IZVEDBENI SKLEP KOMISIJE (EU) 2021/1073

z dne 28. junija 2021

o določitvi tehničnih specifikacij in pravil za izvajanje okvira zaupanja za digitalno COVID potrdilo EU, uvedeno z Uredbo (EU) 2021/953 Evropskega parlamenta in Sveta

(Besedilo velja za EGP)

EVROPSKA KOMISIJA JE –

ob upoštevanju Pogodbe o delovanju Evropske unije,

ob upoštevanju Uredbe (EU) 2021/953 Evropskega parlamenta in Sveta o okviru za izdajanje, preverjanje in priznavanje interoperabilnih potrdil o cepljenju, testu in preboleli bolezni v zvezi s COVID-19 (digitalno COVID potrdilo EU) za olajšanje prostega gibanja med pandemijo COVID-19 ([1]) ter zlasti člena 9(1) in (3) Uredbe,

ob upoštevanju naslednjega:

(1) Uredba (EU) 2021/953 določa digitalno COVID potrdilo EU, ki naj bi se uporabljalo kot dokaz, da je bila oseba cepljena proti COVID-19, da je bil njen rezultat testa negativen ali da je prebolela okužbo.

(2) Za delovanje digitalnega COVID potrdila EU po vsej Uniji je treba določiti tehnične specifikacije in pravila za izpolnjevanje, varno izdajanje in preverjanje digitalnih COVID potrdil, zagotavljanje varstva osebnih podatkov, določitev skupne strukture edinstvene identifikacijske oznake potrdila ter izdajo veljavne, varne in interoperabilne črtne kode. Navedeni okvir zaupanja tudi določa osnovna načela prizadevanj za zagotovitev interoperabilnosti z mednarodnimi standardi in tehnološkimi sistemi ter bi lahko bil kot tak zgled za sodelovanje na svetovni ravni.

(3) Za zmožnost branja in razlage digitalnega COVID potrdila EU sta potrebna skupna struktura podatkov ter dogovor o predvidenem pomenu vsakega podatkovnega polja koristne vsebine in njegovih možnih vrednostih. Da bi se olajšala taka interoperabilnost, je treba opredeliti skupno usklajeno podatkovno strukturo za okvir digitalnega COVID potrdila EU. Smernice za ta okvir je razvila mreža e-zdravje, vzpostavljena na podlagi Direktive 2011/24/EU Evropskega parlamenta in Sveta ([2]). Navedene smernice bi bilo treba upoštevati pri oblikovanju tehničnih specifikacij, ki določajo format in upravljanje zaupanja za digitalno COVID potrdilo EU. Določiti bi bilo treba specifikacijo podatkovne strukture in kodirne mehanizme, pa tudi mehanizem za kodiranje prenosa v strojno berljivem optičnem formatu (QR), ki se lahko prikaže na zaslonu mobilne naprave ali natisne na list papirja.

(4) Poleg tehničnih specifikacij za format in upravljanje zaupanja v zvezi z digitalnim COVID potrdilom EU bi bilo treba določiti splošna pravila za izpolnjevanje potrdil, ki bi se uporabljala za kodirane vrednosti v vsebini digitalnega COVID potrdila EU. Komisija bi morala na podlagi ustreznega dela mreže e-zdravje redno posodabljati in objavljati nabore vrednosti, s katerimi se izvajajo navedena pravila.

(5) V skladu z Uredbo (EU) 2021/953 mora biti mogoče verodostojna potrdila, ki sestavljajo digitalno COVID potrdilo EU, posamično prepoznati na podlagi edinstvene identifikacijske oznake potrdila, pri čemer je treba upoštevati, da se lahko državljanom v času veljavnosti Uredbe (EU) 2021/953 izda več kot eno potrdilo. Edinstvena identifikacijska oznaka potrdila mora biti sestavljena iz alfanumeričnega niza, države članice pa bi morale zagotoviti, da ne vsebuje nobenih podatkov, ki bi jo povezovali z drugimi dokumenti ali identifikacijskimi oznakami, na primer s številkami potnih listov ali osebnih izkaznic, da se prepreči možnost identifikacije imetnika. Za zagotovitev, da je identifikacijska oznaka potrdila edinstvena, bi bilo treba določiti tehnične specifikacije in pravila za njeno skupno strukturo.

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

([2]) Direktiva 2011/24/EU Evropskega parlamenta in Sveta z dne 9. marca 2011 o uveljavljanju pravic pacientov pri čezmejnem zdravstvenem varstvu (UL L 88, 4.4.2011, str. 45).

(6) Varnost, verodostojnost, veljavnost in celovitost potrdil, ki sestavljajo digitalno COVID potrdilo EU, ter njihova skladnost z zakonodajo Unije o varstvu podatkov so ključne za njihovo priznavanje v vseh državah članicah. Ti cilji so doseženi z okvirom zaupanja, ki določa pravila in infrastrukturo za zanesljivo in varno izdajanje in preverjanje digitalnih COVID potrdil EU. Med drugim bi moral okvir zaupanja temeljiti na infrastrukturi javnih ključev z verigo zaupanja od zdravstvenih organov držav članic ali drugih zaupanja vrednih organov do posameznih subjektov, ki izdajajo digitalna COVID potrdila EU. Zato je Komisija za zagotovitev vseevropskega sistema interoperabilnosti vzpostavila centralni sistem – prehod za digitalna COVID potrdila EU (v nadaljnjem besedilu: prehod) –, ki shranjuje javne ključe, ki se uporabljajo za preverjanje. Ko se potrdilo s QR kodo prebere s čitalnikom kod, se digitalni podpis preveri z ustreznim javnim ključem, ki je bil prej shranjen na navedenem centralnem prehodu. Digitalni podpisi se lahko uporabljajo za zagotovitev celovitosti in verodostojnosti podatkov. Infrastrukture javnih ključev vzpostavljajo zaupanje, tako da javne ključe povezujejo z izdajatelji potrdil. Na prehodu se za verodostojnost uporablja več potrdil javnih ključev. Za zagotovitev varne izmenjave podatkov za material javnih ključev med državami članicami in omogočanje široke interoperabilnosti je treba določiti potrdila javnih ključev, ki se lahko uporabljajo, in opredeliti, kako bi jih bilo treba generirati.

(7) Ta sklep omogoča tako izvajanje zahtev iz Uredbe (EU) 2021/953, da je obdelava osebnih podatkov zmanjšana na tisto, kar je potrebno za delovanje digitalnega COVID potrdila EU, in prispeva k temu, da končni upravljavci izvajajo zahteve tako, da se že po zasnovi upošteva varstvo podatkov.

(8) V skladu z Uredbo (EU) 2021/953 so javni ali drugi imenovani organi, pristojni za izdajo potrdil, upravljavci iz člena 4(7) Uredbe (EU) 2016/679 Evropskega parlamenta in Sveta ([3]) v svoji vlogi obdelovalcev osebnih podatkov med postopkom izdaje. Glede na to, kako države članice organizirajo postopek izdaje, lahko obstaja eden ali več javnih ali drugih imenovanih organov, na primer regionalne zdravstvene službe. V skladu z načelom subsidiarnosti o tem odločijo države članice. Zato so države članice v najboljšem položaju, da tam, kjer je več javnih ali drugih imenovanih organov, zagotovijo, da so njihove odgovornosti jasno dodeljene, ne glede na to, ali so ločeni ali skupni upravljavci (vključno z regionalnimi zdravstvenimi službami, ki vzpostavijo skupni portal za paciente za izdajo potrdil). Podobno, kar zadeva preverjanje potrdil s strani pristojnih organov ciljne ali tranzitne države članice ali izvajalcev storitev čezmejnega potniškega prevoza, ki morajo med pandemijo COVID-19 v skladu z nacionalno zakonodajo izvajati nekatere javnozdravstvene ukrepe, morajo ti preveritelji izpolnjevati obveznosti v skladu s pravili o varstvu podatkov.

(9) Osebni podatki se prek prehoda za digitalna COVID potrdila EU ne obdelujejo, saj prehod vsebuje samo javne ključe organov overiteljev potrdil. Ti ključi se nanašajo na organe overitelje in ne omogočajo niti neposredne niti posredne ponovne identifikacije fizične osebe, ki ji je bilo izdano potrdilo. Zato Komisija v vlogi upravljavca prehoda ne bi smela biti niti upravljavec niti obdelovalec osebnih podatkov.

(10) V skladu s členom 42(1) Uredbe (EU) 2018/1725 Evropskega parlamenta in Sveta ([4]) je bilo opravljeno posvetovanje z Evropskim nadzornikom za varstvo podatkov, ki je mnenje podal 22. junija 2021.

(11) Ker so za uporabo Uredbe (EU) 2021/953 od 1. julija 2021 potrebne tehnične specifikacije in pravila, je takojšnji začetek uporabe tega sklepa upravičen.

(12) Ker je treba hitro uvesti digitalno COVID potrdilo EU, bi moral ta sklep začeti veljati na dan objave –

([3]) Uredba (EU) 2016/679 Evropskega parlamenta in Sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov ter o razveljavitvi Direktive 95/46/ES (Splošna uredba o varstvu podatkov) (UL L 119, 4.5.2016, str. 1).

([4]) Uredba (EU) 2018/1725 Evropskega parlamenta in Sveta z dne 23. oktobra 2018 o varstvu posameznikov pri obdelavi osebnih podatkov v institucijah, organih, uradih in agencijah Unije in o prostem pretoku takih podatkov ter o razveljavitvi Uredbe (ES) št. 45/2001 in Sklepa št. 1247/2002/ES (UL L 295, 21.11.2018, str. 39).

SPREJELA NASLEDNJI SKLEP:

Člen 1

Tehnične specifikacije za digitalno COVID potrdilo EU, ki določajo generično podatkovno strukturo, kodirne mehanizme in mehanizem za kodiranje prenosa v strojno berljivem optičnem formatu, so določene v Prilogi I.

Člen 2

Pravila za izpolnjevanje potrdil iz člena 3(1) Uredbe (EU) 2021/953 so določena v Prilogi II k temu sklepu.

Člen 3

Zahteve, ki določajo skupno strukturo edinstvene identifikacijske oznake potrdila, so določene v Prilogi III.

Člen 4

Pravila o upravljanju, ki se uporabljajo za potrdila javnih ključev v zvezi s prehodom za digitalna COVID potrdila EU, ki podpira vidike interoperabilnosti okvira zaupanja, so določena v Prilogi IV.

Ta sklep začne veljati na dan objave v *Uradnem listu Evropske unije*.

V Bruslju, 28. junija 2021

Za Komisijo
predsednica
Ursula VON DER LEYEN

PRILOGA I

FORMAT IN UPRAVLJANJE ZAUPANJA

Generična podatkovna struktura, kodirni mehanizmi in mehanizem za kodiranje prenosa v strojno berljivem optičnem formatu (v nadaljnjem besedilu: QR)

1. Uvod

Tehnične specifikacije iz te priloge vsebujejo generično podatkovno strukturo in kodirne mehanizme za digitalno COVID potrdilo EU (v nadaljnjem besedilu: DCC). Določajo tudi mehanizem za kodiranje prenosa v strojno berljivem optičnem formatu (v nadaljnjem besedilu: QR), ki se lahko prikaže na zaslonu mobilne naprave ali natisne. Vsebniški formati elektronskega zdravstvenega potrdila iz teh specifikacij so generični, vendar se v tem okviru uporabljajo kot nosilci za potrdilo DCC.

2. Terminologija

V tej prilogi „izdajatelji“ pomenijo organizacije, ki uporabljajo te specifikacije za izdajanje zdravstvenih potrdil, „preveritelji“ pa pomenijo organizacije, ki zdravstvena potrdila sprejemajo kot dokaz o zdravstvenem stanju. „Udeleženci“ pomenijo izdajatelje in preveritelje. Udeleženci morajo medsebojno uskladiti nekatere vidike iz te priloge, kot sta upravljanje imenskega prostora in razdelitev kriptografskih ključev. Predpostavlja se, da te naloge opravlja stranka, v nadaljnjem besedilu imenovana „sekretariat“.

3. Vsebniški format elektronskega zdravstvenega potrdila

Vsebniški format elektronskega zdravstvenega potrdila (v nadaljnjem besedilu: HCERT) je zasnovan tako, da zagotavlja enoten in standardiziran nosilec za zdravstvena potrdila različnih izdajateljev (v nadaljnjem besedilu: izdajatelji). Cilj teh specifikacij je uskladiti način predstavitve, kodiranja in podpisa teh zdravstvenih potrdil, da bi se olajšala interoperabilnost.

Za zmožnost branja in razlage potrdila DCC, ki ga izda kateri koli izdajatelj, sta potrebna skupna podatkovna struktura ter dogovor o pomenu vsakega podatkovnega polja koristne vsebine. Za olajšanje take interoperabilnosti je z uporabo sheme JSON, ki predstavlja okvir DCC, opredeljena skupna usklajena podatkovna struktura.

3.1. *Struktura koristne vsebine*

Koristna vsebina je strukturirana in kodirana kot CBOR z digitalnim podpisom COSE. To je splošno znano kot „spletni žeton za CBOR“ (CWT), ki je opredeljen v standardu RFC 8392 ([1]). Koristna vsebina, kot je opredeljena v naslednjih oddelkih, se prenese v trditvi hcert.

Preveritelj mora imeti možnost, da preveri celovitost in verodostojnost izvora podatkov koristne vsebine. Za zagotovitev tega mehanizma mora izdajatelj podpisati CWT z asimetrično shemo digitalnega podpisa, kot je opredeljena v specifikaciji COSE (RFC 8152 ([2])).

3.2. *Trditve CWT*

3.2.1. Pregled strukture CWT

Zaščitena glava

— Algoritem za podpis (alg, oznaka 1)

— Identifikacijska oznaka ključa (kid, oznaka 4)

Koristna vsebina

— Izdajatelj (iss, ključ trditve 1, neobvezno, oznaka ISO 3166-1 alfa-2 izdajatelja)

— Izdano ob (iat, ključ trditve 6)

— Čas izteka veljavnosti (exp, ključ trditve 4)

— Zdravstveno potrdilo (hcert, ključ trditve -260)

— Digitalno COVID potrdilo EU v1 (eu_DCC_v1, ključ trditve 1)

Podpis

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

3.2.2. Algoritem za podpis

Parameter algoritma za podpis (alg) kaže, kateri algoritem je uporabljen za ustvarjanje podpisa. Izpolnjevati mora sedanje smernice SOG-IS, kot so povzete v naslednjih odstavkih, ali jih presegati.

Opredeljena sta en primarni in en sekundarni algoritem. Sekundarni algoritem bi se moral uporabljati le, če primarni algoritem ni sprejemljiv v okviru pravil in predpisov, ki veljajo za izdajatelja.

Da bi se zagotovila varnost sistema, morajo vse izvedbe vključevati sekundarni algoritem. Zato se morata izvajati primarni in sekundarni algoritem.

Ravni za primarne in sekundarne algoritme, določene v SOG-IS, so:

— Primarni algoritem: primarni algoritem je algoritem z eliptično krivuljo za digitalni podpis (Elliptic Curve Digital Signature Algorithm – ECDSA), kot je opredeljen v oddelku 2.3 standarda ISO/IEC 14888–3:2006 in ki uporablja parametre P–256, kot so opredeljeni v Dodatku D (D.1.2.3) k standardu FIPS PUB 186–4, v kombinaciji z zgoščevalnim algoritmom SHA–256, kot je opredeljen v oddelku o funkciji 4 standarda ISO/IEC 10118–3:2004.

To ustreza parametru algoritma COSE ES256.

— Sekundarni algoritem: sekundarni algoritem je RSASSA-PSS, kot je opredeljen v (RFC 8230 ([3])), z 2048-bitnim modulom v kombinaciji z zgoščevalnim algoritmom SHA–256, kot je opredeljen v oddelku o funkciji 4 (ISO/IEC 10118–3:2004).

To ustreza parametru algoritma COSE: PS256.

3.2.3. Identifikacijska oznaka ključa

Trditev „Identifikacijska oznaka ključa“ (kid) označuje potrdilo za podpisovalnik dokumenta (DSC), ki vsebuje javni ključ, ki ga preveritelj uporablja za preverjanje pravilnosti digitalnega podpisa. Upravljanje potrdil javnih ključev, vključno z zahtevami za DSC, je opisano v Prilogi IV.

Preveritelji uporabljajo trditev „Identifikacijska oznaka ključa“ (kid) za izbiro ustreznega javnega ključa s seznama ključev, ki se nanašajo izdajatelja iz trditve „Izdajatelj“ (iss). Izdajatelj lahko iz upravnih razlogov in ob izvedbi menjave ključev vzporedno uporablja več ključev. Identifikacijska oznaka ključa ni varnostno kritično polje. Zato se lahko po potrebi umesti tudi v nezaščiteno glavo. Preveritelji morajo sprejeti obe možnosti. Če sta na voljo obe možnosti, je treba uporabiti identifikacijsko oznako ključa v zaščiteni glavi.

Zaradi skrajšanja identifikacijske oznake (zaradi omejitve prostora) obstaja majhna, vendar ne ničelna verjetnost, da bi lahko celoten seznam potrdil DSC, ki jih je sprejel preveritelj, vseboval potrdila DSC s podvojenimi identifikacijskimi oznakami kid. Zato mora preveritelj preveriti vsa potrdila DSC z navedeno identifikacijsko oznako kid.

3.2.4. Izdajatelj

Trditev „Izdajatelj“ (iss) je vrednost v obliki niza, ki lahko vsebuje ISO 3166-1 alfa-2 kodo države subjekta, ki izda zdravstveno potrdilo. To trditev lahko preveritelj uporabi za določitev, kateri nabor potrdil DSC uporabiti za preverjanje. Za identifikacijo te trditve se uporablja ključ trditve 1.

3.2.5. Čas izteka veljavnosti

Trditev „Čas izteka veljavnosti“ (exp) vsebuje časovni žig v formatu NumericDate (številčni datum) s celimi števili (kot je določen v oddelku 2 RFC 8392 ([4])), ki kaže, kako dolgo se ta podpis za koristno vsebino šteje za veljavnega, po izteku tega obdobja veljavnosti pa mora preveritelj koristno vsebino zavrniti kot poteklo. Namen parametra izteka veljavnosti je uvesti omejitev obdobja veljavnosti zdravstvenega potrdila. Za identifikacijo te trditve se uporablja ključ trditve 4.

Čas izteka veljavnosti ne sme presegati obdobja veljavnosti potrdila DSC.

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

3.2.6. Izdano ob

Trditev „Izdano ob“ (iat) vsebuje časovni žig v formatu NumericDate (številčni datum) s celimi števili (kot je določen v oddelku 2 RFC 8392 ([5])), ki kaže čas, ko je bilo zdravstveno potrdilo ustvarjeno.

Čas v polju „Izdano ob“ ne sme biti pred začetkom obdobja veljavnosti potrdila DSC.

Preveritelji lahko uporabljajo dodatne politike za omejitev veljavnosti zdravstvenega potrdila glede na čas izdaje. Za določitev te trditve se uporablja ključ trditve 6.

3.2.7. Trditev „Zdravstveno potrdilo“

Trditev „Zdravstveno potrdilo“ (hcert) je objekt JSON (RFC 7159 ([6])), ki vsebuje informacije o zdravstvenem stanju. V okviru iste trditve je lahko več različnih vrst zdravstvenih potrdil, ena od njih pa je DCC.

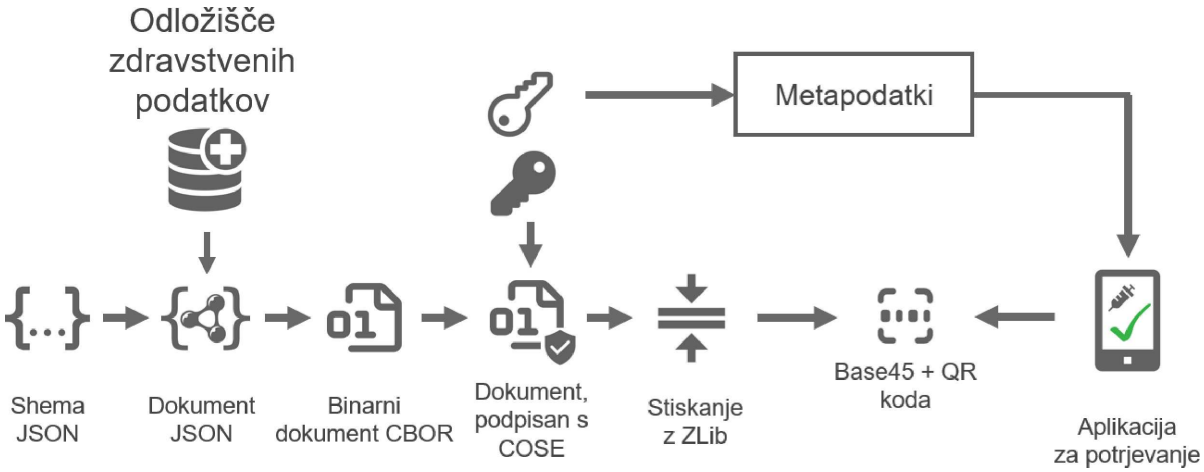
JSON se uporablja zgolj za namene sheme. Kodirni format je CBOR, kot je opredeljen v RFC 7049 ([7]). Razvijalci aplikacij dejansko ne smejo nikoli kodirati v format JSON in dekodirati iz njega, ampak uporabljajo pomnilniško strukturo.

Za določitev te trditve se uporablja ključ trditve -260.

Nize v objektu JSON bi bilo treba normalizirati v skladu z NFC (Normalization Form Canonical Composition), opredeljenim v standardu Unicode. Aplikacije za dekodiranje pa bi morale biti s teh vidikov permisivne in zanesljive, poleg tega se zelo priporoča sprejetje kakršne koli razumne pretvorbe podatkovnega tipa. Če se med dekodiranjem ali v poznejših primerjalnih funkcijah odkrijejo podatki, ki niso normalizirani, bi se morale izvedbe obnašati, kot da so vhodni podatki normalizirani po NFC.

4. **Serializacija in ustvarjanje koristne vsebine potrdila DCC**

Kot vzorec za serializacijo se uporablja naslednja shema:



Postopek se začne s pridobivanjem podatkov, na primer iz odložišča zdravstvenih podatkov (ali zunanjega vira podatkov), pri čemer se pridobljeni podatki strukturirajo v skladu z opredeljenimi shemami DCC. V tem postopku se lahko pretvorba v določen format podatkov in preoblikovanje v berljivost za ljudi izvedeta, preden se začne serializacija v format CBOR. Kratice trditev se v vsakem primeru preslikajo v prikazna imena pred serializacijo in po deserializaciji.

V potrdilih, izdanih v skladu z Uredbo (EU) 2021/953 ([8]), ni dovoljena neobvezna nacionalna vsebina podatkov. Vsebina podatkov je omejena na opredeljene podatkovne elemente v minimalnem naboru podatkov iz Priloge k Uredbi (EU) 2021/953.

([5]) rfc8392 (ietf.org).
([6]) rfc7159 (ietf.org).
([7]) rfc7049 (ietf.org).
([8]) Uredba (EU) 2021/953 Evropskega parlamenta in Sveta z dne 14. junija 2021 o okviru za izdajanje, preverjanje in priznavanje interoperabilnih potrdil o cepljenju, testu in preboleli bolezni v zvezi s COVID-19 (digitalno COVID potrdilo EU) za olajšanje prostega gibanja med pandemijo COVID-19 (UL L 211, 15.6.2021, str. 1).

5. **Kodiranje prenosa**

5.1. *Neobdelano*

Pri poljubnih podatkovnih vmesnikih se lahko vsebnik HCERT in njegove koristne vsebine prenašajo taki, kot so, pri čemer se lahko uporablja kateri koli osnoven, 8-bitni, varen in zanesljiv prenos podatkov. Med temi vmesniki so lahko komunikacija v bližnjem polju (NFC, Near-Field Communication), Bluetooth ali prenos prek protokola aplikacijske plasti, na primer prenos potrdila HCERT od izdajatelja do mobilne naprave imetnika.

Če prenos potrdila HCERT od izdajatelja do imetnika temelji na vmesniku, ki omogoča le predstavitev (npr. SMS, e-pošta), kodiranje prenosa v neobdelani obliki očitno ni ustrezno.

5.2. *Črtna koda*

5.2.1. Stiskanje koristne vsebine (CWT)

Za zmanjšanje velikosti ter izboljšanje hitrosti in zanesljivosti v postopku branja potrdila HCERT se spletni žeton CWT stisne po metodi ZLIB (RFC 1950 ([9])) in z mehanizmom za stiskanje podatkov brez izgub v formatu, opredeljenem v RFC 1951 ([10]).

5.2.2. Dvodimenzionalna črtna koda QR

Za boljše upravljanje obstoječe opreme, zasnovane za obdelavo koristnih vsebin v formatu ASCII, je stisnjeni CWT pred kodiranjem v dvodimenzionalno (2D) črtno kodo kodiran v formatu ASCII z uporabo sheme Base45.

Za generiranje 2D črtnih kod se uporablja format QR, kot je opredeljen v standardu ISO/IEC 18004:2015. Priporočena je stopnja popravljanja napak „Q“ (približno 25 %). Ker se uporablja shema Base45, se mora za kodo QR uporabljati alfanumerično kodiranje (način 2, označen s simboli 0010).

Da bi lahko preveritelji ugotovili vrsto kodiranih podatkov in izbrali ustrezno shemo dekodiranja in obdelave, imajo podatki, kodirani po shemi Base45 (v skladu s to specifikacijo), predpono v obliki niza identifikacijske oznake konteksta „HC1:“. S prihodnjimi različicami te specifikacije, ki bodo vplivale na združljivost za nazaj, bo opredeljena nova identifikacijska oznaka konteksta, medtem ko bo znak, ki sledi „HC“, vzet iz nabora znakov [1–9A–Z]. Vrstni red povečanj je določen v navedenem vrstnem redu, tj. najprej [1–9] in nato [A–Z].

Priporoča se, da se optična koda prikaže na predstavitvenem mediju z velikostjo diagonale 35–60 mm, da se prilagodi čitalnikom s fiksno optiko, pri katerih je treba predstavitveni medij postaviti na površino čitalnika.

Če se optična koda natisne na papir s tiskalniki z nizko ločljivostjo (<300 dpi), je treba paziti, da je vsak simbol (pika) QR kode pravilen kvadrat. Z nesorazmernim spreminjanjem velikosti so simboli v nekaterih vrsticah ali stolpcih QR kode pravokotni, kar v številnih primerih zmanjša berljivost.

6. **Format zanesljivega seznama (seznam CSCA in DSC)**

Vsaka država članica mora predložiti seznam enega ali več državnih organov overiteljev potrdila (Country Signing Certificate Authority – CSCA) in seznam vseh veljavnih potrdil za podpisovalnike dokumentov (Document Signer Certificate – DSC) ter ju redno posodabljati.

6.1. *Poenostavljeni CSCA/DSC*

Od te različice specifikacij države članice ne domnevajo, da se uporabljajo katere koli informacije s seznama preklicanih potrdil (CRL) ali da izvajalci preverjajo obdobje uporabe zasebnega ključa.

Namesto tega je primarni mehanizem veljavnosti prisotnost potrdila na najnovejši različici navedenega seznama potrdil.

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

6.2. *PKI in središča zaupanje za eMRTD organizacije ICAO*

Države članice lahko uporabljajo ločeno potrdilo CSCA, lahko pa tudi predložijo svoja obstoječa potrdila CSCA za strojno berljive elektronske potne listine (eMRTD) in/ali potrdila DSC; lahko se celo odločijo, da bodo ta potrdila kupile od (komercialnih) središč zaupanja, in predložijo taka potrdila. Vendar mora vsako potrdilo DSC vedno podpisati CSCA, ki ga je sporočila zadevna država članica.

7. **Varnostni vidiki**

Pri oblikovanju sheme na podlagi te specifikacije države članice opredelijo, analizirajo in spremljajo nekatere varnostne vidike.

Upoštevati bi bilo treba vsaj naslednje vidike:

7.1. *Obdobje veljavnosti podpisa HCERT*

Izdajatelj potrdil HCERT mora omejiti obdobje veljavnosti podpisa, tako da določi čas izteka veljavnosti podpisa. Zato mora imetnik zdravstvenega potrdila to potrdilo redno podaljševati.

Sprejemljivo obdobje veljavnosti je lahko odvisno od praktičnih omejitev. Potnik med potovanjem v tujino na primer morda ne bo mogel podaljšati zdravstvenega potrdila. Lahko pa se zgodi tudi, da izdajatelj preučuje možnost nekakšne varnostne grožnje, zaradi katere mora umakniti potrdilo DSC (in s tem razveljaviti vsa zdravstvena potrdila, izdana z zadevnim ključem, ki so še vedno veljavna). Posledice takega dogodka se lahko omejijo z rednim menjavanjem ključev izdajatelja in zahtevanjem podaljšanja vseh zdravstvenih potrdil v določenih razumnih časovnih razmikih.

7.2. *Upravljanje ključev*

Ta specifikacija v glavnem temelji na močnih kriptografskih mehanizmih za zagotovitev celovitosti podatkov in avtentikacije izvora podatkov. Zato je treba ohranjati zaupnost zasebnih ključev.

Zaupnost kriptografskih ključev je lahko ogrožena na več različnih načinov, na primer:

— postopek generiranja ključev je lahko pomanjkljiv, posledica pa so šibki ključi;

— ključi so lahko razkriti zaradi človeške napake;

— ključe lahko ukradejo zunanji ali notranji storilci;

— ključi se lahko izračunajo s kriptoanalizo.

Za zmanjšanje tveganja, da bo algoritem za podpis šibek in bo omogočal ogrožanje zasebnih ključev s kriptoanalizo, se s to specifikacijo vsem udeležencem priporoča, naj uvedejo sekundarni algoritem za ponovno pridobitev podpisa, ki temelji na drugačnih parametrih ali drugačnem matematičnem problemu kot primarni.

Kar zadeva navedena tveganja, povezana z operacijskim okoljem izdajateljev, se izvedejo blažilni ukrepi za zagotovitev učinkovitega nadzora, na primer za generiranje, shranjevanje in uporabo zasebnih ključev v varnostnih modulih strojne opreme (Hardware Security Module – HSM). Za podpisovanje zdravstvenih potrdil se zelo spodbuja uporaba varnostnih modulov strojne opreme.

Ne glede na to, ali se izdajatelj odloči za uporabo varnostnih modulov strojne opreme ali ne, bi bilo treba določiti časovni razpored menjave ključev, pri katerem je pogostost menjave ključev sorazmerna z izpostavljenostjo ključev zunanjim omrežjem, drugim sistemom in osebju. Dobro izbran časovni razpored menjave tudi omejuje tveganja, povezana z napačno izdanimi zdravstvenimi potrdili, saj izdajatelju omogoča, da prekliče serije takih zdravstvenih potrdil, tako da po potrebi umakne ključ.

7.3. *Potrjevanje vhodnih podatkov*

Te specifikacije se lahko uporabljajo na način, ki vključuje sprejemanje podatkov iz neverodostojnih virov v sisteme, ki so lahko ključni za izvedbo naloge. Za zmanjšanje tveganj, povezanih s tem napadnim vektorjem, morajo biti vsa vnosna polja ustrezno preverjena glede na vrste podatkov, njihove dolžine in vsebino. Podpis izdajatelja se prav tako preveri pred kakršno koli obdelavo vsebine potrdila HCERT. Vendar potrditev veljavnosti podpisa izdajatelja pomeni, da je treba najprej razčleniti zaščiteno glavo izdajatelja, v katero lahko potencialni napadalec poskuša vnesti skrbno oblikovane informacije, namenjene ogrožanju varnosti sistema.

8. **Upravljanje zaupanja**

Za preverjanje podpisa potrdila HCERT je potreben javni ključ. Države članice dajo te javne ključe na voljo. Na koncu mora imeti vsak preveritelj seznam vseh javnih ključev, ki jim lahko zaupa (ker javni ključ ni del potrdila HCERT).

Sistem je sestavljen iz (samo) dveh slojev; za vsako državo članico eno ali več potrdil na ravni države, vsako od njih pa podpiše eno ali več potrdil za podpisovalnik dokumenta, ki se uporabljajo pri vsakodnevnih dejavnostih.

Potrdila držav članic se imenujejo potrdila državnega organa overitelja potrdila (CSCA) in so (običajno) samopodpisana. Države članice imajo lahko več kot eno tako potrdilo (npr. v primeru regionalne decentralizacije). Ta potrdila CSCA redno podpisujejo potrdila za podpisovalnike dokumentov (DSC), ki se uporabljajo za podpisovanje potrdil HCERT.

„Sekretariat“ ima funkcionalno vlogo. Redno zbira in objavlja potrdila DSC držav članic, potem ko jih preveri na podlagi seznama potrdil CSCA (ki so bila posredovana in preverjena z drugimi sredstvi).

Dobljeni seznam potrdil DSC nato vsebuje združeni nabor sprejemljivih javnih ključev (in ustrezne identifikacijske oznake „kid“), ki jih lahko preveritelji uporabljajo za potrjevanje veljavnosti podpisov v potrdilih HCERT. Preveritelji morajo pridobiti ta seznam in ga redno posodabljati.

Format takih posebnih seznamov za posamezne države članice se lahko prilagodi, da ustreza nacionalnemu okolju. Zato se lahko format datoteke tega zanesljivega seznama razlikuje, in gre lahko na primer za podpisani format JWKS (format niza JWK v skladu z oddelkom 5 RFC 7517 ([11])) ali kateri koli drug format, značilen za tehnologijo, ki se uporablja v zadevni državi članici.

Za zagotovitev enostavnosti lahko države članice predložijo obstoječa potrdila CSCA iz svojih sistemov ICAO eMRTD ali, kot priporoča SZO, ustvarijo potrdilo CSCA posebej za to zdravstveno področje.

8.1. *Identifikacijska oznaka ključa (kid)*

Identifikacijska oznaka ključa (kid) se izračuna ob oblikovanju seznama zaupanja vrednih javnih ključev iz potrdil DSC in je sestavljena iz skrajšanega (prvih 8 bajtov) prstnega odtisa SHA-256 potrdila DSC, kodiranega v formatu DER (neobdelanem).

Preveriteljem ni treba izračunati identifikacijske oznake „kid“ na podlagi potrdila DSC, ampak lahko identifikacijsko oznako ključa v izdanem zdravstvenem potrdilu neposredno povežejo z identifikacijsko oznako „kid“ na zanesljivem seznamu.

8.2. *Razlike glede na model zaupanja PKI za eMRTD organizacije ICAO*

Medtem ko je treba upoštevati dobre prakse v zvezi z modelom zaupanja PKI za eMRTD organizacije ICAO, se zaradi hitrosti uvede več poenostavitev:

— država članica lahko predloži več potrdil CSCA;

— obdobje veljavnosti potrdila DSC (uporaba ključa) je lahko katera koli vrednost, ki ne presega obdobja veljavnosti potrdila CSCA, in lahko sploh ni določeno;

— potrdilo DSC lahko vsebuje identifikacijske oznake politike (uporaba razširjenega ključa), značilne za zdravstvena potrdila;

— države članice se lahko odločijo, da nikoli ne bodo preverjale objavljenih preklicev; namesto tega se lahko zanašajo le na sezname potrdil DSC, ki jih vsak dan dobijo od sekretariata ali jih sestavijo same.

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

PRILOGA II

PRAVILA ZA IZPOLNJEVANJE DIGITALNEGA COVID POTRDILA EU

Splošna pravila glede naborov vrednosti, določenih v tej prilogi, so namenjena zagotavljanju interoperabilnosti na semantični ravni in omogočajo enotne tehnične izvedbe za potrdila DCC. Elementi v tej prilogi se lahko uporabljajo za tri različne primere (cepljenje/testiranje/prebolela bolezen), kot je določeno v Uredbi (EU) 2021/953. V tej prilogi so navedeni samo elementi, pri katerih je potrebna semantična standardizacija prek kodiranih naborov vrednosti.

Za prevajanje kodiranih elementov v nacionalni jezik so odgovorne države članice.

Za vsa podatkovna polja, ki niso navedena v naslednjih opisih naborov vrednosti, je priporočljivo kodiranje UTF-8 (ime, testni center , izdajatelj potrdila). Podatkovna polja s koledarskimi datumi (datum rojstva, datum cepljenja, datum odvzema vzorca za test, datum prvega pozitivnega rezultata testa, datumi veljavnosti potrdila) je priporočljivo kodirati v skladu s standardom ISO 8601.

Če iz kakršnega koli razloga ni mogoče uporabiti spodaj navedenih prednostnih kodnih sistemov, se lahko uporabijo drugi mednarodni kodni sistemi, poleg tega bi bilo treba zagotoviti nasvete, kako kode iz drugega kodnega sistema kod preslikati v prednostni kodni sistem. Besedilo (prikazna imena) se lahko v izjemnih primerih uporabi kot rezervni mehanizem, kadar v opredeljenih naborih vrednosti ni na voljo ustrezna koda.

Države članice, ki v svojih sistemih uporabljajo druge kode, bi morale take kode preslikati v opisane nabore vrednosti. Za vse take preslikave so odgovorne države članice.

Komisija ob podpori mreže e-zdravje in Odbora za zdravstveno varnost redno posodablja nabore vrednosti. Posodobljeni nabori vrednosti se objavijo na ustreznem spletnem mestu Komisije, pa tudi na spletni strani mreže e-zdravje. Zagotoviti bi bilo treba zgodovino sprememb.

1. **Ciljna bolezen ali njen povzročitelj/bolezen ali njen povzročitelj, ki jo/ga je imetnik prebolel: COVID-19 (SARS-CoV-2 ali ena od njegovih različic)**

   Prednostni kodni sistem: SNOMED CT.

   Uporabljati v potrdilih 1, 2 in 3.

   Izbrane kode se nanašajo na COVID-19 ali, če so potrebne podrobnejše informacije o genetski različici SARS-CoV-2, na te različice, če so take podrobne informacije potrebne iz epidemioloških razlogov.

   Primer kode, ki bi jo bilo treba uporabljati, je koda SNOMED CT 840539006 (COVID-19).

2. **Cepivo ali profilaksa proti COVID-19**

   Prednostni sistem kod: SNOMED CT ali klasifikacija ATC.

   Uporabljati v potrdilu 1.

   Primeri kod iz prednostnih kodnih sistemov, ki bi jih bilo treba uporabljati, so kode SNOMED CT 1119305005 (antigensko cepivo proti SARS-CoV-2), 1119349007 (cepivo mRNK proti SARS-CoV-2) ali J07BX03 (cepiva proti COVID-19). Nabor vrednosti bi bilo treba razširiti, ko se razvijejo in začnejo uporabljati nove vrste cepiv.

3. **Zdravilo (cepivo) proti COVID-19**

   Prednostni kodni sistemi (v prednostnem vrstnem redu):

   — register zdravil Unije za cepiva z dovoljenjem, ki velja za celotno EU (številke dovoljenj);

   — svetovni register cepiv, kot bi ga lahko vzpostavila na primer Svetovna zdravstvena organizacija;

   — v drugih primerih ime zdravila (cepiva). Če ime vključuje presledke, jih je treba nadomestiti z vezajem (-).

Ime nabora vrednosti: cepivo.

Uporabljati v potrdilu 1.

Primer kode iz prednostnih kodnih sistemov, ki bi jo bilo treba uporabljati, je EU/1/20/1528 (Comirnaty). Primer imena cepiva, ki bi ga bilo treba uporabljati kot kodo: Sputnik-V (kar pomeni cepivo Sputnik V).

4. **Imetnik dovoljenja za promet s cepivom proti COVID-19 ali izdelovalec cepiva**

Prednostni kodni sistem:

— koda organizacije Evropske agencije za zdravila (sistem SPOR za ISO IDMP);

— svetovni register imetnikov dovoljenj za promet s cepivom ali izdelovalcev cepiv, kot bi ga lahko vzpostavila na primer Svetovna zdravstvena organizacija;

— v drugih primerih ime organizacije. Če ime vključuje presledke, jih je treba nadomestiti z vezajem (-).

Uporabljati v potrdilu 1.

Primer kode iz prednostnega kodnega sistema, ki bi jo bilo treba uporabljati, je ORG-100001699 (AstraZeneca AB). Primer imena organizacije, ki bi ga bilo treba uporabljati kot kodo: Sinovac-Biotech (kar pomeni Sinovac Biotech).

5. **Številka odmerka v seriji in skupno število odmerkov v seriji**

Uporabljati v potrdilu 1.

Dve polji:

(1) število odmerkov, danih v ciklu;

(2) število pričakovanih odmerkov za celoten cikel (specifično za osebo v času dajanja).

Podatek 1/1, 2/2 bo na primer pomenil zaključeno cepljenje; vključno z možnostjo 1/1 za cepiva, pri katerih sta sicer predvidena dva odmerka, vendar zanje država članica uporablja protokol, po katerem državljani, ki jim je bila pred cepljenjem postavljena diagnoza COVID-19, prejmejo samo en odmerek. Skupno število odmerkov v seriji bi moralo biti navedeno glede na informacije, ki so na voljo ob dajanju odmerka. Če je pri določenem cepivu na primer potreben tretji odmerek (poživitveni odmerek) v času zadnjega danega odmerka, naj to odraža številka v drugem polju (na primer 2/3, 3/3 itd.).

6. **Država članica ali tretja država, v kateri je bilo opravljeno cepljenje/testiranje**

Prednostni kodni sistem: oznake držav po ISO 3166.

Uporabljati v potrdilih 1, 2 in 3.

Vsebina nabora vrednosti: popoln seznam dvočrkovnih kod, ki je na voljo kot nabor vrednosti, opredeljen v standardu FHIR (http://hl7.org/fhir/ValueSet/iso3166-1-2).

7. **Vrsta testa**

Prednostni kodni sistem: LOINC.

Uporabljati v potrdilu 2 in potrdilu 3, če se z delegiranim aktom uvede podpora za izdajo potrdil o preboleli bolezni na podlagi vrst testov, ki niso amplifikacijski test nukleinske kisline (NAAT).

Kode v tem naboru vrednosti se nanašajo na metodo testiranja in se izberejo vsaj za ločitev testov NAAT od hitrih antigenskih testov (RAT), kot je izraženo v Uredbi (EU) 2021/953.

Primer kode iz prednostnega kodnega sistema, ki bi jo bilo treba uporabljati, je LP217198-3 (hitri imunotest).

8. **Izdelovalec in trgovsko ime uporabljenega testa (neobvezno za test NAAT)**

Prednostni sistem kod: seznam hitrih antigenskih testov, ki ga je pripravil Odbor za zdravstveno varnost (HSC) in ga vodi Skupno raziskovalno središče (JRC) (podatkovna zbirka *in vitro* diagnostičnih medicinskih pripomočkov in metod testiranja na COVID-19).

Uporabljati v potrdilu 2.

Vsebina nabora vrednosti vključuje izbiro hitrega antigenskega testa, kot je naveden na skupnem in posodobljenem seznamu hitrih antigenskih testov na COVID-19, uvedenem na podlagi Priporočila Sveta 2021/C 24/01 in dogovorjenem z Odborom za zdravstveno varnost. Seznam vodi JRC v okviru podatkovne zbirke *in vitro* diagnostičnih medicinskih pripomočkov in metod testiranja na COVID-19 na spletnem naslovu: https://covid-19-diagnostics.jrc.ec.europa.eu/devices/hsc-common-recognition-rat.

Za ta kodni sistem se uporabljajo ustrezna polja, kot so identifikacijska oznaka naprave za testiranje, ime testa in izdelovalec, v skladu s strukturiranim formatom JRC, ki je na voljo na spletnem naslovu https://covid-19-diagnostics.jrc.ec.europa.eu/devices.

9. **Rezultat testa**

Prednostni sistem kod: SNOMED CT.

Uporabljati v potrdilu 2.

Izbrane kode omogočajo razlikovanje med pozitivnimi in negativnimi rezultati testov (okužba odkrita ali ni odkrita). Dodajo se lahko dodatne vrednosti (kot je „nedoločeno“), če to zahtevajo primeri uporabe.

Primera kod iz prednostnega kodnega sistema, ki bi ju bilo treba uporabljati, sta kodi 260415000 (Okužba ni odkrita) in 260373001 (Okužba odkrita).

PRILOGA III

SKUPNA STRUKTURA EDINSTVENE IDENTIFIKACIJSKE OZNAKE POTRDILA

1. **Uvod**

Vsako digitalno COVID potrdilo EU (DCC) vključuje edinstveno identifikacijsko oznako potrdila (UCI), ki podpira interoperabilnost potrdil DCC. UCI se lahko uporablja za preverjanje potrdila. Za uvedbo UCI so odgovorne države članice. UCI je sredstvo za preverjanje verodostojnosti potrdila in za povezavo s sistemom za registracijo (npr. IIS), kjer je to ustrezno. Te identifikacijske oznake omogočajo tudi navedbe držav članic (na papirju in v digitalni obliki), da so bili posamezniki cepljeni ali testirani.

2. **Sestava edinstvene identifikacijske oznake potrdila**

UCI ima skupno strukturo in format, ki lajšata interpretabilnost za človeka in/ali stroj, ter se lahko nanaša na elemente, kot so država članica cepljenja, samo cepivo in posebna identifikacijska oznaka države članice. Državam članicam zagotavlja prožnost pri njenem oblikovanju ob popolnem spoštovanju zakonodaje o varstvu podatkov. Vrstni red ločenih elementov sledi opredeljeni hierarhiji, ki omogoča prihodnje spremembe gradnikov, hkrati pa ohranja strukturno celovitost.

Možne rešitve za sestavo UCI tvorijo spekter, pri katerem sta modularnost in interpretabilnost za ljudi glavna parametra diverzifikacije in temeljna značilnost:

— modularnost: v kakšnem obsegu je koda sestavljena iz različnih gradnikov, ki vsebujejo semantično različne informacije;

— interpretabilnost za ljudi: kako smiselna je koda za človeškega bralca ali v kakšnem obsegu jo lahko človeški bralec razlaga;

— edinstvenost na svetovni ravni; identifikacijska oznaka države ali organa je dobro upravljana, poleg tega se od vsake države (organa) pričakuje, da bo dobro upravljala svoj segment imenskega prostora in da identifikacijskih oznak ne bo nikoli ponovno uporabila ali izdala. Kombinacija teh značilnosti zagotavlja, da je vsaka identifikacijska oznaka edinstvena na svetovni ravni.

3. **Splošne zahteve**

V zvezi z UCI bi morale biti izpolnjene naslednje splošne zahteve:

(1) nabor znakov: dovoljeni so samo alfanumerični znaki (velike črke) US-ASCII (od „A“ do „Z“, od „0“ do „9“) in dodatni posebni znaki za ločitev od RFC3986 ([1]) ([2])„ in sicer {„/“, „#“, „:“};

(2) največja dolžina: oblikovalci bi si morali prizadevati za dolžino od 27 do 30 znakov ([3]);

(3) predpona različice: nanaša se na različico sheme UCI. Predpona različice za to različico dokumenta je „01“; sestavljena je iz dveh števk;

(4) predpona države: oznaka države je določena s standardom ISO 3166-1. Daljše oznake (npr. trije znaki in več (npr. „UNHCR“)) so rezervirane za prihodnjo uporabo;

(5) pripona kode/kontrolna vsota:

5.1 države članice bi morale uporabiti kontrolno vsoto, kadar obstaja verjetnost prenosa, (človeškega) prepisa ali drugih napak(tj. pri uporabi v tiskane oblike);

5.2 kontrolna vsota se ne sme uporabljati za preverjanje veljavnosti potrdila in tehnično ni del identifikacijske oznake, ampak se uporablja za preverjanje celovitosti kode. Ta kontrolna vsota bi morala biti povzetek celotne oznake UCI v formatu za digitalni prenos/prenos po žici v skladu z ISO-7812-1 (LUHN-10) ([4]). Kontrolna vsota je od preostalega dela UCI ločena z znakom „#“.

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

([2]) Polja, kot so „spol“, „številka serije/lota“, „cepilni center“, „identifikacija zdravstvenega delavca“ in „naslednji datum cepljenja“, morda ne bodo potrebna za druge namene, razen za medicinsko uporabo.

([3]) Pri izvedbi s QR kodami bi lahko države članice razmislile o uporabi dodatnega nabora znakov do skupne dolžine 72 znakov (vključno s 27–30 znaki same identifikacijske oznake) za posredovanje drugih informacij. Specifikacije teh informacij opredelijo države članice.

([4]) Luhnov algoritem mod N je razširitev Luhnovega algoritma (znanega tudi kot algoritem mod 10), ki deluje za numerične kode in se uporablja na primer za izračun kontrolne vsote za kreditne kartice. Razširitev algoritmu omogoča delo z zaporedji vrednosti na kateri koli podlagi (v tem primeru črke).

Zagotoviti bi bilo treba združljivost za nazaj: države članice, ki v daljšem časovnem obdobju spremenijo strukturo identifikacijskih oznak (v okviru glavne različice, ki je trenutno v1), morajo zagotoviti, da kateri koli enaki identifikacijski oznaki predstavljata isto potrdilo/navedbo o cepljenju. Povedano drugače, države članice identifikacijskih oznak ne morejo ponovno uporabiti.

4. **Možnosti za edinstvene identifikacijske oznake potrdil za potrdila o cepljenju**

Smernice mreže e-zdravje za preverljiva potrdila o cepljenju in osnovne elemente interoperabilnosti ([5]) določajo različne možnosti, ki so na voljo državam članicam in drugim stranem in ki lahko soobstajajo v različnih državah članicah. Države članice lahko take različne možnosti uporabijo v različnih različicah sheme UCI.

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

PRILOGA IV

UPRAVLJANJE POTRDIL JAVNIH KLJUČEV

1. Uvod

Države članice si ključe za podpis digitalnih COVID potrdil EU (DCC) med sabo varno in na zaupanja vreden način izmenjujejo prek prehoda za digitalno COVID potrdilo EU (DCCG), ki deluje kot centralno odložišče javnih ključev. S prehodom DCCG so države članice pooblaščene za objavo javnih ključev, ki ustrezajo zasebnim ključem, ki jih uporabljajo za podpisovanje digitalnih COVID potrdil. Države članice, ki se zanašajo na prehod DCCG, ga lahko uporabljajo za pravočasno pridobitev posodobljenega materiala javnih ključev. Pozneje se lahko prehod DCCG razširi na izmenjavo zanesljivih dodatnih informacij, ki jih zagotovijo države članice, na primer pravil za potrjevanje potrdil DCC. Model zaupanja okvira potrdil DCC je infrastruktura javnih ključev (Public Key Infrastructure – PKI). Vsaka država članica ohranja enega ali več državnih overiteljev podpisnikov potrdil (Country Signing Certificate Authority – CSCA), katerih potrdila so razmeroma dolgotrajna. Po odločitvi države članice se lahko uporablja isti CSCA, kot se uporablja za strojno berljive potne listine, ali drug CSCA. CSCA izdaja potrdila javnih ključev za nacionalne kratkotrajne podpisovalnike dokumenta (tj. podpisovalnike za potrdila DCC), ki se imenujejo potrdila za podpisovalnike dokumenta (Document Signer Certificate – DSC). CSCA deluje kot sidro zaupanja, tako da lahko države članice, ki se zanašajo nanj, s potrdilom CSCA potrdijo verodostojnost in celovitost redno spreminjajočih se potrdil DSC. Ko so potrjena, lahko države članice ta potrdila (ali samo javne ključe, ki jih vsebujejo) naložijo v svoje aplikacije za potrjevanje potrdil DCC. Poleg potrdil CSCS in DSC se tudi prehod DCCG opira na infrastrukturo javnih ključev, in sicer za avtentikacijo transakcij in podpisovanje podatkov, kot na podlago za avtentikacijo in kot na način zagotavljanja celovitosti komunikacijskih kanalov med državami članicami in prehodom DCCG.

Digitalni podpisi se lahko uporabljajo za doseganje celovitosti in verodostojnosti podatkov. Infrastrukture javnih ključev vzpostavljajo zaupanje, tako da javne ključe povezujejo s preverjenimi identitetami (ali izdajatelji). To je potrebno, da lahko drugi udeleženci preverijo izvor podatkov in identiteto partnerja, s katerim komunicirajo, ter se odločijo glede zaupanja. Na prehodu DCCG se za verodostojnost uporablja več potrdil javnih ključev. Ta priloga določa, katera potrdila javnih ključev se uporabljajo in kako se oblikujejo, da se omogoči široka interoperabilnost med državami članicami. Zagotavlja več podrobnosti o potrebnih potrdilih javnih ključev ter smernice o predlogah potrdil in obdobjih veljavnosti za države članice, ki želijo upravljati svoja potrdila CSCA. Ker je potrdila DCC mogoče preveriti v določenem časovnem obdobju (od izdaje, veljavnost pa poteče po določenem času), je treba opredeliti model preverjanja za vse podpise, ki se uporabljajo na potrdilih javnih ključev in potrdilih DCC.

2. Terminologija

Naslednja preglednica vsebuje kratice in terminologijo, ki se uporabljajo v tej prilogi.

Pojem	Opredelitev
Potrdilo	Ali potrdilo javnega ključa. Potrdilo X.509 v3, ki vsebuje javni ključ subjekta.
CSCA	Državni organ overitelj potrdila (Country Signing Certificate Authority).
DCC	Digitalno COVID potrdilo EU. Podpisan digitalni dokument, ki vsebuje informacije o cepljenju, testu ali preboleli bolezni.
DCCG	Prehod za digitalno COVID potrdilo EU. Ta sistem se uporablja za izmenjavo potrdil DSC med državami članicami.
$DCCG_{TA}$	Potrdilo sidra zaupanja prehoda DCCG. Ustrezni zasebni ključ se uporablja za podpisovanje seznama vseh potrdil CSCA brez spletne povezave.
$DCCG_{TLS}$	Potrdilo strežnika TLS na prehodu DCCG.
DSC	Potrdilo za podpisovalnik dokumenta. Potrdilo javnega ključa organa države članice za podpisovanje dokumentov (npr. sistem, ki lahko podpisuje potrdila DCC). To potrdilo izda CSCA države članice.
EC-DSA	Algoritem z eliptično krivuljo za digitalni podpis. Kriptografski algoritem za podpis, ki temelji na eliptičnih krivuljah.
Država članica	Država članica Evropske unije.

Pojem	Opredelitev
mTLS	Skupni protokol TLS (Transport Layer Security – varnost prenosnega sloja). Protokol TLS z medsebojno avtentikacijo.
NB	Nacionalno zaledje države članice.
NB_{CSCA}	Potrdilo CSCA države članice (lahko je več kot eno).
NB_{TLS}	Potrdilo nacionalnega zaledja za avtentikacijo odjemalca TLS.
NB_{UP}	Potrdilo, ki ga nacionalno zaledje uporablja za podpisovanje podatkovnih paketov, naloženih na prehod DCCG.
PKI	Infrastruktura javnih ključev. Model zaupanja, ki temelji na potrdilih javnih ključev in organih overiteljih potrdila.
RSA	Asimetrični kriptografski algoritem na osnovi faktorizacije celih števil, ki se uporablja za digitalne podpise ali asimetrično šifriranje.

3. **Komunikacijski tokovi in varnostne storitve prehoda DCCG**

Ta oddelek vsebuje pregled komunikacijskih tokov in varnostnih storitev v sistemu DCCG. V njem je opredeljeno tudi, kateri ključi in potrdila se uporabljajo za zaščito komunikacije, naloženih informacij, potrdil DCC in podpisanega zanesljivega seznama, ki vsebuje vsa sprejeta potrdila CSCA. Prehod DCCG deluje kot podatkovno vozlišče, ki omogoča izmenjavo podpisanih podatkovnih paketov za države članice.

Naložene podatkovne pakete zagotavlja „take, kot so“, kar pomeni, da v paketih, ki jih prejme, ne dodaja ali briše potrdil DSC. Nacionalnemu zaledju držav članic se omogoči preverjanje celovitosti in verodostojnosti naloženih podatkov od konca do konca. Poleg tega bodo nacionalna zaledja in prehod DCCG uporabljali medsebojno avtentikacijo TLS za vzpostavitev varne povezave. Uporabljali jih bodo poleg podpisov v izmenjanih podatkih.

3.1. *Avtentikacija in vzpostavitev povezave*

Prehod DCCG uporablja protokol Transport Layer Security (TLS) z medsebojno avtentikacijo za vzpostavitev avtentificiranega šifriranega kanala med nacionalnim zaledjem države članice in okoljem prehoda. Zato ima prehod DCCG potrdilo strežnika TLS, okrajšano $DCCG_{TLS}$, nacionalno zaledje pa potrdilo odjemalca TLS, okrajšano NB_{TLS}. Predloge potrdil so na voljo v *oddelku 5*. Vsako nacionalno zaledje lahko zagotovi lastno potrdilo TLS. To potrdilo bo izrecno uvrščeno na beli seznam in ga bo zato lahko izdal organ overitelj potrdila, ki uživa javno zaupanje (npr. organ overitelj potrdila, ki upošteva osnovne zahteve foruma CA/Browser Forum), ali nacionalni organ overitelj potrdila ali pa je lahko samopodpisano potrdilo. Vsaka država članica je odgovorna za svoje nacionalne podatke in zaščito zasebnega ključa, ki ga uporablja za vzpostavitev povezave s prehodom DCCG. Za pristop „prinesi svoje potrdilo“ so potrebni natančno opredeljen postopek registracije in identifikacije ter postopka preklica in podaljšanja, kot je navedeno v *oddelkih 4.1 4.2* in *4.3*. Prehod DCCG uporablja beli seznam, na katerega se po uspešni registraciji dodajo potrdila TLS nacionalnih zaledij. Samo nacionalna zaledja, avtentificirana z zasebnim ključem, ki ustreza potrdilu z belega seznama, lahko vzpostavijo varno povezavo s prehodom DCCG. Prehod DCCG bo uporabljal tudi potrdilo TLS, ki nacionalnim zaledjem omogoča, da preverijo, ali dejansko vzpostavljajo povezavo s „pravim“ prehodom DCCG in ne s kakšno zlonamerno entiteto, ki se izdaja za prehod DCCG. Potrdilo prehoda DCCG bo nacionalnemu zaledju zagotovljeno po uspešni registraciji. Potrdilo $DCCG_{TLS}$ bo izdal organ overitelj potrdila, ki uživa javno zaupanje (in je vključen v vse glavne brskalnike). Države članice so odgovorne, da preverijo, ali je njihova povezava s prehodom DCCG varna (npr. s primerjanjem prstnega odtisa potrdila $DCCG_{TLS}$ povezanega strežnika s tistim, pridobljenim po registraciji).

3.2. *Državni organi overitelji potrdila in model potrjevanja*

Države članice, ki sodelujejo v okviru prehoda DCCG, morajo za izdajo potrdil DSC uporabljati CSCA. Države članice imajo lahko več kot en organ CSCA, na primer v primeru regionalne decentralizacije. Vsaka država članica lahko uporablja obstoječe organe overitelje potrdila ali pa za sistem potrdil DCC uvede poseben (po možnosti samopodpisan) organ overitelj potrdila.

Države članice morajo med uradnim postopkom vstopanja upravljavcu prehoda DCCG predložiti svoja potrdila CSCA. Po uspešni registraciji države članice (*za več podrobnosti glej oddelek 4.1*) bo upravljavec prehoda DCCG posodobil podpisan zanesljiv seznam, ki vsebuje vsa potrdila CSCA, aktivna v okviru potrdil DCC. Upravljavec prehoda DCCG bo v okolju brez spletne povezave z namenskim asimetričnim parom ključev podpisal zanesljivi seznam in potrdila. Zasebni ključ ne bo shranjen v spletnem sistemu DCCG, tako da ogroženost spletnega sistema napadalcu ne bo omogočila ogrožanja zanesljivega seznama. Ustrezno potrdilo sidra zaupanja $DCCG_{TA}$ bo nacionalnim zaledjem zagotovljeno med postopkom vstopanja.

Države članice lahko za svoje postopke preverjanja s prehoda DCCG pridobijo zanesljivi seznam. CSCA je opredeljen kot organ overitelj potrdila, ki izdaja potrdila DSC, zato morajo države članice, ki uporabljajo večstopenjsko hierarhijo organov overiteljev potrdila (npr. korenski organ overitelj potrdila -> CSCA -> potrdila DSC), zagotoviti podrejeni organ overitelj potrdila, ki izdaja potrdila DSC. V tem primeru, če država članica uporablja obstoječi organ overitelj potrdila, bo sistem potrdil DCC prezrl vse, kar je nad organom CSCA, in na beli seznam uvrstil samo CSCA kot sidro zaupanja (čeprav gre za podrejeni organ overitelj potrdila). Razlog za to je, da model ICAO omogoča le točno dve ravni – „korenski“ organ CSCA in potrdilo DSC končnega subjekta, ki ga podpiše le navedeni CSCA.

Če država članica upravlja svoj organ CSCA, je odgovorna za varno delovanje in upravljanje ključev tega organa overitelja potrdila. CSCA deluje kot sidro zaupanja za potrdila DSC, zato je zaščita zasebnega ključa CSCA bistvena za celovitost okolja potrdil DCC. Model preverjanja v infrastrukturi javnih ključev DCC je model Shell , v skladu s katerim morajo biti vsa potrdila pri potrjevanju poti potrdil veljavna v določenem trenutku (tj. ob potrditvi podpisa). Zato se uporabljajo naslednje omejitve:

— CSCA ne izdaja potrdil, ki so veljavna dlje časa kot samo potrdilo organa overitelja potrdila;

— podpisovalnik dokumenta ne podpisuje dokumentov, ki so veljavni dlje časa kot samo potrdilo DSC;

— države članice, ki upravljajo svoj organ CSCA, morajo določiti obdobja veljavnosti tega CSCA in vseh izdanih potrdil ter poskrbeti za podaljšanje potrdil.

Oddelek4.2 vsebuje priporočila za obdobja veljavnosti.

3.3. *Celovitost in verodostojnost naloženih podatkov*

Nacionalna zaledja lahko prehod DCCG po uspešni medsebojni avtentikaciji uporabljajo za nalaganje in prenos digitalno podpisanih podatkovnih paketov. Na začetku ti podatkovni paketi vsebujejo potrdila DSC držav članic. Par ključev, ki ga nacionalno zaledje uporablja za digitalni podpis naloženih podatkovnih paketov v sistemu DCCG, se imenuje par ključev nacionalnega zaledja za podpis nalaganja, skrajšana oblika imena ustreznega potrdila javnega ključa pa je potrdilo NB_{UP}. Vsaka država članica zagotovi svoje potrdilo NB_{UP}, ki je lahko samopodpisano ali pa ga izda obstoječi organ overitelj potrdila, na primer javni organ overitelj potrdila (tj. organ, ki izda potrdilo v skladu z osnovnimi zahtevami foruma CAB (CA/Browser Forum)). Potrdilo NB_{UP} se razlikuje od vseh drugih potrdil, ki jih uporablja država članica (tj. CSCA, odjemalec TLS ali potrdila DSC).

Države članice morajo med postopkom prve registracije upravljavcu prehoda DCCG zagotoviti potrdilo za nalaganje (*za več podrobnosti glej oddelek 4.1*). Vsaka država članica je odgovorna za svoje nacionalne podatke in mora zaščititi zasebni ključ, ki se uporablja za podpisovanje nalaganja.

Druge države članice lahko podpisane podatkovne pakete preverijo s potrdili za nalaganje, ki jih zagotovi prehod DCCG. Prehod DCCG s potrdilom nacionalnega zaledja za nalaganje preverja verodostojnost in celovitost naloženih podatkov, preden se ti zagotovijo drugim državam članicam.

3.4. *Zahteve glede tehnične arhitekture prehoda DCCG*

Zahteve glede tehnične arhitekture prehoda DCCG so naslednje:

— prehod DCCG uporablja medsebojno avtentikacijo TLS za vzpostavitev avtentificirane šifrirane povezave z nacionalnimi zaledji. Zato vodi beli seznam registriranih odjemalčevih potrdil NB_{TLS};

— prehod DCCG uporablja dve digitalni potrdili ($DCCG_{TLS}$ in $DCCG_{TA}$) z dvema ločenima paroma ključev. Zasebni ključ para ključev $DCCG_{TA}$ se hrani v sistemu brez spletne povezave (ne na spletnih komponentah prehoda DCCG);

— prehod DCCG vodi zanesljivi seznam NB_{CSCA}, ki je podpisan z zasebnim ključem $DCCG_{TA}$;

— uporabljene šifre morajo izpolnjevati zahteve iz *oddelka 5.1*.

4. **Upravljanje življenjskega cikla potrdil**

4.1. *Registracija nacionalnih zaledij*

Države članice se morajo za sodelovanje v sistemu DCCG registrirati pri njegovem upravljavcu. V tem oddelku je opisan tehnični in operativni postopek, ki ga je treba upoštevati za registracijo nacionalnega zaledja.

Upravljavec prehoda DCCG in država članica si morata izmenjati informacije o kontaktnih tehnikih za postopek vstopanja. Predpostavlja se, da so kontaktne tehnike pooblastile države članice in da se identifikacija/avtentikacija izvaja prek drugih kanalov. Avtentikacija se lahko doseže na primer tako, da kontaktni tehnik države članice prek e-pošte predloži potrdila kot datoteke, šifrirane z geslom, ustrezno geslo pa upravljavcu prehoda DCCG sporoči po telefonu. Lahko se uporabljajo tudi drugi varni kanali, ki jih določi upravljavec prehoda DCCG.

Država članica mora med postopkom registracije in identifikacije predložiti tri digitalna potrdila:

— potrdilo TLS države članice NB_{TLS},

— potrdilo NB_{UP} države članice za nalaganje,

— potrdila CSCA države članice NB_{CSCA}.

Vsa predložena potrdila morajo biti v skladu z zahtevami iz *oddelka 5*. Upravljavec prehoda DCCG bo preveril, ali predloženo potrdilo izpolnjuje zahteve iz *oddelka 5*. Po identifikaciji in registraciji upravljavec prehoda DCCG:

— doda potrdila NB_{CSCA} na zanesljivi seznam, podpisan z zasebnim ključem, ki ustreza javnemu ključu $DCCG_{TA}$;

— doda potrdilo NB_{TLS} na beli seznam končne točke TLS na prehodu DCCG ;

— doda potrdilo NB_{UP} v sistem DCCG;

— državi članici zagotovi potrdili javnega ključa $DCCG_{TA}$ in $DCCG_{TLS}$.

4.2. *Organi overitelji potrdila, obdobja veljavnosti in podaljšanje*

Če želi država članica upravljati svoj organ CSCA, so lahko potrdila CSCA samopodpisana. Delujejo kot sidro zaupanja države članice, zato mora država članica močno zaščititi zasebni ključ, ki ustreza javnemu ključu potrdila CSCA. Priporočljivo je, da države članice za svoj CSCA uporabljajo sistem brez spletne povezave, tj. računalniški sistem, ki ni povezan z nobenim omrežjem. Za dostop do sistema se uporablja nadzor več oseb (npr. v skladu z načelom štirih oči). Po podpisu potrdil DSC se uporabi operativni nadzor, sistem, v katerem je zasebni ključ CSCA, pa se varno shrani s strogim nadzorom dostopa. Za dodatno zaščito zasebnega ključa CSCA se lahko uporabijo varnostni moduli strojne opreme ali pametne kartice. Digitalna potrdila vsebujejo obdobje veljavnosti, ki zahteva podaljšanje potrdila. Podaljšanje je potrebno za uporabo svežih kriptografskih ključev in za prilagoditev velikosti ključev, kadar nove izboljšave računanja ali novi napadi ogrožajo varnost uporabljenega kriptografskega algoritma. Uporablja se model Shell (, glej *oddelek 3.2*).

Glede na enoletno veljavnost digitalnih COVID potrdil se priporočajo naslednja obdobja veljavnosti:

— CSCA: 4 leta;

— DSC: 2 leti;

— potrdilo za nalaganje: 1–2 leti;

— avtentikacija odjemalca TLS: 1–2 leti.

Za pravočasno podaljšanje se priporočajo naslednja obdobja uporabe zasebnega ključa:

— CSCA: 1 leto;

— DSC: 6 mesecev.

Države članice morajo pravočasno ustvariti nova potrdila za nalaganje in potrdila TLS, na primer en mesec pred potekom, da se omogoči nemoteno delovanje. Potrdila CSCA in DSC bi bilo treba podaljšati vsaj en mesec pred prenehanjem uporabe zasebnega ključa (ob upoštevanju potrebnih operativnih postopkov). Države članice morajo upravljavcu prehoda DCCG zagotoviti posodobljena potrdila CSCA, potrdila za nalaganje in potrdila TLS. Potekla potrdila se odstranijo z belega seznama in zanesljivega seznama.

Države članice in upravljavec prehoda DCCG morajo spremljati veljavnost svojih potrdil. Ni centralnega subjekta, ki bi vodil evidenco o veljavnosti potrdil in obveščal udeležence.

4.3. *Preklic potrdil*

Digitalna potrdila lahko na splošno prekliče organ overitelj potrdila (CA), ki jih je izdal, pri čemer uporabi sezname preklicanih potrdil ali odzivnik spletnega protokola za status potrdila (Online Certificate Status Protocol – OCSP). Sezname preklicanih potrdil bi morali zagotoviti organi CSCA za sistem potrdil DCC. Tudi če druge države članice trenutno ne uporabljajo teh seznamov preklicanih potrdil, bi jih bilo treba vključiti za prihodnjo uporabo. Če se organ CSCA odloči, da ne bo predložil seznamov preklicanih potrdil, je treba potrdila DSC tega organa CSCA podaljšati, ko seznami preklicanih potrdil postanejo obvezni. Preveritelji za potrditev potrdil DSC ne bi smeli uporabljati odzivnika OCSP, ampak sezname preklicanih potrdil. Priporočljivo je, da nacionalno zaledje izvede potrebno potrditev potrdil DSC, prenesenih s prehoda DCC, in nacionalnim potrjevalcem potrdil DCC posreduje samo nabor zaupanja vrednih in potrjenih potrdil DSC. Potrjevalci potrdil DCC v postopku potrjevanja ne bi smeli preverjati preklicev DSC. Eden od razlogov za to je varovanje zasebnosti imetnikov potrdil DCC, pri čemer se prepreči kakršna koli možnost, da bi lahko odzivnik OCSP, povezan z določenim potrdilom DSC, spremljal uporabo tega potrdila.

Države članice lahko svoja potrdila DSC same odstranijo s prehoda DCCG z veljavnimi potrdili za nalaganje in potrdili TLS. Odstranitev potrdila DSC pomeni, da bodo vsa potrdila DCC, izdana s tem potrdilom DSC, postala neveljavna, ko bodo države članice pridobile posodobljene sezname DSC. Zaščita materiala zasebnih ključev, ki ustreza potrdilom DSC, je ključna. Države članice morajo upravljavca prehoda DCCG obvestiti, ko morajo preklicati potrdila za nalaganje ali potrdila TLS, na primer zaradi ogrožanja nacionalnega zaledja. Nato lahko upravljavec prehoda DCCG prekliče zaupanje za ogroženo potrdilo, na primer tako, da potrdilo odstrani z belega seznama TLS. Potrdila za nalaganje lahko odstrani iz podatkovne zbirke prehoda DCCG. Paketi, podpisani z zasebnim ključem, ki ustreza temu potrdilu za nalaganje, bodo postali neveljavni, ko bodo nacionalna zaledja preklicala zaupanje v zvezi s preklicanim potrdilom za nalaganje. Če je treba preklicati potrdilo CSCA, države članice o tem obvestijo upravljavca prehoda DCCG in druge države članice, s katerimi imajo vzpostavljen odnos zaupanja. Upravljavec prehoda DCCG bo izdal nov zanesljiv seznam, ki ne bo več vseboval ogroženega potrdila. Vsa potrdila DSC, ki jih je izdal ta CSCA, bodo postala neveljavna, ko bodo države članice posodobile shrambo zaupanja vrednih potrdil v okviru svojega nacionalnega zaledja. Če je treba preklicati potrdilo $DCCG_{TLS}$ ali potrdilo $DCCG_{TA}$, morajo upravljavec prehoda DCCG in države članice skupaj vzpostaviti novo zaupanja vredno povezavo TLS in zanesljivi seznam.

5. **Predloge potrdil**

V tem oddelku so določene kriptografske zahteve in smernice ter zahteve glede predlog potrdil. Poleg tega so v njem opredeljene predloge za potrdila DCCG.

5.1. *Kriptografske zahteve*

Kriptografski algoritmi in nabori šifer TLS se izberejo na podlagi trenutnega priporočila nemškega zveznega urada za informacijsko varnost (Bundesamt für Sicherheit in der Informationstechnik – BSI) ali SOG-IS. Ta priporočila in priporočila drugih institucij in organizacij za standardizacijo so podobna. Priporočila so na voljo v tehničnih smernicah TR 02102-1 in TR 02102-2 ([1]) ali dokumentu SOG-IS Agreed Cryptographic Mechanisms ([2]) (Dogovorjeni kriptografski mehanizmi SOG-IS).

5.1.1. Zahteve glede DSC

Uporabljajo se zahteve iz *oddelka 3.2.2 Priloge I*. Zato je zelo priporočljivo, da podpisovalniki dokumentov uporabljajo algoritem z eliptično krivuljo za digitalni podpis (ECDSA) s krivuljo NIST-p-256 (kot je opredeljena v Dodatku D k standardu FIPS PUB 186-4). Druge eliptične krivulje niso podprte. Zaradi prostorskih omejitev DCC države članice ne bi smele uporabljati algoritma RSA-PSS, niti če je dovoljen kot algoritem za ponovno pridobitev.

([1]) BSI – tehnične smernice TR-02102 (bund.de).
([2]) SOG-IS – podporni dokumenti (sogis.eu).

Če države članice uporabljajo algoritem RSA-PSS, bi morale uporabljati velikost modula 2048 bitov ali največ 3072 bitov. Kot kriptografska zgoščevalna funkcija za podpis potrdil DSC se uporablja SHA-2 z izhodno dolžino ≥ 256 bitov (glej standard ISO/IEC 10118-3:2004).

5.1.2. Zahteve glede potrdila TLS, potrdila za nalaganje in potrdila CSCA

Kar zadeva digitalna potrdila in kriptografske podpise v okviru prehoda DCCG, so glavne zahteve glede kriptografskih algoritmov in dolžine ključev povzete v naslednji preglednici (od leta 2021):

Algoritem za podpis	Velikost ključa	Zgoščevalna funkcija
EC-DSA	Najmanj 250 bitov	SHA-2 z izhodno dolžino ≥ 256 bitov
RSA-PSS (priporočeno zapolnjevanje) RSA-PKCS#1 v1.5 (uveljavljeno zapolnjevanje)	Najmanj 3000-bitni modul RSA (N) z javnim eksponentom e > 2^16	SHA-2 z izhodno dolžino ≥ 256 bitov
DSA	Najmanj 3000-bitno praštevilo p, 250-bitni ključ q	SHA-2 z izhodno dolžino ≥ 256 bitov

Priporočena eliptična krivulja za EC-DSA je NIST-p-256 zaradi njene široke uporabe.

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

Naslednja preglednica vsebuje smernice glede predloge potrdila NB_{CSCA}, če se država članica odloči, da bo za sistem potrdil DCC upravljala svoj CSCA.

Vnosi v **krepkem** tisku so obvezni (morajo biti vključeni v potrdilo), vnosi v *ležečem* tisku pa so priporočeni (bi jih bilo treba vključiti). Za polja, ki niso prikazana v preglednici, ni opredeljenih priporočil.

Polje	Vrednost
Imetnik	**cn=<edinstveno splošno ime, ki ni prazno>,***o=<ponudnik>,* ***c*=<država članica, ki upravlja CSCA>**
Uporaba ključa	(vsaj) **podpisovanje potrdil**, *podpisovanje seznama preklicanih potrdil*
Osnovne omejitve	**CA = true, path length constraints = 0**

Ime imetnika mora biti edinstveno v zadevni državi članici in ne sme biti prazno. Oznaka države (c) se mora ujemati z državo članico, ki bo uporabljala to potrdilo CSCA. Potrdilo mora vsebovati edinstveno identifikacijsko oznako imetnikovega ključa (SKI) v skladu z RFC 5280 ([3]).

5.3. *Potrdilo za podpisovalnik dokumenta (DSC)*

Naslednja preglednica vsebuje smernice za potrdilo DSC. Vnosi v **krepkem** tisku so obvezni (morajo biti vključeni v potrdilo), vnosi v *ležečem* tisku pa so priporočeni (bi jih bilo treba vključiti). Za polja, ki niso prikazana v preglednici, ni opredeljenih priporočil.

Polje	Vrednost
Serijska številka	**edinstvena serijska številka**
Imetnik	**cn=<edinstveno splošno ime, ki ni prazno>**, *o=<ponudnik>,* **c=<država članica, ki uporablja to potrdilo DSC>**
Uporaba ključa	(vsaj) **digitalni podpis**

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

Potrdilo DSC mora biti podpisano z zasebnim ključem, ki ustreza potrdilu CSCA, ki ga uporablja država članica.

Uporabljajo se naslednje razširitve:

— Potrdilo mora vsebovati identifikacijsko oznako organovega ključa (Authority Key Identifier – AKI), ki se ujema z identifikacijsko oznako imetnikovega ključa (Subject Key Identifier – SKI) potrdila izdajatelja CSCA.

— Potrdilo bi moralo vsebovati edinstveno identifikacijsko oznako imetnikovega ključa (v skladu z RFC 5280 ([4])).

Poleg tega bi moralo potrdilo vsebovati razširitev razpošiljevalne točke CRL, ki napotuje na seznam preklicanih potrdil (CRL), ki ga zagotovi C SCA, ki je izdal potrdilo DSC.

Potrdilo DSC lahko vsebuje razširitev za uporabo razširjenega ključa z nič ali več identifikacijskimi oznakami politike uporabe ključa, s katerimi je omejena vrsta potrdil HCERT, ki jih lahko preveri to potrdilo. Če je prisotna ena ali več identifikacijskih oznak, preveritelji primerjajo uporabo ključa s shranjenim potrdilom HCERT. V ta namen so opredeljene naslednje vrednosti extendedKeyUsage:

Polje	Vrednost
extendedKeyUsage	1.3.6.1.4.1.1847.2021.1.1 za izdajatelje potrdil o testiranju
extendedKeyUsage	1.3.6.1.4.1.1847.2021.1.2 za izdajatelje potrdil o cepljenju
extendedKeyUsage	1.3.6.1.4.1.1847.2021.1.3 za izdajatelje potrdil o preboleli bolezni

Če ni razširitve za uporabo ključa (tj. ni razširitev ali pa so prisotne nične razširitve), se lahko to potrdilo uporablja za potrditev katere koli vrste potrdila HCERT. V drugih dokumentih so lahko opredeljene ustrezne dodatne identifikacijske oznake politike uporabe razširjenega ključa, ki se uporabljajo pri potrjevanju potrdil HCERT.

5.4. *Potrdila za nalaganje (NBUP)*

Naslednja preglednica vsebuje smernice za potrdilo nacionalnega zaledja za nalaganje. Vnosi v **krepkem** tisku so obvezni (morajo biti vključeni v potrdilo), vnosi v *ležečem* tisku pa so priporočeni (bi jih bilo treba vključiti). Za polja, ki niso prikazana v preglednici, ni opredeljenih priporočil.

Polje	Vrednost
Imetnik	**cn=<edinstveno splošno ime, ki ni prazno>**, *o=<ponudnik>*,**c=<država članica, ki uporablja to potrdilo za nalaganje>**
Uporaba ključa	(vsaj) **digitalni podpis**

5.5. *Avtentikacija odjemalca TLS v nacionalnem zaledju (NB_{TLS})*

Naslednja preglednica vsebuje smernice za potrdilo nacionalnega zaledja za avtentikacijo odjemalca TLS. Vnosi v **krepkem** tisku so obvezni (morajo biti vključeni v potrdilo), vnosi v *ležečem* tisku pa so priporočeni (bi jih bilo treba vključiti). Za polja, ki niso prikazana v preglednici, ni opredeljenih priporočil.

Polje	Vrednost
Imetnik	**cn=<edinstveno splošno ime, ki ni prazno>,** *o=<ponudnik>*,**c=<nacionalno zaledje države članice>**
Uporaba ključa	(vsaj) **digitalni podpis**
Uporaba razširjenega ključa	avtentikacija odjemalca (1.3.6.1.5.5.7.3.2)

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

Potrdilo lahko vsebuje tudi uporabo razširjenega ključa za *avtentikacijo strežnika (1.3.6.1.5.5.7.3.1)*, vendar to ni obvezno.

5.6. *Potrdilo za podpis zanesljivega seznama ($DCCG_{TA}$)*

V naslednji preglednici je opredeljeno potrdilo sidra zaupanja DCCG.

Polje	Vrednost
Imetnik	**cn=prehod za digitalno zeleno potrdilo** ([5]), **o=<ponudnik>, c=<država>**
Uporaba ključa	(vsaj) **digitalni podpis**

5.7. *Potrdila strežnika TLS na prehodu DCCG ($DCCG_{TLS}$)*

V naslednji preglednici je opredeljeno potrdilo TLS na prehodu DCCG.

Polje	Vrednost
Imetnik	cn=<ime FQDN ali naslov IP DCCG>, o=<ponudnik>, c=<država>
SubjectAltName	dnsName: <ime DNS DCCG> ali iPAddress: <naslov IP DCCG>
Uporaba ključa	(vsaj) **digitalni podpis**
Uporaba razširjenega ključa	avtentikacija strežnika (1.3.6.1.5.5.7.3.1)

Potrdilo lahko vsebuje tudi uporabo razširjenega ključa za *avtentikacijo odjemalca (1.3.6.1.5.5.7.3.2)*, vendar to ni obvezno.

Potrdilo TLS na prehodu DCCG izda organ overitelj potrdila, ki uživa javno zaupanje (in je vključen v vse glavne brskalnike in operacijske sisteme v skladu z osnovnimi zahtevami foruma CAB).

([5]) V tem okviru je namesto „digitalno COVID potrdilo EU“ ohranjen izraz „digitalno zeleno potrdilo“, ker je bil ta izraz trdo kodiran in uveden v potrdilo, preden sta se sozakonodajalca odločila za novo terminologijo.