►B

DECYZJA WYKONAWCZA KOMISJI (UE) 2021/1073

z dnia 28 czerwca 2021 r.

ustanawiająca specyfikacje techniczne i zasady do celów wdrożenia ram zaufania unijnych cyfrowych zaświadczeń COVID ustanowionych rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2021/953

(Tekst mający znaczenie dla EOG)

(Dz.U. L 230 z 30.6.2021, s. 32)

zmieniona przez:

		Dziennik Urzędowy		
		nr	strona	data
►M1	Decyzja wykonawcza Komisji (UE) 2021/2014 z dnia 17 listopada 2021 r.	L 410	180	18.11.2021
►M2	Decyzja wykonawcza Komisji (UE) 2021/2301 z dnia 21 grudnia 2021 r.	L 458	536	22.12.2021
►M3	Decyzja wykonawcza Komisji (UE) 2022/483 z dnia 21 marca 2022 r.	L 98	84	25.3.2022
►M4	Decyzja wykonawcza Komisji (UE) 2022/1516 z dnia 8 września 2022 r.	L 235	61	12.9.2022

▼B

DECYZJA WYKONAWCZA KOMISJI (UE) 2021/1073

z dnia 28 czerwca 2021 r.

ustanawiająca specyfikacje techniczne i zasady do celów wdrożenia ram zaufania unijnych cyfrowych zaświadczeń COVID ustanowionych rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2021/953

(Tekst mający znaczenie dla EOG)

Artykuł 1

Specyfikacje techniczne unijnego cyfrowego zaświadczenia COVID określające ogólną strukturę danych, mechanizmy kodowania oraz mechanizm kodowania transportowego w formacie optycznym nadającym się do odczytu maszynowego są określone w załączniku I.

Artykuł 2

Zasady dotyczące wypełnienia zaświadczeń, o których mowa w art. 3 ust. 1 rozporządzenia (UE) 2021/953, są określone w załączniku II do niniejszej decyzji.

Artykuł 3

Wymogi określające wspólną strukturę niepowtarzalnego identyfikatora zaświadczenia są określone w załączniku III.

▼M1

Artykuł 4

Zasady zarządzania mające zastosowanie do certyfikatów klucza publicznego w odniesieniu do bramy sieciowej unijnych cyfrowych zaświadczeń COVID wspierającej aspekty interoperacyjności ram zaufania określono w załączniku IV.

Artykuł 5

Wspólną skoordynowaną strukturę danych w odniesieniu do danych, które mają być zawarte w zaświadczeniach, o których mowa w art. 3 ust. 1 rozporządzenia (UE) 2021/953, wykorzystującą schemat JSON, określono w załączniku V do niniejszej decyzji.”.

▼M3

Artykuł 5a

Wymiana list unieważnionych certyfikatów

1. Ramy zaufania unijnych cyfrowych zaświadczeń COVID umożliwiają wymianę list unieważnionych certyfikatów za pośrednictwem centralnej bramy sieciowej unijnego cyfrowego zaświadczenia COVID („brama sieciowa”) zgodnie ze specyfikacjami technicznymi zawartymi w załączniku I.

2. W przypadku gdy państwa członkowskie unieważniają unijne cyfrowe zaświadczenia COVID, mogą przedłożyć listę unieważnionych certyfikatów w bramie sieciowej.

▼M3

3. W przypadku gdy państwa członkowskie przedkładają listy unieważnionych certyfikatów, organy wydające prowadzą listę unieważnionych certyfikatów.

4. Jeżeli dane osobowe są wymieniane za pośrednictwem bramy sieciowej, przetwarzanie ogranicza się do celu, jakim jest wspieranie wymiany informacji o unieważnieniu. Takie dane osobowe wykorzystuje się wyłącznie do celów weryfikacji statusu unieważnienia unijnych cyfrowych zaświadczeń COVID wydanych w ramach zakresu stosowania rozporządzenia (UE) 2021/953.

5. Informacje przekazywane do bramy sieciowej obejmują następujące dane zgodnie ze specyfikacjami technicznymi określonymi w załączniku I:

a) pseudonimizowane niepowtarzalne identyfikatory unieważnionych zaświadczeń,

b) data wygaśnięcia przedłożonej listy unieważnionych certyfikatów;

6. W przypadku gdy organ wydający unieważnia unijne cyfrowe zaświadczenia COVID, które wydał na podstawie rozporządzenia (UE) 2021/953 lub rozporządzenia (UE) 2021/954 i zamierza wymieniać przedmiotowe informacje za pośrednictwem bramy sieciowej, przekazuje on do bramy sieciowej w bezpiecznym formacie informacje, o których mowa w ust. 5, w formie list unieważnionych certyfikatów, zgodnie ze specyfikacjami technicznymi określonymi w załączniku I.

7. Organy wydające zapewniają, w miarę możliwości, rozwiązanie mające na celu poinformowanie posiadaczy unieważnionych zaświadczeń – w momencie ich unieważnienia – o statusie unieważnienia ich zaświadczeń i o jego powodach.

8. Brama sieciowa gromadzi otrzymane listy unieważnień certyfikatów. Zapewnia ona narzędzia do przekazywania tych list państwom członkowskim. Automatycznie usuwa listy według terminów ich wygaśnięcia wskazanych dla poszczególnych list przedkładanych przez organ przekazujący.

9. Wyznaczone organy krajowe lub organy urzędowe państw członkowskich przetwarzające dane osobowe za pośrednictwem bramy sieciowej są współadministratorami przetwarzanych danych. Podział odpowiednich obowiązków między współadministratorami przebiega zgodnie z załącznikiem VI.

10. Komisja jest podmiotem przetwarzającym dane osobowe, które podlegają przetwarzaniu za pośrednictwem bramy sieciowej. Do kompetencji Komisji jako podmiotu przetwarzającego dane w imieniu państw członkowskich należy zapewnienie bezpieczeństwa przesyłu i przechowywania danych osobowych w ramach bramy sieciowej oraz wypełnianie obowiązków podmiotu przetwarzającego określonych w załączniku VII.

11. Skuteczność środków technicznych i organizacyjnych służących zapewnieniu bezpieczeństwa przetwarzania danych osobowych za pośrednictwem bramy sieciowej jest regularnie sprawdzana i oceniana przez Komisję i przez współadministratorów.

▼M3

Artykuł 5b

Przedkładanie przez państwa trzecie list unieważnionych certyfikatów

Państwa trzecie wydające zaświadczenia COVID-19, w odniesieniu do których Komisja przyjęła akt wykonawczy na podstawie art. 3 ust. 10 lub art. 8 ust. 2 rozporządzenia (UE) 2021/953, mogą przedkładać listy unieważnionych certyfikatów COVID-19 objętych takim aktem wykonawczym do przetwarzania przez Komisję w imieniu współadministratorów za pośrednictwem bramy sieciowej, jak określono w art. 5a, zgodnie ze specyfikacjami technicznymi określonymi w załączniku I.

Artykuł 5c

Zarządzanie przetwarzaniem danych osobowych w centralnej bramie sieciowej unijnych cyfrowych zaświadczeń COVID

1. Proces decyzyjny współadministratorów jest regulowany przez grupę roboczą ustanowioną w ramach komitetu, o którym mowa w art. 14 rozporządzenia (UE) 2021/953.

2. Wyznaczone organy krajowe lub organy urzędowe państw członkowskich przetwarzające dane osobowe za pośrednictwem bramy sieciowej jako współadministratorzy wyznaczają przedstawicieli do tej grupy.

▼M1

Artykuł 6

Niniejsza decyzja wchodzi w życie z dniem jej opublikowania w *Dzienniku Urzędowym Unii Europejskiej*.

▼B

Niniejsza decyzja wchodzi w życie z dniem jej opublikowania w *Dzienniku Urzędowym Unii Europejskiej*.

▼B

ZAŁĄCZNIK I

FORMAT I ZARZĄDZANIE ZAUFANIEM

Ogólna struktura danych, mechanizmy kodowania i mechanizm kodowania transportowego w formacie optycznym nadającym się do odczytu maszynowego (zwanym dalej „QR”)

1. **Wprowadzenie**

Specyfikacje techniczne określone w niniejszym załączniku zawierają ogólną strukturę danych i mechanizmy kodowania unijnego cyfrowego zaświadczenia COVID („zaświadczenie COVID”). Określają one również mechanizm kodowania transportowego w formacie optycznym nadającym się do odczytu maszynowego („QR”), który można wyświetlić na ekranie urządzenia przenośnego lub wydrukować. Formaty kontenera elektronicznych świadectw zdrowia określone w tych specyfikacjach mają charakter ogólny, ale w tym kontekście wykorzystywane są do przenoszenia zaświadczenia COVID.

2. **Terminologia**

Do celów niniejszego załącznika „wystawcy” oznaczają organizacje korzystające z niniejszych specyfikacji do wystawiania świadectw zdrowia, a „weryfikatorzy” oznaczają organizacje akceptujące świadectwa zdrowia jako dowód statusu zdrowotnego. „Uczestnicy” oznaczają wystawców i weryfikatorów. Niektóre aspekty wymienione w niniejszym załączniku, takie jak zarządzanie przestrzenią nazw i dystrybucja kluczy kryptograficznych, muszą być koordynowane między uczestnikami. Zakłada się, że zadania te wykonuje strona zwana dalej „Sekretariatem”.

3. **Format kontenera elektronicznego świadectwa zdrowia**

Format kontenera elektronicznego świadectwa zdrowia (ang. *electronic health certificate container format*, „HCERT”) ma na celu zapewnienie jednolitego i znormalizowanego nośnika dla świadectw zdrowia wydawanych przez różnych wystawców („wystawcy”). Celem niniejszych specyfikacji jest harmonizacja sposobu przedstawiania, kodowania i podpisywania świadectw zdrowia, aby ułatwić interoperacyjność.

Możliwość odczytu i interpretacji zaświadczenia COVID wydanego przez dowolnego wystawcę wymaga wspólnej struktury danych i porozumienia co do znaczenia każdego pola danych w ładunku (ang. *payload*). Aby ułatwić taką interoperacyjność, wspólną skoordynowaną strukturę danych definiuje się za pomocą schematu JSON, który stanowi szkielet zaświadczenia COVID.

3.1. *Struktura ładunku*

Ładunek jest zorganizowany i zakodowany w formacie CBOR z podpisem cyfrowym w formacie COSE. Jest to powszechnie znane jako „token sieciowy CBOR”, zdefiniowany w specyfikacji RFC 8392 ([1]). Ładunek zdefiniowany w poniższych sekcjach jest transportowany w oświadczeniu hcert.

Integralność i autentyczność pochodzenia danych ładunku musi być możliwa do sprawdzenia przez weryfikatora. W tym celu wystawca musi podpisać token sieciowy CBOR przy użyciu systemu podpisu elektronicznego szyfrowanego asymetrycznie określonego w specyfikacji COSE (RFC 8152 ([2])).

3.2. *Oświadczenia tokena sieciowego CBOR*

3.2.1. Przegląd struktury tokena sieciowego CBOR

Nagłówek chroniony

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

▼B

— Algorytm podpisu (alg, etykieta 1)

— Identyfikator klucza (kid, etykieta 4)

Ładunek danych

— Wystawca (iss, klucz oświadczenia 1, opcjonalny, kod ISO 3166-1 alfa-2 wystawcy)

— Data wydania (iat, klucz oświadczenia 6)

— Czas wygaśnięcia (exp, klucz oświadczenia 4)

— Świadectwo zdrowia (hcert, klucz oświadczenia -260)

— Unijne cyfrowe zaświadczenie COVID v1 (eu_DCC_v1, klucz oświadczenia 1)

Podpis

3.2.2. Algorytm podpisu

Parametr Algorytm podpisu (alg) wskazuje, jakiego algorytmu używa się do utworzenia podpisu. Musi on spełniać lub przewyższać aktualne wytyczne SOG-IS, które streszczono w poniższych punktach.

Zdefiniowano jeden algorytm główny i jeden algorytm dodatkowy. Algorytm dodatkowy powinien być stosowany tylko w przypadku, gdy algorytm główny jest niedopuszczalny w ramach zasad i przepisów obowiązujących wystawcę.

W celu zapewnienia bezpieczeństwa systemu wszystkie wdrożenia muszą zawierać algorytm dodatkowy. Z tego powodu wdrożony musi być zarówno algorytm główny, jak i dodatkowy.

Poziomy ustalone przez SOG-IS w odniesieniu do algorytmu głównego i dodatkowego są następujące:

— Algorytm główny: Algorytmem głównym jest algorytm podpisu cyfrowego krzywej eliptycznej (ECDSA) zdefiniowany w (ISO/IEC 14888-3:2006) sekcja 2.3, wykorzystujący parametry P-256 zdefiniowane w dodatku D (D.1.2.3) do (FIPS PUB 186-4) w połączeniu z algorytmem skrótu SHA-256 zdefiniowanym w (ISO/IEC 10118-3:2004) funkcja 4.

Odpowiada to parametrowi algorytmu COSE ES256.

— Algorytm dodatkowy: Algorytmem dodatkowym jest RSASSA-PSS zdefiniowany w (RFC 8230 [1]) o module 2048 bitów w połączeniu z algorytmem skrótu SHA-256 zdefiniowanym w (ISO/IEC 10118-3:2004) funkcja 4.

Odpowiada to parametrowi algorytmu COSE: PS256.

3.2.3. Identyfikator klucza

Oświadczenie Identyfikator klucza (kid) wskazuje certyfikat dla podpisujących dokumenty (DSC) zawierający klucz publiczny, który ma być stosowany przez weryfikatora do sprawdzania poprawności podpisu cyfrowego. Zarządzanie certyfikatami klucza publicznego, w tym wymogi dotyczące certyfikatów dla podpisujących dokumenty, opisano w załączniku IV.

[1] rfc8230 (ietf.org).

▼B

Weryfikatorzy używają oświadczenia Identyfikator klucza (kid) do wyboru właściwego klucza publicznego z listy kluczy dotyczących wystawcy zawartych w oświadczeniu Wystawca (iss). Ze względów administracyjnych i przy przerzucaniu klucza wystawca może równolegle używać kilku kluczy. Identyfikator klucza nie jest polem o krytycznym znaczeniu dla bezpieczeństwa. Z tego powodu w razie potrzeby może być również umieszczony w nagłówku niechronionym. Weryfikatorzy muszą akceptować obie opcje. Jeżeli występują obie opcje, musi być użyty identyfikator klucza w nagłówku chronionym.

Ze względu na skrócenie identyfikatora (w celu ograniczenia rozmiaru) istnieje niewielkie, ale niezerowe prawdopodobieństwo, że zbiorcza lista certyfikatów dla podpisujących dokumenty (DSC), które akceptuje weryfikator, może zawierać certyfikaty dla podpisujących dokumenty z podwójnymi kid. Z tego powodu weryfikator musi sprawdzić wszystkie certyfikaty dla podpisujących dokumenty z tym kid.

3.2.4. Wystawca

Oświadczenie Wystawca (iss) jest wartością ciągu, która może zawierać kod ISO 3166-1 alfa-2 państwa wystawcy świadectwa zdrowia. Weryfikator może wykorzystywać to oświadczenie w celu zidentyfikowania, który zestaw certyfikatów dla podpisujących dokumenty należy stosować do weryfikacji. Do identyfikacji tego oświadczenia używa się klucza oświadczenia 1.

3.2.5. Czas wygaśnięcia

Oświadczenie Czas wygaśnięcia (exp) musi posiadać znacznik czasu w formacie daty numerycznej (NumericDate) wyrażonej liczbami całkowitymi (jak określono w RFC 8392 ([1]), sekcja 2), wskazujący, przez jaki czas dany podpis dotyczący ładunku uznaje się za ważny; po upływie tego czasu weryfikator musi odrzucić ładunek z powodu jego wygaśnięcia. Celem parametru wygaśnięcia jest wymuszenie ograniczenia okresu ważności świadectwa zdrowia. Do identyfikacji tego oświadczenia używa się klucza oświadczenia 4.

Czas wygaśnięcia nie może przekraczać okresu ważności certyfikatu dla podpisujących dokumenty.

3.2.6. Data wydania

Oświadczenie Data wydania (iat) musi posiadać znacznik czasu w formacie daty numerycznej (NumericDate) wyrażonej liczbami całkowitymi (jak określono w RFC 8392 ([2]), sekcja 2), wskazujący czas utworzenia świadectwa zdrowia.

Pole Data wydania nie może zawierać wartości poprzedzającej okres ważności certyfikatu dla podpisujących dokumenty.

Weryfikatorzy mogą stosować dodatkowe zasady w celu ograniczenia ważności świadectwa zdrowia na podstawie terminu jego wystawienia. Do identyfikacji tego oświadczenia używa się klucza oświadczenia 6.

3.2.7. Oświadczenie Świadectwo zdrowia

Oświadczenie Świadectwo zdrowia (hcert) jest obiektem JSON (RFC 7159 ([3])) zawierającym informacje o statusie zdrowotnym. W ramach tego samego oświadczenia może istnieć kilka różnych rodzajów świadectw zdrowia, z których jednym jest zaświadczenie COVID.

JSON służy wyłącznie do celów schematu. Format odwzorowania to CBOR, zdefiniowany w RFC 7049 ([4]). Programiści aplikacji nie muszą w rzeczywistości nigdy dekodować ani kodować do i z formatu JSON, lecz wykorzystują strukturę w pamięci.

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

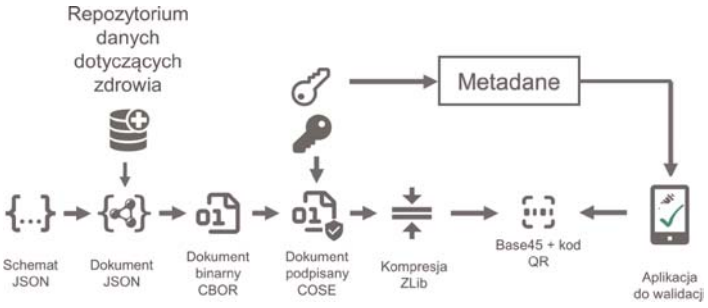
▼B

Do identyfikacji tego oświadczenia używa się klucza oświadczenia -260.

Ciągi w obiekcie JSON powinny być znormalizowane zgodnie z formatem Normalization Form Canonical Composition (NFC) zdefiniowanym w standardzie Unicode. Aplikacje dekodujące powinny być jednak permisywne i niezawodne w tych aspektach; zdecydowanie zachęca się do akceptacji każdej racjonalnej konwersji typu. Jeśli podczas dekodowania lub przy wykonywaniu późniejszych funkcji porównywania zostaną znalezione dane nieznormalizowane, wdrożenia powinny zachowywać się tak, jakby dane wejściowe były znormalizowane do NFC.

4. **Serializacja i tworzenie ładunku zaświadczenia COVID**

Jako wzorzec serializacji stosuje się następujący schemat:



Proces rozpoczyna się od pozyskania danych, np. z repozytorium danych dotyczących zdrowia (lub jakiegoś zewnętrznego źródła danych), i uporządkowania pozyskanych danych zgodnie ze zdefiniowanymi schematami zaświadczenia COVID. W tym procesie przed rozpoczęciem serializacji do CBOR może mieć miejsce konwersja do zdefiniowanego formatu danych oraz przekształcenie do prezentacji czytelnej dla człowieka. Akronimy oświadczeń przyporządkowuje się w każdym przypadku do wyświetlanych nazw przed serializacją i po deserializacji.

Nieobowiązkowa treść danych krajowych nie jest dozwolona w zaświadczeniach wydanych zgodnie z rozporządzeniem (UE) 2021/953 ([1]). Treść danych jest ograniczona do zdefiniowanych elementów danych znajdujących się w minimalnym zestawie danych określonym w załączniku do rozporządzenia (UE) 2021/953.

5. **Kodowanie transportowe**

5.1. *Surowe dane*

W przypadku interfejsów dowolnych danych kontener HCERT i jego ładunki mogą być przekazywane w stanie niezmienionym, z wykorzystaniem dowolnego bazowego 8-bitowego transportu danych charakteryzującego się bezpieczeństwem i niezawodnością. Interfejsy te mogą obejmować komunikację zbliżeniową (ang. *Near-Field Communication* – NFC), Bluetooth lub transfer przez protokół warstwy aplikacji, np. transfer HCERT od wystawcy na urządzenie przenośne posiadacza.

Jeżeli transfer HCERT od wystawcy do posiadacza odbywa się na podstawie interfejsu wyłącznie prezentacyjnego (np. SMS, e-mail), kodowanie transportu surowych danych oczywiście nie ma zastosowania.

([1]) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2021/953 z dnia 14 czerwca 2021 r. w sprawie ram wydawania, weryfikowania i uznawania interoperacyjnych zaświadczeń o szczepieniu, o wyniku testu i o powrocie do zdrowia w związku z COVID-19 (unijne cyfrowe zaświadczenie COVID) w celu ułatwienia swobodnego przemieszczania się w czasie pandemii COVID-19, Dz.U. L 211 z 15.6.2021, s. 1.

▼B

5.2. *Kod kreskowy*

5.2.1. Kompresja ładunku (tokena sieciowego CBOR)

W celu zmniejszenia rozmiaru HCERT oraz poprawy szybkości i niezawodności procesu odczytu HCERT kompresuje się token sieciowy CBOR przy użyciu ZLIB (RFC 1950 ([1])) i mechanizmu kompresji Deflate w formacie określonym w RFC 1951 ([2]).

5.2.2. Dwuwymiarowy kod kreskowy QR

Na potrzeby lepszej obsługi starszych urządzeń przeznaczonych do pracy z ładunkami ASCII skompresowany token sieciowy CBOR przed zakodowaniem do postaci dwuwymiarowego kodu kreskowego koduje się jako ASCII przy użyciu Base45.

Do generowania dwuwymiarowego kodu kreskowego stosuje się format QR zdefiniowany w (ISO/IEC 18004:2015). Zalecany jest poziom korekcji błędów „Q” (ok. 25 %). Ponieważ stosuje się Base45, w kodzie QR musi być zastosowane kodowanie alfanumeryczne (model 2, oznaczony symbolami 0010).

Aby umożliwić weryfikatorom wykrycie rodzaju zakodowanych danych oraz wybór właściwego schematu dekodowania i przetwarzania, dane zakodowane przy użyciu Base45 (zgodnie z niniejszą specyfikacją) poprzedzone są ciągiem identyfikatora kontekstu „HC1:”. W przyszłych wersjach niniejszej specyfikacji, które mają wpływ na kompatybilność wsteczną, zdefiniowany zostanie nowy identyfikator kontekstu, przy czym znak następujący po „HC” musi pochodzić ze zbioru znaków [1-9 A-Z]. Kolejność przyrostów jest zdefiniowana w tym porządku, tj. najpierw [1-9], a następnie [A-Z].

Zaleca się, aby kod optyczny był odwzorowywany na nośniku prezentacyjnym o przekątnej wynoszącej 35–60 mm, aby uwzględnić czytniki ze stałym układem optycznym, w przypadku których wymagane jest umieszczenie nośnika prezentacji na powierzchni czytnika.

Jeżeli kod optyczny jest drukowany na papierze przy użyciu drukarek o niskiej rozdzielczości (< 300 dpi), należy zadbać o to, aby każdy symbol (punkt) kodu QR był przedstawiony jako dokładny kwadrat. Skalowanie nieproporcjonalne spowoduje, że w niektórych wierszach lub kolumnach kodu QR znajdą się symbole prostokątne, co w wielu przypadkach utrudni czytelność.

6. **Format listy zaufania (lista krajowych centrów certyfikacji dla podpisujących i certyfikatów dla podpisujących dokumenty)**

Każde państwo członkowskie jest zobowiązane do dostarczenia listy zawierającej co najmniej jedno krajowe centrum certyfikacji dla podpisujących (CSCA) i listy wszystkich ważnych certyfikatów dla podpisujących dokumenty (DSC) oraz do dbania o aktualność tych list.

6.1. *Uproszczone zasady dotyczące krajowych centrów certyfikacji dla podpisujących i certyfikatów dla podpisujących dokumenty*

Począwszy od niniejszej wersji specyfikacji, państwa członkowskie nie zakładają, że wykorzystywane są jakiekolwiek informacje z listy unieważnionych certyfikatów, ani że okres użytkowania klucza prywatnego jest weryfikowany przez podmioty wdrażające.

Zamiast tego podstawowym mechanizmem sprawdzania ważności jest obecność certyfikatu na najnowszej wersji tej listy certyfikatów.

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

▼B

6.2. *Infrastruktura klucza publicznego elektronicznych dokumentów podróży odczytywanych maszynowo ICAO oraz jej centra zaufania*

Państwa członkowskie mogą korzystać z oddzielnego krajowego centrum certyfikacji dla podpisujących, ale mogą również przedkładać swoje istniejące certyfikaty krajowych centrów certyfikacji dla podpisujących elektroniczne dokumenty podróży odczytywane maszynowo lub certyfikaty dla podpisujących dokumenty; mogą nawet zdecydować się na nabycie certyfikatów od (komercyjnych) centrów zaufania i przedłożenie ich. Każdy certyfikat dla podpisujących dokumenty musi być jednak zawsze podpisany przez krajowe centrum certyfikacji dla podpisujących wskazane przez to państwo członkowskie.

7. **Względy bezpieczeństwa**

Projektując system z wykorzystaniem niniejszej specyfikacji, państwa członkowskie muszą zidentyfikować, przeanalizować i monitorować określone aspekty bezpieczeństwa.

Należy uwzględnić co najmniej następujące aspekty:

7.1. *Czas ważności podpisu HCERT*

Wystawca HCERT jest zobowiązany do ograniczenia okresu ważności podpisu przez określenie czasu wygaśnięcia podpisu. W rezultacie posiadacz świadectwa zdrowia musi okresowo przedłużać jego ważność.

O dopuszczalnym okresie ważności mogą decydować ograniczenia praktyczne. Na przykład podróżny może nie mieć możliwości przedłużenia ważności świadectwa zdrowia podczas podróży za granicą. Może jednak zdarzyć się, że wystawca bierze pod uwagę możliwość pewnego rodzaju naruszenia bezpieczeństwa, co wymaga od niego wycofania certyfikatu dla podpisujących dokumenty (unieważnienia wszystkich świadectw zdrowia wydanych przy użyciu tego klucza, których okres ważności jeszcze nie upłynął). Konsekwencje takiego zdarzenia można ograniczyć przez regularne przerzucanie kluczy wystawców i wymóg przedłużania ważności wszystkich świadectw zdrowia w pewnych rozsądnych odstępach czasu.

7.2. *Zarządzanie kluczami*

Niniejsza specyfikacja w dużym stopniu opiera się na silnych mechanizmach kryptograficznych zabezpieczających integralność danych i uwierzytelnianie pochodzenia danych. W związku z tym konieczne jest utrzymanie poufności kluczy prywatnych.

Poufność kluczy kryptograficznych może być zagrożona na szereg różnych sposobów, na przykład:

— proces generowania kluczy może być wadliwy, w wyniku czego powstają słabe klucze;

— do ujawnienia kluczy może dojść w wyniku błędu ludzkiego;

— klucze mogą zostać skradzione przez zewnętrznych lub wewnętrznych sprawców;

— klucze można obliczyć przy użyciu kryptoanalizy.

Aby ograniczyć ryzyko, że algorytm podpisu okaże się słaby, co umożliwi naruszenie kluczy prywatnych w wyniku kryptoanalizy, w niniejszej specyfikacji zaleca się wszystkim uczestnikom wdrożenie dodatkowego, rezerwowego algorytmu podpisu opartego na innych parametrach lub innym problemie matematycznym niż algorytm główny.

Jeżeli chodzi o wspomniane ryzyko związane ze środowiskami operacyjnymi wystawców, wdraża się środki ograniczające to ryzyko w celu zapewnienia skutecznej kontroli, takie jak generowanie, przechowywanie i stosowanie kluczy prywatnych w sprzętowych modułach bezpieczeństwa (ang. hardware security module, HSM). Zdecydowanie zachęca się do stosowania HSM do podpisywania świadectw zdrowia.

▼B

Niezależnie od tego, czy wystawca zdecyduje się na stosowanie HSM, należy ustanowić harmonogram przerzucania kluczy, w którym częstotliwość przerzucania kluczy jest proporcjonalna do ekspozycji kluczy na sieci zewnętrzne, inne systemy i personel. Dobrze dobrany harmonogram przerzucania ogranicza również ryzyko związane z błędnie wydanymi świadectwami zdrowia, umożliwiając wystawcy unieważnianie w razie potrzeby takich świadectw zdrowia partiami przez wycofanie klucza.

7.3. *Walidacja danych wejściowych*

Niniejsze specyfikacje można wykorzystywać w sposób zakładający wprowadzanie danych z niezaufanych źródeł do systemów, które mogą mieć krytyczne znaczenie dla misji. Aby zminimalizować ryzyko związane z tym wektorem ataku, wszystkie pola danych wejściowych muszą być odpowiednio zwalidowane pod względem poprawności rodzajów danych, długości i zawartości. Podpis wystawcy musi być również weryfikowany przed jakimkolwiek przetworzeniem zawartości formatu kontenera elektronicznego świadectwa zdrowia (HCERT). Walidacja podpisu wystawcy wymaga najpierw analizy chronionego nagłówka wystawcy, w którym potencjalny atakujący może próbować wprowadzić starannie opracowane informacje mające na celu naruszenie bezpieczeństwa systemu.

8. **Zarządzanie zaufaniem**

Podpisanie HCERT wymaga klucza publicznego do weryfikacji. Państwa członkowskie udostępniają te klucze publiczne. Ostatecznie każdy weryfikator musi posiadać listę wszystkich kluczy publicznych, którym chce ufać (ponieważ klucz publiczny nie jest częścią HCERT).

System składa się z (tylko) dwóch warstw: dla każdego państwa członkowskiego istnieje co najmniej jeden certyfikat na szczeblu krajowym, a każdy z tych certyfikatów służy do podpisywania co najmniej jednego certyfikatu dla podpisujących dokumenty, który to certyfikat jest używany w codziennej działalności.

Certyfikaty państw członkowskich nazywane są krajowymi centrami certyfikacji dla podpisujących (CSCA) i są (zazwyczaj) certyfikatami z podpisem własnym. Państwa członkowskie mogą mieć więcej niż jeden taki certyfikat (np. w przypadku decentralizacji regionalnej). Te certyfikaty krajowych centrów certyfikacji dla podpisujących regularnie służą do podpisywania certyfikatów dla podpisujących dokumenty (DSC), które to certyfikaty wykorzystuje się do podpisywania HCERT.

„Sekretariat” jest rolą funkcjonalną. Regularnie gromadzi i publikuje certyfikaty dla podpisujących dokumenty państw członkowskich po zweryfikowaniu ich z listą certyfikatów krajowych centrów certyfikacji dla podpisujących (które przekazano i zweryfikowano w inny sposób).

Otrzymana w ten sposób lista certyfikatów dla podpisujących dokumenty zapewnia następnie zagregowany zbiór akceptowanych kluczy publicznych (i odpowiadających im identyfikatorów kluczy), które weryfikatorzy mogą stosować do walidacji podpisów HCERT. Weryfikatorzy muszą regularnie pobierać i aktualizować tę listę.

Takie listy dotyczące poszczególnych państw członkowskich mogą mieć format dostosowany do ich kontekstu krajowego. W związku z tym format pliku tej listy zaufania może być różny, na przykład może to być podpisany JWKS (format zestawu JWK określony w RFC 7517 ([1]), sekcja 5) lub dowolny inny format właściwy dla technologii używanej w danym państwie członkowskim.

Aby zapewnić prostotę, państwa członkowskie mogą zarówno przedłożyć swoje istniejące certyfikaty krajowych centrów certyfikacji dla podpisujących ze swoich systemów elektronicznych dokumentów podróży odczytywanych maszynowo ICAO, jak i – zgodnie z zaleceniem WHO – utworzyć certyfikat specjalnie dla tej dziedziny zdrowia.

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

▼B

8.1. *Identyfikator klucza (kid)*

Identyfikator klucza (kid) oblicza się podczas tworzenia listy zaufanych kluczy publicznych z certyfikatów dla podpisujących dokumenty i składa się on z obciętego (do pierwszych 8 bajtów) cyfrowego odcisku palca SHA-256 certyfikatu dla podpisujących dokumenty zakodowanego w formacie DER (dane surowe).

Weryfikatorzy nie muszą obliczać identyfikatora klucza na podstawie certyfikatu dla podpisujących dokumenty i mogą bezpośrednio dopasować identyfikator klucza zawarty w wydanym świadectwie zdrowia do identyfikatora klucza znajdującego się na liście zaufania.

8.2. *Różnice w stosunku do modelu zaufania infrastruktury klucza publicznego elektronicznych dokumentów podróży odczytywanych maszynowo ICAO*

Chociaż wzorowano się na najlepszych praktykach modelu zaufania infrastruktury klucza publicznego elektronicznych dokumentów podróży odczytywanych maszynowo ICAO, w celu zapewnienia szybkości wprowadza się szereg uproszczeń:

— państwo członkowskie może przedłożyć wiele certyfikatów krajowych centrów certyfikacji dla podpisujących;

— okres ważności certyfikatu dla podpisujących dokumenty (użytkowania klucza) można ustalić na dowolny okres nieprzekraczający okresu ważności certyfikatu krajowego centrum certyfikacji dla podpisujących bądź można go pominąć;

— certyfikat dla podpisujących dokumenty może zawierać identyfikatory zasad (rozszerzone użytkowanie klucza) specyficzne dla świadectw zdrowia;

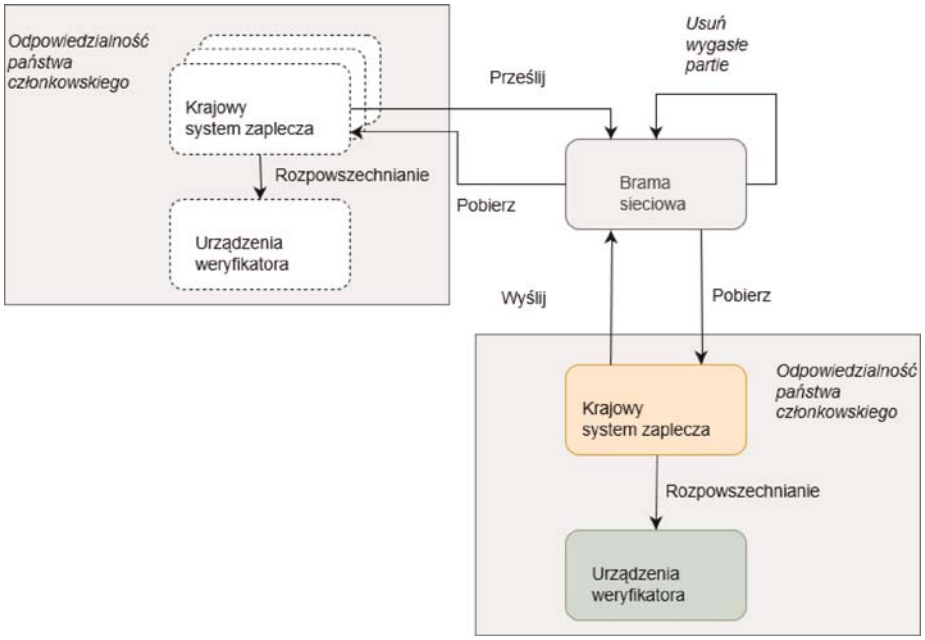
— państwa członkowskie mogą postanowić, że nie będą przeprowadzać żadnej weryfikacji opublikowanych unieważnień, lecz zamiast tego będą polegać wyłącznie na listach certyfikatów dla podpisujących dokumenty, które to listy otrzymują codziennie z Sekretariatu lub sporządzają samodzielnie.

▼M3

9. **Rozwiązanie w zakresie unieważnienia**

9.1. *Tworzenie listy unieważnionych DCC (DRL)*

Brama sieciowa zapewnia punkty końcowe i funkcje umożliwiające przechowywanie list unieważnionych certyfikatów i zarządzanie nimi:



▼M3

9.2. *Model zaufania*

Wszystkie połączenia są ustanawiane na podstawie standardowego modelu zaufania DCCG w certyfikatach NB_{TLS} i NB_{UP} (zob. zarządzanie certyfikatami). Wszystkie informacje są pakowane i przesyłane za pomocą wiadomości CMS w celu zapewnienia integralności.

9.3. *Budowa partii*

9.3.1. Partia (ang. batch)

Każda lista unieważnionych certyfikatów zawiera jedną pozycję lub większą ich liczbę i jest pakowana w partie zawierające zestaw skrótów (ang. hashes) i ich metadanych. Partia jest niezmienna i określa datę wygaśnięcia, która wskazuje, kiedy daną partię można usunąć. Data wygaśnięcia wszystkich pozycji w partii musi być dokładnie taka sama – oznacza to, że partie muszą być pogrupowane według daty wygaśnięcia i podpisania DSC. Każda partia zawiera maksymalnie 1 000 pozycji. Jeżeli lista unieważnionych certyfikatów składa się z ponad 1 000 pozycji, wówczas tworzy się kilka partii. Każda pozycja może występować w co najwyżej jednej partii. Partia jest pakowana do struktury CMS i podpisywana certyfikatem NB_{UP} kraju wysyłającego.

9.3.2. Indeks partii (ang. Batch Index)

Po utworzeniu partii brama sieciowa nadaje jej niepowtarzalne ID i partia jest automatycznie dodawana do indeksu. Indeks partii jest uporządkowany według daty modyfikacji, w porządku chronologicznym rosnącym.

9.3.3. Zachowanie bramy sieciowej

Brama sieciowa przetwarza partie unieważnień bez żadnych zmian: nie może ona aktualizować, usuwać ani dodawać żadnych informacji do partii. Partie są przekazywane wszystkim upoważnionym krajom (zob. rozdział 9.6).

Brama sieciowa aktywnie obserwuje daty wygaśnięcia partii i usuwa partie, które wygasły. Po usunięciu partii brama sieciowa odsyła, w odniesieniu do URL usuniętej partii, komunikat „HTTP 410 Gone”. W związku z tym partia pojawia się w indeksie partii jako „usunięta”.

9.4. *Rodzaje skrótu (ang. Hash Types)*

Lista unieważnionych certyfikatów zawiera skróty, które mogą odpowiadać różnym rodzajom/atrybutom unieważnienia. Te rodzaje lub atrybuty są wskazane w tworzeniu list unieważnionych certyfikatów. Obecne rodzaje są następujące:

Rodzaj	Atrybut	Obliczenie skrótu (ang. Hash Calculation)
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

Tylko pierwsze 128 bitów skrótów zakodowanych jako ciągi (ang. strings) base64 umieszcza się w partiach i wykorzystuje do identyfikacji unieważnionych DCC ([1]).

([1]) W odniesieniu do szczegółowych opisów API należy również wziąć pod uwagę pkt 9.5.1.2.

▼M3

9.4.1. Rodzaj skrótu: SHA256(Podpis DCC)

W tym przypadku skrót oblicza się na podstawie bajtów podpisu COSE_SIGN1 z CWT. W przypadku podpisów RSA cały podpis zostanie wykorzystany jako dane wejściowe. Wzór dla podpisanych certyfikatów EC-DSA wykorzystuje wartość r jako dane wejściowe:

SHA256(r)

[wymagane w przypadku wszystkich nowych wdrożeń]

9.4.2. Rodzaj skrótu: SHA256(UCI)

W tym przypadku skrót oblicza się dla ciągu UCI zakodowanego w UTF-8 i przekształconego na tablicę bajtów (ang. byte array).

[przestarzałe ([1]), ale obsługiwane ze względu na kompatybilność wsteczną]

9.4.3. Rodzaj skrótu: SHA256(Wydawanie CountryCode+UCI)

W tym przypadku CountryCode zakodowano jako ciąg UTF-8 złączony z UCI zakodowanym ciągiem UTF-8. Następnie przekształca się go w tablicę bajtów i wykorzystuje jako dane wejściowe do funkcji skrótu.

[przestarzałe[2], ale obsługiwane ze względu na kompatybilność wsteczną]

9.5. *Struktura API*

9.5.1. API dostarczająca pozycje unieważnienia

9.5.1.1. Cel

API dostarcza pozycje listy unieważnionych certyfikatów w partiach, w tym indeks partii.

9.5.1.2. Punkty końcowe (ang. Endpoints)

9.5.1.2.1. Punkt końcowy pobrania listy partii

Punkty końcowe są zgodne z prostym wzorem i odsyłają listę partii z małą obwolutą (ang. wrapper) dostarczającą metadane. Partie są sortowane według *daty* w porządku *rosnącym (chronologicznym)*:

/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]) Przestarzałe oznacza, że funkcja ta nie jest brana pod uwagę w przypadku nowych wdrożeń, lecz jest obsługiwana w odniesieniu do już realizowanych wdrożeń przez ściśle określony czas.

▼M3

Uwaga: Wynik jest domyślnie ograniczony do 1 000. Jeżeli znacznik „more” jest ustawiony na „true”, odpowiedź wskazuje, że dostępna jest większa liczba partii do pobrania. Aby pobrać więcej pozycji, klient musi ustawić nagłówek (ang. header) If-Modified-Since na datę nie wcześniejszą niż ostatni otrzymany wpis.

Odpowiedź zawiera tablicę JSON o następującej strukturze:

Pole	Definicja
more	Boolean Flag, który wskazuje, że jest więcej partii.
batches	Tablica z istniejącymi partiami.
batchId	https://en.wikipedia.org/wiki/Universally_unique_identifier
country	Kod państwa ISO 3166
date	ISO 8601 Data UTC. Data dodania lub usunięcia partii.
deleted	boolean. „True”, jeżeli usunięto. Po ustawieniu znacznika „deleted” wpis może zostać ostatecznie usunięty z wyników wyszukiwania po 7 dniach.

9.5.1.2.1.1. *Kody* odpowiedzi

Kod	Opis
200	Wszystko ok.
204	Brak treści, jeżeli treść nagłówka „If-Modified-Since” nie ma odpowiednika.

Nagłówek żądania (ang. Request Header)

Nagłówek	Obowiązkowe	Opis
If-Modified-Since	Tak	Ten nagłówek zawiera ostatnią pobraną datę, aby uzyskać tylko najnowsze wyniki. Przy pierwszym wywołaniu nagłówek powinien być ustawiony na „2021-06-01T00:00:00Z”

9.5.1.2.2. Punkt końcowy pobrania partii

Partie zawierają wykaz identyfikatorów certyfikatu:

/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’

}, ..]

}

Odpowiedź zawiera CMS z podpisem, który musi odpowiadać certyfikatowi NB_{UP} państwa. Wszystkie elementy na tablicy JSON mają następującą strukturę:

Pole	Obowiązkowe	Rodzaj	Definicja
expires	Tak	String	Data, w której element można usunąć. ISO8601 data/godzina UTC
country	Tak	String	Kod państwa ISO 3166
hashType	Tak	String	Rodzaj skrótu w podanych pozycjach (zob. rodzaje skrótów)
entries	Tak	JSON Object Array	Zob. pozycje w tabeli
kid	Tak	String	zakodowana base64 KID DSC używanego do podpisywania DCC. Jeżeli KID nie jest znany, można użyć ciągu 'UNKNOWN_KID' (z wyłączeniem ').

Uwagi:

— Partie są grupowane według daty wygaśnięcia i DSC – wszystkie pozycje wygasają w tym samym czasie i zostały podpisane tym samym kluczem.

— Czas wygaśnięcia jest datą/godziną w UTC, ponieważ EU-DCC jest systemem globalnym i konieczne jest używanie jednoznacznego czasu.

— Datę wygaśnięcia trwale unieważnionego DCC ustala się na dzień wygaśnięcia odpowiedniego DSC używanego do podpisania DCC lub na czas wygaśnięcia unieważnionych DCC (w którym to przypadku stosowane godziny NumericDate/epoch traktuje się jako znajdujące się w strefie czasowej UTC).

— Krajowy system zaplecza (NB, ang. National Backend) usuwa pozycje z listy unieważnionych certyfikatów po upływie daty **wygaśnięcia**.

— NB może usunąć pozycje z listy unieważnionych certyfikatów, w przypadku gdy **kid** użyty do podpisania DCC zostanie unieważniony.

▼M3

9.5.1.2.2.1. Pozycje

Pole	Obowiązkowe	Rodzaj	Definicja
hash	Tak	String	Pierwsze 128 bitów skrótu SHA256 zakodowane jako ciąg base64

Uwaga: Obiekt wpisów zawiera obecnie tylko skrót, ale w celu zapewnienia kompatybilności ze zmianami w przyszłości wybrano obiekt, a nie tablicę json.

9.5.1.2.2.2. Kody odpowiedzi

Kod	Opis
200	Wszystko ok.
410	Partia wykorzystana (ang. gone). Partia może zostać usunięta w krajowym systemie zaplecza.

9.5.1.2.2.3. Nagłówki odpowiedzi

Nagłówek	Opis
ETag	Numer identyfikacyjny partii (ang. Batch ID).

9.5.1.2.3. Punkt końcowy przesłania partii

Przesyłanie odbywa się w tym samym punkcie końcowym za pośrednictwem czasownika POST (ang. POST Verb):

/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’
        }, ..]
}
```

Partię należy podpisać za pomocą certyfikatu NB_{UP}. Brama sieciowa sprawdza, czy podpis został ustawiony przez NB_{UP} dla danego *państwa*. Jeżeli kontrola podpisu nie powiodła się, przesłanie nie powiedzie się.

UWAGA: Każda partia jest niezmienna (ang. immutable) i nie może być zmieniana po przesłaniu. Można ją jednak usunąć. Przechowuje się ID każdej usuniętej partii, a przesłanie nowej partii o tym samym ID zostaje odrzucone.

▼M3

9.5.1.2.4. Punkt końcowy usuwania partii

Partia może zostać usunięta z tego samego punktu końcowego za pośrednictwem czasownika DELETE (ang. DELETE Verb):

/revocation-list

Verb: DELETE

Accepts: application/cms

ContentType: application/cms

Request: CMS with Content

Content:

{

»batchId«: »...«

}

lub, ze względu na kompatybilność, do następującego punktu końcowego z czasownikiem POST:

/revocation-list/delete

Verb: POST

Accepts: application/cms

ContentType: application/cms

Request: CMS with Content

Content:

{

»batchId«: »...«

}

9.6. *Ochrona API/RODO*

W niniejszej sekcji określono środki służące wdrożeniu w celu zapewnienia zgodności z przepisami rozporządzenia (UE) 2021/953 w odniesieniu do przetwarzania danych osobowych.

9.6.1. Istniejące uwierzytelnianie

Obecnie brama sieciowa wykorzystuje certyfikat NB_{TLS} do uwierzytelniania państw łączących się z bramą sieciową. Uwierzytelnienie to można wykorzystać do określenia tożsamości państwa podłączonego do bramy sieciowej. Tożsamość tę można następnie wykorzystać do wdrożenia kontroli dostępu.

9.6.2. Kontrola dostępu

Aby móc zgodnie z prawem przetwarzać dane osobowe, brama sieciowa musi wdrożyć mechanizm kontroli dostępu.

Brama sieciowa wdraża wykaz kontroli dostępu połączony z zabezpieczeniem opartym na rolach. W tym systemie należy zachować dwie tabele – jedną tabelę opisującą, które role mogą stosować które operacje do których zasobów, a drugą tabelę opisującą, które role są przypisane do których użytkowników.

W celu przeprowadzenia kontroli wymaganych w niniejszym dokumencie wymagane są trzy role, tj.:

RevocationListReader

RevocationUploader

RevocationDeleter

▼**M3**

Następujące punkty końcowe sprawdzają, czy użytkownik posiada rolę RevocationListReader; jeżeli tak, wówczas dostęp zostanie przyznany, jeżeli nie, wówczas zostanie zwrócony komunikat HTTP 403 Forbidden:

GET/revocation-list/

GET/revocation-list/{batchId}

Następujące punkty końcowe muszą sprawdzić, czy użytkownik (ang. User) posiada rolę (ang. Role) RevocationUploader; jeżeli tak, wówczas dostęp zostanie przyznany, jeżeli nie, wówczas zostanie zwrócony komunikat HTTP 403 Forbidden:

POST/revocation-list

Następujące punkty końcowe muszą sprawdzić, czy użytkownik posiada rolę RevocationDeleter; jeżeli tak, wówczas dostęp zostanie przyznany, jeżeli nie, wówczas zostanie zwrócony komunikat HTTP 403 Forbidden:

DELETE/revocation-list

POST/revocation-list/delete

Brama sieciowa zapewnia również wiarygodną metodę, dzięki której administratorzy mogą zarządzać rolami powiązanymi z użytkownikami w taki sposób, aby zmniejszyć prawdopodobieństwo wystąpienia błędów ludzkich, nie obciążając jednocześnie administratorów funkcjonalnych.

▼M1

ZAŁĄCZNIK II

ZASADY WYPEŁNIANIA UNIJNEGO CYFROWEGO ZAŚWIADCZENIA COVID

Ogólne zasady dotyczące zestawów wartości ustanowione w niniejszym załączniku mają na celu zapewnienie interoperacyjności na poziomie semantycznym i umożliwiają jednolite wdrożenie techniczne unijnego cyfrowego zaświadczenia COVID. Elementy zawarte w niniejszym załączniku można stosować w odniesieniu do trzech różnych kontekstów (szczepienie/test/powrót do zdrowia) przewidzianych w rozporządzeniu (UE) 2021/953. W niniejszym załączniku wymieniono jedynie elementy, w przypadku których konieczna jest normalizacja semantyczna za pomocą zakodowanych zestawów wartości.

Tłumaczenie zakodowanych elementów na język krajowy należy do kompetencji państw członkowskich.

W przypadku wszystkich pól danych niewymienionych w poniższych opisach zestawów wartości kodowanie opisano w załączniku V.

Jeżeli z jakiegokolwiek powodu nie można zastosować preferowanych systemów kodów wymienionych poniżej, można zastosować inne międzynarodowe systemy kodów, przy czym zapewnia się wskazówki dotyczące sposobu przyporządkowywania kodów z innego systemu kodom z systemu preferowanego. W wyjątkowych przypadkach, gdy odpowiedni kod nie jest dostępny w zdefiniowanych zestawach wartości, jako mechanizm rezerwowy można stosować tekst (wyświetlanie nazw).

Państwa członkowskie stosujące w swoich systemach inne kody przyporządkowują takie kody opisanym zestawom wartości. Państwa członkowskie są odpowiedzialne za wszelkie takie przyporządkowania.

►M4 Ponieważ niektóre zestawy wartości oparte na systemach kodowania przewidzianych w niniejszym załączniku, takie jak zestawy wartości do kodowania szczepionek i testów antygenowych, często się zmieniają, Komisja publikuje je i regularnie aktualizuje przy wsparciu sieci e-zdrowie i Komitetu ds. Bezpieczeństwa Zdrowia. ◄ Zaktualizowane zestawy wartości są publikowane na odpowiedniej stronie internetowej Komisji, jak również na stronie internetowej sieci e-zdrowie. Przedstawia się historię zmian.

1. **Choroba lub czynnik chorobotwórczy, której/którego dotyczy szczepienie/choroba lub czynnik chorobotwórczy, w kierunku której/którego wykonano test/choroba lub czynnik chorobotwórczy, po której/którym posiadacz powrócił do zdrowia: COVID-19 (SARS-CoV-2 lub jeden z jego wariantów)**

   Kod stosowany w zaświadczeniach 1, 2 i 3.

   Stosuje się następujący kod:

Kod	Wyświetlanie	Nazwa systemu kodów	URL systemu kodów	OID systemu kodów	Wersja systemu kodów
840539006	COVID-19	SNOMED CT	http://snomed.info/sct	2.16.840.1.113883.6.96	2021-01-31

2. **Szczepionka przeciwko COVID-19 lub profilaktyka COVID-19**

   Preferowany system kodów: SNOMED CT lub klasyfikacja anatomiczno-terapeutyczno-chemiczna (ATC).

   Kod stosowany w zaświadczeniu 1.

   Przykłady kodów z preferowanych systemów kodów, które należy stosować, to kod SNOMED CT 1119305005 (szczepionka zawierająca antygen SARS-CoV-2), 1119349007 (szczepionka zawierająca mRNA SARS-CoV-2) lub J07BX03 (szczepionki przeciwko COVID-19).

   Komisja publikuje i regularnie aktualizuje przy wsparciu sieci e-zdrowie zestaw wartości określający kody, które należy stosować zgodnie z systemami kodów ustanowionymi w niniejszej sekcji. Zestaw wartości należy rozszerzyć, gdy nowe typy szczepionek zostaną opracowane i wprowadzone do użytku.

▼M1

3. **Szczepionka przeciwko COVID-19 stanowiąca produkt leczniczy**

Preferowane systemy kodów (w kolejności preferencji):

— unijny rejestr produktów leczniczych w przypadku szczepionek, dla których wydano pozwolenie na dopuszczenie do obrotu w całej UE (numery pozwoleń);

— światowy rejestr szczepionek, taki jak rejestr, który mogłaby ustanowić Światowa Organizacja Zdrowia;

— w innych przypadkach nazwa szczepionki stanowiącej produkt leczniczy. Jeżeli nazwa zawiera znaki niedrukowane, należy je zastąpić łącznikiem (-).

Nazwa zestawu wartości: szczepionka.

Kod stosowany w zaświadczeniu 1.

Przykładem kodu z preferowanych systemów kodów, który należy stosować, jest EU/1/20/1528 (Comirnaty). Przykład nazwy szczepionki, którą należy stosować jako kod: Sputnik-V (co oznacza Sputnik V).

Komisja publikuje i regularnie aktualizuje przy wsparciu sieci e-zdrowie zestaw wartości określający kody, które należy stosować zgodnie z systemami kodów ustanowionymi w niniejszej sekcji.

Szczepionki są kodowane przy użyciu istniejącego kodu w opublikowanym zestawie wartości, nawet jeśli ich nazwy różnią się w różnych krajach. Wynika to z faktu, że nie istnieje jeszcze światowy rejestr szczepionek obejmujący wszystkie szczepionki, które są obecnie stosowane. Przykład:

— W przypadku szczepionki „COVID-19 Vaccine Moderna Intramuscular Injection”, która jest nazwą szczepionki Spikevax w Japonii, należy użyć kodu EU/1/20/1507, ponieważ jest to nazwa tej szczepionki w UE.

Jeżeli nie jest to możliwe lub zalecane w konkretnym przypadku, w opublikowanym zestawie wartości podany zostanie osobny kod.

▼M4

Jeżeli państwo stosujące unijne cyfrowe zaświadczenie COVID postanowi w trakcie trwających badań klinicznych wydać zaświadczenia o szczepieniu uczestnikom tych badań, szczepionkę stanowiącą produkt leczniczy koduje się zgodnie z wzorcem

CT_*clinical-trial-identifier*

W przypadku gdy badanie kliniczne zostało zarejestrowane w unijnym rejestrze badań klinicznych (EU-CTR), stosuje się identyfikator badania klinicznego z tego rejestru. W pozostałych przypadkach można stosować identyfikatory z innych rejestrów (takich jak clinicaltrials.gov lub rejestr badań klinicznych Australii i Nowej Zelandii).

Identyfikator badania klinicznego musi zawierać prefiks umożliwiający identyfikację rejestru badań klinicznych (np. EUCTR w przypadku unijnego rejestru badań klinicznych, NCT w przypadku rejestru clinicaltrials.gov lub ACTRN w przypadku rejestru badań klinicznych Australii i Nowej Zelandii).

W przypadku gdy Komisja otrzymała od Komitetu ds. Bezpieczeństwa Zdrowia, Europejskiego Centrum ds. Zapobiegania i Kontroli Chorób (ECDC) lub Europejskiej Agencji Leków (EMA) wytyczne dotyczące uznawania zaświadczeń wydawanych na potrzeby szczepionki przeciwko COVID-19 poddawanej badaniom klinicznym, wytyczne te publikuje się bądź jako część dokumentu zawierającego zestawy wartości, bądź oddzielnie.

▼M1

4. **Posiadacz pozwolenia na dopuszczenie do obrotu szczepionki przeciwko COVID-19 lub jej producent**

Preferowany system kodów:

— kod organizacji EMA (system SPOR dla ISO IDMP);

— światowy rejestr posiadaczy pozwoleń na dopuszczenie szczepionki do obrotu lub producentów szczepionek, taki jak rejestr, który mogłaby ustanowić Światowa Organizacja Zdrowia;

— w pozostałych przypadkach nazwa organizacji. Jeżeli nazwa zawiera znaki niedrukowane, należy je zastąpić łącznikiem (-).

Kod stosowany w zaświadczeniu 1.

Przykładem kodu z preferowanych systemów kodów, który należy stosować, jest ORG-100001699 (AstraZeneca AB). Przykład nazwy organizacji, którą należy stosować jako kod: Sinovac-Biotech (co oznacza Sinovac Biotech).

Komisja publikuje i regularnie aktualizuje przy wsparciu sieci e-zdrowie zestaw wartości określający kody, które należy stosować zgodnie z systemami kodów ustanowionymi w niniejszej sekcji.

Różne oddziały tego samego posiadacza pozwolenia na dopuszczenie do obrotu lub tego samego producenta powinny używać kodu istniejącego w opublikowanym zestawie wartości.

Co do zasady w odniesieniu do tej samej szczepionki stosuje się kod odnoszący się do posiadacza pozwolenia na dopuszczenie jej do obrotu w UE, ponieważ nie istnieje jeszcze uzgodniony na szczeblu międzynarodowym rejestr producentów szczepionek ani posiadaczy pozwolenia na dopuszczenie szczepionki do obrotu. Przykłady:

— W przypadku organizacji „Pfizer AG”, która jest posiadaczem pozwolenia na dopuszczenie do obrotu szczepionki „Comirnaty” stosowanej w Szwajcarii, należy zastosować kod ORG-100030215 odnoszący się do BioNTech Manufacturing GmbH, ponieważ jest to posiadacz pozwolenia na dopuszczenie do obrotu (MAH) Comirnaty w UE.

— W przypadku organizacji „Zuellig Pharma”, która jest posiadaczem pozwolenia na dopuszczenie do obrotu szczepionki Covid-19 Vaccine Moderna (Spikevax) stosowanej na Filipinach, należy zastosować kod ORG-100031184 odnoszący się do Moderna Biotech Spain S.L., ponieważ jest to MAH Spikevax w UE.

Jeżeli nie jest to możliwe lub zalecane w konkretnym przypadku, w opublikowanym zestawie wartości podany zostanie osobny kod.

▼M4

Jeżeli państwo stosujące unijne cyfrowe zaświadczenie COVID postanowi w trakcie trwających badań klinicznych wydać zaświadczenia o szczepieniu uczestnikom tych badań, informacje o posiadaczu pozwolenia na dopuszczenie do obrotu szczepionki lub jej producencie koduje się przy użyciu wartości wskazanej w zestawie wartości, o ile jest dostępna. W pozostałych przypadkach posiadacz pozwolenia na dopuszczenie do obrotu lub producent kodowany jest przy użyciu zasady przedstawionej w sekcji 3 „Szczepionka przeciwko COVID-19 stanowiąca produkt leczniczy” (CT_*clinical-trial-identifier*).

▼M1

5. **Numer w serii dawek i łączna liczba dawek w serii;**

Kod stosowany w zaświadczeniu 1.

Dwa pola:

1) Numer w serii dawek szczepionki przeciwko COVID-19 (N);

2) Łączna liczba dawek w serii szczepień (C).

5.1. *Seria szczepienia pierwotnego*

W przypadku gdy dana osoba otrzymuje dawki w ramach szczepienia pierwotnego, tj. serii szczepień mających zapewnić wystarczającą ochronę na początkowym etapie, (C) odzwierciedla łączną liczbę dawek serii standardowego szczepienia pierwotnego (np. 1 lub 2, w zależności od rodzaju podanej szczepionki). Obejmuje to możliwość stosowania krótszej serii (C=1), w przypadku gdy protokół szczepień stosowany przez państwo członkowskie przewiduje podawanie pojedynczej dawki szczepionki 2-dawkowej osobom uprzednio zakażonym SARS-CoV-2. Zakończoną serię szczepień pierwotnych wskazuje się zatem za pomocą N/C = 1. Na przykład:

— 1/1 wskazywałoby na zakończenie cyklu szczepień pierwotnych szczepionką jednodawkową lub zakończenie cyklu szczepień pierwotnych obejmującego jedną dawkę szczepionki 2-dawkowej podanej osobie, która powróciła do zdrowia zgodnie z protokołem szczepień stosowanym przez dane państwo członkowskie;

— 2/2 wskazywałoby na zakończenie 2-dawkowego cyklu szczepień pierwotnych.

W przypadku wydłużenia cyklu szczepień pierwotnych, na przykład dla osób z poważnie osłabionym układem odpornościowymi lub gdy nie przestrzegano zalecanego odstępu między dawkami szczepienia pierwotnego, wszelkie takie dawki należy zakodować jako dawki dodatkowe objęte sekcją 5.2.

▼M2

5.2. *Dawki przypominające*

W przypadku gdy dana osoba otrzymuje dawki po serii szczepień pierwotnych, takie dawki przypominające odzwierciedla się w odpowiednich zaświadczeniach w następujący sposób:

— 2/1 wskazuje na podanie dawki przypominającej po serii szczepień pierwotnych szczepionką jednodawkową lub podanie dawki przypominającej po zakończeniu serii szczepień pierwotnych obejmującej jedną dawkę szczepionki dwudawkowej podanej osobie, która powróciła do zdrowia zgodnie z protokołem szczepień stosowanym przez dane państwo członkowskie. Następnie dawki (X) podawane po pierwszej dawce przypominającej należy wskazać za pomocą (2+X)/(1) > 1 (3/1, na przykład),

— 3/3 wskazuje na podanie dawki przypominającej po dwudawkowej serii szczepień pierwotnych. Następnie dawki (X) podawane po pierwszej dawce przypominającej należy wskazać za pomocą (3+X)/(3+X) = 1 (4/4, na przykład).

Państwa członkowskie wdrażają zasady kodowania określone w niniejszej sekcji do dnia 1 lutego 2022 r.

Państwa członkowskie ponownie wydają, automatycznie lub na wniosek zainteresowanych osób, zaświadczenia, w których podanie dawki przypominającej po serii szczepień pierwotnych szczepionką jednodawkową jest kodowane w taki sposób, że nie można go odróżnić od zakończenia serii szczepień pierwotnych.

▼M2

Do celów niniejszego załącznika odniesienia do „dawek przypominających” należy rozumieć jako obejmujące również dodatkowe dawki podawane w celu lepszej ochrony osób, które po zakończeniu serii standardowego szczepienia pierwotnego wykazują nieodpowiednie reakcje immunologiczne. W ramach prawnych ustanowionych rozporządzeniem (UE) 2021/953 państwa członkowskie mogą przyjąć środki w celu zaradzenia sytuacji grup szczególnie wrażliwych, które mogą otrzymać dodatkowe dawki w trybie priorytetowym. Na przykład jeżeli państwo członkowskie postanowi o podaniu dodatkowych dawek wyłącznie określonym podgrupom populacji, może zdecydować – zgodnie z art. 5 ust. 1 rozporządzenia (UE) 2021/953 – o wydawaniu zaświadczeń o szczepieniach wskazujących na podanie takich dodatkowych dawek wyłącznie na wniosek, a nie automatycznie. W przypadku przyjęcia takich środków państwa członkowskie informują o tym zainteresowane osoby, a także o tym, że mogą one nadal korzystać z zaświadczenia otrzymanego po zakończeniu serii standardowego szczepienia pierwotnego.

▼M1

6. **Państwo członkowskie lub państwo trzecie, w którym podano szczepionkę/wykonano test**

Preferowany system kodów: kody państw ISO 3166.

Kod stosowany w zaświadczeniach 1, 2 i 3.

Zawartość zestawu wartości: pełna lista dwuliterowych kodów, dostępna jako zestaw wartości zdefiniowany w FHIR (http://hl7.org/fhir/ValueSet/iso3166-1-2). Jeżeli szczepienie lub test przeprowadziła organizacja międzynarodowa (taka jak UNHCR lub WHO), a informacje o kraju nie są dostępne, stosuje się kod organizacji. Komisja publikuje i regularnie aktualizuje przy wsparciu sieci e-zdrowie takie dodatkowe kody.

7. **Rodzaj testu**

Kod stosowany w zaświadczeniu 2, a w zaświadczeniu 3 – jeżeli aktem delegowanym wprowadzone zostanie wsparcie dla wydawania zaświadczeń o powrocie do zdrowia opartych na rodzajach testów innych niż test NAAT.

Stosuje się następujące kody.

Kod	Wyświetlanie	Nazwa systemu kodów	URL systemu kodów	OID systemu kodów	Wersja systemu kodów
LP6464-4	Amplifikacja kwasu nukleinowego z sondą detekcyjną	LOINC	http://loinc.org	2.16.840.1.113883.6.1	2.69
LP217198-3	Szybki test immunologiczny	LOINC	http://loinc.org	2.16.840.1.113883.6.1	2.69

▼M4

Kod LP217198-3 (Szybki test immunologiczny) wykorzystuje się do wskazania zarówno szybkich testów antygenowych, jak i laboratoryjnych testów antygenowych

▼M1

8. **Producent i nazwa handlowa wykonanego testu (fakultatywne w przypadku testu NAAT)**

Kod stosowany w zaświadczeniu 2.

▼M4

Zawartość zestawu wartości obejmuje wybór testu antygenowego wymienionego we wspólnym i uaktualnionym wykazie testów antygenowych na COVID-19, ustanowionym na podstawie zalecenia Rady 2021/C 24/01 i uzgodnionym przez Komitet ds. Bezpieczeństwa Zdrowia. Wykaz ten prowadzi JRC w bazie danych dotyczącej wyrobów do diagnostyki in vitro i metod testowania COVID-19 pod adresem: https://covid-19-diagnostics.jrc.ec.europa.eu/devices/hsc-common-recognition-rat.

▼M1

W przypadku tego systemu kodów wykorzystuje się odpowiednie pola, takie jak: identyfikator zestawu testu, nazwa testu i producent, zgodnie ze zorganizowanym formatem JRC dostępnym pod adresem: https://covid-19-diagnostics.jrc.ec.europa.eu/devices

9. **Wynik testu**

Kod stosowany w zaświadczeniu 2.

Stosuje się następujące kody:

Kod	Wyświetlanie	Nazwa systemu kodów	URL systemu kodów	OID systemu kodów	Wersja systemu kodów
260415000	Nie wykryto	SNOMED CT	http://snomed.info/sct	2.16.840.1.113883.6.96	2021-01-31
260373001	Wykryto	SNOMED CT	http://snomed.info/sct	2.16.840.1.113883.6.96	2021-01-31

▼B

ZAŁĄCZNIK III

WSPÓLNA STRUKTURA NIEPOWTARZALNEGO IDENTYFIKATORA ZAŚWIADCZENIA

1. **Wprowadzenie**

Każde unijne cyfrowe zaświadczenie COVID (zaświadczenie COVID) musi zawierać niepowtarzalny identyfikator zaświadczenia, który wspiera interoperacyjność zaświadczeń. Identyfikator ten można wykorzystywać do weryfikacji zaświadczenia. Państwa członkowskie są odpowiedzialne za wdrożenie niepowtarzalnego identyfikatora zaświadczenia. Identyfikator ten służy do weryfikacji prawdziwości zaświadczenia oraz w stosownych przypadkach do połączenia z systemem rejestracji (np. z systemem informacyjnym dotyczącym szczepień – IIS). Identyfikatory te umożliwiają również potwierdzenie przez państwa członkowskie (w formie papierowej i elektronicznej), że dane osoby zaszczepiono lub poddano testowi.

2. **Skład niepowtarzalnego identyfikatora zaświadczenia**

Niepowtarzalny identyfikator zaświadczenia ma wspólną strukturę i wspólny format ułatwiające interpretację informacji przez człowieka lub maszynę i może odnosić się do takich elementów, jak: państwo członkowskie, w którym miało miejsce szczepienie, sama szczepionka i identyfikator właściwy dla danego państwa członkowskiego. Zapewnia on państwom członkowskim elastyczność w zakresie formatu informacji przy pełnym poszanowaniu przepisów o ochronie danych. Kolejność poszczególnych elementów jest zgodna z określoną hierarchią, która może umożliwiać przyszłe modyfikacje bloków z jednoczesnym zachowaniem ich integralności strukturalnej.

Możliwe rozwiązania dotyczące składu niepowtarzalnego identyfikatora zaświadczenia tworzą spektrum, w którym modułowość i możliwość interpretacji przez człowieka są dwoma głównymi parametrami różnicującymi, a ponadto istnieje jedna podstawowa cecha:

— Modułowość: stopień, w jakim kod składa się z odrębnych bloków konstrukcyjnych, które zawierają semantycznie różne informacje.

— Możliwość interpretacji przez człowieka: stopień, w jakim kod jest znaczący lub może być interpretowany przez odczytującego go człowieka.

— powszechna niepowtarzalność: identyfikator państwa lub organu jest dobrze zarządzany, a od każdego państwa (organu) oczekuje się, że będzie dobrze zarządzał swoim segmentem przestrzeni nazw poprzez niestosowanie ani niewydawanie ponownie nigdy tych samych identyfikatorów. Połączenie tych czynników gwarantuje, że każdy identyfikator jest powszechnie niepowtarzalny.

▼M1

3. **Wymogi ogólne**

W odniesieniu do niepowtarzalnego identyfikatora zaświadczenia należy spełnić następujące nadrzędne wymogi:

1) zestaw znaków: dozwolone są tylko znaki alfanumeryczne US-ASCII, w tym wyłącznie duże litery („A”–„Z”, „0”–„9”), wraz z dodatkowymi znakami specjalnymi na potrzeby oddzielenia od RFC3986 ([1]), mianowicie {’/’,’#’,’:’};

2) maksymalna długość: autorzy powinni dążyć do długości wynoszącej 27–30 znaków ([2]);

3) prefiks wersji: odnosi się do wersji schematu niepowtarzalnego identyfikatora zaświadczenia. Prefiks wersji to »01« w przypadku niniejszej wersji dokumentu; prefiks wersji składa się z dwóch cyfr;

([1]) rfc3986 (ietf.org)

([2]) W przypadku wdrożenia wykorzystującego kody QR państwa członkowskie mogłyby rozważyć zastosowanie dodatkowego zestawu znaków o łącznej długości do 72 znaków (w tym 27–30 znaków samego identyfikatora) do przekazywania innych informacji. Określenie tych informacji należy do państw członkowskich.

▼M1

4) prefiks państwa: kod państwa jest określony normą ISO 3166-1. Dłuższe kody (np. zawierające co najmniej trzy znaki, np. „UNHCR”) są zarezerwowane do użytku w przyszłości;

5) sufiks kodu/suma kontrolna:

5.1 Państwa członkowskie mogą stosować sumę kontrolną, gdy istnieje prawdopodobieństwo, że może dojść do transmisji, transkrypcji (przez człowieka) lub innych uszkodzeń kodu (tj. w przypadku używania w druku).

5.2 Suma kontrolna nie jest podstawą do walidacji zaświadczenia i z technicznego punktu widzenia nie stanowi części identyfikatora, lecz służy do weryfikacji integralności kodu. Suma kontrolna jest zgodnym z ISO-7812-1 (LUHN-10) ([1]) streszczeniem całego niepowtarzalnego identyfikatora zaświadczenia w formacie cyfrowym/transportowym. Suma kontrolna jest oddzielona od pozostałej części identyfikatora znakiem „#”.

Zapewnia się kompatybilność wsteczną: państwa członkowskie, które na przestrzeni czasu zmieniają strukturę swoich identyfikatorów (w ramach głównej wersji, obecnie ustalonej jako v1), zapewniają, aby dowolne dwa identyczne identyfikatory odpowiadały temu samemu zaświadczeniu o szczepieniu/potwierdzeniu szczepienia. Innymi słowy, państwa członkowskie nie mogą używać identyfikatorów ponownie.

▼B

4. **Warianty niepowtarzalnych identyfikatorów zaświadczeń o szczepieniu**

W wytycznych sieci e-zdrowie w sprawie podlegających weryfikacji zaświadczeń o szczepieniu i podstawowych elementów interoperacyjności ([2]) przewidziano różne warianty dostępne dla państw członkowskich i innych stron, które to warianty mogą współistnieć w różnych państwach członkowskich. Państwa członkowskie mogą stosować takie różne warianty w różnych wersjach schematu niepowtarzalnego identyfikatora zaświadczenia.

([1]) Algorytm Luhna mod N jest rozszerzoną wersją algorytmu Luhna (zwanego również algorytmem mod 10) dotyczącą kodów numerycznych i stosowaną na przykład do obliczania sumy kontrolnej w przypadku numerów kart kredytowych. Rozszerzona wersja umożliwia stosowanie tego algorytmu do sekwencji wartości przy dowolnej podstawie (w tym przypadku znaków alfabetycznych).

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

▼B

ZAŁĄCZNIK IV

ZARZĄDZANIE CERTYFIKATAMI KLUCZY PUBLICZNYCH

1. **Wprowadzenie**

Bezpieczna i zaufana wymiana kluczy podpisu unijnych cyfrowych zaświadczeń COVID (zaświadczenia COVID) między państwami członkowskimi jest realizowana za pośrednictwem bramy sieciowej unijnych cyfrowych zaświadczeń COVID (brama sieciowa), która pełni funkcję centralnego repozytorium kluczy publicznych. Poprzez bramę sieciową państwa członkowskie są uprawnione do publikowania kluczy publicznych odpowiadających kluczom prywatnym, które stosują do podpisywania cyfrowych zaświadczeń COVID. Państwa członkowskie mogą korzystać z bramy sieciowej, aby na bieżąco pobierać aktualne materiały dotyczące kluczy publicznych. W późniejszym czasie bramę sieciową można rozszerzyć na wymianę godnych zaufania informacji uzupełniających, które dostarczają państwa członkowskie, takich jak zasady walidacji zaświadczeń COVID. Model zaufania ram zaświadczeń COVID to infrastruktura klucza publicznego. Każde państwo członkowskie posiada co najmniej jedno krajowe centrum certyfikacji dla podpisujących, którego certyfikaty mają stosunkowo długi okres ważności. Zgodnie z decyzją państwa członkowskiego krajowe centrum certyfikacji dla podpisujących może być takie samo lub inne niż centrum certyfikacji wykorzystywane w przypadku dokumentów podróży odczytywanych maszynowo. Krajowe centrum certyfikacji dla podpisujących wydaje certyfikaty klucza publicznego dla krajowych krótko działających podmiotów podpisujących dokumenty (tj. podpisujących zaświadczenia COVID), nazywane certyfikatami dla podpisujących dokumenty. Krajowe centrum certyfikacji dla podpisujących pełni funkcję kotwicy zaufania, dzięki czemu państwa członkowskie, które z niego korzystają, mogą stosować certyfikat krajowego centrum certyfikacji dla podpisujących do walidacji autentyczności i integralności regularnie zmieniających się certyfikatów dla podpisujących dokumenty. Po walidacji państwa członkowskie mogą przekazać te certyfikaty (lub tylko zawarte w nich klucze publiczne) do swoich aplikacji służących do weryfikacji zaświadczeń COVID. Oprócz krajowych centrów certyfikacji dla podpisujących i certyfikatów dla podpisujących dokumenty w bramie sieciowej wykorzystuje się również infrastrukturę klucza publicznego do uwierzytelniania transakcji i podpisywania danych jako podstawę uwierzytelniania oraz jako środek zapewniający integralność kanałów komunikacji między państwami członkowskimi a bramą sieciową.

Podpisy cyfrowe można wykorzystywać do osiągnięcia integralności i autentyczności danych. Infrastruktury klucza publicznego budują zaufanie przez wiązanie kluczy publicznych ze zweryfikowanymi tożsamościami (lub wystawcami). Jest to konieczne, aby umożliwić innym uczestnikom weryfikację pochodzenia danych i tożsamości partnera w komunikacji oraz podjęcie decyzji o zaufaniu. W bramie sieciowej używa się wielu certyfikatów klucza publicznego do zapewnienia autentyczności. W niniejszym załączniku określono, które certyfikaty klucza publicznego są wykorzystywane i jak powinny być zaprojektowane, aby umożliwić szeroko zakrojoną interoperacyjność między państwami członkowskimi. Zawiera on więcej szczegółowych informacji na temat niezbędnych certyfikatów klucza publicznego oraz wytyczne dotyczące szablonów certyfikatów i okresów ważności dla państw członkowskich, które chcą prowadzić własne krajowe centrum certyfikacji dla podpisujących. Ponieważ zaświadczenia COVID muszą być możliwe do sprawdzenia w określonych ramach czasowych (począwszy od wydania do wygaśnięcia po upływie określonego czasu), konieczne jest zdefiniowanie modelu weryfikacji wszystkich podpisów stosowanych na certyfikatach klucza publicznego i zaświadczeniach COVID.

2. **Terminologia**

Poniższa tabela zawiera skróty i terminy stosowane w niniejszym załączniku.

Termin	Definicja
Certyfikat	Lub certyfikat klucza publicznego. Certyfikat X.509 v3, który zawiera klucz publiczny podmiotu.

▼B

Termin	Definicja
CSCA	Krajowe centrum certyfikacji dla podpisujących
DCC	Unijne cyfrowe zaświadczenie COVID. Podpisany dokument elektroniczny, który zawiera informacje o szczepieniu, o wyniku testu i o powrocie do zdrowia.
DCCG	Brama sieciowa unijnych cyfrowych zaświadczeń COVID (ang. EU Digital COVID Certificate Gateway). System ten służy do wymiany certyfikatów dla podpisujących dokumenty między państwami członkowskimi.
$DCCG_{TA}$	Certyfikat kotwicy zaufania DCCG. Odpowiedni klucz prywatny wykorzystuje się do podpisywania w trybie offline listy wszystkich certyfikatów krajowego centrum certyfikacji dla podpisujących.
$DCCG_{TLS}$	Certyfikat serwera TLS bramy sieciowej
DSC	Certyfikat dla podpisujących dokumenty. Certyfikat klucza publicznego organu państwa członkowskiego podpisującego dokumenty (np. systemu uprawnionego do podpisywania zaświadczeń COVID). Certyfikat ten wydaje krajowe centrum certyfikacji dla podpisujących państwa członkowskiego.
ECDSA	Algorytm podpisu cyfrowego krzywej eliptycznej (ang. *elliptic curve digital signature algorithm*). Kryptograficzny algorytm podpisu oparty na krzywych eliptycznych.
Państwo członkowskie	Państwo członkowskie Unii Europejskiej
mTLS	TLS z uwierzytelnianiem wzajemnym. Protokół bezpieczeństwa warstwy transportowej (ang. *Transport Layer Security*) z uwierzytelnianiem wzajemnym.
NB	Krajowy system zaplecza (ang. *national backend*) państwa członkowskiego
NB_{CSCA}	Certyfikat krajowego centrum certyfikacji państwa członkowskiego dla podpisujących (może istnieć więcej niż jeden)
NB_{TLS}	Certyfikat uwierzytelniania klienta TLS krajowego systemu zaplecza
NB_{UP}	Certyfikat, którego krajowy system zaplecza używa do podpisywania pakietów danych wysyłanych do DCCG
PKI	Infrastruktura klucza publicznego (ang. *public key infrastructure*). Model zaufania oparty na certyfikatach klucza publicznego i centrach certyfikacji.
RSA	Asymetryczny algorytm kryptograficzny oparty na faktoryzacji liczb całkowitych, stosowany do podpisów cyfrowych lub szyfrowania asymetrycznego.

3. **Przepływ informacji i usługi bezpieczeństwa bramy sieciowej unijnych cyfrowych zaświadczeń COVID**

W niniejszej sekcji przedstawiono przepływ informacji i usługi bezpieczeństwa w systemie bramy sieciowej. Określono w niej również, które klucze i certyfikaty wykorzystuje się do ochrony komunikacji, wysłanych informacji, zaświadczeń COVID oraz podpisanej listy zaufania, która zawiera wszystkie zarejestrowane certyfikaty krajowych centrów certyfikacji dla podpisujących. Brama sieciowa pełni funkcję centrum danych, które umożliwia państwom członkowskim wymianę podpisanych pakietów danych.

▼B

Brama sieciowa dostarcza wysłane pakiety danych w stanie niezmienionym, co oznacza, że do otrzymywanych pakietów nie dodaje się żadnych certyfikatów dla podpisującego dokumenty ani nie usuwa się z nich takich certyfikatów. Krajowe systemy zaplecza państw członkowskich muszą mieć możliwość pełnej weryfikacji integralności i autentyczności wysłanych danych. Ponadto krajowe systemy zaplecza i brama sieciowa będą stosować TLS z uwierzytelnianiem wzajemnym, aby ustanowić bezpieczne połączenie. Stanowi to uzupełnienie podpisów zawartych w wymienianych danych.

3.1. *Uwierzytelnianie i ustanawianie połączenia*

Do ustanowienia uwierzytelnionego, szyfrowanego kanału między krajowym systemem zaplecza (NB) państwa członkowskiego a środowiskiem bramy sieciowej wykorzystuje się w tej bramie protokół bezpieczeństwa warstwy transportowej (TLS) z uwierzytelnianiem wzajemnym. Brama sieciowa posiada zatem certyfikat serwera TLS – w skrócie $DCCG_{TLS}$ – a krajowe systemy zaplecza posiadają certyfikat klienta TLS – w skrócie NB_{TLS}. Szablony certyfikatów przedstawiono w *sekcji 5*. Każdy krajowy system zaplecza może dostarczyć własny certyfikat TLS. Certyfikat ten zostanie wyraźnie umieszczony na białej liście, a zatem może być wydany przez publicznie zaufane centrum certyfikacji (np. centrum certyfikacji, który spełnia podstawowe wymogi CA/Browser Forum), przez krajowe centrum certyfikacji lub z podpisem własnym. Każde państwo członkowskie jest odpowiedzialne za swoje dane krajowe i ochronę klucza prywatnego używanego do ustanawiania połączenia z bramą sieciową. Podejście oparte na używaniu własnego certyfikatu wymaga dobrze zdefiniowanego procesu rejestracji i identyfikacji, jak również procedur unieważniania i przedłużania ważności, które opisano w *sekcjach4.1, 4.2* i *4.3*. Brama sieciowa korzysta z białej listy, do której po udanej rejestracji dodaje się certyfikaty TLS krajowych systemów zaplecza. Bezpieczne połączenie z bramą sieciową mogą nawiązać tylko te krajowe systemy zaplecza, które uwierzytelniają się kluczem prywatnym odpowiadającym certyfikatowi z białej listy. W bramie sieciowej będzie wykorzystywany także certyfikat TLS, który umożliwi krajowym systemom zaplecza weryfikację, czy rzeczywiście ustanawiają połączenie z prawdziwą bramą sieciową, a nie z jakimś złośliwym podmiotem podszywającym się pod tę bramę. Po udanej rejestracji krajowy system zaplecza otrzyma certyfikat bramy sieciowej. Certyfikat $DCCG_{TLS}$ wyda publicznie zaufane centrum certyfikacji (dostępne we wszystkich głównych przeglądarkach internetowych). Obowiązkiem państw członkowskich jest zweryfikowanie, czy ich połączenie z bramą sieciową jest bezpieczne (np. poprzez sprawdzenie zgodności cyfrowego odcisku palca certyfikatu serwera $DCCG_{TLS}$, z którym nawiązano połączenie, z certyfikatem otrzymanym po rejestracji).

3.2. *Krajowe centra certyfikacji dla podpisujących i model walidacji*

Państwa członkowskie uczestniczące w ramach bramy sieciowej muszą korzystać z krajowego centrum certyfikacji dla podpisujących do celów wydawania certyfikatów dla podpisujących dokumenty. Państwa członkowskie mogą posiadać więcej niż jedno takie centrum, np. w przypadku decentralizacji regionalnej. Każde państwo członkowskie może wykorzystywać istniejące centra certyfikacji albo utworzyć specjalne centrum certyfikacji (ewentualnie z podpisem własnym) na potrzeby systemu zaświadczeń COVID.

Państwa członkowskie muszą przedstawić certyfikat(-y) krajowego centrum certyfikacji dla podpisujących operatorowi bramy sieciowej podczas procedury oficjalnej rejestracji. Po udanej rejestracji państwa członkowskiego (*zob. więcej szczegółowych informacji w sekcji 4.1*) operator bramy sieciowej zaktualizuje podpisaną listę zaufania, która zawiera wszystkie certyfikaty krajowych centrów certyfikacji dla podpisujących aktywne w ramach zaświadczeń COVID. Operator bramy sieciowej będzie stosował specjalną parę kluczy asymetrycznych do podpisywania listy zaufania i certyfikatów w środowisku offline. Klucz prywatny nie będzie przechowywany w systemie online bramy sieciowej, tak aby naruszenie bezpieczeństwa systemu online nie umożliwiało atakującemu naruszenia bezpieczeństwa listy zaufania. Podczas procesu rejestracji krajowe systemy zaplecza otrzymają odpowiedni certyfikat kotwicy zaufania $DCCG_{TA}$.

▼B

Państwa członkowskie mogą pobierać listę zaufania z bramy sieciowej na potrzeby swoich procedur weryfikacji. Krajowe centrum certyfikacji dla podpisujących definiuje się jako centrum certyfikacji, które wydaje certyfikaty dla podpisujących dokumenty, w związku z czym państwa członkowskie, które stosują wielopoziomową hierarchię centrów certyfikacji (np. główny urząd certyfikacji -> krajowe centrum certyfikacji dla podpisujących-> certyfikaty dla podpisujących dokumenty), muszą wskazać podrzędne centrum certyfikacji, które wydaje certyfikaty dla podpisujących dokumenty. W takim przypadku jeżeli państwo członkowskie korzysta z istniejącego centrum certyfikacji, w systemie zaświadczeń COVID wszystkie centra certyfikacji poza krajowym centrum certyfikacji dla podpisujących będą ignorowane i tylko to centrum certyfikacji będzie figurowało na białej liście jako kotwica zaufania (mimo że jest to podrzędne centrum certyfikacji). Wynika to z tego, że w modelu ICAO dopuszcza się tylko dwa poziomy – poziom głównego krajowego centrum certyfikacji dla podpisujących i poziom „liścia", tj. certyfikat dla podpisujących dokumenty podpisany przez to właśnie centrum certyfikacji.

W przypadku gdy państwo członkowskie prowadzi własne krajowe centrum certyfikacji dla podpisujących, państwo to jest odpowiedzialne za bezpieczne funkcjonowanie tego centrum i zarządzanie jego kluczami. Krajowe centrum certyfikacji dla podpisujących pełni funkcję kotwicy zaufania w odniesieniu do certyfikatów dla podpisujących dokumenty, w związku z czym ochrona klucza prywatnego tego centrum ma zasadnicze znaczenie dla integralności środowiska zaświadczeń COVID. Modelem weryfikacji w infrastrukturze klucza publicznego zaświadczeń COVID jest model zagnieżdżony, który stanowi, że wszystkie certyfikaty w ścieżce walidacji certyfikatów muszą być ważne w danym momencie (tj. w momencie walidacji podpisu). W związku z tym zastosowanie mają następujące ograniczenia:

— krajowe centrum certyfikacji dla podpisujących nie może wydawać certyfikatów, które są ważne dłużej niż certyfikat samego centrum certyfikacji;

— podpisujący dokument nie może podpisywać dokumentów, które są ważne dłużej niż sam certyfikat dla podpisujących dokumenty;

— państwa członkowskie, które prowadzą własne krajowe centrum certyfikacji dla podpisujących, muszą określić okresy ważności dla tego centrum certyfikacji i wszystkich wydawanych certyfikatów oraz muszą zadbać o przedłużanie ważności certyfikatów.

Sekcja 4.2 zawiera zalecenia dotyczące okresów ważności.

3.3. *Integralność i autentyczność wysłanych danych*

Po udanym uwierzytelnieniu wzajemnym krajowe systemy zaplecza mogą wykorzystywać bramę sieciową, by wysyłać i pobierać podpisane cyfrowo pakiety danych. Na początku te pakiety danych zawierają certyfikaty państw członkowskich dla podpisujących dokumenty. Para kluczy, której krajowy system zaplecza używa do podpisu cyfrowego wysyłanych pakietów danych w systemie bramy sieciowej, jest nazywana parą kluczy do podpisu danych wysyłanych przez krajowy system zaplecza, a odpowiadający jej certyfikat klucza publicznego nazywa się w skrócie certyfikatem NB_{UP}. Każde państwo członkowskie posiada własny certyfikat NB_{UP}, który może być certyfikatem z podpisem własnym lub certyfikatem wydanym przez istniejące centrum certyfikacji, takie jak publiczne centrum certyfikacji (tj. centrum certyfikacji, które wydaje certyfikaty zgodnie z podstawowymi wymogami CA/Browser Forum). Certyfikat NB_{UP} musi różnić się do wszelkich innych certyfikatów, których używa państwo członkowskie (tj. certyfikatu krajowego centrum certyfikacji dla podpisujących, certyfikatu klienta TLS lub certyfikatu dla podpisujących dokumenty).

Państwa członkowskie muszą dostarczyć certyfikat wysyłania danych operatorowi bramy sieciowej podczas procedury pierwszej rejestracji (*zob. więcej szczegółowych informacji w sekcji 4.1*). Każde państwo członkowskie jest odpowiedzialne za swoje dane krajowe i musi chronić klucz prywatny, którego używa się do podpisywania wysyłanych danych.

Inne państwa członkowskie mogą zweryfikować podpisane pakiety danych za pomocą certyfikatów wysyłania danych, których to certyfikatów dostarcza brama sieciowa. Brama sieciowa weryfikuje autentyczność i integralność wysłanych danych za pomocą certyfikatu wysyłania danych krajowego systemu zaplecza, zanim zostaną one udostępnione innym państwom członkowskim.

▼B

3.4. *Wymogi dotyczące architektury technicznej bramy sieciowej*

Wymogi dotyczące architektury technicznej bramy sieciowej są następujące:

— brama sieciowa stosuje TLS z uwierzytelnianiem wzajemnym w celu ustanowienia uwierzytelnionego szyfrowanego połączenia z krajowymi systemami zaplecza. W związku z tym w bramie sieciowej prowadzi się białą listę zarejestrowanych certyfikatów klienta NB_{TLS};

— brama sieciowa wykorzystuje dwa certyfikaty cyfrowe ($DCCG_{TLS}$ i $DCCG_{TA}$) z dwiema różnymi parami kluczy. Klucz prywatny pary kluczy $DCCG_{TA}$ jest przechowywany offline (nie na elementach bramy sieciowej znajdujących się online);

— w bramie sieciowej prowadzi się listę zaufania certyfikatów NB_{CSCA}, która jest podpisana kluczem prywatnym $DCCG_{TA}$;

— stosowane szyfry muszą spełniać wymogi określone w *sekcji 5.1*.

4. **Zarządzanie cyklem życia certyfikatu**

4.1. *Rejestracja krajowych systemów zaplecza*

Państwa członkowskie muszą się zarejestrować u operatora bramy sieciowej, aby uczestniczyć w systemie bramy sieciowej. W niniejszej sekcji opisano procedurę techniczną i operacyjną, której trzeba dopełnić w celu zarejestrowania krajowego systemu zaplecza.

W celu przeprowadzenia procesu rejestracji operator bramy sieciowej i państwo członkowskie muszą wymienić się informacjami na temat osób wyznaczonych do kontaktów w sprawach technicznych. Zakłada się, że osoby te posiadają uprawnienia przyznane przez państwa członkowskie, a identyfikacja/uwierzytelnienie odbywa się innymi kanałami. Na przykład uwierzytelnienie może polegać na tym, że osoba wyznaczona przez dane państwo członkowskie do kontaktów w sprawach technicznych wysyła pocztą elektroniczną certyfikaty jako pliki zaszyfrowane hasłem, a hasło przekazuje operatorowi bramy sieciowej drogą telefoniczną. Można wykorzystać również inne bezpieczne kanały określone przez operatora bramy sieciowej.

W trakcie procesu rejestracji i identyfikacji państwa członkowskie muszą dostarczyć trzy certyfikaty cyfrowe:

— certyfikat TLS państwa członkowskiego NB_{TLS};

— certyfikat wysyłania danych państwa członkowskiego NB_{UP};

— certyfikat(-y) krajowego centrum certyfikacji dla podpisujących państwa członkowskiego NB_{CSCA}.

Wszystkie dostarczone certyfikaty muszą spełniać wymogi określone w *sekcji 5*. Operator bramy sieciowej zweryfikuje, czy przekazane certyfikaty spełniają wymogi określone w *sekcji 5*. Po identyfikacji i rejestracji operator bramy sieciowej:

— dodaje certyfikat(-y) NB_{CSCA} do listy zaufania podpisanej kluczem prywatnym, który odpowiada kluczowi publicznemu $DCCG_{TA}$;

— dodaje certyfikat NB_{TLS} do białej listy punktu końcowego DCCG TLS;

— dodaje certyfikat NB_{UP} do systemu bramy sieciowej;

— dostarcza państwu członkowskiemu certyfikat klucza publicznego $DCCG_{TA}$ i $DCCG_{TLS}$.

▼B

4.2. *Centra certyfikacji, okresy ważności i przedłużanie ważności*

W przypadku gdy państwo członkowskie chce prowadzić własne krajowe centrum certyfikacji dla podpisujących, certyfikaty krajowego centrum certyfikacji dla podpisujących mogą być certyfikatami z podpisem własnym. Pełnią one funkcję kotwic zaufania państwa członkowskiego, dlatego państwo członkowskie musi solidnie chronić klucz prywatny odpowiadający kluczowi publicznemu certyfikatu krajowego centrum certyfikacji dla podpisujących. Zaleca się, aby państwa członkowskie na potrzeby swojego krajowego centrum certyfikacji dla podpisujących korzystały z systemu offline, tj. z systemu komputerowego, który nie jest podłączony do żadnej sieci. W celu uzyskiwania dostępu do systemu stosuje się kontrolę wieloosobową (np. zgodnie z zasadą „czworga oczu"). Po podpisaniu certyfikatów dla podpisujących dokumenty stosuje się kontrole operacyjne, a system, w którym znajduje się klucz prywatny krajowego centrum certyfikacji dla podpisujących, przechowuje się w bezpiecznym miejscu ze ścisłą kontrolą dostępu. Do celów lepszej ochrony klucza prywatnego krajowego centrum certyfikacji dla podpisujących można wykorzystać sprzętowe moduły bezpieczeństwa lub karty elektroniczne. Certyfikaty cyfrowe posiadają okres ważności, który zmusza do przedłużania ważności certyfikatu. Przedłużanie ważności jest konieczne, żeby korzystać z nowych kluczy kryptograficznych i dostosować wielkość klucza, w przypadku gdy nowe usprawnienia obliczeń lub nowe ataki zagrażają bezpieczeństwu stosowanego algorytmu kryptograficznego. Zastosowanie ma model zagnieżdżony (ang. *shell model*) (zob. *sekcja 3.2*).

Z uwagi na jednoroczny okres ważności cyfrowych zaświadczeń COVID zaleca się następujące okresy ważności:

— krajowe centrum certyfikacji dla podpisujących: 4 lata;

— certyfikat dla podpisujących dokumenty: 2 lata;

— certyfikat wysyłania danych: 1–2 lata;

— certyfikat uwierzytelniania klienta TLS: 1–2 lata.

Na potrzeby terminowego przedłużania ważności zaleca się następujące okresy użytkowania kluczy prywatnych:

— krajowe centrum certyfikacji dla podpisujących: 1 rok;

— certyfikat dla podpisujących dokumenty: 6 miesięcy.

Aby zapewnić sprawne działanie, państwa członkowskie muszą tworzyć nowe certyfikaty wysyłania danych i certyfikaty TLS terminowo, np. na miesiąc przed wygaśnięciem. Ważność certyfikatów krajowego centrum certyfikacji dla podpisujących i certyfikatów dla podpisujących dokumenty należy przedłużać co najmniej na miesiąc przed upływem terminu użytkowania klucza prywatnego (biorąc pod uwagę niezbędne procedury operacyjne). Państwa członkowskie muszą dostarczyć operatorowi bramy sieciowej zaktualizowane certyfikaty: certyfikat krajowego centrum certyfikacji dla podpisujących, certyfikat wysyłania danych i certyfikat TLS. Certyfikaty, które utraciły ważność, usuwa się z białej listy i listy zaufania.

Państwa członkowskie i operator bramy sieciowej muszą monitorować ważność swoich certyfikatów. Nie istnieje żaden podmiot centralny, który prowadzi rejestr ważności certyfikatów i przekazuje uczestnikom informacje na ten temat.

▼B

4.3. *Unieważnianie certyfikatów*

Ogólnie rzecz biorąc, certyfikaty cyfrowe może unieważniać wydający je organ certyfikacji, wykorzystując w tym celu listy unieważnionych certyfikatów lub usługę respondera OCSP (ang. *online certificate status protocol*). Na potrzeby systemu zaświadczeń COVID krajowe centra certyfikacji dla podpisujących powinny udostępniać listy unieważnionych certyfikatów. Nawet jeśli inne państwa członkowskie nie korzystają obecnie z tych list unieważnionych certyfikatów, należy zintegrować te listy na potrzeby przyszłych zastosowań. W przypadku gdy krajowe centrum certyfikacji dla podpisujących postanowi nie udostępniać list unieważnionych certyfikatów, należy przedłużyć okres ważności certyfikatów dla podpisujących dokumenty wydanych przez to krajowe centrum certyfikacji, kiedy listy te staną się obowiązkowe. Do walidacji certyfikatów dla podpisujących dokumenty weryfikatorzy powinni korzystać nie z OCSP, a z list unieważnionych certyfikatów. Zaleca się, aby krajowy system zaplecza przeprowadzał niezbędną walidację certyfikatów dla podpisujących dokumenty pobranych z bramy sieciowej zaświadczeń COVID i przekazywał krajowym walidatorom zaświadczeń COVID jedynie zestaw zaufanych i zwalidowanych certyfikatów dla podpisujących dokumenty. W ramach procesu walidacji walidatorzy zaświadczeń COVID nie powinni w odniesieniu do certyfikatów dla podpisujących dokumenty sprawdzać, czy doszło do unieważnienia. Jednym z powodów jest ochrona prywatności posiadaczy zaświadczeń COVID przez unikanie ryzyka, że usługa respondera OCSP umożliwia monitorowanie posługiwania się jakimkolwiek konkretnym certyfikatem dla podpisujących dokumenty.

Państwa członkowskie mogą samodzielnie usuwać swoje certyfikaty dla podpisujących dokumenty z bramy sieciowej, korzystając z ważnych certyfikatów wysyłania danych i certyfikatów TLS. Usunięcie certyfikatu dla podpisujących dokumenty oznacza, że zaświadczenia COVID wydane z wykorzystaniem tego certyfikatu staną się nieważne, w momencie gdy państwa członkowskie pobiorą zaktualizowane listy certyfikatów dla podpisujących dokumenty. Kluczowe znaczenie ma ochrona klucza prywatnego odpowiadającego certyfikatom dla podpisujących dokumenty. W przypadku gdy państwa członkowskie są zmuszone unieważnić certyfikat wysyłania danych lub certyfikat TLS, np. wskutek naruszenia bezpieczeństwa krajowego systemu zaplecza, muszą poinformować o tym operatora bramy sieciowej Operator bramy sieciowej może wówczas cofnąć zaufanie do danego certyfikatu, np. usuwając go z białej listy TLS. Operator bramy sieciowej może usunąć certyfikaty wysyłania danych z bazy danych bramy sieciowej. Pakiety podpisane przy użyciu klucza prywatnego odpowiadającego temu certyfikatowi wysyłania danych staną się nieważne, gdy krajowy system zaplecza cofnie zaufanie w odniesieniu do unieważnionego certyfikatu. W przypadku gdy konieczne jest unieważnienie certyfikatu krajowego centrum certyfikacji dla podpisujących, państwa członkowskie informują o tym operatora bramy sieciowej, jak również pozostałe państwa członkowskie, z którymi utrzymują relacje zaufania. Operator bramy sieciowej wyda nową listę zaufania, która nie będzie już zawierała unieważnionych certyfikatów. Wszystkie certyfikaty dla podpisujących dokumenty wydane przez to krajowe centrum certyfikacji dla podpisujących staną się nieważne, gdy państwa członkowskie zaktualizują magazyny zaufania krajowego systemu zaplecza. W przypadku gdy konieczne jest unieważnienie certyfikatu $DCCG_{TLS}$ lub $DCCG_{TA}$, operator bramy sieciowej i państwa członkowskie muszą współpracować, by ustanowić nowe zaufane połączenie z serwerem TLS i nową listę zaufania.

5. **Szablony certyfikatów**

W niniejszej sekcji określono wymogi i wytyczne kryptograficzne, a także wymogi dotyczące szablonów certyfikatów. Określono w niej również szablony certyfikatów w odniesieniu do certyfikatów bramy sieciowej.

5.1. *Wymogi kryptograficzne*

Algorytmy kryptograficzne i mechanizmy szyfrowania TLS wybiera się na podstawie aktualnego zalecenia niemieckiego Urzędu Federalnego ds. Bezpieczeństwa Informacji (BSI) lub SOG-IS. Zalecenia te i zalecenia innych instytucji i organizacji normalizacyjnych są podobne. Zalecenia te można znaleźć w wytycznych technicznych TR 02102-1 i TR 02102-2 ([1]) lub w uzgodnionych mechanizmach kryptograficznych SOG-IS ([2]).

([1]) BSI – Wytyczne techniczne TR-02102 (bund.de).
([2]) SOG-IS – Dokumenty potwierdzające (sogis.eu)

▼B

5.1.1. Wymogi dotyczące certyfikatu dla podpisujących dokumenty

Zastosowanie mają wymogi przewidziane w *załączniku I sekcja 3.2.2*. W związku z tym zdecydowanie zaleca się, aby podpisujący dokumenty stosowali algorytm podpisu cyfrowego krzywej eliptycznej (ECDSA) z NIST-p-256 (zdefiniowany w dodatku D do FIPS PUB 186-4). Inne krzywe eliptyczne nie są obsługiwane. Ze względu na ograniczone miejsce w zaświadczeniu COVID państwa członkowskie nie powinny stosować schematu RSA-PSS, nawet jeśli jest on dozwolony jako algorytm rezerwowy. W przypadku gdy państwa członkowskie stosują RSA-PSS, powinny stosować rozmiar modułu wynoszący 2048 bitów lub maksymalnie 3072 bity. SHA-2 o długości wyjściowej ≥ 256 bitów stosuje się jako kryptograficzną funkcję skrótu (zob. ISO/IEC 10118-3:2004) w odniesieniu do podpisu certyfikatu dla podpisujących dokumenty.

5.1.2. Wymogi dotyczące certyfikatu TLS, certyfikatu wysyłania danych i certyfikatu krajowego centrum certyfikacji dla podpisujących

W poniższej tabeli podsumowano główne wymogi dotyczące algorytmów kryptograficznych i długości klucza w przypadku certyfikatów cyfrowych i podpisów kryptograficznych w kontekście bramy sieciowej (stan na 2021 r.):

Algorytm podpisu	Wielkość klucza	Funkcja skrótu
ECDSA	Min. 250 bitów	SHA-2 o długości wyjściowej ≥ 256 Bit
RSA-PSS (wypełnienie zalecane) RSA-PKCS#1 v1.5 (wypełnienie starsze)	Min. 3000-bitowy moduł RSA (N) z wykładnikiem publicznym e > 2^16	SHA-2 o długości wyjściowej ≥ 256 Bit
DSA	Min. 3000-bitowa liczba pierwsza p, 250-bitowy klucz q	SHA-2 o długości wyjściowej ≥ 256 Bit

Zalecaną krzywą eliptyczną dla ECDSA jest NIST-p-256 ze względu na jej powszechne stosowanie.

5.2. *Certyfikat krajowego centrum certyfikacji dla podpisujących (NB_{CSCA})*

W poniższej tabeli przedstawiono wytyczne dotyczące szablonu certyfikatu NB_{CSCA}, w przypadku gdy państwo członkowskie postanowi prowadzić własne krajowe centrum certyfikacji dla podpisujących na potrzeby systemu zaświadczeń COVID.

Pozycje **pogrubione** są wymagane (muszą znajdować się w certyfikacie), pozycje *kursywą* są zalecane (powinny znajdować się w certyfikacie). W przypadku nieobecnych pól nie określono żadnych zaleceń.

Pole	Wartość
Podmiot	**cn=<niepusta i niepowtarzalna nazwa pospolita,***o=<dostawca>*, **c=<państwo członkowskie prowadzące krajowe centrum certyfikacji dla podpisujących>**
Użytkowanie klucza	**podpisywanie certyfikatu,***podpisywanie listy unieważnionych certyfikatów* (co najmniej)
Podstawowe ograniczenia	**Centrum certyfikacji = prawda, ograniczenia długości ścieżki = 0**

Nazwa podmiotu nie może być pusta i musi być niepowtarzalna w danym państwie członkowskim. Kod państwa (c) musi odpowiadać państwu członkowskiemu, które będzie korzystało z tego certyfikatu krajowego centrum certyfikacji dla podpisujących. Certyfikat musi zawierać niepowtarzalny identyfikator klucza podmiotu (ang. *subject key identifier*, SKI) zgodny z RFC 5280 ([1]).

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

▼B

5.3. *Certyfikat dla podpisujących dokumenty (DSC)*

Poniższa tabela zawiera wytyczne dotyczące certyfikatu dla podpisujących dokumenty. Pozycje **pogrubione** są wymagane (muszą znajdować się w certyfikacie), pozycje *kursywą* są zalecane (powinny znajdować się w certyfikacie). W przypadku nieobecnych pól nie określono żadnych zaleceń.

Pole	Wartość
Numer seryjny	**niepowtarzalny numer seryjny**
Podmiot	**cn=<niepusta i niepowtarzalna nazwa pospolita**, *o=<dostawca>*, **c=<państwo członkowskie używające tego certyfikatu dla podpisujących dokumenty>**
Użytkowanie klucza	**podpis cyfrowy** (co najmniej)

Certyfikat dla podpisujących dokumenty musi być podpisany kluczem prywatnym odpowiadającym certyfikatowi krajowego centrum certyfikacji dla podpisujących używanemu przez państwo członkowskie.

Należy stosować następujące rozszerzenia:

— Certyfikat musi zawierać identyfikator klucza centrum certyfikacji (ang. *authority key identifier*, AKI) odpowiadający identyfikatorowi klucza podmiotu z certyfikatu krajowego centrum certyfikacji dla podpisujących wydającego certyfikat.

— Certyfikat powinien zawierać niepowtarzalny identyfikator klucza podmiotu (zgodnie z RFC 5280 ([1])).

Ponadto świadectwo powinno zawierać rozszerzenie punktu dystrybucji listy unieważnionych certyfikatów wskazujące listę unieważnionych certyfikatów dostarczaną przez krajowe centrum certyfikacji dla podpisujących, które wydało certyfikat dla podpisujących dokumenty.

Certyfikat dla podpisujących dokumenty może zawierać rozszerzenie użytkowania klucza o zero lub więcej identyfikatorów zasad użytkowania klucza ograniczających rodzaje HCERT, które ten certyfikat może weryfikować. Jeżeli występuje co najmniej jeden identyfikator, weryfikatorzy sprawdzają użytkowania klucza w odniesieniu do przechowywanego HCERT. W tym celu zdefiniowano następujące wartości extendedKeyUsage:

Pole	Wartość
extendedKeyUsage	1.3.6.1.4.1.1847.2021.1.1 w przypadku wystawców zaświadczeń o wyniku testu
extendedKeyUsage	1.3.6.1.4.1.1847.2021.1.2 w przypadku wystawców zaświadczeń o szczepieniu
extendedKeyUsage	1.3.6.1.4.1.1847.2021.1.3 w przypadku wystawców zaświadczeń o powrocie do zdrowia

W przypadku braku jakiegokolwiek rozszerzenia użytkowania klucza (tj. braku rozszerzeń lub zerowych rozszerzeń) certyfikat ten można stosować do walidacji dowolnego rodzaju HCERT. Inne dokumenty mogą zawierać zdefiniowane odpowiednie dodatkowe rozszerzone identyfikatory zasad użytkowania klucza stosowane przy walidacji HCERT.

5.4. *Certyfikaty wysyłania danych (NBUP)*

Poniższa tabela zawiera wytyczne dotyczące certyfikatu wysyłania danych krajowego systemu zaplecza. Pozycje **pogrubione** są wymagane (muszą znajdować się w certyfikacie), pozycje *kursywą* są zalecane (powinny znajdować się w certyfikacie). W przypadku nieobecnych pól nie określono żadnych zaleceń.

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

▼B

Pole	Wartość
Podmiot	**cn=<niepusta i niepowtarzalna nazwa pospolita>**, *o=<dostawca>*, **c=<państwo członkowskie używającego tego certyfikatu wysyłania danych>**
Użytkowanie klucza	**podpis cyfrowy** (co najmniej)

5.5. *Certyfikat uwierzytelniania klienta TLS krajowego systemu zaplecza (NB_{TLS})*

Poniższa tabela zawiera wytyczne dotyczące certyfikatu uwierzytelniania klienta TLS krajowego systemu zaplecza. Pozycje **pogrubione** są wymagane (muszą znajdować się w certyfikacie), pozycje *kursywą* są zalecane (powinny znajdować się w certyfikacie). W przypadku nieobecnych pól nie określono żadnych zaleceń.

Pole	Wartość
Podmiot	**cn=<niepusta i niepowtarzalna nazwa pospolita>**, *o=<dostawca>*, **c=<państwo członkowskie krajowego systemu zaplecza>**
Użytkowanie klucza	**podpis cyfrowy** (co najmniej)
Rozszerzone użytkowanie klucza	uwierzytelnianie klienta (1.3.6.1.5.5.7.3.2)

Certyfikat może również zawierać *uwierzytelnienie serwera (1.3.6.1.5.5.7.3.1)* rozszerzonego użytkowania klucza, lecz nie jest to wymagane.

5.6. *Certyfikat podpisu listy zaufania ($DCCG_{TA}$)*

W poniższej tabeli zdefiniowano certyfikat kotwicy zaufania bramy sieciowej.

Pole	Wartość
Podmiot	**cn = brama sieciowa zielonych zaświadczeń cyfrowych** ([1])**, o=<dostawca>, c=<państwo>**
Użytkowanie klucza	**podpis cyfrowy** (co najmniej)

5.7. *Certyfikaty serwera TLS bramy sieciowej ($DCCG_{TLS}$)*

W poniższej tabeli zdefiniowano certyfikat TLS bramy sieciowej.

Pole	Wartość
Podmiot	cn=<nazwa FQDN lub adres IP bramy sieciowej>, o=<dostawca>, c= <państwo>
SubjectAltName	dNSName: <nazwa DNS bramy sieciowej> lub iPAddress: <adres IP bramy sieciowej>
Użytkowanie klucza	**podpis cyfrowy** (co najmniej)
Rozszerzone użytkowanie klucza	uwierzytelnianie serwera (1.3.6.1.5.5.7.3.1)

([1]) W tym kontekście zachowano termin „zielone zaświadczenie cyfrowe” zamiast „unijne cyfrowe zaświadczenie COVID”, ponieważ termin ten na stałe zapisano i zastosowano w certyfikacie, zanim współprawodawcy zdecydowali się na nowy termin.

▼B

Certyfikat może również zawierać *uwierzytelnienie serwera (1.3.6.1.5.5.7.3.2)* rozszerzonego użytkowania klucza, lecz nie jest to wymagane.

Certyfikat TLS bramy sieciowej wydaje publicznie zaufane centrum certyfikacji (dostępne we wszystkich głównych przeglądarkach i systemach operacyjnych, spełniające podstawowe wymogi CA/Browser Forum).

▼M1

ZAŁĄCZNIK V

SCHEMAT JSON

1. **Wprowadzenie**

Niniejszy załącznik ustanawia techniczną strukturę danych na potrzeby unijnych cyfrowych zaświadczeń COVID, przedstawioną w postaci schematu JSON. Dokument zawiera szczegółowe instrukcje dotyczące poszczególnych pól danych.

2. **Lokalizacja i wersje schematu JSON**

Miarodajny schemat JSON dla unijnych cyfrowych zaświadczeń COVID jest dostępny pod adresem https://github.com/ehn-dcc-development/ehn-dcc-schema. Inne lokalizacje nie są miarodajne, ale mogą być wykorzystywane do przygotowania przyszłych zmian.

Domyślnie aktualna wersja określona w niniejszym załączniku i stosowana przez wszystkie państwa obecnie wydające zaświadczenia jest widoczna pod wskazanym adresem URL.

Kolejna wersja, która ma być stosowana w wyznaczonym terminie przez wszystkie państwa, jest widoczna pod wskazanym adresem URL przy użyciu znakowania wersji, co zostało opisane bardziej szczegółowo w pliku Readme.

▼M3

3. **Wspólne struktury i wymagania ogólne**

Nie wydaje się unijnego cyfrowego zaświadczenia COVID, jeżeli ze względu na brakujące informacje nie wszystkie pola danych można prawidłowo wypełnić zgodnie z niniejszą specyfikacją. **Powyższego nie należy interpretować jako wpływającego na obowiązek państw członkowskich w zakresie wydawania unijnych cyfrowych zaświadczeń COVID.**

Informacje we wszystkich polach można podawać przy użyciu pełnego zestawu znaków UNICODE 13.0 zakodowanych przy użyciu UTF-8, chyba że znaki te wyraźnie ograniczają się do zestawów wartości lub węższych zestawów znaków.

Wspólna struktura jest następująca:

„JSON”:{

„ver”:<informacje dotyczące wersji>,

„nam”:{

<informacje dotyczące imienia i nazwiska osoby>

},

„dob”:<data urodzenia>,

„v” lub „t” lub „r”:[

{<dawka szczepionki lub informacja o badaniu lub powrocie do zdrowia, jeden wpis>}

]

}

Szczegółowe informacje na temat poszczególnych kategorii i pól przedstawiono w kolejnych sekcjach.

W przypadku gdy przepisy wskazują, że pole powinno zostać pominięte, oznacza to, że jego zawartość musi być pusta i że ani nazwa, ani wartość pola nie są dozwolone w treści.

▼M3

3.1. *Wersja*

Należy podać informacje na temat wersji. Zapisywanie wersji następuje zgodnie z wersjonowaniem semantycznym (ang. Semantic Versioning) (semver: https://semver.org). W czasie wydawania zaświadczenia powinna to być jedna z oficjalnie opublikowanych wersji (aktualna lub jedna ze starszych oficjalnie opublikowanych wersji). Więcej informacji na ten temat znajduje się w sekcji dotyczącej lokalizacji schematu JSON (ang. JSON Schema).

ID pola	Nazwa pola	Instrukcje
ver	Wersja schematu	Odpowiada identyfikatorowi wersji schematu wykorzystywanej na potrzeby sporządzania unijnych cyfrowych zaświadczeń COVID-19. Przykład: „ver”:„1.3.0”

3.2. *Imię i nazwisko oraz data urodzenia osoby*

Imię i nazwisko osoby to oficjalne pełne imię i nazwisko osoby, odpowiadające imieniu i nazwisku podanym w dokumentach podróży. Identyfikatorem struktury jest *nam*. Należy podać imię i nazwisko dokładnie 1 (jednej) osoby.

ID pola	Nazwa pola	Instrukcje
nam/fn	Nazwisko(-a)	Nazwisko(-a) posiadacza. Jeżeli posiadacz nie ma nazwiska, a ma imię, pole należy pominąć. We wszystkich pozostałych przypadkach należy podać dokładnie 1 (jedno) pole, które nie jest puste, zawierające wszystkie nazwiska. W przypadku kilku nazwisk należy je oddzielić spacją. Nazwiska wieloczłonowe zawierające łączniki lub podobne znaki muszą jednak pozostać niezmienione. Przykłady: „fn”:„Musterfrau-Gößinger” „fn”:„Musterfrau-Gößinger Müller”
nam/fnt	Znormalizowane nazwisko(-a)	Nazwisko(-a) posiadacza transliterowane przy zastosowaniu tej samej konwencji jak konwencja stosowana w dokumentach podróży posiadacza odczytywanych maszynowo (np. zasady określone w ICAO Doc 9303 część 3). Jeżeli posiadacz nie ma nazwiska, a ma imię, pole należy pominąć. We wszystkich pozostałych przypadkach należy podać dokładnie 1 (jedno) pole, które nie jest puste, zawierające wyłącznie znaki A-Z i <. Maksymalna długość: 80 znaków (zgodnie ze specyfikacją ICAO 9303). Przykłady: „fnt”:„MUSTERFRAU<GOESSINGER” „fnt”:„MUSTERFRAU<GOESSINGER<MUELLER”
nam/gn	Imię(-ona)	Imię(-ona) posiadacza. Jeżeli posiadacz nie ma imienia, a ma nazwisko, pole należy pominąć. We wszystkich pozostałych przypadkach należy podać dokładnie 1 (jedno) pole, które nie jest puste, zawierające wszystkie imiona. W przypadku kilku imion należy je oddzielić spacją. Przykład: „gn”:„Isolde Erika”

▼M3

ID pola	Nazwa pola	Instrukcje
nam/gnt	Znormalizowane imię(-ona)	Imię(-ona) posiadacza transliterowane przy zastosowaniu tej samej konwencji jak konwencja stosowana w dokumentach podróży posiadacza odczytywanych maszynowo (np. zasady określone w ICAO Doc 9303 część 3). Jeżeli posiadacz nie ma imienia, a ma nazwisko, pole należy pominąć. We wszystkich pozostałych przypadkach należy podać dokładnie 1 (jedno) pole, które nie jest puste, zawierające wyłącznie znaki A-Z i <. Maksymalna długość: 80 znaków. Przykład: „gnt":„ISOLDE<ERIKA"
dob	Data urodzenia	Data urodzenia posiadacza cyfrowego zaświadczenia COVID (DCC) Pełna lub częściowa data bez godziny w przedziale od 1900-01-01 do 2099-12-31. Jeżeli znana jest pełna lub częściowa data urodzenia, należy podać dokładnie 1 (jedno) pole, które nie jest puste. „Jeżeli data urodzenia nie jest znana nawet częściowo, pole ustawia się jako pusty ciąg ". Powyższe powinno odpowiadać informacjom podanym w dokumentach podróży. Jeżeli dostępne są informacje o dacie urodzenia, stosuje się jeden z poniższych formatów ISO 8601. Inne formaty nie są obsługiwane. YYYY-MM-DD YYYY-MM YYYY (Aplikacja weryfikatora może wykazywać brakujące części daty urodzenia przy zastosowaniu konwencji XX takiej jak konwencja stosowana w dokumentach podróży odczytywanych maszynowo, np. 1990-XX–XX.) Przykłady: „dob":„1979-04-14" „dob":„901-08" „dob":„1939" „dob":„"

3.3. *Kategorie informacji specyficznych dla danego typu zaświadczenia*

W schemacie JSON obsługiwane są trzy kategorie pozycji obejmujące informacje specyficzne dla danego typu zaświadczenia. Każde unijne cyfrowe zaświadczenie COVID-19 zawiera dokładnie 1 (jedną) kategorię. Puste kategorie nie są dozwolone.

Identyfikator kategorii	Nazwa kategorii	Pozycje
v	Kategoria „szczepienie"	Jeżeli występuje, musi zawierać dokładnie 1 (jedną) pozycję opisującą dokładnie 1 (jedną) dawkę szczepionki (jedną dawkę).
t	Kategoria „test"	Jeżeli występuje, musi zawierać dokładnie 1 (jedną) pozycję opisującą dokładnie 1 (jeden) wynik testu.
r	Kategoria „powrót do zdrowia"	Jeżeli występuje, musi zawierać dokładnie 1 (jedną) pozycję zawierającą 1 (jedno) oświadczenie dotyczące powrotu do zdrowia.

▼M1

4. **Informacje specyficzne dla danego typu zaświadczenia**

4.1. *Zaświadczenie o szczepieniu*

Kategoria „szczepienie", jeżeli występuje, musi zawierać dokładnie 1 (jedną) pozycję opisującą dokładnie jedno szczepienie (jedną dawkę). Wszystkie elementy kategorii „szczepienia" są obowiązkowe, puste wartości nie są obsługiwane.

▼M1

ID pola	Nazwa pola	Instrukcje
v/tg	Choroba lub czynnik chorobotwórczy, której/którego dotyczy szczepienie: COVID-19 (SARS-CoV-2 lub jeden z jego wariantów)	Wartość kodowana z zestawu wartości disease-agent-targeted.json. Ten zestaw wartości ma pojedynczy kod 840539006, który jest kodem dla COVID-19 z SNOMED CT (GPS). Należy podać dokładnie 1 (jedno) pole, które nie jest puste. Przykład: "tg": "840539006"
v/vp	Szczepionka przeciwko COVID-19 lub profilaktyka COVID-19	Rodzaj zastosowanej szczepionki lub profilaktyki. Wartość kodowana z zestawu wartości vaccine-prophylaxis.json. Zestaw wartości jest dystrybuowany z bramy sieciowej unijnych cyfrowych zaświadczeń COVID. Należy podać dokładnie 1 (jedno) pole, które nie jest puste. Przykład: "vp": "1119349007" (szczepionka zawierająca mRNA SARS-CoV-2)
v/mp	Szczepionka przeciwko COVID-19	Produkt leczniczy zastosowany w ramach tej konkretnej dawki szczepień. ►M4 Wartość kodowana z zestawu wartości vaccine-medicinal-product.json. Lub wartość kodowana odnosząca się do badania klinicznego zgodna z zasadą określoną w sekcji 3 załącznika II. ◄ Zestaw wartości jest dystrybuowany z bramy sieciowej unijnych cyfrowych zaświadczeń COVID. Należy podać dokładnie 1 (jedno) pole, które nie jest puste. Przykład: "mp": „EU/1/20/1528” (Comirnaty)
v/ma	Posiadacz pozwolenia na dopuszczenie do obrotu szczepionki przeciwko COVID-19 lub jej producent	Posiadacz pozwolenia na dopuszczenie do obrotu lub producent, jeżeli nie ma posiadacza pozwolenia na dopuszczenie do obrotu. ►M4 Wartość kodowana z zestawu wartościv vaccine-mah-manf.json. Lub wartość kodowana odnosząca się do badania klinicznego zgodna z zasadą określoną w sekcji 4 załącznika II. ◄ Zestaw wartości jest dystrybuowany z bramy sieciowej unijnych cyfrowych zaświadczeń COVID. Należy podać dokładnie 1 (jedno) pole, które nie jest puste. Przykład: "ma": "ORG-100030215" (przedsiębiorstwo Biontech Manufacturing GmbH)
v/dn	Numer w serii dawek	Numer porządkowy (dodatnia liczba całkowita) dawki podanej podczas tego szczepienia. 1 dla pierwszej dawki, 2 dla drugiej dawki itp. Więcej szczegółowych zasad przedstawiono w sekcji 5 załącznika II. Należy podać dokładnie 1 (jedno) pole, które nie jest puste. Przykłady: "dn": "1" (pierwsza dawka) "dn": "2" (druga dawka) "dn": "3" (trzecia dawka)
v/sd	Łączna liczba dawek w serii	Łączna liczba dawek (dodatnia liczba całkowita) w serii szczepień. Bardziej szczegółowe zasady przedstawiono w sekcji 5 załącznika II. Należy podać dokładnie 1 (jedno) pole, które nie jest puste. Przykłady: "sd": "1" (w przypadku 1-dawkowego cyklu szczepień pierwotnych) "sd": "2" (w przypadku 2-dawkowego cyklu szczepień pierwotnych lub dawki dodatkowej po 1-dawkowym cyklu szczepień pierwotnych) "sd": "3" (np. w przypadku dodatkowych dawek po 2-dawkowym cyklu szczepień pierwotnych)

▼M1

ID pola	Nazwa pola	Instrukcje
v/dt	Data szczepienia	Dzień, w którym otrzymano opisaną dawkę, w formacie RRRR-MM-DD (pełna data bez godziny). Inne formaty nie są obsługiwane. Należy podać dokładnie 1 (jedno) pole, które nie jest puste. Przykład: "dt": "2021-03-28"
v/co	Państwo członkowskie lub państwo trzecie, w którym podano szczepionkę	Państwo wyrażone jako dwuliterowy kod ISO3166 (ZALECANE) lub odniesienie do organizacji międzynarodowej odpowiedzialnej za szczepienie (takiej jak UNHCR lub WHO). Jest to wartość kodowana z zestawu wartości country-2-codes.json. Zestaw wartości jest dystrybuowany z bramy sieciowej unijnych cyfrowych zaświadczeń COVID. Należy podać dokładnie 1 (jedno) pole. Przykład: "co": "CZ" "co": "UNHCR"
v/is	Wystawca zaświadczenia	Nazwa organizacji, która wydała zaświadczenie. Identyfikatory są dozwolone jako część nazwy, ale nie zaleca się ich indywidualnego stosowania bez nazwy w postaci tekstu. Maksymalnie 80 znaków w systemie kodowania UTF-8. Należy podać dokładnie 1 (jedno) pole, które nie jest puste. Przykład: "is": "Ministry of Health of the Czech Republic" "is": "Vaccination Centre South District 3"
v/ci	Niepowtarzalny identyfikator zaświadczenia	Niepowtarzalny identyfikator zaświadczenia, jak określono w dokumencie dostępnym pod adresem https://ec.europa.eu/health/sites/default/files/ehealth/docs/vaccination-proof_interoperability-guidelines_en.pdf Uwzględnienie sumy kontrolnej jest fakultatywne. Można dodać prefiks „URN:UVCI:”. Należy podać dokładnie 1 (jedno) pole, które nie jest puste. Przykłady: "ci": "URN:UVCI:01:NL:187/37512422923" "ci": "URN:UVCI:01:AT:10807843F94AEE0EE5093FBC254BD813#B"

4.2. *Zaświadczenie o wyniku testu*

Kategoria „test”, jeżeli występuje, musi zawierać dokładnie 1 (jedną) pozycję opisującą dokładnie jeden wynik testu.

ID pola	Nazwa pola	Instrukcje
t/tg	Choroba lub czynnik chorobotwórczy, w kierunku której/którego wykonano test: COVID-19 (SARS-CoV-2 lub jeden z jego wariantów)	Wartość kodowana z zestawu wartości disease-agent-targeted.json. Ten zestaw wartości ma pojedynczy kod 840539006, który jest kodem dla COVID-19 z SNOMED CT (GPS). Należy podać dokładnie 1 (jedno) pole, które nie jest puste. Przykład: "tg": "840539006"
t/tt	Rodzaj testu	Rodzaj zastosowanego testu w oparciu o materiał, którego dotyczy test. Wartość kodowana z zestawu wartości test-type.json (w oparciu o LOINC). Wartości spoza zestawu wartości nie są dozwolone. Należy podać dokładnie 1 (jedno) pole, które nie jest puste. Przykład: "tt": "LP6464-4" (Amplifikacja kwasu nukleinowego z sondą detekcyjną) "tt": "LP217198-3" (Szybki test immunologiczny)

▼M1

ID pola	Nazwa pola	Instrukcje
t/nm	Nazwa testu (wyłącznie testy z wykorzystaniem amplifikacji kwasów nukleinowych)	Nazwa użytego testu z wykorzystaniem amplifikacji kwasów nukleinowych (NAAT). Nazwa powinna zawierać nazwę producenta testu oraz nazwę handlową testu, oddzielone przecinkiem. W przypadku testu NAAT: pole jest nieobowiązkowe. ►M4 W przypadku testu antygenowego: nie stosuje się tego pola, ponieważ nazwę testu podaje się pośrednio za pomocą identyfikatora zestawu testu (t/ma). ◄ Jeśli pole jest dostępne, nie może być puste. Przykład: "nm": "ELITechGroup, SARS-CoV-2 ELITe MGB® Kit"

▼M4

t/ma	Identyfikator zestawu testu (tylko testy antygenowe)	Identyfikator zestawu testu antygenowego z bazy danych JRC. Zestaw wartości (wspólny wykaz KBZ): — wszystkie testy antygenowe zawarte we wspólnym wykazie KBZ (informacje w formacie czytelnym dla człowieka); — https://covid-19-diagnostics.jrc.ec.europa.eu/devices/hsc-common-recognition-rat (w formacie nadającym się do przetwarzania automatycznego, id_device odpowiada wartości umieszczonej w wykazie zestawu wartości). W krajach UE/EOG wystawca zaświadczenia wydaje zaświadczenia wyłącznie z tytułu testów należących do obowiązującego zestawu wartości. Zestaw wartości jest aktualizowany co 24 godziny. Wartości spoza zestawu wartości mogą być stosowane w zaświadczeniach wydanych przez państwa trzecie, jednak identyfikatory powinny pochodzić z bazy danych JRC. Stosowanie innych identyfikatorów, takich jak identyfikatory udostępniane bezpośrednio przez producentów testów, nie jest dozwolone. Aplikacje kontrolne muszą wykrywać wartości, które nie należą do aktualnego zestawu wartości, i wyświetlać zaświadczenia zawierające takie wartości jako nieważne. Jeżeli z zestawu wartości usunięto identyfikator, zaświadczenia zawierające taki identyfikator mogą być akceptowane maksymalnie przez 72 godziny od daty usunięcia. Zestaw wartości jest dystrybuowany z bramy sieciowej unijnych cyfrowych zaświadczeń COVID. W przypadku testu antygenowego: należy podać dokładnie 1 (jedno) pole, które nie jest puste. W przypadku testu NAAT: pole to nie jest używane, nawet jeżeli identyfikator testu NAAT jest dostępny w bazie danych JRC. Przykład: „ma”: „344”(SD BIOSENSOR Inc, STANDARD F COVID-19 Ag FIA)

▼M1

t/sc	Data i godzina pobrania próbki do testu	Data i godzina pobrania próbki do testu. Godzina obejmuje informacje na temat strefy czasowej. Wartość nie oznacza godziny uzyskania wyniku testu. Należy podać dokładnie 1 (jedno) pole, które nie jest puste. Stosuje się jeden z następujących formatów ISO 8601. Nie obsługuje się innych wariantów. RRRR-MM-DD hh:mm:ssZ RRRR-MM-DD hh:mm:ss[+-]hhmm

▼M1

ID pola	Nazwa pola	Instrukcje
		RRRR-MM-DD hh:mm:ss[+-]hh:mm RRRR-MM-DD hh:mm:ss[+-]hh:mm Przykłady: "sc": "2021-08-20T10:03:12Z" (czas UTC) "sc": "2021-08-20T12:03:12+02" (czas środkowoeuropejski) "sc": "2021-08-20T12:03:12+0200" (czas środkowoeuropejski) "sc": "2021-08-20T12:03:12+02:00" (czas środkowoeuropejski)
t/tr	Wynik testu	Wynik testu. Wartość kodowana z zestawu wartości test-type.json (w oparciu o SNOMED CT, GPS). Należy podać dokładnie 1 (jedno) pole, które nie jest puste. Przykład: "tr": "260415000" (Nie wykryto)
t/tc	Punkt lub obiekt, w którym wykonano test.	Nazwa podmiotu, który przeprowadził test. Identyfikatory są dozwolone jako część nazwy, ale nie zaleca się ich indywidualnego stosowania bez nazwy w postaci tekstu. Maksymalnie 80 znaków w systemie kodowania UTF-8. Wszelkie dodatkowe znaki należy obciąć. Nazwa nie podlega automatycznej weryfikacji. W przypadku testów NAAT: należy podać dokładnie 1 (jedno) pole, które nie jest puste. ►M4 W przypadku testu antygenowego: pole jest nieobowiązkowe. Jeżeli jest dostępne, nie może być puste. ◄ Przykład: "tc": "Test centre west region 245"
t/co	Państwo członkowskie lub państwo trzecie, w którym wykonano test	Państwo wyrażone jako dwuliterowy kod ISO3166 (ZALECANE) lub odniesienie do organizacji międzynarodowej odpowiedzialnej za wykonanie testu (takiej jak UNHCR lub WHO). Jest to wartość kodowana z zestawu wartości country-2-codes.json Zestaw wartości jest dystrybuowany z bramy sieciowej unijnych cyfrowych zaświadczeń COVID. Należy podać dokładnie 1 (jedno) pole. Przykłady: "co": "CZ" "co": "UNHCR"
t/is	Wystawca zaświadczenia	Nazwa organizacji, która wydała zaświadczenie. Identyfikatory są dozwolone jako część nazwy, ale nie zaleca się ich indywidualnego stosowania bez nazwy w postaci tekstu. Maksymalnie 80 znaków w systemie kodowania UTF-8. Należy podać dokładnie 1 (jedno) pole, które nie jest puste. Przykłady: "is": "Ministry of Health of the Czech Republic" "is": "North-West region health authority"

▼M1

ID pola	Nazwa pola	Instrukcje
t/ci	Niepowtarzalny identyfikator zaświadczenia	Niepowtarzalny identyfikator zaświadczenia, jak określono w vaccination-proof_interoperability-guidelines_en.pdf (europa.eu) Uwzględnienie sumy kontrolnej jest fakultatywne. Można dodać prefiks „URN:UVCI:”. Należy podać dokładnie 1 (jedno) pole, które nie jest puste. Przykłady: "ci": "URN:UVCI:01:NL:187/37512422923" "ci": "URN:UVCI:01:AT:10807843F94AEE0EE5093FBC254BD813#B"

4.3. *Zaświadczenie o powrocie do zdrowia*

Kategoria „powrót do zdrowia”, jeżeli występuje, musi zawierać dokładnie 1 (jedną) pozycję zawierającą dokładnie jedno oświadczenie dotyczące powrotu do zdrowia. Wszystkie elementy kategorii „powrót do zdrowia” są obowiązkowe, puste wartości nie są obsługiwane.

ID pola	Nazwa pola	Instrukcje
r/tg	Choroba lub czynnik chorobotwórczy, po której/którym posiadacz powrócił do zdrowia: COVID-19 (SARS-CoV-2 lub jeden z jego wariantów)	Wartość kodowana z zestawu wartości disease-agent-targeted.json. Ten zestaw wartości ma pojedynczy kod 840539006, który jest kodem dla COVID-19 z SNOMED CT (GPS). Należy podać dokładnie 1 (jedno) pole, które nie jest puste. Przykład: "tg": "840539006"
r/fr	Data pierwszego dodatniego wyniku testu ►M4 ————— ◄ posiadacza	Data pobrania próbki do testu ►M4 ————— ◄, który wykazał wynik dodatni, w formacie RRRR-MM-DD (pełna data bez godziny). Inne formaty nie są obsługiwane. Należy podać dokładnie 1 (jedno) pole, które nie jest puste. Przykład: "fr": "2021-05-18"
r/co	Państwo członkowskie lub państwo trzecie, w którym wykonano test	Państwo wyrażone jako dwuliterowy kod ISO3166 (ZALECANE) lub odniesienie do organizacji międzynarodowej odpowiedzialnej za wykonanie testu (takiej jak UNHCR lub WHO). Jest to wartość kodowana z zestawu wartości country-2-codes.json. Zestaw wartości jest dystrybuowany z bramy sieciowej unijnych cyfrowych zaświadczeń COVID. Należy podać dokładnie 1 (jedno) pole. Przykłady: "co": "CZ" "co": "UNHCR"
r/is	Wystawca zaświadczenia	Nazwa organizacji, która wydała zaświadczenie. Identyfikatory są dozwolone jako część nazwy, ale nie zaleca się ich indywidualnego stosowania bez nazwy w postaci tekstu. Maksymalnie 80 znaków w systemie kodowania UTF-8. Należy podać dokładnie 1 (jedno) pole, które nie jest puste. Przykład: "is": "Ministry of Health of the Czech Republic" "is": "Central University Hospital"

▼**M1**

ID pola	Nazwa pola	Instrukcje
r/df	Zaświadczenie ważne od	Pierwszy dzień, w którym zaświadczenie uznaje się za ważne. Dzień ten nie może przypadać wcześniej od dnia obliczonego według wzoru r/fr + 11 days. Wspomniany dzień podaje się w formacie RRRR-MM-DD (pełna data bez godziny). Inne formaty nie są obsługiwane. Należy podać dokładnie 1 (jedno) pole, które nie jest puste. Przykład: "df": "2021-05-29"
r/du	Zaświadczenie ważne do dnia	Ostatni dzień, w którym zaświadczenie uznaje się za ważne, wyznaczony przez wystawcę zaświadczenia. Dzień ten nie może przypadać później od dnia obliczonego według wzoru r/fr + 180 days. Wspomniany dzień podaje się w formacie RRRR-MM-DD (pełna data bez godziny). Inne formaty nie są obsługiwane. Należy podać dokładnie 1 (jedno) pole, które nie jest puste. Przykład: "du": "2021-11-14"
r/ci	Niepowtarzalny identyfikator zaświadczenia	Niepowtarzalny identyfikator zaświadczenia, jak określono w vaccination-proof_interoperability-guidelines_en.pdf (europa.eu) Uwzględnienie sumy kontrolnej jest fakultatywne. Można dodać prefiks „URN:UVCI:”. Należy podać dokładnie 1 (jedno) pole, które nie jest puste. Przykłady: "ci": "URN:UVCI:01:NL:187/37512422923" "ci": "URN:UVCI:01:AT:10807843F94AEE0EE5093FBC254BD813#B"

▼M3

ZAŁĄCZNIK VI

OBOWIĄZKI PAŃSTW CZŁONKOWSKICH JAKO WSPÓŁADMINISTRATORÓW W ODNIESIENIU DO BRAMY SIECIOWEJ UNIJNEGO CYFROWEGO ZAŚWIADCZENIA COVID NA POTRZEBY WYMIANY LIST UNIEWAŻNIONYCH CERTYFIKATÓW DCC

SEKCJA 1

Podsekcja 1

Podział obowiązków

1) Współadministratorzy przetwarzają dane osobowe za pośrednictwem bramy sieciowej ram zaufania zgodnie ze specyfikacjami technicznymi zawartymi w załączniku I.

2) Organy wydające w państwach członkowskich pozostają jedynym administratorem w zakresie gromadzenia, wykorzystywania, ujawniania i wszelkiego innego przetwarzania informacji o unieważnieniu poza bramą sieciową, w tym w odniesieniu do procedury prowadzącej do unieważnienia zaświadczenia.

3) Każdy administrator odpowiada za przetwarzanie danych osobowych za pośrednictwem bramy sieciowej zgodnie z art. 5, 24 i 26 ogólnego rozporządzenia o ochronie danych.

4) Każdy administrator ustanawia punkt kontaktowy posiadający funkcyjną skrzynkę pocztową, która będzie służyć do komunikacji między samymi współadministratorami oraz między współadministratorami a podmiotem przetwarzającym.

5) Powołana przez komitet grupa robocza, o której mowa w art. 14 rozporządzenia (UE) 2021/953, jest upoważniona do podejmowania decyzji w sprawie wszelkich kwestii wynikających z wymiany list unieważnionych certyfikatów oraz ze współadministrowania powiązanego przetwarzania danych osobowych, a także do ułatwiania skoordynowanych instrukcji dla Komisji jako podmiotu przetwarzającego. Proces podejmowania decyzji przez współadministratorów podlega tej grupie roboczej i regulaminowi, który ma zostać przez nią przyjęty. Podstawową zasadą jest, że brak uczestnictwa przez któregokolwiek ze współadministratorów w posiedzeniu tej grupy roboczej, które zostało ogłoszone co najmniej siedem (7) dni przed jego zwołaniem na piśmie, oznacza milczącą zgodę na wyniki tego posiedzenia grupy roboczej. Każdy ze współadministratorów może zwołać posiedzenie tej grupy roboczej.

6) Instrukcje dla podmiotu przetwarzającego są wysyłane przez punkt kontaktowy któregokolwiek z współadministratorów w porozumieniu z pozostałymi współadministratorami, zgodnie z procesem decyzyjnym grupy roboczej, o którym mowa w pkt 5 powyżej. Współadministrator, który wydaje instrukcje, powinien przekazać je podmiotowi przetwarzającemu na piśmie i poinformować o tym wszystkich pozostałych współadministratorów. Jeżeli omawiana kwestia jest na tyle pilna, że nie pozwala na posiedzenie grupy roboczej, o którym mowa w pkt 5 powyżej, można mimo to wydać instrukcje, ale grupa robocza może je unieważnić. Instrukcje te powinny być wydawane na piśmie, a wszyscy pozostali współadministratorzy powinni być o tym informowani w momencie wydawania instrukcji.

7) Grupa robocza ustanowiona zgodnie z pkt 5 powyżej nie wyklucza indywidualnych kompetencji współadministratorów do informowania swojego właściwego organu nadzorczego zgodnie z art. 33 i 24 ogólnego rozporządzenia o ochronie danych. Takie powiadomienie nie wymaga zgody żadnego z pozostałych współadministratorów.

▼M3

8) W zakresie ram zaufania dostęp do wymienianych danych osobowych mogą mieć wyłącznie osoby upoważnione przez wyznaczone organy krajowe lub organy urzędowe.

9) Każdy organ wydający prowadzi rejestr czynności przetwarzania, za które jest odpowiedzialny. W rejestrze tym można wskazać współadministrację.

Podsekcja 2

Obowiązki i role w zakresie rozpatrywania wniosków osób, których dane dotyczą, oraz w zakresie informowania takich osób

1) Każdy administrator danych pełniący rolę organu wydającego przekazuje osobom fizycznym, których zaświadczenia unieważnił („osoby, których dane dotyczą"), informacje o odnośnym unieważnieniu i przetwarzaniu ich danych osobowych w bramie sieciowej unijnych cyfrowych zaświadczeń COVID w celu wsparcia wymiany list unieważnionych certyfikatów zgodnie z art. 14 ogólnego rozporządzenia o ochronie danych, chyba że okaże się to niemożliwe lub wymaga niewspółmiernie dużego wysiłku.

2) Każdy administrator pełni rolę punktu kontaktowego dla osób fizycznych, których zaświadczenie unieważnił i rozpatruje wnioski składane przez osoby, których dane dotyczą, lub ich przedstawicieli w ramach wykonywania ich praw zgodnie z ogólnym rozporządzeniem o ochronie danych. Jeżeli współadministrator otrzyma od osoby, której dane dotyczą, wniosek dotyczący zaświadczenia wydanego przez innego współadministratora, informuje osobę, której dane dotyczą, o tożsamości i danych kontaktowych tego współadministratora. Jeżeli zostaną o to poproszeni przez innego współadministratora, współadministratorzy pomagają sobie nawzajem w rozpatrywaniu wniosków osób, których dane dotyczą, i udzielają sobie nawzajem odpowiedzi bez zbędnej zwłoki, przy czym nie później niż w terminie jednego miesiąca od otrzymania prośby o udzielenie pomocy. Jeżeli wniosek dotyczy danych przedłożonych przez państwo trzecie, administrator, który otrzymuje wniosek, rozpatruje go i informuje osobę, której dane dotyczą, o tożsamości i danych kontaktowych organu wydającego w państwie trzecim.

3) Każdy administrator udostępnia osobom, których dane dotyczą, treść niniejszego załącznika, w tym ustalenia określone w pkt 1 i 2.

SEKCJA 2

Zarządzanie cyberincydentami, w tym naruszeniami ochrony danych osobowych

1) Współadministratorzy pomagają sobie nawzajem w identyfikacji cyberincydentów i reagowaniu na nie, w tym w przypadku naruszeń ochrony danych osobowych, w związku z przetwarzaniem za pośrednictwem bramy sieciowej unijnego cyfrowego zaświadczenia COVID.

2) Współadministratorzy w szczególności powiadamiają się nawzajem o kwestiach takich, jak:

   a) wszelkie potencjalne lub faktyczne ryzyko dla dostępności, poufności lub integralności danych osobowych przetwarzanych za pośrednictwem bramy sieciowej ram zaufania;

   b) każde naruszenie ochrony danych osobowych, prawdopodobne konsekwencje naruszenia ochrony danych osobowych oraz ocena ryzyka naruszenia praw i wolności osób fizycznych, a także wszelkie środki wdrożone w celu przeciwdziałania naruszaniu ochrony danych osobowych i łagodzenia ryzyka naruszenia praw i wolności osób fizycznych;

▼M3

c) każde naruszenie technicznych lub organizacyjnych zabezpieczeń dotyczących operacji przetwarzania za pośrednictwem bramy sieciowej ram zaufania.

3) Współadministratorzy powiadamiają o wszelkich naruszeniach ochrony danych osobowych odnoszących się do operacji przetwarzania za pośrednictwem bramy sieciowej ram zaufania Komisję, właściwe organy nadzorcze i, jeśli jest to wymagane, osoby, których dane dotyczą, zgodnie z art. 33 i 34 ogólnego rozporządzenia o ochronie danych lub po otrzymaniu powiadomienia ze strony Komisji.

4) Każdy organ wydający wdraża odpowiednie środki techniczne i organizacyjne, mające na celu:

a) zapewnienie i ochronę dostępności, integralności i poufności wspólnie przetwarzanych danych osobowych;

b) ochronę danych osobowych będących w jego posiadaniu przed wszelkiego rodzaju przetwarzaniem, utratą, wykorzystaniem, ujawnieniem lub nabyciem, które jest nieuprawnione lub niezgodne z prawem, lub przed nieuprawnionym lub niezgodnym z prawem dostępem do tych danych;

c) zapewnienie, aby dostęp do danych osobowych nie był ujawniany ani nie był umożliwiany nikomu innemu niż odbiorcom lub podmiotom przetwarzającym.

SEKCJA 3

Ocena skutków dla ochrony danych

1) Jeżeli administrator, w celu wypełnienia swoich obowiązków określonych w art. 35 i 36 rozporządzenia (UE) 2016/679, potrzebuje informacji od innego administratora, wysyła specjalny wniosek na adres funkcyjnej skrzynki pocztowej, o której mowa w sekcji 1 podsekcja 1 pkt 4. Administrator, który otrzymał taki wniosek, dokłada wszelkich starań, aby takie informacje przekazać.

▼M3

ZAŁĄCZNIK VII

OBOWIĄZKI KOMISJI JAKO PODMIOTU PRZETWARZAJĄCEGO DANE W ODNIESIENIU DO BRAMY SIECIOWEJ UNIJNEGO CYFROWEGO ZAŚWIADCZENIA COVID NA POTRZEBY WSPIERANIA WYMIANY LIST UNIEWAŻNIONYCH CERTYFIKATÓW DCC

Komisja:

1) Tworzy i zapewnia bezpieczną i niezawodną infrastrukturę łączności w imieniu państw członkowskich, która wspiera wymianę list unieważnionych certyfikatów przedkładanych w bramie sieciowej unijnych cyfrowych zaświadczeń COVID.

2) Aby wywiązać się ze swoich obowiązków jako podmiotu przetwarzającego w ramach bramy sieciowej ram zaufania dla państw członkowskich, Komisja może angażować osoby trzecie jako podwykonawców podmiotu przetwarzającego; Komisja informuje współadministratorów o wszelkich zamierzonych zmianach dotyczących dodania lub zastąpienia innych podwykonawców podmiotu przetwarzającego, dając tym samym współadministratorom możliwość wspólnego wyrażenia sprzeciwu wobec takich zmian. Komisja zapewnia, aby do podwykonawców podmiotu przetwarzającego zastosowanie miały takie same obowiązki dotyczące ochrony danych jak te określone w niniejszej decyzji.

3) Przetwarza dane osobowe wyłącznie na udokumentowane polecenie administratorów, chyba że obowiązek taki nakłada na nią prawo Unii lub prawo państwa członkowskiego; w takim przypadku przed rozpoczęciem czynności przetwarzania Komisja informuje współadministratorów o tym obowiązku prawnym, o ile prawo to nie zabrania udzielania takiej informacji z uwagi na ważny interes publiczny;

   Przetwarzanie danych przez Komisję obejmuje:

   a) uwierzytelnianie krajowych serwerów wewnętrznych (ang. back-end servers) na podstawie krajowych certyfikatów serwerów wewnętrznych;

   b) odbiór danych, o których mowa w art. 5a ust. 3 decyzji, przesłanych przez krajowe serwery wewnętrzne poprzez zapewnienie interfejsu programowania aplikacji, który umożliwia krajowym serwerom wewnętrznym przesyłanie odpowiednich danych;

   c) przechowywanie danych w bramie sieciowej unijnego cyfrowego zaświadczenia COVID;

   d) udostępnianie danych do pobrania przez krajowe serwery wewnętrzne;

   e) usuwanie danych z datą ich wygaśnięcia lub na polecenie administratora, który je przedłożył;

   f) po zakończeniu świadczenia usługi usuwanie wszelkich pozostałych danych, chyba że prawo Unii lub prawo państwa członkowskiego nakazują przechowywanie danych osobowych.

4) Wprowadzenie wszelkich najnowocześniejszych organizacyjnych, fizycznych i logicznych środków bezpieczeństwa służących utrzymaniu bramy sieciowej unijnego cyfrowego zaświadczenia COVID. W tym celu Komisja:

   a) wyznacza podmiot odpowiedzialny za zarządzanie bezpieczeństwem na poziomie bramy sieciowej unijnego cyfrowego zaświadczenia COVID, przekazuje współadministratorom dane kontaktowe tego podmiotu oraz zapewnia jego dostępność w celu reagowania na zagrożenia dla bezpieczeństwa;

▼M3

b) przyjmuje odpowiedzialność za bezpieczeństwo bramy sieciowej unijnych cyfrowych zaświadczeń COVID, w tym za regularne przeprowadzanie testów, ocen i badań środków bezpieczeństwa;

c) zapewnia, aby wszystkie osoby, którym przyznano dostęp do bramy sieciowej unijnego cyfrowego zaświadczenia COVID, podlegały umownemu, zawodowemu lub ustawowemu obowiązkowi zachowania poufności.

5) Wprowadza wszystkie niezbędne środki bezpieczeństwa, aby nie dopuścić do zakłócenia sprawnego funkcjonowania operacyjnego krajowych serwerów wewnętrznych. W tym celu Komisja wprowadza szczególne procedury związane z połączeniem serwerów wewnętrznych z bramą sieciową unijnego cyfrowego zaświadczenia COVID. Procedury te obejmują:

a) procedurę oceny ryzyka, by wykryć i oszacować potencjalne zagrożenia dla systemu;

b) procedurę audytu i przeglądu, aby:

i. sprawdzać zgodność między wprowadzonymi środkami bezpieczeństwa a mającą zastosowanie polityką bezpieczeństwa;

ii. przeprowadzać regularne kontrole integralności plików systemowych, parametrów bezpieczeństwa i przyznanych zezwoleń;

iii. monitorować w celu wykrywania naruszeń bezpieczeństwa i włamań;

iv. wdrażać zmiany, których celem jest ograniczenie istniejących uchybień w zakresie bezpieczeństwa;

v. określić warunki w zakresie upoważniania, w tym na wniosek administratorów, do przeprowadzania niezależnych audytów, w tym kontroli, oraz przeglądów środków bezpieczeństwa, oraz wnoszenia wkładu w przeprowadzanie tych audytów, kontroli i przeglądów, z zastrzeżeniem warunków, które są zgodne z Protokołem (nr 7) do TFUE w sprawie przywilejów i immunitetów Unii Europejskiej;

c) zmianę procedury kontroli, by udokumentować i zmierzyć wpływ zmiany przed jej wdrożeniem oraz na bieżąco informować współadministratorów o wszelkich zmianach, które mogą wpłynąć na łączność z ich infrastrukturą lub na bezpieczeństwo ich infrastruktury;

d) ustanowienie procedury konserwacji i naprawy, by określić zasady i warunki, których należy przestrzegać w przypadku konieczności przeprowadzenia konserwacji lub naprawy sprzętu;

e) ustanowienie procedury dotyczącej cyberincydentów na potrzeby określenia systemu zgłaszania i eskalacji, informowania administratorów, których to dotyczy, bezzwłocznego informowania administratorów, aby mogli poinformować krajowe organy nadzorcze ds. ochrony danych o wszelkich naruszeniach ochrony danych osobowych, a także na potrzeby określenia procesu dyscyplinarnego w przypadku naruszeń zasad bezpieczeństwa.

6) Wprowadza najnowocześniejsze fizyczne lub logiczne środki bezpieczeństwa w odniesieniu do obiektów, w których znajduje się sprzęt bramy sieciowej unijnego cyfrowego zaświadczenia COVID, oraz w odniesieniu do kontroli dostępu do danych logicznych i kontroli bezpiecznego dostępu. W tym celu Komisja:

a) egzekwuje bezpieczeństwo fizyczne, by ustanowić wyraźne granice bezpieczeństwa i umożliwić wykrywanie naruszeń;

▼M3

b) kontroluje dostęp do obiektów i prowadzi rejestr odwiedzających do celów identyfikacyjnych;

c) zapewnia, aby osobom z zewnątrz, którym udzielono dostępu do obiektów, towarzyszył odpowiednio upoważniony członek personelu;

d) zapewnia, aby sprzętu nie można było dodać, wymienić ani usunąć bez uprzedniej zgody wyznaczonych odpowiedzialnych podmiotów;

e) kontroluje dostęp z oraz do krajowych serwerów wewnętrznych do bramy sieciowej ram zaufania;

f) zapewnia, aby osoby, które uzyskują dostęp do bramy sieciowej unijnego cyfrowego zaświadczenia COVID, zostały zidentyfikowane i uwierzytelnione;

g) dokonuje przeglądu uprawnień do udzielania zezwoleń na dostęp do bramy sieciowej unijnego cyfrowego zaświadczenia COVID w przypadku wykrycia naruszenia bezpieczeństwa mającego wpływ na tę infrastrukturę;

h) zachowuje integralność informacji przekazywanych za pośrednictwem bramy sieciowej unijnego cyfrowego zaświadczenia COVID;

i) wprowadza techniczne i organizacyjne środki bezpieczeństwa, by zapobiec nieuprawnionemu dostępowi do danych osobowych;

j) w razie potrzeby wdraża środki mające na celu zablokowanie nieupoważnionego dostępu do bramy sieciowej unijnego cyfrowego zaświadczenia COVID z domeny organów wydających (tj.: zablokowanie lokalizacji/adresu IP).

7) Podejmuje działania w celu ochrony swojej domeny, obejmujące zerwanie połączeń, w przypadku znacznych odstępstw od zasad i koncepcji jakości lub bezpieczeństwa;

8) Utrzymuje plan zarządzania ryzykiem związany ze swoim zakresem odpowiedzialności;

9) Monitoruje – w czasie rzeczywistym – wydajność wszystkich komponentów usług w ramach bramy sieciowej ram zaufania, tworzy regularne statystyki i prowadzi rejestry.

10) Zapewnia wsparcie w odniesieniu do wszystkich usług w ramach bramy sieciowej ram zaufania– w języku angielskim, całodobowo, przez siedem dni w tygodniu, drogą telefoniczną, mailową lub za pośrednictwem portalu internetowego – oraz odbiera połączenia od upoważnionych osób dzwoniących: koordynatorów bramy sieciowej unijnego cyfrowego zaświadczenia COVID-19 i ich odpowiednich punktów informacyjnych, specjalistów ds. projektów i wyznaczonych osób z Komisji.

11) W miarę możliwości wspiera współadministratorów za pomocą odpowiednich środków technicznych i organizacyjnych zgodnie z art. 12 rozporządzenia (UE) 2018/1725 w wywiązywaniu się z obowiązku odpowiadania na żądania osoby, której dane dotyczą, w zakresie wykonywania jej praw określonych w rozdziale III ogólnego rozporządzenia o ochronie danych.

▼**M3**

12) Wspiera współadministratorów poprzez przekazywanie im informacji na temat bramy sieciowej unijnego cyfrowego zaświadczenia COVID w celu realizacji obowiązków przewidzianych w art. 32, 33, 34, 35 i 36 ogólnego rozporządzenia o ochronie danych.

13) Zapewnia, aby dane przetwarzane w ramach bramy sieciowej unijnego cyfrowego zaświadczenia COVID były niemożliwe do odczytania dla każdej osoby, która nie jest uprawniona do uzyskania do nich dostępu.

14) Wprowadza wszelkie odpowiednie środki, by zapobiec sytuacji, w której operatorzy bramy sieciowej unijnego cyfrowego zaświadczenia COVID mogliby uzyskać nieuprawniony dostęp do przekazywanych danych.

15) Wprowadza środki mające na celu ułatwienie interoperacyjności i łączności między wyznaczonymi administratorami bramy sieciowej unijnego cyfrowego zaświadczenia COVID.

16) Prowadzi rejestr czynności przetwarzania dokonywanych w imieniu współadministratorów zgodnie z art. 31 ust. 2 rozporządzenia (UE) 2018/1725.