KOMISIJOS ĮGYVENDINIMO SPRENDIMAS (ES) 2021/1073

2021 m. birželio 28 d.

kuriuo nustatomos ES skaitmeninio COVID pažymėjimo patikimumo užtikrinimo sistemos, nustatytos Europos Parlamento ir Tarybos reglamentu (ES) 2021/953, techninės specifikacijos ir įgyvendinimo taisyklės

(Tekstas svarbus EEE)

EUROPOS KOMISIJA,

atsižvelgdama į Sutartį dėl Europos Sąjungos veikimo,

atsižvelgdama į Europos Parlamento ir Tarybos reglamentą (ES) 2021/953 dėl sąveikiųjų COVID-19 skiepijimo, tyrimo ir persirgimo pažymėjimų (ES skaitmeninio COVID pažymėjimo) išdavimo, tikrinimo ir pripažinimo sistemos, kuria siekiama sudaryti palankesnes sąlygas asmenims laisvai judėti COVID-19 pandemijos metu ([1]), ypač į jo 9 straipsnio 1 ir 3 dalis,

kadangi:

(1) Reglamentu (ES) 2021/953 sukurto ES skaitmeninio COVID pažymėjimo tikslas – įrodyti, kad asmuo buvo paskiepytas nuo COVID-19, jo tyrimo rezultatas yra neigiamas arba jis yra persirgęs šia infekcija;

(2) kad ES skaitmeninis COVID pažymėjimas būtų tinkamas naudoti visoje Sąjungoje, būtina nustatyti technines specifikacijas ir taisykles, kuriomis būtų užtikrinta galimybė pildyti, saugiai išduoti ir tikrinti skaitmeninius COVID pažymėjimus, užtikrinta asmens duomenų apsauga, nustatyta bendra unikalaus pažymėjimo identifikatoriaus struktūra ir sudarytos sąlygos generuoti galiojantį, saugų ir sąveikų brūkšninį kodą. Ta patikimumo užtikrinimo sistema taip pat siekiama užtikrinti sąveikumą su tarptautiniais standartais ir technologinėmis sistemomis, todėl ji galėtų tapti pavyzdžiu plėtojant bendradarbiavimą pasaulio mastu;

(3) kad ES skaitmeninį COVID pažymėjimą būtų įmanoma nuskaityti ir suprasti, būtina nustatyti bendrą duomenų struktūrą ir susitarti dėl kiekvieno naudingųjų duomenų laukelio numatytosios paskirties ir galimų verčių. Kad būtų lengviau užtikrinti tokį sąveikumą, būtina nustatyti bendrą suderintą ES skaitmeninio COVID pažymėjimo sistemos duomenų struktūrą. Pagal Europos Parlamento ir Tarybos direktyvą 2011/24/ES ([2]) įsteigtas E. sveikatos tinklas yra parengęs gaires dėl šios sistemos. Į jas turėtų būti atsižvelgta nustatant su ES skaitmeninio COVID pažymėjimo formatu ir patikimumo užtikrinimu susijusias technines specifikacijas. Turėtų būti pateiktos duomenų struktūros specifikacijos, nurodyti kodavimo mechanizmai, taip pat aprašytas perduodamų duomenų kodavimo kompiuterio skaitomu optiniu formatu (QR kodu, kuris gali būti rodomas mobiliojo įrenginio ekrane arba spausdinamas popieriuje) mechanizmas;

(4) be techninių specifikacijų, susijusių su ES skaitmeninio COVID pažymėjimo formatu ir patikimumo užtikrinimu, turėtų būti nustatytos bendrosios pažymėjimų pildymo taisyklės, kurių laikantis ES skaitmeniniuose COVID pažymėjimuose būtų galima naudoti koduotas reikšmes. Komisija turėtų, atsižvelgdama į atitinkamą E. sveikatos tinklo darbą, reguliariai atnaujinti ir skelbti toms taisyklėms įgyvendinti reikalingus reikšmių rinkinius;

(5) Reglamente (ES) 2021/953 nustatyta, kad, atsižvelgiant į tai, jog Reglamento (ES) 2021/953 galiojimo laikotarpiu piliečiams gali būti išduotas daugiau nei vienas pažymėjimas, kiekvienas ES skaitmeninį COVID pažymėjimą sudarantis autentiškas pažymėjimas turėtų būti atskirai identifikuojamas naudojant unikalų pažymėjimo identifikatorių. Unikalų pažymėjimo identifikatorių turi sudaryti raidžių ir skaitmenų eilutė, o valstybės narės turėtų užtikrinti, kad jame nebūtų jokių duomenų, siejančių jį su kitais dokumentais ar identifikatoriais, pavyzdžiui, su paso ar tapatybės kortelės numeriais, t. y. kad pagal jį nebūtų įmanoma nustatyti turėtojo tapatybės. Siekiant užtikrinti, kad pažymėjimo identifikatorius būtų unikalus, turėtų būti nustatytos techninės specifikacijos ir taisyklės, susijusios su bendra jo struktūra;

([1]) OL L 211, 2021 6 15, p. 1.

([2]) 2011 m. kovo 9 d. Europos Parlamento ir Tarybos direktyva 2011/24/ES dėl pacientų teisių į tarpvalstybines sveikatos priežiūros paslaugas įgyvendinimo (OL L 88, 2011 4 4, p. 45).

(6) kad ES skaitmeninį COVID pažymėjimą sudarantys pažymėjimai būtų pripažįstami visose valstybėse narėse, labai svarbu užtikrinti jų saugumą, autentiškumą, galiojimą, vientisumą ir atitiktį Sąjungos duomenų apsaugos teisės aktams. Įgyvendinti šiuos tikslus padeda patikimumo užtikrinimo sistema, kuria nustatomos patikimo ir saugaus ES skaitmeninių COVID pažymėjimų išdavimo ir tikrinimo taisyklės bei infrastruktūra. Be kita ko, patikimumo užtikrinimo sistema turėtų būti grindžiama viešojo rakto infrastruktūra, o patikimumo užtikrinimo grandinė turėtų apimti įvairius subjektus: nuo valstybių narių sveikatos institucijų ar kitų patikimų institucijų iki atskirų ES skaitmeninius COVID pažymėjimus išduodančių subjektų. Todėl, siekdama užtikrinti ES masto sąveikumą, Komisija sukūrė centrinę sistemą – ES skaitmeninio COVID pažymėjimo tinklų sietuvą (toliau – tinklų sietuvas), kuriame saugomi patikrinimui naudojami viešieji raktai. Naudojant atitinkamus tame tinklų sietuve anksčiau išsaugotus viešuosius raktus, nuskenavus pažymėjimų QR kodus yra patikrinami skaitmeniniai parašai. Skaitmeniniai parašai gali būti naudojami duomenų vientisumui ir autentiškumui užtikrinti. Viešojo rakto infrastruktūra padeda užtikrinti patikimumą, nes viešieji raktai joje yra susiejami su pažymėjimus išduodančiais subjektais. Tinklų sietuve autentiškumui užtikrinti naudojama daugybė viešojo rakto sertifikatų. Siekiant užtikrinti, kad valstybės narės galėtų saugiai keistis viešųjų raktų duomenimis, ir sudaryti sąlygas plataus masto sąveikumui, būtina nustatyti, kokie viešojo rakto sertifikatai gali būti naudojami ir kaip jie turėtų būti generuojami;

(7) šis sprendimas sudaro sąlygas Reglamente (ES) 2021/953 nustatytus reikalavimus įgyvendinti taip, kad būtų tvarkomi tik tie asmens duomenys, kurių reikia, kad ES skaitmeninis COVID pažymėjimas būtų tinkamas naudoti, ir padeda užtikrinti, kad galutiniai duomenų valdytojai šios srities veiklą vykdytų laikydamiesi pritaikytosios duomenų apsaugos reikalavimų;

(8) Reglamente (ES) 2021/953 nustatyta, kad Europos Parlamento ir Tarybos reglamento (ES) 2016/679 ([3]) 4 straipsnio 7 punkte nurodytais duomenų valdytojais laikomos už pažymėjimų išdavimą atsakingos valdžios institucijos ar kitos paskirtosios įstaigos, kurios vykdydamos išdavimo procesą tvarko asmens duomenis. Priklausomai nuo to, kaip valstybės narės organizuoja išdavimo procesą, jį gali vykdyti viena arba kelios institucijos ar paskirtosios įstaigos, pavyzdžiui, regioninės sveikatos tarnybos. Pagal subsidiarumo principą sprendimą šiuo klausimu priima valstybės narės. Todėl jos gali geriausiai užtikrinti, kad tais atvejais, kai esama kelių institucijų ar paskirtųjų įstaigų, būtų aiškiai nustatyta kiekvienos iš jų atsakomybė, nesvarbu, ar jos būtų atskiros, ar bendros duomenų valdytojos (be kita ko, regioninės sveikatos tarnybos, sukūrusios bendrą pacientams skirtą pažymėjimų išdavimo portalą). Pažymėjimus tikrinančios kelionės tikslo ar tranzito valstybės narės kompetentingos institucijos arba tarpvalstybinių keleivių vežimo paslaugų teikėjai, kurie pagal nacionalinę teisę COVID-19 pandemijos metu turi įgyvendinti tam tikras visuomenės sveikatos priemones, taip pat turi vykdyti savo pareigas pagal duomenų apsaugos taisykles;

(9) ES skaitmeninio COVID pažymėjimo tinklų sietuve netvarkomi jokie asmens duomenys, nes jame saugomi tik pasirašančiųjų institucijų viešieji raktai. Tie raktai yra susiję su pasirašančiosiomis institucijomis ir nesuteikia galimybės nei tiesiogiai, nei netiesiogiai atkurti fizinio asmens, kuriam išduotas pažymėjimas, tapatybės. Taigi Komisija, kaip tinklų sietuvo administratorė, neturėtų būti nei asmens duomenų valdytoja, nei jų tvarkytoja;

(10) vadovaujantis Europos Parlamento ir Tarybos reglamento (ES) 2018/1725 ([4]) 42 straipsnio 1 dalimi, buvo konsultuojamasi su Europos duomenų apsaugos priežiūros pareigūnu ir jis pateikė nuomonę 2021 m. birželio 22 d.;

(11) atsižvelgiant į tai, kad, norint taikyti Reglamentą (ES) 2021/953 nuo 2021 m. liepos 1 d., būtina nustatyti technines specifikacijas ir taisykles, yra pagrįsta šį sprendimą taikyti nedelsiant;

(12) todėl, atsižvelgiant į poreikį skubiai įgyvendinti ES skaitmeninio COVID pažymėjimo sistemą, šis sprendimas turėtų įsigalioti jo paskelbimo dieną,

([3]) 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamentas (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo, kuriuo panaikinama Direktyva 95/46/EB (Bendrasis duomenų apsaugos reglamentas) (OL L 119, 2016 5 4, p. 1).

([4]) 2018 m. spalio 23 d. Europos Parlamento ir Tarybos reglamentas (ES) 2018/1725 dėl fizinių asmenų apsaugos Sąjungos institucijoms, organams, tarnyboms ir agentūroms tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo, kuriuo panaikinamas Reglamentas (EB) Nr. 45/2001 ir Sprendimas Nr. 1247/2002/EB (OL L 295, 2018 11 21, p. 39).

PRIĖMĖ ŠĮ SPRENDIMĄ:

1 straipsnis

I priede išdėstomos techninės ES skaitmeninio COVID pažymėjimo specifikacijos, kuriomis nustatoma bendroji duomenų struktūra, kodavimo mechanizmai ir perduodamų duomenų kodavimo kompiuterio skaitomu optiniu formatu mechanizmas.

2 straipsnis

Šio sprendimo II priede nustatomos Reglamento (ES) 2021/953 3 straipsnio 1 dalyje nurodytų pažymėjimo pildymo taisyklės.

3 straipsnis

III priede išdėstomi reikalavimai, kuriais nustatoma bendra unikalaus pažymėjimo identifikatoriaus struktūra.

4 straipsnis

IV priede nustatomos ES skaitmeninio COVID pažymėjimo tinklų sietuve naudojamų viešųjų raktų sertifikatų valdymo taisyklės, padedančios įgyvendinti patikimumo užtikrinimo sistemos sąveikumo aspektus.

Šis sprendimas įsigalioja jo paskelbimo *Europos Sąjungos oficialiajame leidinyje* dieną.

Priimta Briuselyje 2021 m. birželio 28 d.

Komisijos vardu
Pirmininkė
Ursula VON DER LEYEN

I PRIEDAS

FORMATAS IR PATIKIMUMO VALDYMAS

Bendroji duomenų struktūra, kodavimo mechanizmai ir perduodamų duomenų kodavimo kompiuterio skaitomu optiniu formatu (toliau – QR) mechanizmas

1. Įžanga

Šiame priede išdėstytose techninėse specifikacijose pateikiama ES skaitmeninio COVID pažymėjimo (toliau – SCP) bendroji duomenų struktūra ir kodavimo mechanizmai. Jose taip pat apibrėžtas perduodamų duomenų kodavimo kompiuterio skaitomu optiniu formatu (QR kodu, kuris gali būti rodomas mobiliojo įrenginio ekrane arba spausdinamas popieriuje) mechanizmas. Šiose specifikacijose nurodyti elektroninio sveikatos pažymėjimo rinkmenų formatai yra bendri, tačiau šiomis aplinkybėmis naudojami ES skaitmeniniam COVID pažymėjimo (SCP) duomenims perduoti.

2. Terminai

Šiame priede išdavėjai yra organizacijos, naudojančios šias specifikacijas sveikatos pažymėjimams išduoti, o tikrintojai yra organizacijos, priimančios sveikatos pažymėjimus kaip sveikatos būklės įrodymą. Dalyviai yra išdavėjai ir tikrintojai. Kai kuriuos šiame priede nurodytus aspektus, pavyzdžiui, vardų erdvių valdymą ir kriptografinių raktų paskirstymą, dalyviai turi derinti tarpusavyje. Daroma prielaida, kad šias užduotis atlieka šalis, toliau vadinama sekretoriatu.

3. Elektroninio sveikatos pažymėjimo rinkmenos formatas

Elektroninio sveikatos pažymėjimo rinkmenos formatas (toliau – HCERT) sukurtas, kad būtų galima naudoti vienodą ir standartizuotą priemonę, skirtą sveikatos pažymėjimams iš įvairių juos išdavusių subjektų (toliau – išdavėjų) talpinti. Šių specifikacijų tikslas – suderinti tokių sveikatos pažymėjimų atvaizdavimą, kodavimą ir pasirašymą, siekiant palengvinti sąveikumą.

Kad būtų galima nuskaityti ir suprasti bet kurio išdavėjo išduotą SCP, reikalinga bendra duomenų struktūra ir susitarimas dėl kiekvienos naudingųjų duomenų laukelio reikšmės. Siekiant palengvinti sąveikumą, bendra suderinta duomenų struktūra apibrėžiama naudojant JSON schemą, kurios pagrindu suformuota SCP sistema.

3.1. *Naudingųjų duomenų struktūra*

Naudingieji duomenys struktūruojami ir koduojami CBOR formatu, naudojant COSE skaitmeninį parašą. Jis paprastai vadinamas CBOR saityno atpažinimo ženklu (angl. *CBOR Web Token*, CWT) ir yra apibrėžtas standarte RFC 8392 ([1]). Naudingieji duomenys, apibrėžiami tolesniuose skirsniuose, perduodami hcert prašymu.

Tikrintojas turi galėti patikrinti naudingųjų duomenų vientisumą ir kilmės autentiškumą. Kad būtų užtikrintas šis mechanizmas, išdavėjas turi pasirašyti CWT naudodamas asimetrinę elektroninio parašo schemą, kuri apibrėžta COSE specifikacijoje (RFC 8152 ([2])).

3.2. *CWT prašymai*

3.2.1. CWT struktūros apžvalga

Apsaugota antraštė

— Parašo algoritmas (alg, 1 žymena)

— Rakto identifikatorius (kid, 4 žymena)

Naudingieji duomenys

— Išdavėjas (iss, 1 prašymo raktas, neprivalomas, išdavėjo alfa-2 kodas pagal standartą ISO 3166-1)

— Išdavimo laikas (iat, 6 prašymo raktas)

— Galiojimo laikas (exp, 4 prašymo raktas)

— Sveikatos pažymėjimas (hcert, -260 prašymo raktas)

— ES skaitmeninis COVID pažymėjimas, 1-a versija (eu_DCC_v1, 1 prašymo raktas)

Parašas

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

3.2.2. Parašo algoritmas

Parašo algoritmo (alg) parametru nurodoma, koks algoritmas naudojamas parašui sukurti. Jis turi atitikti dabartines SOG-IS gaires, kurios apibendrintai išdėstytos tolesniuose punktuose, arba būti už jas pranašesnis.

Apibrėžiamas vienas pirminis ir vienas antrinis algoritmas. Antrinis algoritmas turėtų būti naudojamas tik jei pirminis algoritmas yra nepriimtinas pagal išdavėjui nustatytas taisykles ir reglamentus.

Kad būtų užtikrintas sistemos saugumas, visose įgyvendinimo priemonėse turi būti įdiegtas antrinis algoritmas. Dėl šios priežasties turi būti įdiegtas ir pirminis, ir antrinis algoritmas.

Toliau nurodyti pirminio ir antrinio algoritmų SOG-IS rinkinių lygiai.

— Pirminis algoritmas. Pirminis algoritmas yra elipsinės kreivės skaitmeninio parašo algoritmas (ECDSA), apibrėžtas standarto ISO/IEC 14888-3:2006) 2.3 skirsnyje; jame naudojami P-256 parametrai, apibrėžti standarto FIPS PUB 186-4 D priedėlyje (D.1.2.3), kartu su šifravimo algoritmu SHA-256, kuris apibrėžtas standarto ISO/IEC 10118-3:2004 4 funkcijoje.

Jis atitinka COSE algoritmo parametrą ES256.

— Antrinis algoritmas. Antrinis algoritmas yra RSASSA-PSS, apibrėžtas standarte RFC 8230 ([3]), su 2048 bitų moduliu, naudojamas kartu su šifravimo algoritmu SHA-256, kuris apibrėžtas standarto ISO/IEC 10118-3:2004 4 funkcijoje.

Jis atitinka COSE algoritmo parametrą PS256.

3.2.3. Rakto identifikatorius

Rakto identifikatoriaus (kid) prašymas reiškia dokumento pasirašytojo sertifikatą (DSC), kuriame yra viešasis raktas, kurį tikrintojas turi naudoti skaitmeninio parašo teisingumui patikrinti. Viešojo rakto sertifikatų valdymas, įskaitant DSC taikomus reikalavimus, aprašytas IV priede.

Rakto identifikatoriaus (kid) prašymą tikrintojai naudoja, kad iš raktų sąrašo pasirinktų tinkamą išdavėjo (iss) prašyme nurodytą su išdavėju susijusį viešąjį raktą. Administravimo tikslais ir atlikdamas raktų atnaujinimą išdavėjas gali lygiagrečiai naudoti kelis raktus. Rakto identifikatorius nėra saugumui svarbus laukelis. Todėl, prireikus, jis taip pat gali būti pateikiamas neapsaugotoje antraštėje. Tikrintojai turi priimti abi parinktis. Esant abiem parinktims, reikia naudoti apsaugotoje antraštėje esantį rakto identifikatorių.

Kadangi identifikatorius yra sutrumpintas (dėl vietos ribojimo priežasčių), yra nedidelė tikimybė (tačiau ji negali būti atmesta), kad bendrame tvirtintojo priimtų DSC sąraše gali būti DSC su vienodais rakto identifikatoriais (kid). Dėl šios priežasties tikrintojas turi patikrinti visus DSC su atitinkamu rakto identifikatoriumi (kid).

3.2.4. Išdavėjas

Išdavėjo (iss) prašymas yra eilutės reikšmė, kurioje gali būti nurodytas sveikatos pažymėjimą išdavusio subjekto šalies kodas alfa-2 formatu pagal standartą ISO 3166-1. Šį prašymą tikrintojas gali naudoti nustatydamas, kurį DSC rinkinį naudoti patvirtinimui. Šiam prašymui identifikuoti naudojamas 1 prašymo raktas.

3.2.5. Galiojimo laikas

Galiojimo pabaigos laiko (exp) prašyme pateikta laiko žyma sveikųjų skaičių (NumericDate) formatu (kaip apibrėžta standarto RFC 8392 ([4]) 2 skirsnyje), žyminti konkretaus parašo, pateikto dėl tų naudingųjų duomenų, galiojimo laiką, po kurio tikrintojas naudinguosius duomenis turi atmesti kaip nebegaliojančius. Galiojimo pabaigos parametro paskirtis – nustatyti sveikatos pažymėjimo galiojimo laikotarpio ribas. Šiam prašymui identifikuoti naudojamas 4 prašymo raktas.

Galiojimo laikas negali viršyti DSC galiojimo laikotarpio.

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

3.2.6. Išdavimo laikas

Išdavimo laiko (iat) prašyme pateikta laiko žyma sveikųjų skaičių (NumericDate) formatu (kaip apibrėžta standarto RFC 8392 ([5]) 2 skirsnyje), žyminti sveikatos pažymėjimo sukūrimo laiką.

Išdavimo laiko laukelio reikšmė negali būti ankstesnė už DSC galiojimo laikotarpį.

Tikrintojai gali taikyti papildomas taisykles, kuriomis siekiama apriboti sveikatos pažymėjimo galiojimą pagal jo išdavimo laiką. Šiam prašymui identifikuoti naudojamas 6 prašymo raktas.

3.2.7. Sveikatos pažymėjimo prašymas

Sveikatos pažymėjimo (hcert) prašymas yra JSON (RFC 7159 ([6])) objektas, kuriame pateikiama sveikatos būklės informacija. Pagal tą patį prašymą gali būti išduodami kelių skirtingų tipų sveikatos pažymėjimai, iš kurių vienas yra SCP.

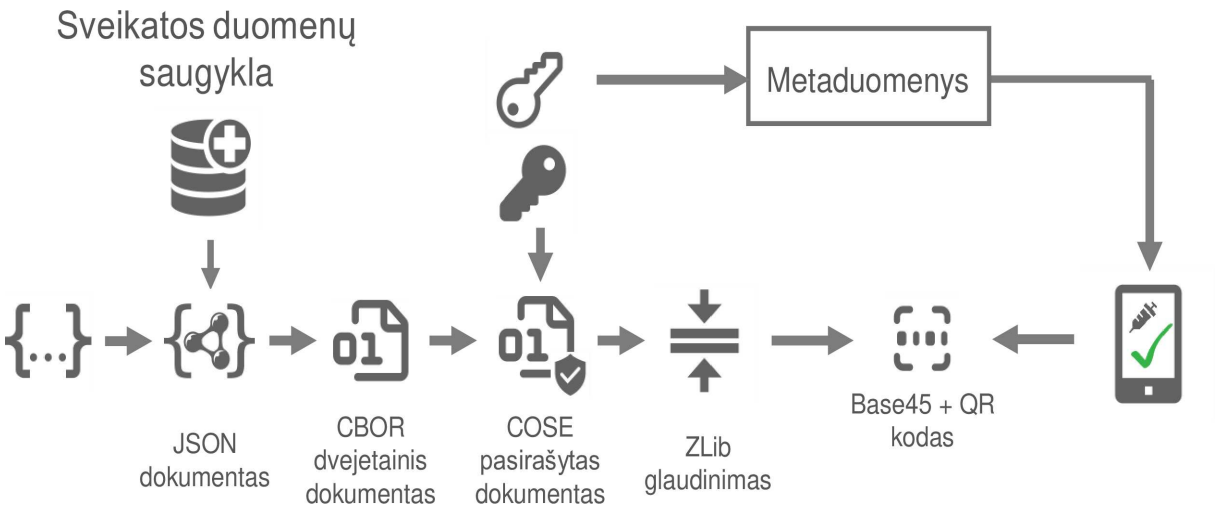
JSON naudojamas tik schemai. Pateikimo formatas yra CBOR, apibrėžtas standarte RFC 7049 ([7]). Taikomųjų programų kūrėjai gali visiškai nekoduoti į JSON formatą ir iš jo, bet naudoti atmintyje išsaugotą struktūrą.

Šiam prašymui identifikuoti naudojamas -260 prašymo raktas.

JSON objekto eilutės turėtų būti normalizuotos pagal unikodo standarte apibrėžtą kanoninės sudėties normalizavimo formą (angl. *Normalization Form Canonical Composition*, NFC). Tačiau šiuo požiūriu dekodavimo taikomosios programos turėtų būti pralaidžios ir patikimos, todėl labai rekomenduojama priimti bet kokį pagrįsto tipo konvertavimą. Jei dekoduojant arba vykdant tolesnes palyginimo funkcijas aptinkama nenormalizuotų duomenų, įdiegtos programos turėtų elgtis taip, tarsi įvestis būtų normalizuota pagal NFC formą.

4. SCP naudingųjų duomenų serializavimas ir sukūrimas

Serializavimui taikoma ši schema:



Procesas prasideda nuo duomenų išgavimo, pavyzdžiui, iš sveikatos duomenų saugyklos (arba iš kokio nors išorinio duomenų šaltinio), struktūruojant gautus duomenis pagal nustatytas SCP schemas. Šio proceso metu, prieš pradedant serializavimą CBOR, gali būti atliekamas perkeitimas į nustatytą duomenų formatą ir transformavimas į žmogui suprantamą formatą. Prieš serializavimą ir deserializavimą prašymų santrumpos visais atvejais turi būti prilyginamos rodomiems pavadinimams.

Pažymėjimuose, išduotuose pagal Reglamentą (ES) 2021/953 ([8]), neleidžiamas pasirinktinis nacionalinių duomenų turinys. Duomenų turinys turi būti apribotas Reglamento (ES) 2021/953 priede nurodyto minimalaus duomenų rinkinio apibrėžtais duomenų elementais.

([5]) rfc8392 (ietf.org).
([6]) rfc7159 (ietf.org).
([7]) rfc7049 (ietf.org).
([8]) 2021 m. birželio 14 d. Europos Parlamento ir Tarybos reglamentas (ES) 2021/953 dėl sąveikiųjų COVID-19 skiepijimo, tyrimo rezultatų ir persirgimo pažymėjimų (ES skaitmeninis COVID pažymėjimas) išdavimo, tikrinimo ir pripažinimo sistemos, kuria siekiama sudaryti palankesnes sąlygas laisvai judėti COVID-19 pandemijos metu (OL L 211, 2021 6 15, p. 1).

5. **Koduotų duomenų perdavimas**

5.1. *Neapdoroti duomenys*

Jei naudojamos bet kokios pasirinktinės duomenų sąsajos, HCERT rinkmena ir jos naudingieji duomenys gali būti perduodami tokie, kokie yra, naudojant bet kokį pagrindinį 8 bitų saugų ir patikimą duomenų perdavimą. Šios sąsajos gali būti keitimosi duomenimis trumpu atstumu technologija (NFC), „Bluetooth“ arba perdavimas per taikomosios programos lygmens protokolą, pavyzdžiui, HCERT perdavimas iš išdavėjo į turėtojo mobiliųjį įrenginį.

Jei HCERT iš išdavėjo turėtojui perduodamas tik naudojant pateikimo sąsają (pvz., žinutes, e. paštą), akivaizdu, kad neapdorotų koduotų duomenų perdavimas netaikomas.

5.2. *Brūkšninis kodas*

5.2.1. Naudingųjų duomenų (CWT) glaudinimas

Siekiant sumažinti HCERT dydį ir padidinti nuskaitymo proceso greitį bei patikimumą, CWT turi būti glaudinamas naudojant programinę įrangą ZLIB (RFC 1950 ([9])) ir glaudinimo mechanizmą „Deflate“, kurio formatas apibrėžtas standarte RFC 1951 ([10]).

5.2.2. QR 2D brūkšninis kodas

Kad būtų galima geriau panaudoti senesnę įrangą, skirtą ASCII naudingiesiems duomenims, suglaudintas CWT, prieš jį koduojant 2D brūkšniniu kodu, pirmiausia koduojamas kaip ASCII naudojant „Base45“.

2D brūkšniniam kodui generuoti naudojamas QR formatas, apibrėžtas standarte ISO/IEC 18004:2015. Rekomenduojama naudoti klaidų taisymo koeficientą „Q“ (apie 25 %). Kadangi naudojamas „Base45“, QR kodas turi būti naudojamas naudojant raidinį skaitmeninį kodavimą (2 būdas, žymimas simboliais 0010).

Kad tikrintojai galėtų nustatyti koduotų duomenų tipą ir parinkti tinkamą iškodavimo ir apdorojimo schemą, prieš „Base45“ koduotus duomenis (pagal šią specifikaciją) įrašoma konteksto identifikatoriaus eilutė „HC1:“. Būsimose šios specifikacijos versijose, turinčiose įtakos atgaliniam suderinamumui, turi būti apibrėžtas naujas konteksto identifikatorius, o po „HC“ einantis simbolis pasitelkiamas iš simbolių rinkinio [1–9A–Z]. Didėjimo tvarka apibrėžiama nurodyta tvarka, t. y. pirma [1–9] ir po to [A–Z].

Optinį kodą rekomenduojama pateikti 35–60 mm įstrižainės pateikimo laikmenoje, kad jį būtų galima nuskaityti skaitytuvais su stacionaria optika, kai pateikimo laikmeną reikia padėti ant skaitytuvo paviršiaus.

Jei optinis kodas spausdinamas popieriuje naudojant mažos skiriamosios gebos (< 300 dpi) spausdintuvus, reikia stengtis, kad kiekvienas QR kodo simbolis (taškas) būtų tiksliai kvadratinis. Dėl neproporcingo mastelio keitimo kai kuriose QR eilutėse ar stulpeliuose simboliai bus stačiakampiai, ir juos daugeliu atvejų bus sunku nuskaityti.

6. **Patikimumo sąrašo formatas (CSCA ir DSC sąrašas)**

Kiekviena valstybė narė privalo pateikti vienos ar daugiau parašą patvirtinančių šalies sertifikavimo įstaigų (CSCA) sąrašą ir visų galiojančių dokumento pasirašytojo sertifikatų (DSC) sąrašą ir šiuos sąrašus nuolat atnaujinti.

6.1. *Supaprastinta CSCA / DSC*

Patvirtinus šią specifikacijų versiją valstybės narės nebegali daryti prielaidos, kad naudojama kokia nors atšauktų sertifikatų sąrašo (CRL) informacija arba kad privačiojo rakto naudojimo laikotarpį tikrina programinės įrangos diegėjai.

Vietoje to pagrindinis galiojimo mechanizmas yra sertifikatas, įtrauktas į naujausią atitinkamo sertifikatų sąrašo versiją.

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

6.2. *ICAO elektroninio mašininio nuskaitymo kelionės dokumento (eMRTD) viešojo rakto infrastruktūra (PKI) ir patikimumo užtikrinimo centrai*

Valstybės narės gali pasitelkti atskirą CSCA, tačiau taip pat gali pateikti savo esamus elektroninio mašininio nuskaitymo kelionės dokumento CSCA sertifikatus ir (arba) DSC; jos netgi gali nuspręsti šiuos sertifikatus įsigyti iš (komercinių) patikimumo užtikrinimo centrų ir juos pateikti. Tačiau bet koks DSC visada turi būti pasirašytas tos valstybės narės nurodytos CSCA.

7. **Saugumo aspektai**

Rengdamos schemą pagal šią specifikaciją valstybės narės nustato, analizuoja ir stebi tam tikrus saugumo aspektus.

Turėtų būti atsižvelgta bent į šiuos aspektus:

7.1. *HCERT parašo galiojimo laikas*

HCERT išdavėjas privalo apriboti parašo galiojimo laiką, nurodydamas parašo galiojimo pabaigos laiką. Tai reiškia, kad sveikatos pažymėjimo turėtojas turi periodiškai jį atnaujinti.

Priimtinas galiojimo laikotarpis gali būti nustatytas atsižvelgiant į praktinius apribojimus. Pavyzdžiui, keliautojas gali neturėti galimybės atnaujinti sveikatos pažymėjimo keliaudamas užsienyje. Tačiau taip pat galimi atvejai, kad išdavėjas numato tam tikro saugumo pažeidimo galimybę, dėl kurios išdavėjas turi atšaukti DSC (panaikindamas visus naudojant tą raktą išduotus sveikatos pažymėjimus, kurių galiojimo laikas dar nepasibaigęs). Tokio atvejo pasekmes galima apriboti reguliariai keičiant išdavėjo raktus ir reikalaujant, kad visi sveikatos pažymėjimai būtų atnaujinami tam tikru pagrįstu periodiškumu.

7.2. *Raktų valdymas*

Ši specifikacija pagrįsta patikimais kriptografiniais mechanizmais, kad būtų užtikrintas duomenų vientisumas ir duomenų kilmės autentiškumas. Todėl būtina užtikrinti privačių raktų konfidencialumą.

Kriptografinių raktų konfidencialumas gali būti pažeistas įvairiais būdais, kaip antai:

— raktas gali būti generuojamas su trūkumais, todėl raktai gali būti nepatikimi;

— raktai gali būti pažeidžiami dėl žmogiškosios klaidos;

— raktai gali būti pavogti išorės arba vidaus nusikaltėlių;

— raktai gali būti apskaičiuoti taikant kriptoanalizės priemones.

Siekiant sumažinti riziką, kad pasirašymo algoritmas gali būti silpnas ir dėl to naudojant kriptoanalizės priemones gali būti pažeisti privatieji raktai, šioje specifikacijoje visiems dalyviams rekomenduojama įdiegti antrinį atsarginį pasirašymo algoritmą, pagrįstą kitais parametrais arba kitu matematiniu uždaviniu nei pagrindinis.

Kalbant apie minėtą riziką, susijusią su išdavėjų veiklos aplinka, turi būti įgyvendinamos veiksmingą kontrolę užtikrinančios rizikos švelninimo priemonės, pavyzdžiui, privačiuosius raktus generuoti, saugoti ir naudoti aparatiniuose saugumo moduliuose (toliau – ASM). Sveikatos pažymėjimams pasirašyti labai rekomenduojama naudoti ASM.

Nepriklausomai nuo to, ar išdavėjas nusprendžia naudoti ASM, turėtų būti sudarytas raktų atnaujinimo grafikas, pagal kurį raktų atnaujinimo dažnumas būtų proporcingas raktų poveikiui išoriniams tinklams, kitoms sistemoms ir personalui. Tinkamai parinkus atnaujinimo grafiką taip pat sumažinama rizika, susijusi su klaidingai išduodamais sveikatos pažymėjimais, nes prireikus išdavėjas gali atšaukti tokius sveikatos pažymėjimus partijomis, anuliuodamas raktą.

7.3. *Įvesties duomenų patvirtinimas*

Šios specifikacijos gali būti panaudojamos taip, kad iš nepatikimų šaltinių būtų gaunami duomenys į sistemas, kurios gali būti kritinės svarbos. Siekiant sumažinti su tokiu atakos vektoriumi susijusią riziką, visi įvesties laukeliai turi būti tinkamai patvirtinti pagal duomenų tipus, ilgį ir turinį. Prieš pradedant tvarkyti HCERT turinį taip pat patikrinamas išdavėjo parašas. Tačiau norint patvirtinti išdavėjo parašą, pirmiausia reikia išanalizuoti apsaugotą išdavėjo antraštę, kurioje potencialus užpuolikas gali bandyti įterpti kruopščiai sukurtą informaciją, kuria siekiama pakenkti sistemos saugumui.

8. **Patikimumo užtikrinimas**

HCERT parašui patikrinti reikalingas viešasis raktas. Valstybės narės suteikia galimybę naudotis šiais viešaisiais raktais. Galiausiai kiekvienas tikrintojas turi turėti visų viešųjų raktų, kuriais jis gali pasitikėti, sąrašą (nes viešasis raktas nėra HCERT dalis).

Sistemą sudaro (tik) du lygiai; kiekvienai valstybei narei – po vieną ar daugiau šalies lygmens sertifikatų, kuriais pasirašoma po vieną ar daugiau dokumento pasirašytojo sertifikatų, naudojamų kasdienėje veikloje.

Valstybių narių sertifikatai vadinami parašą patvirtinančios šalies sertifikavimo įstaigos (CSCA) sertifikatais ir (paprastai) yra savarankiškai pasirašyti sertifikatai. Valstybėse narėse gali būti daugiau nei vienas sertifikatas (pavyzdžiui, regioninės decentralizacijos atveju). Tokiais CSCA sertifikatais nuolat pasirašomi dokumento pasirašytojo sertifikatai (DSC), naudojami HCERT pasirašyti.

Sekretoriato vaidmuo yra funkcinis. Jis reguliariai apibendrina ir skelbia valstybių narių DSC, prieš tai patikrinęs juos pagal CSCA sertifikatų (kurie buvo perduoti ir patikrinti kitais būdais) sąrašą.

Taip gautame DSC sąraše pateikiamas apibendrintas priimtinų viešųjų raktų (ir atitinkamų rakto identifikatorių) rinkinys, kurį tikrintojai gali naudoti HCERT parašams patvirtinti. Tikrintojai turi periodiškai gauti ir atnaujinti šį sąrašą.

Tokie konkrečiai valstybei narei skirti sąrašai gali būti pritaikomi jos nacionalinei aplinkai. Todėl šio patikimumo sąrašo failo formatas gali būti įvairus, pavyzdžiui, tai gali būti pasirašytas JWKS (JWK rinkinio formatas pagal standarto RFC 7517 ([11]) 5 skirsnį) arba bet koks kitas formatas, būdingas toje valstybėje narėje naudojamai technologijai.

Siekdamos užtikrinti paprastumą, valstybės narės gali pateikti esamus CSCA sertifikatus iš savo ICAO elektroninio mašininio nuskaitymo kelionės dokumentų sistemų arba, kaip rekomenduoja PSO, sukurti specialiai šiai sveikatos sričiai skirtą pažymėjimą.

8.1. *Rakto identifikatorius (kid)*

Rakto identifikatorius (kid) apskaičiuojamas sukūrus DSC patikimų viešųjų raktų sąrašą, kurį sudaro sutrumpintas (pirmieji 8 baitai) DSC, koduoto DER (neapdorotu) formatu, SHA-256 pirštų atspaudas.

Tikrintojams nereikia apskaičiuoti rakto identifikatoriaus pagal DSC; jie gali tiesiogiai palyginti išduotame sveikatos pažymėjime esantį rakto identifikatorių su patikimumo sąraše esančiu rakto identifikatoriumi.

8.2. *Skirtumai, palyginti su ICAO elektroninio mašininio nuskaitymo kelionės dokumento viešojo rakto infrastruktūros patikimumo užtikrinimo modeliu*

Nors šis modelis parengtas pagal ICAO elektroninio mašininio nuskaitymo kelionės dokumento viešojo rakto infrastruktūros patikimumo modelio geriausią praktiką, siekiant spartos reikalingi keli supaprastinimai:

— valstybė narė gali pateikti kelis CSCA sertifikatus;

— gali būti nustatytas bet kokios trukmės DSC (rakto naudojimo) galiojimo laikotarpis, neviršijantis CSCA sertifikato galiojimo trukmės, ir jo gali visai nebūti;

— DSC gali būti politikos identifikatorių (išplėstinio rakto naudojimas), kurie yra būdingi sveikatos pažymėjimams;

— valstybės narės gali nuspręsti niekada netikrinti paskelbtų atšaukimo atvejų, o pasikliauti tik DSC sąrašais, kuriuos kasdien gauna iš sekretoriato arba sudaro pačios.

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

II PRIEDAS

ES SKAITMENINIO COVID PAŽYMĖJIMO PILDYMO TAISYKLĖS

Šiame priede nustatytomis bendrosiomis vertybių rinkinių taisyklėmis siekiama užtikrinti sąveiką semantiniu lygmeniu ir sudaryti sąlygas vienodam techniniam SCP įgyvendinimui. Šiame priede esantys elementai gali būti naudojami trims skirtingiems nustatymams (skiepijimo / testavimo / persirgimo), numatytems Reglamente (ES) 2021/953. Šiame priede išvardyti tik tie elementai, kuriuos būtina semantiškai standartizuoti naudojant koduotus reikšmių rinkinius.

Už koduotų elementų vertimą į nacionalinę kalbą atsako valstybės narės.

Visuose duomenų laukuose, nepaminėtuose toliau nurodytuose reikšmių rinkinio aprašymuose, rekomenduojamas UTF-8 kodavimas (vardas pavardė, testavimo centras, pažymėjimo išdavėjas). Duomenų laukelius, kuriuose nurodytos kalendorinės datos (gimimo data, skiepijimo data, tyrimo mėginio paėmimo data, pirmojo teigiamo tyrimo rezultato data, pažymėjimo galiojimo datos), rekomenduojama koduoti pagal ISO 8601.

Jei dėl kokių nors priežasčių negalima naudoti toliau išvardytų pageidaujamų kodų sistemų, galima naudoti kitas tarptautines kodų sistemas ir patarti, kaip kitos kodų sistemos kodus perkelti į pageidaujamą kodų sistemą. Tekstas (rodomi pavadinimai) gali būti naudojamas išimtiniais atvejais kaip atsarginis mechanizmas, kai apibrėžtuose reikšmių rinkiniuose nėra tinkamo kodo.

Valstybės narės, savo sistemose naudojančios kitus kodus, turėtų juos priskirti aprašytiems reikšmių rinkiniams. Valstybės narės yra atsakingos už visus tokio priskyrimo atvejus.

Reikšmių rinkinius nuolat atnaujina Komisija, padedama e. sveikatos tinklo ir Sveikatos saugumo komiteto. Atnaujinti reikšmių rinkiniai skelbiami atitinkamoje Komisijos interneto svetainėje ir e. sveikatos tinklo interneto svetainėje. Reikėtų pateikti pakeitimų istoriją.

1. **Tiriama liga ar sukėlėjas / Liga, kuria turėtojas persirgo, arba ligos sukėlėjas: COVID-19 (SARS-CoV-2 arba vienas iš jų atmainų)**

   Pageidaujama kodų sistema: SNOMED CT.

   Naudotina 1, 2 ir 3 pažymėjimuose.

   Pasirinkti kodai nurodo COVID-19 arba, jei reikia išsamesnės informacijos apie SARS-CoV-2 genetinę atmainą, tas atmainas, jei tokia išsami informacija reikalinga dėl epidemiologinių priežasčių.

   Kodo, kurį reikėtų naudoti, pavyzdys – SNOMED CT kodas 840539006 (COVID-19).

2. **COVID-19 vakcina arba profilaktiktinio gydymo rūšis**

   Pageidaujama kodų sistema: SNOMED CT arba ATC klasifikacija.

   Naudotina 1 pažymėjime.

   Pageidaujamų kodų sistemų kodų, kuriuos reikėtų naudoti, pavyzdžiai: SNOMED CT kodas 1119305005 (SARS-CoV-2 antigenų vakcina), 1119349007 (SARS-CoV-2 mRNA vakcina) arba J07BX03 (COVID-19 vakcinos). Sukūrus ir pradėjus naudoti naujas vakcinų rūšis reikšmių rinkinį reikėtų išplėsti.

3. **COVID-19 vakcinos pavadinimas**

   Pageidaujamos kodų sistemos (eilės tvarka):

   — Sąjungos vakcinų, kuriomis išduotas leidimas prekiauti visoje ES, pavadinimų registras (leidimų numeriai);

   — pasaulinis vakcinų registras, kurį galėtų sukurti Pasaulio sveikatos organizacija;

   — vakcinos pavadinimas kitais atvejais. Jei pavadinime yra tarpų, juos reikėtų pakeisti brūkšneliu (-).

Reikšmių rinkinio pavadinimas: vakcina.

Naudotina 1 pažymėjime.

Pageidaujamų kodų sistemų kodo, kurį reikėtų naudoti, pavyzdys – EU/1/20/1528 („Comirnaty“). Vakcinos pavadinimo, kuris bus naudojamas kaip kodas, pavyzdys – Sputnik-V (reiškia „Sputnik V“).

4. **COVID-19 vakcinos rinkodaros leidimo turėtojas arba gamintojas**

Pageidaujama kodų sistema:

— EMA organizacijos kodas (ISO IDMP atveju – SPOR sistema);

— pasaulinis vakcinų rinkodaros leidimo turėtojų arba gamintojų registras, kurį galėtų sukurti Pasaulio sveikatos organizacija;

— organizacijos pavadinimas kitais atvejais. Jei pavadinime yra tarpų, juos reikėtų pakeisti brūkšneliu (-).

Naudotina 1 pažymėjime.

Pageidaujamų kodų sistemų kodo, kurį reikėtų naudoti, pavyzdys – ORG-100001699 („AstraZeneca AB“). Organizacijos pavadinimo, kuris bus naudojamas kaip kodas, pavyzdys – Sinovac-Biotech (reiškia „Sinovac Biotech“).

5. **Serijos dozių skaičius ir bendras serijos dozių skaičius**

Naudotina 1 pažymėjime.

Du laukeliai:

(1) per ciklą skiriamų dozių skaičius;

(2) numatomų dozių skaičius visam ciklui (konkrečiam asmeniui suleidžiant dozę).

Pavyzdžiui, 1/1, 2/2 reiškia užbaigtą skiepijimą, įskaitant parinktį 1/1 vakcinoms, kurias sudaro dvi dozės, tačiau pagal valstybės narės taikomą protokolą gyventojams, kuriems prieš skiepijimą buvo diagnozuota COVID-19, turi būti suleista viena dozė, žymėti. Bendras dozių skaičius serijoje turi būti nurodomas pagal informaciją, turimą dozės skyrimo metu. Pavyzdžiui, jei tam tikros vakcinos atveju turi būti skiepijama trečią kartą (stiprinamoji dozė), antrajame laukelyje pažymima suleista paskutinioji skiepo dozė (pvz., 2/3, 3/3 ir t. t.).

6. **Valstybė narė arba trečioji valstybė, kurioje buvo paskiepyta ir (arba) atliktas tyrimas**

Pageidaujama kodų sistema: šalių kodai pagal ISO 3166.

Naudotina 1, 2 ir 3 pažymėjimuose.

Reikšmių rinkinio turinys: išsamus 2 raidžių kodų sąrašas, pateikiamas kaip reikšmių rinkinys, apibrėžtas FHIR (http://hl7.org/fhir/ValueSet/iso3166-1-2).

7. **Tyrimo tipas**

Pageidaujama kodų sistema: LOINC.

Naudotina 2 pažymėjime ir, jei deleguotuoju teisės aktu numatoma galimybė išduoti persirgimo pažymėjimus, grindžiamus ne NRA tyrimais, o kitų tipų tyrimais, 3 pažymėjime.

Tokio reikšmių rinkinio kodai nurodo tyrimo metodą ir parenkami bent jau taip, kad NRA tyrimai būtų atskirti nuo greitųjų antigenų testų, kaip nurodyta Reglamente (ES) 2021/953.

Pageidaujamų kodų sistemų kodo, kurių reikėtų naudoti, pavyzdys – LP217198-3 (greitasis imunologinis tyrimas (*Rapid immunoassay*)).

8. **Naudoto tyrimo gamintojas ir komercinis pavadinimas (neprivaloma NRA tyrimo atveju)**

Pageidaujama kodų sistema: SSK greitųjų antigenų tyrimų sąrašas, kurį tvarko JTC (COVID-19 *in vitro* diagnostikos prietaisų ir tyrimų metodų duomenų bazė).

Naudotina 2 pažymėjime.

Reikšmių rinkinio turinį sudaro greitųjų antigenų tyrimai, išvardyti bendrame ir atnaujintame COVID-19 greitųjų antigenų tyrimų sąraše, sudarytame remiantis Tarybos rekomendacija 2021/C 24/01, kuriam pritarė Sveikatos saugumo komitetas. Šį sąrašą JTC tvarko COVID-19 *in vitro* diagnostikos prietaisų ir tyrimų metodų duomenų bazėje: https://covid-19-diagnostics.jrc.ec.europa.eu/devices/hsc-common-recognition-rat.

Šioje kodų sistemoje naudojami atitinkami laukeliai, pavyzdžiui, tyrimo prietaiso identifikatorius, tyrimo pavadinimas ir gamintojas, pagal JTC struktūruotą formatą, kuris pateiktas adresu https://covid-19-diagnostics.jrc.ec.europa.eu/devices.

9. **Tyrimo rezultatas**

Pageidaujama kodų sistema: SNOMED CT.

Naudotina 2 pažymėjime.

Pasirinkti kodai turi sudaryti sąlygas atskirti teigiamus ir neigiamus tyrimo rezultatus (nustatyta arba nenustatyta). Papildomos reikšmės (pvz., neapibrėžta) gali būti pridedamos, jei to reikia naudojimo atvejais.

Pageidaujamų kodų sistemų kodo, kurį reikėtų naudoti, pavyzdžiai: 260415000 (nenustatyta) ir 260373001 (nustatyta).

III PRIEDAS

BENDRA UNIKALAUS PAŽYMĖJIMO IDENTIFIKATORIAUS STRUKTŪRA

1. **Įžanga**

Kiekviename ES skaitmeniniame COVID pažymėjime (SCP) turi būti unikalus pažymėjimo identifikatorius (UPI), užtikrinantis SCP sąveikumą. UPI gali būti naudojamas pažymėjimui patikrinti. Valstybės narės yra atsakingos už UPI įgyvendinimą. UPI – tai priemonė pažymėjimo tikrumui patikrinti ir, jei taikoma, susieti su registravimo sistema (pvz., IIS). Šie identifikatoriai taip pat sudaro sąlygas valstybėms narėms (popierine ir skaitmenine forma) patvirtinti, kad asmenys buvo paskiepyti arba ištirti.

2. **Unikalaus pažymėjimo identifikatoriaus sudėtis**

UPI turi atitikti bendrą struktūrą ir formatą, lengvinantį informacijos aiškinimą žmogui ir (arba) mašinoms, ir gali būti susijęs su tokiais elementais kaip skiepijimo valstybė narė, pati vakcina ir valstybei narei būdingas identifikatorius. Taip valstybėms narėms užtikrinamas lankstumas jį formuojant, visapusiškai laikantis duomenų apsaugos teisės aktų. Atskirų elementų eiliškumas atitinka nustatytą hierarchiją, pagal kurią ateityje galima keisti blokus, išlaikant jų struktūrinį vientisumą.

Galimais UPI sudėties sprendimais suformuojamas spektras, kurio du pagrindiniai varijuojantys parametrai ir viena iš esminių savybių yra moduliškumas ir žmonių gebėjimas jį suprasti:

— Moduliškumas: kiek kodas sudarytas iš atskirų struktūrinių blokų, kuriuose pateikiama semantiškai skirtinga informacija.

— Žmonių gebėjimas jį suprasti: kiek kodas yra prasmingas arba kiek žmogus jį gali suprasti.

— Unikalumas visame pasaulyje: šalies arba institucijos identifikatorius yra gerai valdomas ir tikimasi, kad kiekviena šalis (institucija) gerai valdys savo vardų srities segmentą ir niekada identifikatorių nenaudos pakartotinai ir neišduos iš naujo. Derinant šiuos komponentus užtikrinama, kad kiekvienas identifikatorius būtų unikalus visame pasaulyje.

3. **Bendrieji reikalavimai**

Turėtų būti laikomasi toliau išvardytų bendrųjų reikalavimų, susijusių su UPI:

(1) simbolių rinkinys: leidžiama naudoti tik didžiosiomis raidėmis parašytus raidinius-skaitmeninius simbolius pagal US-ASCII (A–Z, 0–9); su papildomais specialiaisiais ženklais, skirtais atskirti nuo RFC3986 ([1]) ([2]), t. y. {/, #, :};

(2) didžiausias ilgis: kūrėjai turėtų stengtis neviršyti 27–30 ženklų ilgio ([3]);

(3) versijos priešdėlis: jis nurodo UPI schemos versiją. Šios dokumento versijos priešdėlis yra „01“; versijos priešdėlis sudarytas iš dviejų skaitmenų;

(4) šalies priešdėlis: šalies kodas nurodomas pagal standartą ISO 3166-1. Ilgesni kodai (pvz., 3 ir daugiau ženklų (pvz., „UNHCR“) yra rezervuoti naudoti ateityje;

(5) kodo priesaga / kontrolinė suma:

5.1. valstybės narės turėtų naudoti kontrolinę sumą, kai tikėtina, kad gali atsirasti perdavimo, (žmogiškojo) perrašymo ar kitų pažeidimų (t. y. kai naudojama spausdinant);

5.2. kontrolinė suma negali būti naudojama pažymėjimui patvirtinti ir techniškai nėra identifikatoriaus dalis, bet naudojama kodo vientisumui patikrinti. Ši kontrolinė suma turėtų būti viso UPI santrauka pagal ISO-7812-1 (LUHN-10) ([4]) skaitmeninio / laidinio perdavimo formatu. Kontrolinė suma nuo likusios UPI dalies atskiriama ženklu „#“.

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

([2]) Laukeliai, tokie kaip lytis, partijos / siuntos numeris, administruojantis centras, sveikatos priežiūros specialisto identifikacija, kito skiepijimo data, gali būti nereikalingi kitais nei medicininiais tikslais.

([3]) Diegdamos QR kodus, valstybės narės galėtų apsvarstyti galimybę naudoti papildomą simbolių rinkinį, kurio bendras ilgis neviršija 72 simbolių (įskaitant 27–30 paties identifikatoriaus simbolių), kitai informacijai perteikti. Šią informaciją turi nurodyti valstybės narės.

([4]) Algoritmas „Luhn mod N“ yra algoritmo „Luhn“ plėtinys (vadinamasis algoritmas „mod 10“), kuris tinka skaitmeniniams kodams ir naudojamas, pavyzdžiui, kredito kortelių kontrolinei sumai apskaičiuoti. Šis plėtinys sudaro sąlygas naudoti algoritmą su bet kokio pagrindo reikšmių sekomis (mūsų atveju – raidžių simboliais).

Turėtų būti užtikrintas atgalinis suderinamumas: valstybės narės, kurios ilgainiui keičia savo identifikatorių struktūrą (pagal pagrindinę versiją – šiuo metu 1-ą versiją), turi užtikrinti, kad bet kokie du identiški identifikatoriai reikštų tą patį skiepų pažymėjimą ir (arba) patvirtinimą. Kitaip tariant, valstybės narės negali identifikatorių panaudoti iš naujo.

4. **Skiepų pažymėjimų unikalių pažymėjimo identifikatorių parinktys**

E. sveikatos tinklo gairėse dėl patikrinamų skiepų pažymėjimų ir pagrindinių sąveikumo elementų ([5]) numatytos įvairios parinktys, kuriomis gali naudotis valstybės narės ir kitos šalys ir kurios gali egzistuoti kartu skirtingose valstybėse narėse. Valstybės narės gali taikyti tokias skirtingas parinktis skirtingose UPI schemos versijose.

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

IV PRIEDAS

VIEŠOJO RAKTO SERTIFIKATO VALDYMAS

1. **Įžanga**

Saugus ir patikimas keitimasis ES skaitmeninių COVID pažymėjimų (SCP) parašo raktais tarp valstybių narių vykdomas per ES skaitmeninio COVID pažymėjimo tinklų sietuvą (SCPTS), kuris veikia kaip centrinė viešųjų raktų saugykla. Naudodamos SCPTS, valstybės narės turi teisę skelbti viešuosius raktus, atitinkančius privačiuosius raktus, kuriuos jos naudoja COVID skaitmeniniams pažymėjimams pasirašyti. Pasikliaujančios valstybės narės gali naudotis SCPTS, kad laiku gautų naujausią viešojo rakto medžiagą. Vėliau SCPTS gali būti išplėstas, kad būtų galima keistis patikima papildoma informacija, kurią pateikia valstybės narės, pavyzdžiui, SCP patvirtinimo taisyklėmis. SCP sistemos patikimumo modelis yra viešojo rakto infrastruktūra. Kiekviena valstybė narė turi vieną ar daugiau parašą patvirtinančių šalies sertifikavimo įstaigų (CSCA), kurių sertifikatai galioja gana ilgai. Valstybės narės sprendimu, CSCA gali būti ta pati arba kita nei mašininio nuskaitymo kelionės dokumentams naudojama CSCA. CSCA išduoda nacionaliniams trumpalaikiams dokumentų pasirašytojams (t. y. SCP pasirašytojams) viešojo rakto skaitmeninius sertifikatus, kurie vadinami dokumento pasirašytojo sertifikatais (DSC). CSCA veikia kaip patikimumo užtikrinimo priemonė, todėl ja besiremiančios valstybės narės gali naudoti CSCA sertifikatą reguliariai keičiamų DSC autentiškumui ir vientisumui patvirtinti. Patvirtintus sertifikatus (arba tik juose esančius viešuosius raktus) valstybės narės gali pateikti savo SCP patvirtinimo programoms. Be CSCA ir DSC, SCPTS taip pat remiasi viešojo rakto infrastruktūra sandorių autentiškumui nustatyti, duomenims pasirašyti, kaip pagrindu autentiškumui nustatyti ir valstybių narių ir SCPTS ryšių kanalų vientisumui užtikrinti.

Skaitmeniniai parašai gali būti naudojami duomenų vientisumui ir autentiškumui užtikrinti. Viešojo rakto infrastruktūra užtikrina patikimumą, susiedama viešuosius raktus su patikrintomis tapatybėmis (arba išdavėjais). Tai būtina, kad kiti dalyviai galėtų patikrinti duomenų kilmę ir ryšio partnerio tapatybę ir nuspręsti dėl patikimumo. SCPTS autentiškumui patvirtinti naudojami keli viešojo rakto sertifikatai. Šiame priede apibrėžiama, kokie viešojo rakto sertifikatai yra naudojami ir kaip jie turi būti sukurti, kad valstybės narės galėtų užtikrinti išsamų sąveikumą. Jame pateikiama daugiau informacijos apie būtinus viešojo rakto sertifikatus, o valstybėms narėms, norinčioms naudoti savo CSCA, pateikiamos rekomendacijos dėl pažymėjimo šablonų ir galiojimo laikotarpių. Kadangi SCP patikrinamumas turi būti užtikrinamas apibrėžtu laikotarpiu (nuo išdavimo iki galiojimo po tam tikro laiko), būtina nustatyti visų parašų, taikomų viešojo rakto sertifikatams ir SCP, tikrinimo modelį.

2. **Terminai**

Toliau lentelėje pateikiamos šiame priede vartojamos santrumpos ir terminai.

Terminas	Apibrėžtis
Sertifikatas	Arba viešojo rakto sertifikatas. „X.509 v3“ sertifikatas, kuriame yra ūkio subjekto viešasis raktas
CSCA	Parašą patvirtinanti šalies sertifikavimo įstaiga
SCP	ES skaitmeninis COVID pažymėjimas. Pasirašytas skaitmeninis dokumentas, kuriame pateikiama informacija apie skiepijimą, tyrimus arba persirgimą
SCPTS	ES skaitmeninio COVID pažymėjimo tinklų sietuvas. Ši sistema naudojama DSC mainams tarp valstybių narių
$SCPTS_{TA}$	SCPTS patikimumo užtikrinimo priemonės sertifikatas. Atitinkamas privatusis raktas naudojamas visų CSCA sertifikatų sąrašui pasirašyti neprisijungus prie interneto
$SCPTS_{TLS}$	SCPTS perkėlimo lygmens saugumo (TLS) protokolo serverio sertifikatas
DSC	Dokumento pasirašytojo sertifikatas. Valstybės narės dokumentų pasirašymo institucijos (pvz., sistemos, kuriai leidžiama pasirašyti SCP) viešojo rakto sertifikatas. Šį sertifikatą išduoda valstybės narės CSCA
EC-DSA	Elipsinės kreivės skaitmeninio parašo algoritmas. Kriptografinis parašo algoritmas, pagrįstas elipsinėmis kreivėmis
Valstybė narė	Europos Sąjungos valstybė narė

Terminas	Apibrėžtis
mTLS	Abipusio perkėlimo lygmens saugumo (TLS) protokolas. Perkėlimo lygmens saugumo protokolas su abipusio autentiškumo patvirtinimu
NB	Valstybės narės nacionalinė galinė sistema
NB_{CSCA}	Valstybės narės CSCA sertifikatas (gali būti daugiau nei vienas)
NB_{TLS}	Nacionalinės galinės sistemos perkėlimo lygmens saugumo (TLS) kliento autentifikavimo sertifikatas
NB_{UP}	Sertifikatas, kurį nacionalinė galinė sistema naudoja duomenų paketams, įkeliamiems į SCPTS, pasirašyti
PKI	Viešojo rakto infrastruktūra. Viešojo rakto sertifikatais ir sertifikavimo institucijomis pagrįstas patikimumo užtikrinimo modelis
RSA	Asimetrinis kriptografinis algoritmas, pagrįstas sveikųjų skaičių faktorizacija, naudojamas skaitmeniniams parašams arba asimetriniam šifravimui

3. **SCPTS ryšių srautai ir apsaugos paslaugos**

Šiame skirsnyje apžvelgiami SCPTS sistemos ryšių srautai ir apsaugos paslaugos. Jame taip pat apibrėžiama, kokie raktai ir sertifikatai naudojami ryšiui, įkeltai informacijai, SCP ir pasirašytam patikimumo sąrašui, kuriame yra visi įkelti CSCA sertifikatai, apsaugoti. SCPTS veikia kaip duomenų centras, kuriame galima keistis valstybių narių pasirašytais duomenų paketais.

Įkeltus duomenų paketus SCPTS pateikia nepakeistus, t. y. SCPTS į gautus paketus DSC neprideda ir jų nepašalina. Valstybių narių nacionalinėje galinėje sistemoje turi būti galimybė patikrinti įkeltų duomenų vientisumą ir autentiškumą. Be to, nacionalinėse galinėse sistemoje ir SCPTS saugiam ryšiui užmegzti naudojamas abipusis TLS autentiškumo patvirtinimas. Tai yra papildoma priemonė šalia parašų duomenyse, kuriais keičiamasi.

3.1. *Autentiškumo nustatymas ir ryšio užmezgimas*

SCPTS naudoja perkėlimo lygmens saugumo (TLS) protokolą su abipusio autentiškumo patvirtinimu patvirtinto autentiškumo šifruotam kanalui tarp valstybės narės nacionalinės galinės sistemos (NB) ir tinklų sietuvo aplinkos sukurti. Todėl SCPTS suteiktas TLS serverio sertifikatas – $SCPTS_{TLS}$, o nacionalinėms galinėms sistemoms suteiktas TLS kliento sertifikatas – NB_{TLS}. Skaitmeninių sertifikatų šablonai pateikti *5 skirsnyje*. Kiekviena nacionalinė galinė sistema gali pateikti savo TLS sertifikatą. Šis sertifikatas bus aiškiai įtrauktas į baltąjį sąrašą, todėl jį gali išduoti viešai patikima sertifikavimo įstaiga (pavyzdžiui, sertifikavimo įstaiga, kuri laikosi „CA Browser Forum“ pagrindinių reikalavimų), nacionalinė sertifikavimo įstaiga arba jis gali būti pasirašytas savarankiškai. Kiekviena valstybė narė yra atsakinga už savo nacionalinius duomenis ir privačiojo rakto, naudojamo ryšiui su SCPTS užmegzti, apsaugą. Taikant nuosavo sertifikato naudojimo metodą reikia aiškiai apibrėžto registravimo ir identifikavimo proceso, taip pat atšaukimo ir atnaujinimo procedūrų, kaip aprašyta *4.1, 4.2* ir *4.3 skirsniuose*. SCPTS naudojamas baltasis sąrašas, į kurį po sėkmingos registracijos įtraukiami nacionalinių vidinių serverių TLS sertifikatai. Saugų ryšį su SCPTS gali užmegzti tik tie nacionaliniai vidiniai serveriai, kurie autentiškumą patvirtina privačiuoju raktu, atitinkančiu į baltąjį sąrašą įtrauktą sertifikatą. SCPTS taip pat naudos TLS sertifikatą, pagal kurį nacionaliniai vidiniai serveriai gali patikrinti, ar jie iš tikrųjų užmezga ryšį su „tikruoju“ SCPTS, o ne su kokiu nors piktybišku subjektu, besidedančiu SCPTS. Sėkmingai užsiregistravus, nacionaliniam vidiniam serveriui bus suteiktas SCPTS sertifikatas. $SCPTS_{TLS}$ skaitmeninį sertifikatą išduoda viešai patikima sertifikavimo institucija (įtraukta į visas pagrindines naršykles). Valstybės narės privalo patikrinti, ar jų ryšys su SCPTS yra saugus (pavyzdžiui, patikrinti, ar serverio, prie kurio jungiamasi, $SCPTS_{TLS}$ sertifikato pirštų atspaudas atitinka po registracijos pateiktą pirštų atspaudą).

3.2. *Parašą patvirtinančios šalies sertifikavimo įstaigos ir patvirtinimo modelis*

SCPTS sistemoje dalyvaujančios valstybės narės DSC išduoti turi naudoti CSCA. Valstybės narės gali turėti daugiau nei vieną CSCA, pavyzdžiui, regioninės decentralizacijos atveju. Kiekviena valstybė narė gali naudotis esamomis sertifikavimo institucijomis arba gali įsteigti specialią sertifikavimo instituciją SCP sistemai (kuri galbūt pasirašo sertifikatus savarankiškai).

Valstybės narės turi pateikti savo CSCA sertifikatą (-us) SCPTS operatoriui per oficialią prisijungimo procedūrą. Po sėkmingos valstybės narės registracijos (*daugiau informacijos žr. 4.1 skirsnį*) SCPTS operatorius atnaujins pasirašytą patikimumą sąrašą, kuriame yra visi į SCP sistemą įtraukti CSCA sertifikatai. SCPTS operatorius naudos specialią asimetrinių raktų porą patikimumo sąrašui ir skaitmeniniams sertifikatams pasirašyti neprisijungus prie interneto. Privatusis raktas nebus saugomas SCPTS internetinėje sistemoje, kad įsilaužėlis, įsilaužęs į internetinę sistemą, negalėtų pasiekti patikimumo sąrašo. Atitinkamas patikimumo užtikrinimo priemonės sertifikatas $SCPTS_{TA}$ bus pateiktas nacionalinėms galinėms sistemoms prisijungimo metu.

Valstybės narės iš SCPTS gali gauti patikimumą sąrašą, kad galėtų atlikti patikrinimo procedūras. CSCA apibrėžiama kaip DSC išduodanti sertifikavimo institucija, todėl valstybės narės, naudojančios daugiapakopę sertifikavimo įstaigų hierarchiją (pvz., pagrindinė sertifikavimo įstaiga -> CSCA -> DSC), turi nurodyti pavaldžią sertifikavimo įstaigą, išduodančią DSC. Tokiu atveju, jei valstybė narė naudoja esamą sertifikavimo įstaigą, SCP sistema ignoruos visas virš CSCA esančias įstaigas ir į baltąjį sąrašą kaip patikimumo užtikrinimo priemonę įtrauks tik CSCA (net jei ji yra pavaldžioji sertifikavimo įstaiga). Taip yra todėl, kad pagal ICAO modelį galima taikyti tik 2 lygmenis – pagrindinę CSCA ir „lapo“ DSC, kurį pasirašė tik ta CSCA.

Jei valstybė narė turi savo CSCA, ji yra atsakinga už saugų šios sertifikavimo įstaigos veikimą ir raktų valdymą. CSCA veikia kaip DSC patikimumo užtikrinimo priemonė, todėl CSCA privačiojo rakto apsauga yra labai svarbi siekiant užtikrinti SCP aplinkos vientisumą. SCP viešojo rakto infrastruktūros tikrinimo modelis yra karkaso modelis, kuriuo užtikrinama, kad visi sertifikato maršruto tvirtinimo sertifikatai turi galioti konkrečiu laiku (t. y. tvirtinant parašą). Todėl taikomi šie apribojimai:

— CSCA neišduoda sertifikatų, kurie galioja ilgiau nei pats sertifikavimo įstaigos sertifikatas;

— dokumentą pasirašantis asmuo nepasirašo dokumentų, kurie galioja ilgiau nei pats DSC;

— valstybės narės, kurios turi savo CSCA, turi nustatyti savo CSCA ir visų išduotų skaitmeninių sertifikatų galiojimo laikotarpius ir pasirūpinti sertifikatų atnaujinimu.

4.2skirsnyje pateikiamos rekomendacijos dėl galiojimo laikotarpių.

3.3. *Įkeltų duomenų vientisumas ir autentiškumas*

Nacionalinės galinės sistemos gali naudoti SCPTS, kad įkeltų ir parsisiųsdintų skaitmeniniu būdu pasirašytus duomenų paketus po sėkmingo abipusio autentiškumo patvirtinimo. Iš pradžių šiuose duomenų paketuose pateikiami valstybių narių DSC. Raktų pora, kurią nacionalinė galinė sistema naudoja skaitmeniniam įkeltų duomenų paketų pasirašymui SCPTS sistemoje, vadinama nacionalinio vidinio serverio įkeltų duomenų pasirašymo raktų pora, o atitinkamas viešojo rakto skaitmeninis sertifikatas sutrumpintai vadinamas NB_{UP} sertifikatu. Kiekviena valstybė narė turi savo NB_{UP} sertifikatą, kuris gali būti savarankiškai pasirašytas pati arba kurį išduoda esama sertifikavimo įstaiga, pavyzdžiui, viešoji sertifikavimo įstaiga (t. y. sertifikavimo įstaiga, išduodanti sertifikatus pagal „CAB-Forum“ pagrindinius reikalavimus). NB_{UP} sertifikatas turi skirtis nuo visų kitų valstybės narės naudojamų sertifikatų (t. y. CSCA, TLS kliento ar DSC).

Valstybės narės turi pateikti įkėlimo sertifikatą SCPTS operatoriui pirminės registracijos procedūros metu (*daugiau informacijos žr. 4.1 skirsnį*). Kiekviena valstybė narė yra atsakinga už savo nacionalinius duomenis ir privalo apsaugoti privatųjį raktą, naudojamą įkeltiems dokumentams pasirašyti.

Kitos valstybės narės gali patikrinti pasirašytus duomenų paketus naudodamos SCPTS pateiktus duomenų įkėlimo sertifikatus. SCPTS patikrina įkeltų duomenų autentiškumą ir vientisumą naudodamas nacionalinio vietinio serverio įkėlimo sertifikatą, prieš juos pateikiant kitoms valstybėms narėms.

3.4. *Techninės SCPTS architektūros reikalavimai*

Techninei SCPTS architektūrai keliami šie reikalavimai:

— SCPTS naudoja abipusį TLS autentiškumo patvirtinimą, kad užmegztų autentifikuotą šifruotą ryšį su nacionaliniu vidiniu serveriu. Todėl SCPTS tvarko registruotų NB_{TLS} klientų sertifikatų baltąjį sąrašą;

— SCPTS naudoja du skaitmeninius sertifikatus ($SCPTS_{TLS}$ ir $SCPTS_{TA}$) su dviem skirtingomis raktų poromis. $SCPTS_{TA}$ raktų poros privatusis raktas saugomas neprisijungus prie interneto (ne SCPTS internetiniuose komponentuose);

— SCPTS tvarko NB_{CSCA} sertifikatų, pasirašytų $SCPTS_{TA}$ privačiuoju raktu, patikimumą sąrašą;

— Naudojami šifrai turi atitikti *5.1 skirsnio* reikalavimus.

4. **Sertifikato gyvavimo ciklo valdymas**

4.1. *Nacionalinių galinių sistemų registravimas*

Norėdamos dalyvauti SCPTS sistemoje, valstybės narės turi užsiregistruoti per SCPTS operatorių. Šiame skirsnyje aprašoma techninė ir veiklos procedūra, kurios reikia laikytis norint užregistruoti nacionalinę galinę sistemą.

SCPTS operatorius ir valstybė narė turi keistis informacija apie techninius kontaktinius asmenis, atsakingus už prisijungimo prie sistemos procesą. Daroma prielaida, kad techninius kontaktinius asmenis įteisina jų valstybės narės, o tapatybės nustatymas ir (arba) autentiškumo patvirtinimas atliekamas kitais kanalais. Pavyzdžiui, autentiškumo patvirtinimas gali būti atliekamas, kai valstybės narės techninis kontaktinis asmuo e. paštu pateikia sertifikatus kaip slaptažodžiu užšifruotas rinkmenas ir telefonu perduoda atitinkamą slaptažodį SCPTS operatoriui. Taip pat gali būti naudojami kiti saugūs kanalai, kuriuos nustato SCPTS operatorius.

Registravimo ir identifikavimo proceso metu valstybė narė turi pateikti tris skaitmeninius sertifikatus:

— valstybės narės TLS sertifikatą NB_{TLS},

— valstybės narės įkėlimo sertifikatą NB_{UP},

— valstybės narės CSCA sertifikatą (-us) NB_{CSCA}.

Visi pateikti sertifikatai turi atitikti *5 skirsnyje* nustatytus reikalavimus. SCPTS operatorius patikrins, ar pateiktas sertifikatas atitinka *5 skirsnio* reikalavimus. Po identifikavimo ir registracijos SCPTS operatorius:

— įtraukia NB_{CSCA} sertifikatą (-us) į patikimumo sąrašą, pasirašytą privačiuoju raktu, atitinkančiu $SCPTS_{TA}$ viešąjį raktą;

— įtraukia NB_{TLS} sertifikatą į SCPTS TLS procedūros užbaigimo baltąjį sąrašą;

— įtraukia NB_{UP} sertifikatą į SCPTS sistemą;

— pateikia valstybei narei $SCPTS_{TA}$ ir $SCPTS_{TLS}$ viešojo rakto sertifikatą.

4.2. *Sertifikavimo įstaigos, galiojimo laikotarpiai ir atnaujinimas*

Jei valstybė narė nori naudoti savo CSCA, šios įstaigos skaitmeniniai sertifikatai gali būti savarankiškai pasirašyti sertifikatai. Jie veikia kaip valstybės narės patikimumo užtikrinimo priemonė, todėl valstybė narė turi griežtai saugoti privatųjį raktą, atitinkantį CSCA sertifikato viešąjį raktą. Rekomenduojama, kad valstybės narės savo CSCA naudotų sistemą neprisijungus, t. y. kompiuterinę sistemą, kuri nėra prijungta prie jokio tinklo. Prieigai prie sistemos turi būti naudojama kelių asmenų kontrolė (pvz., pagal keturių akių principą). Pasirašius DSC, taikoma veiklos kontrolė, o sistema, kurioje saugomas privatusis CSCA raktas, saugoma taikant griežtą prieigos kontrolę. CSCA privačiajam raktui papildomai apsaugoti galima naudoti aparatinius saugumo modulius arba lustines korteles. Skaitmeniniuose sertifikatuose nurodytas galiojimo laikotarpis, kuriuo užtikrinamas sertifikato atnaujinimas. Atnaujinimas būtinas norint naudoti naujus kriptografinius raktus ir pritaikyti raktų dydžius, kai nauji skaičiavimo patobulinimai arba naujos atakos kelia grėsmę naudojamo kriptografinio algoritmo saugumui. Taikomas karkaso modelis (žr. *3.2 skirsnį*).

Atsižvelgiant į tai, kad skaitmeniniai COVID pažymėjimai galioja vienus metus, rekomenduojami šie galiojimo laikotarpiai:

— CSCA – 4 metai,

— DSC – 2 metai,

— įkėlimas – 1–2 metai,

— TLS kliento autentiškumo nustatymas – 1–2 metai.

Kad informacija būtų atnaujinta laiku, rekomenduojama nustatyti šiuos privačiųjų raktų naudojimo laikotarpius:

— CSCA – 1 metai,

— DSC – 6 mėn.

Valstybės narės turi laiku, pavyzdžiui, likus mėnesiui iki galiojimo pabaigos, sukurti naujus įkėlimo sertifikatus ir TLS sertifikatus, kad būtų užtikrintas sklandus veikimas. CSCA sertifikatai ir DSC turėtų būti atnaujinami likus ne mažiau kaip mėnesiui iki privačiojo rakto naudojimo pabaigos (atsižvelgiant į būtinas veiklos procedūras). Valstybės narės SCPTS operatoriui turi pateikti atnaujintus CSCA, įkėlimo ir TLS sertifikatus. Nebegaliojantys sertifikatai išbraukiami iš baltųjų ir patikimumo sąrašų.

Valstybės narės ir SCPTS operatorius turi stebėti savo sertifikatų galiojimą. Nėra centrinio subjekto, kuris saugotų įrašus apie sertifikato galiojimą ir informuotų dalyvius.

4.3. *Sertifikatų atšaukimas*

Paprastai skaitmeninius sertifikatus gali atšaukti juos išdavusi sertifikavimo įstaiga, naudodama sertifikatų atšaukimo sąrašus arba internetinį sertifikatų būsenos protokolo atsakiklį (OCSP). SCP sistemai CSCA turėtų pateikti sertifikatų atšaukimo sąrašus (CRL). Net jei šiuo metu šių CRL nenaudoja kitos valstybės narės, jie turėtų būti integruoti į būsimas programas. Jei CSCA nusprendžia neteikti CRL, tokios įstaigos DSC turi būti atnaujinti, kai CRL taps privalomi. Tikrintojai neturėtų naudoti OCSP dokumentų pasirašymo sertifikatams (DSC) patvirtinti; vietoje to, jie turėtų naudoti CRL. Rekomenduojama, kad nacionalinė galinė sistema atliktų būtiną iš SCPTS parsisiųsdintų DSC patvirtinimą ir tik patikimų ir patvirtintų DSC rinkinį perduotų nacionaliniams SCP tvirtintojams. SCP tvirtintojai neturėtų atlikti jokio DSC atšaukimo tikrinimo. Viena iš priežasčių – apsaugoti SCP turėtojų privatumą išvengiant bet kokios galimybės, kad bet kurio konkretaus DSC naudojimą gali stebėti su juo susijęs OCSP atsakiklis.

Valstybės narės gali pačios pašalinti savo DSC iš SCPTS, naudodamos galiojančius įkėlimo ir TLS sertifikatus. DSC pašalinimas reiškia, kad visi jį naudojant išduoti SCP taps negaliojantys, kai valstybės narės gaus atnaujintus DSC sąrašus. Labai svarbu apsaugoti DSC atitinkančią privačiojo rakto medžiagą. Valstybės narės turi informuoti SCPTS operatorių, kai jos turi atšaukti įkėlimo arba TLS sertifikatus, pavyzdžiui, dėl nacionalinės galinės sistemos saugumo pažeidimo. Tuomet SCPTS operatorius gali panaikinti pažeisto sertifikato patikimumą, pavyzdžiui, išbraukti jį iš TLS baltojo sąrašo. SCPTS operatorius gali pašalinti įkėlimo sertifikatus iš SCPTS duomenų bazės. Paketai, pasirašyti privačiuoju raktu, atitinkančiu šį įkėlimo sertifikatą, taps negaliojantys, kai nacionalinės galinės sistemos panaikins atšaukto įkėlimo sertifikato patikimumą. Jei CSCA sertifikatas turi būti atšauktas, valstybės narės informuoja SCPTS operatorių ir kitas valstybes nares, su kuriomis jas sieja patikimumo santykiai. SCPTS operatorius išduos naują patikimumo sąrašą, kuriame nebebus paveikto sertifikato. Visi šios CSCA išduoti DSC taps negaliojantys, kai valstybės narės atnaujins savo nacionalinės galinės sistemos patikimumo saugyklą. Jei reikia atšaukti $SCPTS_{TLS}$ arba $SCPTS_{TA}$ sertifikatą, SCPTS operatorius ir valstybės narės turi bendradarbiauti, kad užmegztų naują patikimą TLS ryšį ir sukurtų patikimumo sąrašą.

5. **Sertifikatų šablonai**

Šiame skirsnyje nustatomi kriptografiniai reikalavimai ir rekomendacijos, taip pat sertifikatų šablonams taikomi reikalavimai. Šiame skyriuje taip pat apibrėžiami SCPTS pažymėjimų šablonai.

5.1. *Kriptografiniai reikalavimai*

Kriptografiniai algoritmai ir TLS šifrų rinkiniai pasirenkami pagal dabartines Vokietijos federalinio informacijos saugumo biuro (BSI) arba vyresniųjų pareigūnų grupės informacinių sistemų klausimais (SOG-IS) sistemos rekomendacijas. Šios ir kitų institucijų bei standartizacijos organizacijų rekomendacijos yra panašios. Rekomendacijas galima rasti techninėse gairėse TR 02102-1 ir TR 02102-2 ([1]) arba SOG-IS suderintuose kriptografiniuose mechanizmuose ([2]).

5.1.1. DSC taikomi reikalavimai

Taikomi *I priedo 3.2.2 skirsnyje* nustatyti reikalavimai. Todėl dokumentus pasirašantiems asmenims primygtinai rekomenduojama naudoti elipsinės kreivės skaitmeninio parašo algoritmą (ECDSA) su NIST-p-256 (kaip apibrėžta FIPS PUB 186-4 D priede). Kitos elipsinės kreivės nepalaikomos. Dėl SCP vietos apribojimų valstybės narės neturėtų

([1]) BSI. Techninės gairės TR-02102 (bund.de).
([2]) SOG-IS. Patvirtinamieji dokumentai (sogis.eu).

naudoti RSA-PSS, net jei jis leidžiamas kaip atsarginis algoritmas. Jei valstybės narės naudoja RSA-PSS, jos turėtų naudoti 2048 bitų arba ne didesnį kaip 3072 bitų modulį. DSC parašui, kaip kriptografinė maišos funkcija, naudojamas SHA-2, kurio išvesties ilgis ≥ 256 bitai (žr. ISO/IEC 10118-3:2004).

5.1.2. Reikalavimai, taikomi perkėlimo lygmens saugumo, įkėlimo ir CSCA sertifikatams

Skaitmeniniams sertifikatams ir kriptografiniams parašams aktualūs SCPTS taikomi pagrindiniai reikalavimai kriptografiniams algoritmams ir rakto ilgiui apibendrinti toliau pateiktoje lentelėje (2021 m.):

Parašo algoritmas	Rakto dydis	Maišos funkcija
EC-DSA	Ne mažiau kaip 250 bitų	SHA-2, kurio išvesties ilgis ≥ 256 bitai
RSA-PSS (rekomenduojamas užpildas) RSA-PKCS#1 v1.5 (senesnis užpildas)	Ne mažesnis kaip 3000 bitų RSA modulis (N) su viešąja eksponente e > 2^16	SHA-2, kurio išvesties ilgis ≥ 256 bitai
DSA	Ne mažiau kaip 3000 bitų pagr. p, 250 bitų raktas q	SHA-2, kurio išvesties ilgis ≥ 256 bitai

Dėl plataus įgyvendinimo rekomenduojama EC-DSA elipsinė kreivė yra NIST-p-256.

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

Toliau pateiktoje lentelėje pateikiamos rekomendacijos dėl NB_{CSCA} sertifikato šablono, jei valstybė narė nusprendžia SCP sistemoje naudoti savo CSCA.

Įrašai **paryškintu šriftu** yra privalomi (turi būti įtraukti į sertifikatą), įrašai *kursyvu* yra rekomenduojami (turėtų būti įtraukti). Dėl nesamų laukelių rekomendacijos nenustatytos.

Laukelis	Reikšmė
Objektas	**cn=<ne tuščias ir unikalus bendrinis pavadinimas>***o=<Teikėjas>*, **c=<Valstybė narė, valdanti CSCA>**
Rakto naudojimas	**sertifikatų pasirašymas,***CRL pasirašymas* (mažiausiai)
Pagrindiniai apribojimai	**CA = teisinga, maršruto ilgio apribojimai = 0**

Objekto pavadinimo laukelis nurodytoje valstybėje narėje turi būti ne tuščias ir unikalus. Šalies kodas (c) turi sutapti su valstybe nare, kuri naudos šį CSCA sertifikatą. Sertifikate turi būti unikalus objekto rakto identifikatorius (SKI) pagal RFC 5280 ([3]).

5.3. *Dokumento pasirašytojo sertifikatas (DSC)*

Toliau pateiktoje lentelėje pateikiamos DSC gairės. Įrašai **paryškintu šriftu** yra privalomi (turi būti įtraukti į sertifikatą), įrašai *kursyvu* yra rekomenduojami (turėtų būti įtraukti). Dėl nesamų laukelių rekomendacijos nenustatytos.

Laukelis	Reikšmė
Serijos numeris	**unikalus serijos numeris**
Objektas	**cn=<ne tuščias ir unikalus bendrinis pavadinimas>**, *o=<Teikėjas>*, **c=<Valstybė narė, naudojanti šį DSC>**
Rakto naudojimas	**skaitmeninis parašas** (mažiausiai)

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

DSC turi būti pasirašytas privačiuoju raktu, atitinkančiu valstybės narės naudojamą CSCA sertifikatą.

Turi būti naudojami šie plėtiniai:

— Sertifikate turi būti nurodytas institucijos rakto identifikatorius (AKI), sutampantis su CSCA sertifikato objekto rakto identifikatoriumi (SKI)

— Sertifikate turėtų būti unikalus objekto rakto identifikatorius (pagal RFC 5280 ([4]))

Be to, sertifikate turėtų būti CRL skirstomojo taško plėtinys, nukreipiantis į sertifikatų atšaukimo sąrašą (CRL), kurį pateikia DSC išdavusi CSCA.

DSC gali būti naudojamas išplėstinis rakto plėtinys su nuliu ar daugiau rakto naudojimo politikos identifikatorių, kurie apriboja HCERT tipus, kuriuos leidžiama tikrinti šiuo sertifikatu. Jei jų yra vienas ar daugiau, tikrintojai patikrina rakto naudojimą pagal saugomą HCERT. Šiuo atveju nustatomos šios išplėstinio rakto naudojimo vertės:

Laukelis	Reikšmė
extendedKeyUsage	1.3.6.1.4.1.1847.2021.1.1 tyrimų atsakymų išdavėjams
extendedKeyUsage	1.3.6.1.4.1.1847.2021.1.2 skiepų įrašų išdavėjams
extendedKeyUsage	1.3.6.1.4.1.1847.2021.1.3 persirgimo įrašų išdavėjams

Jei nėra jokio rakto naudojimo plėtinio (t. y. jokių plėtinių ar nulinių plėtinių), šis sertifikatas gali būti naudojamas bet kokio tipo HCERT patvirtinti. Kituose dokumentuose gali būti apibrėžti atitinkami papildomi išplėstinių raktų naudojimo politikos identifikatoriai, naudojami tvirtinant HCERT.

5.4. *Įkėlimo sertifikatai (NBUP)*

Toliau pateiktoje lentelėje pateikiamos nacionalinės galinės sistemos įkėlimo sertifikato gairės. Įrašai **paryškintu šriftu** yra privalomi (turi būti įtraukti į sertifikatą), įrašai *kursyvu* yra rekomenduojami (turėtų būti įtraukti). Dėl nesamų laukelių rekomendacijos nenustatytos.

Laukelis	Reikšmė
Objektas	**cn=<ne tuščias ir unikalus bendrinis pavadinimas>**, *o=<Teikėjas>*,**c=<Valstybė narė, naudojanti šį įkėlimo sertifikatą>**
Rakto naudojimas	**skaitmeninis parašas** (mažiausiai)

5.5. *Nacionalinės galinės sistemos TLS kliento autentiškumo nustatymas (NB_{TLS})*

Toliau pateiktoje lentelėje pateikiamos nacionalinės galinės sistemos TLS kliento autentiškumo nustatymo sertifikato gairės. Įrašai **paryškintu šriftu** yra privalomi (turi būti įtraukti į sertifikatą), įrašai *kursyvu* yra rekomenduojami (turėtų būti įtraukti). Dėl nesamų laukelių rekomendacijos nenustatytos.

Laukelis	Reikšmė
Objektas	**cn=<ne tuščias ir unikalus bendrinis pavadinimas>**, *o=<Teikėjas>*,**c=<Valstybė narė nacionalinėje galinėje sistemoje>**
Rakto naudojimas	**skaitmeninis parašas** (mažiausiai)
Išplėstinio rakto naudojimas	kliento autentiškumo nustatymas (1.3.6.1.5.5.7.3.2)

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

Sertifikate taip pat gali būti naudojamas išplėstinis raktas – *serverio autentiškumo patvirtinimas (1.3.6.1.5.5.7.3.1)*, – tačiau jis nebūtinas.

5.6. *Patikimumo sąrašo parašo sertifikatas ($SCPTS_{TA}$)*

Toliau pateiktoje lentelėje apibrėžiamas SCPTS sertifikatas su patikimumo užtikrinimo priemone.

Laukelis	Reikšmė
Objektas	**cn=skaitmeninio žaliojo pažymėjimo tinklų sietuvas** ([5]), **o=<teikėjas>, c=<šalis>**
Rakto naudojimas	**skaitmeninis parašas** (mažiausiai)

5.7. *SCPTS TLS serverio sertifikatai ($SCPTS_{TLS}$)*

Toliau pateiktoje lentelėje apibrėžiamas SCPTS TLS sertifikatas.

Laukelis	Reikšmė
Objektas	cn=<SCPTS FQDN arba IP adresas>, o=<teikėjas>, c= <šalis>
SubjectAltName	dNSName: <SCPTS DNS pavadinimas> arba IP adresas: <SCPTS IP adresas>
Rakto naudojimas	**skaitmeninis parašas** (mažiausiai)
Išplėstinio rakto naudojimas	serverio autentiškumo tikrinimas (1.3.6.1.5.5.7.3.1)

Sertifikate taip pat gali būti naudojamas išplėstinis raktas – *serverio autentiškumo patvirtinimas (1.3.6.1.5.5.7.3.2)*, – tačiau jis nebūtinas.

SCPTS TLS sertifikatą turi išduoti viešai patikima sertifikavimo įstaiga (įtraukta į visas pagrindines naršykles ir operacines sistemas pagal „CAB Forum“ bazinius reikalavimus).

([5]) Čia vartojamas terminas „Skaitmeninis žaliasis pažymėjimas, o ne „ES skaitmeninis COVID pažymėjimas“, nes jis buvo užkoduotas ir įdiegtas sertifikate prieš teisės aktų leidėjams priimant naują terminą.