РЕШЕНИЕ ЗА ИЗПЪЛНЕНИЕ (ЕС) 2021/1073 НА КОМИСИЯТА

от 28 юни 2021 година

за определяне на техническите спецификации и правила за прилагането на рамката за доверие за Цифровия COVID сертификат на ЕС, въведена с Регламент (ЕС) 2021/953 на Европейския парламент и на Съвета

(текст от значение за ЕИП)

ЕВРОПЕЙСКАТА КОМИСИЯ,

като взе предвид Договора за функционирането на Европейския съюз,

като взе предвид Регламент (ЕС) 2021/953 на Европейския парламент и на Съвета относно рамка за издаването, проверката и приемането на оперативно съвместими сертификати за ваксинация срещу, направено изследване за и преболедуване на COVID-19 (Цифров COVID сертификат на ЕС) с цел улесняване на свободното движение по време на пандемията от COVID-19 ([1]), и по-конкретно член 9, параграфи 1 и 3 от него,

като има предвид, че:

(1) С Регламент (ЕС) 2021/953 се установява Цифровият COVID сертификат на ЕС, чиято цел е да служи за доказателство, че дадено лице е ваксинирано срещу COVID-19, получило е отрицателен резултат от направено изследване или се е възстановило след преболедуване.

(2) За да може Цифровият COVID сертификат на ЕС да функционира в целия Съюз, е необходимо да се установят технически спецификации и правила за попълване, сигурно издаване и проверка на цифровите COVID сертификати, гарантиране на защитата на личните данни, определяне на общата структура на уникалния идентификатор на сертификата и издаване на валиден, сигурен и оперативно съвместим баркод. Тази рамка за доверие също така определя условията за осигуряване на оперативна съвместимост с международните стандарти и технологични системи, като така би могла да осигури модела за сътрудничество на глобално ниво.

(3) Възможността за прочитане и тълкуване на Цифровия COVID сертификат на ЕС изисква обща структура на данните и споразумение за предвиденото значение на всяко поле на полезните данни и възможните му стойности. За да се улесни тази оперативна съвместимост, е необходимо да се определи обща координирана структура на данните за рамката на Цифровия COVID сертификат на ЕС. Насоките за тази рамка са разработени от eHealth Network на базата на Директива 2011/24/ЕС на Европейския парламент и на Съвета ([2]). Тези насоки следва да се вземат предвид при определянето на техническите спецификации, с които се задават формата и управлението на доверието за Цифровия COVID сертификат на ЕС. Следва също така да се определят спецификация на структурата на данните и механизми за кодиране, както и механизъм за кодиране за пренос в машинночетим оптичен формат (QR), който може да се показва на екрана на мобилно устройство или да бъде разпечатан на лист хартия.

(4) В допълнение към техническите спецификации за формата и управлението на доверието на Цифровия COVID сертификат на ЕС следва да се въведат общи правила за попълването на сертификатите, които да се използват за кодираните стойности в съдържанието на Цифровия COVID сертификат на ЕС. Наборите от стойности, които отговарят на тези правила, следва да се актуализират редовно и да се публикуват от Комисията въз основа на съответната работа на мрежата за електронно здравеопазване.

(5) Съгласно Регламент (ЕС) 2021/953 автентичните сертификати, съставляващи Цифровия COVID сертификат на ЕС, трябва да могат да бъдат идентифицирани поотделно чрез уникален идентификатор на сертификата, като се отчита, че на гражданите може да се издаде повече от един сертификат, докато Регламент (ЕС) 2021/953 е в сила. Уникалният идентификатор на сертификата трябва да се състои от буквено-цифров низ и държавите членки следва да осигурят той да не съдържа данни, свързващи го с други документи или идентификатори, като номера на паспорт или лична карта, за да се предотврати идентифицирането на притежателя. С цел да се гарантира, че идентификаторът на сертификата е уникален, следва да бъдат определени технически спецификации и правила за общата му структура.

([1]) ОВ L 211, 15.6.2021 г., стр. 1.

([2]) Директива 2011/24/ЕС на Европейския парламент и на Съвета от 9 март 2011 г. за упражняване на правата на пациентите при трансгранично здравно обслужване (ОВ L 88, 4.4.2011 г., стр. 45).

(6) Сигурността, автентичността, валидността и целостта на сертификатите, съставляващи Цифровия COVID сертификат на ЕС, и тяхното съответствие със законодателството на Съюза за защита на данните са от ключово значение за приемането им във всички държави членки. Тези цели се постигат чрез рамката за доверие, с която се определят правилата и инфраструктурата за надеждното и сигурно издаване и проверка на Цифровите COVID сертификати на ЕС. Наред с другото рамката за доверие следва да се основава на инфраструктура на публичния ключ с верига на доверие от здравните органи на страните членки или други надеждни органи до отделните организации, издаващи Цифрови COVID сертификати на ЕС. Ето защо, за да осигури оперативната съвместимост на системата на ниво ЕС, Комисията изгради централна система — портал за Цифровия COVID сертификат на ЕС (по-долу „порталът“), където се съхраняват публичните ключове, използвани за проверка. Когато QR кодът на сертификата бъде сканиран, се проверява цифровият подпис посредством съответния публичен ключ, който преди това е съхранен в този централен портал. Цифровите подписи могат да се използват за гарантиране на целостта и автентичността на данните. Инфраструктурите на публичния ключ създават доверие, като свързват публичните ключове към издателите на сертификати. На портала се използват множество удостоверения за публичен ключ с цел проверяване на автентичността. За да се гарантира сигурен обмен на публичните ключове между държавите членки и да се позволи широка оперативна съвместимост, е необходимо да се създадат удостоверения за публичен ключ, които могат да се използват, и да се осигури начинът, по който те следва да бъдат генерирани.

(7) Настоящето решение позволява да изпълнят изискванията на Регламент (ЕС) 2021/953 така, че да се ограничи до минимум обработването на лични данни до това, което е необходимо, за да се приведе в действие Цифровият COVID сертификат на ЕС, и спомага за прилагане от страна на крайните администратори, което съответства на защита на данните на етапа на проектирането.

(8) В съответствие с Регламент (ЕС) 2021/953 органите или други упълномощени органи, отговорни за издаването на сертификати, са администратори, както е посочено в член 4, параграф 7 от Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета ([3]), в качеството си на обработващи лични данни в процеса на издаване на сертификатите. В зависимост от организацията на процеса на издаване, създадена от държавите членки, може да има един или няколко органа или упълномощени органи, например регионални здравни служби. В съответствие с принципа на субсидиарност това е избор на държавите членки. Ето защо държавите членки са в най-добра позиция там, където има няколко органа или други упълномощени органи, да осигурят ясно разпределение на съответните отговорности, независимо дали става дума за отделни или съвместни администратори (включително регионални здравни служби с общ пациентски портал за издаване на сертификати). По подобен начин, във връзка с проверката на сертификатите от компетентните органи на държавите членки на местоназначение или транзит, или от оператори на трансгранични пътнически транспортни услуги, за които се изисква по закон да изпълняват определени мерки за опазване на общественото здраве по време на пандемията от COVID-19, изпълнителите на тези проверки трябва да спазват задълженията си в съответствие с правилата за защита на личните данни.

(9) На портала на Цифровия COVID сертификат на ЕС не се извършва обработка на лични данни, тъй като порталът съдържа само публичните ключове на подписващите органи. Тези ключове са свързани с подписващите органи и не допускат пряко или косвено повторно идентифициране на физическото лице, на което се издава сертификатът. В качеството си на управляващ портала Комисията в този смисъл не следва да бъде нито администратор, нито обработващ лични данни.

(10) В съответствие с член 42, параграф 1 от Регламент (ЕС) 2018/1725 на Европейския парламент и на Съвета ([4]) беше проведена консултация с Европейския надзорен орган по защита на данните, който даде становище на 22 юни 2021 г.

(11) Като се има предвид, че за прилагането на Регламент (ЕС) 2021/953 от 1 юли 2021 г. са необходими технически спецификации и правила, незабавното прилагане на настоящото решение е обосновано.

(12) Следователно, предвид необходимостта от бързо прилагане на Цифровия COVID сертификат на ЕС настоящото решение следва да влезе в сила в деня на публикуването му,

([3]) Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27 април 2016 г. относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни и за отмяна на Директива 95/46/ЕО (Общ регламент относно защитата на данните) (ОВ L 119, 4.5.2016 г., стр. 1).

([4]) Регламент (ЕС) 2018/1725 на Европейския парламент и на Съвета от 23 октомври 2018 г. относно защитата на физическите лица във връзка с обработването на лични данни от институциите, органите, службите и агенциите на Съюза и относно свободното движение на такива данни и за отмяна на Регламент (ЕО) № 45/2001 и Решение № 1247/2002/ЕО (ОВ L 295, 21.11.2018 г., стр. 39).

ПРИЕ НАСТОЯЩОТО РЕШЕНИЕ:

Член 1

Техническите спецификации за Цифровия COVID сертификат на ЕС, които определят общата структура на данните, механизмите за кодиране и механизма за кодиране за пренос в машинночетим оптичен формат, са определени в приложение I.

Член 2

Правилата за попълване на сертификатите по член 3, параграф 1 от Регламент (ЕС) 2021/953 са определени в приложение II към настоящото решение.

Член 3

Изискванията, определящи общата структура на уникалния идентификатор на сертификата, са посочени в приложение III.

Член 4

Правилата за управление, приложими към удостоверенията за публичен ключ във връзка с портала на Цифровия COVID сертификат на ЕС за поддържане на аспектите, свързани с оперативната съвместимост на рамката за доверие, са определени в приложение IV.

Настоящото решение влиза в сила в деня на публикуването му в *Официален вестник на Европейския съюз*.

Съставено в Брюксел на 28 юни 2021 година.

За Комисията
Председател
Ursula VON DER LEYEN

ПРИЛОЖЕНИЕ I

ФОРМАТ И УПРАВЛЕНИЕ НА ДОВЕРИЕТО

Обща структура на данните, механизми за кодиране и механизъм за кодиране за пренос в машинночетим оптичен формат (наричан по-долу „QR“)

1. **Увод**

Техническите спецификации, посочени в настоящото приложение, съдържат обща структура на данните и механизми за кодиране за Цифровия COVID сертификат на ЕС („DCC“). Също така с тях се определя механизъм за кодиране за пренос в машинночетим оптичен формат (QR), който може да се показва на екрана на мобилно устройство или да бъде разпечатан. Форматите на контейнерите на електронния здравен сертификат, посочени в тези спецификации, са общи, но в този контекст се използват за пренасяне на DCC.

2. **Терминология**

За целите на настоящото приложение „издатели“ означава организации, които използват тези спецификации за издаване на здравни сертификати, а „проверяващи органи“ означава организации, които приемат здравните сертификати като доказателство за здравното състояние на лицата. „Участници“ означава издатели и проверяващи органи. Някои аспекти, определени в настоящото приложение, трябва да бъдат координирани между участниците, като например управлението на пространството от имена и разпространението на криптографските ключове. Приема се, че тези задачи се извършват от страната, наричана по-долу „Секретариат“.

3. **Формат на контейнера на електронния здравен сертификат**

Форматът на контейнера на електронния здравен сертификат има за цел да осигури единен и стандартизиран носител на здравните сертификати от различните им издатели („издатели“). Целта на настоящите спецификации е да се хармонизират начините, по които тези здравни сертификати се представят, кодират и подписват, така че да се улесни оперативната съвместимост.

За да са възможни четенето и интерпретирането на DCC, издаден от който и да е издател, е необходима обща структура на данните и съгласие за значението на всяко поле на полезните данни. За да се улесни такава оперативна съвместимост, е определена обща координирана структура на данните посредством използването на схема „JSON“, която съставлява рамката на DCC.

3.1. *Структура на полезните данни*

Полезните данни са структурирани и кодирани като CBOR с цифров подпис COSE. Това е известно като „CBOR Web Token“ (CWT) и е определено в RFC 8392 ([1]). Полезните данни, както са определени в следващите секции, се пренасят в заявка hcert.

Целостта и автентичността на произхода на полезните данни трябва да могат да бъдат проверени от проверяващия орган. За да осигури този механизъм, издателят трябва да подпише CWT, като използва асиметрична схема на електронен подпис, както е определена в спецификацията за COSE (RFC 8152 ([2])).

3.2. *ЗАЯВКИ ЗА CWT*

3.2.1. Общ преглед на структурата на CWT

Защитена заглавна част

— Алгоритъм за подпис (alg, етикет 1)

— Идентификатор на ключ (kid, етикет 4)

Полезни данни

— Издател (iss, ключ за заявка 1, незадължителен, ISO 3166-1 двубуквен код на издателя)

— Издаден на (iat, ключ за заявка 6)

— Срок на валидност (exp, ключ за заявка 4)

— Здравен сертификат (hcert, ключ за заявка -260)

— Цифров COVID сертификат на ЕС версия 1 (eu_DCC_v1, ключ за заявка 1)

Подпис

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

3.2.2. Алгоритъм за подпис

Параметърът на алгоритъма за подпис (alg) указва кой алгоритъм се използва за създаването на подписа. Той трябва да отговаря на или да надхвърля текущите насоки на SOG-IT, обобщени в следващите параграфи.

Определят се един основен и един вторичен алгоритъм. Вторичният алгоритъм следва да се използва само ако основният не е допустим в рамките на правилата и наредбите, наложени от издателя.

За да се подсигури сигурността на системата, всички изпълнения трябва да включват вторичния алгоритъм. Поради тази причина трябва да бъдат внедрени както основният, така и вторичният алгоритъм.

Нивата на набора SOG-IT за основния и вторичния алгоритъм са:

— Основен алгоритъм: Основният алгоритъм е Elliptic Curve Digital Signature Algorithm (алгоритъм за електронни подписи по елиптична крива) (ECDSA), определен в (ISO/IEC 14888–3:2006) раздел 2.3, използващ параметрите P–256, определени в допълнение D (D.1.2.3) към (FIPS PUB 186–4), в съчетание с алгоритъма SHA–256 за хеширане, определен в (ISO/IEC 10118–3:2004), функция 4.

Това съответства на параметъра на алгоритъма COSE, ES256.

— Вторичен алгоритъм: Вторичният алгоритъм е RSASSA-PSS, определен в (RFC 8230 ([3])), с модул от 2048 бита, в съчетание с алгоритъма SHA–256 за хеширане, определен в (ISO/IEC 10118–3:2004), функция 4.

Това съответства на параметъра на алгоритъма COSE: PS256.

3.2.3. Идентификатор на ключ

Заявката за идентификатор на ключ (kid) указва сертификата на подписващия документи орган (DSC), съдържащ публичния ключ, който проверяващият орган трябва да използва за проверка на верността на цифровия подпис. Управлението на удостоверението за публичен ключ, включително изискванията за DSC, е описано в приложение IV.

Заявката за идентификатор на ключ (kid) се използва от проверяващите органи за избиране на правилния публичен ключ от списък с ключове, отнасящи се до издателя, указан в заявката на издателя (iss). Издателят може да използва няколко ключа паралелно за административни цели и когато извършва подновяване на ключовете. Идентификаторът на ключ не е поле от съществено значение за сигурността. Ето защо той може да бъде поставен в незащитена заглавна част, ако е необходимо. Проверяващите органи трябва да приемат и двата варианта. Ако са налице и двете възможности, трябва да се използва идентификаторът на ключа в защитената заглавна част.

Поради скъсяването на идентификатора (поради ограничението на размера) има малък, но не и нулев шанс пълният списък с DSC, приемани от потвърждаващ орган, да съдържа DSC с дублирани kid. Ето защо проверяващият орган трябва да провери всички DSC с този kid.

3.2.4. Издател

Заявката на издателя (iss) е низ, която незадължително може да съдържа ISO 3166-1 двубуквен кода на държавата на организацията, издаваща здравния сертификат. Заявката може да се използва от проверяващия орган, за да установи кой набор от DCS да използва за проверка. Ключ за заявка 1 се използва за идентифициране на тази заявка.

3.2.5. Срок на валидност

Заявката за срок на изтичане (exp) следва да съдържа електронен времеви печат в цифров формат на датата (посочен в RFC 8392 ([4]), раздел 2), указващ колко дълго следва да се смята за валиден този конкретен подпис на полезните данни, след което проверяващ орган трябва да отхвърли полезните данни като изтекли. Целта на параметъра за изтичане е да се наложи ограничение на срока на валидност на здравния сертификат. За идентифициране на тази заявка се използва ключ за заявка 4.

Срокът на изтичане не трябва да надхвърля срока на валидност на DSC.

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

3.2.6. Издаден на

Заявката „Издаден на“ (iad) следва да съдържа електронен времеви печат в цифров формат на датата (посочен в RFC 8392 ([5]), раздел 2), указващ момента на създаване на здравния сертификат.

Полето „Издаден на“ не трябва да е с дата, предхождаща срока на валидност на DSC.

Проверяващите органи може да приложат допълнителни правила с цел ограничаване срока на валидност на здравния сертификат в зависимост от момента на издаване. За идентифициране на тази заявка се използва ключ за заявка 6.

3.2.7. Заявка за здравен сертификат

Заявката за здравен сертификат (hcert) е обект JSON (RFC 7159 ([6])), съдържащ информация за здравния статус. Може да съществуват няколко различни типа здравни сертификата в една и съща заявка, като DCC е един от тях.

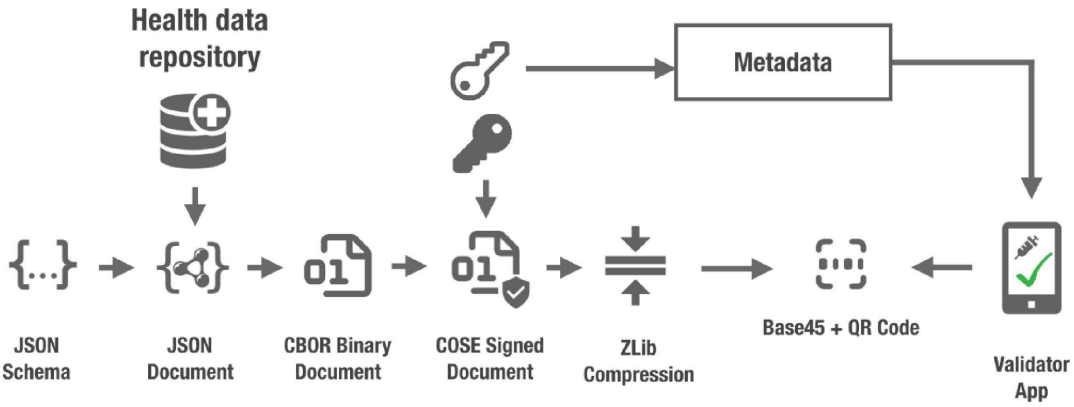
JSON се използва само за целите на схемата. Форматът на представяне е CBOR, както е определен в (RFC 7049 ([7])). Програмистите на приложения всъщност може да не разкодират или да кодират от и във формат JSON, а да използват структурата в паметта.

Ключът за идентифициране на тази заявка е -260.

Низовете в обекта JSON следва да се нормализират съгласно NFC, определен в стандарта Unicode. Приложенията за разкодиране би трябвало обаче да имат гъвкавост и капацитет по отношение на тези аспекти и силно се насърчава приемането на всеки разумен тип преобразуване. Ако по време на разкодиране или при последващи сравнителни функции бъдат открити ненормализирани данни, изпълненията трябва да функционират така, все едно че входните данни са нормализирани съгласно NFC.

4. **Сериализация и създаване на полезните данни на DCC**

Като модел за сериализация се използва следната схема:



Процесът започва с извличане на данни, например от хранилище на здравни данни (или от някой външен източник на данни), като извлечените данни се структурират в съответствие с определените схеми за DCC. При този процес преобразуването в определения формат на данните и преобразуването за четимост от човек може да се извърши преди началото на сериализацията към CBOR. Съкращенията в заявките трябва да бъдат съпоставяни при всички случаи с показваните имена преди сериализацията и след десериализацията.

Незадължителното съдържание на национални данни не е разрешено в сертификатите, издадени съгласно Регламент (ЕС) 2021/953 ([8]). Съдържанието на данни е ограничено до определените елементи на данни в минималния набор от данни, посочен в приложението към Регламент 2021/953.

([5]) rfc8392 (ietf.org)
([6]) rfc7159 (ietf.org)
([7]) rfc7049 (ietf.org)
([8]) Регламент (ЕС) 2021/953 на Европейския парламент и на Съвета от 14 юни 2021 г. относно рамка за издаването, проверката и приемането на оперативно съвместими сертификати за ваксинация срещу, направено изследване за и преболедуване на COVID-19 (Цифров COVID сертификат на ЕС) с цел улесняване на свободното движение по време на пандемията от COVID-19, ОВ L 211, 15.6.2021 г., стр. 1.

5. **Кодирания за пренос**

5.1. *Непреработено*

За произволни интерфейси от данни контейнерът HCERT и полезните му данни може да се прехвърлят без промяна, като се използва всяко основно, 8-битово безопасно и надеждно пренасяне на данните. Тези интерфейси може да включват комуникация в близката зона (на полето) (NFC), Bluetooth или прехвърляне посредством протокол на приложния слой, например прехвърляне на HCERT от издателя до мобилно устройство на притежателя.

Ако прехвърлянето на HCERT от издателя на притежателя е базирано само на изобразяващ интерфейс (например SMS, имейл), кодирането за пренос „непреработено“ очевидно не е приложимо.

5.2. *Баркод*

5.2.1. Компресиране на полезните данни (CWT)

За да се намали размерът и да се увеличат скоростта и надеждността на процеса на разчитане на HCERT, CWT следва да се компресира посредством ZLIB (RFC 1950 ([9])) и механизма за компресиране Deflate във формата, определен в RFC 1951 ([10]).

5.2.2. QR двуизмерен баркод

За да се използва по-добре наследеното оборудване, което е предназначено да оперира с полезни данни в ASCII, компресираният CWT се кодира като ASCII посредством Base45, преди да се кодира в двуизмерен баркод.

QR форматът, определен в (ISO/IEC 18004:2015) следва да се използва за генериране на двуизмерен баркод. Процент на корекция на грешката на „Q“ (около 25 %) е препоръчителен. Тъй като се използва Base45, QR кодът трябва да използва буквено-цифрово кодиране (Mode 2, указан със символите 0010).

За да могат проверяващите органи да установят типа на кодираните данни и да изберат правилната схема за разкодиране и обработване, кодираните с Base45 данни (според настоящата спецификация) следва да са с представка, състояща се от низа с идентификатор на контекста „HC1:“. Бъдещите версии на тази спецификация, които засягат обратната съвместимост, следва да определят нов идентификатор на контекста, при който знаците след „HC“ следва да бъдат взети от набора със знаци [1-9A-Z]. Подредбата на нарастващите стойности се определя в този ред, т.е. първо [1-9], а след това — [A-Z].

Оптичният код е препоръчително да бъде изразен в изобразяващата медия с диагонален размер между 35 mm и 60 mm, за да е съвместим с четци с фиксирана оптика, където изобразяващата медия трябва да бъде поставена на повърхността на четеца.

Ако оптичният код е отпечатан на хартия чрез принтер с ниска резолюция (< 300 dpi), трябва да се внимава всеки символ (точка) на QR кода да се изобразява като точен квадрат. Непропорционалното мащабиране ще доведе до това някои редове и колони в QR кода да са с правоъгълни символи, а това в много случаи ще попречи на прочитането.

6. **Формат на доверителния списък (списък на CSCA и DSC)**

От всяка държава членка се изисква да предостави списък с един или няколко национални подписващи сертификати органа (CSCA), както и списък на всички валидни сертификати на подписващите документи органи (DSC), и да поддържа тези списъци актуални.

6.1. *Опростени CSCA/DSC*

От тази версия на спецификациите държавите членки не следва да приемат, че може да се използва информация от списъка на отменени сертификати (CRL); или че срокът на използване на частния ключ се проверява от внедряващите органи.

Вместо това основният механизъм за проверка е наличието на сертификата в най-новата версия на този списък със сертификати.

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

6.2. *Инфраструктура на публичния ключ (PKI) за еМЧДП на ИКАО и доверителни центрове*

Държавите членки могат да използват отделен CSCA, но могат също така да подадат своите съществуващи сертификати на CSCA за еМЧДП и/или DSC; а може дори да изберат да ги доставят от (търговски) доверителни центрове — и да изпращат тях. Всеки DSC обаче трябва винаги да бъде подписан от CSCA, подаден от тази държава членка.

7. **Съображения за сигурност**

Когато разработват схема, използвайки тази спецификация, държавите членки следва да идентифицират, анализират и проследяват определени аспекти на сигурността.

По-специално би трябвало да бъдат взети под внимание най-малко следните аспекти:

7.1. *Срок на валидност на подписа на HCERT*

Издателят на HCERT трябва да ограничи срока на валидност на подписа, като посочи срок на изтичането му. За това е необходимо притежателят на здравния сертификат да го подновява периодично.

Допустимият срок на валидност може да бъде определен на базата на практически ограничения. Например пътуващият може да не е имал възможност да поднови здравния си сертификат по време на пътуване в чужбина. Може обаче да се случи издател да обмисля възможността за някакъв компромис със сигурността, който изисква от него да оттегли DSC (като така отмени валидността на всички здравни сертификати, издадени с този ключ, чийто срок на валидност още не е изтекъл). Последствията от такова събитие може да се ограничат от редовното подновяване на ключовете на издателя и от изискването за подновяване на всички здравни сертификати през някакъв разумен интервал.

7.2. *Управление на ключовете*

Настоящата спецификация разчита в значителна степен на силни криптографски механизми, за да осигури целостта на данните и потвърждаването на произхода на данните. Ето защо е необходимо да се поддържа поверителността на частните ключове.

Поверителността на криптографските ключове може да бъде компрометирана по различни начини, например:

— Процесът на генериране на ключа може да има дефекти, което да доведе до слаба сигурност на ключовете.

— Ключовете може да са изложени на човешка грешка.

— Ключовете може да бъдат откраднати от външни или вътрешни нарушители.

— Ключовете може да бъдат изчислени посредством криптоанализ.

С цел от смекчаване на рисковете алгоритъмът за подписване да се окаже слаб, което да позволи компрометиране на частните ключове посредством криптоанализ, настоящата спецификация препоръчва всички участници да внедрят вторичен, резервен алгоритъм за подпис, основан на различни параметри или на различен математически проблем от предишния.

По отношение на споменатите рискове, свързани с оперативната среда на издателите, следва да се приложат смекчаващи мерки за осигуряване на ефективен контрол, като например частните ключове да се генерират, съхраняват и използват в хардуерни модули за сигурност (HSM). Използването на HSM за подписване на здравни сертификати силно се насърчава.

Независимо дали издателят реши да използва HSM или не, би трябвало да бъде въведен график за подновяване на ключовете, при който честотата на подновяване е пропорционална на излагането на ключовете във външни мрежи, други системи или персонал. Добре избраният график за подновяване на ключовете също така ограничава рисковете, свързани с погрешно издадени здравни сертификати, като дава възможност на издателя да отмени такива сертификати на партиди, като оттегли даден ключ, ако е необходимо.

7.3. *Потвърждаване на входните данни*

Настоящите спецификации може да се използват по начин, който предполага получаването на данни от ненадеждни източници в системи, които може да са от критично значение. За да се ограничат рисковете, свързани с такива атаки, всички полета за входни данни трябва да бъдат правилно валидирани по типове данни, дължина и съдържание. Подписът на издателя следва също да бъде проверен, преди да се извърши обработване на съдържанието на HCERT. Валидирането на подписа на издателя обаче предполага извършването на синтактичен анализ първо на защитената заглавна част на издателя, в която потенциален нападател може да опита да инжектира внимателно изработена информация с цел да компрометира сигурността на системата.

8. **Управление на доверието**

За проверка на подписа на HCERT е необходим публичен ключ. Тези публични ключове се осигуряват от държавите членки. В крайна сметка всеки проверяващ орган трябва да разполага със списък на всички публични ключове, на които е решил да се довери (тъй като публичният ключ не е част от HCERT).

Системата се състои от (само) два слоя; за всяка държава членка — един или няколко сертификата на ниво държава, като всеки подписва един или няколко сертификата на подписващия документи орган, използвани в ежедневни операции.

Сертификатите на държавите членки се наричат сертификати на националните подписващи сертификати органи (CSCA) и (обикновено) са самоподписващи се. Държавите членки може да имат повече от един (например в случай на регионално самоуправление). Тези сертификати на CSCA редовно подписват сертификатите на подписващия документи орган (DSC), използвани за подписване на HCERT.

„Секретариатът“ има функционална роля. Той следва редовно да обобщава и публикува DSC на държавите членки, след като ги е потвърдил в списъка със сертификати на CSCA (който е предаден и потвърден чрез други средства).

Полученият списък с DSC след това следва да предостави обобщен набор от допустими публични ключове (както и съответстващите kid), който проверяващите органи могат да използват за валидиране на подписите в HCERT. Проверяващите органи трябва редовно да се сдобиват с този списък и да го актуализират.

Такива списъци, които са конкретни за държавите членки, може да бъдат адаптирани във формата, съответстващ на националните им условия. Така форматът на файла на този доверителен списък може да се различава. Например може да бъде подписан JWKS (формат на JWK набор според раздел 5 на RFC 7517 ([11])) или друг формат, който е конкретен за технологията, използвана от съответната държава членка.

За да се осигури опростеност, държавите членки може да изпращат съществуващите си сертификати на CSCA от своите системи за еМЧДП на ИКАО или, както препоръчва СЗО, да създадат такъв конкретно за тази здравна сфера.

8.1. *Идентификатор на ключ (kid)*

Идентификаторът на ключ (kid) се изчислява при изграждането на списъка с доверени публични ключове от DSC и се състои от съкратен отпечатък SHA-256 (първите 8 байта) на DSC, кодиран в DER формат (непреработен).

Проверяващите органи не се налага да изчисляват kid на базата на DSC и могат директно да съпоставят идентификатора на ключа в издадения здравен сертификат с kid в доверителния списък.

8.2. *Разлики в доверителния модел на инфраструктурата на публичния ключ (PKI) за еМЧДП на ИКАО*

Въпреки че за модел са използвани най-добри практики на доверителния модел на инфраструктурата на публичния ключ (PKI) за еМЧДП на ИКАО, ще бъдат извършени няколко опростявания с оглед на скоростта:

— Държава членка може да изпраща няколко сертификата на CSCA.

— Срокът на валидност на DSC (използване на ключа) може да бъде зададен за всякаква продължителност, без да надхвърля валидността на сертификата на CSCA, и може да липсва.

— DSC може да съдържа идентификатори на политика (удължено използване на ключа), конкретни за здравните сертификати.

— Държавите членки може да изберат никога да не извършват проверка на публикувани оттегляния; но вместо това изцяло да разчитат на списъците с DSC, които получават ежедневно от Секретариата, или да ги съставят самостоятелно.

([11]) rfc7517 (ietf.org)

ПРИЛОЖЕНИЕ II

ПРАВИЛА ЗА ПОПЪЛВАНЕТО НА ЦИФРОВИЯ COVID СЕРТИФИКАТ НА ЕС

Общите правила, свързани с наборите от стойности, определени в настоящото приложение, имат за цел да осигурят оперативната съвместимост на семантично ниво и следва да дадат възможност за единни технически изпълнения на DCC. Елементи, съдържащи се в настоящото приложение, може да се използват за трите различни настройки (ваксинация/направено изследване/преболедуване), както е определено в Регламент (ЕС) 2021/953. В настоящото приложение са посочени само елементи с необходимост от семантична стандартизация посредством набори от кодирани стойности.

Преводът на кодираните елементи на националния език е отговорност на държавите членки.

За всички полета с данни, които не са споменати в следните описания на набори от стойности, се препоръчва кодиране в UTF-8 (име, център за изследване, издател на сертификата). Препоръчва се полетата с данни, съдържащи календарни дати (дата на раждане, дата на ваксинация, дата на вземане на проба за изследване, дата на първия положителен резултат от изследването, дати на валидност на сертификата), да бъдат кодирани съгласно ISO 8601.

Ако поради някаква причина предпочитаните кодови системи, посочени по-долу, не могат да бъдат използвани, може да се използват други международни кодови системи и да се разработят съвети за намиране на съответствие на кодовете от другите кодови системи с кодовете в предпочитаната. Текст (показвани имена) може да се използва в изключителни случаи като резервен механизъм, когато не е наличен подходящ код в определените набори от стойности.

Държавите членки, използващи друго кодиране в системите си, трябва да намерят съответствие на тези кодове в описаните набори от стойности. Държавите членки отговарят за всяко такова намиране на съответствие.

Наборите от стойности ще се актуализират редовно от Комисията с помощта на мрежата за електронно здравеопазване и на Комитета за здравна сигурност. Актуализираните набори от стойности ще се публикуват на съответния уебсайт на Комисията, както и на уеб страницата на мрежата за електронно здравеопазване. Следва да се предостави хронология на промените.

1. **Заболяване или патоген/заболяване или патоген, което/който притежателят е преболедувал: COVID-19 (SARS-CoV-2 или някой от неговите варианти)**

   Предпочитана система за кодиране: SNOMED CT.

   Да се използва в сертификати 1, 2 и 3.

   Избраните кодове ще се отнасят за COVID-19 или, ако е необходима по-подробна информация за генетичния вариант на SARS-COV-2 — за тези варианти, ако е нужна толкова подробна информация по епидемиологични причини.

   Примерен код, който следва да се използва, е кодът SNOMED CT 840539006 (COVID-19).

2. **Ваксина срещу COVID-19 или профилактика**

   Предпочитана система за кодиране: SNOMED CT или ATC класификация.

   Да се използва в сертификат 1.

   Примерни кодове, които следва да се използват от предпочитаните системи за кодиране, са кодът SNOMED CT 1119305005 (SARS-CoV-2 антигенна ваксина), 1119349007 (SARS-CoV-2 иРНК ваксина) или J07BX03 (covid-19 ваксини). Наборът от стойности трябва да бъде разширен, когато бъдат разработени и въведени в употреба нови типове ваксини.

3. **Ваксинационен лекарствен продукт срещу COVID-19**

   Предпочитани системи за кодиране (по ред на предпочитание):

   — Регистър на лекарствените продукти на Съюза за ваксини с разрешение за целия ЕС (номера на разрешенията)

   — Глобален регистър на ваксините, например такъв, който би могъл да бъде въведен от Световната здравна организация

   — Име на ваксинационния лекарствен продукт в други случаи. Ако името включва интервали, те трябва да бъдат заменени от тире (-).

Име на набора от стойности: Ваксина.

Да се използва в сертификат 1.

Пример на код, който трябва да се използва от предпочитаната система за кодиране, е EC/1/20/1528 (Comirnaty). Пример на името на ваксината, което да се използва като код: Sputnik-V (за Sputnik V).

4. **Притежател на разрешението за търговия или производител на ваксината срещу COVID-19**

Предпочитана система за кодиране:

— Код на организацията от EMA (система SPOR за ISO IDMP)

— Глобален регистър на притежателите на разрешението за търговия или производителите на ваксината, например такъв, който би могъл да бъде въведен от Световната здравна организация

— Име на организацията в други случаи. Ако името включва интервали, те трябва да бъдат заменени от тире (-).

Да се използва в сертификат 1.

Пример на код, който трябва да се използва от предпочитаната система за кодиране, е ORG-100001699 (AstraZeneca AB). Примерно име на организацията, което да се използва като код: Sinovac-Biotech (за Sinovac Biotech).

5. **Пореден номер при серия от дози, както и общ брой на дозите в серията**

Да се използва в сертификат 1.

Две полета:

(1) Брой дози, поставени в един цикъл

(2) Брой очаквани дози за пълен цикъл (конкретно за дадено лице в момента на поставяне)

Например 1/1, 2/2 ще бъде представено като завършено; включително опцията 1/1 за ваксини, включващи две дози, но за които приложеният протокол от държавата членка е да се постави една доза на лица, диагностицирани с COVID-19 преди ваксинацията. Общият брой на дозите в серията трябва да бъде посочен в съответствие с наличната информация към момента на поставяне на дозата. Ако например конкретна ваксина изисква трето поставяне (стимулатор) към момента на последната поставена ваксина, второто поле за номер ще отразява това (например 2/3, 3/3 и т.н.).

6. **Държава членка или трета държава, в която е поставена ваксината/в която е направено изследването**

Предпочитана система за кодиране: Кодовете на държавите по ISO 3166

Да се използват в сертификати 1, 2 и 3.

Съдържание на набора от стойности: пълният списък от двубуквени кодове, налични като набор от стойности, определен в Ресурсите за бърза оперативна съвместимост в здравеопазването (FHIR) (http://hl7.org/fhir/ValueSet/iso3166-1-2)

7. **Вид на теста**

Предпочитана система за кодиране: LOINC.

Да се използва в сертификат 2 и сертификат 3, ако чрез делегиран акт е въведена възможност за издаването на сертификати за преболедуване въз основа на вида на изследването или теста, различен от NAAT.

Кодовете в този набор от стойности ще се отнасят за начина на извършване на изследването или теста и ще бъдат избрани поне за да разделят изследванията NAAT от изследванията RAT, както е изразено в Регламент (ЕС) 2021/953.

Пример на код, който следва да се използва от предпочитаната система за кодиране, е LP217198-3 (бърз имуноанализ).

8. **Производител и търговско наименование на използван тест (незадължително за изследване NAAT)**

Предпочитана система за кодиране: Списък от КЗС на бързи тестове за антигени, поддържани от JRC (база данни за ин витро диагностични изделия и методи за изпитване, свързани с COVID-19)

Да се използва в сертификат 2.

Съдържанието на набора от стойности ще включва избора на бърз тест за антигени, както е посочен в общия и актуализиран списък на бързи тестове за антигени за COVID-19, определен на базата на Препоръка на Съвета 2021/C 24/01 и одобрен от Комитета за здравна сигурност. Списъкът се поддържа от JRC в базата данни за ин витро диагностични изделия и методи за изпитване, свързани с COVID-19, на адрес: https://covid-19-diagnostics.jrc.ec.europa.eu/devices/hsc-common-recognition-rat

За тази кодова система се използват съответните полета, като идентификаторът на медицинското изделие за извършване на изследването, името на теста и производителя, в съответствие с наличния структуриран от JRC формат на https://covid-19-diagnostics.jrc.ec.europa.eu/devices

9. **Резултат от изследването или теста**

Предпочитана система за кодиране: SNOMED CT.

Да се използва в сертификат 2.

Избраните кодове следва да позволяват разграничаването между положителни и отрицателни резултати от изследването (положителна или отрицателна проба). Допълнителни стойности (като неопределена проба) може да бъдат добавени, ако случаите на използване го изискват.

Примерни кодове, които следва да се използват от предпочитаната система за кодиране, са 260415000 (отрицателна проба) и 260373001 (положителна проба).

ПРИЛОЖЕНИЕ III

ОБЩА СТРУКТУРА НА УНИКАЛНИЯ ИДЕНТИФИКАТОР НА СЕРТИФИКАТА

1. **Увод**

Всеки Цифров COVID сертификат на ЕС (DCC) ще включва уникален идентификатор на сертификата (УИС), който поддържа оперативната съвместимост на DCC. УИС може да се използва за проверка на сертификата. Държавите членки са отговорни за внедряването на УИС. УИС е средство за проверка на достоверността на сертификата, и където е приложимо — за свързване с регистрационна система (например с ИИС). Тези идентификатори също така ще активират удостоверения (хартиени и цифрови) от страна на държавите членки, че лицата са били ваксинирани или тествани.

2. **Съдържание на уникалния идентификатор на сертификата**

УИС ще следва обща структура и формат, които улесняват човешкото и/или машинното интерпретиране на информацията, и може да се отнася до такива елементи като държава членка на ваксинация, самата ваксина и конкретния идентификатор на държавата членка. Той предоставя гъвкавост на държавата членка да го форматира при пълно спазване на законодателството за защита на личните данни. Редът на отделните елементи следва определена йерархия, която може да даде възможност за бъдещи модификации на блоковете, като в същото време поддържа целостта на структурата.

Възможните решения за съдържанието на УИС са в спектър, в който модулността и човешкото интерпретиране са двата основни разграничаващи параметъра и една основополагаща характеристика:

— Модулност: степента, до която кодът е съставен от отделни блокове, съдържащи семантично различна информация

— Човешко интерпретиране: степента, до която кодът е смислен или може да бъде интерпретиран от прочитащия го човек

— Уникален в глобален мащаб; Идентификаторът на държавата или органа се управлява добре; и всяка държава (орган) се очаква да управлява добре своя сегмент от пространството от имена, като никога не рециклира или използва повторно идентификаторите. В комбинация тези мерки осигуряват уникалността на всеки идентификатор в глобален мащаб.

3. **Общи изисквания**

Следните основни изисквания следва да спазени във връзка с УИС:

(1) Набор от знаци: Допускат се само US-ASCII главни буквено-цифрови знаци (от A до Z, от 0 до 9); с допълнителни специални знаци за отделяне от RFC3986 ([1]) ([2]), по-конкретно {„/“, „#“, „:“};

(2) Максимална дължина: разработчиците следва да се стремят към дължина от 27—30 знака ([3]);

(3) Представка за версията: това се отнася до версията на схемата на УИС. Представката за версията е „01“ за настоящата версия на документа; представката за версията се състои от две цифри;

(4) Представка за държавата: кодът на държавата е определен от ISO 3166-1. По-дългите кодове (напр. с 3 или повече знака (например „UNHCR“) са запазени за бъдеща употреба;

(5) Наставка на кода/Контролна сума:

5.1. Държавите членки използват контролна сума, когато има вероятност от възникване на пренос, (човешка) транскрипция или друг вид увреждане (когато се използва в печатна форма).

5.2. Не бива да се разчита на контролната сума за потвърждаване на сертификата, нито пък тя е технически част от идентификатора, а се използва за проверка на целостта на кода. Тази контролна сума следва да бъде обобщената информация ISO-7812-1 (LUHN-10) ([4]) на целия УИС в цифров формат/формат за жичен пренос. Контролната сума се разделя от останалата част на УИС със знак „#“.

([1]) rfc3986 (ietf.org)

([2]) Полета като „Пол“, „Номер на партида“, „Център на поставяне“, „Здравна професионална идентификация“, „Дата на следваща ваксинация“ може да не са необходими за цели, които не са медицински.

([3]) За прилагането с QR кодове държавите членки може да обмислят набор от знаци с обща дължина до 72 знака (включително набора от 27—30 знака на самия идентификатор), който може да се използва за предаване на друга информация. Спецификацията на тази информация следва да се определи от държавата членка.

([4]) Алгоритъмът Luhn mod N е разширение на алгоритъма Luhn (известен още като алгоритъм mod 10), който работи за цифрови кодове и се използва например за изчисление на контролната сума на кредитни карти. Разширението позволява на алгоритъма да работи с поредици от стойности във всяка база (в нашия случай — буквени знаци).

Следва да се осигури обратна съвместимост: Държавите членки, които с течение на времето променят структурата на идентификаторите си (в рамките на основната версия, понастоящем зададена на v1), трябва да направят така, че всеки два идентични идентификатора да представляват един и същ сертификат/удостоверение за ваксинация. Или, с други думи, държавите членки не могат да рециклират идентификаторите.

4. **Опции за уникални идентификатори на сертификати за сертификати за ваксинация**

Насоките на мрежата за електронно здравеопазване за сертификатите за ваксинация с възможност за потвърждаване и основните елементи на оперативната съвместимост ([5]) предоставят различни опции на държавите членки и на други страни, които може да съществуват заедно сред различните държави членки. Държавите членки може да използват такива различни опции в друга версия на схемата на УИС.

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

ПРИЛОЖЕНИЕ IV

УПРАВЛЕНИЕ НА СЕРТИФИКАТИ НА ПУБЛИЧНИ КЛЮЧОВЕ

1. **Увод**

Сигурната и надеждна обмяна на ключове за подпис за Цифровите COVID сертификати на ЕС (DCC) между държавите членки се осъществява от портала на Цифровия COVID сертификат на ЕС (DCCG), който действа като централен архив за публичните ключове. В DCCG държавите членки са упълномощени да публикуват публичните ключове, отговарящи на частните ключове, които използват за подписване на цифрови сертификати за COVID. Държавите членки, които разчитат на DCCG за това, могат своевременно да се сдобиват с актуализирани публични ключове. По-късно DCCG може да бъде разширен, за да включва обмяната на надеждна допълнителна информация, предоставяна от държавите членки, като например правила за валидиране на DCC. Доверителния модел на рамката на DCC е инфраструктура на публичния ключ (PKI). Всяка държава членка поддържа един или няколко национални подписващи сертификати органи (CSCA), чиито сертификати са сравнително дългосрочни. Съгласно решението на държавата членка CSCA може да бъде същия или различен от CSCA, използван за машинночетими пътнически документи. CSCA издава удостоверения за публичен ключ за националните, краткосрочни, подписващи документите органи (т.е. подписващи за DCC), които се наричат сертификати на подписващия документи орган (DSC). CSCA действа като котва на доверие, така че разчитащите на него държави членки могат да използват сертификата на CSCA за валидиране на автентичността и целостта на редовно променящите се DSC. След като ги потвърдят, държавите членки могат да предоставят тези сертификати (или само съдържащите се в тях публични ключове) на приложенията си за валидиране на DCC. Освен на CSCA и DSC, DCCG разчита и на PKI, за да установява автентичността на трансакции, да подписва данни като основа за установяване на автентичността и като средство за осигуряване целостта на комуникационните канали между държавите членки и DCCG.

Цифровите подписи могат да се използват за постигане на цялостност и автентичност на данните. Инфраструктурите на публичните ключове създават доверие, като свързват публичните ключове с проверени идентичности (или издатели). Това е необходимо, за да се позволи на други участници да проверяват произхода на данните и идентичността на комуникационния партньор и да вземат решения относно доверието. В DCCG се използват редица удостоверения за публичен ключ за автентичност. Настоящото приложение определя кои удостоверения за публичен ключ да се използват и как дизайнът им да позволява широка оперативна съвместимост сред държавите членки. То предоставя повече подробности за необходимите удостоверения за публичен ключ и дава указания за шаблоните на удостоверенията и срока им на валидност за държавите членки, които искат да оперират собствен CSCA. Тъй като DCC ще могат да бъдат проверявани за определен период от време (който започва от издаването и изтича след определено време), е необходимо да се определи модел на проверка за всички подписи, прилагани в удостоверенията за публичен ключ и в DCC.

2. **Терминология**

Следващата таблица съдържа съкращения и терминология, използвани в настоящото Приложение.

Термин	Определение
Удостоверение	или удостоверение за публичен ключ. Удостоверение X.509 v3, което съдържа публичния ключ на организация
CSCA	Национален подписващ сертификати орган
DCC	Цифров COVID сертификат на ЕС. Подписан цифров документ, който съдържа информация за ваксинация, тест или преболедуване
DCCG	Портал за Цифровия COVID сертификат на ЕС. Тази система се използва за обмяна на DSC между държавите членки
$DCCG_{TA}$	Сертификатът на котвата на доверие на DCCG. Съответстващият частен ключ се използва за подписване на списъка на всички сертификати на CSCA офлайн
$DCCG_{TLS}$	Сертификатът на TLS сървъра на DCCG
DSC	Сертификат на подписващия документи орган. Удостоверението за публичен ключ на подписващия документи орган на държава членка (например система, която има право да подписва DCC). Този сертификат се издава от CSCA на държавата членка
EC-DSA	Алгоритъм за електронни подписи по елиптична крива. Алгоритъм за криптографски подпис, основан на елиптични криви
Държава членка	Държава — членка на Европейския съюз

Термин	Определение
mTLS	Взаимен TLS. Протоколът за сигурност на транспортния слой с взаимна автентификация
NB	Национален бек-енд на държава членка
NB_{CSCA}	Сертификатът на CSCA на държава членка (може да е повече от един)
NB_{TLS}	TLS клиентски сертификат за автентификация на национален бек-енд
NB_{UP}	Сертификатът, използван от национален бек-енд за подписване на пакети от данни, които се качват в DCCG
PKI	Инфраструктура на публичния ключ (PKI). Доверителен модел, основан на удостоверения на публичен ключ и органи за издаване на сертификати
RSA	Асиметричен криптографски механизъм, базиран на факторизация на цели числа, използван за цифрови подписи или асиметрично криптиране

3. **Дефекти в комуникацията на DCCG и услуги по сигурността**

Настоящият раздел съдържа общ преглед на дефектите в комуникацията и услугите по сигурността на системата на DCCG. Тук също така се определя кои ключове и сертификати се използват за защита на комуникацията, качената информация, DCC и подписания доверителен списък, който съдържа всички приети сертификати на CSCA. DCCG работи като център за данни, който позволява обмяната на подписани пакети от данни за държави членки.

Качените пакети от данни се предоставят от DCCG във вида, в който са. Това означава, че DCCG не добавя, нито изтрива DSC от пакетите, които получава. Националният бек-енд (*NB*) на държава членка трябва да може да проверява целостта и автентичността на качените данни от край до край. В допълнение към това националните бек-ендове и DCCG ще използват взаимна TLS автентификация за създаването на сигурна връзка. Това е в допълнение към подписите в обменяните данни.

3.1. *Автентификация и създаване на връзка*

DCCG използва сигурност на транспортния слой (TLS) с взаимно автентификация, за да създаде автентифициран криптиран канал между националния бек-енд (*NB*) на държава членка и средата на портала. Ето защо DCCG притежава TLS сървърен сертификат — съкратено $DCCG_{TLS}$, а националните бек-ендове притежават TLS клиентски сертификати — съкратено NB_{TLS}. Шаблоните на сертификатите са предоставени в *раздел 5*. Всеки национален бек-енд може да предоставя собствен TLS сертификат. Този сертификат ще бъде отбелязан изрично в разрешения списък и така може да бъде издаван от публично доверен сертифициращ орган (например сертифициращ орган, който спазва основните изисквания на CA/Browser Forum), от национални сертифициращи органи или може да е самоподписан. Всяка държава членка е отговорна за националните си данни и защитата на частния ключ, използван за установяване на връзката към DCCG. Подходът от типа „носете си собствен сертификат“ изисква добре определен процес на регистрация и идентифициране, както и процедури за отмяна и подновяване, както са описани в *секции 4.1, 4.2* и *4.3*. DCCG използва разрешен списък, в който TLS сертификатите на националните бек-енд се добавят след успешната им регистрация. Само национални бек-ендове, които се автентифицират с частен ключ, съответстващ на сертификат от разрешения списък, могат да установят сигурна връзка към DCCG. DCCG също така използва TLS сертификат, който позволява на националните бек-ендове да проверяват дали наистина установяват връзка с „истинския“ DCCG, а не със злонамерена организация, представяща се за DCCG. Сертификатът на DCCG ще бъде представен на *NB* след успешна регистрация. $DCCG_{TLS}$ сертификатът ще бъде издаден от публично доверен сертифициращ орган (включен във всички основни браузъри). Държавите членки носят отговорност да проверяват сигурността на връзката си с DCCG (например като проверяват отпечатъка на $DCCG_{TLS}$ сертификата на сървъра, с който са свързани, спрямо този, предоставен след регистрацията).

3.2. *Национални подписващи сертификати органи и модел на валидиране*

Държавите членки, които взимат участие в рамката на DCCG, трябва да използват CSCA за издаването на DSC. Държавите членки може да имат повече от един CSCA, например в случай на регионална децентрализация. Всяка държава членка може да използва съществуващи сертификационни органи или да създаде специален орган за издаване на (по възможност самоподписани) сертификати за системата на DCC.

Държавите членки трябва да представят сертификата/сертификатите на CSCA на оператора на DCCG по време на официалната процедура по присъединяване. След успешната регистрация на държавата членка (*вижте раздел 4.1 за повече информация*) операторът на DCCG ще актуализира подписан доверителен списък, съдържащ всички сертификати на CSCA, активни в рамката на DCC. Операторът на DCCG ще използва специална двойка асиметрични ключове за подписване на доверителния списък и на сертификатите в офлайн среда. Частният ключ няма да се съхранява в онлайн системата на DCCG, така че компрометиране на онлайн системата да не даде възможност на нападател да компрометира доверителния списък. Съответстващият сертификат на котвата на доверие $DCCG_{TA}$ ще бъде предоставен на националните бек-ендове по време на процеса на присъединяване.

Държавите членки могат да получат доверителния списък от DCCG за целите на процедурите си по проверка. CSCA се определя като сертифициращ орган, който издава DSC, като затова държавите членки, които използват многостепенна йерархия на сертифициращия орган (например основен сертифициращ орган -> CSCA -> DSC), трябва да предоставят информация за подчинения сертифициращ орган, който издава DSC. В такъв случай, ако се използва съществуващ сертифициращ орган, то системата на DCC ще игнорира всичко над CSCA и ще постави в разрешения списък само CSCA като котва на доверие (въпреки че е подчинен сертифициращ орган). Това е като модела на ИКАО, който допуска само 2 нива — основен CSCA и подчинен DSC, подписан точно от този CSCA.

В случай че държава членка оперира собствен CSCA, тя носи отговорност за сигурната работа и управлението на ключовете на този сертифициращ орган. CSCA действа като котва на доверие за DSC, така че защитата на частния ключ на CSCA е от съществено значение за целостта на средата на DCC. Моделът на проверка в PKI на DCC представлява обвивка, която посочва, че всички сертификати, присъстващи в пътя на сертификата, трябва да са валидни в даден момент (тоест в момента на валидиране на подписа). Ето защо са в сила следните ограничения:

— CSCA не издава сертификати, които са с по-продължителна валидност от самия сертификат на сертифициращия орган.

— Подписващият орган не подписва документи, които са с по-продължителна валидност от самия DSC.

— Държавите членки, които оперират собствен CSCA, трябва да определят срокове на валидност за своите CSCA, както и за всички издавани сертификати, и трябва да се погрижат за подновяването на сертификатите.

Раздел 4.2 съдържа препоръки за сроковете на валидност.

3.3. *Цялостност и автентичност на качените данни*

Националните бек-ендове могат да използват DCCG, за да качват и изтеглят цифрово подписани пакети от данни след успешна взаимна автентификация. В началото тези пакети от данни съдържат DSC на държавите членки. Двойката ключове, използвана от националния бек-енд за цифрово подписване на качени пакети от данни в системата на DCCG, се нарича двойка ключове за подписване на качените от националния бек-енд данни, а съответното удостоверение за публичен ключ се съкращава като NB_{UP} сертификат. Всяка държава членка осигурява свой собствен NB_{UP} сертификат, който може да е самоподписан или издаден от съществуващ сертифициращ орган, като например обществен сертифициращ орган (т.е. сертифициращ орган, който издава сертификати в съответствие с основните изисквания на CAB-Forum). NB_{UP} сертификатът се различава от всички други сертификати, издавани от държавата членка (напр. CSCA, TLS клиент или DSC).

Държавите членки трябва да предостави сертификата за качване на оператора на DCCG по време на първоначалната процедура по регистрация (*вижте раздел 4.1 за повече подробности*). Всяка държава членка носи отговорност за националните си данни и трябва да защитава частния ключ, използван за подписване на качените данни.

Други държави членки могат да проверяват подписаните пакети от данни, използвайки качени сертификати, предоставени от DCCG. DCCG проверява автентичността и целостта на качените данни със сертификат на *NB* за качване, преди да ги предостави на други държави членки.

3.4. *Изисквания за техническата архитектура на DCCG*

Изискванията за техническата архитектура на DCCG са, както следва:

— DCCG използва взаимна TLS автентификация, за да установи автентифицирана криптирана връзка с *NB*. Ето защо DCCG поддържа разрешен списък с регистрирани NB_{TLS} клиентски сертификати.

— DCCG използва два цифрови сертификата ($DCCG_{TLS}$ и $DCCG_{TA}$) с две различни двойки ключове. Частният ключ на двойката ключове на $DCCG_{TA}$ се поддържа офлайн (а не в онлайн компонентите на DCCG).

— DCCG поддържа доверителен списък на NB_{CSCA} сертификатите, подписани с частния ключ на $DCCG_{TA}$.

— Използваните шифри трябва да отговарят на изискванията в *раздел 5.1*.

4. **Управление на жизнения цикъл на сертификатите**

4.1. *Регистрация на националните бек-ендове*

Държавите членки трябва да се регистрират в оператора на DCCG, за да участват в системата на DCCG. В настоящия раздел се описва техническата и оперативна процедура, която трябва да се спазва при регистрация на национален бек-енд.

Операторът на DCCG и държавата членка трябва да обменят информация за техническите лица за връзка за процеса на присъединяване. Приема се, че техническите лица за връзка са легитимирани от съответните си държави членки и е извършено идентифициране/потвърждаване на самоличността посредством други канали. Например потвърждаването на самоличността може да се извърши, когато техническото лице за връзка на държавата членка предоставя сертификатите като криптирани с парола файлове посредством имейл и споделя съответната парола с оператора на DCCG по телефона. Могат да се използват и други сигурни канали, определени от оператора на DCCG.

Държавата членка трябва да предостави три цифрови сертификата по време на процеса на регистрация и идентификация:

— TLS сертификата на държавата членка, NB_{TLS}

— Сертификата за качване на държавата членка, NB_{UP}

— Сертификата/сертификатите на CSCA на държавата членка, NBC_{SCA}

Всички предоставени сертификати трябва да спазват изискванията, определени в *раздел 5*. Операторът на DCCG ще провери дали предоставеният сертификат спазва изискванията на *раздел 5*. След идентифицирането и регистрацията операторът на DCCG:

— добавя сертификата/сертификатите NB_{CSCA} към доверителния списък, подписан с частния ключ, който съответства на публичния ключ $DCCG_{TA}$;

— добавя сертификата NB_{TLS} към разрешения списък в крайната точка на TLS на DCCG;

— добавя сертификата NB_{UP} в системата на DCCG;

— предоставя удостоверенията за публичен ключ $DCCG_{TA}$ и $DCCG_{TLS}$ на държавата членка.

4.2. *Сертифициращи органи, срокове на валидност и подновяване*

В случай че държава членка иска да оперира собствен CSCA, сертификатите на CSCA може да са самоподписани. Те действат като котва на доверие на държавата членка и следователно тя трябва надеждно да защитава частния ключ, съответстващ на публичния ключ на сертификата на CSCA. Препоръчително е държавата членка да използва офлайн система за своя CSCA, т.е. компютърна система, която не е свързана към мрежа. Следва да се използва контрол от няколко лица за достъп до системата (например като се следва принципът на четирите очи). След подписване на DSC се прилагат оперативни проверки и системата, която съдържа частния ключ на CSCA, се съхранява на сигурно място с надежден контрол над достъп. Могат да се използват хардуерни модули за сигурност или смарт карти за допълнителна защита на частния ключ на CSCA. Цифровите сертификати съдържат срок на валидност, който налага подновяване на сертификатите. За подновяването трябва да се използват нови криптографски ключове и да се адаптират размерите им към новите подобрения в изчисляването или към новите атаки, застрашаващи сигурността на използвания криптографски алгоритъм. Прилага се моделът на обвивка (виж *раздел 3.2*).

Препоръчват се следните срокове на валидност предвид предоставената едногодишна валидност на цифровите сертификати за COVID:

— CSCA: 4 години

— DSC: 2 години

— Качване: 1 — 2 години

— Автентификация на TLS клиент: 1 — 2 години

За навременно подновяване се препоръчват следните срокове на използване за частните ключове:

— CSCA: 1 година

— DSC: 6 месеца

Държавите членки трябва навреме да създадат нови сертификати за качване и TLS сертификати, например един месец преди изтичането, за да се осигури безпроблемна работа. Сертификатите на CSCA и DSC следва да бъдат подновявани поне един месец преди края на срока на използване на частния ключ (предвид необходимите оперативни процедури). Държавите членки трябва да предоставят актуализирани сертификати на CSCA, сертификати за качване и TLS сертификати на оператора на DCCG. Изтеклите сертификати се премахват разрешения списък и доверителния списък.

Държавите членки и операторът на DCCG трябва да следят за валидността на собствените си сертификати. Няма централно звено, което поддържа справка за валидността на сертификатите и информира участниците.

4.3. *Отмяна на удостоверения*

Като цяло цифровите сертификати могат да се отменят от издаващия ги сертифициращ орган посредством списъци на отменени сертификати или услуга за онлайн протокол за състояние на сертификат (OCSP). CSCA за системата на DCC следва да предоставя списъци на отменени сертификати (CRL). Дори ако тези CRL понастоящем не се използват от други държави членки, те следва да бъдат внедрени за бъдещи приложения. В случай че CSCA реши да не предоставя CRL, DSC на този CSCA трябва да бъдат подновени, когато CRL станат задължителни. Проверяващите органи не следва да използват OCSP за валидиране на DSC, а следва да използват CRL. Препоръчително е националните бек-ендове да извършват необходимото валидиране на DSC, изтегляни от портала за DCC, и да препращат само набор от доверени и валидирани DSC към националните валидиращи органи за DCC. Валидиращите органи за DCC не следва да извършват проверка за отмяна на DSC в процеса си на валидиране. Една от причините за това е да се защити поверителността на притежателите на DCC, като се избягва рискът употребата на конкретен DSC да се следи от свързаната с него OCSP услуга.

Държавите членки могат да премахват самостоятелно своите DSC от DCCG, използвайки валидни сертификати за качване и TLS сертификати. Премахването на DSC означава, че всички DCC, издадени с него, ще станат невалидни, когато държавите членки се сдобият с актуализираните списъци на DSC. Защитата на частния ключ, съответстващ на DSC, е от решаващо значение. Държавите членки трябва да информират оператора на DCCG, когато те трябва да отменят сертификати за качване или сертификати TLS, например поради компрометиране на националния бек-енд. Операторът на DCCG тогава може да премахне доверието от засегнатия сертификат, например като го премахне от разрешения списък за TLS. Операторът на DCCG може да премахва сертификати за качване от базата данни на DCCG. Пакети, подписани с частния ключ, съответстващ на този сертификат за качване, ще станат невалидни, когато националните бек-ендове премахнат доверието от отменения сертификат за качване. В случай че трябва да бъде отменен сертификат на CSCA, държавите членки информират оператора на DCCG, както и другите държави членки, с които имат доверителни отношения. Операторът на DCC ще издаде нов доверителен списък, който вече не съдържа засегнатия сертификат. Всички DSC, издадени от този CSCA, ще станат невалидни, когато държавите членки актуализират доверителното хранилище на националния си бек-енд. В случай че трябва да бъде отменен сертификатът $DCCG_{TLS}$ или сертификатът $DCCG_{TA}$, операторът на DCCG и държавите членки трябва да работят заедно, за да установят нова TLS доверителна връзка и доверителен списък.

5. **Шаблони на сертификати**

В настоящия раздел се разглеждат криптографските изисквания и насоки, както и изискванията за шаблоните на сертификатите. За сертификатите на DCCG настоящия раздел определя шаблоните на сертификатите.

5.1. *Криптографски изисквания*

Криптографските алгоритми и поредиците от TLS шифри се избират на базата на текущата препоръка от Германската федерална служба за сигурност на информацията (BSI) или SOG-IS. Тези препоръки и препоръките на други институции и организации за стандартизация са подобни. Препоръките могат да бъдат намерени в техническите ръководства TR 02102-1 и TR 02102-2 ([1]) или в Договорените криптографски механизми на SOG-IS ([2]).

5.1.1. Изисквания за DSC

Прилагат се изискванията от *приложение I, раздел 3.2.2*. Ето защо е силно препоръчително подписващите органи да използват алгоритъм за електронни подписи по елиптична крива (ECDSA) с NIST-p-256 (както е посочено в допълнение Г към FIPS PUB 186-4). Други елиптични криви не се поддържат. Поради ограниченията за място в DCC държавите членки не следва да използват RSA-PSS, дори ако той е допустим като резервен алгоритъм. В случай

([1]) BSI — Техническо ръководство TR-02102 (bund.de)
([2]) SOG-IS — Поддържаща документация (sogis.eu)

че държавите членки, използват RSA-PSS, те следва да използват размер на модула от 2048 или не повече от 3072 бита. SHA-2 с изходна дължина ≥ 256 бита се използва като криптографска хеш-функция (вж. ISO/IEC 10118-3:2004) за подписа на DSC.

5.1.2. Изисквания към TLS сертификати, сертификати за качване и сертификати за CSCA

За цифрови сертификати и криптографски подписи в контекста на DCCG основните изисквания към криптографските алгоритми и дължината на ключовете са обобщени в следната таблица (от 2021 г.):

Алгоритъм за подпис	Размер на ключовете	Хешираща функция
EC-DSA	Мин. 250 бита	SHA-2 с дължина на изходната стойност ≥ 256 бита
RSA-PSS (препоръчително запълване) RSA-PKCS#1, v1.5 (наследено запълване)	RSA Модул (N) с мин. 3000 бита и с публичен експонент e > 2^16	SHA-2 с дължина на изходната стойност ≥ 256 бита
DSA	Просто число p с мин. 3000 бита, 250 бита ключ q	SHA-2 с дължина на изходната стойност ≥ 256 бита

Препоръчителната елиптична крива за EC-DSA е NIST-p-256 поради широко разпространеното ѝ внедряване.

5.2. *Сертификат на CSCA (NB_{CSCA})*

Следната таблица предоставя насоки за шаблона на сертификата NB_{CSCA}, ако държава членка реши да оперира собствен CSCA за DCC.

Запишете в **получер шрифт** са задължителни (трябва да бъдат включени в сертификата), а тези в *курсив* — препоръчителни (следва да бъдат включени). За отсъстващи полета не са определени препоръки.

Поле	Стойност
Субект	**cn= <не празно и уникално обикновено име>,** *o=<доставчик>,* **c=<държава членка, оперираща CSCA>**
Използване на ключа	**certificate signing,** *CRL signing* (като минимум)
Основни ограничения	**CA = true, path length constraints = 0**

Името на субекта трябва да бъде не празно и уникално в рамките на посочената държава членка. Кодът на държавата (c) трябва да съответства на държавата членка, която ще използва този сертификат на CSCA. Сертификатът трябва да съдържа уникален идентификатор на ключа на субекта (SKI) в съответствие с RFC 5280 ([3]).

5.3. *Сертификат на подписващия документи орган (DSC)*

В таблицата по-долу са дадени насоки относно DSC. Запишете в **получер шрифт** са задължителни (трябва да бъдат включени в сертификата), а тези в *курсив* — препоръчителни (следва да бъдат включени). За отсъстващи полета не са определени препоръки.

Поле	Стойност
Сериен номер	**уникален сериен номер**
Субект	**cn= <не празно и уникално обикновено име>,** *o=<доставчик>,* **c=<държава членка, използваща този DSC>**
Използване на ключа	**digital signature** (като минимум)

([3]) rfc5280 (ietf.org)

DSC трябва да бъде подписан с частен ключ, съответстващ на сертификата на CSCA, използван от държавата членка.

Трябва да се използват следните разширения:

— Сертификатът трябва да съдържа идентификатор на ключа на органа (AKI), съответстващ на идентификатора на ключа на субекта (SKI) на сертификата на издаващия CSCA;

— Сертификатът следва да съдържа уникален идентификатор на ключа на субекта (SKI) (в съответствие с RFC 5280 ([4])).

Освен това сертификатът следва да съдържа разширението на точката на разпределение на CRL, насочващо към списъка на отменени сертификати (CRL), предоставен от CSCA, издал DSC.

DSC може да съдържа разширение за разширено използване на ключовете с нула или повече идентификатори на политика за използване на ключовете, които ограничават типовете HCERT, които този сертификат има право да проверява. Ако е наличен един или повече, проверяващите органи проверят използването на ключа спрямо съхранения HCERT. За тази цел са определени следните стойности на разширеното използване на ключа:

Поле	Стойност
extendedKeyUsage	1.3.6.1.4.1.1847.2021.1.1 за издатели за тестове
extendedKeyUsage	1.3.6.1.4.1.1847.2021.1.2 за издатели за ваксинация
extendedKeyUsage	1.3.6.1.4.1.1847.2021.1.3 за издатели за възстановяване

Ако липсва разширение за използване на ключа (т.е. няма разширения или нула разширения), сертификатът може да се използва за валидиране на всеки тип HCERT. Други документи може да определят съответни допълнителни идентификатори на политика за разширено използване на ключовете, използвани при валидирането на HCERT.

5.4. *Сертификати за качване (NBUP)*

Следната таблица предоставя насоки за сертификата за качване на националните бек-ендове. Записите в **получер шрифт** са задължителни (трябва да бъдат включени в сертификата), а тези в *курсив* — препоръчителни (следва да бъдат включени). За отсъстващи полета не са определени препоръки.

Поле	Стойност
Субект	**cn= <не празно и уникално обикновено име>,** *o=<доставчик>,* **c=<държава членка, използваща този сертификат за качване>**
Използване на ключа	**digital signature** (като минимум)

5.5. *Автентификация на TLS клиент на национален бек-енд (NB_{TLS})*

Следната таблица предоставя насоки за TLS клиентски сертификат на национален бек-енд за автентификация. Записите в **получер шрифт** са задължителни (трябва да бъдат включени в сертификата), а тези в *курсив* — препоръчителни (следва да бъдат включени). За отсъстващи полета не са определени препоръки.

Поле	Стойност
Субект	**cn= <не празно и уникално обикновено име>,** *o=<доставчик>,* **c=<държава членка на *NB*>**
Използване на ключа	**digital signature** (като минимум)
Разширено използване на ключ	**автенитификация на клиента (1.3.6.1.5.5.7.3.2)**

([4]) rfc5280 (ietf.org)

Сертификатът може също да съдържа разширеното използване на ключ *сървърна автентификация (1.3.6.1.5.5.7.3.1*) за разширено използване на ключа, но това не е задължително.

5.6. *Сертификат за подпис на доверителен списък ($DCCG_{TA}$)*

Следната таблица определя сертификата на котвата на доверие на DCCG.

Поле	Стойност
Субект	**cn = Портал за цифров зелен сертификат** ([5]), **o=<доставчик>, c=<държава>**
Използване на ключа	**digital signature** (като минимум)

5.7. *TLS сървърни сертификати на DCCG ($DCCG_{TLS}$)*

Следната таблица определя TLS сертификата на DCCG.

Поле	Стойност
Субект	cn=<FQDN или IP адреса на DCCG>, o=<доставчик>, c=<държава>
SubjectAltName	dNSName: <име на DNS DCCG > или iPAddress: <IP адрес на DCCG>
Използване на ключа	**digital signature** (като минимум)
Разширено използване на ключа	**сървърна автентификация (1.3.6.1.5.5.7.3.1**)

Сертификатът може също да съдържа *клиентска автентификация (1.3.6.1.5.5.7.3.2*) за удължена употреба на ключа, но това не е задължително.

TLS сертификатът на DCCG се издава от публично доверен сертифициращ орган (включително във всички основни браузъри и операционни системи, като се спазват основните изисквания на CAB-Forum).

([5]) Терминът „цифров зелен сертификат“ вместо „цифров COVID сертификат на ЕС“ е запазен в този контекст, тъй като това е терминът, който е записан и използван в сертификата преди съзаконодателите да вземат решение относно нов термин.