DECIZIA DE PUNERE ÎN APLICARE (UE) 2021/1073 A COMISIEI

din 28 iunie 2021

de stabilire a specificațiilor tehnice și a regulilor de punere în aplicare a cadrului de încre dere pentru certificatul digital al UE privind COVID instituit prin Regulamentul (UE) 2021/953 al Parlamentului European și al Consiliului

(Text cu relevanță pentru SEE)

COMISIA EUROPEANĂ,

având în vedere Tratatul privind funcționarea Uniunii Europene,

având în vedere Regulamentul (UE) 2021/953 al Parlamentului European și al Consiliului privind cadrul pentru eliberarea, verificarea și acceptarea certificatelor interoperabile de vaccinare, testare și vindecare de COVID-19 (certificatul digital al UE privind COVID) pentru a facilita libera circulație pe durata pandemiei de COVID-19 ([1]), în special articolul 9 alineatele (1) și (3),

întrucât:

(1) Regulamentul (UE) 2021/953 instituie certificatul digital al UE privind COVID, al cărui scop este să servească drept dovadă a faptului că o persoană a fost vaccinată împotriva COVID-19, a obținut un rezultat negativ la testul pentru depistarea bolii sau s-a vindecat de COVID-19.

(2) Pentru ca certificatul digital al UE privind COVID să fie operațional în întreaga Uniune, trebuie stabilite specificații tehnice și reguli care să asigure completarea, eliberarea în condiții de siguranță și verificarea certificatelor digitale privind COVID, garantarea protecției datelor cu caracter personal, stabilirea structurii comune a identificatorului unic al certificatului și emiterea unui cod de bare valabil, securizat și interoperabil. Acest cadru de încredere stabilește, de asemenea, premisele pentru eforturile de asigurare a interoperabilității cu standardele și sistemele tehnologice internaționale și, ca atare, ar putea servi drept model de cooperare la nivel mondial.

(3) Capacitatea de a citi și interpreta certificatul digital al UE privind COVID presupune o structură de date comună și un consens asupra semnificației preconizate a fiecărui câmp de date al sarcinii utile și asupra valorilor pe care le poate lua. Pentru a facilita această interoperabilitate, trebuie definită o structură comună coordonată a datelor pentru cadrul de funcționare a certificatului digital al UE privind COVID. Orientările pentru acest cadru au fost elaborate de rețeaua de e-sănătate instituită pe baza Directivei 2011/24/UE a Parlamentului European și a Consiliului ([2]). La elaborarea specificațiilor tehnice care stabilesc formatul și gestionarea cadrului de încredere pentru certificatul digital al UE privind COVID ar trebui să se țină cont de orientările respective. Ar trebui prevăzute o specificație privind structura datelor și mecanisme de codare, precum și un mecanism de codare pentru transport într-un format optic care poate fi citit automat (QR), afișabil pe ecranul unui dispozitiv mobil sau imprimabil pe hârtie.

(4) În plus față de specificațiile tehnice pentru formatul și gestionarea cadrului de încredere ale certificatului digital al UE privind COVID, ar trebui stabilite reguli generale privind completarea certificatelor, care să fie utilizate pentru valorile codate din conținutul certificatului digital al UE privind COVID. Seturile de valori prin care sunt puse în aplicare regulile în cauză ar trebui să fie actualizate și publicate periodic de către Comisie, pe baza activității relevante a rețelei de e-sănătate.

(5) În conformitate cu Regulamentul (UE) 2021/953, certificatele autentice care alcătuiesc certificatul digital al UE privind COVID ar trebui să poată fi identificate individual prin intermediul unui identificator unic al certificatului, ținând seama de faptul că cetățenilor li se pot elibera mai multe certificate în perioada în care este în vigoare Regulamentul (UE) 2021/953. Identificatorul unic al certificatului va fi alcătuit dintr-o serie alfanumerică, iar statele membre ar trebui să garanteze că acesta nu conține date care să îl raporteze la alte documente sau la alți identificatori, cum ar fi numărul pașaportului sau al cărții de identitate, pentru a se evita identificarea titularului. Pentru a se asigura că identificatorul certificatului este unic, ar trebui stabilite specificații tehnice și reguli pentru structura comună a acestuia.

([1]) JO L 211, 15.6.2021, p. 1.

([2]) Directiva 2011/24/UE a Parlamentului European și a Consiliului din 9 martie 2011 privind aplicarea drepturilor pacienților în cadrul asistenței medicale transfrontaliere (JO L 88, 4.4.2011, p. 45).

(6) Securitatea, autenticitatea, valabilitatea și integritatea certificatelor care alcătuiesc certificatul digital al UE privind COVID și conformitatea acestora cu legislația Uniunii privind protecția datelor sunt esențiale pentru ca aceste certificate să fie acceptate în toate statele membre. Obiectivele menționate sunt realizate prin intermediul cadrului de încredere, care stabilește regulile și infrastructura pentru emiterea și verificarea fiabilă și sigură a certificatelor digitale ale UE privind COVID. Printre altele, cadrul de încredere ar trebui să se bazeze pe o infrastructură de chei publice cu un lanț de încredere mergând de la autoritățile din domeniul sănătății sau alte autorități de încredere din statele membre până la entitățile individuale care eliberează certificatele digitale ale UE privind COVID. Prin urmare, pentru a se asigura un sistem de interoperabilitate la nivelul întregii UE, Comisia a constituit un sistem central – gateway-ul pentru certificatele digitale ale UE privind COVID („gateway-ul") – care stochează cheile publice utilizate pentru verificare. Atunci când se scanează codul QR al certificatului, se verifică semnătura digitală cu ajutorul cheii publice relevante, stocată în prealabil pe acest gateway central. Pentru a se asigura integritatea și autenticitatea datelor, se pot utiliza semnăturile digitale. Infrastructurile de chei publice creează relații de încredere prin asocierea anumitor chei publice cu anumiți emitenți de certificate. În cadrul gateway-ului se utilizează, pentru autenticitate, mai multe certificate de cheie publică. Pentru a se asigura un schimb securizat de date având ca obiect materialul-cheie pentru cheile publice între statele membre și pentru a permite o interoperabilitate largă, este necesar să se stabilească certificatele de cheie publică ce pot fi utilizate și să se prevadă modul în care ar trebui generate acestea.

(7) Prezenta decizie permite operaționalizarea cerințelor Regulamentului (UE) 2021/953 într-un mod care să reducă la minimum prelucrarea datelor cu caracter personal, limitând-o la ceea ce este necesar pentru ca certificatul digital al UE privind COVID să devină operațional și să contribuie la punerea în aplicare de către operatorii finali astfel încât să se respecte protecția datelor încă din faza de proiectare.

(8) În conformitate cu Regulamentul (UE) 2021/953, autoritățile sau alte organisme desemnate responsabile cu eliberarea certificatelor sunt operatorii menționați la articolul 4 alineatul (7) din Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului ([3]), în rolul lor de prelucrare a datelor cu caracter personal în cursul procesului de eliberare a certificatelor. În funcție de modul în care statele membre organizează acest proces de eliberare a certificatelor, pot exista una sau mai multe autorități sau organisme desemnate, de exemplu serviciile de sănătate regionale. În conformitate cu principiul subsidiarității, această decizie este la latitudinea statelor membre. Prin urmare, în cazul în care există mai multe autorități sau alte organisme desemnate, statele membre sunt cele mai în măsură să se asigure că responsabilitățile fiecăreia sunt clar alocate, indiferent dacă este vorba de operatori separați sau asociați (inclusiv serviciile de sănătate regionale care instituie un portal comun al pacienților pentru eliberarea certificatelor). În mod similar, în ceea ce privește verificarea certificatelor de către autoritățile competente din statul membru de destinație sau de tranzit ori de către operatorii de servicii de transport transfrontalier de călători obligați prin legislația națională să pună în aplicare anumite măsuri de sănătate publică în timpul pandemiei de COVID-19, acești verificatori trebuie să își respecte obligațiile care le revin în temeiul normelor privind protecția datelor.

(9) Prin intermediul gateway-ului pentru certificatele digitale ale UE privind COVID nu se realizează nicio prelucrare a datelor cu caracter personal, întrucât acest gateway conține doar cheile publice ale autorităților semnatare. Aceste chei sunt legate de autoritățile semnatare și nu permit reidentificarea, directă sau indirectă, a unei persoane fizice căreia i s-a eliberat un certificat. Prin urmare, în calitatea sa de administrator al gateway-ului, Comisia nu ar trebui să fie nici operator, nici operator de date cu caracter personal.

(10) Autoritatea Europeană pentru Protecția Datelor, care a fost consultată în conformitate cu articolul 42 alineatul (1) din Regulamentul (UE) 2018/1725 al Parlamentului European și al Consiliului ([4]), a emis un aviz la data de 22 iunie 2021.

(11) Având în vedere că, pentru aplicarea Regulamentului (UE) 2021/953 începând de la 1 iulie 2021, sunt necesare specificații tehnice și reguli, se justifică aplicarea imediată a prezentei decizii.

(12) Prin urmare, având în vedere necesitatea punerii rapide în aplicare a certificatului digital al UE privind COVID, prezenta decizie ar trebui să intre în vigoare la data publicării sale,

([3]) Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor) (JO L 119, 4.5.2016, p. 1).

([4]) Regulamentul (UE) 2018/1725 al Parlamentului European și al Consiliului din 23 octombrie 2018 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal de către instituțiile, organele, oficiile și agențiile Uniunii și privind libera circulație a acestor date și de abrogare a Regulamentului (CE) nr. 45/2001 și a Deciziei nr. 1247/2002/CE (JO L 295, 21.11.2018, p. 39).

ADOPTĂ PREZENTA DECIZIE:

Articolul 1

Specificațiile tehnice pentru certificatul digital al UE privind COVID care stabilesc structura datelor generice, mecanismele de codare și mecanismul de codare pentru transport într-un format optic care poate fi citit automat sunt stabilite în anexa I.

Articolul 2

Regulile de completare a certificatelor menționate la articolul 3 alineatul (1) din Regulamentul (UE) 2021/953 sunt stabilite în anexa II la prezenta decizie.

Articolul 3

Cerințele care stabilesc structura comună a identificatorului unic al certificatului sunt stabilite în anexa III.

Articolul 4

Normele de guvernanță aplicabile certificatelor de chei publice în legătură cu gateway-ul pentru certificatul digital al UE privind COVID care sprijină aspectele de interoperabilitate ale cadrului de încredere sunt prevăzute în anexa IV.

Prezenta decizie intră în vigoare la data publicării în *Jurnalul Oficial al Uniunii Europene*.

Adoptată la Bruxelles, 28 iunie 2021.

Pentru Comisie
Președintele
Ursula VON DER LEYEN

ANEXA I

FORMATUL ȘI GESTIONAREA CADRULUI DE ÎNCREDERE

Structura datelor generice, mecanismele de codare și mecanismul de codare pentru transport într-un format optic care poate fi citit automat (denumit în continuare „QR”)

1. Introducere

Specificațiile tehnice stabilite în prezenta anexă conțin o structură a datelor generice și mecanisme de codare pentru certificatul digital al UE privind COVID („DCC”). Acestea specifică, de asemenea, un mecanism de codare pentru transport într-un format optic care poate fi citit automat („QR”) și care poate fi afișat pe ecranul unui dispozitiv mobil sau imprimat. Formatele container ale certificatului de sănătate electronic aferente specificațiilor menționate sunt generice, dar, în acest context, sunt utilizate pentru a purta DCC.

2. Terminologie

În sensul prezentei anexe, „emitenți” înseamnă organismele care utilizează aceste specificații pentru emiterea certificatelor de sănătate și „verificatori” înseamnă organismele care acceptă certificatele de sănătate ca dovadă a stării de sănătate. „Participanți” înseamnă emitenții și verificatorii. Unele aspecte prevăzute în prezenta anexă, cum ar fi gestionarea unui spațiu de nume și distribuirea cheilor de criptare, trebuie să facă obiectul coordonării între participanți. Se presupune că una dintre părți, denumită în continuare „secretariatul”, îndeplinește aceste sarcini.

3. Formatul container al certificatului de sănătate electronic

Formatul container al certificatului de sănătate electronic (*Electronic Health Certificate Container Format* – HCERT) este conceput pentru a asigura un vehicul uniform și standardizat pentru certificatele de sănătate eliberate de diferiți emitenți („emitenții”). Obiectivul prezentelor specificații este de a armoniza modul în care certificatele de sănătate sunt reprezentate, codate și semnate, cu scopul de a facilita interoperabilitatea.

Capacitatea de a citi și interpreta un DCC, indiferent care este emitentul său, necesită o structură de date comună și ajungerea la un acord cu privire la semnificația fiecărui câmp de date al sarcinii utile. Pentru a facilita o astfel de interoperabilitate, se definește o structură de date comună coordonată, prin utilizarea unei scheme JSON (*JavaScript Object Notation* – notarea obiectelor în JavaScript), care constituie cadrul DCC.

3.1. *Structura sarcinii utile*

Sarcina utilă este structurată și codată sub formă de CBOR (*Concise Binary Object Representation* – reprezentarea concisă a obiectelor binare), cu o semnătură digitală în formatul COSE (*CBOR Object Signing and Encryption* – semnarea și criptarea de obiecte utilizând CBOR). Aceasta este cunoscută sub denumirea de „token web CBOR” (CWT) și este definită în RFC 8392 ([1]). Sarcina utilă, astfel cum este definită în secțiunile următoare, este transportată într-o revendicare hcert.

Integritatea și autenticitatea originii datelor privind sarcina utilă trebuie să poată fi verificate de verificator. Pentru a furniza acest mecanism, emitentul trebuie să semneze CWT utilizând un sistem asimetric de semnătură electronică, astfel cum este definit în specificația privind COSE (RFC 8152 ([2])).

3.2. *Revendicări CWT*

3.2.1. Prezentare generală a structurii CWT

Antet protejat

— Algoritmul de semnătură (alg, eticheta 1)

— Identificatorul cheii (kid, eticheta 4)

Sarcină utilă

— Emitentul (iss, cheia de revendicare 1, opțional, ISO 3166-1 alpha-2 al emitentului)

— Emis la (iat, cheia de revendicare 6)

— Momentul expirării (exp, cheia de revendicare 4)

— Certificatul de sănătate (hcert, cheia de revendicare -260)

— Certificatul digital al UE privind COVID v1 (eu_DCC_v1, cheia de revendicare 1)

Semnătură

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

3.2.2. Algoritmul de semnătură

Parametrul algoritmului de semnătură (alg) indică algoritmul care a fost utilizat pentru crearea semnăturii. Acesta trebuie să respecte sau chiar să depășească orientările actuale ale SOG-IS (*Senior Officials Group Information Systems Security* – Grupul înalților funcționari pentru securitatea sistemelor informatice), astfel cum sunt rezumate în paragrafele următoare.

Se definesc un algoritm primar și unul secundar. Algoritmul secundar ar trebui utilizat numai în cazul în care algoritmul primar nu este acceptabil conform normelor și reglementărilor impuse emitentului.

Pentru a asigura securitatea sistemului, ar trebui ca toate punerile în aplicare să includă algoritmul secundar. Din acest motiv, trebuie aplicat atât algoritmul primar, cât și cel secundar.

Nivelurile stabilite de SOG-IS pentru algoritmul primar și pentru cel secundar sunt următoarele:

— Algoritmul primar: algoritmul primar este algoritmul de semnătură digitală bazat pe curbe eliptice (*Elliptic Curve Digital Signature Algorithm* – ECDSA), astfel cum este definit în secțiunea 2.3 din (ISO/IEC 14888-3: 2006), utilizând parametrii P-256 definiți în apendicele D (D.1.2.3) la (FIPS PUB 186-4), în combinație cu algoritmul de distribuire (*hash*) SHA-256, astfel cum este definit în funcția 4 din (ISO/IEC 10118-3: 2004).

Acesta corespunde parametrului ES256 al algoritmului COSE.

— Algoritmul secundar: algoritmul secundar este RSASSA-PSS, astfel cum este definit în (RFC 8230 ([3])), cu un modul de 2048 biți, în combinație cu algoritmul de distribuire (*hash*) SHA-256, astfel cum este definit în funcția 4 din (ISO/IEC 10118-3: 2004).

Acesta corespunde algoritmului COSE, parametrul PS256.

3.2.3. Identificatorul cheii

Revendicarea privind identificatorul cheii (kid) indică certificatul de semnatar de documente (DSC) care conține cheia publică pe care verificatorul trebuie să o utilizeze atunci când verifică dacă semnătura digitală este corectă. Guvernanța certificatelor de cheie publică, inclusiv cerințele pentru DSC-uri, este descrisă în anexa IV.

Revendicarea privind identificatorul cheii (kid) este utilizată de verificatori pentru selectarea cheii publice corecte dintr-o listă de chei aferente emitentului indicat în revendicarea privind emitentul (iss). Un emitent poate utiliza în paralel mai multe chei, din motive administrative și atunci când efectuează reînnoirea cheilor. Identificatorul cheii nu este un câmp critic din punctul de vedere al securității. Din acest motiv, el poate fi plasat și într-un antet neprotejat, dacă este necesar. Verificatorii trebuie să accepte ambele opțiuni. În cazul în care sunt prezente ambele opțiuni, trebuie utilizat identificatorul cheii din antetul protejat.

Din cauza scurtării identificatorului (din motive de limitare a dimensiunii), există o șansă redusă, dar nu egală cu zero, ca lista globală a DSC-urilor (*Document Signer Certificates* – certificate ale semnatarilor de documente) acceptate de un verificator să conțină DSC-uri cu același kid. Din acest motiv, verificatorul trebuie să verifice toate DSC-urile cukid-ul respectiv.

3.2.4. Emitent

Revendicarea privind emitentul (iss) este o valoare de tip șir care poate conține codul de țară ISO 3166-1 alpha-2 al entității care eliberează certificatul de sănătate. Această revendicare poate fi utilizată de un verificator pentru a identifica setul de DSC-uri care urmează să fie utilizate pentru verificare. Pentru a identifica această revendicare se utilizează cheia de revendicare 1.

3.2.5. Momentul expirării

Revendicarea privind momentul expirării (exp) trebuie să conțină o marcă temporală în formatul de tip număr întreg NumericDate (astfel cum se specifică în RFC 8392 ([4]), secțiunea 2), care indică perioada de valabilitate a acestei semnături specifice asupra sarcinii utile, după încheierea căreia verificatorul trebuie să respingă sarcina utilă ca fiind expirată. Scopul parametrului de expirare este de a impune o limită la perioada de valabilitate a certificatului de sănătate. Pentru a identifica această revendicare se utilizează cheia de revendicare 4.

Momentul expirării nu trebuie să depășească perioada de valabilitate a DSC.

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

3.2.6. Emis la

Revendicarea „emis la” (iat) trebuie să conțină o marcă temporală în formatul de tip număr întreg NumericDate (astfel cum se specifică în RFC 8392 ([5]), secțiunea 2), indicând momentul în care a fost creat certificatul de sănătate.

Câmpul „emis la” nu trebuie să conțină o dată anterioară perioadei de valabilitate a DSC.

Verificatorii pot să aplice și alte politici cu scopul de a limita valabilitatea certificatului de sănătate în funcție de momentul emiterii. Pentru a identifica această revendicare se utilizează cheia de revendicare 6.

3.2.7. Revendicarea privind certificatul de sănătate

Revendicarea privind certificatul de sănătate (hcert) este un obiect JSON (RFC 7159 ([6])) care conține informații privind starea de sănătate. În cadrul aceleiași revendicări pot exista mai multe tipuri de certificate de sănătate, printre care și DCC.

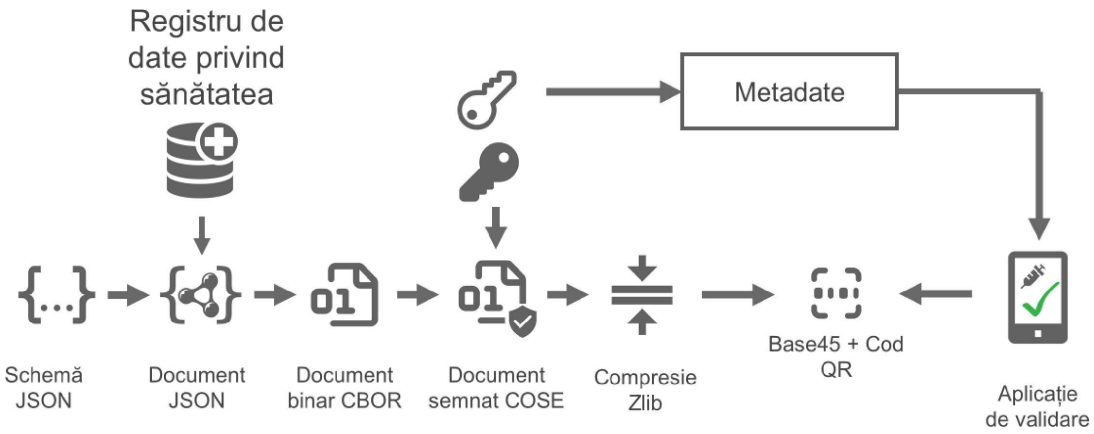
Formatul JSON este utilizat exclusiv pentru scheme. Formatul de reprezentare este CBOR, astfel cum este definit în (RFC 7049 ([7])). Este posibil ca, în realitate, dezvoltatorii de aplicații să nu decodeze sau să codeze niciodată în și din format JSON, ci să utilizeze în schimb structura integrată în memorie.

Pentru a identifica această revendicare se utilizează cheia de revendicare -260.

Șirurile din obiectul JSON ar trebui normalizate în conformitate cu forma de normalizare NFC (*Normalization Form Canonical Composition* - forma de normalizare cu compunere canonică) definită în standardul Unicode. Cu toate acestea, aplicațiile de decodare ar trebui să fie permisive și robuste în aceste privințe, iar acceptarea oricărui tip de conversie rezonabilă este puternic încurajată. În cazul în care, în timpul decodării sau în funcțiile de comparare ulterioară, se descoperă date nenormalizate, punerile în aplicare ar trebui să se comporte ca și cum datele de intrare ar fi normalizate pentru NFC.

4. **Serializarea și crearea sarcinii utile a DCC**

Ca model de serializare, se utilizează următoarea schemă:



Procesul începe cu extragerea de date, de exemplu, dintr-un registru de date privind sănătatea (sau dintr-o sursă de date externă), structurând datele extrase în conformitate cu schemele DCC definite. În acest proces, conversia în formatul de date definit și transformarea pentru a permite lizibilitatea umană pot avea loc înainte de începerea serializării în format CBOR. Acronimele revendicărilor trebuie puse în corespondență, în fiecare caz, cu denumirile de afișare înainte de serializare și după deserializare.

Conținutul opțional de date naționale nu este permis în certificatele eliberate în conformitate cu Regulamentul (UE) nr. 2021/953 ([8]). Conținutul datelor se limitează la elementele de date definite în setul minim de date specificat în anexa la Regulamentul 2021/953.

([5]) rfc8392 (ietf.org)
([6]) rfc7159 (ietf.org)
([7]) rfc7049 (ietf.org)
([8]) Regulamentul (UE) 2021/953 al Parlamentului European și al Consiliului din 14 iunie 2021 privind cadrul pentru eliberarea, verificarea și acceptarea certificatelor interoperabile de vaccinare, testare și vindecare de COVID-19 (certificatul digital al UE privind COVID) pentru a facilita libera circulație pe durata pandemiei de COVID-19, JO L 211, 15.6.2021, p. 1.

5. **Codările pentru transport**

5.1. *Forma brută*

Pentru interfețele de date arbitrare, formatul container al certificatului HCERT și sarcinile sale utile pot fi transferate ca atare, utilizând orice tip de transport de date subiacent sigur și fiabil cu 8 biți. Interfețele respective pot include comunicarea în câmp apropiat (*Near-Field Communication* – NFC), Bluetooth sau transfer prin intermediul unui protocol privind nivelul de aplicație, de exemplu transferul unui certificat HCERT de la emitent către dispozitivul mobil al unui titular.

În cazul în care transferul certificatului HCERT de la emitent către titular se bazează pe o interfață exclusiv de prezentare (de exemplu, SMS sau e-mail), codarea pentru transport brută nu este, în mod evident, aplicabilă.

5.2. *Codul de bare*

5.2.1. Compresia sarcinii utile (CWT)

Pentru a reduce dimensiunea și a îmbunătăți viteza și fiabilitatea procesului de citire a certificatelor HCERT, CWT trebuie comprimat utilizând formatul ZLIB (RFC 1950 ([9])) și mecanismul de compresie *Deflate*, în formatul definit în RFC 1951 ([10]).

5.2.2. Codul de bare QR 2D

Pentru a gestiona mai bine echipamentele tradiționale concepute să funcționeze pe sarcini utile ASCII (*American Standard Code for Information Interchange* – Codul standard american pentru schimbul de informații), CWT comprimat este codificat ca ASCII cu ajutorul schemei de codare Base45, înainte de a fi codat într-un cod de bare 2D.

Pentru generarea de coduri de bare 2D trebuie utilizat formatul QR, astfel cum este definit în (ISO/IEC 18004:2015). Se recomandă o rată de corecție a erorilor egală cu „Q” (de aproximativ 25 %). Deoarece se utilizează Base45, codul QR trebuie să utilizeze codarea alfanumerică (modul 2, indicat de simbolurile 0010).

Pentru ca verificatorii să poată detecta tipul de date codate și să selecteze schema corespunzătoare de decodare și prelucrare, datele codate cu ajutorul schemei de codare Base45 (în conformitate cu prezenta specificație) trebuie să fie precedate de identificatorul de context sub formă de șir „HC1:”. Versiunile viitoare ale prezentei specificații de natură să afecteze compatibilitatea inversă vor defini un nou identificator de context, iar caracterul care urmează după literele „HC” trebuie selectat din setul de caractere [1-9A-Z]. Ordinea incrementelor este definită în această ordine, și anume mai întâi [1-9] și apoi [A-Z].

Se recomandă ca, în cadrul mediului de prezentare, codul optic să aibă o diagonală cuprinsă între 35 mm și 60 mm, pentru a permite utilizarea de cititoare cu elemente optice fixe pentru care mediul de prezentare trebuie amplasat pe suprafața cititorului.

În cazul în care codul optic este imprimat pe hârtie cu ajutorul unei imprimante cu rezoluție mică (< 300 dpi), trebuie să se acorde atenție reprezentării cu precizie a fiecărui simbol (punct) al codului QR, astfel încât acesta să aibă formă pătrată. Scalarea neproporțională va face ca unele rânduri sau coloane din QR să aibă simboluri dreptunghiulare, ceea ce, în multe cazuri, va afecta lizibilitatea.

6. **Formatul listelor de încredere (lista CSCA și lista DSC)**

Fiecare stat membru trebuie să furnizeze o listă cuprinzând una sau mai multe autorități naționale de certificare pentru semnătură (CSCA) și o listă a tuturor certificatelor de semnatar de documente (DSC) în termen de valabilitate, și să asigure actualizarea acestor liste.

6.1. *CSCA/DSC simplificate*

Începând cu versiunea curentă a specificațiilor, statele membre nu trebuie să pornească de la prezumția că informațiile din lista certificatelor revocate (CRL) sunt utilizate sau că perioada de utilizare a cheii private este verificată de către entitățile care asigură punerea în aplicare.

În schimb, mecanismul principal de verificare a perioadei de valabilitate este prezența certificatului pe cea mai recentă versiune a respectivei liste de certificate.

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

6.2. *Documentul de călătorie electronic cu citire optică (eMRTD) și certificatul de cheie publică PKI ale Organizației Aviației Civile Internaționale (OACI) și centrele de încredere*

Statele membre pot utiliza o CSCA separată, dar pot, de asemenea, să transmită certificatele eMRTD emise de CSCA existentă și/sau DSC-urile deja existente și pot alege chiar să achiziționeze certificate de la centre de încredere (comerciale) și să le transmită. Cu toate acestea, orice DSC trebuie să fie întotdeauna semnat de CSCA prezentată de statul membru respectiv.

7. **Considerente de securitate**

Atunci când proiectează o schemă care utilizează această specificație, statele membre trebuie să identifice, să analizeze și să monitorizeze anumite aspecte legate de securitate.

Trebuie luate în considerare cel puțin următoarele aspecte:

7.1. *Perioada de valabilitate a semnăturii certificatelor HCERT*

Emitentul certificatului HCERT trebuie să limiteze perioada de valabilitate a semnăturii prin specificarea momentului la care expiră semnătura. Prin urmare, titularul unui certificat de sănătate este obligat să îl reînnoiască periodic.

Perioada de valabilitate acceptabilă poate fi determinată de constrângeri practice. De exemplu, este posibil ca un călător să nu aibă posibilitatea de a-și reînnoi certificatul de sănătate în timpul unei călătorii în străinătate. Cu toate acestea, se poate întâmpla, de asemenea, ca un emitent să ia în considerare posibilitatea ca securitatea să fie compromisă, emitentul fiind nevoit să retragă un DSC (invalidând toate certificatele de sănătate eliberate cu ajutorul cheii respective care sunt încă valabile). Consecințele unui astfel de eveniment pot fi limitate prin reînnoirea periodică a cheilor emitenților și prin impunerea reînnoirii tuturor certificatelor de sănătate într-un interval rezonabil.

7.2. *Gestionarea cheilor*

Prezenta specificație se bazează în mare măsură pe mecanisme criptografice solide, menite să asigure integritatea datelor și autentificarea originii datelor. Prin urmare, este necesar să se mențină confidențialitatea cheilor private.

Confidențialitatea cheilor criptografice poate fi compromisă în mai multe moduri, de exemplu:

— procesul de generare a cheilor poate fi defectuos, având ca rezultat chei slabe;

— cheile pot fi expuse din cauza unei erori umane;

— cheile pot fi furate de infractori externi sau interni.

— cheile pot fi calculate cu ajutorul criptanalizei.

Pentru a atenua riscurile de a se constata că algoritmul de semnare este slab și permite compromiterea cheilor prin criptanaliză, prezenta specificație recomandă ca toți participanții să aplice un algoritm de semnătură secundar, de rezervă, bazat pe parametri diferiți sau pe o problemă matematică diferită față de cea pentru algoritmul primar.

În ceea ce privește riscurile menționate legate de mediile de operare ale emitenților, trebuie puse în aplicare măsuri de atenuare care să asigure un control eficace, astfel încât să se genereze, să se stocheze și să se utilizeze cheile private din modulele de securitate hardware (HSM). Se încurajează puternic utilizarea modulelor HSM pentru semnarea certificatelor de sănătate.

Indiferent dacă un emitent decide să utilizeze sau nu modulele HSM, ar trebui stabilit un calendar de reînnoire a cheilor care să prevadă o frecvență a reînnoirii cheilor proporțională cu expunerea cheilor la rețele externe, la alte sisteme și la personal. Un calendar de reînnoire bine ales limitează, totodată, riscurile asociate certificatelor de sănătate eliberate în mod eronat, prin faptul că îi permite unui emitent să revoce aceste certificate de sănătate pe loturi, prin retragerea unei chei, dacă acest lucru se dovedește necesar.

7.3. *Validarea datelor de intrare*

Prezentele specificații pot fi utilizate într-un mod care implică primirea de date din surse nefiabile în sisteme care pot fi esențiale pentru îndeplinirea misiunii stabilite. Pentru a reduce la minimum riscurile asociate acestui vector de atac, toate câmpurile de intrare trebuie să fie validate în mod corespunzător, în funcție de tipul, lungimea și conținutul datelor. Înainte de prelucrarea conținutului certificatului HCERT, trebuie verificată, de asemenea, semnătura emitentului. Cu toate acestea, validarea semnăturii emitentului implică analizarea prealabilă a antetului protejat al emitentului, în care un potențial atacator poate încerca să introducă informații atent formulate, concepute pentru a compromite securitatea sistemului.

8. **Gestionarea încrederii**

Semnătura certificatului HCERT necesită o cheie publică pentru a fi verificată. Statele membre trebuie să pună la dispoziție aceste chei publice. În ultimă instanță, fiecare verificator trebuie să aibă o listă a tuturor cheilor publice în care este dispus să aibă încredere (având în vedere faptul că o cheie publică nu face parte din certificatul HCERT).

Sistemul este format din (numai) două niveluri: pentru fiecare stat membru, unul sau mai multe certificate la nivel de țară, fiecare dintre acestea servind la semnarea unuia sau a mai multor certificate de semnatar de documente, care sunt utilizate în operațiunile zilnice.

Certificatele statelor membre se numesc certificate ale autorităților naționale de certificare pentru semnătură (CSCA) și sunt (de regulă) certificate autosemnate. Un stat membru poate avea mai multe astfel de certificate (de exemplu, în cazul deconcentrării regionale). Aceste certificate CSCA semnează periodic certificatele de semnatar de documente (DSC) utilizate pentru semnarea certificatelor HCERT.

„Secretariatul" este un rol funcțional. Acesta trebuie să agrege și să publice periodic DSC-urile statelor membre, după ce verifică dacă acestea se regăsesc în lista certificatelor CSCA (care au fost transmise și verificate prin alte mijloace).

Lista de certificate DSC rezultată trebuie să furnizeze apoi setul agregat de chei publice acceptabile (și kid-urile corespunzătoare) pe care verificatorii le pot utiliza pentru a valida semnăturile pentru certificatele HCERT. Verificatorii trebuie să obțină și să actualizeze această listă în mod regulat.

Aceste liste specifice fiecărui stat membru pot fi adaptate în formatul corespunzător situației existente la nivel național. Din acest motiv, formatul fișierului acestei liste de încredere poate varia, de exemplu, poate fi un JWKS semnat (format pentru seturi de chei web JSON conform RFC 7517 ([11]) secțiunea 5) sau orice alt format specific tehnologiei utilizate în statul membru respectiv.

Pentru a asigura simplitatea, statele membre pot fie să își transmită certificatele CSCA existente din sistemele lor eMRTD conforme cu normele OACI, fie, în conformitate cu recomandările OMS, să creeze un certificat specific pentru acest domeniu al sănătății.

8.1. *Identificatorul cheii (kid)*

Identificatorul cheii (kid) se calculează atunci când se elaborează lista cheilor publice de încredere pe baza certificatelor DSC și constă într-o amprentă digitală SHA-256 trunchiată (primii 8 byți) a DSC, codificată în format DER (brut).

Verificatorii nu trebuie să calculeze kid-ul pe baza certificatului DSC; ei pot corela direct identificatorul cheii din certificatul de sănătate emis cu kid-ul de pe lista de încredere.

8.2. *Diferențe față de modelul de încredere eMRTD PKI al OACI*

Deși se bazează pe cele mai bune practici ale modelului de încredere eMRTD PKI al OACI, din motive de rapiditate, în prezenta specificație trebuie efectuate o serie de simplificări:

— Un stat membru poate prezenta mai multe certificate CSCA.

— Perioada de valabilitate a DSC (utilizarea cheii) poate fi stabilită la orice durată, atât timp cât aceasta nu depășește certificatul CSCA, și poate să lipsească.

— DSC poate să conțină identificatori ai politicilor (utilizarea extinsă a cheii) care sunt specifici certificatelor de sănătate.

— Statele membre pot alege să nu efectueze niciodată verificări ale revocărilor publicate și să se bazeze exclusiv pe listele DSC pe care le primesc zilnic de la secretariat sau le compilează ele însele.

([11]) rfc7517 (ietf.org)

ANEXA II

REGULI DE COMPLETARE A CERTIFICATULUI DIGITAL AL UE PRIVIND COVID

Regulile generale privind seturile de valori stabilite în prezenta anexă au scopul de a asigura interoperabilitatea la nivel semantic și trebuie să permită punerea în aplicare tehnică uniformă pentru DCC. Elementele cuprinse în prezenta anexă pot fi utilizate pentru cele trei contexte diferite (vaccinare/testare/vindecare), astfel cum se prevede în Regulamentul (UE) 2021/953. Numai elementele pentru care este necesară standardizarea semantică prin seturi de valori codate sunt enumerate în prezenta anexă.

Responsabilitatea pentru traducerea elementelor codate în limba națională le revine statelor membre.

Pentru toate câmpurile de date care nu sunt menționate în următoarele descrieri ale seturilor de valori, se recomandă codarea în format UTF-8 (nume, centru de testare, emitentul certificatului). Se recomandă codificarea câmpurilor de date care conțin date calendaristice (data nașterii, data vaccinării, data prelevării probei testate, data primului rezultat pozitiv al testului, datele corespunzătoare perioadei de valabilitate a certificatului) în conformitate cu standardul ISO 8601.

În cazul în care, dintr-un motiv oarecare, nu pot fi utilizate sistemele de coduri preferate enumerate mai jos, pot fi utilizate alte sisteme de coduri internaționale și ar trebui elaborate recomandări privind punerea în corespondență a codurilor din celelalte sisteme de coduri cu sistemul de coduri preferat. Textul (denumirile de afișare) poate fi utilizat, în cazuri excepționale, ca mecanism de rezervă, atunci când în seturile de valori definite nu este disponibil niciun cod adecvat.

Statele membre care utilizează alte coduri în sistemele lor ar trebui să pună în corespondență aceste coduri cu seturile de valori descrise. Statele membre sunt responsabile pentru orice astfel de puneri în corespondență.

Seturile de valori trebuie actualizate periodic de către Comisie, cu sprijinul rețelei de e-sănătate și al Comitetului pentru securitate sanitară. Seturile de valori actualizate trebuie publicate pe site-ul relevant al Comisiei, precum și pe pagina web a rețelei de e-sănătate. Ar trebui furnizat un istoric al modificărilor.

1. **Boala sau agentul vizat/boala sau agentul de care s-a vindecat titularul: COVID-19 (SARS-CoV-2 sau una dintre variantele sale)**

   Sistemul de coduri preferat: SNOMED CT.

   A se utiliza în certificatele 1, 2 și 3.

   Codurile selectate trebuie să menționeze COVID-19 sau, în cazul în care sunt necesare informații mai detaliate privind varianta genetică a SARS-CoV-2, varianta respectivă, dacă aceste informații detaliate sunt necesare din motive epidemiologice.

   Un exemplu de cod care ar trebui utilizat este codul SNOMED CT 840539006 (COVID-19).

2. **Vaccinul împotriva COVID-19 sau metodele profilactice împotriva COVID-19**

   Sistemul de coduri preferat: SNOMED CT sau clasificarea ATC (anatomică, terapeutică și chimică).

   A se utiliza în certificatul 1.

   Exemple de coduri care ar trebui utilizate din sistemele de coduri preferate sunt codul SNOMED CT 1119305005 (vaccin antigenic împotriva SARS-CoV-2), 1119349007 (vaccin de tip ARNm împotriva SARS-CoV-2) sau J07BX03 (vaccinuri împotriva COVID-19). Setul de valori ar trebui extins atunci când se dezvoltă și se introduc noi tipuri de vaccinuri.

3. **Medicamentul reprezentând vaccinul împotriva COVID-19**

   Sistemele de coduri preferate (în ordinea preferințelor):

   — Registrul UE al medicamentelor reprezentând vaccinuri autorizate la nivelul întregii UE (numerele autorizațiilor)

   — Un registru mondial al vaccinurilor, precum cel care ar putea fi instituit de Organizația Mondială a Sănătății

   — Denumirea medicamentului reprezentând vaccinul în alte cazuri. Dacă denumirea include spații albe, acestea ar trebui înlocuite cu o cratimă (-).

Denumirea setului de valori: vaccin.

A se utiliza în certificatul 1.

Din sistemul de coduri preferat, un exemplu de cod care ar trebui utilizat este EU/1/20/1528 (Comirnaty). Un exemplu de denumire a vaccinului care poate fi utilizată drept cod: Sputnik-V (pentru Sputnik V).

4. **Deținătorul autorizației de comercializare sau producătorul vaccinului împotriva COVID-19**

Sistemul de coduri preferat:

— Codul organizației furnizat de Agenția Europeană pentru Medicamente (sistemul SPOR pentru ISO IDMP)

— Un registru mondial al deținătorilor de autorizații de comercializare sau al producătorilor de vaccinuri, precum cel care ar putea fi instituit de Organizația Mondială a Sănătății

— Denumirea organizației, în celelalte cazuri. Dacă denumirea include spații albe, acestea ar trebui înlocuite cu o cratimă (-).

A se utiliza în certificatul 1.

Din sistemul de coduri preferat, un exemplu de cod care ar trebui utilizat este ORG-100001699 (AstraZeneca AB). Un exemplu de denumire a organizației care poate fi utilizată drept cod: Sinovac-Biotech (pentru Sinovac Biotech).

5. **Numărul dintr-o serie de doze, precum și numărul total de doze din serie**

A se utiliza în certificatul 1.

Două câmpuri:

(1) numărul de doze administrate într-un ciclu

(2) numărul de doze preconizate pentru un ciclu complet (specific fiecărei persoane la momentul administrării)

De exemplu, 1/1, 2/2 înseamnă că ciclul este complet; la fel și opțiunea 1/1 pentru vaccinurile care includ două doze, dar pentru care protocolul aplicat de statul membru este de a administra o singură doză cetățenilor care au fost diagnosticați cu COVID-19 înainte de vaccinare. Numărul total de doze dintr-o serie ar trebui indicat conform informațiilor disponibile la momentul administrării dozei. De exemplu, dacă un anumit vaccin necesită o a treia doză (rapel), trebuie ca, în momentul în care se administrează ultima doză, al doilea număr al câmpului să reflecte acest lucru (de exemplu 2/3, 3/3 etc.).

6. **Statul membru sau țara terță în care s-a administrat vaccinul/s-a efectuat testul**

Sistemul de coduri preferat: codurile ISO 3166 ale țărilor.

A se utiliza în certificatele 1, 2 și 3.

Conținutul setului de valori: lista completă a codurilor de 2 litere, disponibilă ca set de valori definit în FHIR (*Fast Healthcare Interoperability Resources* – resurse rapide de interoperabilitate în domeniul sănătății) (http://hl7.org/fhir/ValueSet/iso3166-1-2)

7. **Tipul testului**

Sistemul de coduri preferat: LOINC.

A se utiliza în certificatul 2 și în certificatul 3 în cazul în care se introduce, printr-un act delegat, posibilitatea de a elibera certificate de vindecare pe baza altor tipuri de teste decât NAAT (*nucleic acid amplification technique* – tehnica amplificării acidului nucleic).

Codurile din acest set de valori trebuie să facă referire la metoda de realizare a testului și trebuie selectate astfel încât să asigure cel puțin distincția dintre testele NAAT și testele RAT (testele antigenice rapide), astfel cum se prevede în Regulamentul (UE) 2021/953.

Din sistemul de coduri preferat, un exemplu de cod care ar trebui utilizat este LP217198-3 (*Rapid immunoassay* – test imunologic rapid).

8. **Producătorul și denumirea comercială a testului utilizat (opționale pentru testul NAAT)**

Sistemul de coduri preferat: lista de teste antigenice rapide a Comitetului pentru securitate sanitară, gestionată de JRC (baza de date despre dispozitivele și metodele de testare in vitro vizând diagnosticarea COVID-19).

A se utiliza în certificatul 2.

Setului de valori trebuie să includă selectarea testului antigenic rapid, astfel cum este menționat în lista comună actualizată a testelor antigenice rapide pentru COVID-19, stabilită pe baza Recomandării 2021/C 24/01 a Consiliului și aprobată de Comitetul pentru securitate sanitară. Lista este actualizată de JRC în baza de date despre dispozitivele și metodele de testare in vitro vizând diagnosticarea COVID-19, la adresa: https://covid-19-diagnostics.jrc.ec.europa.eu/devices/hsc-common-recognition-rat

Pentru acest sistem de coduri, trebuie să se utilizeze câmpuri relevante precum identificatorul dispozitivului de testare, denumirea testului și a producătorului, în formatul structurat al JRC, disponibil la adresa https://covid-19-diagnostics.jrc.ec.europa.eu/devices

9. **Rezultatul testului**

Sistemul de coduri preferat: SNOMED CT.

A se utiliza în certificatul 2.

Codurile selectate trebuie să permită distincția între rezultatele pozitive și cele negative ale testelor (detectat sau nedetectat). Se pot adăuga și alte valori (de exemplu, nedeterminat) dacă pe parcursul utilizării apar cazuri care impun acest lucru.

Din sistemul de coduri preferat, exemplele de coduri care ar trebui utilizate sunt 260415000 (nedetectat) și 260373001 (detectat).

ANEXA III

STRUCTURA COMUNĂ A IDENTIFICATORULUI UNIC AL CERTIFICATULUI

1. **Introducere**

Fiecare certificat digital al UE privind COVID (DCC) trebuie să includă un identificator unic al certificatului (UCI) care asigură interoperabilitatea DCC-urilor. UCI poate fi utilizat pentru a verifica certificatul. Responsabilitatea punerii în aplicare a UCI le revine statelor membre. Identificatorul UCI este un mijloc de verificare a veridicității certificatului și, după caz, de conectare la un sistem de înregistrare (de exemplu, un sistem de informații privind imunizarea). De asemenea, acești identificatori trebuie să le permită statelor membre să ateste (pe suport de hârtie și în format digital) că persoanele au fost vaccinate sau testate.

2. **Compoziția identificatorului unic al certificatului**

Identificatorul UCI trebuie să urmeze o structură și un format comune care facilitează interpretabilitatea informațiilor de către om și/sau mașină și care se pot referi la elemente precum statul membru de vaccinare, vaccinul în sine și un identificator specific pentru fiecare stat membru. UCI asigură faptul că statele membre dispun de flexibilitate în ceea ce privește configurarea sa, cu respectarea deplină a legislației privind protecția datelor. Ordinea elementelor separate urmează o ierarhie definită care poate permite modificări viitoare ale componentelor, menținând în același timp integritatea structurală a identificatorului.

Soluțiile posibile pentru compoziția UCI formează un spectru în cadrul căruia modularitatea și interpretabilitatea umană reprezintă cei doi parametri principali de diversificare și o caracteristică fundamentală:

— Modularitatea: măsura în care codul este format din componente distincte care conțin informații diferite din punct de vedere semantic

— Interpretabilitatea umană: măsura în care codul este semnificativ sau poate fi interpretat de cititorul uman

— Unic la nivel mondial; identificatorul țării sau al autorității este bine gestionat și se preconizează că fiecare țară (autoritate) își va gestiona în mod corespunzător segmentul din spațiul de nume, fără să recurgă vreodată la reciclarea sau reemiterea identificatorilor. Combinația dintre aceste elemente asigură faptul că fiecare identificator este unic la nivel mondial.

3. **Cerințe generale**

Următoarele cerințe generale ar trebui să fie îndeplinite în ceea ce privește identificatorul UCI:

(1) setul de caractere: sunt permise numai caracterele alfanumerice US-ASCII majuscule (de la „A” la „Z”, de la „0” la „9”), cu caractere speciale suplimentare pentru separare în conformitate cu RFC3986 ([1]) ([2]), și anume {„/”, „#”, „:”};

(2) lungimea maximă: proiectanții ar trebui să își propună ca obiectiv o lungime de 27-30 de caractere ([3]);

(3) prefixul versiunii: acesta se referă la versiunea schemei UCI. Prefixul versiunii este „01” pentru prezenta versiune a documentului; prefixul versiunii este compus din două cifre;

(4) prefixul țării: codul de țară este specificat în ISO 3166-1. Codurile mai lungi [de exemplu, de 3 caractere și mai mult (de exemplu, „UNHCR”)] sunt rezervate pentru o utilizare viitoare;

(5) Sufixul codului/suma de verificare.

5.1. Statele membre ar trebui să utilizeze o sumă de verificare atunci când este probabil să apară erori de transmisie, de transcriere (umană) sau alte tipuri de deteriorare a datelor (cu alte cuvinte, atunci când sunt utilizate în format tipărit).

5.2. Suma de verificare nu trebuie să fie utilizată pentru validarea certificatului și nu face parte, din punct de vedere tehnic, din identificator, ci este utilizată pentru a verifica integritatea codului. Această sumă de verificare ar trebui să fie rezumatul conform standardului ISO-7812-1 (LUHN-10) ([4]) al întregului UCI în format digital/de reprezentare a datelor în vederea transportului. Suma de verificare este separată de restul UCI printr-un caracter „#”.

([1]) rfc3986 (ietf.org)

([2]) Este posibil ca anumite câmpuri precum sexul, numărul lotului, centrul de administrare, identificarea personalului medico-sanitar, data următoarei vaccinări să nu fie necesare decât în scopuri medicale.

([3]) Pentru punerea în aplicare cu coduri QR, statele membre ar putea lua în considerare un set suplimentar de caractere, cu o lungime totală de până la 72 de caractere (inclusiv cele 27-30 ale identificatorului propriu-zis) pentru a transmite alte informații. Precizarea acestor informații ține de competența statelor membre.

([4]) Algoritmul Luhn mod N este o extensie a algoritmului Luhn (cunoscut și sub denumirea de algoritm mod 10) care funcționează pentru coduri numerice și este utilizat, de exemplu, pentru calcularea sumei de verificare a cardurilor de credit. Extensia îi permite algoritmului să funcționeze cu secvențe de valori în orice bază (în cazul nostru, caractere alfa).

Ar trebui să se asigure compatibilitatea inversă: statele membre care schimbă, în timp, structura identificatorilor lor (în versiunea principală, stabilită în prezent ca fiind v1) trebuie să se asigure că doi identificatori identici reprezintă același certificat/mențiune de vaccinare. Cu alte cuvinte, statele membre nu pot recicla identificatorii.

4. **Opțiuni privind identificatorii unici ai certificatului pentru certificatele de vaccinare**

Orientările rețelei de e-sănătate privind certificatele verificabile de vaccinare și elementele de interoperabilitate de bază ([5]) prevăd diferite opțiuni aflate la dispoziția statelor membre și a altor părți care pot coexista între diferitele state membre. Statele membre pot introduce astfel de opțiuni diferite în diferite versiuni ale schemei UCI.

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

ANEXA IV

GUVERNANȚA CERTIFICATELOR CU CHEIE PUBLICĂ

1. **Introducere**

Schimbul securizat și fiabil de chei de semnătură pentru certificatele digitale ale UE privind COVID (DCC) între statele membre este realizat cu ajutorul Gateway-ului pentru certificatele digitale ale UE privind COVID (DCCG), care funcționează ca un registru central pentru cheile publice. Prin intermediul DCCG, statele membre sunt împuternicite să publice cheile publice corespunzătoare cheilor private pe care le utilizează pentru a semna certificatele digitale privind COVID. Statele membre care se bazează pe DCCG pot utiliza portalul pentru a obține în timp util materiale actualizate privind cheile publice. Ulterior, DCCG poate fi extins pentru a face schimb de informații suplimentare fiabile furnizate de statele membre, cum ar fi normele de validare pentru DCC-uri. Modelul de încredere al cadrului DCC este o infrastructură de chei publice (*Public Key Infrastructure* – PKI). Fiecare stat membru deține una sau mai multe autorități naționale de certificare pentru semnătură (CSCA), ale căror certificate au o durată de viață relativ lungă. În funcție de decizia statului membru, CSCA poate fi aceeași cu CSCA utilizată pentru documentele de călătorie care pot fi citite automat sau poate fi diferită. CSCA emite certificate de cheie publică pentru semnatarii de documente naționale cu durată scurtă de viață (și anume, semnatarii pentru DCC-uri), care sunt denumite certificate de semnatar de documente (DSC). CSCA acționează ca o ancoră de încredere, care le permite statelor membre care se bazează pe aceasta să utilizeze certificatul CSCA pentru a valida autenticitatea și integritatea DSC-urilor, care suferă modificări periodice. Odată ce validarea a fost efectuată, statele membre pot folosi aceste certificate (sau doar cheile publice pe care le conțin) pentru aplicațiile lor de validare a DCC. Pe lângă CSCA și DSC, DCCG se bazează, de asemenea, pe infrastructurile de chei publice (PKI) pentru autentificarea tranzacțiilor, semnarea datelor, ca bază pentru autentificare și ca mijloc de asigurare a integrității canalelor de comunicare dintre statele membre și DCCG.

Semnăturile digitale pot fi utilizate pentru a se asigura integritatea și autenticitatea datelor. Infrastructurile de chei publice creează încredere prin asocierea obligatorie a unor chei publice cu anumite identități verificate (sau emitenți verificați). Acest lucru este necesar pentru a le permite celorlalți participanți să verifice originea datelor și identitatea partenerului de comunicare și să decidă dacă pot avea încredere în acestea. În cadrul DCCG se utilizează mai multe certificate de cheie publică pentru autenticitate. Prezenta anexă definește certificatele de cheie publică utilizate și modul în care acestea trebuie concepute astfel încât să permită o interoperabilitate largă între statele membre. Aceasta oferă mai multe detalii cu privire la certificatele de cheie publică necesare și oferă îndrumări cu privire la modelele de certificate și perioadele de valabilitate pentru statele membre care doresc să opereze propria lor CSCA. Întrucât DCC-urile trebuie să poată fi verificate pentru un interval de timp definit (începând de la emitere, expiră după o anumită perioadă de timp), este necesar să se definească un model de verificare pentru toate semnăturile aplicate pe certificatele de cheie publică și pe DCC.

2. **Terminologie**

Tabelul următor conține abrevierile și terminologia utilizate în prezenta anexă.

Termen	Definiție
Certificat	Sau certificat de cheie publică. Un certificat X.509 v3 care conține cheia publică a unei entități
CSCA	Autoritate Națională de Certificare pentru Semnătură
DCC	Certificatul digital al UE privind COVID. Un document digital semnat care conține informații despre vaccinare, testare sau vindecare
DCCG	Gateway-ul pentru certificatele digitale ale UE privind COVID. Acest sistem este utilizat pentru schimbul de DSC-uri între statele membre
$DCCG_{TA}$	Certificatul de ancoră de încredere (*Trust Anchor*) al DCCG. Cheia privată corespunzătoare este utilizată pentru a semna lista tuturor certificatelor CSCA offline
$DCCG_{TLS}$	Certificatul de server TLS (*Transport Layer Security* – securitatea nivelurilor de transport) de server eliberat de DCCG.
DSC	Certificatul de semnatar de documente. Certificatul de cheie publică al autorității de semnare a documentelor dintr-un stat membru (de exemplu, un sistem autorizat să semneze DCC-urile). Acest certificat este eliberat de CSCA a statului membru
EC-DSA	Algoritmul de semnătură digitală bazat pe curbe eliptice. Un algoritm de semnătură criptografică bazat pe curbe eliptice
Stat membru	Statul membru al Uniunii Europene

Termen	Definiție
mTLS	TLS reciproc. Protocolul de securitate pe nivelul de transport cu autentificare reciprocă
NB	Sistemul back-end național al unui stat membru
NB_{CSCA}	Certificatul CSCA al unui stat membru (pot exista mai multe)
NB_{TLS}	Certificatul de autentificare TLS la nivel de client aferent unui sistem back-end național
NB_{UP}	Certificatul pe care un sistem back-end național îl utilizează pentru a semna pachete de date care sunt încărcate în DCCG
PKI	Infrastructura de chei publice. Model de încredere bazat pe certificate de cheie publică și pe autorități de certificare
RSA	Algoritmul criptografic asimetric bazat pe factorizarea numerelor întregi, utilizat pentru semnăturile digitale sau pentru criptarea asimetrică

3. **Fluxurile de comunicații și serviciile de securitate ale DCCG**

Prezenta secțiune oferă o imagine de ansamblu asupra fluxurilor de comunicații și a serviciilor de securitate din cadrul sistemului DCCG. Acesta definește, de asemenea, cheile și certificatele utilizate pentru a proteja comunicarea, informațiile încărcate, DCC-urile și o listă de încredere semnată care conține toate certificatele CSCA integrate. DCCG funcționează ca un centru de date care face posibil schimbul de pachete de date semnate pentru statele membre.

Pachetele de date încărcate sunt furnizate de DCCG „ca atare”, ceea ce înseamnă că DCCG nu adaugă și nu șterge DSC-uri din pachetele pe care le primește. Sistemul back-end național (NB) al statelor membre trebuie să fie abilitat să verifice integritatea și autenticitatea datelor încărcate de la un capăt la altul. În plus, sistemele back-end naționale și DCCG vor utiliza autentificarea TLS reciprocă pentru a stabili o conexiune securizată. Aceasta este în plus față de semnăturile incluse în datele care fac obiectul schimbului.

3.1. *Autentificarea și stabilirea conexiunii*

DCCG utilizează protocolul de securitate pe nivelul de transport (*Transport Layer Security* – TLS) cu autentificare reciprocă pentru a crea un canal criptat autentificat între sistemul back-end național al statului membru (NB) și mediul gateway-ului. Prin urmare, DCCG deține un certificat de server TLS, abreviat $DCCG_{TLS}$, iar sistemele back-end naționale dețin un certificat de client TLS – abreviat NB_{TLS}. Modelele de certificate sunt furnizate în *secțiunea 5*. Fiecare sistem back-end național poate furniza propriul certificat TLS. Acest certificat va fi inclus în mod explicit în lista albă și, prin urmare, poate fi eliberat de o autoritate de certificare de încredere publică (de exemplu, o autoritate de certificare care respectă cerințele de bază ale Forumului autorităților de certificare și al furnizorilor de browsere – Forumul CA/Browser) ori de o autoritate națională de certificare sau poate fi autosemnat. Fiecare stat membru este responsabil de datele sale naționale și de protecția cheii private utilizate pentru stabilirea conexiunii cu DCCG. Abordarea „adu-ți propriul certificat” necesită o procedură de înregistrare și identificare bine definită, precum și proceduri de revocare și de reînnoire, astfel cum sunt descrise în *secțiunile 4.1, 4.2* și *4.3*. DCCG utilizează o listă albă pe care sunt adăugate certificatele TLS ale sistemelor back-end naționale după ce au fost înregistrate cu succes. Numai sistemele back-end naționale care se autentifică cu o cheie privată ce corespunde unui certificat inclus în lista albă pot stabili o conexiune sigură cu DCCG. DCCG va utiliza, de asemenea, un certificat TLS care să le permită sistemelor back-end naționale să verifice dacă stabilesc într-adevăr o conexiune cu DCCG „reală” și nu cu o entitate răuvoitoare care se prezintă drept DCCG. Certificatul DCCG va fi furnizat sistemelor back-end naționale după ce au fost înregistrate cu succes. Certificatul $DCCG_{TLS}$ va fi emis de o autoritate de certificare de încredere publică (inclusă în toate browserele importante). Responsabilitatea de a verifica dacă au stabilit o conexiune sigură cu DCCG (de exemplu, prin compararea amprentei digitale a certificatului $DCCG_{TLS}$ al serverului la care s-au conectat cu amprenta furnizată după înregistrare) le revine statelor membre.

3.2. *Autoritățile naționale de certificare pentru semnătură și modelul de validare*

Statele membre care participă la cadrul DCCG trebuie să utilizeze o CSCA pentru emiterea DSC-urilor. Un stat membru poate avea mai multe CSCA, de exemplu, în cazul deconcentrării regionale. Fiecare stat membru poate fie să utilizeze autoritățile de certificare existente, fie să înființeze o autoritate de certificare specială (eventual autosemnată) pentru sistemul DCC.

Statele membre trebuie să își prezinte certificatul (certificatele) CSCA operatorului DCCG în timpul procedurii oficiale de integrare. După înregistrarea cu succes a statului membru (*a se vedea secțiunea 4.1 pentru mai multe detalii*), operatorul DCCG va actualiza o listă de încredere semnată cuprinzând toate certificatele CSCA care sunt active în cadrul DCC. Operatorul DCCG va utiliza o pereche specială de chei asimetrice pentru a semna lista de încredere și certificatele într-un mediu offline. Cheia privată nu va fi stocată în sistemul DCCG online, astfel încât compromiterea sistemului online să nu îi permită unui atacator să compromită lista de încredere. Certificatul de ancoră de încredere $DCCG_{TA}$ corespunzător va fi furnizat sistemelor back-end naționale în timpul procesului de integrare.

Statele membre pot obține lista de încredere de pe gateway-ul DCCG pentru procedurile lor de verificare. CSCA este definită ca fiind autoritatea de certificare care eliberează DSC-urile; prin urmare, statele membre care utilizează o ierarhie pe mai multe niveluri a autorităților de certificare (de exemplu, Root CA –> CSCA –> DSC) trebuie să indice autoritatea de certificare subordonată care eliberează DSC-urile. În acest caz, dacă un stat membru utilizează o autoritate de certificare existentă, atunci sistemul DCC va face abstracție de tot ceea ce se află deasupra CSCA și va include în lista albă doar CSCA ca ancoră de încredere (chiar dacă este o autoritate de certificare subordonată). Acest lucru se explică prin faptul că modelul OACI permite doar două niveluri – o CSCA „rădăcină” și un DSC „frunză” semnat doar de CSCA respectivă.

În cazul în care un stat membru operează propria CSCA, acel stat membru este responsabil de funcționarea și gestionarea cheilor respectivei autorități de certificare în condiții de siguranță. CSCA acționează ca ancoră de încredere pentru DSC-uri și, prin urmare, protejarea cheii private a CSCA este esențială pentru integritatea mediului DCC. Modelul de verificare din infrastructura de cheie privată a DCC este modelul *shell*, care prevede că toate certificatele prezente în validarea traseului certificatelor trebuie să fie valabile la un anumit moment (și anume, la momentul validării semnăturii). Prin urmare, se aplică următoarele restricții:

— CSCA nu trebuie să emită certificate a căror perioadă de valabilitate o depășește pe cea a certificatului autorității de certificare;

— semnatarul de documente nu trebuie să semneze documente a căror perioadă de valabilitate o depășește pe cea a DSC;

— statele membre care operează propria lor CSCA trebuie să definească perioade de valabilitate pentru CSCA respectivă și toate certificatele eliberate și trebuie să se ocupe de reînnoirea certificatelor.

Secțiunea 4.2 conține recomandări privind perioadele de valabilitate.

3.3. *Integritatea și autenticitatea datelor încărcate*

Sistemele back-end naționale pot utiliza DCCG pentru a încărca și a descărca pachete de date semnate digital după autentificarea reciprocă reușită. La început, aceste pachete de date conțin DSC-urile statelor membre. Perechea de chei care este utilizată de sistemul back-end național pentru semnătura digitală a pachetelor de date încărcate în sistemul DCCG se numește pereche de chei pentru semnătura de încărcare a sistemului back-end național, iar denumirea abreviată a certificatului de cheie publică corespunzător este certificatul NB_{UP}. Fiecare stat membru își aduce propriul certificat NB_{UP}, care poate fi autosemnat sau emis de o autoritate de certificare existentă, cum ar fi o autoritate de certificare publică (și anume, o autoritate de certificare care eliberează certificatul în conformitate cu cerințele de bază ale forumului CA/Browser). Certificatul NB_{UP} trebuie să fie diferit de orice alt certificat utilizat de statul membru respectiv (și anume de CSCA, de certificatul TLS de client sau de DSC-uri).

Statele membre trebuie să furnizeze certificatul de încărcare operatorului DCCG în timpul procedurii inițiale de înregistrare (*a se vedea secțiunea 4.1 pentru mai multe detalii*). Fiecare stat membru este responsabil de datele sale naționale și trebuie să protejeze cheia privată utilizată pentru semnarea încărcărilor.

Celelalte state membre pot verifica pachetele de date semnate cu ajutorul certificatelor de încărcare furnizate de DCCG. DCCG verifică autenticitatea și integritatea datelor încărcate, comparându-le cu certificatul de încărcare al sistemului back-end național, înainte ca datele să fie furnizate altor state membre.

3.4. *Cerințe privind arhitectura tehnică a DCCG*

Cerințele privind arhitectura tehnică a DCCG sunt următoarele:

— DCCG utilizează autentificarea TLS reciprocă pentru a stabili o conexiune criptată autentificată cu sistemele back-end naționale. Prin urmare, DCCG actualizează periodic lista albă a certificatelor de client NB_{TLS} înregistrate;

— DCCG utilizează două certificate digitale ($DCCG_{TLS}$ și $DCCG_{TA}$), cu două perechi de chei distincte. Cheia privată a perechii de chei DCCGTA se actualizează offline (nu pe componentele online ale DCCG);

— DCCG actualizează periodic lista de încredere a certificatelor NB_{CSCA}, care este semnată cu cheia privată $DCCG_{TA}$;

— criptarea utilizată trebuie să îndeplinească cerințele prevăzute în *secțiunea 5.1*.

4. Gestionarea ciclului de viață a certificatelor

4.1. *Înregistrarea sistemelor back-end naționale*

Pentru a participa la sistemul DCCG, statele membre trebuie să se înregistreze la operatorul DCCG. Prezenta secțiune descrie procedura tehnică și operațională care trebuie urmată pentru a înregistra un sistem back-end național.

Operatorul DCCG și statul membru trebuie să facă schimb de informații privind persoanele de contact pentru aspecte tehnice legate de procesul de integrare. Se presupune că persoanele de contact pentru aspecte tehnice sunt legitimate de statele lor membre și că identificarea/autentificarea se efectuează prin intermediul altor canale. De exemplu, autentificarea poate fi realizată atunci când persoana de contact pentru aspecte tehnice a unui stat membru transmite prin e-mail certificatele sub formă de fișiere criptate, cu parolă, și comunică telefonic parola corespunzătoare operatorului DCCG. De asemenea, pot fi utilizate și alte canale securizate definite de operatorul DCCG.

Statul membru trebuie să furnizeze trei certificate digitale în timpul procesului de înregistrare și identificare:

— certificatul TLS de tip NB_{TLS} al statului membru

— certificatul de încărcare de tip NB_{UP} al statului membru

— certificatul (certificatele) CSCA de tip NB_{CSCA} al(e) statului membru

Toate certificatele furnizate trebuie să respecte cerințele definite în *secțiunea 5*. Operatorul DCCG va verifica dacă certificatul transmis respectă cerințele din *secțiunea 5*. După identificare și înregistrare, operatorul DCCG:

— adaugă certificatul (certificatele) NB_{CSCA} pe lista de încredere semnată cu cheia privată care corespunde cheii publice $DCCG_{TA}$;

— adaugă certificatul NLS_{TLS} pe lista albă a punctului final TLS din cadrul DCCG;

— adaugă certificatul NB_{UP} în sistemul DCCG;

— furnizează statului membru certificatul $DCCG_{TA}$ și certificatul de cheie publică $DCCG_{TLS}$.

4.2. *Autoritățile de certificare, perioadele de valabilitate și reînnoirea*

În cazul în care un stat membru dorește să opereze propria sa CSCA, certificatele CSCA pot fi certificate autosemnate. Acestea acționează ca ancoră de încredere a statului membru și, prin urmare, statul membru trebuie să protejeze cu fermitate cheia privată corespunzătoare cheii publice a certificatului CSCA. Se recomandă ca statele membre să utilizeze un sistem offline pentru CSCA-urile proprii, și anume un sistem informatic care nu este conectat la nicio rețea. Pentru a avea acces la sistem, trebuie utilizată o metodă de control care presupune mai multe persoane (de exemplu, urmând principiul celor patru ochi). După semnarea DSC-urilor, trebuie efectuate controale operaționale, iar sistemul care deține cheia privată a CSCA se stochează în condiții de siguranță, cu controale stricte al accesului. Pentru a asigura o protecție suplimentară a cheii private a CSCA se pot utiliza module de securitate hardware sau carduri inteligente. Certificatele digitale cuprind o perioadă de valabilitate care impune reînnoirea certificatelor. Reînnoirea este necesară pentru a utiliza noi chei criptografice și pentru a adapta dimensiunile cheilor atunci când apar noi îmbunătățiri ale tehnicii de calcul sau atunci când noi atacuri amenință securitatea algoritmului criptografic utilizat. Se aplică modelul *shell* (a se vedea *secțiunea 3.2*).

Se recomandă următoarele perioade de valabilitate, având în vedere valabilitatea de un an a certificatelor digitale privind COVID:

— CSCA: 4 ani

— DSC: 2 ani

— Certificate de încărcare: 1-2 ani

— Certificate TLS de autentificare la nivel de client: 1-2 ani

Pentru o reînnoire în timp util, se recomandă următoarele perioade de utilizare pentru cheile private:

— CSCA: 1 an

— DSC: 6 luni

Statele membre trebuie să creeze noi certificate de încărcare și noi certificate TLS în timp util, de exemplu, cu o lună înainte de expirare, pentru a permite buna funcționare a certificatelor respective. Ar trebui ca certificatele CSCA și DSC-urile să fie reînnoite cu cel puțin o lună înainte de încheierea perioadei de utilizare a cheii private (având în vedere procedurile operaționale necesare). Statele membre trebuie să îi furnizeze operatorului DCCG certificate CSCA, certificate de încărcare și certificate TLS actualizate. Certificatele expirate trebuie eliminate de pe lista albă și de pe lista de încredere.

Statele membre și operatorul DCCG trebuie să urmărească valabilitatea propriilor certificate. Nu există nicio entitate centrală care să țină evidența valabilității certificatelor și să informeze participanții.

4.3. *Revocarea certificatelor*

În general, certificatele digitale pot fi revocate de autoritatea de certificare emitentă prin utilizarea listelor certificatelor revocate sau de respondentul la Protocolul de verificare online a stării certificatelor (*Online Certificate Status Protocol* – OCSP). Ar trebui ca CSCA-urile pentru sistemul DCC să furnizeze liste ale certificatelor revocate (CRL). Chiar dacă aceste liste nu sunt utilizate în prezent de alte state membre, ar trebui ca ele să fie integrate în aplicațiile viitoare. În cazul în care o CSCA decide să nu furnizeze liste ale certificatelor revocate, certificatele DSC ale respectivei CSCA vor trebui reînnoite atunci când listele certificatelor revocate vor deveni obligatorii. Verificatorii nu ar trebui să utilizeze protocolul OCSP pentru validarea DSC-urilor, ci listele certificatelor revocate. Se recomandă ca sistemul back-end național să efectueze validarea necesară a DSC-urilor descărcate de pe gateway-ul DCC și să transmită mai departe validatorilor naționali ai DCC-urilor doar un set de DSC-uri de încredere și validate. Ar trebui ca validatorii DCC să nu efectueze nicio verificare a revocării în ceea ce privește DSC în cadrul procesului lor de validare. Unul dintre motive este protejarea vieții private a deținătorilor DCC-urilor prin evitarea oricărei posibilități ca utilizarea unei anumite DSC să poată fi monitorizată de către respondentul OCSP asociat.

Statele membre își pot elimina DSC-urile din DCCG pe cont propriu, utilizând certificate de încărcare și certificate TLS valabile. Eliminarea unui DSC înseamnă că toate DCC-urile eliberate cu acest certificat își pierd valabilitatea în momentul în care statele membre obțin listele DSC actualizate. Este esențial să se asigure protecția materialelor de cheie privată corespunzătoare DSC-urilor. Statele membre trebuie să informeze operatorul DCCG atunci când sunt nevoite să revoce certificate de încărcare sau certificate TLS, de exemplu din cauza compromiterii sistemului back-end național. Operatorul DCCG poate apoi să retragă încrederea acordată certificatului afectat, de exemplu, prin eliminarea acestuia de pe lista albă a TLS. Operatorul DCCG poate elimina certificatele de încărcare din baza de date a DCCG. Pachetele semnate cu cheia privată corespunzătoare respectivelor certificate de încărcare își pierd valabilitatea în momentul în care sistemul back-end național retrage încrederea acordată certificatelor de încărcare revocate. În cazul în care un certificat CSCA trebuie revocat, statele membre trebuie să informeze operatorul DCCG, precum și alte state membre cu care au relații de încredere. Operatorul DCCG va emite o nouă listă de încredere, pe care certificatul afectat nu va mai figura. Toate DSC-urile emise de respectiva CSCA își pierd valabilitatea în momentul în care statele membre își actualizează registrul de încredere („trust store") back-end național. În cazul în care certificatul $DCCG_{TLS}$ sau certificatul $DCCG_{TA}$ trebuie revocate, operatorul DCCG și statele membre trebuie să colaboreze pentru a stabili o nouă listă de conexiuni TLS de încredere și o nouă listă de încredere.

5. **Modele de certificate**

Prezenta secțiune stabilește cerințe și îndrumări criptografice, precum și cerințe privind modelele de certificate. De asemenea, aceasta definește modelele de certificate pentru certificatele DCCG.

5.1. *Cerințe criptografice*

Algoritmii criptografici și suitele de cifrare TLS trebuie alese pe baza recomandării actuale a Biroului federal german pentru securitatea informațiilor (BSI) sau a Comitetului consultativ privind securitatea sistemelor informatice (*Advisory Committee on information systems security*, SOG-IS). Aceste recomandări sunt similare cu recomandările altor instituții și organizații de standardizare. Recomandările pot fi găsite în orientările tehnice TR 02102-1 și TR 02102-2 ([1]) sau în mecanismele criptografice convenite în cadrul SOG-IS ([2]).

5.1.1. Cerințe privind DSC

Trebuie aplicate cerințele prevăzute în *anexa I, secțiunea 3.2.2*. Prin urmare, se recomandă insistent ca semnatarii de documente să utilizeze algoritmul de semnătură digitală bazat pe curbe eliptice (ECDSA) cu NIST-p-256 (astfel cum este definit în apendicele D la standardul federal de prelucrare a informațiilor FIPS PUB 186-4). Nu sunt acceptate alte curbe eliptice. Din cauza restricțiilor de spațiu ale DCC, statele membre nu ar trebui să utilizeze algoritmul RSA-PSS, chiar dacă utilizarea acestuia ca algoritm alternativ este permisă. În cazul în care statele membre

([1]) BSI - Orientări tehnice TR-02102 (bund.de)
([2]) SOG-IS - documente justificative (sogis.eu).

utilizează algoritmul RSA-PSS, acestea ar trebui să utilizeze o dimensiune a modulului de 2048 biți sau de maximum 3072 biți. Pentru semnătura DSC trebuie utilizat, ca funcție de distribuire (hash) criptografică, algoritmul hash securizat SHA-2 cu o lungime a rezultatului ≥ 256 biți (a se vedea ISO/IEC 10118-3:2004).

5.1.2. Cerințe privind certificatele TLS, certificatele de încărcare și certificatele CSCA

Pentru certificatele digitale și semnăturile criptografice în contextul DCCG, principalele cerințele privind algoritmii criptografici și lungimea cheii sunt rezumate în următorul tabel (în 2021):

Algoritmul de semnătură	Dimensiunea cheii	Funcția de distribuire (hash)
EC-DSA	Min. 250 biți	SHA-2 cu o lungime a rezultatului ≥ 256 biți
RSA-PSS (padding recomandat) RSA-PKCS #1 v1.5 (padding tradițional)	O dimensiune a modulului (N) RSA de min. 3000 biți, cu un exponent public > 2^16	SHA-2 cu o lungime a rezultatului ≥ 256 biți
DSA	Numărul prim p de min. 3000 biți, cheia q de 250 biți	SHA-2 cu o lungime a rezultatului ≥ 256 biți

Curba eliptică recomandată pentru EC-DSA este NIST-p-256, datorită punerii sale în aplicare pe scară largă.

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

Tabelul următor oferă îndrumări cu privire la modelul de certificat NB_{CSCA}, în cazul în care un stat membru decide să opereze propria CSCA pentru sistemul DCC.

Intrările cu caractere **aldine** sunt obligatorii (trebuie să fie incluse în certificat), intrările cu caractere *cursive* sunt recomandate (ar trebui incluse). Pentru câmpurile absente, nu sunt definite recomandări.

Câmp	Valoare
Subiect	**cn = <denumire comună unică ce nu poate fi lăsată necompletată>**, *o = <furnizor>*, **c = <statul membru care operează CSCA>**
Utilizarea cheii	**semnarea certificatului,** *semnarea CRL* (cel puțin)
Restricții de bază	**CA = adevărat, restricții de lungime a traseului = 0**

Denumirea subiectului nu trebuie să fie lăsată necompletată și trebuie să fie unică în statul membru specificat. Codul de țară (c) trebuie să corespundă statului membru care va utiliza certificatul CSCA. Certificatul trebuie să conțină un identificator unic al cheii subiectului (SKI), în conformitate cu RFC 5280 ([3]).

5.3. *Certificatul de semnatar de documente (DSC)*

Tabelul următor oferă îndrumări cu privire la DSC. Intrările cu caractere **aldine** sunt obligatorii (trebuie să fie incluse în certificat), intrările cu caractere *cursive* sunt recomandate (ar trebui incluse). Pentru câmpurile absente, nu sunt definite recomandări.

Câmp	Valoare
Nr. de serie	**numărul de serie unic**
Subiect	**cn = <denumire comună unică ce nu poate fi lăsată necompletată>**, *o = <furnizor>*, **c = <statul membru care utilizează acest DSC>**
Utilizarea cheii	**semnătură digitală** (cel puțin)

([3]) rfc5280 (ietf.org)

DSC trebuie să fie semnat cu cheia privată care corespunde unui certificat CSCA utilizat de statul membru.

Se utilizează următoarele extensii:

— Certificatul trebuie să conțină un identificator pentru cheia publică a autorității (*Authority Key Identifier* – AKI) care corespunde identificatorului cheii subiectului (*Subject Key Identifier* – SKI) al certificatului CSCA emitente

— Certificatul ar trebui să conțină un identificator unic al cheii subiectului (în conformitate cu RFC 5280 ([4])).

În plus, ar trebui ca certificatul să conțină extensia punctului de distribuție a CRL care trimite la lista certificatelor revocate (CRL) furnizată de CSCA care a emis DSC.

DSC poate conține o extensie de utilizare extinsă a cheii cu zero sau mai mulți identificatori ai politicii de utilizare a cheii care limitează tipurile de certificate HCERT pe care acest certificat este autorizat să le verifice. În cazul în care sunt prezenți unul sau mai mulți identificatori, verificatorii trebuie să verifice utilizarea cheii prin comparație cu certificatul HCERT stocat. În acest scop, pentru câmpul extendedKeyUsage sunt definite următoarele valori:

Câmp	Valoare
extendedKeyUsage	1.3.6.1.4.1.1847.2021.1.1 pentru emitenții de certificate de testare
extendedKeyUsage	1.3.6.1.4.1.1847.2021.1.2 pentru emitenții de certificate de vaccinare
extendedKeyUsage	1.3.6.1.4.1.1847.2021.1.3 pentru emitenții de certificate de vindecare

În absența oricărei extensii a utilizării cheii (adică fără extensii sau cu extensii având valoarea zero), acest certificat poate fi utilizat pentru a valida orice tip de certificat HCERT. Alte documente pot defini și alți identificatori relevanți ai politicii de utilizare extinsă a cheii folosiți la validarea certificatelor HCERT.

5.4. *Certificate de încărcare (NBUP)*

Tabelul următor oferă îndrumări cu privire la certificatul de încărcare pentru sistemul back-end național. Intrările cu caractere **aldine** sunt obligatorii (trebuie să fie incluse în certificat), intrările cu caractere *cursive* sunt recomandate (ar trebui incluse). Pentru câmpurile absente, nu sunt definite recomandări.

Câmp	Valoare
Subiect	**cn = <denumire comună unică ce nu poate fi lăsată necompletată>**, *o = <furnizor>*, **c = <statul membru care utilizează acest certificat de încărcare>**
Utilizarea cheii	**semnătură digitală** (cel puțin)

5.5. *Certificatul de autentificare TLS la nivel de client aferent unui sistem back-end național (NB_{TLS})*

Tabelul următor oferă îndrumări cu privire la certificatul de autentificare TLS la nivel de client aferent unui sistem back-end național. Intrările cu caractere **aldine** sunt obligatorii (trebuie să fie incluse în certificat), intrările cu caractere *cursive* sunt recomandate (ar trebui incluse). Pentru câmpurile absente, nu sunt definite recomandări.

Câmp	Valoare
Subiect	**cn = <denumire comună unică ce nu poate fi lăsată necompletată>**, *o = <furnizor>*, **c = <statul membru în sistemul back-end național>**
Utilizarea cheii	**semnătură digitală** (cel puțin)
Utilizarea extinsă a cheii	autentificare la nivel de client (1.3.6.1.5.5.7.3.2)

([4]) rfc5280 (ietf.org)

Certificatul poate conține, de asemenea, *autentificarea la nivel de server (1.3.6.1.5.5.7.3.1)* aferentă utilizării extinse a cheii, dar aceasta nu este necesară.

5.6. *Certificatul de semnătură pentru lista de încredere ($DCCG_{TA}$)*

Următorul tabel definește certificatul pentru ancora de încredere a DCCG.

Câmp	Valoare
Subiect	**cn = Gateway-ul pentru adeverințele electronice verzi** ([5])**, o = <furnizor>, c = <țară>**
Utilizarea cheii	**semnătură digitală** (cel puțin)

5.7. *Certificatele de server TLS ale DCCG ($DCCG_{TLS}$)*

Următorul tabel definește certificatul TLS al DCCG.

Câmp	Valoare
Subiect	CN = < FQDN (*Fully Qualified Domain Name* – numele de domeniu complet calificat) sau adresa IP a DCCG >, o = <furnizor>, c = <țară>
SubjectAltName	dNSName: < denumirea DNS al DCCG>sau iPAddress: <adresa IP a DCCG>
Utilizarea cheii	**semnătură digitală** (cel puțin)
Utilizarea extinsă a cheii	autentificare la nivel de server (1.3.6.1.5.5.7.3.1)

Certificatul poate conține, de asemenea, *autentificarea la nivel de client (1.3.6.1.5.5.7.3.2)* aferentă utilizării extinse a cheii, dar aceasta nu este necesară.

Certificatul TLS al DCCG trebuie eliberat de o autoritate de certificare de încredere publică (inclusă în toate browserele și sistemele de operare importante, în conformitate cu cerințele de bază ale forumului CA/Browser).

([5]) În acest context a fost menținut termenul „adeverință electronică verde” în loc de „certificat digital al UE privind COVID”, deoarece acesta este termenul care a fost integrat și utilizat în certificat înainte ca colegiuitorii să decidă să folosească un nou termen.