DEĊIŻJONI TA' IMPLIMENTAZZJONI TAL-KUMMISSJONI (UE) 2021/1073

tat-28 ta' Ġunju 2021

li tistabbilixxi speċifikazzjonijiet tekniċi u regoli għall-implimentazzjoni tal-qafas ta' fiduċja għaċ-Ċertifikat COVID Diġitali tal-UE stabbilit bir-Regolament (UE) 2021/953 tal-Parlament Ewropew u tal-Kunsill

(Test b'rilevanza għaż-ŻEE)

IL-KUMMISSJONI EWROPEA,

Wara li kkunsidrat it-Trattat dwar il-Funzjonament tal-Unjoni Ewropea,

Wara li kkunsidrat ir-Regolament (UE) 2021/953 tal-Parlament Ewropew u tal-Kunsill dwar qafas għall-ħruġ, għall-verifika u għall-aċċettazzjoni ta' ċertifikati COVID-19 interoperabbli tat-tilqim, tat-testijiet u tal-fejqan (Ċertifikat COVID Diġitali tal-UE) għall-faċilitazzjoni tal-moviment liberu waqt il-pandemija tal-COVID-19 ([1]), u b'mod partikolari l-Artikolu 9(1) u (3) tiegħu,

Billi:

(1) Ir-Regolament (UE) 2021/953 jistabbilixxi ċ-Ċertifikat COVID Diġitali tal-UE li għandu l-għan iservi ta' prova li persuna tkun irċeviet it-tilqima kontra l-COVID-19, irriżultat negattiv għat-test jew fieqet mill-infezzjoni.

(2) Biex iċ-Ċertifikat COVID Diġitali tal-UE jkun jista' jintuża madwar l-Unjoni, jeħtieġ jiġu stabbiliti speċifikazzjonijiet tekniċi u regoli biex iċ-Ċertifikati tal-COVID Diġitali jimtlew, jinħarġu u jiġu verifikati b'mod sigur, biex tkun żgurata l-protezzjoni tad-*data* personali, biex tiġi stabbilita l-istruttura komuni tal-identifikatur uniku taċ-ċertifikat, u biex jinħareġ barcode validu, sigur u interoperabbli. Dak il-qafas ta' fiduċja jistabbilixxi wkoll il-bażi li tiżgura l-interoperabbiltà mal-istandards internazzjonali u mas-sistemi teknoloġiċi u, għaldaqstant, jista' jipprovdi l-mudell għal kooperazzjoni fil-livell dinji.

(3) Għal qari u interpretazzjoni taċ-Ċertifikat COVID Diġitali tal-UE hemm bżonn struttura tad-*data* u ftehim komuni dwar it-tifsira maħsuba ta' kull entrata tad-*data* fil-payload u l-valuri possibbli tagħha. Biex tiġi ffaċilitata interoperabbiltà bħal din, jeħtieġ tiġi definita struttura tad-*data* kkoordinata komuni għall-qafas taċ-Ċertifikat COVID Diġitali tal-UE. Il-linji gwida għal dan il-qafas ġew żviluppati min-Network tas-servizzi tas-saħħa elettronika stabbilit abbażi tad-Direttiva 2011/24/UE tal-Parlament Ewropew u tal-Kunsill ([2]). Dawk il-linji gwida jenħtieġ jitqiesu biex jiġu stabbiliti l-ispeċifikazzjonijiet tekniċi li jistabbilixxu l-format u l-ġestjoni tal-fiduċja għaċ-Ċertifikat COVID Diġitali tal-UE. Jenħtieġ jiġu speċifikati l-ispeċifikazzjoni tal-istruttura tad-*data* u l-mekkaniżmi tal-ikkowdjar, u mekkaniżmu tal-ikkowdjar tat-trasport b'format ottiku (QR) li jinqara minn u li jista' jintwera fuq l-iskrin ta' apparat mobbli jew jiġi stampat fuq karta.

(4) Apparti l-ispeċifikazzjonijiet tekniċi għall-format u għall-ġestjoni tal-fiduċja taċ-Ċertifikat COVID Diġitali tal-UE, jenħtieġ jiġu stabbiliti regoli ġenerali għall-fini tal-popolazzjoni taċ-ċertifikati biex jintużaw għall-valuri kkodifikati fil-kontenut taċ-Ċertifikat COVID Diġitali tal-UE. Is-settijiet tal-valur li jimplimentaw dawk ir-regoli jenħtieġ jiġu aġġornati regolarment u ppubblikati mill-Kummissjoni, abbażi tal-ħidma rilevanti tan-Network tas-saħħa elettronika.

(5) Skont ir-Regolament (UE) 2021/953, iċ-ċertifikati awtentiċi li jiffurmaw iċ-Ċertifikat COVID Diġitali tal-UE jenħtieġ ikunu identifikabbli individwalment b'identifikatur uniku taċ-ċertifikat, filwaqt li jitqies li ċ-ċittadini jista' jinħarġilhom aktar minn ċertifikat wieħed fiż-żmien meta r-Regolament (UE) 2021/953 ikun fis-seħħ. L-identifikatur uniku taċ-ċertifikat jinkludi string alfanumerika, u l-Istati Membri jenħtieġ jiżguraw li din ma jkun fiha l-ebda *data* li torbtu ma' dokumenti jew identifikaturi oħra, bħal numri tal-passaport jew tal-karta tal-identità, biex id-detentur ma jkunx jista' jiġi identifikat. Biex ikun żgurat li l-identifikatur taċ-ċertifikat hu uniku, jenħtieġ jiġu stabbiliti speċifikazzjonijiet tekniċi u regoli għall-istruttura komuni tiegħu.

([1]) ĠU L 211, 15.6.2021, p. 1.

([2]) Id-Direttiva 2011/24/UE tal-Parlament Ewropew u tal-Kunsill tad-9 ta' Marzu 2011 dwar l-applikazzjoni tad-drittijiet tal-pazjenti fil-qasam tal-kura tas-saħħa transkonfinali (ĠU L 88, 4.4.2011, p. 45).

(6) Is-sigurtà, l-awtentiċità, il-validità u l-integrità taċ-ċertifikati li jinkludu ċ-Ċertifikat COVID Diġitali tal-UE u l-konformità tagħhom mal-leġiżlazzjoni tal-Unjoni dwar il-protezzjoni tad-*data* huma kruċjali għall-aċċettazzjoni tagħhom fl-Istati Membri kollha. Dawk l-objettivi jintlaħqu mill-qafas ta' fiduċja li jistabbilixxi r-regoli dwar u l-infrastruttura għall-ħruġ u l-verifika affidabbli u siguri taċ-ċertifikati COVID Diġitali tal-UE. Fost l-oħrajn, il-qafas ta' fiduċja jenħtieġ ikun ibbażat fuq infrastruttura bi kjavi pubbliċi b'katina ta' fiduċja mill-awtoritajiet tas-saħħa tal-Istati Membri jew minn awtoritajiet fdati oħra lill-entitajiet individwali li joħorġu ċ-ċertifikati COVID Diġitali tal-UE. Għalhekk, biex tiġi żgurata sistema ta' interoperabbiltà madwar l-UE kollha, il-Kummissjoni bniet sistema ċentrali – il-gateway taċ-Ċertifikat COVID Diġitali tal-UE (il-"gateway") – li taħżen il-kjavi pubbliċi użati għall-verifika. Meta ċ-ċertifikat bil-kodiċi QR jiġi skennjat, il-firma diġitali tiġi vverifikata bil-kjavi pubblika rilevanti, li tkun inħażnet qabel f'din il-gateway ċentrali. Il-firem diġitali jistgħu jintużaw biex jiżguraw l-integrità u l-awtentiċità tad-*data*. L-Infrastrutturi tal-Kjavi Pubbliċi jistabbilixxu l-fiduċja billi jorbtu l-kjavi pubbliċi mal-emittenti taċ-ċertifikati. Fil-gateway, jintużaw diversi ċertifikati tal-kjavi pubbliċi għall-awtentiċità. Biex ikun żgurat skambju tad-*data* sigur għal materjal bi kjavi pubblika bejn l-Istati Membri u biex tkun permessa interoperabbiltà wiesgħa, jenħtieġ jiġu stabbiliti ċ-ċertifikati bi kjavi pubblika li jistgħu jintużaw u jipprovdu l-mod kif jenħtieġ jiġu ġġenerati.

(7) Din id-Deċiżjoni tippermetti li r-rekwiżiti tar-Regolament (UE) 2021/953 isiru operazzjonali b'mod li l-ipproċessar tad-*data* personali jkun limitat għal dak li hu meħtieġ biex iċ-Ċertifikat COVID Diġitali tal-UE jsir operazzjonali u jikkontribwixxi għal implimentazzjoni mill-kontrolluri finali li tirrispetta l-protezzjoni tad-*data* mid-disinn.

(8) F'konformità mar-Regolament (UE) 2021/953, l-awtoritajiet jew korpi maħtura oħra responsabbli għall-ħruġ taċ-ċertifikati huma kontrolluri msemmija fl-Artikolu 4(7) tar-Regolament (UE) 2016/679 tal-Parlament Ewropew u tal-Kunsill ([3]) fir-rwol tagħhom li jipproċessaw id-*data* personali waqt il-proċess tal-ħruġ. Skont kif l-Istati Membri jorganizzaw il-proċess tal-ħruġ, jista' jkun hemm awtorità jew korp maħtur wieħed jew aktar, pereżempju servizzi tas-saħħa reġjonali. F'konformità mal-prinċipju tas-sussidjarjetà, dik hi għażla għall-Istati Membri. Għalhekk, l-Istati Membri huma fl-aħjar pożizzjoni biex jiżguraw, meta jkun hemm bosta awtoritajiet jew korpi maħtura oħra, li r-responsabbiltajiet rispettivi tagħhom jiġu allokati b'mod ċar, indipendentement minn jekk humiex kontrolluri separati jew konġunti (inkluż servizzi tas-saħħa reġjonali li jistabbilixxu portal konġunt tal-pazjenti għall-ħruġ taċ-ċertifikati). Bl-istess mod, fir-rigward tal-verifika taċ-ċertifikati mill-awtoritajiet kompetenti tal-Istat Membru tad-destinazzjoni jew tat-tranżitu, jew mill-operaturi tas-servizzi tat-trasport transfruntieri tal-passiġġieri meħtieġa bil-liġi nazzjonali biex jimplimentaw ċerti miżuri tas-saħħa pubblika waqt il-pandemija tal-COVID-19, dawk il-verifikaturi jridu jikkonformaw mal-obbligi tagħhom skont ir-regoli dwar il-protezzjoni tad-*data*.

(9) Ma jsir l-ebda pproċessar tad-*data* personali mill-gateway taċ-Ċertifikat COVID Diġitali tal-UE, għax il-gateway fiha biss il-kjavi pubbliċi tal-awtoritajiet firmatarji. Dawk il-kjavi huma relatati mal-awtoritajiet firmatarji u ma jippermettux l-identifikazzjoni mill-ġdid diretta jew indiretta ta' persuna fiżika li lilha jkun inħareġ ċertifikat. Għaldaqstant, fir-rwol tagħha bħala l-maniġer tal-gateway, il-Kummissjoni jenħtieġ la tkun kontrollur u lanqas proċessur tad-*data* personali.

(10) Il-Kontrollur Ewropew għall-Protezzjoni tad-*Data* ġie kkonsultat f'konformità mal-Artikolu 42(1) tar-Regolament (UE) 2018/1725 tal-Parlament Ewropew u tal-Kunsill ([4]) u ta opinjoni fit-22 ta' Ġunju 2021.

(11) Meta wieħed iqis li l-ispeċifikazzjonijiet tekniċi u r-regoli huma meħtieġa għall-applikazzjoni tar-Regolament (UE) 2021/953 mill-1 ta' Lulju 2021, l-applikazzjoni minnufih ta' din id-Deċiżjoni hija ġġustifikata.

(12) Għaldaqstant, fid-dawl tal-ħtieġa għal implimentazzjoni rapida taċ-Ċertifikat COVID Diġitali tal-UE, din id-Deċiżjoni jenħtieġ tidħol fis-seħħ fil-jum tal-pubblikazzjoni tagħha,

([3]) Ir-Regolament (UE) 2016/679 tal-Parlament Ewropew u tal-Kunsill tas-27 ta' April 2016 dwar il-protezzjoni tal-persuni fiżiċi fir-rigward tal-ipproċessar ta' *data* personali u dwar il-moviment liberu ta' tali *data*, u li jħassar id-Direttiva 95/46/KE (Regolament Ġenerali dwar il-Protezzjoni tad-*Data*) (ĠU L 119, 4.5.2016, p. 1).

([4]) Ir-Regolament (UE) 2018/1725 tal-Parlament Ewropew u tal-Kunsill tat-23 ta' Ottubru 2018 dwar il-protezzjoni ta' persuni fiżiċi fir-rigward tal-ipproċessar ta' *data* personali mill-istituzzjonijiet, korpi, uffiċċji u aġenziji tal-Unjoni u dwar il-moviment liberu ta' tali *data*, u li jħassar ir-Regolament (KE) Nru 45/2001 u d-Deċiżjoni Nru 1247/2002/KE (ĠU L 295, 21.11.2018, p. 39).

ADOTTAT DIN ID-DEĊIŻJONI:

Artikolu 1

L-ispeċifikazzjonijiet tekniċi taċ-Ċertifikat COVID Diġitali tal-UE li jistabbilixxu l-istruttura ġenerika tad-*data*, il-mekkaniżmi tal-ikkowdjar, u l-mekkaniżmu tal-ikkowdjar tat-trasport b'format ottiku li jinqara minn magna huma stabbiliti fl-Anness I.

Artikolu 2

Ir-regoli għall-mili taċ-ċertifikati kif jissemma fl-Artikolu 3(1) tar-Regolament (UE) 2021/953 huma stabbiliti fl-Anness II ta' din id-Deċiżjoni.

Artikolu 3

Ir-rekwiżiti li jistabbilixxu l-istruttura komuni tal-identifikatur uniku taċ-ċertifikat huma stabbiliti fl-Anness III.

Artikolu 4

Ir-regoli ta' governanza applikabbli għaċ-ċertifikat tal-kjavi pubbliċi fir-rigward tal-gateway taċ-Ċertifikat COVID Diġitali tal-UE, li jappoġġa l-aspetti tal-interoperabbiltà tal-qafas ta' fiduċja, huma stabbiliti fl-Anness IV.

Din id-Deċiżjoni għandha tidħol fis-seħħ fil-jum tal-pubblikazzjoni tagħha f'*Il-Ġurnal Uffiċjali tal-Unjoni Ewropea*.

Magħmul fi Brussell, it-28 ta' Ġunju 2021.

Għall-Kummissjoni
Il-President
Ursula VON DER LEYEN

ANNESS I

IL-FORMAT U L-ĠESTJONI TAL-FIDUĊJA

Struttura ġenerika tad-data, mekkaniżmi tal-ikkowdjar u mekkaniżmu tal-ikkowdjar tat-trasport b'format ottiku li jinqara mill-magni (minn hawn 'il quddiem imsejjaħ "QR")

1. Introduzzjoni

L-ispeċifikazzjonijiet tekniċi stabbiliti f'dan l-Anness fihom struttura ġenerika tad-*data* u mekkaniżmi tal-ikkowdjar għaċ-Ċertifikat COVID Diġitali tal-UE ("DCC"). Dawn jispeċifikaw ukoll mekkaniżmu tal-ikkowdjar tat-trasport b'format ottiku ("QR") li jinqara mill-magni u li jista' jintwera fuq l-iskrin ta' apparat mobbli jew jiġi stampat. Il-formati elettroniċi tal-kontenitur taċ-ċertifikat tas-saħħa b'dawn l-ispeċifikazzjonijiet huma ġeneriċi, iżda f'dan il-kuntest jintużaw biex iġorru d-DCC.

2. Terminoloġija

Għall-finijiet ta' dan l-Anness, "emittenti" tfisser organizzazzjonijiet li jużaw dawn l-ispeċifikazzjonijiet għall-ħruġ ta' ċertifikati tas-saħħa u "verifikaturi" tfisser organizzazzjonijiet li jaċċettaw iċ-ċertifikati tas-saħħa bħala prova tal-istatus tas-saħħa. "Parteċipanti" tfisser emittenti u verifikaturi. Xi aspetti stabbiliti f'dan l-Anness iridu jiġu kkoordinati bejn il-parteċipanti, bħall-ġestjoni tal-ispazju tal-isem u d-distribuzzjoni tal-kjavi kriptografiċi. Hu preżunt li parti, imsejħa s-"Segretarjat", twettaq dawn il-kompiti.

3. Il-Format Elettroniku tal-Kontenitur taċ-Ċertifikat tas-Saħħa

Il-Format Elettroniku tal-Kontenitur taċ-Ċertifikat tas-Saħħa ("HCERT") tfassal biex jipprovdi mezz uniformi u standardizzat għaċ-ċertifikati tas-saħħa mill-emittenti differenti tagħhom ("emittenti"). L-għan ta' dawn l-ispeċifikazzjonijiet hu l-armonizzazzjoni ta' dawk iċ-ċertifikati tas-saħħa fejn jidħlu r-rappreżentazzjoni, l-ikkowdjar u l-firem biex tiġi ffaċilitata l-interoperabbiltà.

Il-kapaċità li DCC maħruġ minn emittent ikun jinqara u jiġi interpretat tenħtieġ struttura komuni tad-*data* u ftehim dwar is-sinifikat ta' kull entrata tad-*data* tal-payload. Biex tiġi ffaċilitata din l-interoperabbiltà, struttura komuni kkordinata tad-*data* hi definita bl-użu tal-iskema "JSON" li tikkostitwixxi t-tfassil tad-DCC.

3.1. *L-Istruttura tal-payload*

Il-payload hija strutturata u kkodifikata bħala CBOR b'firma diġitali COSE. Dan hu magħruf b'mod komuni bħala "CBOR Web Token" (CWT), u huwa definit f'RFC 8392 ([1]). Il-payload, kif definita fit-taqsimiet li ġejjin, tiġi ttrasportata fi claim hcert.

L-integrità u l-awtentiċità tal-oriġini tad-*data* dwar il-payload iridu jkunu verifikabbli mill-verifikatur. Biex jipprovdi dan il-mekkaniżmu, l-emittent irid jiffirma s-CWT billi juża skema ta' firma elettronika asimmetrika kif definit fl-ispeċifikazzjoni COSE (RFC 8152 ([2])).

3.2. *Claims CWT*

3.2.1. Ħarsa ġenerali lejn l-istruttura tas-CWT

Header Protett

— Algoritmu tal-Firma (alg, tikketta 1)

— Identifikatur tal-Kjavi (kid, tikketta 4)

Payload

— Emittent (iss, kjavi tal-claim 1, fakultattiva, ISO 3166-1 alfa-2 tal-emittent)

— Maħruġ Fi (iat, kjavi tal-claim 6)

— Ħin tal-Iskadenza (exp, kjavi tal-claim 4)

— Ċertifikat tas-Saħħa (hcert, kjavi tal-claim -260)

— Ċertifikat COVID Diġitali tal-UE v1 (eu_DCC_v1, kjavi tal-claim 1)

Firma

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

3.2.2. Algoritmu tal-Firma

Il-parametru tal-Algoritmu tal-Firma (alg) jindika liema algoritmu jintuża għall-ħolqien tal-firma. Irid jissodisfa jew imur oltre mil-linji gwida attwali SOG-IS kif miġbura fil-qosor fil-paragrafi li ġejjin.

Hu definit algoritmu primarju wieħed u algoritmu sekondarju wieħed. L-algoritmu sekondarju jenħtieġ jintuża biss meta l-algoritmu primarju ma jkunx aċċettabbli skont ir-regoli u r-regolamenti imposti mill-emittent.

Biex tiġi żgurata s-sigurtà tas-sistema, l-implimentazzjonijiet kollha jridu jinkorporaw l-algoritmu sekondarju. Għal din ir-raġuni, kemm l-algoritmu primarju kif ukoll dak sekondarju jridu jiġu implimentati.

Il-livelli stabbiliti mis-SOG-IS għall-algoritmi primarji u sekondarji huma:

— L-Algoritmu Primarju: L-algoritmu primarju hu Algoritmu tal-Firma Diġitali b'Kurva Ellittika (ECDSA) kif definit fit-taqsima 2.3 (ISO/IEC 14888–3:2006), bl-użu tal-parametri P–256 kif definit fl-appendiċi D (D.1.2.3) ta' (FIPS PUB 186–4) flimkien mal-algoritmu SHA–256 hash kif definit fil-funzjoni 4 (ISO/IEC 10118–3:2004).

Dan jikkorrispondi għall-parametru tal-algoritmu COSE ES256.

— Algoritmu Sekondarju: L-algoritmu sekondarju hu RSASSA-PSS kif definit f'(RFC 8230 ([3])) b'modulus ta' 2048 bits flimkien mal-algoritmu SHA-256 hash kif definit fil-funzjoni 4 (ISO/IEC 10118-3:2004).

Dan jikkorrispondi għall-parametru tal-algoritmu COSE: PS256.

3.2.3. L-Identifikatur tal-Kjavi

Il-claim tal-Identifikatur tal-Kjavi (kid) tindika ċ-Ċertifikat tal-Firem tad-Dokumenti (DSC) li jkun fih il-kjavi pubblika li trid tintuża mill-verifikatur biex jivverifika l-korrettezza tal-firma diġitali. Il-governanza taċ-ċertifikat tal-kjavi pubblika, inkluż ir-rekwiżiti għad-DSCs, hi deskritta fl-Anness IV.

Il-clain tal-Identifikatur tal-Kjavi (kid) jużawha l-verifikaturi biex jagħżlu l-kjavi pubblika t-tajba minn lista ta' kjavi li jappartjenu għall-emittent indikat fil-claim (iss) tal-emittent. Jistgħu jintużaw diversi kjavi b'mod paralleli minn emittent għal raġunijiet amministrattivi u meta jsiru rollovers ta' kjavi. L-Identifikatur tal-Kjavi mhux entrata kritika għas-sigurtà. Għal din ir-raġuni, jista' jitqiegħed ukoll f'header mhux protett jekk ikun meħtieġ. Il-verifikaturi jridu jaċċettaw iż-żewġ alternattivi. Jekk iż-żewġ alternattivi jkunu preżenti, irid jintuża l-Identifikatur tal-Kjavi fl-intestatura protetta.

Minħabba tqassir tal-identifikatur (minħabba raġunijiet ta' limitazzjoni ta' daqs), hemm ċans żgħir ħafna, iżda mhux żero, li l-lista ġenerali tad-DSCs aċċettata minn verifikatur jaf ikun fiha DSCs b'kids duplikati. Għal din ir-raġuni, verifikatur irid jivverifika d-DSCs kollha ma' dak il-kid.

3.2.4. Emittent

Il-claim tal-Emittent (iss) hi valur ta' string li jista' jkollu b'mod fakultattiv il-Kodiċi tal-Pajjiż ISO 3166-1 alfa-2 tal-entità li toħroġ iċ-ċertifikat tas-saħħa. Din il-claim tista' tintuża minn verifikatur biex jidentifika liema sett ta' DSCs irid juża għall-verifika. Il-Kjavi tal-Claim 1 tintuża biex tidentifika din il-claim.

3.2.5. Ħin tal-Iskadenza

Il-claim tal-Ħin tal-Iskadenza (exp) għandu jkollha kronogramma bil-format ta' NumericDate (kif speċifikat f'RFC 8392 ([4]), taqsima 2) li tindika għal kemm żmien din il-firma partikolari fuq il-payload għandha tiġi kkunsidrata valida u, wara, verifikatur irid jirrifjuta l-payload bħala skaduta. L-għan tal-parametru tal-iskadenza hu li jisforza limitu tal-perjodu ta' validità taċ-ċertifikat tas-saħħa. Il-kjavi tal-claim 4 tintuża biex tidentifika din il-claim.

Il-Ħin tal-Iskadenza ma jridx jaqbeż il-perjodu ta' validità tad-DSC.

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

3.2.6. Maħruġ Fi

Il-claim tal-Maħruġa Fi (iat) għandu jkun fiha timbru tal-ħin b'format ta' intiġer NumericDate (kif speċifikat fi RFC 8392 ([5]), it-Taqsima 2) li jindika l-ħin meta nħoloq iċ-ċertifikat tas-saħħa.

L-entrata Maħruġ Fi ma tridx tkun datata qabel il-perjodu ta' validità tad-DSC.

Il-verifikaturi jistgħu japplikaw politiki addizzjonali biex jillimitaw il-validità taċ-ċertifikat tas-saħħa abbażi tal-ħin tal-ħruġ. Il-kjavi tal-claim 6 tintuża biex tidentifika din il-claim.

3.2.7. Il-Claim taċ-Ċertifikat tas-Saħħa

Il-claim taċ-Ċertifikat tas-Saħħa (hcert) hi oġġett JSON (RFC 7159 ([6])) li fih l-informazzjoni dwar l-istatus tas-saħħa. Jistgħu jeżistu diversi tipi differenti ta' ċertifikati tas-saħħa fl-istess claim, id-DCC hu wieħed minnhom.

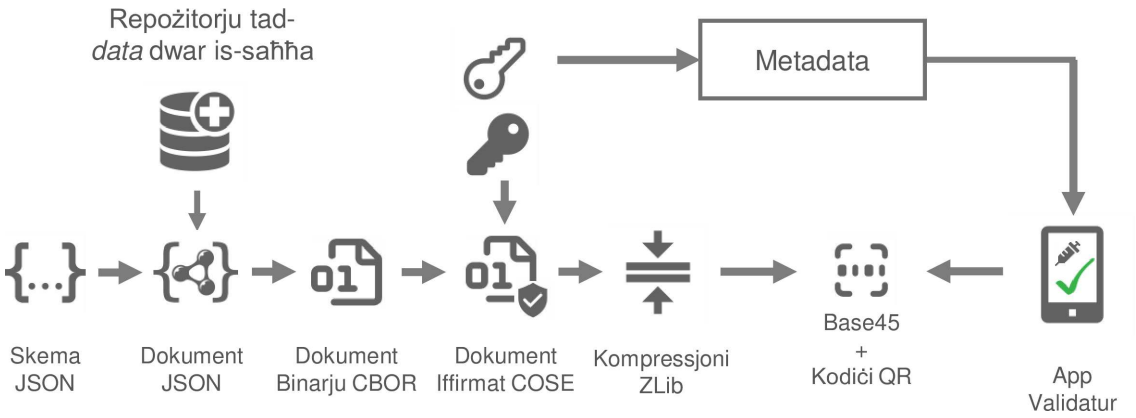
Il-JSON hu purament għal skopijiet ta' skema. Il-format tar-rappreżentazzjoni hu CBOR, kif definit fi (RFC 7049 ([7])). L-iżviluppaturi tal-applikazzjonijiet ma jistgħux fil-fatt jiddekowdjaw, jew jikkowdjaw lil u mill-format JSON, iżda jużaw l-istruttura ta' memorja fih.

Il-kjavi tal-claim li għandha tintuża biex tiġi identifikata din il-claim hija -260.

L-istrings fl-oġġett JSON jenħtieġ jiġu normalizzati skont il-Kompożizzjoni Kanonika tal-Forma tan-Normalizzazzjoni (NFC) definita fl-istandard tal-Unicode. Madankollu, id-dekowdjar tal-applikazzjonijiet jenħtieġ ikun permissiv u robust f'dawn l-aspetti, u l-aċċettazzjoni ta' kwalunkwe tip ta' konverżjoni raġonevoli hija mħeġġa ħafna. Jekk tinstab *data* mhux normalizzata waqt id-dekowdjar, jew f'funzjonijiet ta' tqabbil sussegwenti, l-implimentazzjonijiet jenħtieġ iġibu ruħhom daqslikieku l-input hu normalizzat skont l-NFC.

4. **Is-serjalizzazzjoni u l-ħolqien tal-payload tad-DCC**

Bħala mudell ta' serjalizzazzjoni, tintuża l-iskema li ġejja:



Il-proċess jibda bl-estrazzjoni tad-*data*, pereżempju minn Repożitorju tad-*Data* dwar is-Saħħa (jew minn xi sors tad-*data* estern), li jistruttura d-*data* estratta skont l-Iskemi tad-DCC definiti. F'dan il-proċess, il-konverżjoni għall-format definit tad-*data* u t-trasformazzjoni għal-leġġibbiltà mill-bniedem tista' ssir qabel tibda s-serjalizzazzjoni għal CBOR. L-akronimi tal-claims għandhom jiġu mmappjati f'kull każ għall-ismijiet murija qabel is-serjalizzazzjoni u wara d-deserjalizzazzjoni.

Il-kontenut tad-*data* nazzjonali fakultattiv mhux permess f'ċertifikati maħruġin skont ir-Regolament (UE) 2021/953 ([8]). Il-kontenut tad-*data* hu limitat għall-elementi tad-*data* definiti fis-sett tad-*data* minimu speċifikat fl-Anness tar-Regolament 2021/953.

([5]) rfc8392 (ietf.org)
([6]) rfc7159 (ietf.org)
([7]) rfc7049 (ietf.org)
([8]) Ir-Regolament (UE) 2021/953 tal-Parlament Ewropew u tal-Kunsill tal-14 ta' Ġunju 2021 dwar qafas għall-ħruġ, għall-verifika u għall-aċċettazzjoni ta' ċertifikati COVID-19 interoperabbli tat-tilqim, tat-testijiet u tal-fejqan (Ċertifikat COVID Diġitali tal-UE) għall-faċilitazzjoni tal-moviment liberu waqt il-pandemija tal-COVID-19, ĠU L 211, 15.6.2021, p. 1.

5. **Ikkowdjar tat-Trasport**

5.1. *Raw*

Għal interfaċċi tad-*data* arbitrarja, il-kontenitur tal-HCERT u l-payload tiegħu jistgħu jiġu ttrasferiti kif inhuma, bl-użu ta' xi trasport tad-*data* sottostanti, affidabbli u sikur, b'8 bits. Dawn l-interfaċċi jistgħu jinkludu komunikazzjoni b'kamp fil-qrib (NFC), Bluetooth jew trasferiment bi protokoll ta' saff ta' applikazzjoni, pereżempju trasferiment ta' HCERT mill-Emittent lejn apparat mobbli tad-detentur.

Jekk it-trasferiment tal-HCERT mill-Emittent għad-detentur ikun ibbażat fuq interfaċċa ta' preżentazzjoni biss (pereżempju, SMS, email), l-ikkowdjar tat-trasport raw ovvjament ma jkunx applikabbli.

5.2. *Barcode*

5.2.1. Kompressjoni tal-payload (CWT)

Biex jitnaqqas id-daqs u jittejbu l-veloċità u l-affidabbiltà fil-proċess tal-qari tal-HCERT, is-CWT għandu jiġi kkompressat biż-ZLIB (RFC 1950 ([9])) u bil-mekkaniżmu ta' kompressjoni Deflate bil-format definit f'RFC 1951 ([10]).

5.2.2. Barcode QR 2D

Biex jiġi mmaniġġat aħjar it-tagħmir legat disinjat biex jopera fuq payloads tal-ASCII, is-CWT ikkompressat jiġi kkowdjat bħala ASCII bl-użu ta' Base45 qabel ma jiġi kkowdjat f'barcode 2D.

Il-format QR kif definit f'(ISO/IEC 18004:2015) għandu jintuża għall-ġenerazzjoni tal-barcode 2D. Hi rakkomandata rata ta' korrezzjoni tal-erruri ta' "Q" (madwar 25 %). Peress li jintuża Base45, il-kodiċi QR trid tuża kodifikazzjoni alfanumerika (il-Modalità 2, indikata bis-simboli 0010).

Biex il-verifikaturi jkunu jistgħu jidentifikaw it-tip ta' *data* kkowdjata u jagħżlu l-iskema xierqa tad-dekowdjar u tal-ipproċessar, id-*data* kkowdjata Base45 (skont din l-ispeċifikazzjoni) għandu jkollha l-istring tal-Identifikatur tal-Kuntest "HC1:" bħala prefiss. Verżjonijiet futuri ta' din l-ispeċifikazzjoni li jħallu impatt fuq il-kompatibbiltà b'lura għandhom jiddefinixxu Identifikatur ta' Kuntest ġdid, filwaqt li l-karattru li jsegwi "HC" għandu jitneħħa mis-sett ta' karattri [1-9 A-Z]. L-ordni taż-żidiet hi definita f'dik l-ordni, jiġifieri, l-ewwel [1-9] u mbagħad [A-Z].

Hu rakkomandat li l-kodiċi ottiku jiġi pprovdut fuq il-midja tal-preżentazzjoni b'daqs djagonali ta' bejn 35 mm u 60 mm biex jakkomoda qarrejja b'ottika fissa, meta jkun meħtieġ li l-midja tal-preżentazzjoni titqiegħed fuq wiċċ il-qarrej.

Jekk il-kodiċi ottiku jiġi stampat fuq karta bl-użu ta' stampaturi b'riżoluzzjoni baxxa (< 300 dpi), trid tingħata attenzjoni biex kull simbolu (tikka) tal-kodiċi QR ikun eżattament kwadru. Skalar mhux proporzjonali se jwassal biex jinħolqu ringieli jew kolonni fil-QR b'simboli rettangolari, li se jfixklu l-leġibbiltà f'ħafna każijiet.

6. **Format tal-Lista ta' Fiduċja (lista tas-CSCA u tad-DSC)**

Kull Stat Membru jeħtieġ jipprovdi lista ta' Awtorità taċ-Ċertifikazzjoni tal-Iffirmar taċ-Ċertifikat (CSCA) waħda jew aktar u lista taċ-Ċertifikati tal-Iffirmar tad-Dokumenti (DSCs) validi kollha, u jżommhom aġġornati.

6.1. *CSCA/DSC Issimplifikat*

Minn din il-verżjoni tal-ispeċifikazzjonijiet, l-Istati Membri ma għandhomx jassumu li tista' tintuża kwalunkwe informazzjoni tal-Lista ta' Revoka taċ-Ċertifikati (CRL); jew li l-Perjodu ta' Użu tal-Kjavi Privata jkun ivverifikat mill-implimentaturi.

Minflok, il-mekkaniżmu ta' validità primarju hu l-preżenza taċ-ċertifikat fl-aktar verżjoni riċenti ta' dik il-lista ta' ċertifikati.

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

6.2. *Il-PKI tal-eMRTD tal-ICAO u ċ-Ċentri ta' Fiduċja*

L-Istati Membri jistgħu jużaw CSCA separata – iżda jistgħu jissottomettu wkoll iċ-ċertifikati eżistenti tagħhom tas-CSCA u/jew tad-DSC tal-eMRTD; u jistgħu wkoll jagħżlu li jakkwistaw dawn mingħand ċentri ta' fiduċja (kummerċjali) – u jissottomettuhom. Madankollu, kull DSC irid dejjem jiġi ffirmat mis-CSCA sottomessa minn dak l-Istat Membru.

7. **Kunsiderazzjonijiet ta' Sigurtà**

Meta jfasslu skema bl-użu ta' din l-ispeċifikazzjoni, l-Istati Membri għandhom jidentifikaw, janalizzaw u jimmonitorjaw ċerti aspetti tas-sigurtà.

Jenħtieġ li l-aspetti li ġejjin jiġu kkunsidrati bħala minimu:

7.1. *Ħin ta' validità tal-firma tal-HCERT*

L-emittent tal-HCERTs jeħtieġ jillimita l-perjodu ta' validità tal-firma billi jispeċifika ħin tal-iskadenza tal-firma. Dan jirrikjedi li d-detentur ta' ċertifikat tas-saħħa jġeddidha f'intervalli perjodiċi.

Il-perjodu ta' validità aċċettabbli jista' jiġi determinat minn restrizzjonijiet prattiċi. Pereżempju, vjaġġatur jista' ma jkollux il-possibbiltà li jġedded iċ-ċertifikat tas-saħħa waqt vjaġġ barra mill-pajjiż. Madankollu, jista' jkun ukoll il-każ li emittent ikun qed jikkunsidra l-possibbiltà ta' kompromess ta' sigurtà ta' xi tip, li jirrikjedi li l-emittent jirtira DSC (li jinvalida ċ-ċertifikati kollha tas-saħħa maħruġa billi juża dik il-kjavi li tkun għadha fil-perjodu ta' validità tagħhom). Il-konsegwenzi ta' avveniment bħal dan jistgħu jkunu limitati billi l-kjavi tal-Emittent jiġu rreġistrati b'mod regolari u jkun jenħtieġ it-tiġdid taċ-ċertifikati tas-saħħa kollha, fuq xi intervall raġonevoli.

7.2. *Il-ġestjoni tal-kjavi*

Din l-ispeċifikazzjoni tiddependi ħafna fuq mekkaniżmi kriptografiċi sodi biex jiġu żgurati l-integrità tad-*data* u l-awtentikazzjoni tal-oriġini tad-*data*. Għalhekk jeħtieġ tinżamm il-kunfidenzjalità tal-kjavi privati.

Il-kunfidenzjalità tal-kjavi kriptografiċi tista' tiġi kompromessa b'għadd ta' modi differenti, pereżempju:

— Il-proċess tal-ġenerazzjoni tal-kjavi jista' jkun difettuż, u jirriżulta fi kjavi dgħajfa.

— Il-kjavi jistgħu jiġu esposti għal żball uman.

— Il-kjavi jistgħu jinsterqu minn awturi esterni jew interni.

— Il-kjavi jistgħu jiġu kkalkolati bl-użu tal-kriptanaliżi.

Biex ittaffi r-riskji li l-algoritmu tal-iffirmar jinstab dgħajjef, u b'hekk il-kjavi privati jkunu jistgħu jiġu kompromessi bi kriptanaliżi, din l-ispeċifikazzjoni tirrakkomanda lill-parteċipanti kollha jimplimentaw algoritmu tal-firma ta' riżerva sekondarju abbażi ta' parametri differenti jew abbażi ta' problema matematika differenti minn dik primarja.

Fir-rigward tar-riskji msemmija relatati mal-ambjenti operatorji tal-emittenti, iridu jiġu implimentati miżuri ta' mitigazzjoni biex ikun żgurat kontroll effettiv, bħal eżempju biex jiġu ġġenerati, maħżuna u użati l-kjavi privati fil-Moduli tas-Sigurtà tal-Hardware (HSMs). L-użu tal-HSMs għall-iffirmar taċ-ċertifikati tas-saħħa hu mħeġġeġ ħafna.

Irrispettivament minn jekk emittent jiddeċidix li juża l-HSMs jew le, jenħtieġ tiġi stabbilita skeda tat-tibdil tal-kjavi fejn il-frekwenza tat-tibdil tal-kjavi tkun proporzjonata mal-esponiment tal-kjavi għal networks esterni, sistemi oħra u persunal. Skeda tat-tibdil magħżula sew tillimita wkoll ir-riskji assoċjati ma' ċertifikati tas-saħħa maħruġin b'erruri, billi tippermetti lil emittent jirrevoka dawn iċ-ċertifikati tas-saħħa f'lottijiet, billi jirtira kjavi, jekk ikun meħtieġ.

7.3. *Validazzjoni tad-data tal-input*

Dawn l-ispeċifikazzjonijiet jistgħu jintużaw b'mod li jimplika li tiġi riċevuta *data* minn sorsi mhux fdati f'sistemi li jista' jkollhom natura kritika għall-missjoni. Biex jitnaqqsu kemm jista' jkun ir-riskji assoċjati ma' dan il-mezz ta' attakk, l-entrati kollha tal-input iridu jiġu vvalidati kif xieraq skont it-tipi tad-*data*, it-tulijiet u l-kontenut. Il-firma tal-emittent għandha tiġi vverifikata wkoll qabel ma jsir xi pproċessar tal-kontenut tal-HCERT. Madankollu, il-validazzjoni tal-Firma tal-emittent timplika li l-ewwel jiġi analizzat il-Header Protett tal-Emittent, li fih attakkant potenzjali jista' jipprova jdaħħal informazzjoni mfassla bir-reqqa ddisinjata biex tikkompromietti s-sigurtà tas-sistema.

8. **Ġestjoni tal-Fiduċja**

Il-firma tal-HCERT teħtieġ kjavi pubblika għall-verifika. L-Istati Membri għandhom jagħmlu dawn il-kjavi pubbliċi disponibbli. Fl-aħħar mill-aħħar, kull verifikatur irid ikollu lista tal-kjavi pubbliċi kollha li jkun lest li jafda (għax il-kjavi pubblika mhix parti mill-HCERT).

Is-sistema tikkonsisti (biss) f'żewġ saffi; għal kull Stat Membru, ċertifikat wieħed jew aktar li jiffirmwaw fil-livell tal-pajjiż, li kull wieħed jiffirma Ċertifikat tal-Iffirmar tad-Dokumenti wieħed jew aktar li jintużaw f'operazzjonijiet ta' kuljum.

Iċ-ċertifikati tal-Istati Membri jissejħu ċertifikati tal-Awtoritajiet taċ-Ċertifikazzjoni tal-Firem taċ-Ċertifikat (CSCA) u (tipikament) ikunu ċertifikati awtoffirmati. L-Istati Membri jista' jkollhom aktar minn wieħed (pereżempju, fil-każ ta' devoluzzjonijiet reġjonali). Dawn iċ-ċertifikati tas-CSCA jiffirmaw b'mod regolari ċ-Ċertifikati tal-Iffirmar tad-Dokumenti (DSCs) użati għall-iffirmar tal-HCERTs.

Is-"Segretarjat" jaqdi rwol funzjonali. Għandu jiġbor flimkien u jippubblika regolarment id-DSCs tal-Istati Membri, wara li jkun ivverifikahom mal-lista taċ-ċertifikati tas-CSCA (li jkunu ntbagħtu u li jkunu ġew ivverifikati b'mezzi oħra).

Il-lista riżultanti tad-DSCs għandha mbagħad tipprovdi s-sett aggregat ta' kjavi pubbliċi aċċettabbli (u l-kids korrispondenti) li l-verifikaturi jistgħu jużaw biex jivvalidaw il-firem fuq l-HCERTs. Il-verifikaturi jridu jġibu u jaġġornaw din il-lista regolarment.

Tali listi speċifiċi għall-Istati Membri jistgħu jiġu adattati fil-format għall-konfigurazzjoni nazzjonali tagħhom stess. Għaldaqstant, il-format tal-fajl ta' din il-lista ta' fiduċja jista' jvarja, pereżempju, jista' jkollu format iffirmat JWKS (format issettjat JWK skont RFC 7517 ([11]), it-Taqsima 5) jew xi format speċifiku ieħor għat-teknoloġija użata f'dak l-Istat Membru.

Biex tiġi żgurata s-sempliċità, l-Istati Membri jistgħu t-tnejn jippreżentaw iċ-ċertifikati tas-CSCA eżistenti tagħhom mis-sistemi tal-ICAO eMRTD tagħhom jew, kif rakkomandat mid-WHO, joħolqu wieħed speċifikament għal dan il-qasam tas-saħħa.

8.1. *L-Identifikatur tal-Kjavi (kids)*

L-identifikatur tal-kjavi (kid) jiġi kkalkolat meta tiġi stabbilita l-lista ta' kjavi pubbliċi ta' fiduċja mid-DSCs u jikkonsisti f'impronta SHA-256 maqtugħa (l-ewwel 8 bytes) tad-DSC ikkowdjat b'format DER (mhux ipproċessat).

Il-verifikaturi m'għandhomx għalfejn jikkalkulaw il-kid abbażi tad-DSC u jistgħu jqabblu direttament l-identifikatur tal-kjavi fiċ-ċertifikat tas-saħħa maħruġ mal-kid fuq il-lista ta' fiduċja.

8.2. *Differenzi għall-mudell ta' fiduċja tal-eMRTD tal-ICAO*

Filwaqt li dan jitfassal skont l-aqwa prattiki tal-mudell ta' fiduċja tal-eMRTD PKI tal-ICAO, għandhom isiru għadd ta' simplifikazzjonijiet fl-interess tal-ħeffa:

— Stat Membru jista' jissottometti diversi ċertifikati tas-CSCA.

— Il-perjodu ta' validità tad-DSC (użu tal-kjavi) jista' jiġi ssettjat għal kwalunkwe tul li ma jaqbiżx dak taċ-ċertifikat tas-CSCA u jista' jkun assenti.

— Id-DSC jista' jkun fih identifikaturi ta' politika (Użu Estiż tal-Kjavi) li huma speċifiċi għaċ-ċertifikati tas-saħħa.

— L-Istati Membri jistgħu jagħżlu li qatt ma jagħmlu verifika tar-revoki ppubblikati; iżda minflok jiddependu biss fuq il-listi tad-DSC li jiksbu kuljum mis-Segretarjat jew li jikkumpilaw huma stess.

([11]) rfc7517 (ietf.org)

ANNESS II

REGOLI GĦALL-FINI TAL-MILI TAĊ-ĊERTIFIKAT COVID DIĠITALI TAL-UE

Ir-regoli ġenerali li jikkonċernaw is-settijiet ta' valur stabbiliti f'dan l-Anness għandhom l-għan li jiżguraw l-interoperabbiltà fil-livell semantiku u għandhom jippermettu implimentazzjonijiet tekniċi uniformi għad-DCC. L-elementi li jinsabu f'dan l-Anness jistgħu jintużaw għat-tliet xenarji differenti (tilqim/ittestjar/fejqan), kif previst fir-Regolament (UE) 2021/953. F'dan l-Anness jiġu elenkati biss l-elementi bil-ħtieġa ta' standardizzazzjoni semantika b'settijiet ta' valur kodifikati.

It-traduzzjoni tal-elementi kodifikati bil-lingwa nazzjonali hi fir-responsabbiltà tal-Istati Membri.

Għall-entrati kollha tad-*data* mhux imsemmija fid-deskrizzjonijiet tas-sett ta' valuri li ġejjin, hu rakkomandat ikkowdjar bil-UTF-8 (isem, ċentru tal-ittestjar, emittent taċ-ċertifikat). Hu rakkomandat li l-entrati tad-*data* li fihom dati kalendarji (data tat-twelid, data tat-tilqim, data tal-ġbir tal-kampjun tat-test, data tal-ewwel riżultat pożittiv tat-test, dati tal-validità taċ-ċertifikat) jiġu kkodifikati skont l-ISO 8601.

Jekk għal xi raġuni ma jkunux jistgħu jintużaw is-sistemi tal-kodiċi preferuti elenkati hawn taħt, jistgħu jintużaw sistemi tal-kodiċi internazzjonali oħra u jenħtieġ jiġi stabbilit parir dwar kif iridu jiġu mmappjati l-kodiċijiet mis-sistema tal-kodiċi l-oħra għas-sistema tal-kodiċi preferuta. It-test (turija ta' ismijiet) jista' jintuża f'każijiet eċċezzjonali bħala mekkaniżmu ta' riżerva meta kodiċi xieraq ma jkunx disponibbli fis-settijiet ta' valur definit.

L-Istati Membri li jużaw ikkowdjar ieħor fis-sistemi tagħhom, jenħtieġ jimmappjaw dawn il-kodiċijiet mas-settijiet ta' valur deskritti. L-Istati Membri huma responsabbli għal kull mmappjar bħal dan.

Is-settijiet ta' valur għandhom jiġu aġġornati regolarment mill-Kummissjoni bl-appoġġ tan-Network tas-Saħħa elettronika u tal-Kumitat għas-Sigurtà tas-Saħħa. Is-settijiet ta' valur aġġornati għandhom jiġu ppubblikati fuq is-sit web rilevanti tal-Kummissjoni u fuq il-paġna web tan-Network tas-Saħħa elettronika. Jenħtieġ tingħata l-istorja tal-bidliet.

1. **Marda jew aġent fil-mira/Marda jew aġent li d-detentur fieq minnha/u: COVID-19 (SARS-CoV-2 jew wieħed mill-varjanti tiegħu)**

   Sistema tal-Kodiċi Preferuta: SNOMED CT.

   Għall-użu fiċ-ċertifikati 1, 2 u 3.

   Il-kodiċijiet magħżula għandhom jirreferu għall-COVID-19 jew, jekk tkun meħtieġa informazzjoni aktar dettaljata dwar il-varjant ġenetiku tas-SARS-CoV-2, għal dawn il-varjanti jekk din l-informazzjoni dettaljata tkun meħtieġa minħabba raġunijiet epidemjoloġiċi.

   Eżempju ta' kodiċi li jenħtieġ jintuża hu l-kodiċi SNOMED CT 840539006 (COVID-19).

2. **Vaċċin jew profilassi tal-COVID-19**

   Sistema tal-Kodiċi Preferuta: SNOMED CT jew Klassifikazzjoni ATC.

   Għall-użu fiċ-ċertifikat 1.

   Eżempji ta' kodiċijiet li jenħtieġ jintużaw mis-sistemi tal-kodiċi ppreferuti huma l-kodiċi SNOMED CT 1119305005 (vaċċin antiġene SARS-CoV-2), 1119349007 (vaċċin SARS-CoV-2 mRNA) jew J07BX03 (vaċċini COVID-19). Is-sett ta' valur jenħtieġ jiġi estiż meta jiġu żviluppati tipi ġodda ta' vaċċini u jibdew jintużaw.

3. **Prodott mediċinali tal-vaċċin kontra l-COVID-19**

   Sistemi tal-Kodiċi Preferuti (fl-ordni ta' preferenza):

   — Reġistru tal-Unjoni tal-prodotti mediċinali għall-vaċċini b'awtorizzazzjoni madwar l-UE (numri ta' awtorizzazzjoni)

   — Reġistru dinji tal-vaċċini bħal dak li jista' jiġi stabbilit mill-Organizzazzjoni Dinjija tas-Saħħa

   — L-isem tal-prodott mediċinali tal-vaċċin f'każijiet oħra. Jekk l-isem jinkludi spazji bojod, dawn jenħtieġ jiġu sostitwiti b'sing (-).

Isem is-Sett ta' Valur: Vaċċin.

Għall-użu fiċ-ċertifikat 1.

Eżempju ta' kodiċi li jenħtieġ li jintuża mis-sistemi tal-kodiċi preferuti hu EU/1/20/1528 (Comirnaty). Eżempju tal-isem tal-vaċċin li għandu jintuża bħala kodiċi: Sputnik-V (li jfisser Sputnik V).

4. **Detentur jew manifattur tal-awtorizzazzjoni għat-tqegħid fis-suq tal-vaċċin tal-COVID-19**

Sistema ta' Kodiċi Preferuta:

— Kodiċi tal-organizzazzjoni mill-EMA (sistema SPOR għall-ISO IDMP)

— Detentur tal-awtorizzazzjoni għat-tqegħid fis-suq ta' vaċċin jew reġistru tal-manifattur fil-livell dinji, bħal dak li jista' jiġi stabbilit mill-Organizzazzjoni Dinjija tas-Saħħa

— L-isem tal-organizzazzjoni f'każijiet oħra. Jekk l-isem jinkludi spazji bojod, dawn jenħtieġ jiġu sostitwiti b'sing (-).

Għall-użu fiċ-ċertifikat 1.

Eżempju ta' kodiċi li jenħtieġ jintuża mis-sistema tal-kodiċi preferuta hu ORG-100001699 (AstraZeneca AB). Eżempju tal-isem tal-organizzazzjoni li għandu jintuża bħala kodiċi: Sinovac-Biotech (li jfisser Sinovac Biotech).

5. **Numru f'serje ta' doża u n-numru dinji ta' doża fis-serje**

Għall-użu fiċ-ċertifikat 1.

Żewġ entrati:

(1) In-numru ta' doża mogħtija f'ċiklu

(2) In-numru ta' dożi mistennija għal ċiklu sħiħ (speċifiku għal persuna fil-ħin tal-għoti tat-tilqima)

Pereżempju, 1/1, 2/2 se jiġu ppreżentati bħala lesti; inkluż l-għażla 1/1 għall-vaċċini li jinkludu żewġ dożi, iżda li l-protokoll applikat għalihom mill-Istat Membru hu li tingħata doża waħda liċ-ċittadini li jkunu ġew dijanjostikati bil-COVID-19 qabel it-tilqima. In-numru dinji ta' dożi fis-serje jenħtieġ jiġi indikat skont l-informazzjoni disponibbli fil-ħin meta tingħata d-doża. Pereżempju, jekk vaċċin speċifiku jkun jenħtieġ it-tielet doża (booster) waqt il-ħin tal-aħħar tilqima mogħtija, it-tieni numru tal-entrata għandu jirrifletti dan (pereżempju 2/3, 3/3 eċċ.).

6. **Stat Membru jew pajjiż terz fejn ingħata l-vaċċin/sar it-test**

Sistema tal-Kodiċi Preferuta: Kodiċijiet tal-Pajjiżi ISO 3166.

Għall-użu fiċ-ċertifikati 1, 2 u 3.

Kontenut tas-sett ta' valur: il-lista sħiħa ta' kodiċijiet b'2 ittri, disponibbli bħala sett ta' valur definit fl-FHIR (http://hl7.org/fhir/ValueSet/iso3166-1-2)

7. **It-tip ta' test**

Sistema tal-Kodiċi Preferuta: LOINC.

Għall-użu fiċ-ċertifikat 2, u fiċ-ċertifikat 3 jekk b'att delegat jiġi introdott appoġġ għall-ħruġ ta' ċertifikati tal-fejqan abbażi tat-tipi ta' test, għajr l-NAAT.

Il-kodiċijiet f'dan is-sett ta' valuri għandhom jirreferu għall-metodu tat-test u għandhom jintgħażlu tal-anqas biex jiġu sseparati t-testijiet tal-NAAT mit-testijiet tar-RAT kif espress fir-Regolament (UE) 2021/953.

Eżempju ta' kodiċi li jenħtieġ jintuża mis-sistema tal-kodiċi preferuta hu LP217198-3 (Immunoassaġġ rapidu).

8. **Manifattur u isem kummerċjali tat-test użat (fakultattiv għat-test tal-NAAT)**

Sistema tal-Kodiċi Preferuta: Lista mill-HSC tat-Testijiet Rapidi tal-Antiġeni kif miżmuma mill-JRC (Bażi tad-Data ta' Tagħmir Dijanjostiku in vitro u tal-Metodi ta' Ttestjar għall-COVID-19).

Għall-użu fiċ-ċertifikat 2.

Il-kontenut tas-Sett ta' Valuri għandu jinkludi l-għażla tat-test rapidu tal-antiġeni kif elenkat fil-lista komuni u aġġornata tat-testijiet rapidi tal-antiġeni tal-COVID-19, stabbilita abbażi tar-Rakkomandazzjoni tal-Kunsill 2021/C 24/01 u maqbula mill-Kumitat għas-Sigurtà tas-Saħħa. Il-lista tinżamm mill-JRC fil-Bażi tad-*Data* ta' Tagħmir Dijanjostiku *in vitro* u tal-Metodi ta' Ttestjar tal-COVID-19 fuq: https://covid-19-diagnostics.jrc.ec.europa.eu/devices/hsc-common-recognition-rat

Għal din is-sistema tal-kodiċi, għandhom jintużaw entrati rilevanti bħall-identifikatur tal-apparat tat-test, l-isem tat-test u tal-manifattur, bil-format strutturat tal-JRC disponibbli fuq https://covid-19-diagnostics.jrc.ec.europa.eu/devices

9. **Riżultat tat-test**

Sistema tal-Kodiċi Preferuta: SNOMED CT.

Għall-użu fiċ-ċertifikat 2.

Il-kodiċijiet magħżula għandhom jippermettu li ssir distinzjoni bejn ir-riżultati pożittivi u negattivi tat-test (identifikati jew mhux identifikati). Jistgħu jiżdiedu valuri addizzjonali (bħal dawk mhux determinati) jekk il-każijiet tal-użu jkunu jeħtieġu dan.

Eżempji ta' kodiċijiet li jenħtieġ jintużaw mis-sistema tal-kodiċi preferuta huma 260415000 (Mhux identifikat) u 260373001 (Identifikat).

ANNESS III

STRUTTURA KOMUNI TAL-IDENTIFIKATUR UNIKU TAĊ-ĊERTIFIKAT

1. **Introduzzjoni**

Kull ċertifikat COVID Diġitali tal-UE (DCC) għandu jinkludi identifikatur uniku taċ-ċertifikat (UCI) li jappoġġa l-interoperabbiltà tad-DCCs. Il-UCI jista' jintuża biex jiġi vverifikat iċ-ċertifikat. L-Istati Membri għandhom ikunu responsabbli għall-implimentazzjoni tal-UCI. Il-UCI hu mezz biex tiġi vverifikata l-veraċità taċ-ċertifikat u, meta applikabbli, biex ikun hemm rabta ma' sistema ta' reġistrazzjoni (pereżempju, IIS). Dawn l-identifikaturi għandhom jippermettu wkoll affermazzjonijiet (stampati u diġitali) mill-Istati Membri li l-individwi jkunu tlaqqmu jew ġew ittestjati.

2. **Il-kompożizzjoni tal-identifikatur uniku taċ-ċertifikat**

Il-UCI għandu jsegwi struttura u format komuni li jiffaċilita l-interpretazzjoni tal-informazzjoni mill-bniedem u/jew mill-magni u tista' tkun relatata ma' elementi bħall-Istat Membru tat-tilqim, il-vaċċin innifsu u identifikatur speċifiku ta' Stat Membru. Dan jiżgura l-flessibbiltà lill-Istati Membri biex jifformattjawh, b'rispett sħiħ tal-leġiżlazzjoni dwar il-protezzjoni tad-*data*. L-ordni tal-elementi separati ssegwi ġerarkija definita li tista' tippermetti modifiki futuri tal-elementi filwaqt li żżomm l-integrità strutturali tiegħu.

Is-soluzzjonijiet possibbli għall-kompożizzjoni tal-UCI jiffurmaw spettru fejn il-modularità u l-interpretazzjoni mill-bniedem huma ż-żewġ parametri ewlenin diversifikanti u karatteristika fundamentali waħda:

— Modularità: il-grad sa fejn il-kodiċi hu magħmul minn elementi fundamentali distinti li fihom informazzjoni semantikament differenti

— Interpretazzjoni mill-bniedem: il-grad sa fejn il-kodiċi hu sinifikanti jew jista' jiġi interpretat mill-qarrej uman

— Globalment uniku; l-identifikatur tal-Pajjiż jew tal-Awtorità hu ġestit tajjeb; u kull pajjiż (awtorità) mistenni jimmaniġġa s-segment tiegħu tal-ispazju tal-isem tajjeb billi qatt ma jirriċiklaw identifikaturi jew jerġgħu joħorġuhom. Il-kombinament ta' dan tiżgura li kull identifikatur ikun globalment uniku.

3. **Rekwiżiti ġenerali**

Ir-rekwiżiti ġenerali li ġejjin jenħtieġ jiġu ssodisfati fir-rigward tal-UCI:

(1) Charset: Huma permessi biss karattri alfanumeriċi kapitali US-ASCII alfa ("A" sa "Z", "0" sa "9"); b'karattri speċjali addizzjonali għas-separazzjoni mill-RFC3986 ([1]) ([2]), jiġifieri {'/','#',':'};

(2) Tul massimu: id-disinjaturi jenħtieġ jipprovaw jimmiraw għal tul ta' 27-30 karattru ([3]);

(3) Prefiss tal-verżjoni: dan jirreferi għall-verżjoni tal-iskema tal-UCI. Il-prefiss tal-verżjoni hu "01" għal din il-verżjoni tad-dokument; il-prefiss tal-verżjoni hu magħmul minn żewġ ċifri;

(4) Prefiss tal-pajjiż: il-kodiċi tal-pajjiż hu speċifikat mill-ISO 3166-1. Kodiċijiet itwal (eż... 3 karattri u aktar (pereżempju, "UNHCR") huma riżervati għall-użu futur;

(5) Suffiss tal-kodiċi/Checksum:

5.1. L-Istati Membri jenħtieġ jużaw checksum meta aktarx isseħħ trażmissjoni, traskrizzjoni (umana) jew korruzzjoni oħra (jiġifieri meta tintuża fl-istampar).

5.2. Wieħed ma jridx jibbaża fuq iċ-checksum għall-validazzjoni taċ-ċertifikat u ċ-checksum mhix teknikament parti mill-identifikatur iżda tintuża biex tiġi vverifikata l-integrità tal-kodiċi. Din iċ-checksum jenħtieġ tkun is-sommarju ISO-7812-1 (LUHN-10) ([4]) tal-UCI kollu b'format ta' trasport diġitali/bil-wire. Iċ-checksum hi separata mill-bqija tal-UCI bil-karattru "#".

([1]) rfc3986 (ietf.org)

([2]) Entrati bħal Ġeneru, Lott/numru tal-lott, Ċentru ta' Amministrazzjoni, identifikazzjoni tal-Professjonista tas-Saħħa, data tat-tilqim li jmiss jistgħu ma jkunux meħtieġa għal skopijiet oħra għajr għall-użu mediku.

([3]) Għall-implimentazzjoni tal-kodiċijiet QR, l-Istati Membri jistgħu jikkunsidraw li jintuża sett addizzjonali ta' karattri b'tul totali sa 72 karattru (inkluż is-27-30 tal-identifikatur innifsu) biex iwassal informazzjoni oħra. L-ispeċifikazzjoni ta' din l-informazzjoni hi f'idejn l-Istati Membri biex jiddefinixxuha.

([4]) L-algoritmu Luhn mod N hu estensjoni għall-algoritmu Luhn (magħruf ukoll bħala algoritmu mod 10) li jaħdem għal kodiċijiet numeriċi u jintuża pereżempju għall-kalkolu taċ-checksums tal-karti ta' kreditu. L-estensjoni tippermetti lill-algoritmu jaħdem b'sekwenzi ta' valuri fi kwalunkwe bażi (karattri alfa fil-każ tagħna).

Jenħtieġ tiġi żgurata kompatibbiltà b'lura: L-Istati Membri li maż-żmien jibdlu l-istruttura tal-identifikaturi tagħhom (fil-verżjoni ewlenija, attwalment stabbilita għal v1) iridu jiżguraw li kwalunkwe żewġ identifikaturi li jkunu identiċi jirrappreżentaw l-istess ċertifikat/dikjarazzjoni ta' tilqim. Jew, fi kliem ieħor, l-Istati Membri ma jistgħux jirriċiklaw l-identifikaturi.

4. **Alternattivi għal identifikaturi uniċi taċ-ċertifikat, għaċ-ċertifikati tat-tilqim**

Il-linji gwida tan-Network tas-Saħħa elettronika għaċ-ċertifikati ta' tilqim verifikabbli u l-elementi bażiċi tal-interoperabbiltà ([5]) jipprevedu għażliet differenti disponibbli għall-Istati Membri u partijiet oħra li jistgħu jeżistu flimkien fost Stati Membri differenti. L-Istati Membri jistgħu jużaw dawn l-għażliet differenti f'verżjoni differenti tal-iskema tal-UCI.

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

ANNESS IV

GOVERNANZA TAĊ-ĊERTIFIKATI TAL-KJAVI PUBBLIĊI

1. **Introduzzjoni**

L-iskambju sigur u fdat tal-kjavi tal-firma għaċ-ċertifikati COVID diġitali tal-UE (DCCs) bejn l-Istati Membri jitwettaq mill-Gateway taċ-Ċertifikat COVID Diġitali tal-UE (DCCG), li jaġixxi bħala repożitorju ċentrali għall-kjavi pubbliċi. Bid-DCCG, l-Istati Membri għandhom is-setgħa li jippubblikaw il-kjavi pubbliċi li jikkorrespondu għall-kjavi privati li huma użaw biex jiffirmaw iċ-Ċertifikati COVID Diġitali. L-Istati Membri dipendenti jistgħu użaw id-DCCG biex jiksbu materjal aġġornat u fil-ħin dwar kjavi pubbliċi. Imbagħad id-DCCG jista' jiġi estiż għall-iskambju tal-informazzjoni supplimentari affidabbli li l-Istati Membri jipprovdu, bħar-regoli ta' validazzjoni għad-DCCs. Il-mudell ta' fiduċja tal-qafas tad-DCC hu Infrastruttura tal-Kjavi Pubblika (PKI). Kull Stat Membru jżomm Awtorità Nazzjonali taċ-Ċertifikazzjoni tal-Firem (CSCA) waħda jew aktar, li ċ-ċertifikati tagħha għandhom ħajja relattivament twila. Wara d-deċiżjoni tal-Istat Membru, is-CSCA tista' tkun l-istess jew differenti mis-CSCA użata għal dokumenti tal-ivvjaġġar li jinqraw mill-magni. Is-CSCA toħroġ ċertifikati tal-kjavi pubblika għall-Firmatarji tad-Dokumenti nazzjonali, b'ħajja qasira (jiġifieri l-firmatarji għad-DCCs), li jissejħu Ċertifikati tal-Firem tad-Dokumenti (DSCs). Is-CSCA taġixxi bħala ankra ta' fiduċja b'tali mod li l-Istati Membri dipendenti jkunu jistgħu użaw iċ-ċertifikat tas-CSCA biex jivvalidaw l-awtenticità u l-integrità tad-DSCs li jinbidlu b'mod regolari. Ladarba jiġu vvalidati, l-Istati Membri jistgħu jipprovdu dawn iċ-ċertifikati (jew sempliċiment il-kjavi pubbliċi li jinsabu fihom) għall-applikazzjonijiet ta' validazzjoni tad-DCC tagħhom. Minbarra s-CSAs u d-DSCs, id-DCCG jiddependi wkoll fuq il-PKI biex jawtentika t-tranżazzjonijiet, jiffirma d-*data*, bħala l-bażi għall-awtentikazzjoni u bħala mezz biex tiġi żgurata l-integrità tal-mezzi tal-komunikazzjoni bejn l-Istati Membri u d-DCCG.

Il-firem diġitali jistgħu jintużaw biex jinkisbu l-integrità u l-awtenticità tad-*data*. L-infrastrutturi tal-Kjavi Pubbliċi jistabbilixxu l-fiduċja bi kjavi pubbliċi vinkolanti għal identitajiet verifikati (jew emittenti). Dan hu meħtieġ biex parteċipanti oħra jitħallew jivverifikaw l-oriġini tad-*data* u l-identità tas-sieħeb tal-komunikazzjoni u biex jiddeċiedu dwar il-fiduċja. Fid-DCCG, jintużaw diversi ċertifikati tal-kjavi pubbliċi għall-awtenticità. Dan l-Anness jiddefinixxi liema ċertifikati tal-kjavi pubbliċi jintużaw u kif għandhom jitfasslu biex jippermettu interoperabbiltà wiesgħa fost l-Istati Membri. Dan jipprovdi aktar dettalji dwar iċ-ċertifikati tal-kjavi pubbliċi meħtieġa u jagħti gwida dwar mudelli taċ-ċertifikati u l-perjodi ta' validità għall-Istati Membri li jridu joperaw is-CSCA tagħhom stess. Peress li d-DCCs għandhom ikunu verifikabbli għal perjodu ta' żmien definit (li jibda mill-ħruġ u jiskadi wara żmien partikolari), jeħtieġ jiġi definit mudell ta' verifika għall-firem kollha applikati fuq iċ-ċertifikati tal-kjavi pubbliċi u d-DCCs.

2. **Terminoloġija**

It-tabella li ġejja fiha l-abbrevjazzjonijiet u t-terminoloġija użati f'dan l-Anness kollu.

Terminu	Definizzjoni
Ċertifikat	Jew ċertifikat tal-kjavi pubblika. Ċertifikat X. 509 v3 li fih il-kjavi pubblika ta' entità
CSCA	Awtorità Nazzjonali taċ-Ċertifikazzjoni tal-Firem
DCC	Ċertifikat COVID Diġitali tal-UE. Dokument diġitali ffirmat li jkun fih informazzjoni dwar it-tilqim, it-test jew il-fejqan
DCCG	Gateway taċ-Ċertifikat COVID Diġitali tal-UE. Din is-sistema tintuża għall-iskambju tad-DSCs bejn l-Istati Membri
$DCCG_{TA}$	Iċ-ċertifikat ta' Ankra ta' Fiduċja tad-DCCG. Il-kjavi privata korrispondenti tintuża biex tiġi ffirmata l-lista taċ-ċertifikati kollha tas-CSCA offline
$DCCG_{TLS}$	Iċ-ċertifikat tas-server TLS tad-DCCG
DSC	Ċertifikat tal-Firem tad-Dokumenti. Iċ-Ċertifikat tal-Kjavi Pubblika ta' awtorità għall-iffirmar tad-dokumenti ta' Stat Membru (pereżempju, sistema li titħalla tiffirma DCCs). Dan iċ-ċertifikat jinħareġ mis-CSCA tal-Istat Membru
EC-DSA	Algoritmu tal-Firma Diġitali b'Kurvi Ellittiċi. Algoritmu tal-firma kriptografika bbażat fuq kurvi ellittiċi
Stat Membru	Stat Membru tal-Unjoni Ewropea

Terminu	Definizzjoni
mTLS	TLS reċiproku. Il-Protokoll għas-Sigurtà tas-Saff tat-Trasport b'awtentikazzjoni reċiproka
NB	Backend Nazzjonali ta' Stat Membru
NB_{CSCA}	Iċ-ċertifikat tas-CSCA ta' Stat Membru (jista' jkun aktar minn wieħed)
NB_{TLS}	Iċ-ċertifikat ta' awtentikazzjoni tat-TLS tal-klijent ta' backend nazzjonali
NB_{UP}	Iċ-ċertifikat li juża backend nazzjonali biex jiffirma pakketti ta' *data* li jittellgħu fid-DCCG
PKI	Infrastruttura tal-Kjavi Pubblika. Mudell ta' fiduċja bbażat fuq iċ-ċertifikati tal-kjavi pubbliċi u fuq l-awtoritajiet taċ-ċertifikazzjoni
RSA	Algoritmu kriptografiku asimmetriku bbażat fuq fattorizzazzjoni integer użata għall-firem diġitali jew għall-kriptaġġ asimmetriku

3. **Flussi tal-komunikazzjoni u servizzi tas-sigurtà tad-DCCG**

Din it-taqsima tagħti ħarsa ġenerali lejn il-flussi tal-komunikazzjoni u s-servizzi tas-sigurtà fis-sistema tad-DCCG. Tiddefinixxi wkoll liema kjavi u ċertifikati jintużaw biex tiġi protetta l-komunikazzjoni, l-informazzjoni mtellgħa, id-DCCs, u lista ta' fiduċja ffirmata li fiha ċ-ċertifikati tas-CSCA mtellgħin kollha. Id-DCCG jaħdem bħala ċentru tad-*data* li jippermetti l-iskambju ta' pakketti tad-*data* ffirmati għall-Istati Membri.

Pakketti tad-*data* mtellgħin huma pprovduti mid-DCCG "kif inhuma", li jfisser li d-DCCG ma jżidx jew ma jħassarx id-DSCs mill-pakketti li jirċievi. Il-backend nazzjonali (NB) tal-Istati Membri għandu jkun jista' jivverifika l-integrità u l-awtenticità minn tarf sa tarf tad-*data* mtellgħa. Minbarra dan, il-backends nazzjonali u d-DCCG se jużaw awtentikazzjoni reċiproka tat-TLS biex jistabbilixxu konnessjoni sigura. Dan minbarra l-firem fid-*data* skambjata.

3.1. *Awtentikazzjoni u stabbiliment tal-konnessjoni*

Id-DCCG juża Saff ta' Sigurtà tat-Trasport (TLS) b'awtentikazzjoni reċiproka biex jistabbilixxi mezz kriptat awtentikat bejn il-backend nazzjonali (NB) tal-Istat Membru u l-ambjent tal-Gateway. Għalhekk, id-DCCG għandu ċertifikat tas-server tat-TLS, $DCCG_{TLS}$ fil-qosor; u l-backends nazzjonali għandhom ċertifikat tat-TLS tal-klijent, fil-qosor NB_{TLS}. Mudelli ta' ċertifikati huma pprovduti fit-*Taqsima 5*. Kull backend nazzjonali jista' jipprovdi ċ-ċertifikat tat-TLS tiegħu stess. Dan iċ-ċertifikat se jsirlu whitelisting b'mod espliċitu u għalhekk jista' jinħareġ minn awtorità taċ-ċertifikazzjoni fdata pubblikament (pereżempju, awtorità taċ-ċertifikazzjoni li ssegwi r-rekwiżiti bażi tal-Forum tal-Browser CA), minn awtorità nazzjonali taċ-ċertifikazzjoni jew jista' jiġi ffirmat minnha stess. Kull Stat Membru hu responsabbli għad-*data* nazzjonali tiegħu u għall-protezzjoni tal-kjavi privata użata biex tiġi stabbilita l-konnessjoni mad-DCCG. L-approċċ ta' "ġib iċ-ċertifikat tiegħek stess" jeħtieġ proċess definit sew ta' reġistrazzjoni u identifikazzjoni, u proċeduri ta' revoka u tiġdid kif deskritt fit-*Taqsimiet 4.1, 4.2* and *4.3*. Id-DCCG juża whitelist fejn jiżdiedu ċ-ċertifikati tat-TLS tan-NBs wara li r-reġistrazzjoni tagħhom tkun irnexxiet. NBs biss li jawtentikaw lilhom infushom bi kjavi privata li tikkorrispondi għal ċertifikat fil-whitelist jistgħu jistabbilixxu konnessjoni sigura mad-DCCG. Id-DCCG se juża wkoll ċertifikat tat-TLS li jippermetti lin-NBs jivverifikaw li tabilħaqq qed jistabbilixxu konnessjoni mad-DCCG "reali" u mhux ma' xi entità malizzjuża li tagħmilha ta' DCCG. Iċ-ċertifikat tad-DCCG se jingħata lin-NBs wara reġistrazzjoni b'suċċess. Iċ-ċertifikat tad-$DCCG_{TLS}$ se jinħareġ minn CA fdata pubblikament (inkluż fil-browsers ewlenin kollha). Hi r-responsabbiltà tal-Istati Membri li jivverifikaw li l-konnessjoni tagħhom mad-DCCG hi sigura (pereżempju, billi jivverifikaw il-marka tas-swaba' taċ-ċertifikat DCCGTLS tas-server imqabbad magħha għal dik ipprovduta wara r-reġistrazzjoni).

3.2. *Awtoritajiet Nazzjonali taċ-Ċertifikazzjoni tal-Firem u l-Mudell ta' Validazzjoni*

L-Istati Membri li jieħdu sehem fil-qafas tad-DCCG iridu jużaw CSCA biex joħorġu d-DSCs. L-Istati Membri jista' jkollhom aktar minn CSCA waħda, pereżempju, fil-każ ta' devoluzzjoni reġjonali. Kull Stat Membru jista' juża l-awtoritajiet taċ-ċertifikazzjoni eżistenti jew inkella jista' jistabbilixxi awtorità taċ-ċertifikazzjoni ddedikata (possibbilment awtoffirmata) għas-sistema tad-DCC.

L-Istati Membri jridu jippreżentaw iċ-ċertifikat(i) tas-CSCA tagħhom lill-operatur tad-DCCG waqt il-proċedura uffiċjali ta' onboarding. Wara r-reġistrazzjoni b'suċċess tal-Istat Membru (*ara t-Taqsima 4.1 għal aktar dettalji*), l-operatur tad-DCCG se jaġġorna lista ta' fiduċja ffirmata li jkun fiha ċ-ċertifikati kollha tas-CSCA li huma attivi fil-qafas tad-DCC. L-operatur tad-DCCG se juża par kjavi asimmetriku ddedikat biex jiffirma l-lista ta' fiduċja u ċ-ċertifikati f'ambjent offline. Il-kjavi privata ma tinħażinx fuq is-sistema tad-DCCG online, b'tali mod li kompromess tas-sistema online ma jippermettix li attakkant jikkompromett l-lista ta' fiduċja. Iċ-ċertifikat ta' ankra ta' fiduċja $DCCG_{TA}$ korrispondenti, se jingħata lin-national backends waqt il-proċess ta' onboarding.

L-Istati Membri jistgħu jirkupraw il-lista ta' fiduċja mid-DCCG għall-proċeduri ta' verifika tagħhom. Is-CSCA hi definita bħala l-awtorità taċ-ċertifikazzjoni li toħroġ id-DSCs, għaldaqstant l-Istati Membri li jużaw ġerarkija tal-CA f'diversi livelli (pereżempju, Root CA -> CSCA -> DSCs) iridu jipprovdu l-awtorità taċ-ċertifikazzjoni subordinarja li toħroġ id-DSCs. F'dan il-każ, jekk Stat Membru juża awtorità taċ-ċertifikazzjoni eżistenti, allura s-sistema tad-DCC se tinjora kwalunkwe ħaġa 'l fuq mis-CSCA u tqis biss bħala whitelist is-CSCA bħala l-ankra ta' fiduċja (anki jekk din tkun CA subordinat). Dan hu bħall-mudell tal-ICAO, li jippermetti biss eżattament 2 livelli – "root" CSCA u "leaf" DSC – iffirmati minn dik is-CSCA biss.

Jekk Stat Membru jkun jopera s-CSCA tiegħu stess, l-Istat Membru jkun responsabbli għall-operazzjoni sigura u għall-ġestjoni tal-kjavi ta' din is-CA. Is-CSCA taġixxi bħala l-ankra ta' fiduċja għad-DSCs, u għalhekk il-protezzjoni tal-kjavi privata tas-CSCA hi essenzjali għall-integrità tal-ambjent tad-DCC. Il-mudell ta' verifika fid-DCC PKI hu l-mudell primarju, li jiddikjara li ċ-ċertifikati kollha fil-validazzjoni tal-mogħdija taċ-ċertifikat iridu jkunu validi fi żmien partikolari (jiġifieri l-ħin tal-validazzjoni tal-firma). Għalhekk, japplikaw ir-restrizzjonijiet li ġejjin:

— Is-CSCA m'għandhiex toħroġ ċertifikati li huma validi għal aktar żmien miċ-ċertifikat CA nnifsu;

— Il-firmatur tad-dokument m'għandux jiffirma dokumenti li jkunu validi għal aktar tul mid-DSC innifsu;

— L-Istati Membri li joperaw is-CSCA tagħhom stess iridu jiddefinixxu l-perjodi ta' validità għas-CSCA tagħhom u għaċ-ċertifikati kollha maħruġa u jridu jieħdu ħsieb it-tiġdid taċ-ċertifikati.

It-*Taqsima 4.2* fiha rakkomandazzjonijiet għall-perjodi ta' validità.

3.3. *Integrità u awtenticità tad-data mtellgħa*

Il-backends nazzjonali jistgħu jużaw id-DCCG biex itellgħu u jniżżlu pakketti ta' *data* ffirmati b'mod diġitali wara awtentikazzjoni reċiproka b'suċċess. Fil-bidu, dawn il-pakketti ta' *data* jkollhom id-DSCs tal-Istati Membri. Il-par kjavi li jintuża mill-backend nazzjonali għall-firma diġitali ta' pakketti tad-*data* mtellgħin fis-sistema tad-DCCG jissejjaħ il-par kjavi tal-firma tal-upload tal-backend nazzjonali u ċ-ċertifikat tal-kjavi pubblika korrispondenti huwa mqassar bħala ċertifikat NB_{UP}. Kull Stat Membru jġib iċ-ċertifikat NB_{UP} tiegħu stess, li jista' jiġi ffirmat minnu stess, jew jinħareġ minn awtorità taċ-ċertifikazzjoni eżistenti, bħal awtorità taċ-ċertifikazzjoni pubblika (jiġifieri awtorità taċ-ċertifikazzjoni li toħroġ ċertifikat f'konformità mar-rekwiżiti bażiċi tal-Forum CAB). Iċ-ċertifikat NB_{UP} għandu jkun differenti minn kwalunkwe ċertifikat ieħor użat mill-Istat Membru (jiġifieri CSCA, klijent tat-TLS jew DSCs).

L-Istati Membri jridu jipprovdu ċ-ċertifikat għall-upload lill-operatur tad-DCCG waqt il-proċedura ta' reġistrazzjoni inizjali (*ara t-Taqsima 4.1 għal aktar dettalji*). Kull Stat Membru hu responsabbli għad-*data* nazzjonali tiegħu u jrid jipproteġi l-kjavi privata li tintuża għall-iffirmar tal-uploads.

Stati Membri oħra jistgħu jivverifikaw il-pakketti tad-*data* ffirmati billi jużaw iċ-ċertifikati mtellgħin li huma pprovduti mid-DCCG. Id-DCCG jivverifika l-awtenticità u l-integrità tad-*data* mtellgħa maċ-ċertifikat imtella' tan-NB qabel ma tiġi pprovduta lil Stati Membri oħra.

3.4. *Rekwiżiti dwar l-arkitettura teknika tad-DCCG*

Ir-rekwiżiti dwar l-arkitettura teknika tad-DCCG huma kif ġej:

— Id-DCCG juża l-awtentikazzjoni ta' TLS reċiproka biex jistabbilixxi konnessjoni kriptata awtentikata mal-NBs. Għalhekk, id-DCCG iżomm whitelist taċ-ċertifikati tal-klijenti reġistrati NB_{TLS};

— Id-DCCG juża żewġ ċertifikati diġitali ($DCCG_{TLS}$ u $DCCG_{TA}$) b'żewġ pari kjavi distinti. Il-kjavi privata tal-par kjavi tad-$DCCG_{TA}$ tinżamm offline (mhux fuq il-komponenti online tad-DCCG);

— Id-DCCG iżomm lista ta' fiduċja taċ-ċertifikati NB_{CSCA} li hija ffirmata bil-kjavi privata tad-$DCCG_{TA}$;

— Iċ-ċifri li jintużaw iridu jissodisfaw ir-rekwiżiti mit-*Taqsima 5.1*.

4. Ġestjoni taċ-Ċiklu tal-ħajja taċ-Ċertifikat

4.1. *Ir-reġistrazzjoni tal-Backends Nazzjonali*

L-Istati Membri jridu jirreġistraw mal-operatur tad-DCCG biex jieħdu sehem fis-sistema tad-DCCG. Din it-taqsima tiddeskrivi l-proċedura teknika u operazzjonali li trid tiġi segwita għar-reġistrazzjoni ta' backend nazzjonali.

L-operatur tad-DCCG u l-Istat Membru jridu jiskambjaw informazzjoni dwar persuni tekniċi ta' kuntatt għall-proċess ta' onboarding. Hu preżunt li l-persuni tekniċi ta' kuntatt ikunu leġittimati mill-Istati Membri tagħhom u l-identifikazzjoni/l-awtentikazzjoni titwettaq b'mezzi oħra. Pereżempju, l-awtentikazzjoni tista' tinkiseb meta l-kuntatt tekniku tal-Istati Membri jipprovdi ċ-ċertifikati bħala fajls kriptati b'password permezz tal-email u jikkondividi l-password korrispondenti mal-operatur tad-DCCG permezz tat-telefown. Jistgħu jintużaw ukoll mezzi siguri oħra definiti mill-operatur tad-DCCG.

L-Istat Membru jrid jipprovdi tliet ċertifikati diġitali waqt il-proċess ta' reġistrazzjoni u identifikazzjoni:

— Iċ-ċertifikat tat-TLS tal-Istat Membru NB_{TLS}

— Iċ-ċertifikat imtella' tal-Istat Membru NB_{UP}

— Iċ-ċertifikat(i) tas-CSCA tal-Istat Membru NB_{CSCA}

Iċ-ċertifikati kollha pprovduti jridu jaderixxu mar-rekwiżiti definiti fit-*Taqsima 5*. L-operatur tad-DCCG jivverifika li ċ-ċertifikat ipprovdut jaderixxi mar-rekwiżiti tat-*Taqsima 5*. Wara l-identifikazzjoni u r-reġistrazzjoni, l-operatur tad-DCCG:

— iżid iċ-ċertifikat(i) tan-NB_{CSCA} fil-lista ta' fiduċja ffirmata bil-kjavi privata li tikkorrispondi għall-kjavi pubblika tad-$DCCG_{TA}$;

— iżid iċ-ċertifikat tan-NB_{TLS} fil-whitelist tal-punt ta' tmiem tat-TLS tad-DCCG;

— iżid iċ-ċertifikat tan-NB_{UP} fis-sistema tad-DCCG;

— jipprovdi ċ-ċertifikat tal-kjavi pubblika tad-$DCCG_{TA}$ u tad-$DCCG_{TLS}$ lill-Istat Membru.

4.2. *L-awtoritajiet taċ-ċertifikazzjoni, il-perjodi ta' validità u t-tiġdid*

F'każ li Stat Membru jkun irid jopera s-CSCA tiegħu stess, iċ-ċertifikati tas-CSCA jistgħu jkunu ċertifikati awtoffirmati. Huma jaġixxu bħala l-ankra ta' fiduċja tal-Istat Membru u għalhekk l-Istat Membru jrid jipproteġi bil-qawwa l-kjavi privata li tikkorrispondi għall-kjavi pubblika taċ-ċertifikat tas-CSCA. Hu rakkomandat li l-Istati Membri jużaw sistema offline għas-CSCA tagħhom, jiġifieri sistema tal-kompjuter li mhix konnessa ma' xi network. Kontroll ta' aktar minn persuna waħda għandu jintuża għall-aċċess tas-sistema (pereżempju, il-prinċipju ta' erba' għajnejn). Wara l-iffirmar tad-DSCs, għandhom jiġu applikati kontrolli operazzjonali, u s-sistema bil-kjavi privata tas-CSCA għandha tinħażen b'mod sikur b'kontrolli tal-aċċess sodi. Moduli tas-Sigurtà tal-Hardware jew Smart Cards jistgħu jintużaw biex jipproteġu ulterjorment il-kjavi privata tas-CSCA. Iċ-ċertifikati diġitali fihom perjodu ta' validità li jinforza t-tiġdid taċ-ċertifikat. It-tiġdid huwa meħtieġ biex jintużaw kjavi kriptografiċi ġodda u biex jiġu adattati d-daqsijiet tal-kjavi meta titjib ġdid fil-komputazzjoni jew attakki ġodda jheddu s-sigurtà tal-algoritmu kriptografiku użat. Japplika l-mudell primarju (ara t-*Taqsima 3.2*).

Il-perjodi ta' validità li ġejjin huma rakkomandati, meta wieħed iqis il-validità ta' sena għaċ-ċertifikati COVID diġitali:

— CSCA: 4 snin

— DSC: sentejn

— Upload: sena-sentejn

— Awtentikazzjoni tal-klijent tat-TLS: sena-sentejn

Għal tiġdid fil-ħin, huma rakkomandati l-perjodi ta' użu li ġejjin għall-kjavi privati:

— CSCA: sena

— DSC: sitt xhur

L-Istati Membri jridu joħolqu ċertifikati ġodda għall-upload u ċertifikati tat-TLS f'ħin regolari, pereżempju, xahar qabel l-iskadenza biex tkun tista' ssir operazzjoni bla xkiel. Jenħtieġ li ċ-ċertifikati tas-CSCA u d-DSCs jiġġeddu mill-inqas xahar qabel ma jintemm l-użu tal-kjavi privata (b'kunsiderazzjoni tal-proċeduri operazzjonali meħtieġa). L-Istati Membri jridu jipprovdu ċertifikati tas-CSCA, ċertifikati tal-upload u ċertifikati tat-TLS aġġornati lill-operatur tad-DCCG. Ċertifikati skaduti għandhom jitneħħew mill-whitelist u mil-lista ta' fiduċja.

L-Istati Membri u l-operatur tad-DCCG iridu jżommu rendikont tal-validità taċ-ċertifikati tagħhom stess. Mhemm l-ebda entità ċentrali li żżomm rekord tal-validità taċ-ċertifikati u li tinforma lill-parteċipanti.

4.3. *Revoka taċ-ċertifikati*

B'mod ġenerali, iċ-ċertifikati diġitali jistgħu jiġu revokati mill-CA tal-ħruġ tagħhom bl-użu ta' listi ta' revoka taċ-ċertifikati jew permezz ta' Risponder tal-Protokoll tal-Istatus taċ-Ċertifikat Online (OCSP). Is-CSCAs għas-sistema tad-DCC jenħtieġ jipprovdu listi ta' revoka taċ-ċertifikati (CRLs). Anke jekk dawn is-CRLs bħalissa mhumiex użati minn Stati Membri oħra, dawn jenħtieġ jiġu integrati għal applikazzjonijiet futuri. Jekk CSCA tiddeċiedi li ma tipprovdix CRLs, id-DSCs ta' din is-CSCA iridu jiġġeddu meta s-CRLs isiru obbligatorji. Il-verifikaturi jenħtieġ ma jużawx l-OCSP għall-validazzjoni tad-DSCs u jenħtieġ jużaw is-CRLs. Hu rakkomandat li l-backend nazzjonali jwettaq il-validazzjoni meħtieġa tad-DCCs li jitniżżlu mill-Gateway tad-DCC u jibgħat biss sett ta' DSC fdati u validati lill-validaturi nazzjonali tad-DCC. Jenħtieġ li l-validaturi tad-DCC ma jwettqu l-ebda verifika ta' revoka fuq id-DSC fil-proċess ta' validazzjoni tagħhom. Waħda mir-raġunijiet għal dan hi biex titħares il-privatezza tad-detenturi tad-DCC billi tiġi evitata kull possibbiltà li l-użu ta' xi DSC partikolari jiġi monitorjat mir-rispondent assoċjat tiegħu tal-OCSP.

L-Istati Membri jistgħu jneħħu d-DSCs tagħhom mid-DCCG waħedhom bl-użu ta' ċertifikati validi tal-upload u tat-TLS. It-tneħħija ta' DSC tfisser li d-DCCs kollha maħruġa b'dan id-DSC se jsiru invalidi meta l-Istati Membri jfittxu l-listi aġġornati tad-DSCs. Il-protezzjoni tal-materjal ta' kjavi privata li jikkorrispondi għad-DSCs hi kruċjali. L-Istati Membri jridu jinfurmaw lill-operatur tad-DCCG meta huma jkunu jridu jirrevokaw iċ-ċertifikati tal-upload jew tat-TLS, pereżempju minħabba kompromess fil-backend nazzjonali. L-operatur tad-DCCG imbagħad jista' jneħħi l-fiduċja għaċ-ċertifikat affettwat, pereżempju billi jneħħi dan mill-whitelist tat-TLS. L-operatur tad-DCCG jista' jneħħi ċ-ċertifikati mtellgħin mill-bażi tad-*data* tad-DCCG. Il-pakketti ffirmati bil-kjavi privata li jikkorrispondu għal dan iċ-ċertifikat imtella' se jsiru invalidi meta l-backends nazzjonali jneħħu l-fiduċja taċ-ċertifikat revokat imtella'. F'każ li ċ-ċertifikat tas-CSCA irid jiġi revokat, l-Istati Membri għandhom jinformaw lill-operatur tad-DCCG kif ukoll lil Stati Membri oħra li jkollhom relazzjonijiet ta' fiduċja magħhom. L-operatur tad-DCCG joħroġ lista ta' fiduċja ġdida fejn iċ-ċertifikat affettwat ma jibqax fiha. Id-DSCs kollha maħruġa minn din is-CSCA isiru invalidi meta l-Istati Membri jaġġornaw il-maħżen ta' fiduċja tal-backend nazzjonali tagħhom. F'każ li ċ-ċertifikat tad-$DCCG_{TLS}$ jew iċ-ċertifikat tad-$DCCG_{TA}$ iridu jiġu revokati, l-operatur tad-DCCG u l-Istati Membri jridu jaħdmu flimkien biex jistabbilixxu konnessjoni ta' TLS affidabbli ġdida u lista ta' fiduċja.

5. **Mudelli taċ-Ċertifikati**

Din it-taqsima tistabbilixxi rekwiżiti kriptografiċi u gwida kif ukoll rekwiżiti dwar il-mudelli taċ-ċertifikati. Għaċ-ċertifikati tad-DCCG, din it-taqsima tiddefinixxi l-mudelli taċ-ċertifikati.

5.1. *Rekwiżiti kriptografiċi*

L-algoritmi kriptografiċi u s-settijiet ta' ċifraturi tat-TLS għandhom jintgħażlu abbażi tar-rakkomandazzjoni attwali mill-Uffiċċju Federali Ġermaniż għas-Sigurtà tal-informazzjoni (BSI) jew is-SOG-IS. Dawn ir-rakkomandazzjonijiet u r-rakkomandazzjonijiet ta' istituzzjonijiet oħrajn u ta' organizzazzjoni tal-istandardizzazzjoni huma simili. Ir-rakkomandazzjonijiet jistgħu jinstabu fil-linji gwida tekniċi TR 02102-1 u TR 02102-2 ([1]) jew fil-Mekkaniżmi Kriptografiċi Miftiehma mal-SOG-IS ([2]).

5.1.1. Rekwiżiti dwar id-DSC

Għandhom japplikaw ir-rekwiżiti previsti fit-*Taqsima 3.2.2 tal-Anness I*. Għalhekk, hu rakkomandat ħafna li l-Firmatarji tad-Dokumenti jużaw l-Algoritmu tal-Firma Diġitali b'Kurvi Ellittiċi (ECDSA) bl-NIST-p-256 (kif definit fl-appendiċi D tal-FIPS PUB 186-4). Kurvi ellittiċi oħrajn ma humiex appoġġati. Minħabba r-restrizzjonijiet ta' spazju tad-DCC, jenħtieġ li l-Istati Membri ma jużawx l-RSA-PSS, anki jekk dan ikun permess bħala algoritmu li

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

jintuża f'każ ta' bżonn. F'każ li l-Istati Membri jużaw RSA-PSS, jenħtieġ li jużaw daqs ta' modulus ta' 2048 jew ta' massimu ta' 3072 bit. SHA-2 b'tul tal-output ta' ≥ 256 bits għandu jintuża bħala funzjoni ta' hash kriptografika (ara ISO/IEC 10118-3:2004) għall-firma tad-WLTP.

5.1.2. Rekwiżiti dwar iċ-ċertifikati tat-TLS, tal-Upload u tas-CSCA

Għaċ-ċertifikati diġitali u l-firem kriptografiċi fil-kuntest tad-DCCG, ir-rekwiżiti ewlenin dwar l-algoritmi kriptografiċi u t-tul tal-kjavi huma miġbura fil-qosor fit-tabella li ġejja (mill-2021):

Algoritmu tal-Firma	Tul tal-Kjavi	Funzjoni hash
EC-DSA	Min. 250 bit	SHA-2 b'tul tal-output ≥ 256 Bit
RSA-PSS (padding rakkomandat) RSA-PKCS#1 v1.5 (padding legat)	Min. 3000 bit RSA Modulus (N) b'esponent pubbliku e > 2^16	SHA-2 b'tul tal-output ≥ 256 Bit
DSA	Min. 3000 Bit prime p, 250 Bit key q	SHA-2 b'tul tal-output ≥ 256 Bit

Il-kurva ellittika rakkomandata għall-EC-DSA hija NIST-p-256 minħabba l-implimentazzjoni mifruxa tagħha.

5.2. *ĊERTIFIKAT TAS-CSCA (NB_{CSCA})*

It-tabella li ġejja tagħti gwida dwar il-mudell taċ-ċertifikat tan-NB_{CSCA} jekk Stat Membru jiddeċiedi li jopera s-CSCA tiegħu stess għas-sistema tad-DCC.

Huma meħtieġa entrati **b'tipa grassa** (iridu jiġu inklużi fiċ-ċertifikat), huma rakkomandati entrati bil-*korsiv* (jenħtieġ li jiġu inklużi). Għall-entrati neqsin, mhi definita l-ebda rakkomandazzjoni.

Entrata	Valur
Suġġett	**cn=<mhux vojt u isem komuni uniku>**, *o=<Fornitur>*,**c=<Stat Membru li jopera s-CSCA>**
Użu tal-kjavi	**iffirmar taċ-ċertifikat,***iffirmar tal-CRL* (bħala minimu)
Restrizzjonijet bażiċi	**CA = limitazzjonijiet fit-tul tal-mogħdija, veri = 0**

L-isem tas-suġġett irid ikun mhux vojt u uniku fl-Istat Membru speċifikat. Il-kodiċi tal-pajjiż (c) irid jaqbel mal-Istat Membru li se juża dan iċ-ċertifikat tas-CSCA. Iċ-ċertifikat irid ikun fih identifikatur tal-kjavi tas-suġġett uniku (SKI) skont l-RFC 5280 ([3]).

5.3. *Ċertifikat tal-Firmatarju tad-Dokument (DSC)*

It-tabella li ġejja tipprovdi gwida dwar id-DSC. Huma meħtieġa entrati b'**tipa grassa** (iridu jiġu inklużi fiċ-ċertifikat), huma rakkomandati entrati bil-*korsiv* (jenħtieġ li jiġu inklużi). Għall-entrati neqsin, mhi definita l-ebda rakkomandazzjoni.

Entrata	Valur
Numru tas-serje	**numru tas-serje uniku**
Suġġett	**cn=<mhux vojt u isem komuni uniku>**, o=<Fornitur>, **c=<Stat Membru li juża dan id-DSC>**
Użu tal-kjavi	**firma diġitali** (bħala minimu)

([3]) rfc5280 (ietf.org)

Id-DSC irid jiġi ffirmat bil-kjavi privata li tikkorrispondi għal ċertifikat tas-CSCA li jintuża mill-Istat Membru.

Għandhom jintużaw l-estensjonijiet li ġejjin:

— Iċ-ċertifikat irid ikun fih Identifikatur tal-Kjavi tal-Awtorità (AKI) li jaqbel mal-Identifikatur tal-Kjavi tas-Suġġett (SKI) taċ-ċertifikat tas-CSCA tal-ħruġ

— Iċ-ċertifikat jenħtieġ li jkun fih Identifikatur tal-Kjavi tas-Suġġett uniku (skont l-RFC 5280 ([4]))

Barra minn hekk, iċ-ċertifikat jenħtieġ li jkun fih l-estensjoni tal-punt ta' distribuzzjoni tas-CRL li tipponta lejn il-lista ta' revoka taċ-ċertifikati (CRL) li hija pprovduta mis-CSCA li tkun ħarġet id-DSC.

Id-DSC jista' jkun fih estensjoni estiża tal-użu tal-kjavi b'żero jew aktar identifikaturi tal-politika dwar l-użu tal-kjavi li jillimitaw it-tipi ta' HCERTs li dan iċ-ċertifikat huwa permess jivverifika. Jekk ikun hemm preżenti wieħed jew aktar, il-verifikaturi għandhom jivverifikaw l-użu tal-kjavi kontra l-HCERT maħżun. Għal dan, huma definiti l-valuri extendedKeyUsage li ġejjin:

Entrata	Valur
extendedKeyUsage	1.3.6.1.4.1.1847.2021.1.1 għall-Emittenti tat-Test
extendedKeyUsage	1.3.6.1.4.1.1847.2021.1.2 għall-Emittenti tat-Tilqim
extendedKeyUsage	1.3.6.1.4.1.1847.2021.1.3 għall-Emittenti tal-Fejqan

Fin-nuqqas ta' kwalunkwe estensjoni tal-użu tal-kjavi (jiġifieri ebda estensjoni jew żero estensjonijiet), dan iċ-ċertifikat jista' jintuża biex jivvalida kwalunkwe tip ta' HCERT. Dokumenti oħrajn jistgħu jiddefinixxu identifikaturi addizzjonali tal-politika dwar l-użu estiż tal-kjavi rilevanti użati mal-validazzjoni tal-HCERTs.

5.4. *Ċertifikati Mtellgħin (NBUP)*

It-tabella li ġejja tipprovdi gwida għall-upload taċ-ċertifikat fil-backend nazzjonali. Huma meħtieġa entrati b'**tipa grassa** (iridu jiġu inklużi fiċ-ċertifikat), huma rakkomandati entrati bil-*korsiv* (jenħtieġ li jiġu inklużi). Għall-entrati neqsin, mhi definita l-ebda rakkomandazzjoni.

Entrata	Valur
Suġġett	**cn=<mhux vojt u isem komuni uniku>**, *o=<Fornitur>*, **c=<Stat Membru li juża din l-upload taċ-ċertifikat>**
Użu tal-kjavi	**firma diġitali** (bħala minimu)

5.5. *Awtentikazzjoni tal-klijent tat-TLS għall-backend nazzjonali (NB_{TLS})*

It-tabella li ġejja tipprovdi gwida għaċ-ċertifikat ta' awtentikazzjoni tal-klijent tat-TLS għall-backend nazzjonali. Huma meħtieġa entrati b'**tipa grassa** (iridu jiġu inklużi fiċ-ċertifikat), huma rakkomandati entrati bil-*korsiv* (jenħtieġ li jiġu inklużi). Għall-entrati neqsin, mhi definita l-ebda rakkomandazzjoni.

Entrata	Valur
Suġġett	cn=<mhux vojt u isem komuni uniku>, o=<Fornitur>, c=<Stat Membru fuq in-NB>
Użu tal-kjavi	**firma diġitali** (bħala minimu)
Użu estiż tal-Kjavi	**awtentikazzjoni tal-klijent (1.3.6.1.5.5.7.3.2)**

([4]) rfc5280 (ietf.org)

Iċ-ċertifikat jista' jkun fih ukoll l-*awtentikazzjoni tas-server* (*1.3.6.1.5.5.7.3.1*) tal-użu tal-kjavi estiż, iżda dan ma huwiex obbligatorju.

5.6. *Ċertifikat tal-firma tal-lista ta' fiduċja (DCCG$_{TA}$)*

It-tabella li ġejja tiddefinixxi ċ-ċertifikat ta' Ankra ta' Fiduċja tad-DCCG.

Entrata	Valur
Suġġett	**cn = Gateway taċ-Ċertifikat Ekoloġiku Diġitali** ([5])**, o=<Fornitur>, c=<pajjiż>**
Użu tal-kjavi	**firma diġitali** (bħala minimu)

5.7. *Ċertifikati tat-TLS Server tad-DCCG (DCCG$_{TLS}$)*

It-tabella li ġejja tiddefinixxi ċ-ċertifikat TLS tad-DCCG.

Entrata	Valur
Suġġett	cn=<FQDN jew l-indirizz IP tad-DCCG>, o=<Fornitur>, c=<pajjiż>
SubjectAltName	dNSName: <DCCG DNS isem> jew indirizzIP: <Indirizz IP ta' DCCG>
Użu tal-kjavi	**firma diġitali** (bħala minimu)
Użu Estiż tal-Kjavi	**awtentikazzjoni tas-server (1.3.6.1.5.5.7.3.1**)

Iċ-ċertifikat jista' jkun fih ukoll l-*awtentikazzjoni tal-klijent (1.3.6.1.5.5.7.3.2*) għall-użu tal-kjavi estiż, iżda dan ma huwiex obbligatorju.

Iċ-ċertifikat tat-TLS tad-DCCG għandu jinħareġ minn awtorità taċ-ċertifikazzjoni fdata pubblikament (inkluż fil-browsers ewlenin kollha u fis-sistemi operattivi, skont ir-rekwiżiti tal-linja bażi tal-Forum CAB).

([5]) It-terminoloġija taċ-"Ċertifikat Ekoloġiku Diġitali" minflok iċ-"Ċertifikat COVID Diġitali tal-UE" inżammet f'dan il-kuntest minħabba li din hija t-terminoloġija li ġiet hardcoded u użata fiċ-ċertifikat qabel ma l-koleġiżlaturi ddeċidew fuq terminoloġija ġdida.