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)

KOMISJA EUROPEJSKA,

uwzględniając Traktat o funkcjonowaniu Unii Europejskiej,

uwzględniając 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 ([1]), w szczególności jego art. 9 ust. 1 i 3,

a także mając na uwadze, co następuje:

(1) W rozporządzeniu (UE) 2021/953 ustanowiono unijne cyfrowe zaświadczenie COVID, które ma służyć jako dowód na to, że dana osoba otrzymała szczepionkę przeciwko COVID-19, uzyskała ujemny wynik testu lub powróciła do zdrowia po zakażeniu.

(2) Aby unijne cyfrowe zaświadczenie COVID mogło funkcjonować w całej Unii, konieczne jest ustanowienie specyfikacji technicznych i zasad na potrzeby wypełniania, bezpiecznego wydawania i weryfikacji cyfrowych zaświadczeń COVID, zapewnienia ochrony danych osobowych, określenia wspólnej struktury niepowtarzalnego identyfikatora zaświadczenia oraz wydawania ważnego, bezpiecznego i interoperacyjnego kodu kreskowego. Te ramy zaufania stanowią również podstawę do dążenia do zapewnienia interoperacyjności z międzynarodowymi normami i systemami technologicznymi i jako takie mogą stanowić model współpracy na szczeblu światowym.

(3) Możliwość odczytu i interpretacji unijnego cyfrowego zaświadczenia COVID wymaga wspólnej struktury danych i porozumienia co do zamierzonego znaczenia każdego pola danych w ładunku i jego możliwych wartości. Aby ułatwić taką interoperacyjność, konieczne jest określenie wspólnej skoordynowanej struktury danych na potrzeby ram unijnego cyfrowego zaświadczenia COVID. Wytyczne dotyczące tych ram opracowała sieć e-zdrowie ustanowiona na podstawie dyrektywy Parlamentu Europejskiego i Rady 2011/24/UE ([2]). Wytyczne te należy wziąć pod uwagę przy ustanawianiu specyfikacji technicznych określających format unijnego cyfrowego zaświadczenia COVID i zarządzanie zaufaniem do niego. Należy określić specyfikację struktury danych i mechanizmy kodowania, a także mechanizm kodowania transportowego w formacie optycznym nadającym się do odczytu maszynowego (QR), który można wyświetlić na ekranie urządzenia przenośnego lub wydrukować na kartce papieru.

(4) Oprócz specyfikacji technicznych dotyczących formatu unijnego cyfrowego zaświadczenia COVID i zarządzania zaufaniem do niego należy ustanowić ogólne zasady wypełniania zaświadczeń stosowane w odniesieniu do wartości kodowanych w treści unijnego cyfrowego zaświadczenia COVID. Komisja powinna regularnie aktualizować i publikować zestawy wartości wdrażające te zasady, kierując się odpowiednimi pracami sieci e-zdrowie.

(5) Zgodnie z rozporządzeniem (UE) 2021/953 autentyczne zaświadczenia stanowiące unijne cyfrowe zaświadczenie COVID powinny być indywidualnie identyfikowalne za pomocą niepowtarzalnego identyfikatora zaświadczenia, biorąc pod uwagę, iż w okresie obowiązywania tego rozporządzenia posiadaczom może zostać wydane więcej niż jedno zaświadczenie. Niepowtarzalny identyfikator zaświadczenia ma składać się z ciągu alfanumerycznego, a państwa członkowskie powinny zapewnić, aby nie zawierał on żadnych danych łączących go z innymi dokumentami lub identyfikatorami, takimi jak numer paszportu lub dowodu tożsamości, aby uniemożliwić identyfikację posiadacza. W celu zapewnienia niepowtarzalności identyfikatora zaświadczenia należy ustanowić specyfikacje techniczne i zasady dotyczące jego wspólnej struktury.

([1]) Dz.U. L 211 z 15.6.2021, s. 1.

([2]) Dyrektywa Parlamentu Europejskiego i Rady 2011/24/UE z dnia 9 marca 2011 r. w sprawie stosowania praw pacjentów w transgranicznej opiece zdrowotnej (Dz.U. L 88 z 4.4.2011, s. 45).

(6) Bezpieczeństwo, autentyczność, ważność i integralność zaświadczeń składających się na unijne cyfrowe zaświadczenie COVID, a także ich zgodność z unijnymi przepisami o ochronie danych mają kluczowe znaczenie dla uznawania zaświadczeń we wszystkich państwach członkowskich. Cele te osiąga się dzięki ramom zaufania określającym zasady i infrastrukturę na potrzeby niezawodnego i bezpiecznego wydawania i weryfikowania unijnych cyfrowych zaświadczeń COVID. Ramy zaufania powinny opierać się na infrastrukturze klucza publicznego z łańcuchem zaufania, od organów ds. zdrowia w państwach członkowskich lub innych organów godnych zaufania, aż po poszczególne podmioty wydające unijne cyfrowe zaświadczenia COVID. Dlatego też w celu zapewnienia ogólnounijnego systemu interoperacyjności Komisja utworzyła system centralny – bramę sieciową unijnych cyfrowych zaświadczeń COVID („brama sieciowa") – w którym przechowywane są klucze publiczne wykorzystywane do weryfikacji. Po zeskanowaniu kodu QR podanego w zaświadczeniu podpis cyfrowy jest weryfikowany przy użyciu odpowiedniego klucza publicznego, przechowywanego wcześniej w tej centralnej bramie sieciowej. Podpisy cyfrowe można wykorzystywać do zapewnienia integralności i autentyczności danych. Infrastruktury klucza publicznego budują zaufanie przez wiązanie kluczy publicznych z wystawcami zaświadczeń. W bramie sieciowej używa się wielu certyfikatów klucza publicznego do zapewnienia autentyczności. Aby zapewnić bezpieczną wymianę danych między państwami członkowskimi w zakresie materiałów zawierających klucz publiczny oraz umożliwić szeroko zakrojoną interoperacyjność, konieczne jest ustanowienie certyfikatów klucza publicznego, które mogą być wykorzystywane, oraz określenie sposobu ich generowania.

(7) Niniejsza decyzja umożliwia wdrożenie wymogów rozporządzenia (UE) 2021/953 w sposób ograniczający przetwarzanie danych osobowych do tego, co jest rzeczywiście konieczne do stosowania unijnego cyfrowego zaświadczenia COVID, i przyczyniający się do przetwarzania tych danych przez administratorów końcowych z poszanowaniem uwzględnienia ochrony danych w fazie projektowania.

(8) Zgodnie z rozporządzeniem (UE) 2021/953 organy lub inne wyznaczone podmioty odpowiedzialne za wydawanie zaświadczeń są administratorami, o których mowa w art. 4 pkt 7 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 ([3]), ze względu na swoją rolę polegającą na przetwarzaniu danych osobowych w procesie wydawania zaświadczeń. W zależności od tego, w jaki sposób państwa członkowskie organizują proces wydawania zaświadczeń, może istnieć jeden organ lub wyznaczony podmiot, np. regionalna służba zdrowia, bądź większa ich liczba. Zgodnie z zasadą pomocniczości decyzja w tej kwestii należy do państw członkowskich. Dlatego w przypadku gdy istnieje wiele organów lub innych wyznaczonych podmiotów, to państwa członkowskie są w stanie najlepiej zapewnić wyraźny podział ich obowiązków, niezależnie od tego, czy są one odrębnymi administratorami czy współadministratorami (w tym regionalna służba zdrowia tworząca wspólny portal dla pacjentów służący do wydawania zaświadczeń). Podobnie jeżeli chodzi o weryfikację zaświadczeń przez właściwe organy państwa członkowskiego przeznaczenia bądź tranzytu lub przez podmioty świadczące transgraniczne usługi transportu pasażerskiego, zobowiązane na mocy krajowych przepisów do wdrożenia niektórych środków dotyczących zdrowia publicznego podczas pandemii COVID-19, weryfikatorzy ci muszą wypełniać obowiązki wynikające z przepisów o ochronie danych.

(9) Za pośrednictwem bramy sieciowej unijnych cyfrowych zaświadczeń COVID nie przetwarza się danych osobowych, ponieważ brama ta zawiera jedynie klucze publiczne organów podpisujących. Klucze te odnoszą się do organów podpisujących i nie umożliwiają ani bezpośredniej, ani pośredniej ponownej identyfikacji osoby fizycznej, której wydano zaświadczenie. Pełniąc funkcję podmiotu zarządzającego bramą sieciową, Komisja nie powinna zatem być ani administratorem danych osobowych, ani podmiotem przetwarzającym dane osobowe.

(10) Zgodnie z art. 42 ust. 1 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2018/1725 ([4]) skonsultowano się z Europejskim Inspektorem Ochrony Danych; swoją opinię wydał on w dniu 22 czerwca 2021 r.

(11) Biorąc pod uwagę fakt, że specyfikacje techniczne i zasady są niezbędne do stosowania rozporządzenia (UE) 2021/953 od dnia 1 lipca 2021 r., uzasadnione jest natychmiastowe stosowanie niniejszej decyzji.

(12) Zatem w świetle potrzeby szybkiego wdrożenia unijnego cyfrowego zaświadczenia COVID niniejsza decyzja powinna wejść w życie z dniem jej opublikowania,

([3]) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.U. L 119 z 4.5.2016, s. 1).

([4]) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2018/1725 z dnia 23 października 2018 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez instytucje, organy i jednostki organizacyjne Unii i swobodnego przepływu takich danych oraz uchylenia rozporządzenia (WE) nr 45/2001 i decyzji nr 1247/2002/WE (Dz.U. L 295 z 21.11.2018, s. 39).

PRZYJMUJE NINIEJSZĄ DECYZJĘ:

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.

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.

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

Sporządzono w Brukseli dnia 28 czerwca 2021 r.

W imieniu Komisji
Ursula VON DER LEYEN
Przewodnicząca

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

— 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

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

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 ([3])) 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.

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

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 ([5]), 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 ([6])) zawierającym informacje o statusie zdrowotnym. W ramach tego samego oświadczenia może istnieć kilka różnych rodzajów świadectw zdrowia, z których jednym jest zaświadczenie COVID.

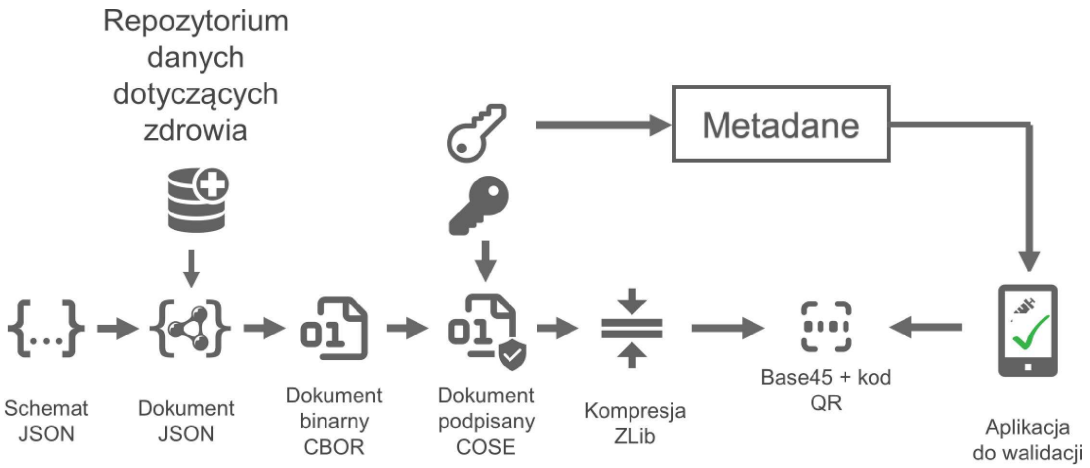
JSON służy wyłącznie do celów schematu. Format odwzorowania to CBOR, zdefiniowany w RFC 7049 ([7]). Programiści aplikacji nie muszą w rzeczywistości nigdy dekodować ani kodować do i z formatu JSON, lecz wykorzystują strukturę w pamięci.

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 ([8]). Treść danych jest ograniczona do zdefiniowanych elementów danych znajdujących się w minimalnym zestawie danych określonym w załączniku do rozporządzenia (UE) 2021/953.

([5]) rfc8392 (ietf.org).
([6]) rfc7159 (ietf.org).
([7]) rfc7049 (ietf.org).
([8]) 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.

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.

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 ([9])) i mechanizmu kompresji Deflate w formacie określonym w RFC 1951 ([10]).

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.

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

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.

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 ([11]), 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.

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.

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

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 zaświadczeń 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 zaleca się kodowanie w UTF-8 (nazwa, punkt, w którym wykonano test, wystawca zaświadczenia). Pola danych zawierające daty kalendarzowe (data urodzenia, data szczepienia, data pobrania próbki do testu, data pierwszego dodatniego wyniku testu, daty ważności zaświadczeń) zaleca się kodować zgodnie z normą ISO 8601.

Jeżeli z jakiegokolwiek powodu nie można zastosować preferowanych systemów kodów wymienionych poniżej, można zastosować inne międzynarodowe systemy kodów, przy czym należy zapewnić 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 powinny przyporządkować takie kody opisanym zestawom wartości. Państwa członkowskie są odpowiedzialne za wszelkie takie przyporządkowania.

Komisja regularnie aktualizuje zestawy wartości 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. Należy przedstawić 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)**

   Preferowany system kodów: SNOMED CT.

   Kod stosowany w zaświadczeniach 1, 2 i 3.

   Wybrane kody odnoszą się do COVID-19 lub, w przypadku gdy potrzebne są bardziej szczegółowe informacje na temat wariantu genetycznego SARS-CoV-2, do tych wariantów, jeżeli takie szczegółowe informacje są potrzebne ze względów epidemiologicznych.

   Przykładem kodu, który należy stosować, jest kod SNOMED CT 840539006 (COVID-19).

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). Zestaw wartości należy rozszerzyć, gdy nowe typy szczepionek zostaną opracowane i wprowadzone do użytku.

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).

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 do obrotu szczepionki 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).

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

Kod stosowany w zaświadczeniu 1.

Dwa pola:

1) numer dawki podanej w cyklu;

2) liczba oczekiwanych dawek w pełnym cyklu (właściwa dla danej osoby w momencie podawania dawki).

Na przykład kody 1/1 i 2/2 będą oznaczały ukończony cykl, łącznie z opcją 1/1 w przypadku szczepionek dwudawkowych, dla których protokół stosowany przez państwo członkowskie przewiduje podanie jednej dawki obywatelom, u których przed szczepieniem zdiagnozowano COVID-19. Ogólną liczbę dawek w serii należy podać zgodnie z informacjami dostępnymi w momencie podawania dawki. Na przykład jeżeli w czasie ostatnio podanej dawki dana szczepionka wymaga podania trzeciego zastrzyku (dawki przypominającej), cyfra w drugim polu powinna to odzwierciedlać (np. 2/3, 3/3 itd.).

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).

7. **Rodzaj testu**

Preferowany system kodów: LOINC.

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

Kody w tym zestawie wartości odnoszą się do metody testowania i wybiera się je w taki sposób, aby co najmniej rozróżnić testy NAAT od testów RAT, jak określono w rozporządzeniu (UE) 2021/953.

Przykładem kodu z preferowanych systemów kodów, który należy stosować, jest LP217198-3 (szybki test immunologiczny).

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

Preferowany system kodów: otrzymany od Komitetu ds. Bezpieczeństwa Zdrowia wykaz szybkich testów antygenowych prowadzony przez JRC (baza danych dotycząca wyrobów medycznych do diagnostyki in vitro i metod testowania zakażeń COVID-19).

Kod stosowany w zaświadczeniu 2.

Zawartość zestawu wartości obejmuje wybór szybkiego testu antygenowego wymienionego we wspólnym i uaktualnionym wykazie szybkich 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 medycznych do diagnostyki in vitro i metod testowania zakażeń COVID-19 pod adresem: https://covid-19-diagnostics.jrc.ec.europa.eu/devices/hsc-common-recognition-rat

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**

Preferowany system kodów: SNOMED CT.

Kod stosowany w zaświadczeniu 2.

Wybrane kody muszą umożliwiać odróżnienie dodatnich wyników testów od ujemnych (wykryto lub nie wykryto). Można dodać dodatkowe wartości (takie jak „nieokreślony"), jeżeli wymagają tego przypadki użycia.

Przykładami kodu z preferowanego systemu kodów, które należy stosować, są 260415000 (nie wykryto) i 260373001 (wykryto).

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.

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]) ([2]), mianowicie {'/','#',':'};

2) maksymalna długość: autorzy powinni dążyć do długości wynoszącej 27–30 znaków ([3]);

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;

4) prefiks państwa: kod państwa jest określony normą ISO 3166-1. Dłuższe kody (np. zawierające od trzech znaków (np. „UNHCR”) są zarezerwowane do użytku w przyszłości;

5) sufiks kodu/suma kontrolna:

5.1. Państwa członkowskie powinny 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 może być podstawą do walidacji zaświadczenia i z technicznego punktu widzenia nie stanowi części identyfikatora, lecz służy do weryfikacji integralności kodu. Suma kontrolna powinna być zgodnym z ISO-7812-1 (LUHN-10) ([4]) streszczeniem całego niepowtarzalnego identyfikatora zaświadczenia w formacie cyfrowym/transportowym. Suma kontrolna jest oddzielona od pozostałej części identyfikatora znakiem „#”.

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

([2]) Takie pola, jak: płeć, numer serii/partii, punkt, w którym podano szczepionkę, identyfikacja pracownika służby zdrowia, data następnego szczepienia, nie mogą być potrzebne do celów innych niż medyczne.

([3]) W celu wdrożenia z kodami 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.

([4]) 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).

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

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

W wytycznych sieci e-zdrowie w sprawie podlegających weryfikacji zaświadczeń o szczepieniu i podstawowych elementów interoperacyjności ([5]) 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.

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

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.
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

Termin	Definicja
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.

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 $DCCG_{TA}$.

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.

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 $DCCG_{TLS}$.

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.

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]).

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

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

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 ([3]).

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)

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

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 ([4])).

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.

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)

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

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** ([5])**, 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)

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).

([5]) 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.