru mērķis ir ierobežot veselības sertifikāta derīgumu, pamatojoties uz izdošanas laiku. Šā pieprasījuma identificēšanai izmanto pieprasījuma atslēgu 6.

3.2.7. Veselības sertifikāta pieprasījums

Veselības sertifikāta (hcert) pieprasījums ir *JSON* (*RFC 7159* ([6])) objekts, kas satur veselības stāvokļa informāciju. Ar vienu un to pašu pieprasījumu var apzīmēt vairākus dažāda veida veselības sertifikātus, un *DCC* ir viens no tiem.

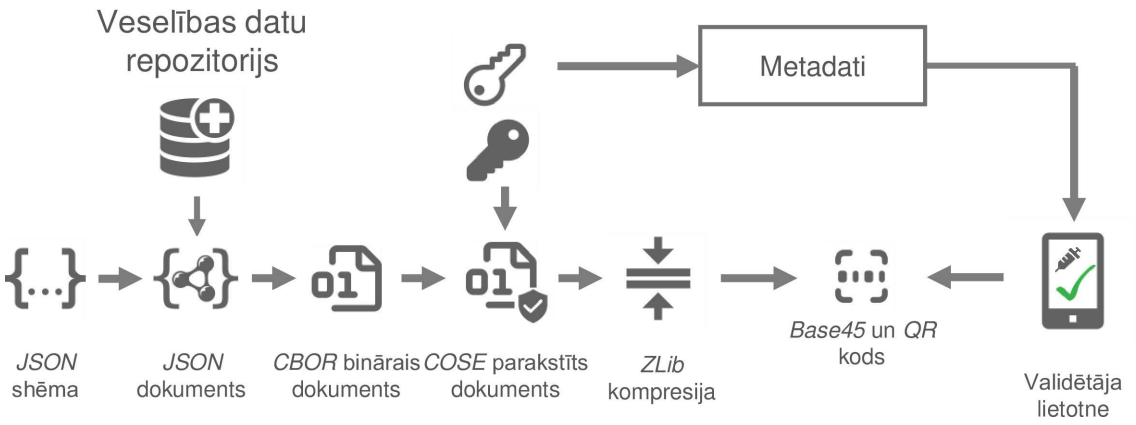
JSON izmanto tikai shematiskām vajadzībām. Tam izmanto *CBOR* atveides formātu, kas noteikts (*RFC 7049* ([7])). Lietotņu izstrādātāji nedrīkst faktiski atkodēt vai kodēt uz *JSON* formātu un no tā, bet gan izmanto atmiņā esošo struktūru.

Šā pieprasījuma identificēšanai izmanto pieprasījuma atslēgu -260.

JSON objekta virknes normalizē atbilstoši *Unicode* standartā definētajai normalizācijas formas kanoniskajai kompozīcijai (*Normalization Form Canonical Composition*, *NFC*). Tomēr atkodēšanas lietotnēm šajā ziņā ir jābūt pielaidīgākām un noturīgākām, un tiek stingri mudināts akceptēt jebkādu piemērota veida konvertēšanu. Ja atkodēšanas laikā vai ar vēlāk izmantotām salīdzināšanas funkcijām tiek konstatēti nenormalizēti dati, izpildījumam būtu jāreaģē tā, it kā ievadītie dati ir normalizēti atbilstoši *NFC*.

4. *DCC* pamatdatu serializēšana un izveide

Serializēšanai izmanto šādu shēmu:



Process sākas ar datu iegūšanu, piemēram, no Veselības datu repozitorija (vai kāda ārēja datu avota), iegūtos datus strukturējot atbilstoši noteiktajām *DCC* shēmām. Šajā procesā, pirms sākas serializēšana uz *CBOR*, var notikt pārvēršana uz noteikto datu formātu un pārveidošana, lai atvieglotu salasāmību cilvēkiem. Pieprasījuma akronīmus kartē katrā gadījumā, lai parādītu nosaukumus pirms serializācijas un pēc deserializācijas.

Sertifikātos, kas izdoti saskaņā ar Regulu (ES) 2021/953 ([8]), fakultatīvais valsts datu saturs nav atļauts. Ir pieļaujams tikai tāds datu saturs, kas atbilst definētajiem datu elementiem minimālajā datu kopā, kura norādīta Regulas 2021/953 pielikumā.

([5]) rfc8392 (ietf.org).
([6]) rfc7159 (ietf.org).
([7]) rfc7049 (ietf.org).
([8]) Eiropas Parlamenta un Padomes Regula (ES) 2021/953 (2021. gada 14. jūnijs) par sadarbspējīgu Covid-19 vakcinācijas, testa un pārslimošanas sertifikātu (ES digitālais Covid sertifikāts) izdošanas, verifikācijas un akceptēšanas satvaru nolūkā atvieglot brīvu pārvietošanos Covid-19 pandēmijas laikā (OV L 211, 15.6.2021., 1. lpp.).

5. **Pārneses kodēšana**

5.1. *Jēldati*

Attiecībā uz dažādām datu saskarnēm *HCERT* konteineru un tā pamatdatus var pārnest tādus, kādi tie ir, izmantojot jebkādu pamatā esošu 8 bitu drošu, uzticamu datu pārnesi. Šādas saskarnes var būt tuva darbības lauka komunikācija (*NFC*), *Bluetooth* vai pārnese pa lietotņslāņa protokolu, piemēram, *HCERT* pārnese no izdevēja uz turētāja mobilo ierīci.

Ja *HCERT* pārnese no izdevēja turētājam pamatā ir tikai uzrādīšanas saskarne (piem., *SMS*, e-pasts), tad jēldatu pārneses kodēšanu, protams, nepiemēro.

5.2. *Svītrkods*

5.2.1. Pamatdatu (CWT) kompresija

Lai samazinātu izmēru un uzlabotu *HCERT* nolasīšanas ātrumu un uzticamību, *CWT* kompresē, izmantojot *ZLIB* (*RFC 1950* ([9])) un *Deflate* kompresijas mehānismu formātā, kas noteikts (*RFC 1951* ([10])).

5.2.2. QR 2D svītrkods

Lai labāk pielāgotos novecojušām iekārtām, ar kurām paredzēts apstrādāt *ASCII* pamatdatus, kompresēto *CWT* pirms kodēšanas 2D svītrkodā kodē kā *ASCII*, izmantojot *Base45*.

2D svītrkoda ģenerēšanai izmanto *QR* formātu, kas noteikts standartā ISO/IEC 18004:2015. Ieteicams izmantot kļūdu labošanas koeficientu "Q" (ap 25 %). Tā kā izmanto *Base45*, *QR* kodam ir jāizmanto burtciparu kodējums (2. režīms, ko apzīmē ar simboliem 0010).

Lai verificētāji spētu noteikt kodēto datu veidu un izvēlēties pareizo atkodēšanas un apstrādes shēmu, *Base45* kodēto datu (atbilstoši šai specifikācijai) priekšā iekļauj kontekstuālā identifikatora virkni "HC1:". Šīs specifikācijas turpmākajās versijās, kas ietekmē atgriezenisko savietojamību, definē jaunu kontekstuālo identifikatoru, rakstzīmes pēc "HC" izvēloties no rakstzīmju kopas [1-9A-Z]. Papildu rakstzīmju secība ir tāda, kā norādīts, t. i., sākumā [1-9] un tad [A-Z].

Optisko kodu ieteicams atveidot uz informācijas nesēja, kura izmērs pa diagonāli ir no 35 mm līdz 60 mm, lai tas būtu pielāgots lasītājiem ar fiksētu optiku, kurai nepieciešams, ka informācijas nesējs ir novietots uz lasītāja virsmas.

Ja optiskais kods ir izdrukāts uz papīra, izmantojot zemas izšķirtspējas (< 300 dpi) printeri, jāraugās, lai katrs *QR* koda simbols (punkts) būtu kvadrāts. Neproporcionālas mērogošanas rezultātā dažās *QR* koda līnijās vai ailēs var rasties taisnstūrveida simboli, kas daudzos gadījumos apgrūtinās nolasīšanu.

6. **Uzticamības saraksta formāts (*CSCA* un *DSC* saraksts)**

Katrai dalībvalstij jāiesniedz saraksts ar vienu vai vairākām valsts parakstīšanas sertificēšanas iestādēm (*CSCA*) un saraksts ar visiem derīgiem dokumentu parakstītāju sertifikātiem (*DSC*), un šie saraksti ir jāatjaunina.

6.1. *Vienkāršots CSCA/DSC*

Sākot ar šo specifikāciju versiju, dalībvalstis nepieņem, ka tiek izmantota sertifikāta atsaukšanas saraksta (*CRL*) informācija vai ka izpildītāji verificē privāto atslēgu lietošanas periodu.

Tā vietā kā primāro derīguma mehānismu izmanto sertifikāta esību jaunākajā sertifikāta saraksta versijā.

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

6.2. *ICAO eMRTD PKI un uzticamības centri*

Dalībvalstis var izmantot atsevišķu *CSCA*, bet var iesniegt arī savus esošos *eMRTD CSCA* sertifikātus un/vai *DSC*; un tās pat var izvēlēties tos iegādāties no (komerciāliem) uzticamības centriem un iesniegt tos. Tomēr *DSC* vienmēr jāparaksta attiecīgās dalībvalsts norādītajai *CSCA*.

7. **Drošības apsvērumi**

Veidojot shēmu uz šīs specifikācijas pamata, dalībvalstis identificē, analizē un uzrauga dažus drošības aspektus.

Jāņem vērā vismaz šādi aspekti:

7.1. *HCERT paraksta derīguma laiks*

HCERT izdevējam ir jāierobežo paraksta derīguma periods, nosakot paraksta derīguma laiku. Tas nozīmē, ka veselības sertifikāta turētājam periodiski sertifikāts ir jāatjaunina.

Pieņemamo derīguma periodu var noteikt praktiski apsvērumi. Piemēram, ceļotājam var nebūt iespēja atjaunot veselības sertifikātu ceļojuma laikā ārvalstīs. Tomēr, iespējams, ka izdevējs ņem vērā kaut kādus drošības apsvērumus, kuru dēļ tam ir jāanulē *DSC* (tādējādi anulējot visus veselības sertifikātus, kas izdoti ar attiecīgo atslēgu, kuras derīguma periods vēl nav beidzies). Šāda notikuma sekas var ierobežot, ja regulāri, bet saprātīgā intervālā maina izdevēja atslēgas un pieprasa atjaunot visus veselības sertifikātus.

7.2. *Atslēgu pārvaldība*

Šī specifikācija lielā mērā ir atkarīga no spēcīgiem kriptogrāfiskiem mehānismiem, ar kuriem nodrošina datu integritāti un datu izcelsmes autentifikāciju. Tāpēc ir nepieciešams saglabāt privāto atslēgu konfidencialitāti.

Kriptogrāfisko atslēgu konfidencialitāte var tikt apdraudēta dažādos veidos, piemēram:

— atslēgas ģenerēšanas process var būt kļūdains, kā rezultātā atslēgas ir vājas,

— atslēgas var tikt atklātas cilvēka kļūdas dēļ,

— atslēgas var nozagt ārējs vai iekšējs likumpārkāpējs,

— atslēgas var aprēķināt, izmantojot kriptoanalīzes metodes.

Lai mazinātu risku, ka paraksta algoritms ir vājš, proti, privāto atslēgu aizsardzību var apdraudēt ar kriptoanalīzes metodēm, šajā specifikācijā visiem dalībniekiem ir ieteikts ieviest sekundāro rezerves paraksta algoritmu, kura pamatā ir atšķirīgi parametri vai atšķirīgas matemātiskās problēmas nekā primārajā algoritmā.

Attiecībā uz risku, kas saistīts ar izdevēju darbības vidi, ir jāveic risku mazinoši pasākumi, ar kuriem nodrošina efektīvu kontroli, piemēram, privāto atslēgu ģenerēšana, uzglabāšana un izmantošana aparatūras drošības moduļos (*HSM*). Veselības sertifikātu parakstīšanai ļoti ieteicams izmantot *HSM*.

Neatkarīgi no tā, vai izdevējs nolemj lietot *HSM*, būtu jāizveido atslēgu maiņas grafiks, kurā atslēgas maiņas biežums ir proporcionāls tam, cik bieži atslēgas nonāk ārējos tīklos, citās sistēmās vai tās apstrādā darbinieki. Labā maiņas grafikā arī vajadzētu ierobežot risku, kas saistīts ar kļūdaini izdotiem veselības sertifikātiem, tādējādi dodot izdevējam iespēju atsaukt šādus veselības sertifikātus visus kopā, vajadzības gadījumā izmantojot vienu atslēgu.

7.3. *Ievades datu validācija*

Šīs specifikācijas var izmantot tādā veidā, kas netieši pieļauj datu saņemšanu no neuzticamiem avotiem tādās sistēmās, kas var būt ļoti svarīgas. Lai līdz minimumam samazinātu risku ar šāda uzbrukuma vektoru, visi ievades dati ir pienācīgi jāvalidē, pārbaudot datu veidu, garumu un saturu. Pirms *HCERT* satura apstrādes jāvalidē arī izdevēja paraksts. Tomēr izdevēja paraksta validēšana netieši nozīmē, kas visupirms tiek parsēta aizsargātā izdevēja galvene, kurā iespējamais uzbrucējs var ievietot īpaši pielāgotu informāciju, ar kuru mazināt sistēmas drošību.

8. **Uzticamības pārvaldība**

Lai verificētu *HCERT* parakstu, ir vajadzīga publiska atslēga. Dalībvalstis minētās publiskās atslēgas dara pieejamas. Katram verificētājam ir jābūt visu uzticamo publisko atslēgu sarakstam (jo publiskā atslēga nav daļa no *HCERT*).

Sistēmai ir (tikai) divi slāņi; katrai dalībvalstij viens vai vairāki valsts līmeņa sertifikāti, ar kuriem paraksta vienu vai vairākus dokumentu parakstītāju sertifikātus, kurus izmanto ikdienas darbībām.

Dalībvalsts sertifikātus dēvē par valsts parakstīšanas sertificēšanas iestādes (*CSCA*) sertifikātiem, un tie (parasti) ir pašparakstīti sertifikāti. Dalībvalstīm var būt vairāk nekā viens sertifikāts (piemēram, reģionālu atšķirību gadījumā). Šos *CSCA* sertifikātus regulāri paraksta ar dokumentu parakstītāju sertifikātiem (*DSC*), ko izmanto *HCERT* parakstīšanai.

"Sekretariāts" ir funkcionāla loma. Tas regulāri apkopo un publicē dalībvalstu *DSC* pēc tam, kad ir tie verificēti, salīdzinot tos ar *CSCA* sertifikātu sarakstu (ko nodod un verificē ar citiem līdzekļiem).

Iegūto *DSC* sarakstu apkopo, lai iegūtu akceptējamo publisko atslēgu kopu (un attiecīgos atslēgas identifikatorus), ko verificētāji var izmantot, lai validētu *HCERT* parakstus. Verificētājiem šis saraksts regulāri jāiegūst un jāatjaunina.

Šādus dalībvalstīm paredzētus sarakstus var pielāgot formātam, ko izmanto valsts līmenī. Šāda uzticamības saraksta datnes formāts var būt atšķirīgs, piemēram, tas var būt parakstīts *JWKS* (*JWK* formāts atbilstoši *RFC 7517* ([11]), 5. iedaļa) vai kādā citā formātā, kas piemērots attiecīgajā dalībvalstī izmantotajai tehnoloģijai.

Vienkāršības labad dalībvalstis var iesniegt esošos *CSCA* sertifikātus no *ICAO eMRTD* sistēmām vai, ievērojot PVO ieteikumu, izveidot īpašu sertifikātu šai veselības jomai.

8.1. *Atslēgas identifikators (kid)*

Atslēgas identifikatoru (*kid*) aprēķina, kad tiek veidots *DSC* uzticamo publisko atslēgu saraksts, un to veido saīsināts *DSC* (pirmie 8 baiti) SHA-256 digitālnospiedums, kas kodēts *DER* (*raw*) formātā.

Verificētājiem nav jāaprēķina *kid*, kura pamatā ir *DSC*, un tas tieši atbilst atslēgas identifikatoram izdotajā veselības sertifikātā, kura *kid* ir uzticamības sarakstā.

8.2. *Atšķirības no ICAO eMRTD PKI uzticamības modeļa*

Lai arī *ICAO eMRTD PKI* uzticamības modeļa pamatā ir paraugprakse, tomēr ātrdarbības labad ir veikti vairāki vienkāršojumi:

— dalībvalstis var iesniegt vairākus *CSCA* sertifikātus,

— *DSC* (atslēgas lietojuma) derīguma periodu var brīvi noteikt, nepārsniedzot *CSCA* sertifikāta derīguma periodu, un to var arī neiekļaut,

— *DSC* var iekļaut noteikumu identifikatorus (paplašināts atslēgas lietojums), kas atbilst veselības sertifikātiem,

— Dalībvalstis var izvēlēties neveikt publisko atsaukumu verifikāciju, bet tā vietā vienkārši paļauties uz *DSC* sarakstiem, ko tās katru dienu saņem no sekretariāta vai apkopo pašas.

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

II PIELIKUMS

NOTEIKUMI ATTIECĪBĀ UZ ES DIGITĀLĀ COVID SERTIFIKĀTA AIZPILDĪŠANU

Vispārīgo noteikumu, kas attiecas uz šajā pielikumā noteiktajām vērtību kopām, mērķis ir nodrošināt sadarbspēju semantiskā līmenī un panākt *DCC* vienotu tehnisko ieviešanu. Šajā pielikumā ietvertos elementus var izmantot trijos dažādos iestatījumos (vakcinācija/tests/pārslimošana), kā noteikts Regulā (ES) 2021/953. Šajā pielikumā ir uzskaitīti tikai tie elementi, kam nepieciešama semantiska standartizācija, izmantojot kodētas vērtību kopas.

Kodēto elementu tulkošana valsts valodā ir dalībvalstu kompetencē.

Visiem datu laukiem, kas nav minēti turpmākajos vērtību kopu aprakstos, ieteicams izmantot *UTF-8* kodējumu (nosaukums, testēšanas centrs, sertifikāta izdevējs). Datu laukus, kuros ir kalendāra datumi (dzimšanas datums, vakcinācijas datums, testa parauga ņemšanas datums, pirmā pozitīvā testa rezultāta datums, sertifikāta derīguma datumi), ieteicams kodēt atbilstoši ISO 8601.

Ja kāda iemesla dēļ turpmāk norādītās vēlamās kodu sistēmas nevar izmantot, tad drīkst izmantot citas starptautiskas kodu sistēmas un izstrādāt ieteikumus par to, kā vēlamajā kodu sistēmā attēlot citas kodu sistēmas kodus. Ja noteiktajās vērtību kopās nav pieejams piemērots kods, izņēmuma gadījumos kā rezerves mehānismu var izmantot tekstu (parādīt nosaukumus).

Dalībvalstīm, kas savās sistēmās izmanto cita veida kodēšanu, šādi kodi būtu jāsamēro ar aprakstītajām vērtību kopām. Par šādu samērošanu atbildīgas ir dalībvalstis.

Komisija ar e-veselības tīkla un Veselības drošības komitejas atbalstu regulāri atjaunina vērtību kopas. Atjauninātās vērtību kopas publicē attiecīgajā Komisijas tīmekļvietnē, kā arī e-veselības tīkla tīmekļa lapā. Jānodrošina izmaiņu vēsture.

1. **Mērķa slimība vai ierosinātājs/slimība, ko sertifikāta turētājs ir pārslimojis, vai tās ierosinātājs: Covid-19 (SARS-CoV-2 vai viens no tā variantiem)**

   Vēlamā kodu sistēma: *SNOMED CT*.

   Jāizmanto sertifikātā Nr. 1, 2, 3.

   Izvēlētie kodi attiecas uz Covid-19 vai, ja vajadzīga sīkāka informācija par SARS-CoV-2 ģenētisko variantu, uz minētajiem variantiem, ja šāda detalizēta informācija ir vajadzīga epidemioloģisku apsvērumu dēļ.

   Izmantojamā koda piemērs: *SNOMED CT* kods 840539006 (Covid-19).

2. **Covid-19 vakcīna vai profilakse**

   Vēlamā kodu sistēma: *SNOMED CT* vai *ATC* klasifikācija.

   Jāizmanto sertifikātā Nr. 1.

   Piemēri no vēlamajām kodu sistēmām izmantojamajiem kodiem: *SNOMED CT* kods 1119305005 (SARS-CoV-2 antigēna vakcīna), 1119349007 (SARS-CoV-2 mRNS vakcīna) vai J07BX03 (Covid-19 vakcīnas). Vērtību kopa būtu jāpaplašina, kad tiek izstrādāti un ieviesti jauni vakcīnu veidi.

3. **Covid-19 vakcīna (zāles)**

   Vēlamās kodu sistēmas (prioritārā secībā):

   — Savienības Zāļu reģistrs, kurā iekļautas ES mērogā atļautas vakcīnas (atļaujas numuri),

   — pasaules mēroga vakcīnu reģistrs, ko varētu izveidot Pasaules Veselības organizācija,

   — pārējos gadījumos vakcīnas (zāļu) nosaukums. Ja nosaukums ietver atstarpes, tās jāaizstāj ar defisi (-).

Vērtību kopas nosaukums: vakcīna.

Jāizmanto sertifikātā Nr. 1.

Piemērs no vēlamajām kodu sistēmām izmantojamajam kodam: EU/1/20/1528 (*Comirnaty*). Vakcīnas nosaukuma, ko izmanto kā kodu, piemērs: Sputnik-V (nozīmē *Sputnik V*).

4. **Covid-19 vakcīnas tirdzniecības atļaujas turētājs vai ražotājs**

Vēlamā kodu sistēma:

— *EMA* organizācijas kods (*SPOR* sistēma attiecībā uz *ISO IDMP*),

— pasaules mēroga vakcīnu tirdzniecības atļaujas turētāju vai ražotāju reģistrs, ko varētu izveidot Pasaules Veselības organizācija,

— pārējos gadījumos organizācijas nosaukums. Ja nosaukums ietver atstarpes, tās jāaizstāj ar defisi (-).

Jāizmanto sertifikātā Nr. 1.

Piemērs no vēlamās kodu sistēmas izmantojamajam kodam: ORG-100001699 (*AstraZeneca AB*). Organizācijas nosaukuma, ko izmanto kā kodu, piemērs: Sinovac-Biotech (nozīmē *Sinovac Biotech*).

5. **Devas kārtas numurs vakcinācijas kursā, kā arī kopējais devu skaits vakcinācijas kursā**

Jāizmanto sertifikātā Nr. 1.

Divi lauki:

1) saņemtās devas kārtas skaitlis vakcinācijas ciklā;

2) pilnā ciklā paredzamo devu skaits (attiecas uz personu devas saņemšanas laikā).

Piemēram, 1/1, 2/2 nozīmē pabeigtu kursu; arī 1/1 norādīšanas iespēja attiecībā uz vakcīnām, kurām paredzētas divas devas, bet kurām dalībvalsts piemēro protokolu, proti, ievadīt vienu devu tām personām, kurām Covid-19 ir diagnosticēts pirms vakcinācijas. Kopējais devu skaits vakcinācijas kursā jānorāda saskaņā ar informāciju, kas pieejama devas saņemšanas laikā. Piemēram, ja konkrētai vakcīnai pēdējās devas saņemšanas laikā ir vajadzīga trešā deva (aktivizējošai iedarbībai), uz to norāda otrais lauka numurs (piemēram, 2/3, 3/3 utt.).

6. **Dalībvalsts vai trešā valsts, kurā saņemta vakcīna/veikts tests**

Vēlamā kodu sistēma: ISO 3166 valstu kodi.

Jāizmanto sertifikātā Nr. 1, 2, 3.

Vērtību kopas saturs: pilns divu burtu kodu saraksts, pieejams kā vērtību kopa, kas noteikta *FHIR* (http://hl7.org/fhir/ValueSet/iso3166-1-2).

7. **Testa veids**

Vēlamā kodu sistēma: *LOINC*.

Jāizmanto sertifikātā Nr. 2, kā arī sertifikātā Nr. 3, ja ar deleģēto aktu tiek ieviests atbalsts tādu pārslimošanas sertifikātu izdošanai, kuru pamatā ir citi testu veidi, nevis *NAAT*.

Kodi šajā vērtību kopā attiecas uz testa metodi, un tos atlasa, lai vismaz nodalītu *NAAT* testus no *RAT* testiem, kā noteikts Regulā (ES) 2021/953.

Piemērs no vēlamās kodu sistēmas izmantojamajam kodam: LP217198-3 (ātrā imūnanalīze).

8. **Izmantotā testa ražotājs un tirdzniecības nosaukums (*NAAT* testa gadījumā fakultatīvi)**

Vēlamā kodu sistēma: Veselības drošības komitejas ātro antigēna testu saraksts, ko uztur *JRC* (Covid-19 *in vitro* diagnostikas iekārtu un testēšanas metožu datubāze).

Jāizmanto sertifikātā Nr. 2.

Vērtību kopas saturs ietver tāda ātrā antigēna testa atlasi, kas iekļauts Covid-19 ātro antigēna testu kopīgajā un atjauninātajā sarakstā, kurš izveidots, pamatojoties uz Padomes Ieteikumu 2021/C 24/01, un saskaņots ar Veselības drošības komiteju. Šo sarakstu uztur *JRC* Covid-19 *in vitro* diagnostikas iekārtu un testēšanas metožu datubāzē, kas pieejama tīmekļa lapā https://covid-19-diagnostics.jrc.ec.europa.eu/devices/hsc-common-recognition-rat.

Šai kodu sistēmai izmanto attiecīgos laukus, piemēram, testa ierīces identifikators, testa nosaukums un ražotājs, ievērojot *JRC* strukturēto formātu, kas pieejams tīmekļa lapā https://covid-19-diagnostics.jrc.ec.europa.eu/devices.

9. **Testa rezultāts**

Vēlamā kodu sistēma: *SNOMED CT*.

Jāizmanto sertifikātā Nr. 2.

Atlasītie kodi ļauj atšķirt pozitīvos un negatīvos testa rezultātus (konstatēts vai nav konstatēts). Nepieciešamības gadījumos var pievienot papildu vērtības (piemēram, nenoteikts).

Piemērs no vēlamajām kodu sistēmām izmantojamajam kodam: 260415000 (nav konstatēts) un 260373001 (konstatēts).

III PIELIKUMS

UNIKĀLĀ SERTIFIKĀTA IDENTIFIKATORA KOPĪGĀ STRUKTŪRA

1. **Ievads**

Katrā ES digitālajā Covid sertifikātā (*DCC*) iekļauj unikālu sertifikāta identifikatoru (*UCI*), kas atbalsta *DCC* sadarbspēju. *UCI* var izmantot sertifikāta verifikācijai. Par *UCI* ieviešanu atbildīgas ir dalībvalstis. *UCI* izmanto, lai pārliecinātos par sertifikāta patiesumu un attiecīgā gadījumā savienotos ar reģistrācijas sistēmu (piemēram, *IIS*). Šie identifikatori arī dalībvalstīm ļauj (papīra formātā un digitāli) apliecināt, ka personas ir vakcinētas vai testētas.

2. **Unikālā sertifikāta identifikatora sastāvs**

UCI veido atbilstoši kopīgai struktūrai un formātam, kas atvieglo informācijas sniegšanu cilvēklasāmā un/vai mašīnlasāmā formātā un var attiekties uz tādiem elementiem kā vakcinācijas dalībvalsts, pati vakcīna un dalībvalsts īpašais identifikators. Tas nodrošina dalībvalstīm elastību *UCI* noformēšanā, pilnībā ievērojot datu aizsardzības tiesību aktus. Atsevišķo elementu secība atbilst noteiktai hierarhijai, kas var iespējot bloku turpmāku pārveidošanu, vienlaikus saglabājot strukturālo integritāti.

Iespējamie risinājumi attiecībā uz *UCI* sastāvu veido spektru, kura divi galvenie dažādojošie parametri ir modularitāte un cilvēklasāms formāts un kuram ir viena pamatīpašība:

— modularitāte: cik lielā mērā kods sastāv no atšķirīgiem veidojošiem blokiem, kas satur semantiski atšķirīgu informāciju,

— cilvēklasāms formāts: cik lielā mērā kods ir jēgpilns vai cik lielā mērā cilvēks to var nolasīt,

— unikalitāte pasaulē: valsts vai iestādes identifikators ir labi pārvaldīts; tiek gaidīts, ka katra valsts (iestāde) labi pārvalda savu nosaukumu telpas segmentu, identifikatorus nekad nereciklē un neizdod atkārtoti. Šāda kombinācija nodrošina, ka katrs identifikators ir pasaulē unikāls.

3. **Vispārīgas prasības**

Attiecībā uz *UCI* ir jāizpilda šādas galvenās prasības:

1) rakstzīmju kopa: ir atļautas tikai lielo burtu *US-ASCII* burtciparu rakstzīmes (no "A" līdz "Z", no "0" līdz "9"), izmantojot *RFC3986* ([1]) ([2]) noteiktās papildu īpašās rakstzīmes atdalīšanai, proti, {"/","#",":"};

2) maksimālais garums: izstrādātājiem jāmēģina sasniegt 27-30 rakstzīmes ([3]);

3) versijas prefikss: attiecas uz *UCI* shēmas versiju. Šīs dokumenta redakcijas versijas prefikss ir "01"; versijas prefiksu veido divi cipari;

4) valsts prefikss: ISO 3166-1 norādītais valsts kods. Garāki kodi (t. i., trīs un vairāk rakstzīmes (piemēram, "UNHCR")) ir rezervēti izmantošanai nākotnē;

5) koda sufikss/kontrolsumma:

5.1. Dalībvalstīm jāizmanto kontrolsumma, ja ir iespējams, ka var rasties pārneses, (cilvēka) pārrakstīšanās vai cita veida kļūdas (t. i., ja izmanto drukātā veidā).

5.2. Kontrolsummu nedrīkst izmantot sertifikāta validēšanā, un tā ir nevis identifikatora tehniskā daļa, bet gan tiek izmantota, lai pārliecinātos par koda integritāti. Šai kontrolsummai jāatbilst ISO-7812-1 (*Luhn-10*) ([4]) kopsavilkumam attiecībā uz visu *UCI* digitāli/pa vadiem pārnestā formātā. Kontrolsummu no pārējā *UCI* atdala ar zīmi "#".

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

([2]) Tādus laukus kā dzimums, partijas/sērijas numurs, vakcinācijas centrs, veselības aprūpes speciālista identifikācija, nākamais vakcinācijas datums drīkst izmantot tikai medicīniskas izmantošanas mērķiem.

([3]) Attiecībā uz īstenošanu ar QR kodiem dalībvalstis varētu apsvērt papildu rakstzīmju kopumu, kura kopējais garums nepārsniedz 72 rakstzīmes (tostarp paša identifikatora 27-30 rakstzīmes), lai sniegtu citu informāciju. Šīs informācijas specifikācija ir dalībvalstu ziņā.

([4]) Lūna *mod N* algoritms ir Lūna algoritma (saukta arī par *mod 10* algoritmu) paplašinājums, kas lietojams ciparu kodiem un ko izmanto, piemēram, kredītkaršu numuru kontrolsummas aprēķināšanai. Paplašinājums ļauj algoritmam darboties ar vērtību sekvencēm jebkurā bāzē (dotajā gadījumā – ar burtciparu rakstzīmēm).

Jānodrošina atgriezeniskā savietojamība: dalībvalstīm, kas laika gaitā maina savu identifikatoru struktūru (galvenās versijas ietvaros, pašlaik v1), jānodrošina, ka jebkuri divi identiski identifikatori attiecas uz vienu un to pašu vakcinācijas sertifikātu/apliecinājumu. Vai, citiem vārdiem sakot, dalībvalstis nedrīkst reciklēt identifikatorus.

4. **Vakcinācijas sertifikātu unikālo sertifikāta identifikatoru iespējas**

E-veselības tīkla pamatnostādnēs par verificējamiem vakcinācijas sertifikātiem un sadarbspējas pamatelementiem ([5]) ir paredzētas atšķirīgas iespējas, kas pieejamas dalībvalstīm un citām pusēm un kas dažādās dalībvalstīs var pastāvēt līdzās. Dalībvalstis var izmantot šādas atšķirīgas iespējas dažādās *UCI* shēmas versijās.

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

IV PIELIKUMS

PUBLISKĀS ATSLĒGAS SERTIFIKĀTU PĀRVALDĪBA

1. Ievads

Drošu un uzticamu ES digitālo Covid sertifikātu (*DCC*) parakstīšanas atslēgu apmaiņu starp dalībvalstīm īsteno ES digitālo Covid sertifikātu vārteja (*DCCG*), kas darbojas kā publisko atslēgu centrālais repozitorijs. *DCCG* dod dalībvalstīm tiesības publicēt publiskās atslēgas, kas atbilst privātajām atslēgām, kuras tās izmanto digitālo Covid sertifikātu parakstīšanai. Piedalīgās dalībvalstis ES digitālo Covid sertifikātu vārteju var izmantot, lai savlaicīgi saņemtu jaunākos materiālus par publiskajām atslēgām. *DCCG* pēc tam var paplašināt, lai apmainītos ar uzticamu papildu informāciju, ko sniedz dalībvalstis, piemēram, par *DCC* validēšanas noteikumiem. *DCC* sistēmas uzticamības modelis ir publiskās atslēgas infrastruktūra (*PKI*). Katrai dalībvalstij ir viena vai vairākas valsts parakstīšanas sertificēšanas iestādes (*CSCA*), kuru sertifikāti ir salīdzinoši ilglaicīgi. Atbilstoši dalībvalsts lēmumam *CSCA* var būt tā pati *CSCA*, ko izmanto mašīnlasāmiem ceļošanas dokumentiem, vai arī cita. *CSCA* izdod publiskās atslēgas sertifikātus īstermiņa valsts dokumentu parakstītājiem (t. i., *DCC* parakstītājiem), un tos sauc par dokumentu parakstītāju sertifikātiem (*DSC*). *CSCA* darbojas kā uzticamības enkurs, kas nodrošina, ka piedalīgās dalībvalstis *CSCA* sertifikātu var izmantot, lai validētu regulāri mainīgo *DSC* autentiskumu un integritāti. Pēc validācijas dalībvalstis šos sertifikātus (vai tikai tajos ietvertās publiskās atslēgas) var izmantot saviem *DCC* validācijas pieteikumiem. Lai autentificētu transakcijas, parakstītu datus, izmantotu par pamatu autentificēšanai un nodrošinātu komunikācijas kanālu integritāti starp dalībvalstīm un *DCCG*, ES digitālo Covid sertifikātu vārteja papildus *CSCA* un *DSC* izmanto arī *PKI*.

Digitālos parakstus var izmantot, lai nodrošinātu datu integritāti un autentiskumu. Publisko atslēgu infrastruktūras ir uzticamas, jo publiskās atslēgas tiek piesaistītas verificētām identitātēm (vai izdevējiem). Tas ir nepieciešams, lai ļautu citiem dalībniekiem pārliecināties par komunikācijas partnera datu izcelsmi un identitāti un lemt par uzticēšanos. ES digitālo Covid sertifikātu vārtejā autentificēšanai tiek izmantoti vairāki publisko atslēgu sertifikāti. Šajā pielikumā ir noteikts, kuri publiskās atslēgas sertifikāti tiek izmantoti un kā tie jāizstrādā tā, lai nodrošinātu plašu sadarbspēju starp dalībvalstīm. Tajā sniegta sīkāka informācija par nepieciešamajiem publiskās atslēgas sertifikātiem un sniegti norādījumi par sertifikātu veidnēm un derīguma periodiem dalībvalstīm, kuras vēlas izmantot savu *CSCA*. Tā kā *DCC* ir verificējami noteiktā laikposmā (no izdošanas brīža līdz beigu termiņam pēc noteikta laika), ir jānosaka verifikācijas modelis attiecībā uz visiem parakstiem, ko izmanto publiskās atslēgas sertifikātos un *DCC*.

2. Terminoloģija

Nākamajā tabulā ir ietverti šajā pielikumā izmantotie saīsinājumi un terminoloģija.

Termins	Definīcija
Sertifikāts	Vai publiskās atslēgas sertifikāts. X.509 v3 sertifikāts, kas satur subjekta publisko atslēgu
CSCA	Valsts parakstīšanas sertificēšanas iestāde
DCC	ES digitālais Covid sertifikāts. Parakstīts elektroniskais dokuments, kas satur informāciju par vakcināciju, testu vai pārslimošanu
DCCG	ES digitālo Covid sertifikātu vārteja. Šo sistēmu izmanto, lai starp dalībvalstīm apmainītos ar *DSC*
$DCCG_{TA}$	*DCCG* uzticamības enkura sertifikāts. Attiecīgo privāto atslēgu izmanto, lai visu *CSCA* sertifikātu sarakstu parakstītu bezsaistē
$DCCG_{TLS}$	*DCCGTLS* servera sertifikāts
DSC	Dokumenta parakstītāja sertifikāts. Dalībvalsts dokumentu parakstītājiestādes (piemēram, sistēma, kas ir pilnvarota parakstīt *DCC*) publiskās atslēgas sertifikāts. Šo sertifikātu izdod dalībvalsts *CSCA*
EC-DSA	Eliptiskās līknes digitālā paraksta algoritms. Paraksta šifrēšanas algoritms, kura pamatā ir eliptiskas līknes
Dalībvalsts	Eiropas Savienības dalībvalsts

Termins	Definīcija
mTLS	Savstarpēja *TLS*. Transporta slāņa drošības protokols ar savstarpēju autentifikāciju
NB	Dalībvalsts nacionālā aizmugursistēma
NB_{CSCA}	Dalībvalsts *CSCA* sertifikāts (var būt vairāk nekā viens)
NB_{TLS}	Nacionālās aizmugursistēmas *TLS* klienta autentifikācijas sertifikāts
NB_{UP}	Sertifikāts, ko nacionālajā aizmugursistēmā izmanto, lai parakstītu datu pakotnes, kas augšupielādētas *DCCG*
PKI	Publiskās atslēgas infrastruktūra. Uzticamības modelis, kura pamatā ir publiskās atslēgas sertifikāti un sertificēšanas iestādes
RSA	Asimetrisks šifrēšanas algoritms, kura pamatā ir sadalīšana reizinātājos, ko izmanto digitālajiem parakstiem vai asimetriskai šifrēšanai

3. ***DCCG* komunikācijas plūsmas un drošības pakalpojumi**

Šajā iedaļā sniegts pārskats par komunikācijas plūsmām un drošības pakalpojumiem *DCCG* sistēmā. Tajā arī noteikts, kuras atslēgas un sertifikātus izmanto, lai aizsargātu komunikāciju, augšupielādēto informāciju, *DCC* un parakstītu uzticamības sarakstu, kurā ir visi ietvertie *CSCA* sertifikāti. *DCCG* darbojas kā datu centrs, kas dalībvalstīm ļauj apmainīties ar parakstīto datu pakotnēm.

Augšupielādētās datu pakotnes ES digitālo Covid sertifikātu vārteja nodrošina "faktiskajā stāvoklī", proti, saņemtajām pakotnēm vārtejā *DSC* netiek pievienoti un netiek no tām izņemti. Dalībvalstu nacionālajai aizmugursistēmai (*NB*) ir jāspēj verificēt augšupielādēto datu pilnīgumu un autentiskumu visā komunikācijas ceļā. Turklāt, lai izveidotu drošu savienojumu, nacionālās aizmugursistēmas un *DCCG* izmanto savstarpēju *TLS* autentifikāciju. Šī darbība papildina parakstus datos, ar kuriem notiek apmaiņa.

3.1. *Autentifikācija un savienojuma izveide*

Lai izveidotu autentificētu šifrētu kanālu starp dalībvalsts nacionālo aizmugursistēmu (*NB*) un vārtejas vidi, *DCCG* izmanto transporta slāņa drošību (*TLS*) ar savstarpēju autentifikāciju. Šajā nolūkā ES digitālo Covid sertifikātu vārtejai ir *TLS* servera sertifikāts (saīsinājumā $DCCG_{TLS}$) un nacionālajām aizmugursistēmām ir *TLS* klienta sertifikāts (saīsinājumā NB_{TLS}). Sertifikātu veidnes ir sniegtas *5. iedaļā*. Katra nacionālā aizmugursistēma var nodrošināt savu *TLS* sertifikātu. Šo sertifikātu skaidri norāda baltajā sarakstā, un tāpēc to var izdot uzticama publiska sertifikācijas iestāde (piemēram, sertifikācijas iestāde, kas atbilst *CA/Browser Forum* pamatprasībām), valsts sertificēšanas iestāde vai tā var būt pašparakstīta. Katra dalībvalsts ir atbildīga par saviem valsts datiem un privātās atslēgas aizsardzību, ko izmanto, lai izveidotu savienojumu ar *DCCG*. Pieeja "lesniedz savu sertifikātu" prasa skaidri definētu reģistrācijas un identifikācijas procesu, kā arī atsaukšanas un atjaunošanas procedūras, kas aprakstītas *4.1., 4.2.* un *4.3. iedaļā*. *DCCG* izmanto balto sarakstu, kurā pēc sekmīgas reģistrācijas tiek pievienoti nacionālo aizmugursistēmu *TLS* sertifikāti. Drošu savienojumu ar *DCCG* var izveidot tikai tādas *NB*, kas autentificējas ar privātu atslēgu, kura atbilst baltajā sarakstā iekļautam sertifikātam. *DCCG* izmanto arī *TLS* sertifikātu, kas ļauj *NB* pārliecināties, ka tās izveido savienojumu ar "patieso" *DCCG*, nevis kādu citu subjektu, kas ļaunprātīgi uzdodas par *DCCG*. Nacionālajām aizmugursistēmām *DCCG* sertifikāts tiek nodrošināts pēc sekmīgas reģistrācijas. $DCCG_{TLS}$ sertifikātu izdod uzticama publiska sertificēšanas iestāde (iekļauta visās lielākajās pārlūkprogrammās). Dalībvalstu pienākums ir pārliecināties, ka to pieslēgums *DCCG* ir drošs (piemēram, pārbaudīt pieslēgtā servera $DCCG_{TLS}$ sertifikāta digitālnospiedumu salīdzinājumā ar digitālnospiedumu, kas sniegts pēc reģistrācijas).

3.2. *Valsts parakstīšanas sertificēšanas iestādes un validācijas modelis*

Dalībvalstīm, kas piedalās *DCCG* satvarā, DSC izdošanai jāizmanto *CSCA*. Dalībvalstīm var būt vairāk nekā viens *CSCA*, piemēram, ja vara nodota reģioniem. Katra dalībvalsts var vai nu izmantot pastāvošas sertificēšanas iestādes, vai izveidot īpašu (varbūt pašparakstītu sertifikātu) sertificēšanas iestādi *DCC* sistēmai.

Dalībvalstīm savi *CSCA* sertifikāti jāuzrāda *DCCG* operatoram oficiālās pievienošanas procedūras gaitā. Kad dalībvalsts būs reģistrēta (*sīkākai informācijai sk. 4.1. iedaļu*), *DCCG* operators atjauninās parakstītu uzticamības sarakstu, kurā ir visi *CSCA* sertifikāti, kas ir aktīvi *DCC* satvarā. *DCCG* operators izmantos īpašu asimetrisku atslēgu pāri, lai uzticamības sarakstu un sertifikātus varētu parakstīt bezsaistes vidē. Šī privātā atslēga netiks uzglabāta tiešsaistes *DCCG* sistēmā, lai gadījumā, ja tiešsaistes sistēma tiktu kompromitēta, uzbrucējs nevarētu kompromitēt uzticamības sarakstu. Nacionālajām aizmugursistēmām pievienošanas procesā tiks izsniegts atbilstošais uzticamības enkura sertifikāts $DCCG_{TA}$.

Dalībvalstis uzticamības sarakstu var iegūt no *DCCG* savām verifikācijas procedūrām. *CSCA* ir definēta kā sertificēšanas iestāde, kas izdod *DSC*, tāpēc dalībvalstīm, kas izmanto daudzlīmeņu *CA* hierarhiju (piemēram, *Root CA -> CSCA -> DSC*), jānorāda padotā sertificēšanas iestāde, kas izdod *DSC*. Šajā gadījumā, ja dalībvalsts izmanto pastāvošu sertificēšanas iestādi, tad *DCC* sistēma ignorēs visu, kas ir virs *CSCA*, un baltajā sarakstā kā uzticamības enkuru iekļaus tikai *CSCA* (kaut arī tā ir padota sertificēšanas iestāde). Tas ir tāpēc, ka *ICAO* modelis pieļauj tikai tieši divus līmeņus – "*root*" *CSCA* un "*leaf*" *DSC*", ko parakstījusi šī konkrētā *CSCA*.

Ja dalībvalstij ir pašai sava *CSCA*, tad dalībvalsts ir atbildīga par šīs sertificēšanas iestādes drošu darbību un atslēgu pārvaldību. *CSCA* funkcionē kā *DSC* uzticamības enkurs, un tāpēc DCC vides integritātes nolūkā būtiski ir aizsargāt *CSCA* privāto atslēgu. Verifikācijas modelis *DCC PKI* ir čaulas modelis, kas nosaka, ka visiem sertifikātiem sertifikātu ķēdes validācijā jābūt derīgiem konkrētajā laika momentā (t. i., paraksta validēšanas laikā). Tāpēc piemēro šādus ierobežojumus:

— *CSCA* neizdod sertifikātus, kas ir derīgi ilgāk nekā pats sertificēšanas iestādes sertifikāts,

— dokumentu parakstītājs neparaksta dokumentus, kas ir derīgi ilgāk nekā pats *DSC*,

— Dalībvalstīm, kurām ir sava *CSCA*, jānosaka derīguma termiņi savai *CSCA* un visiem izdotajiem sertifikātiem, un tām jārūpējas par sertifikātu pagarināšanu.

Ieteikumi par derīguma termiņiem ir izklāstīti *4.2. iedaļā*.

3.3. *Augšupielādēto datu integritāte un autentiskums*

Nacionālās aizmugursistēmas var *DCCG* izmantot digitāli parakstītas datu pakotnes augšupielādēšanai un lejupielādēšanai pēc sekmīgas savstarpējas autentifikācijas. Sākumā šīs datu pakotnes satur dalībvalstu *DSC*. Atslēgu pāri, ko izmanto nacionālajā aizmugursistēmā augšupielādētu datu pakotņu digitālai parakstīšanai *DCCG* sistēmā, sauc par nacionālās aizmugursistēmas augšupielādes paraksta atslēgu pāri, un atbilstošais publiskās atslēgas sertifikāts saīsināti tiek saukts par NB_{UP} sertifikātu. Katrai dalībvalstij ir pašai savs NB_{UP} sertifikāts, kas var būt pašparakstīts vai to var būt izdevusi pastāvoša sertificēšanas iestāde, piemēram, publiska sertificēšanas iestāde (t. i., sertificēšanas iestāde, kas sertifikātu izdod atbilstoši *CAB Forum* pamatprasībām). NB_{UP} sertifikātam jāatšķiras no visiem citiem sertifikātiem, ko izmanto dalībvalsts (t. i., *CSCA*, *TLS* klients vai *DSC*).

Dalībvalstīm jāizsniedz augšupielādes sertifikāts *DCCG* operatoram sākotnējās reģistrācijas procedūras gaitā (*sīkākai informācijai sk. 4.1. iedaļu*). Katra dalībvalsts ir atbildīga par saviem valsts datiem, un tai jāaizsargā privātā atslēga, kas tiek izmantota augšupielāžu parakstīšanai.

Citas dalībvalstis parakstītās datu pakotnes var verificēt, izmantojot augšupielādes sertifikātus, ko sniedz *DCCG*. *DCCG* verificē augšupielādēto datu autentiskumu un integritāti ar *NB* augšupielādes sertifikātu, pirms tie tiek sniegti citām dalībvalstīm.

3.4. *Tehniskās DCCG arhitektūras prasības*

Tehniskās *DCCG* arhitektūras prasības ir šādas.

— *DCCG* izmanto savstarpēju *TLS* autentificēšanu, lai izveidotu autentificētu šifrētu savienojumu ar *NB*. Tāpēc *DCCG* uztur balto sarakstu ar reģistrētiem NB_{TLS} klientu sertifikātiem.

— *DCCG* izmanto divus digitālos sertifikātus ($DCCG_{TLS}$ un $DCCG_{TA}$) ar diviem atšķirīgiem atslēgu pāriem. $DCCG_{TA}$ atslēgu pāra privātā atslēga tiek turēta bezsaistē (nevis uz *DCCG* tiešsaistes komponentiem).

— *DCCG* uztur uzticamības sarakstu ar NB_{CSCA} sertifikātiem, kas tiek parakstīts ar $DCCG_{TA}$ privāto atslēgu.

— Izmantotajiem šifriem jāatbilst prasībām, kas izklāstītas *5.1. iedaļā.*

4. Sertifikātu dzīves cikla pārvaldība

4.1. *Nacionālo aizmugursistēmu reģistrācija*

Lai dalībvalstis varētu piedalīties *DCCG* sistēmā, tām jāreģistrējas pie *DCCG*. Šajā iedaļā ir aprakstīta tehniskā un operatīvā procedūra, kas jāizpilda, lai reģistrētu nacionālo aizmugursistēmu.

DCCG operatoram un dalībvalstij jāapmainās ar informāciju par tehniskajām kontaktpersonām pievienošanas procesā. Pieņem, ka dalībvalstis ir legalizējušas savas tehniskās kontaktpersonas un ka identifikācija/autentifikācija tiek veikta, izmantojot citus kanālus. Piemēram, autentificēšanu var paveikt tad, kad dalībvalsts tehniskā kontaktpersona izsniedz sertifikātus ar paroli aizsargātu datņu veidā pa e-pastu un attiecīgo paroli pasaka *DCCG* operatoram pa tālruni. Var izmantot arī citus drošus kanālus, ko nosaka *DCCG* operators.

Dalībvalstij reģistrācijas un identificēšanas procesā jāsniedz trīs digitālie sertifikāti:

— dalībvalsts *TLS* sertifikāts $NB_{TLS,}$

— dalībvalsts augšupielādes sertifikāts $NB_{UP,}$

— dalībvalsts *CSCA* sertifikāts(-i) $NB_{CSCA.}$

Visiem sniegtajiem sertifikātiem jāatbilst prasībām, kas noteiktas *5. iedaļā*. *DCCG* operators pārbaudīs, vai sniegtais sertifikāts atbilst *5. iedaļā* izklāstītajām prasībām. Pēc identificēšanas un reģistrēšanas *DCCG* operators:

— pievieno NB_{CSCA} sertifikātu(-us) uzticamības sarakstam, kas parakstīts ar privāto atslēgu, kura atbilst $DCCG_{TA}$ publiskajai atslēgai,

— pievieno NB_{TLS} sertifikātu *DCCG TLS* galapunkta baltajam sarakstam,

— ievada NB_{UP} sertifikātu *DCCG* sistēmā,

— izsniedz $DCCG_{TA}$ un $DCCG_{TLS}$ publiskās atslēgas sertifikātu dalībvalstij.

4.2. *Sertificēšanas iestādes, derīguma termiņi un pagarināšana*

Ja dalībvalsts vēlas izmantot savu *CSCA*, *CSCA* sertifikāti var būt pašparakstīti sertifikāti. Tie pilda dalībvalsts uzticamības enkura funkciju, un tāpēc dalībvalstij labi jāaizsargā privātā atslēga, kas atbilst *CSCA* sertifikāta publiskajai atslēgai. Dalībvalstīm savai *CSCA* ir ieteicams izmantot bezsaistes sistēmu, proti, datorsistēmu, kas nav savienota ne ar vienu tīklu. Sistēmas piekļuvei jāizmanto vairāku personu kontrole (piemēram, četru acu princips). Pēc *DSC* parakstīšanas piemēro darbības kontroles, un sistēmu, kurā glabājas privātā *CSCA* atslēga, tur drošībā ar stingru piekļuves kontroli. Lai vēl labāk aizsargātu *CSCA* privāto atslēgu, var izmantot aparatūras drošības moduļus vai viedkartes. Digitālajos sertifikātos ir ietverts derīguma termiņš, kas mudina sertifikātu pagarināt. Pagarināšana ir vajadzīga, lai varētu izmantot jaunas šifrēšanas atslēgas un pielāgot atslēgu izmērus, kad jauni uzlabojumi skaitļošanā vai jauni uzbrukumi kompromitē izmantotā šifrēšanas algoritma drošību. Izmanto čaulas modeli (sk. *3.2. iedaļu*).

Ņemot vērā digitālo Covid sertifikātu viena gada derīguma termiņu, ir ieteicami šādi derīguma termiņi:

— *CSCA*: 4 gadi,

— *DSC*: 2 gadi,

— Augšupielāde: 1–2 gadi,

— *TLS* klienta autentifikācija: 1–2 gadi.

Lai pagarināšana notiktu savlaicīgi, ir ieteicami šādi privāto atslēgu izmantošanas periodi:

— *CSCA*: 1 gads,

— *DSC*: 6 mēneši.

Dalībvalstīm jauni augšupielādes sertifikāti un *TLS* jāizveido savlaicīgi, piemēram, mēnesi pirms derīguma termiņa beigām, lai darbība notiktu bez traucējumiem. *CSCA* sertifikāti un *DSC* jāpagarina vismaz mēnesi pirms privātās atslēgas izmantošanas beigām (ņemot vērā vajadzīgās darbības procedūras). Dalībvalstīm atjauninātie *CSCA* sertifikāti, augšupielādes un *TLS* sertifikāti jāizsniedz *DCCG* operatoram. Sertifikāti, kuriem derīguma termiņš beidzies, jāizņem no baltā saraksta un uzticamības saraksta.

Dalībvalstīm un *DCCG* operatoram pašam jāseko līdzi savu sertifikātu derīgumam. Nav tādu centrālu struktūru, kas sertifikātu derīguma termiņam sekotu līdzi un formētu dalībniekus.

4.3. *Sertifikātu atsaukšana*

Principā digitālos sertifikātus var atsaukt tā sertificēšanas iestāde, kas tos izdevusi, un tam izmanto sertifikātu atsaukšanas sarakstus jeb tiešsaistes sertifikātu statusa pārbaudes protokolu (*OCSP* pakalpojumu). *CSCA* iestādei *DCC* sistēmai jānodrošina sertifikātu atsaukšanas saraksti (*CRL*). Lai arī citas dalībvalstis šos *CRL* pašlaik neizmanto, tiem jābūt integrētiem izmantošanai nākotnē. Ja *CSCA* nolemj *CRL* nenodrošināt, šīs *CSCA DSC* jābūt pagarinātiem, kad *CRL* kļūs obligāti. Verificētājiem *DSC* validēšanai jāizmanto *CRL*, nevis *OCSP*. Nacionālajai aizmugursistēmai ieteicams validēt no *DCC* vārtejas lejupielādētos *DSC* un pārsūtīt nacionālajiem *DCC* validētājiem tikai noteiktus uzticamus un validētus *DSC*. *DCC* validētājiem savā validācijas procesā nevajadzētu veikt nekādu *DSC* atsaukšanas pārbaudi. Viens iemesls ir tāds, lai aizsargātu *DCC* īpašnieku privātumu, nepieļaujot nekādu iespēju, ka kāda konkrēta DSC izmantošanu varētu pārraudzīt ar to saistītais *OCSP*.

Dalībvalstis var pašas no *DCCG* izņemt savus *DSC*, izmantojot derīgus augšupielādes un *TLS* sertifikātus. *DSC* izņemšana nozīmē, ka visi *DCC*, kas izdoti ar šo *DSC*, kļūs nederīgi, kad dalībvalstis dabūs atjauninātos *DSC* sarakstus. Ļoti svarīgi ir aizsargāt privāto atslēgu materiālu, kas atbilst *DSC*. Dalībvalstīm jāinformē *DCCG* operators, kad tām jāatsauc augšupielādes vai *TLS* sertifikāti, piemēram, tāpēc, ka ir kompromitēta nacionālā aizmugursistēma. *DCCG* operators tad var noņemt uzticamību skartajam sertifikātam, piemēram, izņemot to no *TLS* baltā saraksta. *DCCG* operators var izņemt augšupielādes sertifikātus no *DCCG* datubāzes. Pakotnes, kas parakstītas ar privāto atslēgu, kura atbilst šim augšupielādes sertifikātam, kļūs nederīgas, kad nacionālās aizmugursistēmas noņems atceltā augšupielādes sertifikāta uzticamību. Ja jāatsauc *CSCA* sertifikāts, dalībvalstis informē *DCCG* operatoru, kā arī citas dalībvalstis, ar kurām tām ir uzticamības attiecības. *DCCG* operators izdos jaunu uzticamības sarakstu, kurš vairs nesatur skarto sertifikātu. Visi šīs *CSCA* izdotie *DSC* kļūs nederīgi, kad dalībvalstis atjauninās savu nacionālās aizmugursistēmas uzticamības krātuvi. Ja jāatceļ $DCCG_{TLS}$ sertifikāts vai $DCCG_{TA}$ sertifikāts, *DCCG* operatoram un dalībvalstīm jāsadarbojas un jāizveido jauns uzticams *TLS* savienojums un uzticamības saraksts.

5. **Sertifikātu veidnes**

Šajā iedaļā ir izklāstītas šifrēšanas prasības un norādījumi, kā arī sertifikātu veidņu prasības. Šajā iedaļā ir noteiktas *DCCG* sertifikātu veidnes.

5.1. *Šifrēšanas prasības*

Šifrēšanas algoritmus un *TLS* šifra komplektus izvēlas, pamatojoties uz Vācijas Federālā informācijas drošības biroja (*BSI*) vai *SOG-IS* pašreizējo ieteikumu. Šie un citu iestāžu un standartizācijas organizācijas ieteikumi ir līdzīgi. Ieteikumi ir atrodami tehniskajos norādījumos Nr. TR 02102-1 un Nr. TR 02102-2 ([1]) vai dokumentā "*SOG-IS Agreed Cryptographic Mechanisms* ([2])".

5.1.1. Prasības attiecībā uz *DSC*

Piemēro prasības, kas izklāstītas *I pielikuma 3.2.2. iedaļā*. Tāpēc ir stingri ieteicams, lai dokumentu parakstītāji izmantotu *ECDSA* (*Elliptic Curve Digital Signature Algorithm*) ar NIST-p-256 (kas definēts FIPS PUB 186-4 D papildinājumā). Citas eliptiskās līknes netiek atbalstītas. Tā kā digitālajā Covid sertifikātā trūkst vietas,

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

dalībvalstīm nevajadzētu izmantot *RSA-PSS*, lai arī tas atļauts kā rezerves algoritms. Ja dalībvalstis *RSA-PSS* izmanto, izmantotajam modulim jābūt 2048 vai maks. 3072 bitus lielam. Par DSC paraksta šifrēšanas jaucējfunkciju izmanto *SHA*-2 ar izvades garumu ≥ 256 biti (sk. ISO/IEC 10118-3:2004).

5.1.2. *TLS*, augšupielādes un *CSCA* sertifikātu prasības

Digitālajiem sertifikātiem un šifrēšanas parakstiem *DCCG* kontekstā galvenās prasības attiecībā uz šifrēšanas algoritmiem un atslēgu garumu ir rezumētas turpmāk dotajā tabulā (no 2021. gada).

Paraksta algoritms	Atslēgas izmērs	Jaucējfunkcija
EC-DSA	Min. 250 biti	*SHA*-2 ar izvades garumu ≥ 256 biti
RSA-PSS (ieteicamais papildinājums) RSA-PKCS#1 v1.5 (mantotais papildinājums)	Min. 3000 bitu *RSA* modulis (N) ar publisko eksponentu e > 2^16	*SHA*-2 ar izvades garumu ≥ 256 biti
DSA	Min. 3000 bitu prime p, 250 bitu atslēga q	*SHA*-2 ar izvades garumu ≥ 256 biti

Ieteicamā *EC-DSA* eliptiskā līkne ir NIST-p-256, pamatojoties uz tās plašo izmantojumu.

5.2. *CSCA sertifikāts (NB_{CSCA})*

Turpmāk dotajā tabulā ir norādījumi par NB_{CSCA} sertifikāta veidni, ja dalībvalsts nolemj *DCC* sistēmai izmantot savu *CSCA*.

Treknrakstā iespiestie ieraksti ir obligāti (jābūt iekļautiem sertifikātā), *slīprakstā* iespiestie ieraksti ir ieteikti (vajadzētu iekļaut). Tukšie lauki nozīmē, ka par tiem ieteikumu nav.

Lauks	Vērtība
Tēma	**cn=<netukšs un unikāls vispārīgais nosaukums>,** *o=<Nodrošinātājs>*,**c=<Dalībvalsts, kas izmanto *CSCA*>**
Atslēgas lietojums	**certificate signing,***CRL signing* (vismaz)
Pamatierobežojumi	**CA = true, path length constraints = 0**

Tēmas nosaukumam jābūt netukšam un unikālam norādītajā dalībvalstī. Valsts kodam (c) jāatbilst dalībvalstij, kas šo *CSCA* sertifikātu izmantos. Sertifikātam jāsatur unikāls tēmas atslēgas identifikators (*SKI*), kas atbilst *RFC* 5280 ([3]).

5.3. *Dokumenta parakstītāja sertifikāts (DSC)*

Turpmāk dotajā tabulā ir norādījumi par *DSC*. **Treknrakstā** iespiestie ieraksti ir obligāti (jābūt iekļautiem sertifikātā), *slīprakstā* iespiestie ieraksti ir ieteikti (vajadzētu iekļaut). Tukšie lauki nozīmē, ka par tiem ieteikumu nav.

Lauks	Vērtība
Sērijas numurs	**unikālais sērijas numurs**
Tēma	**cn=<netukšs un unikāls kopējais nosaukums>,***o=<Nodrošinātājs>*, **c=<Dalībvalsts, kas izmanto *CSCA*>**
Atslēgas lietojums	**digital signature** (vismaz)

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

DSC jāparaksta ar privāto atslēgu, kas atbilst *CSCA* sertifikātam, kuru dalībvalsts izmanto.

Jāizmanto šādi paplašinājumi.

— Sertifikātam jāsatur sertificēšanas iestādes atslēgas identifikators (*AKI*), kas atbilst izdevējas *CSCA* sertifikāta tēmas atslēgas identifikatoram (*SKI*).

— Sertifikātam jāsatur unikāls tēmas atslēgas identifikators (atbilstoši *RFC* 5280 ([4])).

Turklāt sertifikātam jāsatur *CRL* izplatīšanas punkta pagarinājums, kas norāda uz sertifikāta atsaukšanas sarakstu (*CRL*), ko nodrošina *CSCA*, kas *DSC* izdevusi.

DSC var saturēt paplašinātas atslēgas lietošanas paplašinājumu ar nulles vai vairākiem atslēgas lietojuma politikas identifikatoriem, kas ierobežo to, kāda veda *HCERT* ar šo sertifikātu atļauts verificēt. Ja ir viens vai vairāki identifikatori, verificētāji pārbauda atslēgas lietojumu pret uzglabāto *HCERT*. Šim nolūkam ir noteiktas šādas paplašinātas atslēgas lietošanas (*extendedKeyUsage*) vērtības

Lauks	Vērtība
extendedKeyUsage	1.3.6.1.4.1.1847.2021.1.1“testa” izdevējiem
extendedKeyUsage	1.3.6.1.4.1.1847.2021.1.2 “vakcinācijas” izdevējiem
extendedKeyUsage	1.3.6.1.4.1.1847.2021.1.3 “pārslimošanas” izdevējiem

Ja atslēgas lietojuma paplašinājuma nav (proti, paplašinājuma nav vai paplašinājums ir nulle), šo sertifikātu var izdot, lai validētu jebkāda veida *HCERT*. Citi dokumenti var noteikt attiecīgos papildu paplašinātās atslēgas lietošanas politikas identifikatorus, kas tiek izmantoti ar HCERT validēšanu.

5.4. *Augšupielādes sertifikāti (NBUP)*

Turpmāk dotajā tabulā ir norādījumi par nacionālās aizmugursistēmas augšupielādes sertifikātu. **Treknrakstā** iespiestie ieraksti ir obligāti (jābūt iekļautiem sertifikātā), *slīprakstā* iespiestie ieraksti ir ieteikti (vajadzētu iekļaut). Tukšie lauki nozīmē, ka par tiem ieteikumu nav.

Lauks	Vērtība
Tēma	**cn=<netukšs un unikāls kopējais nosaukums>,** *o=<Nodrošinātājs>*,**c=<Dalībvalsts, kas izmanto šo augšupielādes sertifikātu>**
Atslēgas lietojums	**digital signature** (vismaz)

5.5. *Nacionālās aizmugursistēmas TLS klienta autentificēšana (NB_{TLS})*

Turpmāk dotajā tabulā ir norādījumi par nacionālās aizmugursistēmas *TLS* klienta autentificēšanas sertifikātu. **Treknrakstā** iespiestie ieraksti ir obligāti (jābūt iekļautiem sertifikātā), *slīprakstā* iespiestie ieraksti ir ieteikti (vajadzētu iekļaut). Tukšie lauki nozīmē, ka par tiem ieteikumu nav.

Lauks	Vērtība
Tēma	**cn=<netukšs un unikāls vispārīgais nosaukums>,** *o=<Nodrošinātājs>*,**c=<Dalībvalsts NB>**
Atslēgas lietojums	**digital signature** (vismaz)
Paplašināta atslēgas lietošana	client authentication (1.3.6.1.5.5.7.3.2)

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

Sertifikātā var būt iekļauts arī paplašinātais atslēgas lietojums *server authentication (1.3.6.1.5.5.7.3.1)*, bet tas nav obligāts.

5.6. *Uzticamības saraksta paraksta sertifikāts ($DCCG_{TA}$)*

Turpmāk dotajā tabulā ir definēts *DCCG* uzticamības enkura sertifikāts.

Lauks	Vērtība
Tēma	**cn = Digital Green Certificate Gateway** ([5]), **o=<Nodrošinātājs>, c=<valsts>**
Atslēgas lietojums	**digital signature** (vismaz)

5.7. *DCCG TLS servera sertifikāti ($DCCG_{TLS}$)*

Turpmāk dotajā tabulā ir definēts *DCCG TLS* sertifikāts.

Lauks	Vērtība
Tēma	cn=<FQDN vai *DCCG* IP adrese>, o=<Nodrošinātājs>, c=<valsts>
SubjectAltName	dNSName: <*DCCG DNS* nosaukums> vai iPAddress: <*DCCG* IP adrese>
Atslēgas lietojums	**digital signature** (vismaz)
Extended Key usage	server authentication (1.3.6.1.5.5.7.3.1)

Sertifikātā var būt iekļauts arī paplašinātais atslēgas lietojums *client authentication (1.3.6.1.5.5.7.3.2)*, bet tas nav obligāts.

DCCG TLS sertifikātu izdod publiski uzticama sertificēšanas iestāde (iekļauta visos lielākajās pārlūkprogrammās un operētājsistēmās, ievērojot *CAB Forum* pamatprasības).

([5]) Šajā kontekstā ir saglabāts termins "*digitālais zaļais sertifikāts*" (Digital Green Certificate), nevis "ES digitālais Covid sertifikāts" (EU Digital COVID Certificate), jo tas ir termins, kas tika izmantots sertifikātā ar aparatūras kodu, pirms likumdevējiestādes nolēma lietot jaunu terminu.