PROVEDBENA ODLUKA KOMISIJE (EU) 2021/1073

od 28. lipnja 2021.

o utvrđivanju tehničkih specifikacija i pravila za uspostavljanje okvira povjerenja za EU digitalnu COVID potvrdu, uspostavljenu Uredbom (EU) 2021/953 Europskog parlamenta i Vijeća

(Tekst značajan za EGP)

EUROPSKA KOMISIJA,

uzimajući u obzir Ugovor o funkcioniranju Europske unije,

uzimajući u obzir Uredbu (EU) 2021/953 Europskog parlamenta i Vijeća o okviru za izdavanje, provjeru i prihvaćanje interoperabilnih potvrda o cijepljenju, testiranju i preboljenju bolesti COVID-19 (EU digitalna COVID potvrda) radi olakšavanja slobodnog kretanja tijekom pandemije bolesti COVID-19 ([1]), a posebno njezin članak 9. stavke 1. i 3.,

budući da:

(1) Uredbom (EU) 2021/953 utvrđena je EU digitalna COVID potvrda da bi poslužila kao dokaz da je osoba cijepljena protiv bolesti COVID-19, da je dobila negativan rezultat testa ili da je preboljela bolest.

(2) Da bi EU digitalna COVID potvrda mogla funkcionirati u cijeloj Uniji, trebalo bi utvrditi tehničke specifikacije i pravila za ispunjavanje, sigurno izdavanje i provjeru digitalnih COVID potvrda, zaštitu osobnih podataka, definiranje zajedničke strukture jedinstvenog identifikatora potvrde i izdavanje valjanog, sigurnog i interoperabilnog crtičnog koda. Taj okvir povjerenja ujedno uvodi temeljne pretpostavke za interoperabilnost s međunarodnim normama i tehničkim sustavima te bi u tom smislu mogao biti model za suradnju na globalnoj razini.

(3) Za čitanje i tumačenje EU digitalne COVID potvrde potrebno je imati zajedničku strukturu podataka i dogovor o namjeravanom značenju svakog podatkovnog polja korisnog sadržaja i o njegovim mogućim vrijednostima. Da bi se olakšalo postizanje takve interoperabilnosti, potrebno je definirati zajedničku koordiniranu strukturu podataka za EU digitalnu COVID potvrdu. Mreža e-zdravstva, uspostavljena na temelju Direktive 2011/24/EU Europskog parlamenta i Vijeća ([2]), sastavila je smjernice za taj okvir. Te bi smjernice trebalo uzeti u obzir u utvrđivanju tehničkih specifikacija formata i upravljanja povjerenjem za EU digitalnu COVID potvrdu. Trebalo bi utvrditi specifikaciju strukture podataka, mehanizme kodiranja i mehanizam prijenosnog kodiranja u strojno čitljivom optičkom formatu (QR), koji se može prikazati na zaslonu mobilnog uređaja ili otisnuti na papiru.

(4) Uz tehničke specifikacije formata i upravljanja povjerenjem EU digitalne COVID potvrde trebalo bi donijeti opća pravila za ispunjavanje potvrda koja se trebaju koristiti za kodirane vrijednosti sadržaja EU digitalne COVID potvrde. Komisija bi na temelju rada mreže e-zdravstva trebala redovito ažurirati i objavljivati skupove vrijednosti za provedbu tih pravila.

(5) U skladu s Uredbom (EU) 2021/953 Europskog parlamenta i Vijeća vjerodostojne potvrde od kojih je sastavljena EU digitalna COVID potvrda trebale bi se moći jedinstveno identificirati jedinstvenim identifikatorom potvrde, pri čemu se treba uzeti u obzir da se građanima tijekom razdoblja valjanosti Uredbe (EU) 2021/953 može izdati više od jedne potvrde. Jedinstveni identifikator potvrde treba biti alfanumerički niz za koji bi se države članice trebale pobrinuti da ne sadržava nikakve podatke koji ga povezuju s drugim ispravama ili identifikacijskim podacima, npr. s brojevima putovnice ili osobne iskaznice, kako bi se spriječilo identificiranje nositelja potvrde. Da bi identifikator potvrde bio jedinstven, trebalo bi uspostaviti tehničke specifikacije i pravila za zajedničku strukturu.

([1]) SL L 211, 15.6.2021., str. 1.

([2]) Direktiva 2011/24/EU Europskog parlamenta i Vijeća od 9. ožujka 2011. o primjeni prava pacijenata u prekograničnoj zdravstvenoj skrbi (SL L 88, 4.4.2011., str. 45.).

(6) Sigurnost, vjerodostojnost, cjelovitost i valjanost potvrda koje čine EU digitalnu COVID potvrdu i njihova usklađenost s pravom Unije o zaštiti podataka ključne su za njihovo prihvaćanje u svim državama članicama. Ti se ciljevi postižu okvirom povjerenja kojim se utvrđuju pravila i infrastruktura za pouzdano i sigurno izdavanje i provjeru EU digitalnih COVID potvrda. Jedan od temelja okvira povjerenja trebala bi biti infrastruktura javnih ključeva s lancem povjerenja od zdravstvenih i drugih tijela od povjerenja država članica do pojedinačnih subjekata koji izdaju EU digitalne COVID potvrde. Komisija je stoga s ciljem uspostavljanja interoperabilnog sustava na razini EU-a izradila središnji sustav – pristupnik za EU digitalnu COVID potvrdu (dalje u tekstu „pristupnik") – u kojem su pohranjeni javni ključevi koji služe za provjeru. Kad se QR kod skenira, provjerava se njegov digitalni potpis na temelju relevantnog javnog ključa koji je prethodno pohranjen u tom središnjem pristupniku. Digitalni potpisi mogu služiti za jamčenje cjelovitosti i vjerodostojnosti podataka. Infrastrukture javnih ključeva stvaraju povjerenje jer povezuju javne ključeve s izdavateljima potvrda. Pristupnik se služi višestrukim certifikatima javnih ključeva radi potvrđivanja vjerodostojnosti. Radi sigurne razmjene podataka za materijale javnih ključeva među državama članicama i opće interoperabilnosti potrebno je definirati certifikate javnih ključeva koji se smiju upotrebljavati te propisati kako bi ih se trebalo generirati.

(7) Ovom se Odlukom omogućuje provedba zahtjeva Uredbe (EU) 2021/953 u praksi tako da se obrada osobnih podataka svede na nužan minimum za funkcioniranje EU digitalne COVID potvrde i da se pridonese tome da krajnji voditelji obrade provedu zahtjeve u skladu s integriranom zaštitom podataka.

(8) U skladu s Uredbom (EU) 2021/953 nadležna ili druga imenovana tijela odgovorna za izdavanje potvrda su voditelji obrade iz članka 4. stavka 7. Uredba (EU) 2016/679 Europskog parlamenta i Vijeća ([3]) u svojoj ulozi obrade osobnih podataka u postupku izdavanja potvrda. Ovisno o tome kako države članice organiziraju izdavanje, moguće je da imaju više nadležnih ili imenovanih tijela, npr. regionalne zdravstvene službe. U skladu s načelom supsidijarnosti to odabiru države članice. Stoga su, ako postoje višestruka nadležna ili druga imenovana tijela, države članice u najboljem položaju da se pobrinu da su odgovarajuće odgovornosti jasno dodijeljene, neovisno o tome postoje li odvojeni ili zajednički voditelji obrade (uključujući regionalne zdravstvene službe koje su uspostavile zajednički portal za izdavanje potvrda). Kad je riječ o provjerama potvrda koje provode nadležna tijela države članice odredišta ili tranzita ili pružatelji usluga prekograničnog prijevoza putnika koji su u skladu s nacionalnim pravom obvezni provoditi određene javnozdravstvene mjere tijekom pandemije bolesti COVID-19, ti vršitelji provjera moraju ispunjavati obveze proizašle iz pravila o zaštiti podataka.

(9) Budući da pristupnik za EU digitalne COVID potvrde sadržava samo javne ključeve tijela potpisnika, pristupnik ne obrađuje osobne podatke. Ti se ključevi odnose na tijela potpisnike i ne omogućavaju ni izravno ni neizravno identificiranje fizičke osobe kojoj je potvrda izdana. Komisija kao upravitelj pristupnika stoga ne bi trebala biti ni voditelj ni izvršitelj obrade osobnih podataka.

(10) Provedeno je savjetovanje s Europskim nadzornikom za zaštitu podataka u skladu s člankom 42. stavkom 1. Uredbe (EU) 2018/1725 Europskog parlamenta i Vijeća ([4]), koji je dostavio mišljenje 22. lipnja 2021.

(11) Budući da su tehničke specifikacije i pravila nužni da bi se Uredba (EU) 2021/953 primjenjivala od 1. srpnja 2021., primjena ove Odluke bez odgode je opravdana.

(12) Budući da je potrebno brzo uvesti EU digitalnu COVID potvrdu, ova Odluka trebala bi stupiti na snagu na dan objave,

([3]) Uredba (EU) 2016/679 Europskog parlamenta i Vijeća od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Direktive 95/46/EZ (Opća uredba o zaštiti podataka) (SL L 119, 4.5.2016., str. 1.).

([4]) Uredba (EU) 2018/1725 Europskog parlamenta i Vijeća od 23. listopada 2018. o zaštiti pojedinaca u vezi s obradom osobnih podataka u institucijama, tijelima, uredima i agencijama Unije i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Uredbe (EZ) br. 45/2001 i Odluke br. 1247/2002/EZ (SL L 295, 21.11.2018., str. 39.).

DONIJELA JE OVU ODLUKU:

Članak 1.

U Prilogu I. utvrđene su tehničke specifikacije za EU digitalnu COVID potvrdu, u kojima se utvrđuju opća struktura podataka, mehanizmi kodiranja i mehanizam prijenosnog kodiranja u strojno čitljivom optičkom formatu.

Članak 2.

U Prilogu II. ovoj Odluci utvrđena su pravila za ispunjavanje potvrda iz članka 3. stavka 1. Uredbe (EU) 2021/953.

Članak 3.

U Prilogu III. utvrđeni su zahtjevi kojima se utvrđuje zajednička struktura jedinstvenog identifikatora potvrde.

Članak 4.

U Prilogu IV. utvrđena su pravila upravljanja za certifikate javnih ključeva s obzirom na pristupnik za EU digitalnu COVID potvrdu kojima se podupiru aspekti interoperabilnosti.

Ova Odluka stupa na snagu na dan objave u *Službenom listu Europske unije*.

Sastavljeno u Bruxellesu 28. lipnja 2021.

Za Komisiju
Predsjednica
Ursula VON DER LEYEN

PRILOG I.

FORMAT I UPRAVLJANJE POVJERENJEM

Opća struktura podataka, mehanizmi kodiranja i mehanizmi prijenosnog kodiranja u strojno čitljivom optičkom formatu (dalje u tekstu „QR”)

1. Uvod

Tehničke specifikacije utvrđene u ovom Prilogu definiraju opću strukturu podataka i mehanizme kodiranja za EU digitalnu COVID potvrdu (DCC). Utvrđuju i mehanizam prijenosnog kodiranja u strojno čitljivom optičkom formatu (QR), koji se može prikazati na zaslonu mobilnog uređaja ili otisnuti na papiru. Formati spremnika elektroničkih zdravstvenih potvrda iz ovih specifikacija jesu generički, ali ovdje služe za DCC.

2. Terminologija

Za potrebe ovog Priloga „izdavatelji” znači organizacije koje se ovim specifikacijama služe za izdavanje zdravstvenih potvrda, a „vršitelji provjera” znači organizacije koje prihvaćaju zdravstvene potvrde kao dokaz zdravstvenog statusa. „Sudionici” znači izdavatelji i vršitelji provjera. Sudionici moraju koordinirati neke aspekte utvrđene u ovom Prilogu, npr. upravljanje imenskim prostorom i distribuciju kriptografskih ključeva. Pretpostavlja se da te zadaće obavlja određena služba, dalje u tekstu „tajništvo”.

3. Format spremnika elektroničkih zdravstvenih potvrda

Format spremnika elektroničkih zdravstvenih potvrda (HCERT) je osmišljen kao jedinstveno i standardizirano sredstvo za čuvanje zdravstvenih potvrda različitih izdavatelja („izdavatelji”). Cilj tih specifikacija je uskladiti prikazivanje, kodiranje i potpisivanje zdravstvenih potvrda radi lakše interoperabilnosti.

Za čitanje i tumačenje DCC-a bilo kojeg izdavatelja potrebno je imati zajedničku strukturu podataka i dogovor o značenju svakog podatkovnog polja korisnog sadržaja. Za potrebe takve interoperabilnosti zajednička koordinirana struktura podataka definirana je JSON shemom koja je okvir DCC-a.

3.1. *Struktura korisnog sadržaja*

Korisni sadržaj je strukturiran i kodiran kao CBOR i digitalno potpisan protokolom COSE. To se obično naziva CBOR-ovim *web*-tokenom (CBOR Web Token ili CWT), koji je definiran u RFC-u 8392 ([1]). Korisni sadržaj, definiran u odjeljcima u nastavku, prenosi se u hcert tvrdnji.

Vršitelj provjere mora moći provjeriti cjelovitost i vjerodostojnost porijekla podataka u korisnom sadržaju. Za potrebe tog mehanizma izdavatelj mora potpisati CWT asimetričnom shemom elektroničkog potpisa kako je definirano u specifikaciji COSE-a (RFC 8152 ([2])).

3.2. *CWT tvrdnje*

3.2.1. Pregled strukture CWT-a

Zaštićeno zaglavlje

— Potpisni algoritam (alg, oznaka 1)

— Identifikator ključa (kid, oznaka 4)

Korisni sadržaj

— Izdavatelj (iss, ključ tvrdnje 1, opcionalno, ISO 3166-1 alfa-2 izdavatelja)

— Izdan (iat, ključ tvrdnje 6)

— Istek (exp, ključ tvrdnje 4)

— Zdravstvena potvrda (hcert, ključ tvrdnje -260)

— EU digitalna COVID potvrda v1 (eu_DCC_v1, ključ tvrdnje 1)

Potpis

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

3.2.2. Potpisni algoritam

Parametar Potpisni algoritam (alg) sadržava algoritam kojim je izrađen potpis. Taj algoritam mora biti barem na razini trenutačnih SOG-IS-ovih smjernica, kako su sažete u sljedećim odlomcima.

Definirana su dva algoritma, primarni i sekundarni. Sekundarni algoritam upotrebljava se samo ako primarni algoritam nije prihvatljiv zbog pravila i propisa koje je uveo izdavatelj.

Zbog sigurnosti sustava sve implementacije sustava moraju sadržavati sekundarni algoritam. To znači da i primarni i sekundarni algoritam moraju biti implementirani.

SOG-IS-ove razine za primarne i sekundarne algoritme su:

— primarni algoritam: primarni algoritam je algoritam za digitalno potpisivanje na temelju eliptičkih krivulja (ECDSA), kako je definiran u odjeljku 2.3. norme ISO/IEC 14888–3:2006, s P–256 parametrima, kako su definirani u Dodatku D (D.1.2.3) norme FIPS PUB 186–4 u kombinaciji s algoritmom za SHA–256 hash kontrolne brojeve, kako je definiran u funkciji 4 norme ISO/IEC 10118–3:2004,

To odgovara parametru COSE algoritma ES256.

— sekundarni algoritam: sekundarni algoritam je RSASSA-PSS, kako je definiran u RFC-u 8230 ([3]), s modulom od 2048 bita u kombinaciji s algoritmom za SHA–256 hash kontrolne brojeve, kako je definiran u funkciji 4 norme ISO/IEC 10118–3:2004.

To odgovara parametru COSE algoritma PS256.

3.2.3. Identifikator ključa

Tvrdnja Identifikator ključa (kid) pokazuje potpisni certifikat za dokumente (DSC) s javnim ključem koji vršitelj provjere koristi za provjeru ispravnosti digitalnog potpisa. Upravljanje certifikatima javnih ključeva, uključujući zahtjeve za DSC-ove, opisano je u Prilogu IV.

Vršitelji provjere koriste tvrdnju Identifikator ključa (kid) da odaberu pravi javni ključ s popisa ključeva koji se odnose na izdavatelja iz tvrdnje Izdavatelj (iss). Izdavatelj zbog administrativnih razloga ili zbog prebacivanja na druge ključeve može istodobno koristiti nekoliko ključeva. Polje Identifikator ključa nije sigurnosno kritično. Zbog toga može biti i u nezaštićenom zaglavlju ako je potrebno. Vršitelji provjere moraju prihvaćati obje opcije. Ako Identifikator ključa postoji i u nezaštićenom i u zaštićenom zaglavlju, koristi se onaj iz zaštićenog zaglavlja.

Budući da se identifikator skraćuje (zbog ograničenja veličine), postoji vrlo mala mogućnost da na cijelom popisu DSC-ova koje vršitelj provjere prihvaća postoje DSC-ovi s jednakim kid-ovima. Zbog toga vršitelj provjere mora provjeriti sve DSC-ove s tim kid-om.

3.2.4. Izdavatelj

Tvrdnja Izdavatelj (iss) je niz koji opcionalno može sadržavati alfa-2 oznaku zemlje, u skladu s normom ISO3166-1, subjekta koji izdaje zdravstvenu potvrdu. Vršitelj provjere može iskoristiti tu tvrdnju za utvrđivanje koji skup DSC-ova treba uzeti za provjeru valjanosti. Ključ tvrdnje 1 služi za identifikaciju te tvrdnje.

3.2.5. Istek

Tvrdnja Istek (exp) sadržava vremenski žig kao cijeli broj u formatu NumericDate (kako je definirano u odjeljku 2. RFC-a 8392 ([4])), koji pokazuje dokad se taj potpis korisnog sadržaja smatra valjanim, nakon čega vršitelj provjere mora odbaciti sadržaj zbog isteka. Svrha parametra isteka je prisilno ograničiti razdoblje valjanosti zdravstvene potvrde. Ključ tvrdnje 4 služi za identifikaciju te tvrdnje.

Vrijednost tvrdnje Istek ne smije biti vrijeme nakon razdoblja valjanosti DSC-a.

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

3.2.6. Izdan

Tvrdnja Izdan (iat) sadržava vremenski žig kao cijeli broj u formatu NumericDate (kako je definirano u odjeljku 2. RFC-a 8392 ([5])), koji pokazuje kad je zdravstvena potvrda nastala.

Vrijednost polja Izdan ne smije biti vrijeme prije razdoblja valjanosti DSC-a.

Vršitelji provjere smiju uvesti dodatna pravila da ograniče valjanost zdravstvene potvrde na temelju vremena izdavanja. Ključ tvrdnje 6 služi za identifikaciju te tvrdnje.

3.2.7. Tvrdnja Zdravstvena potvrda

Tvrdnja Zdravstvena potvrda (hcert) je JSON objekt (RFC 7159 ([6])) koji sadržava podatke o zdravstvenom statusu. U istoj tvrdnji može postojati nekoliko različitih vrsta zdravstvenih potvrda, jedna od kojih je DCC.

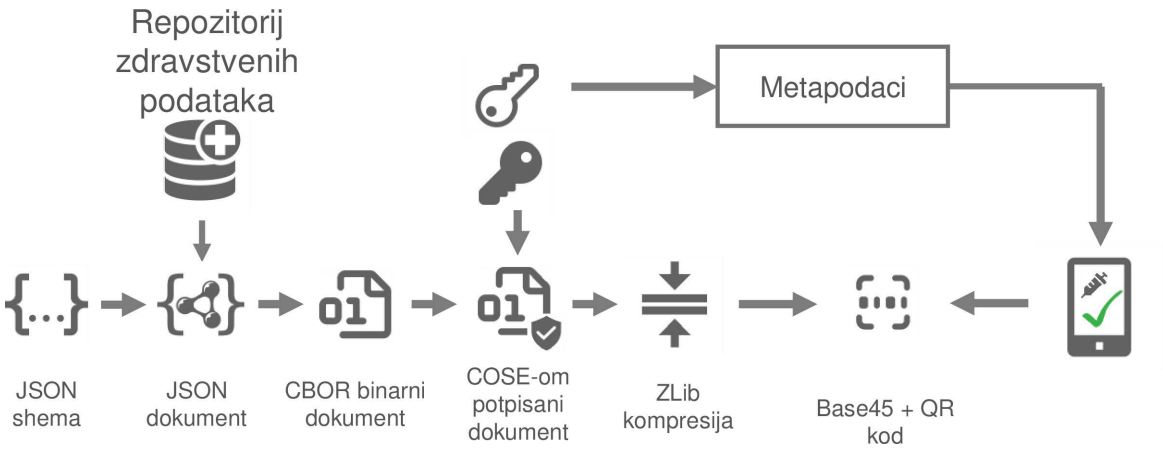
JSON služi isključivo za davanje sheme. Prezentacijski je format CBOR, kako je definiran u (RFC 7049 ([7])). Razvojni programeri zapravo ne moraju nikada dekodirati niti kodirati u/iz JSON-a nego mogu koristiti strukturu u memoriji.

Ključ tvrdnje za identifikaciju te tvrdnje je -260.

Nizovi u JSON objektu trebali bi biti normalizirani u skladu s kanonskim sastavljanjem normalizacijskog oblika (NFC) definiranim u normi Unicode. Aplikacije za dekodiranje trebale bi biti blage i robusne u tim aspektima, pri čemu je vrlo poželjno da se prihvaća bilo koja razumna konverzija tipa. Ako se u dekodiranju ili naknadnim funkcijama usporedbe naiđe na nenormalizirane podatke, implementacije bi se trebale ponašati kao da su ulazni podaci normalizirani u skladu s NFC-om.

4. Serijalizacija i izrada korisnog sadržaja DCC-a

Obrazac serijalizacije prikazan je na sljedećoj slici:



Proces počinje ekstrakcijom podataka, npr. iz repozitorija zdravstvenih podataka (ili nekog vanjskog izvora podataka), pri čemu se dobiveni podaci strukturiraju u skladu s definiranim shemama DCC-a. U tom se procesu konverzija podataka u definirani format i prilagođavanje da budu čitljivi ljudima mogu izvršiti prije serijalizacije u CBOR. Pokrate tvrdnji u svim se slučajevima povezuju s prikaznim imenima prije serijalizacije i nakon deserijalizacije.

Opcionalni nacionalni podatkovni sadržaj nije dopušten u potvrdama izdanima na temelju Uredbe (EU) 2021/953 ([8]). Podatkovni sadržaj je ograničen na definirane podatkovne elemente u minimalnom skupu podataka utvrđenom u Prilogu Uredbi 2021/953.

([5]) rfc8392 (ietf.org)
([6]) rfc7159 (ietf.org)
([7]) rfc7049 (ietf.org)
([8]) Uredba (EU) 2021/953 Europskog parlamenta i Vijeća od 14. lipnja 2021. o okviru za izdavanje, provjeru i prihvaćanje interoperabilnih potvrda o cijepljenju, testiranju i preboljenju bolesti COVID-19 (EU digitalna COVID potvrda) radi olakšavanja slobodnog kretanja tijekom pandemije bolesti COVID-19, SL L 211, 15.6.2021., str. 1.

5. **Prijenosno kodiranje**

5.1. *Neformatirano*

Kroz sučelja za proizvoljne podatke HCERT spremnik i njegovi korisni sadržaji mogu se prenositi u početnom obliku bilo kojim temeljnim pouzdanim prijenosom podataka koji je siguran za 8-bitno kodirane podatke. Među tim sučeljima su Near-Field Communication (NFC), Bluetooth ili prijenos protokolom na aplikacijskom sloju, na primjer prijenos HCERT-a od izdavatelja do nositeljeva mobilnog uređaja.

Ako se prijenos HCERT-a od izdavatelja do nositelja temelji na sučelju koje je samo za pokazivanje (npr. SMS, e-poruka), neformatirano prijenosno kodiranje očito nije primjenjivo.

5.2. *Crtični kod*

5.2.1. Komprimiranje korisnog sadržaja (CWT-a)

Da bi se smanjila veličina i da bi se povećale brzina i pouzdanost procesa čitanja HCERT-a, CWT se komprimira ZLIB-om (RFC 1950 ([9])) i kompresijskim mehanizmom Deflate u formatu definiranom u RFC-u 1951 ([10]).

5.2.2. QR 2D crtični kod

Da bi bolje radio sa starijom opremom koja je projektirana za rad s korisnim sadržajima u ASCII-ju, prije kodiranja u 2D crtični kod komprimirani CWT kodira se u ASCII kodnom shemom Base45.

Za generiranje 2D crtičnog koda koristi se QR format definiran u normi ISO/IEC 18004:2015. Preporučena je stopa ispravljanja pogrešaka Q (približno 25 %). Budući da se koristi Base45, QR kod mora koristiti alfanumeričko kodiranje (način 2, označen simbolima 0010).

Da bi vršitelji provjere mogli utvrditi tip kodiranih podataka i odabrati odgovarajuću shemu za dekodiranje i obradu, podaci kodirani s Base45 (kao u ovoj specifikaciji) moraju imati niz Identifikator konteksta, prefiks „HC1:”. Buduće verzije ove specifikacije koje utječu na kompatibilnost s prijašnjim verzijama definirat će novi niz Identifikator konteksta, pri čemu znak iza „HC” mora biti iz skupa znakova [1-9 A-Z]. Poredak povećanja definiran je tim redom, tj. prvo [1-9], a onda [A-Z].

Preporučeno je da prezentacijski medij na kojem se nalazi optički kod bude veličine dijagonale od 35 mm do 60 mm da bi ga mogli očitati čitači s fiksnim optičkim mehanizmima u kojima se prezentacijski medij postavlja na površinu čitača.

Ako je optički kod otisnut pisačem niske rezolucije (< 300 dpi), mora se paziti da je svaki simbol (točka) QR koda pravilan kvadrat. Nerazmjerna promjena veličine značila bi da bi neki redovi ili stupci QR koda imali pravokutne simbole, što bi u mnogim slučajevima smanjilo čitljivost.

6. **Format popisa povjerenja (popis CSCA-ova i DSC-ova)**

Svaka država članica dužna je dostaviti popis s najmanje jednim krovnim nacionalnim certifikacijskim tijelom za potpisivanje certifikata (CSCA) i popis svih valjanih potpisnih certifikata za dokumente (DSC-ovi).

6.1. *Pojednostavnjeni CSCA/DSC*

U ovoj verziji specifikacija države članice ne pretpostavljaju da se upotrebljavaju informacije iz popisa povučenih certifikata (CRL) niti da vršitelji provjere provjeravaju razdoblje upotrebe privatnog ključa.

Umjesto toga, primarni mehanizam za provjeru valjanosti je prisutnost certifikata na najnovijoj verziji tog popisa certifikata.

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

6.2. *PKI i centri povjerenja za ICAO-ove eMRTD-ove*

Države članice smiju imati zasebni CSCA – ali mogu i prijaviti i certifikate postojećih CSCA-ova ili DSC-ove za strojno čitljive putne isprave (eMRTD-ovi) ili ih čak nabavljati od (komercijalnih) centara povjerenja – pa ih prijavljivati. Međutim, svaki DSC mora biti potpisan od CSCA-a koji je država članica prijavila.

7. **Sigurnosni elementi**

U razvoju shema na temelju ove specifikacije države članice identificiraju, analiziraju i prate određene sigurnosne aspekte.

Trebalo bi uzeti u obzir barem aspekte u nastavku.

7.1. *Razdoblje valjanosti potpisa HCERT-a*

Izdavatelj HCERT-a dužan je ograničiti razdoblje valjanosti potpisa definiranjem isteka potpisa. Zbog toga nositelj mora periodično obnavljati zdravstvenu potvrdu.

Prihvatljivo razdoblje valjanosti određuje se na temelju praktičnih ograničenja. Na primjer, putnik možda ne bude mogao obnoviti zdravstvenu potvrdu za vrijeme puta u inozemstvo. Moguće je i da izdavatelj razmatra mogućnost neke sigurnosne prijetnje zbog koje bi izdavatelj morao povući DSC (što podrazumijeva prestanak valjanosti svih zdravstvenih potvrda potpisanih tim ključem prije isteka). Posljedice takvog događaja mogu se ograničiti redovitim zamjenama ključeva izdavatelja i zahtijevanjem obnavljanja svih zdravstvenih potvrda u razumnim intervalima.

7.2. *Upravljanje ključevima*

Radi osiguravanja cjelovitosti podataka i provjeravanja autentičnosti porijekla podataka ova se specifikacija u velikoj mjeri oslanja na jake kriptografske mehanizme. Stoga je potrebno štititi povjerljivost privatnih ključeva.

Povjerljivost kriptografskih ključeva može biti kompromitirana zbog različitih razloga, npr.:

— proces generiranja ključeva mogao je imati nedostatke, pa su generirani slabi ključevi,

— ključevi su mogli biti izloženi zbog ljudske pogreške,

— unutarnji ili vanjski počinitelji mogli su ukrasti ključeve,

— ključevi se mogu izračunati kriptoanalizom.

Radi umanjivanja rizika zbog preslabog potpisnog algoritma, zbog čega se ključevi mogu kompromitirati kriptoanalizom, u ovoj je specifikaciji preporučeno da svi sudionici uvedu sekundarni, pričuvni potpisni algoritam koji će se od primarnog razlikovati na temelju parametara ili matematičkog problema.

Kad su navedeni rizici posljedica izdavateljeva radnog okruženja, moraju se uvesti mjere ublažavanja kojima se osigurava djelotvorna kontrola, npr. generiranje, pohranjivanje i upotrebljavanje ključeva u hardverskim sigurnosnim modulima (HSM-ovi). Snažno se potiče korištenje HSM-ova za potpisivanje zdravstvenih potvrda.

Neovisno o tome koristi li izdavatelj HSM-ove, trebalo bi definirati raspored prebacivanja na nove ključeve s učestalošću zamjena ključeva koja je razmjerna izloženosti ključeva vanjskim mrežama, drugim sustavima i osoblju. Dobro odabran raspored prebacivanja na druge ključeve također smanjuje rizike povezane s pogrešno izdanim zdravstvenim potvrdama jer izdavatelj može prema potrebi povlačenjem ključa skupno povući takve zdravstvene potvrde.

7.3. *Provjera valjanosti ulaznih podataka*

Ove specifikacije mogu se primijeniti tako da se podrazumijeva da se podaci, koji se unose u sustave koji bi mogli biti kritični za rad, primaju iz nepouzdanih izvora. Da bi se rizici povezani s tim vektorom napada sveli na najmanju moguću mjeru, mora se provjeriti valjanost svih ulaznih polja na temelju vrste podataka, duljine i sadržaja. Izdavateljev potpis mora se provjeriti prije bilo kakva obrade sadržaja HCERT-a. Međutim, provjera izdavatelja potpisa znači da se prvo mora proći kroz izdavateljevo zaštićeno zaglavlje u koje potencijalni napadač može pokušati ubaciti pažljivo sastavljene informacije osmišljene za kompromitiranje sigurnosti sustava.

8. **Upravljanje povjerenjem**

Da bi se provjerio potpis HCERT-a, potreban je javni ključ. Države članice objavljuju te javne ključeve. Svaki vršitelj provjere treba imati popis svih javnih ključeva kojima je spreman vjerovati (jer javni ključ nije dio HCERT-a).

Sustav se sastoji od (samo) dva sloja: za svaku državu članicu najmanje jedan certifikat na nacionalnoj razini, kakvim se potpisuju potpisni certifikati za dokumente koji se koriste u svakodnevnom radu.

Certifikati država članica zovu se certifikati krovnog nacionalnog certifikacijskog tijela za potpisivanje certifikata (CSCA) i obično su samopotpisani certifikati. Države članice mogu imati više CSCA-ova, npr. ako prenose obveze na regionalnu razinu. Certifikatima CSCA-ova redovito se potpisuju potpisni certifikati za dokumente (DSC-ovi), kojima se potpisuju HCERT-ovi.

„Tajništvo" je funkcija. Ono redovito objedinjuje i objavljuje DSC-ove država članica, nakon što ih provjeri na temelju popisa certifikata CSCA-ova (koji je dostavljen i provjeren na drugi način).

Dobiveni popis DSC-ova je objedinjeni skup prihvatljivih javnih ključeva (i odgovarajućih identifikatora ključeva) koji vršitelji provjere mogu koristiti za provjeru potpisa na HCERT-ovima. Vršitelji provjera moraju redovito preuzimati taj popis pa ažurirati svoju kopiju.

Format takvih popisa specifičnih za pojedinačnu državu članicu može se prilagoditi za pojedinačno nacionalno okruženje. Zbog toga format datoteke tog popisa povjerenja može biti različit, npr. može biti potpisani JWKS (format JWK skupa u skladu s odjeljkom 5. RFC-a 7517 ([11])) ili bilo koji drugi format specifičan za tehnologiju u primjeni u toj državi članici.

Radi jednostavnosti države članice mogu dostaviti certifikate postojećih CSCA-ova za svoje sustave za ICAO-ve eMRTD-ove ili, kako preporučuje Svjetska zdravstvena organizacija, generirati novi koji će biti namjenski za zdravstvo.

8.1. *Identifikator ključa (kids)*

Identifikator ključa (kid) izračunava se u trenutku sastavljanja popisa pouzdanih javnih ključeva od DSC-ova i sastoji se od skraćenog (prvih 8 bajtova) SHA-256 otiska DCS-a kodiranog u DER (neformatiranom) formatu.

Vršitelji provjere ne moraju izračunavati identifikator ključa na temelju DSC-a i mogu izravno usporediti identifikator ključa u izdanoj zdravstvenoj potvrdi s identifikatorom ključa na popisu povjerenja.

8.2. *Razlike u odnosu na model povjerenja infrastrukture javnih ključeva za ICAO-ove eMRTD-ove*

Iako se ovaj model temelji na najboljim praktičnim rješenjima modela povjerenja infrastrukture javnih ključeva za ICAO-ove eMRTD-ove, radi brzine je uvedeno nekoliko pojednostavnjenja:

— svaka država članica smije dostaviti više certifikata CSCA-ova,

— razdoblje valjanosti DSC-a (upotreba ključa) smije biti bilo koja vrijednost unutar razdoblja valjanosti certifikata CSCA-a, koja ne mora ni biti deklarirana,

— DSC može sadržavati identifikatore pravila (proširena upotreba ključa) koja su specifična za zdravstvene potvrde,

— države članice, ako tako odluče, nikad ne moraju provjeravati objavljena povlačenja, nego se mogu samo oslanjati na popise DSC-ova koje im svakodnevno šalje tajništvo ili koje same sastavljaju.

([11]) rfc7517 (ietf.org)

PRILOG II.

PRAVILA ZA ISPUNJAVANJE EU DIGITALNIH COVID POTVRDA

Cilj je općih pravila za skupove vrijednosti utvrđenih u ovom Prilogu postići interoperabilnost na semantičkoj razini i omogućiti dosljednost u tehničkim implementacijama DCC-a. Elementi iz ovog Priloga mogu se upotrebljavati za tri različite vrijednosti (cijepljenje/testiranje/preboljenje), kako je propisano u Uredbi (EU) 2021/953. U ovom su Prilogu popisani samo elementi koje je potrebno semantički standardizirati skupovima kodiranih vrijednosti.

Države članice su odgovorne za prevođenje kodiranih elemenata na nacionalni jezik.

Za sva podatkovna polja koja nisu navedena u sljedećim opisima skupova vrijednosti preporučeno je da budu kodirana u UTF-8 (ime, centar za testiranje, izdavatelj potvrde). Za podatkovna polja koja sadržavaju datume (datum rođenja, datum uzimanja uzorka, datum prvog pozitivnog rezultata testa, datumi valjanosti potvrde) preporučeno je da budu kodirana u skladu s normom ISO 8601.

Ako iz nekog razloga nije moguće primijeniti najpoželjniji kodni sustav, mogu se upotrijebiti drugi međunarodni kodni sustavi, pri čemu bi trebalo navesti kako se kodovi tog drugog sustava mapiraju na najpoželjnijiji kodni sustav. U iznimnim slučajevima tekst (prikazna imena) smije poslužiti kao pričuvni mehanizam ako odgovarajući kod nije dostupan u definiranim skupovima vrijednosti.

Države članice koje upotrebljavaju druga kodiranja u svojim sustavima trebala bi mapirati takve kodove na opisane skupove vrijednosti. Države članice su odgovorne za sva takva mapiranja.

Komisija je uz potporu mreže e-zdravstva i Odbora za zdravstvenu sigurnost dužna redovito ažurirati te skupove vrijednosti. Ažurirani skupovi vrijednosti objavljuju se na odgovarajućim internetskim stranicama Komisije i na internetskim stranicama mreže e-zdravstva. Na raspolaganju bi trebala postojati evidencija promjena.

1. **Bolest ili agens na koji se cilja/bolest ili agens koji je nositelj prebolio: COVID-19 (SARS-CoV-2 ili jedna od njegovih varijanti)**

   Najpoželjniji kodni sustav: SNOMED CT.

   Za upotrebu u potvrdi 1, 2 i 3.

   Odabrani kodovi odnose se na COVID-19 ili, ako su potrebni detaljniji podaci o genetskoj varijanti virusa SARS-CoV-2, na te varijante ako su zbog epidemioloških razloga potrebne tako detaljni podaci.

   Primjer koda koji bi trebalo koristiti je, za kod SNOMED CT, 840539006 (COVID-19).

2. **Cjepivo ili profilaksa protiv bolesti COVID-19**

   Najpoželjniji kodni sustav: SNOMED CT ili klasifikacija ATC.

   Za upotrebu u potvrdi 1.

   Primjeri kodova koje bi trebalo koristiti iz najpoželjnijih kodnih sustava su, za kod SNOMED CT, 1119305005 (antigensko cjepivo protiv virusa SARS-CoV-2), 1119349007 (mRNA cjepivo protiv virusa SARS-CoV-2) ili J07BX03 (cjepiva protiv bolesti COVID-19). Trebalo bi proširiti skup vrijednosti u skladu s razvojem i puštanjem u uporabu novih vrsta cjepiva.

3. **Lijek (cjepivo) protiv bolesti COVID-19**

   Najpoželjniji kodni sustavi (od najpoželjnijeg):

   — Registar lijekova unije za cjepiva s odobrenjem na razini EU-a (brojevi odobrenja)

   — Neki svjetski registar cjepiva, npr. registar koji bi mogla uspostaviti Svjetska zdravstvena organizacija

   — Naziv lijeka (cjepiva) u ostalim slučajevima; sve bjeline u nazivu zamjenjuju se spojnicom (-).

Ime skupa vrijednosti: Cjepivo.

Za upotrebu u potvrdi 1.

Primjer koda koji bi trebalo koristiti je, za najpoželjnije kodne sustave, EU/1/20/1528 (Comirnaty). Primjer ako se kao kod koristi naziv cjepiva: Sputnik-V (za Sputnik V).

4. **Nositelj odobrenja za stavljanje u promet cjepiva protiv bolesti COVID-19 ili proizvođač tog cjepiva**

Najpoželjniji kodni sustav:

— Kod organizacije iz EMA-e (SPOR za ISO norme za identifikaciju lijekova)

— Neki svjetski registar nositelja odobrenja za stavljanje u promet cjepiva ili proizvođača tog cjepiva, npr. registar koji bi mogla uspostaviti Svjetska zdravstvena organizacija

— Ime organizacije u ostalim slučajevima; sve bjeline u nazivu zamjenjuju se spojnicom (-).

Za upotrebu u potvrdi 1.

Primjer koda koji bi trebalo koristiti je, za najpoželjniji kodni sustav, ORG-100001699 (AstraZeneca AB). Primjer ako se kao kod koristi ime organizacije: Sinovac-Biotech (za Sinovac Biotech).

5. **Broj doze u seriji i ukupan broj doza u seriji**

Za upotrebu u potvrdi 1.

Dva polja:

(1) broj doze u ciklusu

(2) broj očekivanih doza za cijeli ciklus (specifičan za osobu u vrijeme cijepljenja).

Na primjer, 1/1 i 2/2 smatraju se cijelim ciklusom, što obuhvaća i opciju 1/1 za cjepiva koja se sastoje od dvije doze, ali u slučaju građana kojima je prije cijepljenja dijagnosticiran COVID-19 država članica primjenjuje protokol cijepljenja jednom dozom. Ukupan broj doza u seriji navodi se u skladu s podacima dostupnima u trenutku cijepljenja. Na primjer, ako je za neko cjepivo potrebno cijepljenje trećom dozom (docjepljivanje) u trenutku zadnjeg cijepljenja, to bi se trebalo vidjeti iz broja u drugom polju (2/3, 3/3 itd.).

6. **Država članica ili treća zemlja u kojoj je cjepivo primljeno/u kojoj je obavljeno testiranje**

Najpoželjniji kodni sustav: Oznake zemalja ISO 3166.

Za upotrebu u potvrdi 1, 2 i 3.

Sadržaj skupa vrijednosti: cijeli popis dvoslovnih oznaka, dostupan kao skup vrijednosti u FHIR-u (http://hl7.org/fhir/ValueSet/iso3166-1-2).

7. **Vrsta testa**

Najpoželjniji kodni sustav: LOINC.

Za upotrebu u potvrdi 2 i, ako se delegiranim aktom uvede izdavanje potvrda o preboljenju na temelju testova koji nisu NAAT, za upotrebu u potvrdi 3.

Kodovi u ovom skupu vrijednosti odnose se na metodu testiranja i odabiru se tako da se barem vidjeti razlika između NAAT testova i brzih antigenskih testova, kako je navedeno u Uredbi (EU) 2021/953.

Primjer koda koji bi trebalo koristiti je, za najpoželjniji kodni sustav, LP217198-3 (brzi imunološki test).

8. **Proizvođač i trgovačko ime testa (nije obvezno za test NAAT)**

Najpoželjniji kodni sustav: HSC-ov popis brzih antigenskih testova, kako ga vodi JRC (baza podataka o *in vitro* dijagnostičkim proizvodima i metodama za testiranje na COVID-19).

Za upotrebu u potvrdi 2.

Sadržaj skupa vrijednosti su brzi antigenski testovi sa zajedničkog i ažuriranog popisa brzih antigenskih testova za COVID-19 koji je sastavljen na temelju Preporuke Vijeća 2021/C 24/01 i dogovoren s Odborom za zdravstvenu sigurnost. Taj popis održava JRC u bazi podataka o *in vitro* dijagnostičkim proizvodima i metodama za testiranje na COVID-19: https://covid-19-diagnostics.jrc.ec.europa.eu/devices/hsc-common-recognition-rat

U tom kodnom sustavu upotrebljavaju se relevantna polja, npr. identifikator proizvoda za testiranje, naziv testa i ime proizvođača, u skladu s JRC-ovim strukturiranim formatom dostupnim na https://covid-19-diagnostics.jrc.ec.europa.eu/devices.

9. **Rezultat testa**

Najpoželjniji kodni sustav: SNOMED CT.

Za upotrebu u potvrdi 2.

Na temelju odabranih kodova mora se vidjeti razlika između pozitivnog (otkriveno) i negativnog (nije otkriveno) rezultata testa. Dodatne vrijednosti (npr. neodređeno) mogu se dodati u slučaju potrebe.

Primjeri kodova koje bi trebalo koristiti su, za najpoželjniji kodni sustav, 260415000 (nije otkriveno) i 260373001 (otkriveno).

PRILOG III.

ZAJEDNIČKA STRUKTURA JEDINSTVENOG IDENTIFIKATORA POTVRDE

1. **Uvod**

Svaka EU digitalna COVID potvrda (DCC) mora sadržavati jedinstveni identifikator potvrde (UCI) na temelju kojeg je moguća interoperabilnost DCC-ova. UCI može poslužiti za provjeru potvrde. Države članice su odgovorne za praktičnu primjenu UCI-ja. UCI je način za provjeravanje istinitosti potvrde i, ako je primjenjivo, za povezivanje s registracijskim sustavom (npr. IIS-om). Na temelju tih identifikatora funkcioniraju i (papirnate i digitalne) tvrdnje država članica da su pojedinci cijepljeni ili testirani.

2. **Elementi jedinstvenog identifikatora potvrde**

UCI ima zajedničku strukturu i format na temelju kojeg strojevi i ljudi mogu lako tumačiti podatke i može biti povezan s elementima kao što su država članica cijepljenja, samo cjepivo i identifikator države članice. Državama članicama daje fleksibilnost da ga formatiraju uz potpuno poštovanje propisa o zaštiti podataka. Poredak zasebnih elemenata slijedi definiranu hijerarhiju koja omogućuje da se blokovi u budućnosti mijenjaju, a da se ne naruši njezina strukturna cjelovitost.

Moguća rješenja za sastav UCI-ja čine raspon u kojem su modularnost i razumljivost za ljude dva glavna parametra na temelju kojih nastaju razlike, a u kojem postoji jedna temeljna karakteristika:

— modularnost: stupanj u kojem je kod sastavljen od jasno različitih blokova sa semantički različitim informacijama,

— razumljivost za ljude: stupanj u kojem kod ima značenje ili u kojem ga čovjek može protumačiti,

— globalna jedinstvenost: dobro upravljanje identifikatorom zemlje ili tijela, pri čemu se od svake zemlje (od svakog tijela) očekuje da upravlja svojim dijelom imenskog prostora tako da nikada ne upotrijebi ili ne izda isti identifikator. Ta kombinacija omogućava da svaki identifikator bude globalno jedinstven.

3. **Opći zahtjevi**

Za UCI moraju biti ispunjeni sljedeći temeljni zahtjevi:

(1) skup znakova: dopušteni su samo veliki alfanumerički znakovi iz skupa US-ASCII (velika slova od „A” do „Z” i brojke od „0” do „9”), u kombinaciji sa specijalnim znakovima za razdvajanje iz RFC-a 3986 [1] [2], tj. {,/,'#,':'};

(2) najveća duljina: u osmišljavanju rješenja trebalo bi ciljati na 27-30 znakova [3];

(3) prefiks verzije: odnosi se na verziju UCI sheme. Prefiks verzije je „01” za ovu verziju dokumenta; prefiks verzije je dvoznamenkasti broj;

(4) prefiks zemlje: oznaka zemlje je utvrđena u normi ISO 3166 – 1. Dulje oznake (najmanje 3 znaka, npr. „UNHCR”) rezervirane su za buduću upotrebu;

(5) sufiks koda/kontrolni zbroj:

5.1. države članice trebale bi koristiti kontrolne zbrojeve ako je vjerojatno da bi moglo doći do pogreške zbog prijenosa, (ljudske) transkripcije ili drugog razloga (tj. u slučaju pisanog oblika);

5.2. kontrolni zbroj ne smije biti temelj provjere valjanosti potvrde niti je tehnički dio identifikatora; on služi samo za provjeru cjelovitosti koda. Kontrolni zbroj izračunava se u skladu s normom ISO-7812 – 1 (LUHN-10) [4] na temelju cijelog UCI-ja u digitalnom/fizičkom prijenosnom formatu. Kontrolni zbroj mora biti odvojen od ostatka UCI-ja znakom „#”.

---

[1] rfc3986 (ietf.org)

[2] Polja kao što su spol, broj serije/lota, punkt za cijepljenje, identifikacija zdravstvenog radnika, datum sljedećeg cijepljenja nisu nužno potrebna osim za medicinsku uporabu.

[3] Kad je riječ o rješenjima s QR kodovima, države članice trebale bi razmotriti dodatni skup znakova ukupne duljine od 72 znaka (uključujući 27-30 znakova samog identifikatora) koji može prenositi druge informacije. Definiranje specifikacija tih informacija je u nadležnosti država članica.

[4] Algoritam Luhn mod N je proširenje Luhnova algorithma (poznatog i kao algoritam mod 10) koji služi za brojčane oznake, a koristi se, npr., za izračun kontrolnog zbroja na kreditnim karticama. Proširenje omogućuje algoritmu da radi s nizovima vrijednosti bilo koje baze (u našem slučaju s alfa znakovima).

Trebalo bi osigurati kompatibilnost s prijašnjim verzijama: države članice koje s vremenom promijene strukturu svojih identifikatora (unutar glavne verzije, trenutačno v1) moraju se pobrinuti da se bilo koja dva identična identifikatora odnose na istu potvrdu o cijepljenju/tvrdnju. Drugim riječima, države članice ne smiju ponovno upotrijebiti isti identifikator.

4. **Opcije za jedinstvene identifikatore potvrde za potvrde o cijepljenju**

U smjernicama mreže e-zdravstva za provjerive potvrde o cijepljenju i za osnovne elemente interoperabilnosti ([5]) predviđene su različite opcije na raspolaganju državama članicama i drugim stranama, pri čemu u različitim državama članicama mogu istodobno postojati različite opcije. Države članice mogu primijeniti te opcije u različitim verzijama UCI sheme.

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

PRILOG IV.

UPRAVLJANJE CERTIFIKATIMA JAVNIH KLJUČEVA

1. Uvod

Države članice sigurno i pouzdano razmjenjuju potpisne ključeve za EU digitalne COVID potvrde pristupnikom za EU digitalnu COVID potvrdu (DCCG), koji je središnji repozitorij za javne ključeve. DCCG omogućava državama članicama da objavljuju javne ključeve koji su parovi privatnim ključevima kojima potpisuju digitalne COVID potvrde. Države članice se mogu osloniti na DCCG da pravodobno preuzmu ažurne materijale javnih ključeva. DCCG se naknadno može proširiti za razmjenu pouzdanih dopunskih informacija država članica, npr. pravila valjanosti za DCC-ove. Model povjerenja okvira za DCC je infrastruktura javnih ključeva (PKI). Svaka država članica mora imati najmanje jedno krovno nacionalno certifikacijsko tijelo za potpisivanje certifikata (CSCA), čiji certifikati imaju relativno dugo razdoblje valjanosti. Ovisno o odluci države članice, CSCA može biti isti CSCA koji se koristi za strojno čitljive putne isprave, ali se može i razlikovati od njega. CSCA izdaje certifikate javnih ključeva nacionalnim, kratkoročnim potpisnicima (tj. potpisnicima za DCC-ove), a ti se certifikati nazivaju potpisni certifikati za dokumente (DSC-ovi). CSCA je temelj povjerenja čiji certifikat države članice mogu iskoristiti da provjere vjerodostojnost i cjelovitost redovito mijenjanih DSC-ova. Nakon potvrde valjanosti države članice mogu dostaviti te certifikate (ili samo njihove javne ključeve) svojim aplikacijama za provjeru valjanost DCC-ova. Uz CSCA-ove i DSC-ove DCCG se također oslanja na PKI za provjeru vjerodostojnosti transakcija i potpisivanje podataka te kao na temelj autentifikacije i način jamčenja cjelovitosti komunikacijskih kanala između država članica i DCCG-a.

Digitalni potpisi mogu služiti da se postignu cjelovitost i vjerodostojnost podataka. Infrastrukture javnih ključeva stvaraju povjerenje jer povezuju javne ključeve s provjerenim identitetima (ili izdavateljima). To je potrebno da bi drugi sudionici mogli provjeriti porijeklo podataka i identitet komunikacijskog partnera, pa odlučiti vjeruju li im. DCCG se služi višestrukim certifikatima javnih ključeva radi potvrđivanja vjerodostojnosti. Da bi se postigla opća interoperabilnost među državama članicama, ovim Prilogom određuje se koji se certifikati javnih ključeva koriste i kako se generiraju. Navedeni su detaljniji podaci o certifikatima javnih ključeva i daju se smjernice za predloške certifikata i razdoblja valjanosti za države članice koje žele imati vlastiti CSCA. Budući da DCC-ovi moraju biti provjerivi u definiranom razdoblju (od izdavanja do zadanog isteka), potrebno je definirati model provjere za sve potpise primijenjene na certifikate javnih ključeva i DCC-ove.

2. Terminologija

Sljedeća tablica sadržava pokrate i terminologiju koji se koriste u ovom Prilogu.

Pojam	Definicija
Certifikat	Ili certifikat javnog ključa. X.509 v3 certifikat s javnim ključem subjekta.
CSCA	Krovno nacionalno certifikacijsko tijelo za potpisivanje certifikata.
DCC	EU digitalna COVID potvrda. Potpisani digitalni dokument s informacijama o cijepljenju, testiranju ili preboljenju.
DCCG	Pristupnik za EU digitalnu COVID potvrdu. Sustav za razmjenu DSC-ova među državama članicama.
$DCCG_{TA}$	Certifikat temelj povjerenja DCCG-a. Odgovarajući privatni ključ koristi se za potpisivanje svih certifikata CSCA-ova izvan mrežnog okruženja.
$DCCG_{TLS}$	TLS certifikat poslužitelja DCCG-a.
DSC	Potpisni certifikat za dokumente. Certifikat javnog ključa tijela potpisnika dokumenata države članice (npr. sustava koji smije potpisivati DCC-ove). Ovaj certifikat izdaje CSCA države članice.
EC-DSA	Algoritam za digitalno potpisivanje na temelju eliptičkih krivulja.
Država članica	Država članica Europske unije.

Pojam	Definicija
mTLS	Uzajamni TLS. TLS protokol s uzajamnom autentifikacijom.
NB	Nacionalni *backend* sustav države članice.
NB_{CSCA}	Certifikat CSCA-a države članice (može postojati više od jednog CSCA-a).
NB_{TLS}	Autentifikacijski TLS certifikat klijenta nacionalnog *backend* sustava.
NB_{UP}	Certifikat koji nacionalni *backend* sustav koristi za potpisivanje podatkovnih paketa koji se šalju DCCG-u.
PKI	Infrastruktura javnih ključeva. Model povjerenja koji se temelji na certifikatima javnih ključeva i certifikacijskim tijelima.
RSA	Asimetrični kriptografski algoritam koji se temelji na rastavljanju na cjelobrojne faktore korišten za digitalne potpise ili asimetrično šifriranje.

3. **Komunikacijski tokovi i sigurnosne usluge DCCG-a**

Ovaj odjeljak je pregled komunikacijskih tokova i sigurnosnih usluga u DCCG-u. U njemu je također definirano koji se ključevi i certifikati koriste za zaštitu komunikacije, primljenih informacija, DCC-ova i potpisanog popisa povjerenja koji sadržava sve uvrštene certifikate CSCA-ova. DCCG funkcionira kao podatkovno čvorište na kojem države članice mogu razmjenjivati potpisane podatkovne pakete.

DCCG predaje primljene podatkovne pakete doslovno, tj. DCCG niti briše niti dodaje DSC-ove iz primljenih paketa. NB-ovi država članica moraju moći provjeravati cjelovitost i vjerodostojnost primljenih podataka u cijeloj komunikaciji. U tu svrhu nacionalni NB-ovi i DCCG koriste uzajamnu TLS autentifikaciju da uspostave sigurnu vezu. To je dodatna mjera uz potpise razmijenjenih podataka.

3.1. *Autentifikacija i uspostava veze*

DCCG koristi TLS s uzajamnom autentifikacijom za uspostavljanje autentificiranog šifriranog kanala između NB-a države članice i okruženja pristupnika. DCCG ima TLS certifikat poslužitelja, skraćeno $DCCG_{TLS}$, a NB TLS certifikat klijenta, skraćeno NB_{TLS}. Predlošci certifikata nalaze se u *odjeljku 5*. Svaki NB može dati vlastiti TLS certifikat. Taj certifikat bit će izričito naveden kao prihvatljiv pa ga može izdati certifikacijsko tijelo od javnog povjerenja (npr. certifikacijsko tijelo koje ispunjava osnovne zahtjeve konzorcija CA Browser Forum) ili nacionalno certifikacijsko tijelo, a može biti i samopotpisan. Svaka država članica odgovorna je za svoje nacionalne podatke i za zaštitu privatnog ključa kojim uspostavlja vezu s DCCG-om. Pristup „ponesi svoj certifikat" zahtijeva precizno definirane postupke registracije i identifikacije te povlačenja i obnavljanja, kako je opisano u *odjeljcima 4.1.*, *4.2.* i *4.3*. DCCG koristi popis dopuštenih certifikata na koji se nakon uspješne registracije dodaju TLS certifikati NB-ova. Samo NB-ovi koji se autentificiraju privatnim ključem koji odgovara certifikatu s popisa dopuštenih certifikata mogu uspostaviti sigurnu vezu s DCCG-om. DCCG će također upotrebljavati TLS certifikat kojim će NB-ovi moći provjeriti da stvarno uspostavljaju vezu s „pravim" DCCG-om, a ne sa zlonamjernim subjektom koji se predstavlja kao DCCG. NB-ovi će dobiti certifikat DCCG-a nakon uspješne registracije. $DCCG_{TLS}$ izdaje CA od javnog povjerenja (takvi CA-ovi su prisutni u svim najvažnijim preglednicima). Države članice dužne su provjeriti da je njihova veza s DCCG-om sigurna (npr. uspoređivanjem kontrolnog otiska (*fingerprint*) certifikata $DCCG_{TLS}$ poslužitelja na koji su spojeni s onim koji su dobile nakon registracije).

3.2. *Krovna nacionalna certifikacijska tijela za potpisivanje certifikata i model provjere*

Države članice koje sudjeluju u okviru DCCG-a moraju koristiti CSCA za izdavanje DSC-ova. Države članice mogu imati više CSCA-ova, npr. ako prenose obveze na regionalnu razinu. Svaka država članica može ili koristiti postojeća certifikacijska tijela ili uspostaviti namjensko (moguće i samopotpisano) certifikacijsko tijelo za sustav za DCC.

Države članice moraju pokazati certifikate svojih CSCA-ova operateru DCCG-a tijekom službenog postupka početnog priključivanja. Nakon uspješne registracije države članice (*vidjeti odjeljak 4.1. za više informacija*) operater DCCG-a ažurira potpisani popis povjerenja koji sadržava sve certifikate CSCA-ova koji su aktivni u okviru za DCC. Operater DCCG-a potpisuje popis povjerenja i certifikate namjenskim asimetričnim parom ključeva u okruženju koje nije priključeno na mrežu. Privatni ključ ne smije biti pohranjen u sustavu DCCG-a priključenom na mrežu zato da kompromitiranje sustava priključenog na mrežu ne omogući napadaču da kompromitira popis povjerenja. Tijekom postupka priključivanja NB-ovi će dobiti odgovarajući certifikat temelj povjerenja $DCCG_{TA}$.

Države članice mogu s DCCG-a preuzeti popis povjerenja za svoje postupke provjere. CSCA je definiran kao certifikacijsko tijelo koje izdaje DSC-ove pa države članice koje imaju višestupanjsku hijerarhiju certifikacijskih tijela (npr. vršno certifikacijsko tijelo -> CSCA -> DSC-ovi) moraju prijaviti podređeno certifikacijsko tijelo koje izdaje DSC-ove. U tom slučaju, ako država članica koristi postojeće certifikacijsko tijelo, sustav za DCC će zanemariti sve iznad razine CSCA-a i na dopušteni popis staviti samo CSCA kao temelj povjerenja (iako je riječ o podređenom certifikacijskom tijelu). To je zato što ICAO-ov model dopušta točno dvije razine – vršni CSCA i podređeni DCS koji je potpisao taj CSCA.

Ako država članica vodi vlastiti CSCA, njezina je odgovornost da to certifikacijsko tijelo radi i upravlja ključevima na siguran način. Budući da je CSCA temelj povjerenja za DSC-ove, zaštita privatnog ključa CSCA-a je ključna za cjelovitost okruženja za DCC. Model provjere u infrastrukturi javnih ključeva za DCC je tzv. model školjke u kojem svi certifikati u provjeri lanca certifikata moraju biti valjani u tom trenutku (tj. u trenutku provjere potpisa). To znači da postoje sljedeća ograničenja:

— CSCA ne smije izdavati certifikate koji istječu nakon certifikata samog certifikacijskog tijela,

— potpisnik dokumenta ne smije potpisati dokumente koji istječu nakon samog DSC-a,

— države članice koje vode vlastite CSCA-ove moraju definirati razdoblja valjanosti za svoje CSCA-ove i sve izdane certifikate te se pobrinuti za obnavljanje certifikata.

Odjeljak 4.2. sadržava preporuke za razdoblja valjanosti.

3.3. *Cjelovitost i vjerodostojnost poslanih podataka*

Nakon uspješne uzajamne autentifikacije NB-ovi mogu slati digitalno potpisane podatkovne pakete DCCG-u i preuzimati takve pakete od njega. U početku ti podatkovni paketi sadržavaju DSC-ove država članica. Par ključeva kojim NB digitalno potpisuje podatkovne pakete poslane u sustav DCCG-a zove se par ključeva nacionalnog *backend* sustava za slanje, a odgovarajući certifikat javnog ključa skraćen je kao certifikat NB_{UP}. Svaka država članica ima vlastiti certifikat NB_{UP}, koji može biti samopotpisan ili izdan od postojećeg certifikacijskog tijela (npr. certifikacijskog tijela koje izdaje certifikate u skladu s osnovnim zahtjevima konzorcija CAB-Forum). Certifikat NB_{UP} mora se razlikovati od svih drugih certifikata koje država članica koristi (tj. od certifikata CSCA-a, TLS certifikata klijenta ili DSC-ova).

U postupku početne registracije (*vidjeti odjeljak 4.1. za više informacija*) države članice moraju operateru DCCG-a dostaviti certifikat za slanje. Svaka država članica odgovorna je za svoje nacionalne podatke i za zaštitu privatnog ključa kojim potpisuje poslane podatke.

Druge države članice mogu provjeriti potpisane podatkovne pakete certifikatima za slanje koje je dao DCCG. DCCG provjerava vjerodostojnost i cjelovitost poslanih podataka certifikatom NB-a za slanje prije nego što ih stavi na raspolaganje drugim državama članicama.

3.4. *Zahtjevi za tehničku arhitekturu DCCG-a*

Zahtjevi za tehničku arhitekturu DCCG-a su:

— DCCG koristi TLS s uzajamnom autentifikacijom za uspostavljanje autentificiranog šifriranog kanala s NB-ovima. DCCG zbog toga vodi dopušteni popis registriranih klijentskih certifikata NB_{TLS},

— DCCG koristi dva digitalna certifikata ($DCCG_{TLS}$ i $DCCG_{TA}$) s dva različita para ključeva. Privatni ključ para ključeva $DCCG_{TA}$ čuva se izvan mrežnog okruženja (tj. nije na komponenti DCCG-a koja je povezana s mrežom),

— DCCG vodi popis povjerenja s certifikatima NB_{CSCA} koji je potpisan privatnim ključem $DCCG_{TA}$,

— korištene šifre moraju ispunjavati zahtjeve iz *odjeljka 5.1*.

4. **Upravljanje životnim vijekom certifikata**

4.1. *Registracija nacionalnih backend sustava*

Da bi se priključile u sustav DCCG-a, države članice moraju se registrirati kod operatera DCCG-a. U ovom je odjeljku opisan tehnički i operativni postupak za registraciju nacionalnog *backend* sustava.

Da bi proveli postupak priključivanja, operater DCCG-a i država članica moraju razmijeniti podatke za kontakt osoba za tehnička pitanja. Pretpostavlja se da su države članice ovlastile svoje osobe za tehnička pitanja i da se identifikacija/autentifikacija provodi drugim kanalima. Na primjer, autentifikacija se može obaviti tako što osoba za tehnička pitanja države članice e-poštom pošalje šifrirane datoteke s certifikatima pa telefonski javi odgovarajuću lozinku operateru DCCG-a. Mogu se upotrebljavati i drugi sigurni kanali koje odredi operater DCCG-a.

U registracijskom i identifikacijskom postupku država članica mora dostaviti tri certifikata:

— TLS certifikat države članice, NB_{TLS},

— certifikat države članice za slanje, NB_{UP},

— certifikate CSCA-ova države članice, NB_{CSCA}.

Svi dostavljeni certifikati moraju ispunjavati zahtjeve iz *odjeljka 5*. Operater DCCG-a provjerava da dostavljeni certifikati ispunjavaju zahtjeve iz *odjeljka 5*. Nakon identifikacije i registracije operater DCCG-a:

— dodaje certifikate NB_{CSCA} na popis povjerenja potpisan privatnim ključem koji odgovara javnom ključu $DCCG_{TA}$,

— dodaje certifikat NB_{TLS} na dopušteni popis DCCG-ove krajnje točke TLS-a,

— dodaje certifikat NB_{UP} u sustav DCCG-a,

— dostavlja certifikate javnih ključeva $DCCG_{TA}$ i $DCCG_{TLS}$ državi članici.

4.2. *Certifikacijska tijela, razdoblja valjanosti i obnavljanje*

Ako država članica želi voditi vlastiti CSCA, certifikati CSCA-a mogu biti samopotpisani. Ti certifikati su temelj povjerenja države članice pa država članica stoga mora snažno štititi privatni ključ koji odgovara javnom ključu certifikata CSCA-a. Preporučeno je da država članica za svoj CSCA koristi sustav izvan mrežnog okruženja, tj. računalni sustav koji nije priključen ni na kakvu mrežu. Pristup sustavu mora kontrolirati više osoba (npr. primjena načela četiri oka). Nakon potpisivanja DSC-ova primjenjuju se operativne kontrole pa se sustav s privatnim ključem CSCA-a sigurno pohranjuje uz stroge kontrole pristupa. Za dodatnu zaštitu privatnog ključa CSCA-a mogu se upotrebljavati hardverski sigurnosni moduli ili pametne kartice. Digitalni certifikati imaju razdoblje valjanosti zbog kojih je nužno obnavljanje certifikata. Obnavljanje je potrebno radi korištenja svježih kriptografskih ključeva i prilagođavanja duljina ključeva kad dođe do poboljšanja u računalstvu ili ako neki novi napad ugrozi sigurnost korištenog kriptografskog algoritma. Primjenjuje se model oklopa (vidjeti *odjeljak 3.2.*).

Preporučena su sljedeća razdoblja valjanosti, s obzirom na jednogodišnju valjanost digitalnih COVID potvrda:

— CSCA: 4 godine

— DSC: 2 godine

— certifikat za slanje: 1-2 godine

— autentifikacijski TLS certifikat klijenta: 1-2 godine

Preporučena su sljedeća razdoblja upotrebe radi pravodobnog obnavljanja:

— CSCA: 1 godina

— DSC: 6 mjeseci

Da bi zajamčile neprekidan rad, države članice moraju pravodobno generirati nove certifikate za slanje i TLS certifikate, npr. mjesec dana prije isteka. Certifikate CSCA-ova i DSC-ove trebalo bi obnavljati barem mjesec dana prije isteka upotrebe privatnog ključa (zbog potrebnih operativnih postupaka). Države članice moraju operateru DCCG-a dostaviti ažurirane certifikate CSCA-ova, certifikate za slanje i TLS certifikate. Istekli certifikati brišu se s popisa dopuštenih certifikata i popisa povjerenja.

Države članice i operater DCCG-a moraju pratiti valjanost vlastitih certifikata. Ne postoji središnji subjekt koji bi pratio valjanost certifikata pa obavještavao sudionike o isteku.

4.3. *Povlačenje certifikata*

Certifikacijsko tijelo izdavatelj u pravilu može povlačiti digitalne certifikate pomoću popisa povučenih certifikata ili responderima internetskog protokola za utvrđivanje statusa certifikata (OCSP). CSCA-ovi bi za potrebe sustava za DCC trebali dostavljati popise povučenih certifikata (CRL-ovi). Ako druge države članice trenutačno i ne koriste te CRL-ove, CRL-ovi bi trebali biti dio sustava zbog budućih primjena. Ako CSCA odluči ne dostavljati CRL-ove, DSC-ovi tog CSCA-a moraju se obnoviti kad CRL-ovi postanu obvezni. Vršitelji provjera ne bi trebali provjeravati DSC-ove OCSP-om nego na temelju CRL-ova. Preporučeno je da nacionalni *backend* sustav provede potrebne provjere DSC-ova preuzetih s pristupnika za DCC pa da nacionalnim vršiteljima provjere DCC-a proslijedi samo skup pouzdanih i provjerenih DSC-ova. Vršitelji provjera DCC-ova ne bi u svojim provjerama trebali provjeravati jesu li DSC-ovi povučeni. Među razlozima za to je zaštita privatnosti nositelja DCC-a izbjegavanjem svake mogućnosti da se određeni DSC možda prati odgovarajućim OCSP responderom.

Države članice mogu samostalno ukloniti svoje DSC-ove s DCCG-a valjanim certifikatima za slanje i TLS certifikatima. Uklanjanje DSC-a znači da svi DCC-ovi izdani tim DSC-om prestaju važiti kad države članice preuzmu ažurirane popise DSC-ova. Zaštita materijala privatnih ključeva koji odgovaraju DSC-ovima je od ključne važnosti. Države članice dužne su obavijestiti operatera DCCG-a ako moraju povući certifikate za slanje ili TLS certifikate, npr. zbog kompromitiranog nacionalnog *backend* sustava. Operater DCCG-a tad može povući povjerenje zahvaćenom certifikatu, npr. tako da ga ukloni s popisa dopuštenih TLS certifikata. Operater DCCG-a može ukloniti certifikate za slanje iz baze podataka DCCG-a. Paketi potpisani privatnim ključem koji odgovara tom certifikatu za slanje prestat će važiti kad nacionalni *backend* prestane imati povjerenje u povučeni certifikat za slanje. Ako se mora povući certifikat CSCA-a, države članice obavješćuju operatera DCCG-a i države članice s kojima su uspostavile odnos povjerenja. Operater DCCG-a izdat će novi popis povjerenja na kojem više nema zahvaćenog certifikata. Svi DSC-ovi koje je taj CSCA izdao prestaju važiti kad države članice ažuriraju svoju arhivu povjerenja u nacionalnom *backend* sustavu. Ako se mora povući certifikat $DCCG_{TLS}$ ili $DCCG_{TA}$, operater DCCG-a i države članice moraju zajednički uspostaviti novu pouzdanu TLS vezu i novi popis povjerenja.

5. **Predlošci certifikata**

U ovom se odjeljku utvrđuju kriptografski zahtjevi i smjernice te zahtjevi za predloške certifikata. U ovom se odjeljku utvrđuju predlošci certifikata DCCG-a.

5.1. *Kriptografski zahtjevi*

Kriptografski algoritmi i skupovi šifri TLS-a odabiru se na temelju trenutačne preporuke njemačkog Saveznog ureda za informatičku sigurnost (BSI) ili SOG-IS-a. Te preporuke su slične preporukama drugih institucija i normizacijskih organizacija. Preporuke su dostupne u tehničkim smjernicama TR 02102-1 i TR 02102-2 ([1]) ili SOG-IS-ovom dokumentu Agreed Cryptographic Mechanisms ([2]).

5.1.1. Zahtjevi za DSC

Primjenjuju se zahtjevi iz *odjeljka 3.2.2. Priloga I.* Stoga je veoma preporučeno da potpisnici dokumenata koriste algoritam za digitalno potpisivanje na temelju eliptičkih krivulja (ECDSA) s NIST-p-256 (kako je definiran u Dodatku D norme FIPS PUB 186-4). Nisu podržane druge eliptičke krivulje. Zbog ograničenja prostora na DCC-u

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

države članice ne bi trebale koristiti RSA-PSS, iako je dopušten kao pričuvni algoritam. Ako države članice koriste RSA-PSS, veličina modula bi trebala biti 2048 bita ili najviše 3072 bita. Kriptografska hash funkcija (vidjeti ISO/IEC 10118-3:2004) za potpis DSC-A je SHA-2 s izlaznom duljinom ≥ 256 bita.

5.1.2. Zahtjevi za TLS certifikate, certifikate za slanje i certifikate CSCA-ova

Za digitalne certifikate i kriptografske potpise u kontekstu DCCG-a pregled glavnih zahtjeva naveden je u sljedećoj tablici (od 2021.):

Potpisni algoritam	Duljina ključa	Hash funkcija
EC-DSA	najmanje 250 bita	SHA-2 s izlaznom duljinom ≥ 256 bita
RSA-PSS (preporučeno dopunjavanje) RSA-PKCS#1 v1.5 (prijašnje dopunjavanje)	najmanje 3000 bitni RSA modul (N) s javnim eksponentom e > 2^16	SHA-2 s izlaznom duljinom ≥ 256 bita
DSA	najmanje 3000 bitni primarni broj p, 250 bitni ključ q	SHA-2 s izlaznom duljinom ≥ 256 bita

Preporučena eliptička krivulja za EC-DSA je NIST-p-256 jer je njezina primjena veoma raširena.

5.2. *Certifikat CSCA-a (NB_{CSCA})*

U sljedećoj su tablici smjernice za predložak certifikata NB_{CSCA} ako država članica odluči voditi vlastiti CSCA za sustav za DCC.

Ako je unos **podebljan**, obvezan je (mora biti u certifikatu), ako je u *kurzivu*, preporučen je (trebao bi biti u certifikatu). Ako polja nema, nema definiranih preporuka.

Polje	Vrijednost
Subject	**cn=<ne smije biti prazan, mora biti jedinstveno zajedničko ime>,** *o=<pružatelj>,* **c=<država članica koja vodi CSCA>**
Key usage	**potpisivanje certifikata,** *potpisivanje CRL-a* (minimalno)
Basic Constraints	**CA = true, path length constraints = 0**

Ime subjekta ne smije biti prazno i mora biti jedinstveno u navedenoj državi članici. Oznaka zemlje (c) mora odgovarati državi članici koja će koristiti taj certifikat CSCA-a. Certifikat mora sadržavati jedinstveni identifikator ključa subjekta (SKI) u skladu s RFC-om 5280 ([3]).

5.3. *Potpisni certifikat za dokumente (DSC)*

U sljedećoj su tablici smjernice za DSC. Ako je unos **podebljan**, obvezan je (mora biti u certifikatu), ako je u *kurzivu*, preporučen je (trebao bi biti u certifikatu). Ako polja nema, nema definiranih preporuka.

Polje	Vrijednost
Serial Number	**jedinstveni serijski broj**
Subject	**cn=<ne smije biti prazan, mora biti jedinstveno zajedničko ime>,** *o=<pružatelj>,* **c=<država članica koja koristi ovaj DSC>**
Key Usage	**digitalni potpis** (minimalno)

([3]) rfc5280 (ietf.org)

DSC mora biti potpisan privatnim ključem koji odgovara certifikatu CSCA-a koji koristi država članica.

Treba koristiti sljedeća proširenja:

— certifikat mora sadržavati identifikator ključa tijela (AKI) koji odgovara identifikatoru ključa subjekta (SKI) certifikata CSCA-a izdavatelja,

— certifikat treba sadržavati jedinstveni identifikator ključa subjekta (SKI) u skladu s RFC-om 5280 ([4]).

Certifikat bi uz to trebao sadržavati proširenje za distribucijsku točku CRL-a koja pokazuje popis povučenih certifikata (CRL) koji je dostavio CSCA koji je izdao DSC.

DSC može sadržavati proširenje proširene upotrebe ključa s identifikatorima pravila za proširenu upotrebu ključa koja ograničavaju vrste HCERT-ova koji se smiju provjeriti ovim certifikatom; to proširenje ne mora imati nijedan takav identifikator. Ako je neki identifikator prisutan, vršitelji provjere provjeravaju upotrebu ključa s obzirom na pohranjeni HCERT. U tu svrhu su definirane sljedeće vrijednosti extendedKeyUsage:

Polje	Vrijednost
extendedKeyUsage	1.3.6.1.4.1.1847.2021.1.1 za izdavatelje potvrda o testiranju
extendedKeyUsage	1.3.6.1.4.1.1847.2021.1.2 za izdavatelje potvrda o cijepljenju
extendedKeyUsage	1.3.6.1.4.1.1847.2021.1.3 za izdavatelje potvrda o preboljenju

Ako nema nijednog proširenja upotrebe ključa (tj. proširenja nema ili je proširenje nulto), na temelju ovog certifikata može se provjeriti valjanost svake vrste HCERT-a. Moguće je da se u drugim dokumentima definiraju dodatni identifikatori pravila za proširenu upotrebu ključa koji se koriste za provjeru HCERT-ova.

5.4. *Certifikati za slanje (NBUP)*

U sljedećoj su tablici smjernice za certifikate za slanje nacionalnih *backend* sustava. Ako je unos **podebljan**, obvezan je (mora biti u certifikatu), ako je u *kurzivu*, preporučen je (trebao bi biti u certifikatu). Ako polja nema, nema definiranih preporuka.

Polje	Vrijednost
Subject	**cn=<ne smije biti prazan, mora biti jedinstveno zajedničko ime>,** *o=<pružatelj>,* **c=<država članica koja koristi ovaj certifikat za slanje>**
Key Usage	**digitalni potpis** (minimalno)

5.5. *Autentifikacijski TLS certifikat klijenta nacionalnog backend sustava (NB_{TLS})*

U sljedećoj su tablici smjernice za autentifikacijski TLS certifikat klijenta nacionalnih *backend* sustava. Ako je unos **podebljan**, obvezan je (mora biti u certifikatu), ako je u *kurzivu*, preporučen je (trebao bi biti u certifikatu). Ako polja nema, nema definiranih preporuka.

Polje	Vrijednost
Subject	**cn=<ne smije biti prazan, mora biti jedinstveno zajedničko ime>,** *o=<pružatelj>,* **c=<država članica NB-a>**
Key Usage	**digitalni potpis** (minimalno)
Extended key usage	autentifikacija klijenta (1.3.6.1.5.5.7.3.2)

([4]) rfc5280 (ietf.org)

Certifikat može sadržavati proširenu upotrebu ključa *autentifikacija poslužitelja (1.3.6.1.5.5.7.3.1)*, ali to nije obvezno.

5.6. *Potpisni certifikat popisa povjerenja ($DCCG_{TA}$)*

U sljedećoj je tablici definiran certifikat temelj povjerenja DCCG-a.

Polje	Vrijednost
Subject	**cn = Digital Green Certificate Gateway** ([5]), **o=<pružatelj>, c=<zemlja>**
Key Usage	**digitalni potpis** (minimalno)

5.7. *DCCG-ovi TLS certifikati poslužitelja ($DCCG_{TLS}$)*

U sljedećoj je tablici definiran TLS certifikat DCCG-a.

Polje	Vrijednost
Subject	cn=<FQDN ili IP adresa DCCG-a>, o=<pružatelj>, c=<zemlja>
SubjectAltName	dNSName: <DCCG DNS name> ili iPAddress: <DCCG IP address>
Key Usage	**digitalni potpis** (minimalno)
Extended key usage	autentifikacija poslužitelja (1.3.6.1.5.5.7.3.1)

Certifikat može sadržavati proširenu upotrebu ključa *client authentication (1.3.6.1.5.5.7.3.2.)*, ali to nije obvezno.

TLS certifikat DCCG-a izdaje certifikacijsko tijelo od javnog povjerenja (takav CA je prisutan u svim najvažnijim preglednicima i operativnim sustavima, u skladu s osnovnim zahtjevima konzorcija CA Browser Forum).

([5]) Termin „digitalna zelena potvrda” je zadržana u ovom kontekstu umjesto „EU digitalne COVID potvrde” jer je termin upisan u kod i primijenjen u certifikatu prije nego što su suzakonodavci odlučili o novom terminu.