►B

VYKONÁVACIE ROZHODNUTIE KOMISIE (EÚ) 2021/1073

z 28. júna 2021,

ktorým sa stanovujú technické špecifikácie a pravidlá pre vykonávanie rámca dôvery pre digitálny COVID preukaz EÚ zriadený nariadením Európskeho parlamentu a Rady (EÚ) 2021/953

(Text s významom pre EHP)

(Ú. v. EÚ L 230, 30.6.2021, s. 32)

Zmenené a doplnené:

		Úradný vestník		
		Č.	Strana	Dátum
►M1	Vykonávacie rozhodnutie Komisie (EÚ) 2021/2014 zo 17. novembra 2021	L 410	180	18.11.2021
►M2	Vykonávacie rozhodnutie Komisie (EÚ) 2021/2301 z 21. decembra 2021	L 458	536	22.12.2021
►M3	Vykonávacie rozhodnutie Komisie (EÚ) 2022/483 z 21. marca 2022	L 98	84	25.3.2022
►M4	Vykonávacie rozhodnutie Komisie (EÚ) 2022/1516 z 8. septembra 2022	L 235	61	12.9.2022

▼B

VYKONÁVACIE ROZHODNUTIE KOMISIE (EÚ) 2021/1073

z 28. júna 2021,

ktorým sa stanovujú technické špecifikácie a pravidlá pre vykonávanie rámca dôvery pre digitálny COVID preukaz EÚ zriadený nariadením Európskeho parlamentu a Rady (EÚ) 2021/953

(Text s významom pre EHP)

Článok 1

Technické špecifikácie pre digitálny COVID preukaz EÚ, ktorými sa stanovuje generická štruktúra údajov, mechanizmy kódovania a transportný mechanizmus kódovania v strojovo čitateľnom optickom formáte, sa uvádzajú v prílohe I.

Článok 2

Pravidlá vypĺňania potvrdení uvedených v článku 3 ods. 1 nariadenia (EÚ) 2021/953 sa uvádzajú v prílohe II k tomuto rozhodnutiu.

Článok 3

Požiadavky, ktorými sa stanovuje spoločná štruktúra jedinečného identifikátora potvrdenia, sa uvádzajú v prílohe III.

▼M1

Článok 4

Pravidlá správy certifikátov verejného kľúča v súvislosti s bránou digitálneho COVID preukazu EÚ, ktorými sa podporujú aspekty interoperability rámca dôvery, sa uvádzajú v prílohe IV.

Článok 5

Spoločná koordinovaná dátová štruktúra pre údaje, ktoré sa majú zahrnúť do potvrdení uvedených v článku 3 ods. 1 nariadenia (EÚ) 2021/953 s použitím schémy zápisu objektu v jazyku JavaScript (JavaScript Object Notation, JSON), je stanovená v prílohe V k tomuto rozhodnutiu.

▼M3

Článok 5a

Výmena zoznamov zrušených potvrdení

1. Rámec dôvery pre digitálny COVID preukaz EÚ umožňuje výmenu zoznamov zrušených potvrdení prostredníctvom centrálnej brány digitálneho COVID preukazu EÚ (ďalej len „brána“) v súlade s technickými špecifikáciami uvedenými v prílohe I.

2. Ak členské štáty zrušia digitálne COVID preukazy EÚ, môžu do brány odoslať zoznamy zrušených potvrdení.

▼M3

3. Ak členské štáty odošlú zoznamy zrušených potvrdení, vydávajúce orgány vedú zoznam zrušených potvrdení.

4. Ak sa prostredníctvom brány vymieňajú osobné údaje, spracúvanie sa obmedzuje na účel podpory výmeny informácií o zrušených potvrdeniach. Takéto osobné údaje sa použijú len na účely overenia stavu zrušenia digitálnych COVID preukazov EÚ vydaných v rozsahu pôsobnosti nariadenia (EÚ) 2021/953.

5. Informácie odoslané do brány obsahujú v súlade s technickými špecifikáciami uvedenými v prílohe I tieto údaje:

a) pseudonymizované jedinečné identifikátory zrušených potvrdení;

b) dátum uplynutia platnosti odoslaného zoznamu zrušených potvrdení.

6. Ak vydávajúci orgán zruší digitálne COVID preukazy EÚ, ktoré vydal podľa nariadenia (EÚ) 2021/953 alebo nariadenia (EÚ) 2021/954, a ak má v úmysle vymieňať si príslušné informácie prostredníctvom brány, informácie uvedené v odseku 5 v podobe zoznamov zrušených potvrdení zašle do brány v bezpečnom formáte v súlade s technickými špecifikáciami uvedenými v prílohe I.

7. Vydávajúce orgány v čo najväčšej možnej miere zabezpečujú riešenie na informovanie držiteľov zrušených potvrdení o stave zrušenia ich potvrdení a o dôvode zrušenia v čase zrušenia.

8. Brána zhromažďuje prijaté zoznamy zrušených potvrdení. Poskytuje pritom nástroje na distribúciu týchto zoznamov členským štátom. Zoznamy automaticky vymaže v súlade s dátumami uplynutia platnosti, ktoré zasielajúci orgán uvedie v prípade každého odoslaného zoznamu.

9. Spoločnými prevádzkovateľmi spracúvaných údajov sú určené vnútroštátne orgány alebo verejné subjekty členských štátov, ktoré spracúvajú osobné údaje v bráne. Spoločným prevádzkovateľom sa prideľujú príslušné zodpovednosti v súlade s prílohou VI.

10. Sprostredkovateľom osobných údajov spracúvaných v bráne je Komisia. Komisia v postavení sprostredkovateľa v mene členských štátov zaisťuje bezpečnosť prenosu a ukladania osobných údajov v bráne a dodržiava povinnosti sprostredkovateľa stanovené v prílohe VII.

11. Komisia a spoloční prevádzkovatelia pravidelne testujú, posudzujú a hodnotia účinnosť technických a organizačných opatrení na zaistenie bezpečnosti spracúvania osobných údajov v bráne.

▼M3

Článok 5b

Odosielanie zoznamov zrušených potvrdení tretími krajinami

Tretie krajiny vydávajúce potvrdenia súvisiace s ochorením COVID-19, v súvislosti s ktorými Komisia prijala vykonávací akt podľa článku 3 ods. 10 alebo článku 8 ods. 2 nariadenia (EÚ) 2021/953, môžu odoslať zoznamy zrušených potvrdení súvisiacich s ochorením COVID-19, na ktoré sa vzťahuje takýto vykonávací akt, aby ich Komisia spracovala v mene spoločných prevádzkovateľov v bráne, ako sa uvádza v článku 5a, a to v súlade s technickými špecifikáciami uvedenými v prílohe I.

Článok 5c

Riadenie spracúvania osobných údajov v centrálnej bráne digitálneho COVID preukazu EÚ

1. Rozhodovací proces spoločných prevádzkovateľov riadi pracovná skupina zriadená v rámci výboru uvedeného v článku 14 nariadenia (EÚ) 2021/953.

2. Určené vnútroštátne orgány alebo verejné subjekty členských štátov, ktoré spracúvajú osobné údaje v bráne ako spoloční prevádzkovatelia, určia zástupcov uvedenej skupiny.

▼M1

Článok 6

Toto rozhodnutie nadobúda účinnosť dňom jeho uverejnenia v *Úradnom vestníku Európskej únie*.

▼B

Toto rozhodnutie nadobúda účinnosť dňom jeho uverejnenia v *Úradnom vestníku Európskej únie*.

▼B

PRÍLOHA I

FORMÁT A SPRÁVA DÔVERYHODNOSTI

Generická štruktúra údajov, mechanizmy kódovania a transportný mechanizmus kódovania v strojovo čitateľnom optickom formáte (ďalej len „QR“)

1. **Úvod**

V technických špecifikáciách stanovených v tejto prílohe sa uvádza generická štruktúra údajov a mechanizmy kódovania pre digitálny COVID preukaz EÚ. Určuje sa v nich aj transportný mechanizmus kódovania v strojovo čitateľnom optickom formáte („QR“), ktorý možno zobraziť na obrazovke mobilného zariadenia alebo vytlačiť. Formáty kontajnera elektronického zdravotného potvrdenia v týchto špecifikáciách sú generické, v tomto kontexte však slúžia na prenos digitálneho COVID preukazu EÚ.

2. **Terminológia**

Na účely tejto prílohy sú „vystavitelia“ organizácie, ktoré používajú tieto špecifikácie na vystavovanie zdravotných potvrdení, a „overovatelia“ sú organizácie, ktoré uznávajú zdravotné potvrdenia ako dôkaz o zdravotnom stave. „Účastníci“ sú vystavitelia a overovatelia. V prípade niektorých aspektov stanovených v tejto prílohe sa vyžaduje koordinácia medzi účastníkmi, napríklad pokiaľ ide o správu priestoru názvov a distribúciu kryptografických kľúčov. Predpokladá sa, že tieto úlohy vykonáva strana, ktorá sa ďalej označuje ako „sekretariát“.

3. **Formát kontajnera elektronického zdravotného potvrdenia**

Formát kontajnera elektronického zdravotného potvrdenia (ďalej len „HCERT“) slúži ako jednotný a štandardizovaný prenosový prostriedok pre zdravotné potvrdenia od rôznych vystaviteľov. Cieľom týchto špecifikácií je harmonizovať spôsob zobrazovania, kódovania a podpisovania zdravotných potvrdení, aby sa uľahčila interoperabilita.

Z hľadiska schopnosti čítať a interpretovať digitálny COVID preukaz EÚ vystavený ktorýmkoľvek vystaviteľom sa vyžaduje spoločná štruktúra údajov a dohoda o význame jednotlivých dátových polí nosného obsahu. S cieľom uľahčiť takúto interoperabilitu sa spoločná koordinovaná štruktúra údajov vymedzuje pomocou schémy „JSON“, ktorá tvorí rámec digitálneho COVID preukazu EÚ.

3.1. *Štruktúra nosného obsahu*

Nosný obsah je štruktúrovaný a kódovaný vo formáte CBOR s digitálnym podpisom COSE. Tento formát sa bežne označuje ako „webový token CBOR“ (ďalej len „CWT“) a je vymedzený v dokumente RFC 8392 ([1]). Nosný obsah vymedzený v ďalších oddieloch sa transportuje v rámci deklarácie hcert.

Overovateľ musí mať možnosť overiť integritu a pravosť pôvodu nosného obsahu. Na poskytnutie tohto mechanizmu musí vystaviteľ podpísať CWT pomocou schémy asymetrického elektronického podpisu, ako sa vymedzuje v špecifikácii COSE (RFC 8152 ([2])).

3.2. *Hodnoty CWT*

3.2.1. Prehľad štruktúry CWT

Chránené záhlavie

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

▼B

— Algoritmus podpisu (alg, označenie 1)

— Identifikátor kľúča (kid, označenie 4)

Nosný obsah

— Vystaviteľ (iss, kľúč deklarácie 1, voliteľné, kód vystaviteľa podľa normy ISO 3166-1 alpha-2)

— Čas vystavenia (iat, kľúč deklarácie 6)

— Čas exspirácie (exp, kľúč deklarácie 4)

— Zdravotné potvrdenie (hcert, kľúč deklarácie -260)

— Digitálny COVID preukaz EÚ v. 1 (eu_DCC_v1, kľúč deklarácie 1)

Podpis

3.2.2. Algoritmus podpisu

Parameter algoritmu podpisu (alg) označuje, aký algoritmus slúži na vytvorenie podpisu. Musí spĺňať alebo prekračovať aktuálne usmernenia organizácie SOG-IS, ktorých súhrn je uvedený v ďalších odsekoch.

Je vymedzený jeden primárny a jeden sekundárny algoritmus. Sekundárny algoritmus sa má použiť, len ak primárny algoritmus nie je prijateľný v rámci pravidiel a predpisov, ktoré sa vzťahujú na vystaviteľa.

S cieľom zaistiť zabezpečenie systému musia všetky implementácie zahŕňať sekundárny algoritmus. Z tohto dôvodu sa musí zaviesť primárny aj sekundárny algoritmus.

Pre primárny a sekundárny algoritmus platia tieto úrovne stanovené SOG-IS:

— Primárny algoritmus: primárny algoritmus je algoritmus pre digitálny podpis na báze eliptických kriviek (ECDSA), ako sa vymedzuje v oddiele 2.3 (normy ISO/IEC 14888-3:2006), s využitím parametrov P-256, ako sa vymedzujú v dodatku D (D.1.2.3) k (norme FIPS PUB 186-4), v kombinácii s hašovacím algoritmom SHA-256, ako sa vymedzuje v rámci funkcie 4 (normy ISO/IEC 10118-3:2004).

Zodpovedá to parametru ES256 algoritmu COSE.

— Sekundárny algoritmus: sekundárny algoritmus je RSASSA-PSS, ako sa vymedzuje v dokumente (RFC 8230 ([1])), s modulom 2048 bitov v kombinácii s hašovacím algoritmom SHA-256, ako sa vymedzuje v rámci funkcie 4 (normy ISO/IEC 10118–3:2004).

V rámci algoritmu COSE to zodpovedá parametru: PS256.

3.2.3. Identifikátor kľúča

Deklarácia identifikátora kľúča (kid) označuje certifikát podpisovateľa dokumentov (DSC) obsahujúci verejný kľúč, ktorý má overovateľ použiť na kontrolu správnosti digitálneho podpisu. Správa certifikátov verejného kľúča vrátane požiadaviek na DSC je opísaná v prílohe IV.

([1]) rfc8230 (ietf.org).

▼B

Deklaráciu identifikátora kľúča (kid) používajú overovatelia na výber správneho verejného kľúča zo zoznamu kľúčov vzťahujúcich sa na vystaviteľa, ako určuje deklarácia vystaviteľa (iss). Vystaviteľ môže používať súčasne viacero kľúčov, a to z administratívnych dôvodov alebo pri aktualizácii kľúčov. Pole identifikátora kľúča nie je kritické z hľadiska bezpečnosti. Môže sa preto v prípade potreby nachádzať v nechránenom záhlaví. Overovatelia musia akceptovať obe možnosti. Ak sú prítomné obe možnosti, musí sa použiť identifikátor kľúča v chránenom záhlaví.

Vzhľadom na skrátenie identifikátora (kvôli veľkostným obmedzeniam) existuje malá, nie však nulová pravdepodobnosť, že celkový zoznam podpisových certifikátov dokumentu (ďalej len „certifikát DSC“), ktoré overovateľ akceptuje, môže obsahovať certifikáty DSC s duplicitnými identifikátormi kid. Z tohto dôvodu musí overovateľ skontrolovať všetky podpisové certifikáty dokumentu s daným identifikátorom kid.

3.2.4. Vystaviteľ

Deklarácia vystaviteľa (iss) je hodnota reťazca, v ktorom sa voliteľne môže uvádzať kód krajiny podľa normy ISO 3166-1 alpha-2 vzťahujúci sa na subjekt, ktorý vystavuje zdravotné potvrdenie. Pomocou tejto deklarácie môže overovateľ identifikovať, ktorá množina certifikátov DSC sa má použiť na overenie. Na identifikáciu tejto deklarácie slúži kľúč deklarácie 1.

3.2.5. Čas exspirácie

Deklarácia času exspirácie (exp) musí obsahovať časovú pečiatku v celočíselnom formáte NumericDate (ako sa uvádza v časti 2 dokumentu RFC 8392 ([1])), ktorou sa uvádza, po aký čas sa má tento konkrétny podpis nosného obsahu považovať za platný, pričom po uplynutí toho času musí overovateľ odmietnuť nosný obsah z dôvodu uplynutia jeho platnosti. Účelom parametra exspirácie je vynútiť obmedzenie obdobia platnosti zdravotného potvrdenia. Na identifikáciu tejto hodnoty slúži kľúč deklarácie 4.

Čas exspirácie nesmie presiahnuť obdobie platnosti certifikátu DSC.

3.2.6. Čas vystavenia

Deklarácia času vystavenia (iat) musí obsahovať časovú pečiatku v celočíselnom formáte NumericDate (ako sa uvádza v časti 2 dokumentu RFC 8392 ([2])), ktorou sa uvádza čas vytvorenia zdravotného potvrdenia.

V poli Čas vystavenia sa nesmie uvádzať čas pred obdobím platnosti certifikátu DSC.

Overovatelia môžu uplatňovať dodatočné politiky, ktorých účelom je obmedzenie platnosti zdravotného potvrdenia na základe času vystavenia. Na identifikáciu tejto hodnoty slúži kľúč deklarácie 6.

3.2.7. Deklarácia zdravotného potvrdenia

Deklarácia zdravotného potvrdenia (hcert) je objekt JSON (RFC 7159 ([3])), ktorý obsahuje informácie o zdravotnom stave. V rámci rovnakej deklarácie môže existovať niekoľko rôznych druhov zdravotných potvrdení, z ktorých jedno je digitálny COVID preukaz EÚ.

Formát JSON slúži výlučne na účely schémy. Zobrazovací formát je CBOR, ako sa vymedzuje v dokumente (RFC 7049 ([4])). Vývojári aplikácií v skutočnosti vôbec nemusia vykonávať dekódovanie alebo kódovanie do formátu JSON alebo z neho, ale môžu používať príslušnú štruktúru v pamäti.

([1]) rfc8392 (ietf.org).
([2]) rfc8392 (ietf.org).
([3]) rfc7159 (ietf.org).
([4]) rfc7049 (ietf.org).

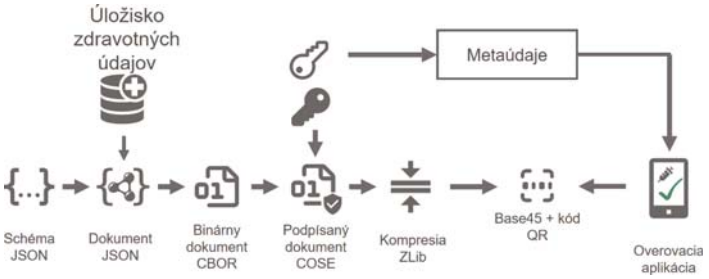
▼B

Na identifikáciu tejto deklarácie slúži kľúč deklarácie -260.

Reťazce v objekte JSON by sa mali normalizovať podľa normalizačnej formy s kanonickým zložením (NFC) vymedzenej v norme Unicode. V dekódovacích aplikáciách by sa však mal pri týchto aspektoch uplatňovať permisívny a robustný prístup a dôrazne sa odporúča akceptovanie akéhokoľvek primeraného druhu konverzie. Ak sa počas dekódovania alebo v rámci následných porovnávacích funkcií zistia údaje, ktoré nie sú normalizované, pri implementáciách by sa malo postupovať tak, akoby bol vstup normalizovaný metódou NFC.

4. **Serializácia a vytvorenie nosného obsahu digitálneho COVID preukazu EÚ**

Ako vzor serializácie slúži táto schéma:



Proces sa začína extrakciou údajov napríklad z úložiska zdravotných údajov (alebo z externého zdroja údajov), pričom sa na tieto extrahované údaje uplatní štruktúra podľa vymedzených schém digitálneho COVID preukazu EÚ. V tomto procese sa pred tým, ako začne serializácia na formát CBOR, môže uskutočniť konverzia na vymedzený formát údajov a transformácia na účely ľudskej čitateľnosti. Skratky deklarácií sa v každom prípade priradia zobrazovaným názvom pred serializáciou a po deserializácii.

Voliteľný vnútroštátny obsah údajov nie je povolený v potvrdeniach vystavených podľa nariadenia (EÚ) 2021/953 ([1]). Obsah údajov je obmedzený na vymedzené dátové prvky v minimálnom súbore údajov, ktorý je určený v prílohe k nariadeniu (EÚ) 2021/953.

5. **Transportné kódovania**

5.1. *Nespracované (Raw)*

Pri rozhraniach pre nešpecifikované (ľubovoľné) údaje možno prenášať kontajner HCERT a jeho nosný obsah tak, ako sú, s využitím akéhokoľvek základného transportu údajov, ktorý je bezpečný z hľadiska 8-bitového kódovania a spoľahlivý. Tieto rozhrania môžu zahŕňať komunikáciu na krátke vzdialenosti (NFC), Bluetooth alebo prenos prostredníctvom protokolu aplikačnej vrstvy, napríklad prenos potvrdenia HCERT od vystaviteľa do mobilného zariadenia držiteľa.

Ak sa pri prenose potvrdenia HCERT od vystaviteľa k držiteľovi používa rozhranie len s možnosťou zobrazenia (napríklad SMS, e-mail:), nespracované transportné kódovanie nie je zo zrejmých dôvodov použiteľné.

([1]) Nariadenie Európskeho parlamentu a Rady (EÚ) 2021/953 zo 14. júna 2021 o rámci pre vydávanie, overovanie a uznávanie interoperabilných potvrdení o očkovaní proti ochoreniu COVID-19, o vykonaní testu a prekonaní tohto ochorenia (digitálny COVID preukaz EÚ) s cieľom uľahčiť voľný pohyb počas pandémie ochorenia COVID-19 (Ú. v. EÚ L 211, 15.6.2021, s. 1).

▼B

5.2. *Čiarový kód*

5.2.1. Kompresia nosného obsahu (CWT)

S cieľom zmenšiť veľkosť a zlepšiť rýchlosť a spoľahlivosť procesu načítania potvrdenia HCERT sa CWT komprimuje pomocou formátu ZLIB (RFC 1950 ([1])) a kompresného mechanizmu Deflate vo formáte vymedzenom v dokumente RFC 1951 ([2]).

5.2.2. Dvojrozmerný čiarový kód QR

Aby sa zabezpečila lepšia kompatibilita so staršími zariadeniami navrhnutými na spracúvanie nosného obsahu vo formáte ASCII, komprimovaný CWT sa kóduje vo formáte ASCII pomocou kódovania Base45 pred tým, ako sa zakóduje do dvojrozmerného čiarového kódu.

Na generovanie dvojrozmerného čiarového kódu sa použije formát QR vymedzený v norme (ISO/IEC 18004:2015). Odporúča sa miera korekcie chýb „Q“ (približne 25 %). Keďže sa Base45, QR kód musí používať alfanumerické kódovanie (režim 2 označený symbolmi 0010).

Aby mohli overovatelia zistiť typ zakódovaných údajov a vybrať správnu schému na dekódovanie a spracovanie, pred údajmi s kódovaním Base45 (podľa tejto špecifikácie) sa uvedie reťazec identifikátora kontextu „HC1:“. V budúcich verziách tejto špecifikácie, ktoré budú mať vplyv na spätnú kompatibilitu, sa vymedzí nový identifikátor kontextu, pričom znak nasledujúci za reťazcom „HC“ sa zvolí zo súboru znakov [1-9A-Z]. Poradie prírastkov sa vymedzuje tak, aby zodpovedalo tomuto poradiu, t. j. najskôr [1-9] a potom [A-Z].

Odporúča sa, aby bol optický kód na prezentačnom médiu vykreslený s uhlopriečkou od 35 mm do 60 mm, čo vyhovuje čítacím zariadeniam s pevnou optikou, pri ktorých je potrebné umiestniť prezentačné médium na povrch čítacieho zariadenia.

Ak sa optický kód tlačí na papier pomocou tlačiarní s nízkym rozlíšením (< 300 dpi), je nevyhnutné zabezpečiť, aby mal každý symbol (bod) kódu QR presne štvorcový tvar. V prípade neproporcionálnej zmeny mierky budú v niektorých riadkoch alebo stĺpcoch kódu QR symboly s obdĺžnikovým tvarom, čím sa v mnohých prípadoch sťaží čitateľnosť.

6. **Formát dôveryhodných zoznamov (zoznam CSCA a DSC)**

Od každého členského štátu sa vyžaduje poskytnutie zoznamu jedného alebo viacerých národných orgánov certifikácie podpisov (CSCA) a zoznamu všetkých platných certifikátov podpisovateľa dokumentov (DSC), ako aj udržiavanie týchto zoznamov v aktualizovanom stave.

6.1. *Zjednodušené riešenie z hľadiska orgánov CSCA/certifikátov DSC*

Pri tejto verzii špecifikácií členské štáty nepredpokladajú, že sa budú používať akékoľvek informácie o zozname zrušených certifikátov, ani že budú implementátori overovať obdobie používania súkromného kľúča.

Namiesto toho je hlavným mechanizmom na overenie platnosti to, že sa certifikát uvádza v najaktuálnejšej verzii daného zoznamu certifikátov.

([1]) rfc1950 (ietf.org).
([2]) rfc1951 (ietf.org).

▼B

6.2. *Infraštruktúra verejných kľúčov ICAO eMRTD a centrá dôveryhodnosti*

Členské štáty môžu použiť samostatný orgán CSCA, môžu však predložiť aj svoje existujúce certifikáty eMRTD CSCA a/alebo DSC, prípadne sa môžu rozhodnúť, že si ich obstarajú z (komerčných) centier dôveryhodnosti a predložia tie. Každý certifikát DSC však musí byť vždy podpísaný orgánom CSCA, ktorý daný členský štát oznámil.

7. **Bezpečnostné aspekty**

Pri návrhu schémy s využitím tejto špecifikácie musia členské štáty identifikovať, analyzovať a monitorovať určité bezpečnostné aspekty.

Do úvahy by sa mali vziať prinajmenšom tieto aspekty:

7.1. *Čas platnosti podpisu potvrdenia HCERT*

Vystaviteľ potvrdení HCERT je povinný obmedziť obdobie platnosti podpisu určením času uplynutia platnosti podpisu. Tým sa od držiteľa zdravotného potvrdenia vyžaduje, aby si ho v pravidelných intervaloch obnovoval.

Prijateľné obdobie platnosti môže byť určené na základe praktických obmedzení. Napríklad cestujúci nemusí mať možnosť obnoviť si zdravotné potvrdenie počas cesty do zahraničia. Môže však ísť aj o prípad, že vystaviteľ uvažuje nad možnosťou určitého narušenia zabezpečenia, keď by musel vystaviteľ odvolať certifikát DSC (čím by sa zneplatnili všetky zdravotné potvrdenia vystavené pomocou príslušného kľúča, pri ktorom ešte neuplynulo obdobie platnosti). Dôsledky takejto udalosti možno obmedziť pravidelným nasadzovaním kľúčov vystaviteľa a požadovaním obnovenia všetkých zdravotných potvrdení v určitom primeranom intervale.

7.2. *Správa kľúčov*

Táto špecifikácia vychádza vo veľkej miere zo silných kryptografických mechanizmov s cieľom zabezpečiť integritu údajov a overenie pôvodu údajov. Je preto nevyhnutné zachovanie dôvernosti súkromných kľúčov.

K narušeniu dôvernosti kryptografických kľúčov môže dôjsť rôznymi spôsobmi, napríklad:

— proces generovania kľúčov môže byť chybný, takže vygenerované kľúče sú slabé,

— kľúče môžu byť odhalené v dôsledku ľudskej chyby,

— môže dôjsť ku krádeži kľúčov páchateľmi z vonkajšieho alebo vnútorného prostredia,

— kľúče môžu byť vypočítané pomocou kryptoanalýzy.

S cieľom zmierniť riziká, že podpisový algoritmus sa ukáže ako slabý, čím sa umožní narušenie súkromných kľúčov pomocou kryptoanalýzy, sa v tejto špecifikácii odporúča, aby všetci účastníci zaviedli sekundárny záložný podpisový algoritmus, ktorý vychádza z odlišných parametrov alebo odlišného matematického problému než primárny algoritmus.

Pokiaľ ide o uvedené riziká v súvislosti s prevádzkovými prostrediami vystaviteľov, musia sa zaviesť zmierňujúce opatrenia na zabezpečenie účinnej kontroly, napríklad generovanie, ukladanie a používanie súkromných kľúčov v hardvérových bezpečnostných moduloch. Dôrazne sa odporúča používanie hardvérových bezpečnostných modulov na podpisovanie zdravotných potvrdení.

▼B

Bez ohľadu na to, či sa vystaviteľ rozhodne používať hardvérové bezpečnostné moduly, mal by sa stanoviť plán aktualizácií kľúčov, v ktorom by frekvencia aktualizácií kľúčov bola úmerná vystaveniu kľúčov externým sieťam, iným systémom a pracovníkom. Vhodne zvoleným plánom aktualizácií sa obmedzujú aj riziká súvisiace s chybne vystavenými zdravotnými potvrdeniami, keďže vystaviteľ má v prípade potreby možnosť zrušiť takéto zdravotné potvrdenia v dávkach odvolaním kľúča.

7.3. *Validácia vstupných údajov*

Tieto špecifikácie možno použiť spôsobom, pri ktorom sa predpokladá prijímanie údajov z nedôveryhodných zdrojov do systémov, ktoré môžu mať kritický význam. Aby sa minimalizovali riziká súvisiace s týmto vektorom útoku, všetky vstupné polia musia byť riadne validované podľa typov, dĺžok a obsahu údajov. Aj podpis vystaviteľa sa musí overiť, skôr ako dôjde k akémukoľvek spracovaniu obsahu potvrdenia HCERT. Pri overení podpisu vystaviteľa sa však predpokladá, že sa najskôr analyzuje chránené záhlavie vystaviteľa, v ktorom sa potenciálny útočník môže pokúsiť vsunúť starostlivo pripravené informácie navrhnuté s cieľom narušiť zabezpečenie systému.

8. **Správa dôveryhodnosti**

Na overenie podpisu potvrdenia HCERT sa vyžaduje verejný kľúč. Členské štáty sprístupnia tieto verejné kľúče. V konečnom dôsledku musí mať každý overovateľ zoznam všetkých verejných kľúčov, ktorým je ochotný dôverovať (keďže verejný kľúč nie je súčasťou potvrdenia HCERT).

Systém je zložený (len) z dvoch vrstiev: v každom členskom štáte je to jeden alebo viacero certifikátov na úrovni krajiny, ktoré slúžia na podpisovanie jedného alebo viacerých certifikátov podpisovateľa dokumentov (DSC), ktoré sa používajú v každodennej prevádzke.

Certifikáty členských štátov sa označujú ako certifikáty národných orgánov certifikácie podpisov (CSCA) a sú (zvyčajne) samopodpísané. Členské štáty môžu mať viacero takýchto certifikátov (napríklad v prípade regionálneho prenesenia právomocí). Tieto certifikáty CSCA slúžia na pravidelné podpisovanie certifikátov podpisovateľa dokumentov (DSC), pomocou ktorých sa podpisujú potvrdenia HCERT.

„Sekretariát“ predstavuje funkčnú rolu. Pravidelne zhromažďuje a zverejňuje certifikáty DSC členských štátov po ich overení na základe zoznamu certifikátov CSCA (ktoré sa preniesli a overili inými prostriedkami).

Vo výslednom zozname certifikátov DSC sa potom bude nachádzať súhrnný súbor akceptovateľných verejných kľúčov (a zodpovedajúcich identifikátorov kľúčov – kid), pomocou ktorých môžu overovatelia validovať podpisy v potvrdeniach HCERT. Overovatelia musia pravidelne získavať a aktualizovať tento zoznam.

Formát takýchto osobitných zoznamov členských štátov sa môže prispôsobiť ich vlastným vnútroštátnym podmienkam. Formát súboru tohto dôveryhodného zoznamu sa ako taký môže líšiť, môže to byť napríklad podpísaný JWKS (formát súboru JWK podľa časti 5 dokumentu RFC 7517 ([1])) alebo akýkoľvek iný formát špecificky zodpovedajúci technológii používanej v danom členskom štáte.

V záujme jednoduchosti môžu členské štáty buď predložiť svoje existujúce certifikáty CSCA zo svojich systémov ICAO eMRTD, alebo podľa odporúčaní WHO vytvoriť takýto certifikát osobitne pre túto zdravotnú oblasť.

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

▼B

8.1. *Identifikátor kľúča (kid)*

Identifikátor kľúča (kid) sa vypočíta pri vytváraní zoznamu dôveryhodných verejných kľúčov z certifikátov DSC a skladá sa zo skráteného (prvých 8 bajtov) odtlačku SHA-256 certifikátu DSC zakódovaného v (nespracovanom) formáte DER.

Overovatelia nemusia vypočítať identifikátor kid na základe certifikátu DSC a môžu priamo priradiť identifikátor kľúča vo vydanom zdravotnom potvrdení k identifikátoru kid v dôveryhodnom zozname.

8.2. *Rozdiely voči modelu zabezpečenia dôveryhodnosti infraštruktúry verejných kľúčov ICAO eMRTD*

Hoci sa vychádza z najlepších postupov modelu zabezpečenia dôveryhodnosti infraštruktúry verejných kľúčov ICAO eMRTD, v záujme rýchlosti sa pristúpilo k viacerým zjednodušeniam:

— Členské štáty môžu predložiť viaceré certifikáty CSCA.

— Môže sa nastaviť akákoľvek dĺžka obdobia platnosti certifikátu DSC (používanie kľúča), ktorá neprekračuje obdobie platnosti certifikátu CSCA, a obdobie platnosti nemusí byť uvedené.

— Certifikát DSC môže obsahovať identifikátory politiky (rozšírené používanie kľúča), ktoré sú špecifické pre zdravotné potvrdenia.

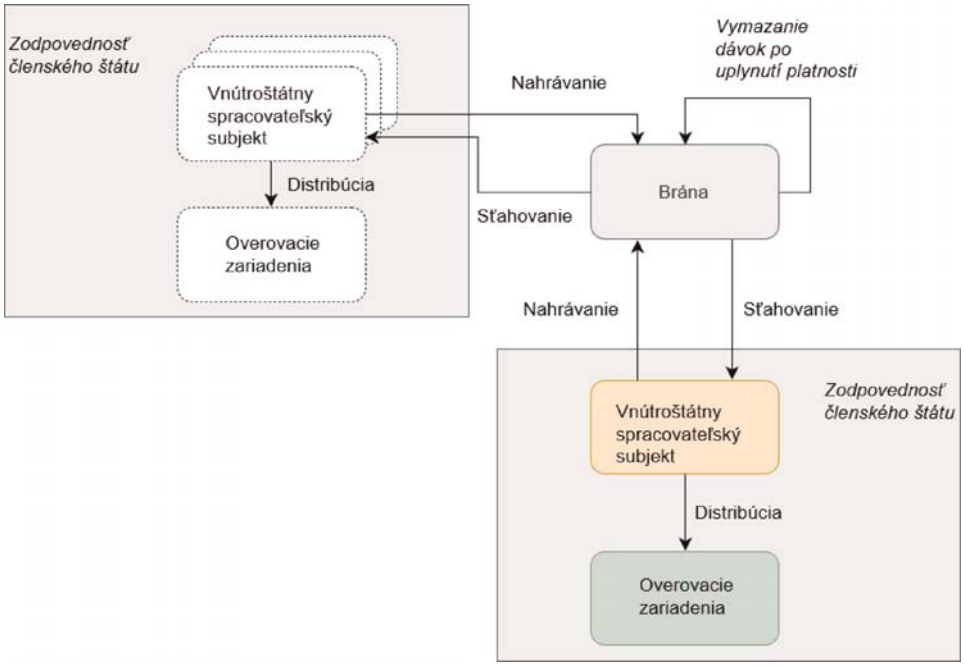
— Členské štáty sa môžu rozhodnúť, že nebudú nikdy vykonávať overenie zverejnených zrušení, ale že sa namiesto toho budú spoliehať len na zoznamy certifikátov DSC, ktoré na dennej báze prijímajú od sekretariátu, alebo si budú zostavovať vlastné zoznamy.

▼M3

9. **Riešenie týkajúce sa postupu zrušenia**

9.1. *Poskytnutie zoznamu zrušených digitálnych COVID preukazov EÚ (DCC)*

Brána poskytuje koncové body a funkcie vedenia a správy zoznamov zrušených potvrdení:



▼M3

9.2. *Model zabezpečenia dôveryhodnosti*

Všetky spojenia sú vytvorené štandardným modelom zabezpečenia dôveryhodnosti DCCG pomocou certifikátov NB_{TLS} a NB_{UP} (pozri správu certifikátov). Všetky informácie sú zbalené a nahraté prostredníctvom správ CMS, aby sa zabezpečila integrita.

9.3. *Vytvorenie dávky*

9.3.1. Dávka

Každý zoznam zrušených potvrdení obsahuje jeden alebo viacero zápisov a balí sa do dávok, ktoré obsahujú súbor hašov (*hashes*) a ich metaúdaje. Dávka je nezameniteľná (*immutable*) a je v nej zadefinovaný dátum uplynutia platnosti, ktorý určuje, kedy ju možno vymazať. Dátum uplynutia platnosti všetkých položiek v dávke musí byť presne rovnaký, čo znamená, že dávky musia byť zoskupené podľa dátumu uplynutia platnosti a podpisu DSC. Každá dávka obsahuje najviac 1 000 zápisov. Ak zoznam zrušených potvrdení obsahuje viac ako 1 000 zápisov, vytvorí sa viacero dávok. Každý zápis sa môže vyskytnúť maximálne v jednej dávke. Dávka sa zbalí do štruktúry CMS a podpíše certifikátom NB_{UP} nahrávajúcej krajiny.

9.3.2. Index dávok (Batch Index)

Pri vytvorení dávky jej brána pridelí jedinečný identifikátor ID a automaticky sa pridá do indexu. Index dávok je zoradený podľa dátumu úprav vo vzostupnom chronologickom poradí.

9.3.3. Správanie brány

Brána spracúva dávky (*batches*) zrušených potvrdení bez akýchkoľvek zmien: dávky nemôže aktualizovať, odstrániť ani do nich pridať žiadne informácie. Dávky sa ďalej zasielajú do všetkých autorizovaných krajín (pozri bod 9.6).

Brána aktívne monitoruje dátumy uplynutia platnosti dávok a dávky po uplynutí platnosti odstraňuje. Po vymazaní dávky brána v prípade adresy URL vymazanej dávky zobrazí hlásenie „HTTP 410 Gone“. Preto sa táto dávka zobrazuje v indexe dávok ako „vymazaná“ (*deleted*).

9.4. *Druhy hašov (Hash Types)*

Zoznam zrušených potvrdení obsahuje haše, ktoré môžu predstavovať rôzne druhy/atribúty zrušených potvrdení. Tieto druhy alebo atribúty sa uvedú pri poskytovaní zoznamov zrušených potvrdení. Aktuálnymi druhmi sú:

Druh	Atribút	Výpočet hašu
SIGNATURE	DCC Signature	SHA256 of DCC Signature
UCI	UCI (Unique Certificate Identifier)	SHA256 of UCI
COUNTRYCODEUCI	Issuing Country Code + UCI	SHA256 of Issuing Country-Code + UCI

Do dávok sa vkladá len prvých 128 bitov hašov kódovaných ako reťazce (*strings*) base64, ktoré sa používajú na identifikáciu zrušeného DCC ([1]).

([1]) Podrobné opisy API sa uvádzajú aj v bode 9.5.1.2.

▼M3

9.4.1. Druh hašu: SHA256(podpis DCC)

V tomto prípade sa haš vypočíta podľa bajtov podpisu COSE_SIGN1 z CWT. V prípade podpisov RSA sa ako vstup použije celý podpis. Vo vzorci v prípade certifikátov podpísaných algoritmom EC-DSA sa používa ako vstup hodnota r:

SHA256(r).

[vyžaduje sa v prípade všetkých nových implementácií]

9.4.2. Druh hašu: SHA256(UCI)

V tomto prípade sa haš vypočíta podľa reťazca UCI kódovaného v UTF-8 a konvertovaného na bajtové pole (*byte array*).

[zastarané ([1]), ale podporované v prípade spätnej kompatibility]

9.4.3. Druh hašu: SHA256(kód vydávajúcej krajiny Issuing CountryCode+UCI)

V tomto prípade kód krajiny CountryCode kódovaný ako reťazec UTF-8 zreťazený s identifikátorom UCI kódovaným pomocou reťazca UTF-8. Ten sa následne konvertuje na bajtové pole a použije sa ako vstup do hašovacej funkcie.

[zastarané [2], ale podporované v prípade spätnej kompatibility]

9.5. *Štruktúra API*

9.5.1. API na zadávanie zápisov zrušených potvrdení

9.5.1.1. Účel

API posiela zápisy zoznamov zrušených potvrdení v dávkach vrátane indexu dávok.

9.5.1.2. Koncové body (endpoints)

9.5.1.2.1. Koncový bod – sťahovanie zoznamu dávok

Koncové body sa riadia jednoduchou koncepciou a vracajú zoznam dávok s malým obalom (*wrapper*) poskytujúcim metaúdaje (*metadata*). Dávky sú roztriedené podľa *dátumu* vo *vzostupnom (chronologickom)* poradí:

/revocation-list

Verb: GET

Content-Type: application/json

Response: JSON Array

```
{
    ‘more‘:true|false,
    ‘batches‘:
            [{
                ‘batchId‘: ‘{uuid}‘,
                ‘country‘: ‘XY‘,
                ‘date‘: ‘2021-11-01T00:00:00Z‘
                ‘deleted‘: true | false
            }, ..
            ]
}
```

([1]) Zastarané znamená, že táto funkcia sa nezohľadňuje pri nových implementáciách, ale podporuje sa v prípade existujúcich implementácií počas presne vymedzeného obdobia.

▼M3

Poznámka: Výsledok je obmedzený na predvolený počet 1 000. Ak je príznak „more“ nastavený na hodnotu „true“, odpoveď naznačuje, že na stiahnutie je k dispozícii viac dávok. Na stiahnutie viacerých položiek musí klient nastaviť záhlavie (*header*) If-Modified-Since na dátum, ktorý nie je skorší ako posledný prijatý zápis.

Odpoveď obsahuje pole JSON s touto štruktúrou:

Pole	Vymedzenie
more	Booleovský príznak, ktorý naznačuje, že existuje viac dávok.
batches	Pole s existujúcimi dávkami.
batchId	https://en.wikipedia.org/wiki/Universally_unique_identifier
country	Kód krajiny podľa normy ISO 3166.
date	Dátum vo formáte UTC podľa normy ISO 8601. Dátum, keď bola dávka pridaná alebo vymazaná.
deleted	boolean. Hodnota „true“ v prípade vymazania. Keď sa nastaví príznak „vymazaný“ (*deleted*), zápis možno s konečnou platnosťou odstrániť z výsledkov vyhľadávania po siedmich dňoch.

9.5.1.2.1.1. *Kódy* odpovedí

Kód	Opis
200	Všetko je v poriadku.
204	Žiadny obsah, ak obsah záhlavia „If-Modified-Since“ nemá zhodu.

Záhlavie požiadavky

Záhlavie	Povinné	Opis
If-Modified-Since	áno	Toto záhlavie obsahuje posledný dátum stiahnutia, aby sa zobrazili len najnovšie výsledky. Pri prvom volaní by záhlavie malo byť nastavené na „2021-06-01T00:00:00Z“.

9.5.1.2.2. Koncový bod – sťahovanie dávok

Dávky obsahujú zoznam identifikátorov potvrdení:

/revocation-list/{batchId}

Verb: GET

Accepts: application/cms

Response:CMS with Content

{

‘country‘: ‘XY‘,

‘expires‘: ‘2022-11-01T00:00:00Z‘,

▼**M3**

‘kid‘:‘23S+33f=‘,

‘hashType’:’SIGNATURE‘,

‘entries‘:[{

‘hash‘:‘e2e2e2e2e2e2e2e2‘

}, ..]

}

Odpoveď obsahuje CMS s podpisom, ktorý sa musí zhodovať s certifikátom NB_{UP} danej krajiny. Všetky položky v poli JSON majú túto štruktúru:

Pole	Povinné	Druh	Vymedzenie
expires	áno	String	Dátum, keď možno položku odstrániť. Dátum/čas vo formáte UTC podľa normy ISO 8601.
country	áno	String	Kód krajiny podľa normy ISO 3166.
hashType	áno	String	Druh hašu zadaných zápisov (pozri Druhy hašov).
entries	áno	JSON Object Array	Pozri tabuľku Zápisy.
kid	áno	String	Identifikátor KID certifikátu DSC s kódovaním base64, ktorý sa použil na podpísanie DCC. Ak KID nie je známy, možno použiť reťazec „UNKNOWN_KID“ (bez „“).

Poznámky:

— Dávky sa zoskupujú podľa dátumu uplynutia platnosti a DSC – platnosť všetkých položiek musí uplynúť v rovnakom čase a musia byť podpísané tým istým kľúčom.

— Čas uplynutia platnosti je dátum/čas vo formáte UTC, pretože EU-DCC je globálny systém a musí sa používať jednoznačný čas.

— Dátum uplynutia platnosti trvalo zrušeného DCC sa stanovuje na dátum uplynutia platnosti príslušného DSC použitého na podpísanie DCC alebo na čas uplynutia platnosti zrušeného DCC (v tomto prípade sa s použitými časmi NumericDate/epoch zaobchádza, ako keby boli v časovom pásme UTC).

— Vnútroštátny spracovateľský subjekt (*National Backend*, NB) odstraňuje položky zo svojho zoznamu zrušených potvrdení po dátume **uplynutia platnosti**.

— NB môže odstrániť položky zo svojho zoznamu zrušených potvrdení, ak bol **kid** použitý na podpísanie DCC zrušený.

▼M3

9.5.1.2.2.1. Zápisy

Pole	Povinné	Druh	Vymedzenie
hash	áno	String	Prvých 128 bitov hašu SHA256 kódovaných ako reťazec base64.

Poznámka: Objekt zápisov aktuálne obsahuje len haš, ale v záujme kompatibility so zmenami v budúcnosti bol namiesto poľa json vybraný objekt.

9.5.1.2.2.2. Kódy odpovedí

Kód	Opis
200	Všetko je v poriadku.
410	Dávka nenájdená. Dávku možno vymazať vo vnútroštátnom spracovateľskom subjekte.

9.5.1.2.2.3. Záhlavia odpovedí

Záhlavie	Opis
ETag	ID dávky.

9.5.1.2.3. Koncový bod – nahrávanie dávok

Nahrávanie sa uskutočňuje cez ten istý koncový bod pomocou slovesa POST (odoslať):

/revocation-list

Verb: POST

Accepts: application/cms

Request: CMS with Content

ContentType: application/cms

Content:

```
{
    ‘country‘: ‘XY‘,
    ‘expires‘: ‘2022-11-01T00:00:00Z‘,
    ‘kid‘:‘23S+33f=‘,
    ‘hashType‘:‘SIGNATURE‘,
    ‘entries‘:[{
        ‘hash‘:‘e2e2e2e2e2e2e2e2‘
        }, ..]
}
```

Dávka sa podpisuje pomocou certifikátu NB_{UP}. Brána overuje, či sa podpis v prípade danej *krajiny* nastavil pomocou NB_{UP}. Ak je kontrola podpisu neúspešná, nahrávanie zlyhá.

POZNÁMKA: Každá dávka je nezameniteľná (*immutable*) a po nahratí ju nemožno zmeniť. Možno ju však vymazať. ID každej vymazanej dávky sa uloží a nahratie novej dávky s rovnakým ID sa zamietne.

▼**M3**

9.5.1.2.4. Koncový bod – vymazanie dávok

Dávku možno vymazať cez ten istý koncový bod pomocou slovesa (*verb*) VYMAZAŤ (*DELETE*):

/revocation-list

Verb: DELETE

Accepts: application/cms

ContentType: application/cms

Request: CMS with Content

Content:

{

‘batchId‘: ‘...‘

}

alebo v záujme kompatibility sa odošle na tento koncový bod pomocou slovesa (*verb*) ODOSLAŤ (*POST*):

/revocation-list/delete

Verb: POST

Accepts: application/cms

ContentType: application/cms

Request: CMS with Content

Content:

{

‘batchId‘: ‘...‘

}

9.6. *Ochrana API/všeobecné nariadenie o ochrane údajov*

V tomto oddiele sa špecifikujú opatrenia na zabezpečenie súladu vykonávania s ustanoveniami nariadenia 2021/953, pokiaľ ide o spracúvanie osobných údajov.

9.6.1. Existujúca autentifikácia

Brána aktuálne používa na autentifikáciu krajín, ktoré sa k nej pripájajú, certifikát NB_{TLS}. Túto autentifikáciu možno použiť na určenie identity krajiny pripojenej k bráne. Uvedená identita sa následne môže použiť na vykonanie kontroly prístupu.

9.6.2. Kontrola prístupu

Brána uplatňuje mechanizmus kontroly prístupu, aby mohla spracúvať osobné údaje v súlade s právnymi predpismi.

V rámci brány sa zavádza zoznam kontroly prístupu v kombinácii s bezpečnosťou na základe rolí. V tomto systéme sa vedú dve tabuľky – jedna tabuľka opisuje, ktoré roly môžu uplatňovať ktoré operácie na ktoré zdroje, a druhá tabuľka opisuje, ktoré roly sú pridelené ktorým používateľom.

Na vykonávanie kontrol požadovaných v tomto dokumente sa vyžadujú tri roly, a to:

RevocationListReader

RevocationUploader

RevocationDeleter

▼**M3**

Uvedené koncové body (*endpoints*) kontrolujú, či má používateľ rolu RevocationListReader; ak má, prístup sa udelí, ak nemá, následne sa zobrazí hlásenie HTTP 403 Forbidden:

GET/revocation-list/

GET/revocation-list/{batchId}

Uvedené koncové body kontrolujú, či má používateľ (*User*) rolu (*Role*) RevocationUploader; ak má, prístup sa udelí, ak nemá, následne sa zobrazí hlásenie HTTP 403 Forbidden:

POST/revocation-list

Uvedené koncové body kontrolujú, či má používateľ rolu RevocationDeleter; ak má, prístup sa udelí, ak nemá, následne sa zobrazí hlásenie HTTP 403 Forbidden:

DELETE/revocation-list

POST/revocation-list/delete

Brána takisto poskytuje spoľahlivú metódu, pomocou ktorej správcovia môžu spravovať roly spojené s používateľmi, a to takým spôsobom, aby sa znížila pravdepodobnosť ľudských chýb a aby sa zároveň nezaťažovali funkční správcovia.

▼M1

PRÍLOHA II

PRAVIDLÁ NA ÚČELY VYPĹŇANIA DIGITÁLNEHO COVID PREUKAZU EÚ

Cieľom všeobecných pravidiel týkajúcich sa súborov hodnôt, ktoré sa stanovujú v tejto prílohe, je zabezpečiť interoperabilitu na sémantickej úrovni a umožniť jednotné technické vykonávanie digitálneho COVID preukazu EÚ. Prvky uvedené v tejto prílohe možno použiť v troch odlišných kontextoch (očkovanie/testovanie/prekonanie ochorenia), ako sa stanovuje v nariadení (EÚ) 2021/953. V tejto prílohe sa uvádzajú len prvky, pri ktorých sa vyžaduje sémantická normalizácia prostredníctvom kódovaných súborov hodnôt.

Za preklad kódovaných prvkov do svojho úradného jazyka zodpovedajú príslušné členské štáty.

Pre všetky dátové polia, ktoré nie sú uvedené v nasledujúcich opisoch súborov hodnôt, sa kódovanie opisuje v prílohe V.

Ak z akéhokoľvek dôvodu nemožno použiť uprednostňované systémy kódov uvedené ďalej, môžu sa použiť iné medzinárodné systémy kódov, pričom sa zverejní usmernenie k spôsobu priradenia kódov z iného systému kódov k uprednostňovanému systému kódov. Vo výnimočných prípadoch sa môže použiť text (zobrazované názvy) ako záložný mechanizmus, keď vo vymedzených súboroch hodnôt nie je k dispozícii vhodný kód.

Členské štáty, ktoré vo svojich systémoch používajú iné kódovanie, priradia takéto kódy k opísaným súborom hodnôt. Za každé takéto priradenie zodpovedajú členské štáty.

►M4 Keďže niektoré súbory hodnôt založené na systémoch kódov stanovených v tejto prílohe, ako napríklad súbory hodnôt na kódovanie vakcín a antigénových testov, sa často menia, Komisia ich s podporou siete elektronického zdravotníctva a Výboru pre zdravotnú bezpečnosť uverejňuje a pravidelne aktualizuje. ◄ Aktualizované súbory hodnôt sa zverejnia na príslušnom webovom sídle Komisie, ako aj na webovej stránke siete elektronického zdravotníctva. História zmien sa sprístupní.

1. **Ochorenie alebo pôvodca ochorenia, na ktoré sa potvrdenie vzťahuje/ochorenie alebo pôvodca ochorenia, ktoré držiteľ prekonal: ochorenie COVID-19 (vírus SARS-CoV-2 alebo niektorý z jeho variantov)**

   Má sa používať v potvrdení 1, 2 a 3.

   Používajú sa tieto kódy:

Kód	Zobrazenie	Názov systému kódov	URL systému kódov	OID systému kódov	Verzia systému kódov
840539006	COVID-19	SNOMED CT	http://snomed.info/sct	2.16.840.1.113883.6.96	2021-01-31

2. **Vakcína alebo profylaxia proti ochoreniu COVID-19**

   Uprednostňovaný systém kódov: SNOMED CT alebo klasifikácia ATC.

   Má sa používať v potvrdení 1.

   Medzi príklady kódov, ktoré sa použijú z uprednostňovaných systémov kódov, patrí kód SNOMED CT 1119305005 (vakcína s antigénmi proti vírusu SARS-CoV-2), 1119349007 (vakcína mRNA proti vírusu SARS-CoV-2) alebo J07BX03 (vakcíny proti ochoreniu COVID-19).

   Komisia s podporou siete elektronického zdravotníctva uverejní a pravidelne aktualizuje súbor hodnôt, v ktorom sa určujú kódy, ktoré sa majú používať podľa systémov kódov stanovených v tomto oddiele. Keď sa vyvinú a začnú používať nové typy vakcín, súbor hodnôt sa rozšíri.

▼M1

3. **Vakcinačná látka proti ochoreniu COVID-19**

Uprednostňované systémy kódov (v uprednostňovanom poradí):

— register liekov Únie pre vakcíny s povolením pre celú EÚ (čísla povolení),

— celosvetový register vakcín, napríklad register, ktorý by mohla zriadiť Svetová zdravotnícka organizácia,

— v ostatných prípadoch názov vakcinačnej látky. Ak názov obsahuje medzery, nahradia sa spojovníkom (-).

Názov súboru hodnôt: Vakcína.

Má sa používať v potvrdení 1.

Príkladom kódu, ktorý sa použije z uprednostňovaných systémov kódov, je EU/1/20/1528 (Comirnaty). Príklad názvu vakcíny, ktorý sa má použiť ako kód: Sputnik-V (označuje Sputnik V).

Komisia s podporou siete elektronického zdravotníctva uverejní a pravidelne aktualizuje súbor hodnôt, v ktorom sa určujú kódy, ktoré sa majú používať podľa systémov kódov stanovených v tomto oddiele.

Vakcíny sa kódujú pomocou existujúceho kódu z uverejneného súboru hodnôt, aj keď sa ich názvy v jednotlivých krajinách líšia. Dôvodom je, že zatiaľ neexistuje celosvetový register vakcín, ktorý by zahŕňal všetky v súčasnosti používané vakcíny. Príklad:

— V prípade vakcíny „COVID-19 Vaccine Moderna Intramuscular Injection“, čo je názvov vakcíny Spikevax v Japonsku, použite kód EU/1/20/1507, keďže takto sa táto vakcína nazýva v EÚ.

Ak to v danom prípade nie je možné alebo vhodné, v uverejnenom súbore hodnôt sa uvedenie samostatný kód.

▼M4

Ak sa krajina, ktorá používa digitálny COVID preukaz EÚ, rozhodne vydávať potvrdenia o očkovaní účastníkom klinického skúšania počas prebiehajúceho klinického skúšania, vakcinačná látka sa kóduje podľa vzoru

CT*_clinical-trial-identifier*

Ak bolo klinické skúšanie zaregistrované v registri klinických skúšaní EÚ (EU-CTR), použije sa identifikátor klinického skúšania z tohto registra. V iných prípadoch sa môžu použiť identifikátory z iných registrov (ako sú webové stránky clinicaltrials.gov alebo austrálsko-novozélandský register klinických skúšaní).

Identifikátor klinického skúšania musí obsahovať predponu umožňujúcu identifikáciu registra klinických skúšaní (ako je EUCTR pre register klinického skúšania EÚ, NCT pre clinicaltrials.gov, ACTRN pre austrálsko-novozélandský register klinických skúšaní).

Ak Komisia dostane usmernenie od Výboru pre zdravotnú bezpečnosť, Európskeho centra pre prevenciu a kontrolu chorôb (ECDC) alebo Európskej agentúry pre lieky (EMA), pokiaľ ide o uznávanie potvrdení vydaných pre vakcínu proti ochoreniu COVID-19, ktorá je predmetom klinického skúšania, uvedené usmernenie sa uverejní buď ako súčasť dokumentu obsahujúceho súbor hodnôt, alebo samostatne.

▼M1

4. **Držiteľ povolenia na uvedenie vakcíny proti ochoreniu COVID-19 na trh alebo jej výrobca**

Uprednostňovaný systém kódov:

— kód organizácie podľa EMA (systém SPOR pre normu ISO IDMP),

— celosvetový register držiteľov povolenia na uvedenie vakcíny na trh alebo výrobcov vakcín, napríklad register, ktorý by mohla zriadiť Svetová zdravotnícka organizácia,

— v ostatných prípadoch názov organizácie. Ak názov obsahuje medzery, nahradia sa spojovníkom (-).

Má sa používať v potvrdení 1.

Príkladom kódu, ktorý sa použije z uprednostňovaného systému kódov, je ORG-100001699 (AstraZeneca AB). Príklad názvu organizácie, ktorý sa má použiť ako kód: Sinovac-Biotech (označuje Sinovac Biotech).

Komisia s podporou siete elektronického zdravotníctva uverejní a pravidelne aktualizuje súbor hodnôt, v ktorom sa určujú kódy, ktoré sa majú používať podľa systémov kódov stanovených v tomto oddiele.

Rôzne pobočky toho istého držiteľa povolenia na uvedenie na trh alebo toho istého výrobcu použijú existujúci kód z uverejneného súboru hodnôt.

Vo všeobecnosti platí, že v prípade tej istej vakcinačnej látky sa použije kód označujúci držiteľa povolenia na jej uvedenie na trh v EÚ, keďže zatiaľ neexistuje medzinárodne dohodnutý register výrobcov vakcín alebo držiteľov povolenia na ich uvedenie na trh. Príklady:

— V prípade organizácie „Pfizer AG“, ktorá je držiteľom povolenia na uvedenie na trh pre vakcínu „Comirnaty“ používanú vo Švajčiarsku, použite kód ORG-100030215 označujúci spoločnosť BioNTech Manufacturing GmbH, keďže táto spoločnosť je držiteľom povolenia na uvedenie vakcíny Comirnaty na trh v EÚ.

— V prípade organizácie „Zuellig Pharma“, ktorá je držiteľom povolenia na uvedenie na trh pre vakcínu proti ochoreniu COVID-19 Moderna (Spikevax) používanú na Filipínach, použite kód ORG-100031184 označujúci spoločnosť Moderna Biotech Spain S.L., keďže táto spoločnosť je držiteľom povolenia na uvedenie vakcíny Spikevax na trh v EÚ.

Ak to v danom prípade nie je možné alebo vhodné, v uverejnenom súbore hodnôt sa uvedenie samostatný kód.

▼M4

Ak sa krajina, ktorá používa digitálny COVID preukaz EÚ, rozhodne vydávať potvrdenia o očkovaní účastníkom klinického skúšania počas prebiehajúceho klinického skúšania, držiteľ povolenia na uvedenie vakcíny na trh alebo výrobca vakcíny sa kóduje pomocou hodnoty, ktorá mu bola určená v stanovenom súbore hodnôt, ak je k dispozícii. V ostatných prípadoch sa držiteľ povolenia na uvedenie vakcíny na trh alebo výrobca vakcíny kóduje podľa pravidla opísaného v oddiele 3 Vakcinačná látka (CT_*clinical-trial-identifier*).

▼M1

5. **Poradie v sérii dávok, ako aj celkový počet dávok v sérii**

Má sa používať v potvrdení 1.

Dve polia:

1. Poradie v sérii vakcinačných dávok vakcíny proti ochoreniu COVID-19 (N),

2. Celkový počet dávok vo vakcinačnej sérii (C).

5.1. *Primárna vakcinačná séria*

Ak sa osobe podávajú dávky primárnej vakcinačnej série, t. j. vakcinačnej série určenej na zabezpečenie dostatočnej ochrany v počiatočnom štádiu, (C) musí vyjadrovať celkový počet dávok štandardnej primárnej vakcinačnej série (napr. 1 alebo 2, v závislosti od typu podanej vakcíny). Zahŕňa to aj možnosť použitia kratšej série (C = 1), ak sa vo vakcinačnom protokole používanom členským štátom stanovuje podanie jedinej dávky 2-dávkovej vakcíny osobám, ktoré boli už predtým infikované vírusom SARS-CoV-2. Dokončená primárna vakcinačná séria sa preto označí ako N/C = 1. Napríklad:

— Označenie 1/1 by znamenalo, že sa dokončila primárna 1-dávková vakcinačná séria, resp. že sa dokončila primárna séria pozostávajúca z jednej dávky 2-dávkovej vakcíny podanej osobe, ktorá prekonala ochorenie, v súlade s vakcinačným protokolom používaným členským štátom;

— Označenie 2/2 by znamenalo, že sa dokončila primárna 2-dávková vakcinačná séria.

Ak je primárna vakcinačná séria rozšírená, napríklad v prípade osôb s vážne oslabeným imunitným systémom, alebo ak nebol dodržaný odporúčaný interval medzi primárnymi dávkami, všetky takéto dávky sa kódujú ako dodatočné dávky patriace do oddielu 5.2.

▼M2

5.2. *Posilňovacie dávky*

Ak sú osobe podané dávky po primárnej vakcinačnej sérii, takéto posilňovacie dávky sa v príslušných potvrdeniach uvedú takto:

— Označenie 2/1 znamená, že bola podaná posilňovacia dávka po primárnej 1-dávkovej vakcinačnej sérii, resp. že bola podaná posilňovacia dávka po dokončení primárnej série pozostávajúcej z jednej dávky 2-dávkovej vakcíny podanej osobe, ktorá prekonala ochorenie, v súlade s vakcinačným protokolom používaným členským štátom. Potom sa dávky (X) podané po prvej posilňovacej dávke uvedú ako (2 + X)/(1) > 1 (napríklad 3/1).

— Označenie 3/3 znamená, že bola podaná posilňovacia dávka po primárnej 2-dávkovej vakcinačnej sérii. Potom sa dávky (X) podané po prvej posilňovacej dávke uvedú ako (3 + X)/(3 + X) = 1 (napríklad 4/4).

Členské štáty zavedú pravidlá kódovania stanovené v tomto oddiele do 1. februára 2022.

Členské štáty automaticky alebo na žiadosť dotknutých osôb opätovne vydajú potvrdenia, v ktorých je podanie posilňovacej dávky po primárnej 1-dávkovej vakcinačnej sérii kódované takým spôsobom, že ho nemožno odlíšiť od dokončenia primárnej vakcinačnej série.

▼M2

Na účely tejto prílohy by sa odkazy na „posilňovacie dávky“ mali chápať tak, že zahŕňajú aj dodatočné dávky podávané na lepšiu ochranu jednotlivcov, ktorí po dokončení štandardnej primárnej vakcinačnej série vykazujú neadekvátne imunitné reakcie. V medziach právneho rámca stanoveného nariadením (EÚ) 2021/953 môžu členské štáty prijať opatrenia na riešenie situácie zraniteľných skupín, ktorým sa môžu dodatočné dávky podávať prednostne. Ak sa napríklad členský štát rozhodne podávať dodatočné dávky len určitým podskupinám obyvateľstva, môže sa v súlade s článkom 5 ods. 1 nariadenia (EÚ) 2021/953 rozhodnúť, že vystaví potvrdenia o očkovaní uvádzajúce podanie takýchto dodatočných dávok len na požiadanie, a nie automaticky. Ak sa takéto opatrenia prijmú, členské štáty informujú dotknuté osoby o takýchto opatreniach, ako aj o tom, že môžu naďalej používať potvrdenie získané po dokončení štandardnej primárnej vakcinačnej série.

▼M1

6. **Členský štát alebo tretia krajina, kde bola podaná vakcína/kde sa vykonal test**

Uprednostňovaný systém kódov: kódy krajiny podľa normy ISO 3166.

Má sa používať v potvrdení 1, 2 a 3.

Obsah súboru hodnôt: úplný zoznam kódov pozostávajúcich z dvoch písmen, k dispozícii ako súbor hodnôt vymedzených v rámci FHIR (http://hl7.org/fhir/ValueSet/iso3166-1-2). Ak očkovanie alebo test vykonala medzinárodná organizácia (ako napríklad UNHCR alebo WHO), no nie sú k dispozícii žiadne informácie o krajine, použije sa kód organizácie. Komisia s podporou siete elektronického zdravotníctva takéto dodatočné kódy uverejní a pravidelne aktualizuje.

7. **Typ testu**

Má sa používať v potvrdení 2 a, ak sa prostredníctvom delegovaného aktu zavedie podpora pre vydávanie potvrdení o prekonaní ochorenia na základe iných typov testov, než je test NAAT, tak aj v potvrdení 3.

Používajú sa tieto kódy:

Kód	Zobrazenie	Názov systému kódov	URL systému kódov	OID systému kódov	Verzia systému kódov
LP6464-4	Amplifikácia nukleových kyselín s použitím sondy na detekciu	LOINC	http://loinc.org	2.16.840.1.113883.6.1	2.69
LP217198-3	Rýchly imunologický test	LOINC	http://loinc.org	2.16.840.1.113883.6.1	2.69

▼M4

Kód LP217198-3 (rýchly imunologický test) sa používa na označenie rýchlych antigénových testov, ako aj laboratórnych antigénových analýz.

▼M1

8. **Výrobca a obchodný názov použitého testu (voliteľné pre test NAAT)**

Má sa používať v potvrdení 2.

▼M4

Obsah súboru hodnôt zahŕňa výber antigénových testov, ako sa uvádzajú v spoločnom a aktualizovanom zozname antigénových testov na COVID-19 vytvorenom na základe odporúčania Rady 2021/C 24/01, ktorý odsúhlasil Výbor pre zdravotnú bezpečnosť. Zoznam vedie Spoločné výskumné centrum v databáze diagnostických pomôcok a testovacích metód in vitro zameraných na COVID-19 na adrese: https://covid-19-diagnostics.jrc.ec.europa.eu/devices/hsc-common-recognition-rat.

▼M1

V prípade tohto systému kódov sa použijú príslušné polia, ako je identifikátor testovacej pomôcky, názov testu a výrobca, a to podľa štruktúrovaného formátu Spoločného výskumného centra, ktorý je k dispozícii na adrese: https://covid-19-diagnostics.jrc.ec.europa.eu/devices

9. **Výsledok testu**

Má sa používať v potvrdení 2.

Používajú sa tieto kódy:

Kód	Zobrazenie	Názov systému kódov	URL systému kódov	OID systému kódov	Verzia systému kódov
260415000	Prítomnosť nezistená	SNOMED CT	http://snomed.info/sct	2.16.840.1.113883.6.96	2021-01-31
260373001	Prítomnosť zistená	SNOMED CT	http://snomed.info/sct	2.16.840.1.113883.6.96	2021-01-31

▼B

PRÍLOHA III

SPOLOČNÁ ŠTRUKTÚRA JEDINEČNÉHO IDENTIFIKÁTORA POTVRDENIA

1. **Úvod**

Každý digitálny COVID preukaz EÚ obsahuje jedinečný identifikátor potvrdenia (ďalej len „UCI“), ktorý podporuje interoperabilitu digitálneho COVID preukazu EÚ. Jedinečný identifikátor potvrdenia sa môže použiť na overenie potvrdenia. Členské štáty sú zodpovedné za zavedenie jedinečného identifikátora potvrdenia. Jedinečný identifikátor potvrdenia je prostriedok na overenie pravosti potvrdenia, prípadne na prepojenie na registračný systém (napríklad IIS). Tieto identifikátory zároveň musia členským štátom umožňovať (v papierovej a digitálnej podobe) vyhlásiť, že jednotlivci boli očkovaní alebo testovaní.

2. **Zloženie jedinečného identifikátora potvrdenia**

Jedinečný identifikátor potvrdenia má spoločnú štruktúru a formát, ktoré uľahčujú ľudskú a/alebo strojovú čitateľnosť informácií a ktoré sa môžu týkať prvkov, ako je členský štát očkovania, samotná očkovacia látka a špecifický identifikátor členského štátu. Členským štátom poskytuje flexibilitu pri formátovaní, a to pri plnom rešpektovaní právnych predpisov v oblasti ochrany údajov. Z hľadiska poradia osobitných prvkov sa dodržiava vymedzená hierarchia, vďaka ktorej sú možné budúce úpravy blokov pri súčasnom zachovaní štrukturálnej integrity.

Možné riešenia zloženia UCI tvoria spektrum, v ktorom sa uplatňuje modularita a ľudská čitateľnosť ako dva hlavné diverzifikujúce parametre, ako aj jedna základná vlastnosť:

— modularita: miera, do akej je kód zložený zo samostatných stavebných blokov, ktoré obsahujú sémanticky odlišné informácie,

— ľudská čitateľnosť: miera, do akej je kód zmysluplný alebo čitateľný pre človeka,

— globálna jedinečnosť: identifikátor krajiny alebo orgánu je vhodne riadený a očakáva sa, že každá krajina (orgán) vhodne riadi svoj segment priestoru názvov tak, aby sa identifikátory nikdy nerecyklovali ani sa opätovne nevydávali. Touto kombináciou sa zabezpečí, že každý identifikátor je globálne jedinečný.

▼M1

3. **Všeobecné požiadavky**

Vo vzťahu k UCI sa vyžaduje splnenie týchto súhrnných požiadaviek:

1. znaková sada: povoľujú sa len alfanumerické znaky veľkých písmen US-ASCII („A“ až „Z“, „0“ až „9“); s dodatočnými osobitnými oddeľovacími znakmi z dokumentu RFC3986 ([1]), konkrétne {„/“, „#“, „:“};

2. maximálna dĺžka: tvorcovia sa musia snažiť dodržať dĺžku 27 – 30 znakov ([2]);

3. predpona verzie: vzťahuje sa na verziu schémy UCI. Predpona verzie pre túto verziu dokumentu je „01“; predpona verzie je zložená z dvoch číslic;

([1]) rfc3986 (ietf.org)

([2]) Na používanie QR kódov by členské štáty mohli zvážiť dodatočný súbor znakov do celkovej dĺžky 72 znakov (vrátane 27 – 30 znakov samotného identifikátora), ktorý sa môže použiť na poskytnutie ďalších informácií. Špecifikáciu týchto informácií vymedzia členské štáty.

▼M1

4. predpona krajiny: kód krajiny sa určuje na základe normy ISO 3166-1. Dlhšie kódy [napr. 3 a viac znakov (napríklad „UNHCR“)] sú vyhradené na budúce použitie;

5. prípona kódu/kontrolný súčet:

5.1 Členské štáty môžu využiť kontrolný súčet, keď je pravdepodobné, že môže dôjsť k prenosu, prepisu (človekom) alebo k iným znehodnoteniam (napríklad pri použití v tlačenej podobe).

5.2 Na kontrolný súčet sa nemožno spoliehať pri overovaní platnosti potvrdenia a technicky nie je súčasťou identifikátora, ale slúži na overenie integrity kódu. Týmto kontrolným súčtom je zhrnutie celého UCI v digitálnom/elektronickom prenosovom formáte podľa normy ISO-7812-1 (LUHN-10) ([1]). Kontrolný súčet je od zvyšku UCI oddelený znakom „#“.

Zabezpečí sa spätná kompatibilita: členské štáty, ktoré postupom času zmenia štruktúru svojich identifikátorov (v rámci hlavnej verzie, v súčasnosti stanovenej na v1), zabezpečia, že akékoľvek dva identické identifikátory sa vzťahujú na rovnaké potvrdenie/vyhlásenie o očkovaní. Inými slovami, členské štáty nemôžu identifikátory opätovne používať.

▼B

4. **Možnosti jedinečného identifikátora potvrdenia pre potvrdenia o očkovaní**

V usmerneniach siete elektronického zdravotníctva o overiteľných potvrdeniach o očkovaní a základných prvkoch interoperability ([2]) sa uvádzajú rôzne možnosti dostupné členským štátom a iným stranám, ktoré môžu súbežne existovať naprieč rôznymi členskými štátmi. Členské štáty môžu využiť takéto rôzne možnosti v rôznych verziách schémy UCI.

([1]) Luhnov algoritmus modulu N je rozšírením Luhnovho algoritmu (známeho aj ako algoritmus modulu 10), ktorý funguje pre číselné kódy a používa sa napríklad na výpočet kontrolného súčtu kreditných kariet. Týmto rozšírením sa umožní, aby algoritmus fungoval so sekvenciami hodnôt na akomkoľvek základe (v našom prípade abecedné znaky).

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

▼B

PRÍLOHA IV

SPRÁVA CERTIFIKÁTOV VEREJNÉHO KĽÚČA

1. **Úvod**

Bezpečná a dôveryhodná výmena podpisových kľúčov pre digitálne COVID preukazy EÚ (ďalej len „DCC“) medzi členskými štátmi sa realizuje prostredníctvom brány digitálnych COVID preukazov EÚ (ďalej len „DCCG“), ktorá slúži ako centrálne úložisko verejných kľúčov. Členské štáty sú prostredníctvom DCCG oprávnené zverejňovať verejné kľúče zodpovedajúce súkromným kľúčom, ktoré využívajú na podpisovanie digitálnych COVID preukazov. Členské štáty, ktoré túto možno využívajú, môžu použiť DCCG na včasné získanie aktuálneho materiálu verejných kľúčov. DCCG sa neskôr môže rozšíriť na výmenu dôveryhodných doplňujúcich informácií, ktoré poskytujú členské štáty, ako sú pravidlá validácie DCC. Modelom dôvery rámca DCC je infraštruktúra verejných kľúčov (PKI). Každý členský štát udržiava jeden alebo viac národných orgánov certifikácie podpisov (ďalej len „CSCA“), ktorých certifikáty majú pomerne dlhú životnosť. Na základe rozhodnutia členského štátu môže byť CSCA rovnaký alebo odlišný od CSCA použitého v prípade strojovo čitateľných cestovných dokladov. CSCA vystavuje certifikáty verejného kľúča pre vnútroštátnych, krátkodobých podpisovateľov dokumentov (t. j. podpisujúce subjekty pre DCC), ktoré sa označujú ako certifikáty podpisovateľa dokumentov (ďalej len „DSC“). CSCA vystupuje ako bod dôvery (trust anchor), aby členské štáty, ktoré túto možno využívajú, mohli využiť certifikát CSCA na overenie pravosti a integrity pravidelne sa meniacich certifikátov DSC. Po validácii môžu členské štáty poskytnúť tieto certifikáty (alebo len v nich obsiahnuté verejné kľúče) svojim aplikáciám na validáciu DCC. DCCG sa okrem CSCA a DSC spolieha aj na PKI pri autentifikácii transakcií a podpisovaní údajov, pričom slúži aj ako základ pre autentifikáciu a ako prostriedok na zabezpečenie integrity komunikačných kanálov medzi členskými štátmi a DCCG.

Na zaistenie integrity a pravosti údajov je možné použiť digitálne podpisy. Infraštruktúry verejných kľúčov vytvárajú dôveru previazaním verejných kľúčov s overenými identitami (alebo vystaviteľmi). To je nevyhnutné, aby si ostatní účastníci mohli overiť pôvod údajov a identitu komunikačného partnera a rozhodnúť sa, či im budú dôverovať. V DCGG sa v záujme zabezpečenia pravosti využívajú viaceré certifikáty verejného kľúča. V tejto prílohe sa vymedzuje, ktoré certifikáty verejného kľúča sa využívajú a ako by sa mali navrhnúť, aby umožnili širokú interoperabilitu medzi členskými štátmi. Poskytujú sa v nej ďalšie podrobnosti o potrebných certifikátoch verejného kľúča a uvádza sa v nej usmernenie o vzoroch certifikátov a obdobiach platnosti pre členské štáty, ktoré chcú prevádzkovať svoje vlastné CSCA. Keďže DCC musia byť overiteľné počas vymedzeného časového rámca (počnúc vydaním, pričom platnosť uplynie po danom čase), je potrebné vymedziť model overenia pre všetky podpisy použité na certifikátoch verejného kľúča a DCC.

2. **Terminológia**

V nasledujúcej tabuľke sa uvádzajú skratky a terminológia použitá v tejto prílohe.

Termín	Vymedzenie pojmu
Certifikát	Alebo certifikát verejného kľúča. Certifikát X.509 v3, ktorý obsahuje verejný kľúč subjektu

▼B

Termín	Vymedzenie pojmu
CSCA	Národný orgán certifikácie podpisov
DCC	Digitálny COVID preukaz EÚ. Podpísaný digitálny dokument, ktorý obsahuje informácie o očkovaní, testovaní alebo prekonaní ochorenia
DCCG	Brána digitálneho COVID preukazu EÚ. Tento systém sa používa na výmenu DSC medzi členskými štátmi.
$DCCG_{TA}$	Certifikát bodu dôvery DCCG. Zodpovedajúci súkromný kľúč sa používa na podpísanie zoznamu všetkých certifikátov CSCA offline
$DCCG_{TLS}$	Certifikát TLS servera DCCG
DSC	Certifikát podpisovateľa dokumentov. Certifikát verejného kľúča orgánu členského štátu podpisujúceho dokumenty (napríklad systém, ktorý má povolenie podpisovať DCC). Tento certifikát vystavuje CSCA členského štátu.
EC-DSA	Algoritmus digitálneho podpisu na báze eliptických kriviek (Elliptic Curve Digital Signature Algorithm). Algoritmus kryptografického podpisu na základe eliptických kriviek
Členský štát	členský štát Európskej únie
mTLS	Vzájomný protokol TLS Protokol TLS (Transport Layer Security) so vzájomnou autentifikáciou
NB	Vnútroštátny spracovateľský subjekt („backend“) členského štátu
NB_{CSCA}	Certifikát národného orgánu certifikácie podpisov členského štátu (môže ich byť viacero)
NB_{TLS}	Certifikát klientskej autentifikácie TLS vnútroštátneho spracovateľského subjektu
NB_{UP}	Certifikát, ktorý vnútroštátny spracovateľský subjekt používa na podpisovanie dátových balíkov, ktoré sa nahrávajú do DCCG
PKI	Infraštruktúra verejných kľúčov. Model dôvery založený na certifikátoch verejného kľúča a certifikačných autoritách
RSA	Asymetrický kryptografický algoritmus založený na celočíselnej faktorizácii, ktorý sa používa pre digitálne podpisy alebo asymetrické šifrovanie

3. **Komunikačné toky a služby zabezpečenia DCCG**

V tomto oddiele sa uvádza prehľad komunikačných tokov a služieb zabezpečenia v systéme DCCG. Takisto sa v ňom vymedzuje, ktoré kľúče a certifikáty sa používajú na ochranu komunikácie, nahraných informácií, DCC a podpísaného dôveryhodného zoznamu, ktorý obsahuje všetky nahrané certifikáty CSCA. Brána DCCG funguje ako dátový uzol, ktorý umožňuje výmenu podpísaných balíkov údajov pre členské štáty.

▼B

Nahrané balíky údajov poskytuje DCCG „tak, ako sú“, čo znamená, že DCCG nepridáva ani neodstraňuje DSC v prípade balíkov, ktoré prijíma. Vnútroštátny spracovateľský subjekt (national backend – NB) členských štátov musí byť schopný overiť integritu a pravosť nahraných údajov medzi koncovými bodmi. Vnútroštátne spracovateľské subjekty a DCCG okrem toho využijú vzájomnú autentifikáciu TLS na vytvorenie zabezpečeného spojenia. Predstavuje to dodatok k podpisom vo vymieňaných údajoch.

3.1. *Autentifikácia a nadviazanie spojenia*

DCCG používa zabezpečenie TSL (Transport Layer Security) so vzájomnou autentifikáciou s cieľom vytvoriť autentifikovaný šifrovaný kanál medzi vnútroštátnym spracovateľským subjektom (NB) členského štátu a prostredím brány. DCCG má preto serverový certifikát TLS (skratka $DCCG_{TLS}$) a vnútroštátny spracovateľský subjekt má klientský certifikát TLS (skratka NB_{TLS}). Vzory certifikátov sa uvádzajú v *oddiele 5*. Každý vnútroštátny spracovateľský subjekt môže poskytnúť svoj vlastný certifikát TLS. Tento certifikát sa výslovne uvedie na bielu listinu, a teda ho môže vystaviť verejne dôveryhodná certifikačná autorita (napríklad certifikačná autorita, ktorá dodržiava základné požiadavky organizácie CA/Browser Forum), národná certifikačná autorita alebo môže ísť o samopodpísaný certifikát. Každý členský štát je zodpovedný za svoje vnútroštátne údaje a za ochranu súkromného kľúča použitého na vytvorenie spojenia s DCCG. Prístup na základe poskytnutia vlastného certifikátu si vyžaduje vhodne vymedzený proces registrácie a identifikácie, ako aj postupy zrušenia a obnovenia, ako sa uvádza v *oddieloch 4.1, 4.2* a *4.3*. DSSG využíva bielu listinu, na ktorú sa po úspešnej registrácii pridávajú certifikáty TLS vnútroštátnych spracovateľských subjektov. Len vnútroštátne spracovateľské subjekty, ktoré sa autentifikujú súkromným kľúčom, ktorý zodpovedá certifikátu z bielej listiny, môžu vytvoriť zabezpečené spojenie s DCCG. DCCG takisto použije certifikát TLS, ktorý vnútroštátnym spracovateľským subjektom umožňuje overiť, že naozaj vytvárajú spojenie so „skutočnou“ DCCG a nie so subjektom so zlými úmyslami, ktorý vystupuje ako DCCG. Certifikát DCCG sa poskytne vnútroštátnym spracovateľským subjektom po úspešnej registrácii. Certifikát $DCCG_{TLS}$ vystaví verejne dôveryhodná certifikačná autorita (začlenená vo všetkých hlavných prehliadačoch). Povinnosťou členských štátov je overiť, že je ich spojenie s DCCG zabezpečené (napríklad kontrolou odtlačku certifikátu $DCCG_{TLS}$ pripojeného servera voči odtlačku poskytnutému po registrácii).

3.2. *Národné orgány certifikácie podpisov a model validácie*

Členské štáty, ktoré sa zúčastňujú na rámci DCCG, musia pri vystavovaní DSC využiť CSCA. Členské štáty môžu mať viac než jeden CSCA, napríklad v prípade regionálneho prenesenia právomocí. Každý členský štát môže buď využiť existujúce certifikačné autority, alebo si pre systém DCC môže vytvoriť špecifickú certifikačnú autoritu (prípadne samopodpísanú).

Členské štáty musia predložiť svoj certifikát (certifikáty) CSCA prevádzkovateľovi DCCG počas oficiálneho postupu nadviazania spolupráce. Prevádzkovateľ DCCG po úspešnej registrácii členského štátu (*pozri ďalšie informácie v oddiele 4.1*) aktualizuje podpísaný dôveryhodný zoznam, ktorý obsahuje všetky certifikáty CSCA, ktoré sú aktívne v rámci DCC. Prevádzkovateľ DCCG použije vyhradený asymetrický kľúčový pár na podpísanie dôveryhodného zoznamu a certifikátov v offline prostredí. Súkromný kľúč sa nebude uchovávať v online systéme DCCG, aby narušenie online systému neumožnilo útočníkovi narušiť dôveryhodný zoznam. Zodpovedajúci certifikát bodu dôvery $DCCG_{TA}$ sa poskytne vnútroštátnym spracovateľským subjektom počas postupu nadviazania spolupráce.

▼B

Členské štáty môžu získať dôveryhodný zoznam od DCCG pre svoje postupy overenia. CSCA sa vymedzuje ako certifikačná autorita, ktorá vystavuje DSC, a teda členské štáty, ktoré využívajú viacúrovňovú hierarchiu certifikačných autorít (napríklad koreňová CA-> CSCA -> DSC), musia zabezpečiť podriadenú certifikačnú autoritu, ktorá vystavuje DSC. V tomto prípade, ak členský štát využíva existujúcu certifikačnú autoritu, systém DCC bude ignorovať všetko nad úrovňou CSCA a na bielu listinu uvedie len CSCA ako bod dôvery (hoci ide o podriadenú certifikačnú autoritu). Zodpovedá to modelu ICAO, umožňuje však len presne dve úrovne – „koreňový“ CSCA a koncový („listový“) DSC podpísaný len týmto CSCA.

Ak členský štát prevádzkuje vlastný CSCA, je daný členský štát zodpovedný za bezpečnú prevádzku a riadenie jeho kľúčov. CSCA pôsobí ako bod dôvery pre DSC, a preto je ochrana súkromného kľúča CSCA nevyhnutná pre integritu prostredia DCC. Model overovania v infraštruktúre verejných kľúčov DCC je tzv. shell model, podľa ktorého všetky certifikáty pri validácii cesty certifikátov musia byť platné v danom čase (t. j. v čase validácie podpisu). Uplatňujú sa preto tieto obmedzenia:

— CSCA nesmie vystavovať certifikáty, ktoré platia dlhšie ako samotný certifikát certifikačnej autority,

— podpisovateľ dokumentov nepodpíše dokumenty, ktoré platia dlhšie ako samotný DSC,

— členské štáty, ktoré prevádzkujú vlastný CSCA, musia vymedziť obdobia platnosti svojich CSCA a všetkých vystavených certifikátov a musia sa postarať o obnovovanie certifikátov.

V *oddiele 4.2* sa uvádzajú odporúčania pre obdobia platnosti.

3.3. *Integrita a pravosť nahraných údajov*

Vnútroštátne spracovateľské subjekty môžu použiť DCCG na nahranie a stiahnutie digitálne podpísaných balíkov údajov po úspešnej vzájomnej autentifikácii. Tieto balíky údajov na začiatku obsahujú DSC členských štátov. Kľúčový pár, ktorý používa vnútroštátny spracovateľský subjekt pre digitálny podpis nahraných balíkov údajov v systéme DCCG, sa nazýva kľúčový pár podpisu vnútroštátneho spracovateľského subjektu na nahrávanie a zodpovedajúci certifikát verejného kľúča sa skracuje ako certifikát NB_{UP}. Každý členský štát poskytne svoj vlastný certifikát NB_{UP}, ktorý môže byť samopodpísaný alebo ho môže vystaviť existujúca certifikačná autorita, ako je verejná certifikačná autorita (t. j. certifikačná autorita, ktorá vystavuje certifikáty v súlade so základnými požiadavkami organizácie CA/Browser Forum). Certifikát NB_{UP} musí byť odlišný od všetkých ostatných certifikátov využívaných členským štátom (t. j. CSCA, klientský TLS alebo DSC).

Členské štáty musia poskytnúť certifikát na nahrávanie prevádzkovateľovi DCCG pri prvej registrácii (*pozri ďalšie informácie v oddiele 4.1*). Každý členský štát je zodpovedný za svoje vnútroštátne údaje a musí chrániť súkromný kľúč, ktorý sa používa na podpísanie nahraných súborov.

Ostatné členské štáty môžu overiť podpísané balíky údajov pomocou certifikátov na nahrávanie, ktoré poskytuje DCCG. DCCG overuje pravosť a integritu nahraných údajov pomocou certifikátu vnútroštátneho spracovateľského subjektu na nahrávanie pred tým, ako sa poskytnú iným členským štátom.

▼B

3.4. *Požiadavky na technickú architektúru DCCG*

Pokiaľ ide o technickú architektúru DCCG, uplatňujú sa tieto požiadavky:

— DCCG využíva vzájomnú autentifikáciu TLS s cieľom nadviazať autentifikované šifrované spojenie s vnútroštátnymi spracovateľskými subjektmi. DCCG preto vedie bielu listinu registrovaných klientskych certifikátov NB_{TLS},

— DCCG používa dva digitálne certifikáty ($DCCG_{TLS}$ a $DCCG_{TA}$) s dvoma samostatnými kľúčovými pármi. Súkromný kľúč kľúčového páru $DCCG_{TA}$ sa uchováva offline (nie v online zložkách DCCG),

— DCCG vedie dôveryhodný zoznam certifikátov NB_{CSCA}, ktorý sa podpisuje súkromným kľúčom $DCCG_{TA}$,

— použité šifry musia spĺňať požiadavky uvedené v *oddiele 5.1*.

4. **Riadenie životného cyklu certifikátov**

4.1. *Registrácia vnútroštátnych spracovateľských subjektov*

Členské štáty sa musia zaregistrovať u prevádzkovateľa DCCG, aby sa mohli zapojiť do systému DCCG. V tomto oddiele sa opisuje technický a prevádzkový postup, ktorý sa musí dodržať pri registrácii vnútroštátneho spracovateľského subjektu.

Prevádzkovateľ DCCG a členský štát si musia vymieňať informácie o technických kontaktných osobách pre postup nadviazania spolupráce. Predpokladá sa, že technické kontaktné osoby sú legitimizované svojimi členskými štátmi a identifikácia/autentifikácia sa vykonáva prostredníctvom iných kanálov. Autentifikáciu je napríklad možné dosiahnuť, keď technická kontaktná osoba členského štátu poskytne certifikáty e-mailom ako súbory šifrované heslom a zodpovedajúce heslo oznámi prevádzkovateľovi DCCG telefonicky. Môžu sa využiť aj iné zabezpečené kanály vymedzené prevádzkovateľom DCCG.

Členský štát musí počas procesu registrácie a identifikácie poskytnúť tri digitálne certifikáty:

— certifikát TLS členského štátu – NB_{TLS},

— certifikát členského štátu na nahrávanie – NB_{UP},

— certifikát (certifikáty) CSCA členského štátu – NB_{CSCA}.

Všetky poskytnuté certifikáty musia spĺňať požiadavky vymedzené v *oddiele 5*. Prevádzkovateľ DCCG overí, či poskytnutý certifikát spĺňa požiadavky uvedené v *oddiele 5.* Prevádzkovateľ DCCG po identifikácii a registrácii:

— pridá certifikát (certifikáty) NB_{CSCA} do dôveryhodného zoznamu podpísaného súkromným kľúčom, ktorý zodpovedá verejnému kľúču $DCCG_{TA}$,

— pridá certifikát NB_{TLS} na bielu listinu koncového bodu TLS DCCG,

— pridá certifikát NB_{UP} do systému DCCG,

— poskytne certifikát verejného kľúča $DCCG_{TA}$ a $DCCG_{TLS}$ členskému štátu.

▼B

4.2. *Certifikačné autority, obdobia platnosti a obnovenie*

Ak chce členský štát prevádzkovať svoj vlastný CSCA, certifikáty CSCA môžu byť samopodpísané certifikáty. Vystupujú ako bod dôvery členského štátu, a preto musí členský štát dôsledne chrániť súkromný kľúč zodpovedajúci verejnému kľúču certifikátu CSCA. Odporúča sa, aby členské štáty pre svoje CSCA využívali offline systém, t. j. počítačový systém, ktorý nie je napojený k žiadnej sieti. Na prístup do systému sa využije kontrola viacerými osobami (napríklad podľa zásady štyroch očí). Po podpísaní DSC sa uplatnia operačné kontroly a systém, ktorý drží súkromný kľúč CSCA, sa bezpečne uloží s využitím silných prvkov kontroly prístupu. Na dodatočnú ochranu súkromného kľúča CSCA sa môžu využiť hardvérové bezpečnostné moduly alebo čipové karty. Digitálne certifikáty obsahujú obdobie platnosti, na základe ktorého sa vyžaduje obnovenie certifikátu. Obnovenie je nevyhnutné na použitie čerstvých kryptografických kľúčov a na prispôsobenie veľkostí kľúčov, keď nové vylepšenia z hľadiska výpočtov alebo nové útoky ohrozujú bezpečnosť použitého kryptografického algoritmu. Uplatňuje sa tzv. shell model (pozri *oddiel 3.2*).

Vzhľadom na ročnú platnosť digitálnych COVID preukazov EÚ sa odporúčajú tieto obdobia platnosti:

— CSCA: 4 roky

— DSC: 2 roky

— Nahrávanie: 1 až 2 roky

— Klientská autentifikácia TLS: 1 až 2 roky

Na včasnú obnovu sa odporúčajú tieto obdobia používania súkromných kľúčov:

— CSCA: 1 rok

— DSC: 6 mesiacov

Členské štáty musia včas vytvoriť nové certifikáty na nahrávanie a certifikáty TLS, napríklad jeden mesiac pred exspiráciou, aby sa zabezpečila plynulá prevádzka. Certifikáty CSCA a DSC by sa mali obnovovať aspoň mesiac pred skončením obdobia používania súkromného kľúča (vzhľadom na potrebné prevádzkové postupy). Členské štáty musia prevádzkovateľovi DCCG poskytnúť aktualizované certifikáty CSCA, certifikáty na nahrávanie a certifikáty TLS. Exspirované certifikáty sa odstránia z bielej listiny a z dôveryhodného zoznamu.

Členské štáty a prevádzkovateľ DCCG musia sledovať platnosť svojich certifikátov. Neexistuje žiadny centrálny subjekt, ktorý by zaznamenával platnosť certifikátov a informoval o nej účastníkov.

▼B

4.3. *Zrušenie certifikátov*

Digitálne certifikáty vo všeobecnosti môže zrušiť ich vystavujúca certifikačná autorita pomocou zoznamov zrušených certifikátov alebo odpovedajúceho subjektu protokolu OCSP (Online Certificate Status Protocol). CSCA pre systém DCC by mali poskytnúť zoznamy zrušených certifikátov (ďalej len „CRL“). Aj keď tieto CRL v súčasnosti iné členské štáty nevyužívajú, mali by sa začleniť pre budúce použitie. V prípade, že sa CSCA rozhodne neposkytnúť CRL, certifikáty DSC tohto CSCA sa musia obnoviť, keď sa CRL stanú povinnými. Overovatelia by nemali využívať protokol OCSP na validáciu DSC a mali by využívať CRL. Odporúča sa, aby vnútroštátny spracovateľský subjekt vykonal potrebnú validáciu certifikátov DSC stiahnutých z brány DCC a vnútroštátnym validátorom DCC poslal len súbor dôveryhodných a validovaných DSC. Validátori DCC by vo svojom procese validácie nemali vykonávať kontrolu zrušenia DSC. Jedným z dôvodov je ochrana súkromia držiteľov DCC, keďže sa predíde akejkoľvek možnosti, že by príslušný odpovedajúci subjekt protokolu OSCP mohol monitorovať použitie ktoréhokoľvek konkrétneho DSC.

Členské štáty môžu samy odstrániť svoje DSC z DCCG pomocou platných certifikátov na nahrávanie a certifikátov TLS. Odstránenie certifikátu DSC znamená, že všetky DCC vystavené s týmto DSC sa stanú neplatnými, keď členské štáty získajú aktualizované zoznamy DSC. Rozhodujúci význam má ochrana materiálu súkromných kľúčov zodpovedajúcich DSC. Členské štáty musia informovať prevádzkovateľa DCCG, ak musia zrušiť certifikáty na nahrávanie alebo certifikáty TLS, napríklad v dôsledku narušenia vnútroštátneho spracovateľského subjektu. Prevádzkovateľ DCCG môže potom odstrániť dôveru voči dotknutému certifikátu, a to napríklad jeho odstránením z bielej listiny TLS. Prevádzkovateľ DCCG môže odstrániť certifikáty na nahrávanie z databázy DCCG. Balíky podpísané súkromným kľúčom zodpovedajúcim tomuto certifikátu na nahrávanie sa stanú neplatnými, keď vnútroštátne spracovateľské subjekty odstránia dôveru voči zrušenému certifikátu na nahrávanie. Ak sa musí zrušiť certifikát CSCA, členské štáty informujú prevádzkovateľa DCCG, ako aj ostatné členské štáty, s ktorými majú vzťah dôvery. Prevádzkovateľ DCCG vystaví nový dôveryhodný zoznam, v ktorom sa už dotknutý certifikát nebude uvádzať. Všetky DSC vystavené týmto CSCA sa stanú neplatnými, keď členské štáty aktualizujú svoje úložisko vzťahov dôvery vnútroštátneho spracovateľského subjektu. V prípade, že sa musí zrušiť certifikát $DCCG_{TLS}$ alebo certifikát $DCCG_{TA}$, prevádzkovateľ DCCG a členské štáty musia spolupracovať na vytvorení nového dôveryhodného spojenia TLS a dôveryhodného zoznamu.

5. **Vzory certifikátov**

V tomto oddiele sa stanovujú kryptografické požiadavky a usmernenie, ako aj požiadavky na vzory certifikátov. V prípade certifikátov DCCG sa v tomto oddiele vymedzujú vzory certifikátov.

5.1. *Kryptografické požiadavky*

Kryptografické algoritmy a šifrovacie balíky TLS sa zvolia na základe aktuálneho odporúčania nemeckého Federálneho úradu pre bezpečnosť informácií (BSI) alebo organizácie SOG-IS. Tieto odporúčania a odporúčania iných inštitúcií a normalizačných organizácií sú podobné. Odporúčania možno nájsť v technických usmerneniach TR 02102-1 a TR 02102-2 ([1]) alebo dohodnutých kryptografických mechanizmoch SOG-IS ([2]).

([1]) BSI – Technické usmernenia TR-02102 (bund.de).
([2]) SOG-IS – Podporné dokumenty (sogis.eu).

▼B

5.1.1. Požiadavky na DSC

Uplatňujú sa požiadavky stanovené v *oddiele 3.2.2 prílohy I*. Dôrazne sa preto odporúča, aby podpisovatelia dokumentov využili algoritmus digitálneho podpisu na báze eliptických kriviek (ECDSA) s NIST-p-256 (ako sa vymedzuje v prílohe D k dokumentu FIPS PUB 186-4). Iné eliptické krivky sa nepodporujú. V dôsledku obmedzení veľkosti DCC by členské štáty nemali využívať algoritmus RSA-PSS, hoci je povolený ako záložný algoritmus. V prípade, že členské štáty využívajú algoritmus RSA-PSS, mali by využiť veľkosť modulu 2048 alebo max. 3072 bitov. Pre podpis DSC sa ako kryptografická hašovacia funkcia použije SHA-2 s dĺžkou výstupu ≥ 256 bitov (pozri ISO/IEC 10118-3:2004).

5.1.2. Požiadavky na certifikáty TLS, certifikáty na nahrávanie a certifikáty CSCA

V prípade digitálnych certifikátov a kryptografických podpisov v kontexte DCCG sú hlavné požiadavky na kryptografické algoritmy a dĺžku kľúča zhrnuté v tejto tabuľke (pre rok 2021):

Algoritmus podpisu	Veľkosť kľúča	Hašovacia funkcia
EC-DSA	min. 250 bitov	SHA-2 s dĺžkou výstupu ≥ 256 bitov
RSA-PSS (odporúčaný padding) RSA-PKCS#1 v1.5 (legacy padding)	RSA modul (N) min. 3000 bitov s verejným exponentom e > 2^16	SHA-2 s dĺžkou výstupu ≥ 256 bitov
DSA	prvočíslo p min. 3000 bitov, kľúč q 250 bitov	SHA-2 s dĺžkou výstupu ≥ 256 bitov

Odporúčaná eliptická krivka pre EC-DSA je NIST-p-256, a to pre jej rozšírenú implementáciu.

5.2. *Certifikát CSCA (NB_{CSCA})*

V nasledujúcej tabuľke sa uvádza usmernenie o vzore certifikátu NB_{CSCA}, ak sa členský štát rozhodne pre systém DCC prevádzkovať vlastný CSCA.

Hrubo vytlačené položky sa vyžadujú (musia sa začleniť do certifikátu), položky označené *kurzívou* sa odporúčajú (mali by sa začleniť). Pri chýbajúcich poliach nie je vymedzené žiadne odporúčanie.

Pole	Hodnota
Subjekt	**cn=<neprázdny a jedinečný všeobecný názov>,***o=<poskytovateľ>,***c=<členský štát prevádzkujúci CSCA>**
Používanie kľúča	**podpísanie certifikátu,***podpísanie CRL* (minimálne)
Základné obmedzenia	**CA = pravda, obmedzenia dĺžky cesty = 0**

Názov predmetu musí byť neprázdny a jedinečný v rámci špecifikovaného členského štátu. Kód krajiny c) musí zodpovedať členskému štátu, ktorý bude používať tento certifikát CSCA. Certifikát musí obsahovať jedinečný identifikátor kľúča subjektu (SKI) podľa dokumentu RFC 5280 ([1]).

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

▼B

5.3. *Certifikát podpisovateľa dokumentov (DSC)*

V nasledujúcej tabuľke sa poskytuje usmernenie k certifikátu DSC. **Hrubo vytlačené** položky sa vyžadujú (musia sa začleniť do certifikátu), položky označené *kurzívou* sa odporúčajú (mali by sa začleniť). Pri chýbajúcich poliach nie je vymedzené žiadne odporúčanie.

Pole	Hodnota
Sériové číslo	**jedinečné sériové číslo**
Subjekt	**cn=<neprázdny a jedinečný všeobecný názov>,***o=<poskytovateľ>*,**c=<členský štát, ktorý využíva tento DSC>**
Používanie kľúča	**digitálny podpis** (minimálne)

DSC musí byť podpísaný súkromným kľúčom zodpovedajúcim certifikátu CSCA, ktorý používa členský štát.

Použijú sa tieto rozšírenia:

— certifikát musí obsahovať identifikátor kľúča autority (AKI) zodpovedajúci identifikátoru kľúča subjektu (SKI) certifikátu vystavujúceho CSCA,

— certifikát by mal obsahovať jedinečný identifikátor kľúča subjektu (v súlade s dokumentom RFC 5280 ([1])).

Certifikát by mal okrem toho obsahovať rozšírenie distribučného bodu CRL odkazujúce na zoznam zrušených certifikátov (CRL) poskytnutý zo strany CSCA, ktorý vystavil DSC.

Certifikát DSC môže obsahovať rozšírenie pre rozšírené používanie kľúča s nula alebo viacerými identifikátormi politiky používania kľúča, ktoré obmedzujú typy potvrdení HCERT, ktoré možno pomocou tohto certifikátu overiť. Ak je prítomný jeden alebo viacero identifikátorov, overovatelia overia použitie kľúča na základe uloženého HCERT. Na to sú vymedzené tieto hodnoty extendedKeyUsage:

Pole	Hodnota
extendedKeyUsage	1.3.6.1.4.1.1847.2021.1.1 pre vystaviteľov potvrdenia o teste
extendedKeyUsage	1.3.6.1.4.1.1847.2021.1.2 pre vystaviteľov potvrdenia o očkovaní
extendedKeyUsage	1.3.6.1.4.1.1847.2021.1.3 pre vystaviteľov potvrdenia o prekonaní ochorenia

V prípade, že neexistuje žiadne rozšírenie pre používanie kľúčov (t. j. žiadne rozšírenia alebo nulové rozšírenia), je možné tento certifikát použiť na overenie akéhokoľvek typu HCERT. Príslušné doplnkové identifikátory politiky rozšíreného používania kľúča, ktoré sa používajú pri overovaní potvrdení HCERT, sa môžu vymedziť v iných dokumentoch.

5.4. *Certifikát na nahrávanie (NB_{UP})*

V nasledujúcej tabuľke sa poskytuje usmernenie pre certifikát vnútroštátneho spracovateľského subjektu na nahrávanie. **Hrubo vytlačené** položky sa vyžadujú (musia sa začleniť do certifikátu), položky označené *kurzívou* sa odporúčajú (mali by sa začleniť). Pri chýbajúcich poliach nie je vymedzené žiadne odporúčanie.

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

▼B

Pole	Hodnota
Subjekt	**cn=<neprázdny a jedinečný všeobecný názov>,***o=<poskytovateľ>,***c=<členský štát, ktorý používa tento certifikát na nahrávanie>**
Používanie kľúča	**digitálny podpis** (minimálne)

5.5. *Klientská autentifikácia TLS vnútroštátneho spracovateľského subjektu (NB_{TLS})*

V nasledujúcej tabuľke sa poskytuje usmernenie pre certifikát klientskej autentifikácie TLS vnútroštátneho spracovateľského subjektu. **Hrubo vytlačené** položky sa vyžadujú (musia sa začleniť do certifikátu), položky označené *kurzívou* sa odporúčajú (mali by sa začleniť). Pri chýbajúcich poliach nie je vymedzené žiadne odporúčanie.

Pole	Hodnota
Subjekt	**cn=<neprázdny a jedinečný všeobecný názov>,***o=<poskytovateľ>,***c=<členský štát vnútroštátneho spracovateľského subjektu>**
Používanie kľúča	**digitálny podpis** (minimálne)
Rozšírené používanie kľúča	**autentifikácia klienta (1.3.6.1.5.5.7.3.2**)

Certifikát môže obsahovať aj rozšírené používanie kľúča *serverová autentifikácia (1.3.6.1.5.5.7.3.1*), nie je to však povinné.

5.6. *Podpisový certifikát dôveryhodného zoznamu ($DCCG_{TA}$)*

V nasledujúcej tabuľke sa vymedzuje certifikát bodu dôvery DCCG.

Pole	Hodnota
Subjekt	**cn = Brána digitálneho zeleného osvedčenia** ([1])**, o=<poskytovateľ>, c=<krajina>**
Používanie kľúča	**digitálny podpis** (minimálne)

5.7. *Serverové certifikáty TLS pre DCCG ($DCCG_{TLS}$)*

V nasledujúcej tabuľke sa vymedzuje certifikát TLS DCCG.

Pole	Hodnota
Subjekt	cn=<FQDN alebo IP adresa DCCG>, o=<poskytovateľ>, c=<krajina>
SubjectAltName	dNSName: <názov DNS DCCG> alebo iPAddress: <IP adresa DCCG>
Používanie kľúča	**digitálny podpis** (minimálne)
Rozšírené používanie kľúča	**serverová autentifikácia (1.3.6.1.5.5.7.3.1**)

([1]) V tejto súvislosti sa zachoval výraz „digitálne zelené osvedčenie“ namiesto výrazu „digitálny COVID preukaz EÚ“, keďže ide o terminológiu, ktorá bola pevne zakódovaná a využitá v potvrdení ešte pred tým, ako sa spoluzákonodarcovia rozhodli pre novú terminológiu.

▼B

Certifikát môže obsahovať aj rozšírené používanie kľúča *klientská autentifikácia (1.3.6.1.5.5.7.3.2*), nie je to však povinné.

Certifikát TLS DCCG vystavuje verejne dôveryhodná certifikačná autorita (začlenená vo všetkých hlavných prehliadačoch a operačných systémoch v zmysle základných požiadaviek organizácie CA/Browser Forum).

▼M1

PRÍLOHA V

SCHÉMA ZÁPISU OBJEKTU V JAZYKU JAVASCRIPT (JAVASCRIPT OBJECT NOTATION, JSON)

1. **Úvod**

V tejto prílohe sa stanovuje technická štruktúra údajov pre digitálne COVID preukazy EÚ, ktorá je znázornená ako schéma JSON. V tomto dokumente sa uvádzajú konkrétne pokyny k jednotlivým dátovým poliam.

2. **Umiestnenie a verzie schémy JSON**

Autentická oficiálna schéma JSON pre digitálne COVID preukazy EÚ je k dispozícii na adresehttps://github.com/ehn-dcc-development/ehn-dcc-schema. Iné umiestnenia nie sú autentické, ale môžu sa použiť na prípravu nadchádzajúcich revízií.

Súčasná verzia, ktorá je stanovená v tejto prílohe a podporili ju všetky krajiny, ktoré v súčasnosti generujú preukazy, sa na uvedenej URL adrese zobrazuje ako východisková verzia.

Nadchádzajúcu ďalšiu verziu, ktorú musia k stanovenému dátumu podporiť všetky krajiny, možno nájsť na uvedenej URL adrese ako označenú verziu, ktorá je podrobnejšie opísaná v súbore Readme.

▼M3

3. **Spoločné štruktúry a všeobecné požiadavky**

Digitálny COVID preukaz EÚ sa nesmie vystaviť, pokiaľ z dôvodu chýbajúcich informácií nemožno všetky dátové polia správne vyplniť v súlade s touto špecifikáciou. **Nesmie sa to však vykladať tak, že je tým ovplyvnená povinnosť členských štátov vystavovať digitálne COVID preukazy EÚ.**

Informácie sa môžu vo všetkých poliach vypĺňať pomocou úplného súboru znakov UNICODE 13.0 kódovaných pomocou UTF-8, pokiaľ nie sú osobitne obmedzené na súbory hodnôt alebo užšie súbory znakov.

Spoločná štruktúra je takáto:

„JSON“:{

„ver“:<informácie o verzii>,

„nam“:{

<informácie o mene osoby>

},

„dob“:<dátum narodenia>,

„v“ alebo „t“ alebo „r“:[

{<vakcinačná dávka alebo informácie o teste alebo informácie o prekonaní, jeden zápis>}

]

}

Podrobné informácie o jednotlivých skupinách a poliach sú uvedené v ďalších oddieloch.

Keď sa v pravidlách uvádza, že pole sa vynechá, znamená to, že jeho obsah musí byť prázdny a že meno ani hodnota poľa nie sú v obsahu povolené.

▼M3

3.1. *Verzia*

Uvedú sa informácie o verzii. Správa verzií sa riadi sémantickou správou verzií (*Semantic Versioning*) (semver: https://semver.org). Pri generovaní preukazu sa musí použiť jedna z oficiálne vydaných verzií (súčasná verzia alebo jedna zo starších oficiálne vydaných verzií). Podrobnejšie informácie sú uvedené v oddiele o umiestnení schémy (*Schema location*) JSON.

ID poľa	Názov poľa	Pokyny
ver	Verzia schémy	Zodpovedá identifikátoru verzie schémy, ktorá bola použitá na vygenerovanie EUDCC. Príklad: „ver“: „1.3.0“

3.2. *Meno osoby a dátum narodenia*

Meno osoby je celé úradné meno osoby, ktoré sa zhoduje s menom uvedeným v cestovných dokladoch. Identifikátor štruktúry je *nam*. Zadá sa presne 1 (jedno) meno osoby.

ID poľa	Názov poľa	Pokyny
nam/fn	Priezvisko(-á)	Priezvisko(-á) držiteľa Ak držiteľ nemá priezviská a má rodné meno, pole sa vynechá. Vo všetkých ostatných prípadoch sa zadá presne 1 (jedno) pole s obsahom, v ktorom sa uvedú všetky priezviská. V prípade viacerých priezvisk sa tieto priezviská oddelia medzerou. Zložené mená vrátane tých, ktoré obsahujú spojovníky alebo podobné znaky, však musia zostať rovnaké. Príklady: „fn“:„Musterfrau-Gößinger“ „fn“:„Musterfrau-Gößinger Müller“
nam/fnt	Štandardizované priezvisko(-á)	Priezvisko(-á) držiteľa sa prepíše(-u) s použitím rovnakého dohovoru, aký sa použil v strojovo čitateľných cestovných dokladoch držiteľa (ako sú napríklad pravidlá vymedzené v časti 3 dokumentu ICAO Doc 9303). Ak držiteľ nemá priezviská a má rodné meno, pole sa vynechá. Vo všetkých ostatných prípadoch sa zadá presne 1 (jedno) pole s obsahom, v ktorom sa použijú iba znaky A – Z a <. Maximálna dĺžka: 80 znakov (podľa špecifikácií dokumentu ICAO 9303). Príklady: „fnt“:„MUSTERFRAU<GOESSINGER“ „fnt“:„MUSTERFRAU<GOESSINGER<MUELLER“
nam/gn	Rodné meno(-á)	Rodné meno(-á), ako napríklad rodné meno(-á) držiteľa. Ak držiteľ nemá rodné mená a má priezvisko, pole sa vynechá. Vo všetkých ostatných prípadoch sa zadá presne 1 (jedno) pole s obsahom, v ktorom sa uvedú všetky rodné mená. V prípade viacerých rodných mien sa tieto mená oddelia medzerou. Príklad: „gn“:„Isolde Erika“

▼M3

ID poľa	Názov poľa	Pokyny
nam/gnt	Štandardizované rodné meno(-á)	Rodné meno(-á) držiteľa sa prepíše(-u) s použitím rovnakého dohovoru, aký sa použil v strojovo čitateľných cestovných dokladoch držiteľa (ako sú napríklad pravidlá vymedzené v časti 3 dokumentu ICAO Doc 9303). Ak držiteľ nemá rodné mená a má priezvisko, pole sa vynechá. Vo všetkých ostatných prípadoch sa zadá presne 1 (jedno) pole s obsahom, v ktorom sa použijú iba znaky A – Z a <. Maximálna dĺžka: 80 znakov Príklad: „gnt“:„ISOLDE<ERIKA“
dob	Dátum narodenia	Dátum narodenia držiteľa digitálneho COVID preukazu EÚ Úplný alebo čiastočný dátum bez časového údaja, ktorý sa bude pohybovať v rozpätí vymedzenom od 1900-01-01 do 2099-12-31. Zadá sa presne 1 (jedno) pole s obsahom, ak je známy úplný alebo čiastočný dátum narodenia. Ak dátum narodenia nie je známy ani čiastočne, pole sa nastaví ako prázdny reťazec „“. To by malo zodpovedať informáciám uvedeným v cestovných dokladoch. Ak sú k dispozícii informácie o dátume narodenia, použije sa jeden z týchto formátov ISO 8601. Iné možnosti nie sú podporované. YYYY-MM-DD YYYY-MM YYYY (Overovacia aplikácia môže zobraziť chýbajúce časti dátumu narodenia s použitím dohovoru XX rovnako ako pri strojovo čitateľných cestovných dokladoch, napr. 1990-XX-XX.) Príklady: „dob“:„1979-04-14“ „dob“:„1901-08“ „dob“:„1939“ „dob“:„“

3.3. *Skupiny so špecifickými informáciami o type potvrdenia*

Schéma JSON podporuje tri skupiny zápisov, ktoré obsahujú špecifické informácie o type potvrdenia. Každý digitálny COVID preukaz EÚ obsahuje presne 1 (jednu) skupinu. Prázdne skupiny nie sú povolené.

Identifikátor skupiny	Názov skupiny	Zápisy
v	Skupina o očkovaní	Ak je k dispozícii, obsahuje presne 1 (jeden) zápis opisujúci presne 1 (jednu) dávku vakcíny (jednu dávku).
t	Skupina o vykonaní testu	Ak je k dispozícii, obsahuje presne 1 (jeden) zápis opisujúci presne 1 (jeden) výsledok testu.
r	Skupina o prekonaní ochorenia	Ak je k dispozícii, obsahuje presne 1 (jeden) zápis opisujúci presne 1 (jedno) vyhlásenie o prekonaní ochorenia.

▼M1

4. **Špecifické informácie o type potvrdenia**

4.1. *Potvrdenie o očkovaní*

Ak je k dispozícii skupina o očkovaní, obsahuje presne 1 (jeden) zápis opisujúci presne jednu očkovaciu udalosť (jednu dávku). Všetky prvky skupiny o očkovaní sú povinné, prázdne hodnoty nie sú podporované.

▼**M1**

ID poľa	Názov poľa	Pokyny
v/tg	Ochorenie alebo pôvodca ochorenia, na ktoré sa potvrdenie vzťahuje: ochorenie COVID-19 (vírus SARS-CoV-2 alebo niektorý z jeho variantov)	Kódovaná hodnota zo súboru hodnôt disease-agent-targeted.json. Tento súbor hodnôt má jediný zápis 840539006, ktorý je kódom pre COVID-19 v SNOMED CT (GPS). Zadá sa presne 1 (jedno) pole s obsahom. Príklad: „tg“: „840539006“
v/vp	Vakcína alebo profylaxia proti ochoreniu COVID-19	Druh použitej vakcíny alebo profylaxie. Kódovaná hodnota zo súboru hodnôt vaccine-prophylaxis.json.. Súbor hodnôt sa distribuuje z brány digitálneho COVID preukazu EÚ. Zadá sa presne 1 (jedno) pole s obsahom. Príklad: „vp“: „1119349007“ (vakcína mRNA proti vírusu SARS-CoV-2)
v/mp	Vakcinačná látka proti ochoreniu COVID-19	Liek používaný na túto špecifickú dávku vakcinácie. ►**M4** Kódovaná hodnota zo súboru hodnôt vaccine-medicinal-product.json. Alebo kódovaná hodnota odkazujúca na klinické skúšanie, ktorá sa riadi pravidlom vymedzeným v oddiele 3 prílohy II. ◄ Súbor hodnôt sa distribuuje z brány digitálneho COVID preukazu EÚ. Zadá sa presne 1 (jedno) pole s obsahom. Príklad: „mp“: „EU/1/20/1528“ (Comirnaty)
v/ma	Držiteľ povolenia na uvedenie vakcíny proti ochoreniu COVID-19 na trh alebo jej výrobca	Držiteľ povolenia na uvedenie na trh alebo výrobca, ak neexistuje žiadny držiteľ povolenia na uvedenie na trh. ►**M4** Kódovaná hodnota zo súboru hodnôt vaccine-medicinal-product.json. Alebo kódovaná hodnota odkazujúca na klinické skúšanie, ktorá sa riadi pravidlom vymedzeným v oddiele 4 prílohy II. ◄ Súbor hodnôt sa distribuuje z brány digitálneho COVID preukazu EÚ. Zadá sa presne 1 (jedno) pole s obsahom. Príklad: „ma“: „ORG-100030215“ (Biontech Manufacturing GmbH)
v/dn	Poradie v sérii dávok	Poradové číslo (kladné celé číslo) dávky podanej počas tejto očkovacej udalosti. 1 pre prvú dávku, 2 pre druhú dávku atď. Podrobnejšie pravidlá sú uvedené v oddiele 5 prílohy II. Zadá sa presne 1 (jedno) pole s obsahom. Príklady: „dn“: „1“ (prvá dávka) „dn“: „2“ (druhá dávka) „dn“: „3“ (tretia dávka)
v/sd	Celkový počet dávok v sérii.	Celkový počet dávok (kladné celé číslo) vo vakcinačnej sérii. Podrobnejšie pravidlá sú uvedené v oddiele 5 prílohy II. Zadá sa presne 1 (jedno) pole s obsahom. Príklady: „sd“: „1“ (v prípade 1-dávkovej primárnej vakcinačnej série) „sd“: „2“ (v prípade 2-dávkovej primárnej vakcinačnej série alebo v prípade dodatočnej dávky po 1-dávkovej primárnej vakcinačnej sérii) „sd“: „3“ (napr. v prípade dodatočných dávok po 2-dávkovej primárnej vakcinačnej sérii)

▼**M1**

ID poľa	Názov poľa	Pokyny
v/dt	Dátum očkovania	Dátum podania opísanej dávky vo formáte RRRR-MM-DD (celý dátum bez času). Iné formáty nie sú podporované. Zadá sa presne 1 (jedno) pole s obsahom. Príklad: „dt“: „2021-03-28“
v/co	Členský štát alebo tretia krajina, v ktorom/ktorej bola vakcína podaná;	Krajina vyjadrená ako dvojpísmenový kód ISO3166 (ODPORÚČANÉ) alebo odkaz na medzinárodnú organizáciu zodpovednú za očkovaciu udalosť (ako je UNHCR alebo WHO). Kódovaná hodnota zo súboru hodnôt country-2-codes.json. Súbor hodnôt sa distribuuje z brány digitálneho COVID preukazu EÚ. Zadá sa presne 1 (jedno) pole. Príklad: „co“: „CZ“ „co“: „UNHCR“
v/is	Vystaviteľ potvrdenia	Názov organizácie, ktorá potvrdenie vystavila. Identifikátory sú povolené ako súčasť názvu, ale neodporúča sa ich samostatné používanie bez uvedenia názvu v podobe textu. Maximálne 80 znakov UTF-8. Zadá sa presne 1 (jedno) pole s obsahom. Príklad: „is“: „Ministry of Health of the Czech Republic“ „is“: „Vaccination Centre South District 3“
v/ci	Jedinečný identifikátor potvrdenia	Jedinečný identifikátor potvrdenia, ako sa uvádza v https://ec.europa.eu/health/sites/default/files/ehealth/docs/vaccination-proof_interoperability-guidelines_en.pdf Zahrnutie kontrolného súčtu je nepovinné. Môže sa doplniť predpona „URN:UVCI:“ . Zadá sa presne 1 (jedno) pole s obsahom. Príklady: „ci“: „URN:UVCI:01:NL:187/37512422923“ „ci“: „URN:UVCI:01:AT:10807843F94AEE0EE5093FBC254BD813#B“

4.2. *Potvrdenie o vykonaní testu*

Ak je k dispozícii skupina o vykonaní testu, obsahuje presne 1 (jeden) zápis opisujúci presne jeden výsledok testu.

ID poľa	Názov poľa	Pokyny
t/tg	Ochorenie alebo pôvodca ochorenia, na ktoré sa potvrdenie vzťahuje: ochorenie COVID-19 (vírus SARS-CoV-2 alebo niektorý z jeho variantov)	Kódovaná hodnota zo súboru hodnôt disease-agent-targeted.json. Tento súbor hodnôt má jediný zápis 840539006, ktorý je kódom pre COVID-19 v SNOMED CT (GPS). Zadá sa presne 1 (jedno) pole s obsahom. Príklad: „tg“: „840539006“
t/tt	Typ testu	Typ použitého testu na základe materiálu, na ktorý sa test zameriava. Kódovaná hodnota zo súboru hodnôt test-type.json (na základe LOINC). Hodnoty mimo súboru hodnôt nie sú povolené. Zadá sa presne 1 (jedno) pole s obsahom. Príklad: „tt“: „LP6464-4“ (Amplifikácia nukleových kyselín s použitím sondy na detekciu) „tt“: „LP217198-3“ (Rýchly imunologický test)

▼M1

ID poľa	Názov poľa	Pokyny
t/nm	Názov testu (iba testy amplifikácie nukleových kyselín)	Názov použitého testu amplifikácie nukleových kyselín (NAAT). Názov by mal obsahovať názov výrobcu testu a obchodný názov testu oddelený čiarkou. V prípade NAAT: toto pole je nepovinné. ►M4 V prípade antigénového testu: pole sa nepoužije, pretože názov testu sa poskytuje nepriamo prostredníctvom identifikátora testovacieho zariadenia (t/ma). ◄ Ak sa poskytne, pole nesmie byť prázdne. Príklad: „nm“: „ELITechGroup, SARS-CoV-2 ELITe MGB® Kit“

▼M4

t/ma	Identifikátor testovacieho zariadenia (len antigénové testy)	Identifikátor zariadenia na antigénový test z databázy JRC. Súbor hodnôt (spoločný zoznam HSC): — všetky antigénové testy v spoločnom zozname HSC (čitateľné ľudským okom), — https://covid-19-diagnostics.jrc.ec.europa.eu/devices/hsc-common-recognition-rat (strojovo čitateľné, hodnoty poľa id_device zo zoznamu súboru hodnôt). V krajinách EÚ/EHP môžu vystavitelia vystaviť potvrdenia len na testy, ktoré patria do aktuálne platného súboru hodnôt. Súbor hodnôt sa aktualizuje každých 24 hodín. V potvrdeniach vystavených tretími krajinami sa môžu použiť hodnoty mimo súboru hodnôt, avšak identifikátory musia pochádzať aj napriek tomu z databázy JRC. Použitie iných identifikátorov, napríklad tých, ktoré poskytujú priamo výrobcovia testov, nie je povolené. Overovacie aplikácie odhalia hodnoty, ktoré nepatria do aktualizovaného súboru hodnôt, a potvrdenia obsahujúce takéto súbory hodnôt zobrazia ako neplatné. Ak je niektorý identifikátor odstránený zo súboru hodnôt, potvrdenia, ktoré ho obsahujú, sa môžu akceptovať maximálne 72 hodín od dátumu odstránenia. Súbor hodnôt sa distribuuje z brány digitálneho COVID preukazu EÚ. V prípade antigénového testu: zadá sa presne 1 (jedno) pole s obsahom. V prípade NAAT: pole sa nesmie použiť, a to ani vtedy, ak je identifikátor testu NAA dostupný v databáze JRC. Príklad: „ma“: „344“ (SD BIOSENSOR Inc, STANDARD F COVID-19 Ag FIA)

▼M1

t/sc	Dátum a čas odberu testovanej vzorky	dátum a čas, keď sa odobrala testovaná vzorka. Čas zahŕňa informácie o časovom pásme. Hodnota nemá označovať čas, keď bol vyhotovený výsledok testu. Zadá sa presne 1 (jedno) pole s obsahom. Použije sa jeden z týchto formátov ISO 8601. Iné možnosti nie sú podporované. RRRR-MM-DDThh:mm:ssZ RRRR-MM-DDThh:mm:ss[+-]hh.

▼**M1**

ID poľa	Názov poľa	Pokyny
		RRRR-MM-DDThh:mm:ss[+-]hhmm RRRR-MM-DDThh:mm:ss[+-]hh:mm Príklady: „sc“: „2021-08-20T10:03:12Z“ (čas UTC) „sc“: „2021-08-20T12:03:12+02“ (čas CEST) „sc“: „2021-08-20T12:03:12+0200“ (čas CEST) „sc“: „2021-08-20T12:03:12+02:00“ (čas CEST)
t/tr	Výsledok testu	Výsledok testu. Kódovaná hodnota zo súboru hodnôt test-type.json (na základe SNOMED CT, GPS). Zadá sa presne 1 (jedno) pole s obsahom. Príklad: „tr“: „260415000“ (nezistená prítomnosť)
t/tc	Testovacie centrum alebo zariadenie	Názov subjektu, ktorý test vykonal. Identifikátory sú povolené ako súčasť názvu, ale neodporúča sa ich samostatné používanie bez názvu v podobe textu. Maximálne 80 znakov UTF-8. Všetky ďalšie znaky by sa mali skrátiť. Názov nie je určený na automatizované overovanie. V prípade testov NAAT: zadá sa presne 1 (jedno) pole s obsahom. ►**M4** V prípade antigénového testu: toto pole je nepovinné. Ak sa poskytne, nesmie byť prázdne. ◄ Príklad: „tc“: „Test centre west region 245“
t/co	Členský štát alebo tretia krajina, v ktorom/ktorej sa test vykonal	Krajina vyjadrená ako dvojpísmenový kód ISO3166 (ODPORÚČANÉ) alebo odkaz na medzinárodnú organizáciu zodpovednú za vykonanie testu (ako napríklad UNHCR alebo WHO). Ide o kódovanú hodnotu zo súboru hodnôt country-2-codes.json. Súbor hodnôt sa distribuuje z brány digitálneho COVID preukazu EÚ. Zadá sa presne 1 (jedno) pole. Príklady: „co“: „CZ“ „co“: „UNHCR“
t/is	Vystaviteľ potvrdenia	Názov organizácie, ktorá potvrdenie vystavila. Identifikátory sú povolené ako súčasť názvu, ale neodporúča sa ich samostatné používanie bez uvedenia názvu v podobe textu. Maximálne 80 znakov UTF-8. Zadá sa presne 1 (jedno) pole s obsahom. Príklady: „is“: „Ministry of Health of the Czech Republic“ „is“: „North-West region health authority“

▼**M1**

ID poľa	Názov poľa	Pokyny
t/ci	Jedinečný identifikátor potvrdenia	Jedinečný identifikátor potvrdenia (UVCI), ako sa uvádza v vaccination-proof_interoperability-guidelines_en.pdf (europa.eu) Zahrnutie kontrolného súčtu je nepovinné. Môže sa doplniť predpona „URN:UVCI:“ . Zadá sa presne 1 (jedno) pole s obsahom. Príklady: „ci“: „URN:UVCI:01:NL:187/37512422923“ „ci“: „URN:UVCI:01:AT:10807843F94AEE0EE5093FBC254BD813#B“

4.3. *Potvrdenie o prekonaní ochorenia*

Ak je k dispozícii skupina o prekonaní ochorenia, obsahuje presne 1 (jeden) zápis opisujúci presne jedno vyhlásenie o prekonaní ochorenia. Všetky prvky skupiny o prekonaní ochorenia sú povinné, prázdne hodnoty nie sú podporované.

ID poľa	Názov poľa	Pokyny
r/tg	Ochorenie alebo pôvodca ochorenia, ktoré držiteľ prekonal: ochorenie COVID-19 (vírus SARS-CoV-2 alebo niektorý z jeho variantov)	Kódovaná hodnota zo súboru hodnôt disease-agent-targeted.json. Tento súbor hodnôt má jediný zápis 840539006, ktorý je kódom pre COVID-19 v SNOMED CT (GPS). Zadá sa presne 1 (jedno) pole s obsahom. Príklad: „tg“: „840539006“
r/fr	Dátum držiteľovho prvého pozitívneho výsledku testu ►**M4** ——— ◄	Dátum, keď bola odobratá vzorka na test ►**M4** ——— ◄ s pozitívnym výsledkom, vo formáte RRRR-MM-DD (úplný dátum bez času). Iné formáty nie sú podporované. Zadá sa presne 1 (jedno) pole s obsahom. Príklad: „fr“: „2021-05-18“
r/co	Členský štát alebo tretia krajina, v ktorom/ktorej sa test vykonal	Krajina vyjadrená ako dvojpísmenový kód ISO3166 (ODPORÚČANÉ) alebo odkaz na medzinárodnú organizáciu zodpovednú za vykonanie testu (ako napríklad UNHCR alebo WHO). Ide o kódovanú hodnotu zo súboru hodnôt country-2-codes.json. Súbor hodnôt sa distribuuje z brány digitálneho COVID preukazu EÚ. Zadá sa presne 1 (jedno) pole. Príklady: „co“: „CZ“ „co“: „UNHCR“
r/is	Vystaviteľ potvrdenia	Názov organizácie, ktorá potvrdenie vystavila. Identifikátory sú povolené ako súčasť názvu, ale neodporúča sa ich samostatné používanie bez názvu v podobe textu. Maximálne 80 znakov UTF-8. Zadá sa presne 1 (jedno) pole s obsahom. Príklad: „is“: „Ministry of Health of the Czech Republic“ „is“: „Central University Hospital“

▼**M1**

ID poľa	Názov poľa	Pokyny
r/df	Potvrdenie platné od	Prvý dátum, ku ktorému sa potvrdenie považuje za platné. Dátum nesmie byť skorší ako dátum vypočítaný ako r/fr + 11 dní Dátum sa uvedie vo formáte RRRR-MM-DD (úplný dátum bez času). Iné formáty nie sú podporované. Zadá sa presne 1 (jedno) pole s obsahom. Príklad: „df“: „2021-05-29“
r/du	Potvrdenie platné do	Posledný dátum, ku ktorému sa potvrdenie považuje za platné, pridelený vystavovateľom potvrdenia. Dátum nesmie byť neskorší ako dátum vypočítaný ako r/fr + 180 dní. Dátum sa uvedie vo formáte RRRR-MM-DD (úplný dátum bez času). Iné formáty nie sú podporované. Zadá sa presne 1 (jedno) pole s obsahom. Príklad: „du“: „2021-11-14“
r/ci	jedinečný identifikátor potvrdenia	Jedinečný identifikátor potvrdenia (UVCI), ako sa uvádza v vaccination-proof_interoperability-guidelines_en.pdf (europa.eu) Zahrnutie kontrolného súčtu je nepovinné. Môže sa doplniť predpona „„URN:UVCI:“ . Zadá sa presne 1 (jedno) pole s obsahom. Príklady: „„ci“: „URN:UVCI:01:NL:187/37512422923“ „ci“: „URN:UVCI:01:AT:10807843F94AEE0EE5093FBC254BD813#B“

▼M3

PRÍLOHA VI

ZODPOVEDNOSTI ČLENSKÝCH ŠTÁTOV AKO SPOLOČNÝCH PREVÁDZKOVATEĽOV BRÁNY DIGITÁLNEHO COVID PREUKAZU EÚ NA VÝMENU ZOZNAMOV ZRUŠENÝCH DIGITÁLNYCH COVID PREUKAZOV EÚ

ODDIEL 1

Pododdiel 1

Rozdelenie zodpovedností

1. Spoloční prevádzkovatelia spracúvajú osobné údaje prostredníctvom brány založenej na rámci dôvery v súlade s technickými špecifikáciami uvedenými v prílohe I.

2. Vydávajúce orgány členských štátov zostávajú jediným prevádzkovateľom, pokiaľ ide o zber, používanie, zverejňovanie a akékoľvek iné spracúvanie informácií o zrušených potvrdeniach mimo brány, a to aj pri postupe vedúcom k zrušeniu potvrdenia.

3. Každý prevádzkovateľ je v súlade s článkami 5, 24 a 26 všeobecného nariadenia o ochrane údajov zodpovedný za spracúvanie osobných údajov v bráne založenej na rámci dôvery.

4. Každý prevádzkovateľ zriadi kontaktné miesto s funkčnou e-mailovou schránkou, ktorá bude slúžiť na vzájomnú komunikáciu medzi spoločnými prevádzkovateľmi a na komunikáciu medzi spoločnými prevádzkovateľmi a sprostredkovateľom.

5. Pracovná skupina zriadená výborom uvedeným v článku 14 nariadenia (EÚ) 2021/953 je poverená preskúmaním akýchkoľvek problémov vyplývajúcich z výmeny zoznamov zrušených potvrdení a zo spoločného prevádzkovania súvisiaceho spracúvania osobných údajov a uľahčením koordinovaných pokynov pre Komisiu ako sprostredkovateľa. Táto pracovná skupina usmerňuje rozhodovací proces spoločných prevádzkovateľov, ktorý sa riadi jej rokovacím poriadkom. Základným pravidlom je, že neúčasť ktoréhokoľvek zo spoločných prevádzkovateľov na zasadnutí tejto pracovnej skupiny, ktoré bolo oznámené aspoň sedem (7) dní pred jej písomným zvolaním, vedie k tichému súhlasu s výsledkami tohto zasadnutia pracovnej skupiny. Zasadnutie tejto pracovnej skupiny môže zvolať ktorýkoľvek zo spoločných prevádzkovateľov.

6. Pokyny pre sprostredkovateľa posiela ktorékoľvek kontaktné miesto spoločných prevádzkovateľov po dohode s ostatnými spoločnými prevádzkovateľmi, a to na základe rozhodovacieho procesu pracovnej skupiny uvedeného v bode 5. Spoločný prevádzkovateľ, ktorý poskytuje pokyny, by ich mal v písomnej podobe poskytnúť sprostredkovateľovi a informovať o tom všetkých ostatných spoločných prevádzkovateľov. Ak je predmetná záležitosť natoľko naliehavá, že neumožňuje zasadnutie pracovnej skupiny podľa bodu 5, pokyn sa môže poskytnúť aj tak, no pracovná skupina ho môže zrušiť. Tento pokyn by sa mal vydať písomne a všetci ostatní spoloční prevádzkovatelia by o tom mali byť v čase vydania pokynu informovaní.

7. Pracovná skupina zriadená podľa bodu 5 nevylučuje individuálnu právomoc spoločných prevádzkovateľov informovať svoj príslušný dozorný orgán v súlade s článkami 33 a 24 všeobecného nariadenia o ochrane údajov. Takéto oznámenie si nevyžaduje súhlas žiadneho z ostatných spoločných prevádzkovateľov.

▼M3

8. V bráne založenej na rámci dôvery majú prístup k vymieňaným osobným údajom len osoby autorizované určenými vnútroštátnymi orgánmi alebo verejnými subjektmi.

9. Každý vydávajúci orgán vedie záznamy o činnostiach spracúvania údajov, za ktoré zodpovedá. V záznamoch môže byť uvedené aj spoločné prevádzkovanie.

Pododdiel 2

Zodpovednosti a úlohy pri vybavovaní žiadostí a informovaní dotknutých osôb

1. Každý prevádzkovateľ vo svojej úlohe vydávajúceho orgánu poskytuje fyzickým osobám, ktorých potvrdenie(-ia) zrušil (ďalej len „dotknuté osoby“), informácie o uvedenom zrušení potvrdenia a spracúvaní ich osobných údajov v bráne digitálneho COVID preukazu EÚ na účely podpory výmeny zoznamov zrušených potvrdení v súlade s článkom 14 všeobecného nariadenia o ochrane údajov, pokiaľ sa to neukáže ako nemožné alebo by s tým súviselo neprimerané úsilie.

2. Každý prevádzkovateľ koná ako kontaktné miesto pre fyzické osoby, ktorých potvrdenie zrušil, a vybavuje žiadosti predložené dotknutými osobami alebo ich zástupcami pri výkone ich práv v súlade so všeobecným nariadením o ochrane údajov. Ak spoločný prevádzkovateľ dostane od dotknutej osoby žiadosť, ktorá sa týka potvrdenia vydaného iným spoločným prevádzkovateľom, informuje dotknutú osobu o identite a kontaktných údajoch daného zodpovedného spoločného prevádzkovateľa. Na požiadanie od iného spoločného prevádzkovateľa si spoloční prevádzkovatelia pri vybavovaní žiadostí dotknutých osôb navzájom pomáhajú a vzájomne si odpovedajú bez zbytočného odkladu, a to najneskôr do jedného mesiaca od doručenia žiadosti o pomoc. Ak sa žiadosť týka údajov predložených treťou krajinou, prevádzkovateľ, ktorý dostane žiadosť, ju vybaví a dotknutú osobu informuje o identite a kontaktných údajoch vydávajúceho orgánu v tretej krajine.

3. Každý prevádzkovateľ sprístupní dotknutým osobám obsah tejto prílohy vrátane opatrení stanovených v bodoch 1 a 2.

ODDIEL 2

Riadenie kybernetických incidentov vrátane prípadov porušenia ochrany osobných údajov

1. Spoloční prevádzkovatelia si navzájom pomáhajú pri identifikácii a riešení všetkých kybernetických incidentov vrátane prípadov porušenia ochrany osobných údajov, ktoré sú spojené so spracúvaním v bráne digitálneho COVID preukazu EÚ.

2. Spoloční prevádzkovatelia sa navzájom informujú najmä o týchto skutočnostiach:

   a) všetkých potenciálnych alebo skutočných rizikách týkajúcich sa dostupnosti, dôvernosti a/alebo integrity osobných údajov, ktoré sa spracúvajú v bráne založenej na rámci dôvery;

   b) všetkých prípadoch porušenia ochrany osobných údajov, pravdepodobných dôsledkoch porušenia ochrany osobných údajov a posúdení rizika v súvislosti s právami a so slobodami fyzických osôb, ako aj o všetkých prijatých opatreniach na riešenie porušovania ochrany osobných údajov a zmierňovanie rizika v súvislosti s právami a so slobodami fyzických osôb;

▼M3

c) všetkých prípadoch porušenia technických a/alebo organizačných záruk týkajúcich sa spracovateľských operácií v bráne založenej na rámci dôvery.

3. Spoloční prevádzkovatelia oznamujú Komisii, príslušným orgánom dohľadu a v prípade potreby dotknutým osobám všetky prípady porušenia ochrany osobných údajov týkajúce sa spracovateľských operácií realizovaných v bráne založenej na rámci dôvery v súlade s článkami 33 a 34 všeobecného nariadenia o ochrane údajov alebo po oznámení Komisie.

4. Každý vydávajúci orgán zavedie vhodné technické a organizačné opatrenia, ktorých účelom je:

a) zabezpečiť a chrániť dostupnosť, integritu a dôvernosť spoločne spracúvaných osobných údajov;

b) chrániť pred akýmkoľvek neoprávneným alebo nezákonným spracúvaním, stratou, použitím, zverejnením alebo získaním akýchkoľvek osobných údajov, ktorými disponuje, alebo pred prístupom k týmto údajom;

c) zabezpečiť, aby sa prístup k osobným údajom neudelil ani nepovolil iným osobám ako príjemcom alebo sprostredkovateľom.

ODDIEL 3

Posúdenie vplyvu na ochranu údajov

1. Ak prevádzkovateľ v záujme plnenia svojich povinností stanovených v článkoch 35 a 36 nariadenia (EÚ) 2016/679 potrebuje informácie od iného prevádzkovateľa, zašle osobitnú žiadosť do funkčnej e-mailovej schránky uvedenej v oddiele 1 pododdiele 1 bode 4. Oslovený prevádzkovateľ vynaloží maximálne úsilie na poskytnutie týchto informácií.

▼M3

PRÍLOHA VII

ZODPOVEDNOSTI KOMISIE AKO SPROSTREDKOVATEĽA ÚDAJOV BRÁNY DIGITÁLNEHO COVID PREUKAZU EÚ NA PODPORU VÝMENY ZOZNAMOV ZRUŠENÝCH DIGITÁLNYCH COVID PREUKAZOV EÚ

Komisia:

1. V mene členských štátov zriadi a zaistí bezpečnú a spoľahlivú komunikačnú infraštruktúru, ktorá podporuje výmenu zoznamov zrušených potvrdení odoslaných do brány digitálneho COVID preukazu.

2. V záujme plnenia svojich povinností ako sprostredkovateľa údajov v bráne založenej na dôvere pre členské štáty môže Komisia zapojiť tretie strany ako ďalších sprostredkovateľov; Komisia informuje spoločných prevádzkovateľov o všetkých zamýšľaných zmenách týkajúcich sa doplnenia alebo výmeny iných ďalších sprostredkovateľov, pričom prevádzkovatelia budú mať možnosť proti takýmto zmenám spoločne vzniesť námietku. Komisia zabezpečí, aby sa na týchto ďalších sprostredkovateľov vzťahovali rovnaké povinnosti v oblasti ochrany údajov, ako sú povinnosti stanovené v tomto rozhodnutí.

3. Spracúva osobné údaje len na základe zdokumentovaných pokynov od prevádzkovateľov s výnimkou prípadu, keď sa to vyžaduje podľa práva Únie alebo členského štátu; v takom prípade Komisia oznámi spoločným prevádzkovateľom túto právnu požiadavku ešte predtým, ako bude pokračovať s činnosťou spracúvania, pokiaľ sa podľa daného práva predkladanie takéhoto oznámenia zo závažných dôvodov verejného záujmu nezakazuje.

   Spracúvanie údajov zo strany Komisie zahŕňa tieto činnosti:

   a) autentifikáciu vnútroštátnych zálohových severov založenú na vnútroštátnych certifikátoch zálohových serverov;

   b) získavanie údajov uvedených v článku 5a ods. 3 rozhodnutia, ktoré boli nahraté vnútroštátnymi zálohovými servermi, a to poskytnutím aplikačného programového rozhrania, ktoré umožní vnútroštátnym zálohovým serverom príslušné údaje nahrať;

   c) uchovávanie údajov v bráne digitálneho COVID preukazu EÚ;

   d) sprístupnenie údajov na stiahnutie prostredníctvom vnútroštátnych zálohových serverov;

   e) vymazanie údajov po dátume uplynutia ich platnosti alebo na pokyn prevádzkovateľa, ktorý ich odoslal;

   f) vymazanie všetkých zostávajúcich údajov po skončení poskytovania služieb, pokiaľ sa podľa práva Únie alebo členského štátu nevyžaduje tieto osobné údaje uchovávať.

4. Prijíma všetky špičkové organizačné, fyzické a logické bezpečnostné opatrenia na spravovanie brány digitálneho COVID preukazu EÚ. Na tento účel Komisia:

   a) určí zodpovedný subjekt na riadenie bezpečnosti na úrovni brány digitálneho COVID preukazu EÚ, oznámi spoločným prevádzkovateľom jeho kontaktné údaje a zabezpečí, aby bol subjekt k dispozícii, ak bude potrebné reagovať na bezpečnostné hrozby;

▼M3

b) prevezme zodpovednosť za bezpečnosť brány digitálneho COVID preukazu EÚ vrátane pravidelného vykonávania testov, hodnotení a posúdení bezpečnostných opatrení;

c) zabezpečí, aby sa na všetky osoby, ktorým je udelený prístup do brány digitálneho COVID preukazu EÚ, vzťahovala zmluvná, profesionálna alebo zákonná povinnosť zachovávať dôvernosť.

5. Prijíma všetky potrebné bezpečnostné opatrenia, aby nedošlo k ohrozeniu bezproblémového prevádzkového fungovania vnútroštátnych zálohových serverov. Komisia na tento účel zavedie osobitné postupy týkajúce sa pripojenia zo zálohových serverov do brány digitálneho COVID preukazu EÚ. To zahŕňa:

a) postup na posúdenie rizika s cieľom identifikovať a odhadnúť potenciálne hrozby pre systém;

b) audit a preskúmanie s cieľom:

i) overiť zhodu medzi zavádzanými bezpečnostnými opatreniami a platnou bezpečnostnou politikou;

ii) pravidelne kontrolovať integritu súborov systému, bezpečnostné parametre a udelené autorizácie;

iii) monitorovať prípady narušenia bezpečnosti a neoprávnených vniknutí;

iv) vykonať zmeny na zmiernenie existujúcich nedostatkov v zabezpečení;

v) vymedziť podmienky, za ktorých možno, a to aj na žiadosť prevádzkovateľov, povoliť vykonávanie nezávislých auditov vrátane inšpekcií a preskúmaní bezpečnostných opatrení za podmienok, ktoré sú v súlade s protokolom (č. 7) k ZFEÚ o výsadách a imunitách Európskej únie, a prispievať k ich vykonávaniu;

c) zmenu postupu kontroly s cieľom zdokumentovať a zmerať vplyv zmeny pred jej vykonaním a informovať spoločných prevádzkovateľov o všetkých zmenách, ktoré môžu ovplyvniť komunikáciu s ich infraštruktúrami a/alebo ich bezpečnosť;

d) stanovenie postupu údržby a opravy s cieľom špecifikovať pravidlá a podmienky, ktoré treba dodržať pri údržbe a/alebo oprave vybavenia;

e) stanovenie postupu týkajúceho sa kybernetických incidentov s cieľom vymedziť systém hlásení a eskalácie, bezodkladne informovať dotknutých prevádzkovateľov, bezodkladne informovať prevádzkovateľov, aby upovedomili vnútroštátne dozorné orgány pre ochranu údajov o akomkoľvek prípade porušenia ochrany osobných údajov, a vymedziť disciplinárne konanie pre prípady narušenia bezpečnosti.

6. Prijíma špičkové fyzické a/alebo logické bezpečnostné opatrenia pre zariadenia, v ktorých sa nachádza brána digitálneho COVID preukazu EÚ, a pre kontroly prístupu k logickým údajom a prístupu k zabezpečeniu. Na tento účel Komisia:

a) zaisťuje fyzickú bezpečnosť s cieľom vytvoriť osobitné bezpečnostné zóny a umožniť odhaľovanie prípadov narušenia;

▼M3

b) kontroluje prístup do zariadení a vedie register návštevníkov na účely sledovania;

c) zabezpečuje, aby externé osoby, ktorým bol udelený prístup do priestorov, sprevádzali riadne autorizovaní zamestnanci;

d) zabezpečuje, aby vybavenie nebolo možné pridať, vymeniť ani odstrániť bez predchádzajúceho súhlasu určených zodpovedných orgánov;

e) kontroluje prístup z/do vnútroštátnych zálohových serverov prepojených s bránou založenou na rámci dôvery;

f) zabezpečuje, aby všetci jednotlivci, ktorí majú prístup do brány digitálneho COVID preukazu EÚ, boli identifikovaní a overení;

g) preskúmava prístupové práva týkajúce sa prístupu do brány digitálneho COVID preukazu EÚ v prípade narušenia bezpečnosti, ktoré má vplyv na túto infraštruktúru;

h) zachováva integritu informácií prenášaných prostredníctvom brány digitálneho COVID preukazu EÚ;

i) realizuje technické a organizačné bezpečnostné opatrenia s cieľom zabrániť neoprávnenému prístupu k osobným údajom;

j) v prípade potreby realizuje opatrenia na zablokovanie neoprávneného prístupu do brány digitálneho COVID preukazu EÚ z domény vydávajúcich orgánov (t. j.: blokovanie polohy/IP adresy).

7. Podniká kroky na ochranu svojej domény vrátane prerušenia pripojení v prípade výraznej odchýlky od zásad a koncepcií v oblasti kvality alebo bezpečnosti.

8. Vypracúva a aktualizuje plán riadenia rizík v oblasti svojej pôsobnosti.

9. Monitoruje – v reálnom čase – výkonnosť všetkých zložiek služby v rámci svojich služieb brány založenej na rámci dôvery, zostavuje pravidelnú štatistiku a vedie záznamy.

10. Poskytuje podporu pre všetky služby brány založenej na rámci dôvery v angličtine, a to 24 hodín denne a 7 dní v týždni cez telefón, mailom alebo cez webový portál a prijíma hovory od autorizovaných volajúcich, ktorými sú: koordinátori brány digitálneho COVID preukazu EÚ a ich príslušné asistenčné služby, projektoví manažéri a určené osoby z Komisie.

11. Primeranými technickými a organizačnými opatreniami a pokiaľ je to možné v súlade s článkom 12 nariadenia (EÚ) 2018/1725 pomáha spoločným prevádzkovateľom pri plnení ich povinnosti reagovať na žiadosti o výkon práv dotknutej osoby stanovených v kapitole III všeobecného nariadenia o ochrane údajov.

▼**M3**

12. Podporuje spoločných prevádzkovateľov poskytovaním informácií týkajúcich sa brány digitálneho COVID preukazu EÚ na účely plnenia povinností vyplývajúcich z článkov 32, 33, 34, 35 a 36 všeobecného nariadenia o ochrane údajov.

13. Zabezpečuje, aby boli údaje spracúvané v rámci brány digitálneho COVID preukazu EÚ nezrozumiteľné pre všetky osoby, ktoré nemajú oprávnenie na prístup k nim.

14. Prijíma všetky príslušné opatrenia, ktorými sa zabraňuje, aby mali prevádzkovatelia brány digitálneho COVID preukazu EÚ neoprávnený prístup k prenášaným údajom.

15. Prijíma opatrenia na uľahčenie interoperability a komunikácie medzi určenými prevádzkovateľmi brány digitálneho COVID preukazu EÚ.

16. Vedie záznamy o spracovateľských činnostiach, ktoré vykonala v mene spoločných prevádzkovateľov, v súlade s článkom 31 ods. 2 nariadenia (EÚ) 2018/1725.