PROVÁDĚCÍ ROZHODNUTÍ KOMISE (EU) 2021/1073

ze dne 28. června 2021,

kterým se stanoví technické specifikace a pravidla k provedení rámce pro důvěryhodnost pro digitální certifikát EU COVID stanoveného nařízením Evropského parlamentu a Rady (EU) 2021/953

(Text s významem pro EHP)

EVROPSKÁ KOMISE,

s ohledem na Smlouvu o fungování Evropské unie,

s ohledem na nařízení Evropského parlamentu a Rady (EU) 2021/953 o rámci pro vydávání, ověřování a uznávání interoperabilních certifikátů o očkování, o testu a o zotavení v souvislosti s onemocněním COVID-19 (digitální certifikát EU COVID) za účelem usnadnění volného pohybu během pandemie COVID-19 ([1]), a zejména na čl. 9 odst. 1 a 3 uvedeného nařízení,

vzhledem k těmto důvodům:

(1) Nařízení (EU) 2021/953 stanoví digitální certifikát EU COVID, který má sloužit jako doklad o tom, že dané osobě byla podána očkovací látka proti COVID-19, že měla negativní výsledek testu nebo že se z onemocnění zotavila.

(2) Aby digitální certifikát EU COVID fungoval v celé Unii, je nezbytné zavést technické specifikace a pravidla pro vyplňování, bezpečné vydávání a ověřování digitálních certifikátů COVID, zajištění ochrany osobních údajů, stanovení společné struktury jedinečného identifikátoru certifikátu a vydávání platného, bezpečného a interoperabilního čárového kódu. Rámec pro důvěryhodnost rovněž vytváří předpoklady pro snahu o zajištění interoperability s mezinárodními normami a technologickými systémy a jako takový by mohl poskytnout model pro spolupráci na celosvětové úrovni.

(3) K tomu, aby bylo možné číst a interpretovat digitální certifikát EU COVID, jsou zapotřebí společná datová struktura a dohoda na zamýšleném významu jednotlivých datových polí informačního obsahu a jejich možných hodnotách. K usnadnění této interoperability je nutné pro rámec pro digitální certifikát EU COVID definovat společnou koordinovanou datovou strukturu. Pokyny pro tento rámec vypracovala síť pro elektronické zdravotnictví zřízená na základě směrnice Evropského parlamentu a Rady 2011/24/EU ([2]). Tyto pokyny by měly být zohledněny při stanovení technických specifikací určujících formát a řízení důvěryhodnosti pro digitální certifikát EU COVID. Měla by být stanovena specifikace datové struktury a mechanismy kódování, jakož i mechanismus kódování při přenosu ve strojově čitelném optickém formátu (QR), který lze zobrazit na displeji mobilního zařízení nebo vytisknout na papír.

(4) Kromě technických specifikací pro formát a řízení důvěryhodnosti digitálního certifikátu EU COVID by měla být stanovena obecná pravidla pro účely vyplňování certifikátů, která by se měla používat pro kódované hodnoty v obsahu digitálního certifikátu EU COVID. Komise by měla s využitím příslušné práce odvedené sítí pro elektronické zdravotnictví pravidelně aktualizovat a zveřejňovat soubory hodnot, kterými se tato pravidla provádějí.

(5) Jak stanoví nařízení (EU) 2021/953, pravé certifikáty tvořící digitální certifikát EU COVID by měly být jednotlivě identifikovatelné pomocí jedinečného identifikátoru certifikátu, a to s přihlédnutím ke skutečnosti, že občanům může být během doby platnosti nařízení (EU) 2021/953 vydán více než jeden certifikát. Jedinečný identifikátor certifikátu má sestávat z alfanumerického řetězce a členské státy by měly zajistit, aby neobsahoval žádné údaje, které by jej spojovaly s jinými doklady nebo identifikátory, například s číslem pasu nebo průkazu totožnosti, aby se zabránilo možnosti identifikace držitele. Za účelem zajištění jedinečnosti identifikátoru certifikátu by měly být stanoveny technické specifikace a pravidla pro jeho obecnou strukturu.

([1]) Úř. věst. L 211, 15.6.2021, s. 1.

([2]) Směrnice Evropského parlamentu a Rady 2011/24/EU ze dne 9. března 2011 o uplatňování práv pacientů v přeshraniční zdravotní péči (Úř. věst. L 88, 4.4.2011, s. 45).

(6) Bezpečnost, pravost, platnost a integrita certifikátů tvořících digitální certifikát EU COVID a jejich soulad s právem Unie v oblasti ochrany údajů jsou klíčové pro jejich přijetí ve všech členských státech. Těchto cílů je dosaženo prostřednictvím rámce pro důvěryhodnost, který stanoví pravidla a infrastrukturu pro spolehlivé a bezpečné vydávání a ověřování digitálních certifikátů EU COVID. Rámec pro důvěryhodnost by měl být mimo jiné založen na infrastruktuře veřejných klíčů s řetězem důvěry sahajícím od zdravotnických orgánů členských států nebo jiných důvěryhodných orgánů po jednotlivé subjekty vydávající digitální certifikáty EU COVID. S cílem zajistit systém interoperability v celé EU proto Komise vybudovala centrální systém – bránu pro digitální certifikát EU COVID (dále jen „brána"), která uchovává veřejné klíče používané pro ověřování. Při naskenování QR kódu certifikátu se digitální podpis ověří pomocí příslušného veřejného klíče, který byl předtím uložen v této centrální bráně. K zajištění integrity a pravosti dat lze použít digitální podpisy. Infrastruktury veřejných klíčů vytvářejí důvěru tím, že zajišťují vazbu veřejných klíčů na vydavatele certifikátů. V bráně se pro zajištění pravosti používá více certifikátů veřejných klíčů. V zájmu zajištění bezpečné výměny dat mezi členskými státy, pokud jde o veřejné klíče, a s cílem umožnit širokou interoperabilitu je nezbytné stanovit certifikáty veřejných klíčů, které je možné používat, a poskytnout informace o tom, jak se mají generovat.

(7) Toto rozhodnutí umožňuje zajistit funkčnost požadavků nařízení (EU) 2021/953 způsobem, který minimalizuje zpracování osobních údajů na míru nezbytnou pro zprovoznění digitálního certifikátu EU COVID a přispívá k tomu, aby provádění ze strany konečných správců zajišťovalo záměrnou ochranu osobních údajů.

(8) V souladu s nařízením (EU) 2021/953 se orgány nebo jiné určené subjekty odpovědné za vydávání certifikátů v průběhu procesu vydávání ve své roli zpracovatelů osobních údajů považují za správce ve smyslu čl. 4 odst. 7 nařízení Evropského parlamentu a Rady (EU) 2016/679 ([3]). V závislosti na tom, jak členské státy organizují proces vydávání, může existovat jeden nebo více orgánů nebo určených subjektů, například oblastní zdravotní služby. V souladu se zásadou subsidiarity je tato volba na členských státech. Členské státy tedy mohou nejlépe zajistit, aby v případě existence více orgánů nebo jiných určených subjektů byla jasně stanovena jejich odpovědnost, a to nezávisle na tom, zda se jedná o samostatné nebo společné správce (včetně oblastních zdravotních služeb zřizujících společný portál pro pacienty pro vydávání certifikátů). Stejně tak, pokud jde o ověřování certifikátů příslušnými orgány členského státu určení nebo tranzitu nebo provozovateli služeb přeshraniční osobní dopravy, kteří jsou podle vnitrostátních právních předpisů povinni provádět během pandemie COVID-19 určitá opatření v oblasti veřejného zdraví, musí tito ověřovatelé dodržovat své povinnosti podle pravidel ochrany údajů.

(9) Prostřednictvím brány pro digitální certifikát EU COVID nedochází ke zpracování osobních údajů, protože brána obsahuje pouze veřejné klíče podepisujících orgánů. Tyto klíče se vztahují k podepisujícím orgánům a neumožňují přímou ani nepřímou opětovnou identifikaci fyzické osoby, které byl vydán certifikát. Komise by tedy v roli správce brány neměla být správcem ani zpracovatelem osobních údajů.

(10) V souladu s čl. 42 odst. 1 nařízení Evropského parlamentu a Rady (EU) 2018/1725 ([4]) byl konzultován evropský inspektor ochrany údajů, který vydal stanovisko dne 22. června 2021.

(11) Vzhledem k tomu, že pro uplatňování nařízení (EU) 2021/953 od 1. července 2021 jsou nezbytné technické specifikace a pravidla, je odůvodněné, aby toto rozhodnutí bylo okamžitě použitelné.

(12) Vzhledem k potřebě rychlého zavedení digitálního certifikátu EU COVID by proto toto rozhodnutí mělo vstoupit v platnost dnem vyhlášení,

([3]) Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů) (Úř. věst. L 119, 4.5.2016, s. 1).

([4]) Nařízení Evropského parlamentu a Rady (EU) 2018/1725 ze dne 23. října 2018 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů orgány, institucemi a jinými subjekty Unie a o volném pohybu těchto údajů a o zrušení nařízení (ES) č. 45/2001 a rozhodnutí č. 1247/2002/ES (Úř. věst. L 295, 21.11.2018, s. 39).

PŘIJALA TOTO ROZHODNUTÍ:

Článek 1

Technické specifikace pro digitální certifikát EU COVID, které stanoví obecnou datovou strukturu, mechanismy kódování a mechanismus kódování při přenosu ve strojově čitelném optickém formátu, jsou stanoveny v příloze I.

Článek 2

Pravidla pro vyplňování certifikátů uvedených v čl. 3 odst. 1 nařízení (EU) 2021/953 jsou stanovena v příloze II tohoto rozhodnutí.

Článek 3

Požadavky na společnou strukturu jedinečného identifikátoru certifikátu jsou stanoveny v příloze III.

Článek 4

Pravidla správy platná pro certifikáty veřejných klíčů ve vztahu k bráně pro digitální certifikát EU COVID, která podporují aspekty interoperability rámce pro důvěryhodnost, jsou stanovena v příloze IV.

Toto rozhodnutí vstupuje v platnost dnem vyhlášení v *Úředním věstníku Evropské unie*.

V Bruselu dne 28. června 2021.

Za Komisi
předsedkyně
Ursula VON DER LEYEN

PŘÍLOHA I

FORMÁT A ŘÍZENÍ DŮVĚRY

Obecná datová struktura, mechanismy kódování a mechanismus kódování při přenosu ve strojově čitelném optickém formátu (dále jen „QR“)

1. Úvod

Technické specifikace uvedené v této příloze obsahují obecnou datovou strukturu a mechanismy kódování pro digitální certifikát EU COVID („DCC“). Specifikují rovněž mechanismus kódování při přenosu ve strojově čitelném optickém formátu („QR“), který lze zobrazit na displeji mobilního zařízení nebo vytisknout. Formáty kontejneru pro elektronický zdravotní certifikát v těchto specifikacích jsou obecné, ale v této souvislosti se používají k přenosu DCC.

2. Terminologie

Pro účely této přílohy se „vydavateli“ rozumí organizace, které používají tyto specifikace pro vydávání zdravotních certifikátů, a „ověřovateli“ se rozumí organizace, které zdravotní certifikáty uznávají jako doklad o zdravotním stavu. „Účastníky“ se rozumí vydavatelé a ověřovatelé. Některé aspekty stanovené v této příloze musí být mezi účastníky koordinovány, například správa jmenného prostoru a distribuce kryptografických klíčů. Předpokládá se, že tyto úkoly vykonává strana, dále nazývaná „sekretariát“.

3. Formát kontejneru pro elektronický zdravotní certifikát

Formát kontejneru pro elektronický zdravotní certifikát („HCERT“) je navržen tak, aby poskytoval jednotný a standardizovaný nosič pro zdravotní certifikáty od různých vydavatelů. Cílem těchto specifikací je harmonizovat způsob, jakým jsou tyto zdravotní certifikáty reprezentovány, kódovány a podepisovány, a to se záměrem usnadnit interoperabilitu.

K tomu, aby bylo možné číst a interpretovat DCC vydaný jakýmkoli vydavatelem, jsou zapotřebí společná datová struktura a dohoda na významu jednotlivých datových polí informačního obsahu. K usnadnění této interoperability je pomocí schématu „JSON“ definována společná koordinovaná datová struktura, která tvoří rámec pro DCC.

3.1. *Struktura informačního obsahu*

Informační obsah je strukturován a kódován ve formátu CBOR s digitálním podpisem COSE. Tento formát je běžně znám jako „CBOR Web Token“ (CWT) a je definován v RFC 8392 ([1]). Informační obsah, jak je definován v následujících oddílech, se přenáší v deklaraci hcert.

Integrita a pravost původu dat informačního obsahu musí být ověřitelné ověřovatelem. K zajištění tohoto mechanismu musí vydavatel podepsat CWT s použitím schématu asymetrického elektronického podpisu definovaného ve specifikaci COSE (RFC 8152 ([2])).

3.2. *Deklarace CWT*

3.2.1. Přehled struktury CWT

Chráněné záhlaví

— Algoritmus podpisu (alg, návěstí 1)

— Identifikátor klíče (kid, návěstí 4)

Informační obsah

— Vydavatel (iss, klíč deklarace 1, volitelný, dvoupísmenný kód země vydavatele dle ISO 3166-1)

— Datum a čas vydání (iat, klíč deklarace 6)

— Datum a čas skončení platnosti (exp, klíč deklarace 4)

— Zdravotní certifikát (hcert, klíč deklarace -260)

— Digitální certifikát EU COVID v1 (eu_DCC_v1, klíč deklarace 1)

Podpis

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

3.2.2. Algoritmus podpisu

Algoritmus podpisu (alg) je parametr, který označuje, jaký algoritmus se používá pro vytvoření podpisu. Musí splňovat přinejmenším požadavky stávajících pokynů Poradního výboru pro bezpečnost informačních systémů (SOG-IS), které jsou shrnuty v následujících odstavcích.

Je definován jeden primární a jeden sekundární algoritmus. Sekundární algoritmus by měl být použit pouze v případě, že primární algoritmus není přijatelný v rámci pravidel a předpisů, kterými je vydavatel vázán.

Pro zajištění bezpečnosti systému musí všechny implementace zahrnovat sekundární algoritmus. Z tohoto důvodu musí být implementován jak primární, tak sekundární algoritmus.

Pro primární a sekundární algoritmy stanovil výbor SOG-IS tyto úrovně:

— Primární algoritmus: Primárním algoritmem je algoritmus digitálního podpisu ECDSA (Elliptic Curve Digital Signature Algorithm) definovaný v oddíle 2.3 (ISO/IEC 14888–3:2006), který používá parametry P-256 definované v dodatku D (D.1.2.3) (FIPS PUB 186–4) v kombinaci s hašovacím algoritmem SHA-256 definovaným v (ISO/IEC 10118–3:2004) – funkce 4.

To v COSE odpovídá parametru algoritmu ES256.

— Sekundární algoritmus: Sekundární algoritmus je RSASSA-PSS definovaný v (RFC 8230 ([3])) s 2048bitovým modulem v kombinaci s hašovacím algoritmem SHA-256 definovaným v (ISO/IEC 10118–3:2004) – funkce 4.

To v COSE odpovídá parametru algoritmu PS256.

3.2.3. Identifikátor klíče

Deklarace identifikátoru klíče (kid) označuje certifikát signatáře dokumentu (DSC) obsahující veřejný klíč, který má ověřovatel použít pro kontrolu správnosti digitálního podpisu. Správu certifikátů veřejných klíčů, včetně požadavků na DSC, popisuje příloha IV.

Deklarace identifikátoru klíče (kid) slouží ověřovatelům pro výběr správného veřejného klíče ze seznamu klíčů vztahujících se k vydavateli, který je uveden v deklaraci vydavatele (iss). Z administrativních důvodů a při obměně klíčů může vydavatel používat souběžně více klíčů. Identifikátor klíče není z hlediska bezpečnosti kritické pole. Z tohoto důvodu může být v případě potřeby umístěn i v nechráněném záhlaví. Ověřovatelé musí akceptovat obě možnosti. Jsou-li přítomny obě možnosti, musí se použít identifikátor klíče v chráněném záhlaví.

Z důvodu zkrácení identifikátoru (kvůli omezení délky) existuje malá, ale nenulová šance, že celkový seznam DSC akceptovaných ověřovatelem může obsahovat DSC s duplicitními kid. Z tohoto důvodu musí ověřovatel zkontrolovat všechny DSC s daným kid.

3.2.4. Vydavatel

Deklarace vydavatele (iss) je hodnota typu řetězec, která může volitelně obsahovat dvoupísmenný kód země (dle ISO 3166-1) subjektu vydávajícího zdravotní certifikát. Na základě této deklarace může ověřovatel určit, kterou sadu DSC má k ověření použít. Tuto deklaraci identifikuje klíč deklarace 1.

3.2.5. Datum a čas skončení platnosti

Deklarace data a času skončení platnosti (exp) obsahuje časové razítko v celočíselném formátu NumericDate (specifikovaném v oddíle 2 dokumentu RFC 8392 ([4])), jež udává, do kdy je tento konkrétní podpis informačního obsahu považován za platný; poté musí ověřovatel tento informační obsah zamítnout z důvodu skončení platnosti. Datum skončení platnosti je parametr, jehož účelem je omezit dobu platnosti zdravotního certifikátu. Tuto deklaraci identifikuje klíč deklarace 4.

Datum a čas skončení platnosti nesmí přesáhnout dobu platnosti DSC.

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

3.2.6. Datum a čas vydání

Deklarace Datum a čas vydání (iat) obsahuje časové razítko v celočíselném formátu NumericDate (specifikovaném v oddíle 2 dokumentu RFC 8392 ([5])), jež udává, kdy byl tento zdravotní certifikát vytvořen.

Pole Datum a čas vydání nesmí předcházet době platnosti DSC.

Ověřovatelé mohou uplatňovat další pravidla pro omezení platnosti zdravotního certifikátu na základě data a času jeho vydání. Tuto deklaraci identifikuje klíč deklarace 6.

3.2.7. Deklarace zdravotního certifikátu

Deklarace zdravotního certifikátu (hcert) je objekt JSON (RFC 7159 ([6])), který obsahuje informace o zdravotním stavu. Stejná deklarace může obsahovat více různých typů zdravotních certifikátů, z nichž jedním je digitální certifikát EU COVID.

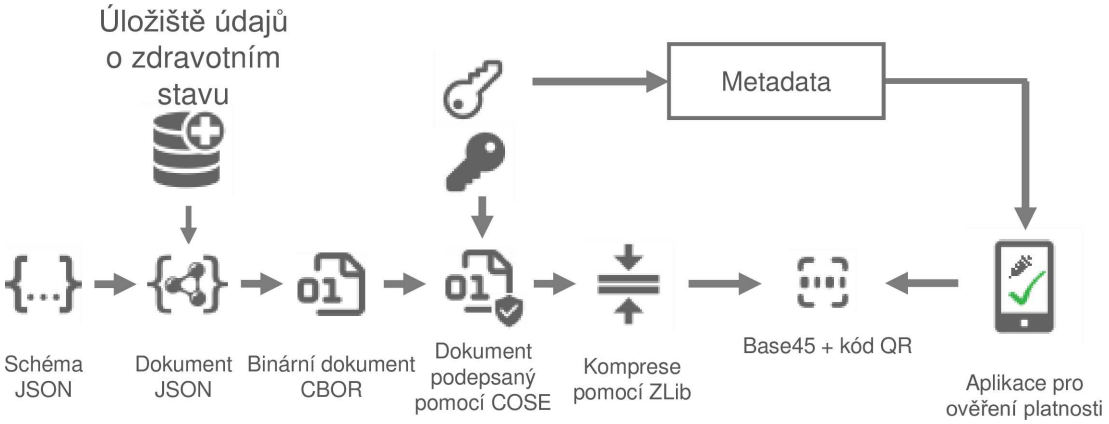
Objekt JSON slouží pouze pro účely schématu. Formátem pro reprezentaci je CBOR definovaný v (RFC 7049 ([7])). Vývojáři aplikací nemusí vůbec dekódovat nebo kódovat z/do formátu JSON, nýbrž mohou používat strukturu v paměti.

Tuto deklaraci identifikuje klíč deklarace -260.

Řetězce v objektu JSON by měly být normalizovány do formy NFC (Normalization Form Canonical Composition) definované v normě Unicode. Dekódující aplikace by však měly být v těchto ohledech tolerantní a robustní a doporučuje se akceptovat veškeré rozumné typové konverze. Pokud se v rámci dekódování nebo následných porovnávacích funkcí objeví nenormalizovaná data, měly by se implementace chovat, jako kdyby byl vstup normalizován do formy NFC.

4. Serializace a vytvoření informačního obsahu DCC

Jako serializační vzor se používá následující schéma:



Proces začíná extrakcí dat, například z úložiště údajů o zdravotním stavu (nebo z nějakého externího zdroje dat), přičemž extrahovaná data jsou strukturována podle definovaných schémat DCC. V rámci tohoto procesu může před začátkem serializace do formátu CBOR proběhnout konverze do definovaného datového formátu a transformace v zájmu srozumitelnosti pro člověka. Zkratky deklarací se v každém případě před serializací a po deserializaci mapují na zobrazované názvy.

V certifikátech vydaných po přijetí nařízení (EU) 2021/953 ([8]) není povolen volitelný vnitrostátní datový obsah. Datový obsah je omezen na definované datové prvky uvedené v minimálním datovém souboru, který je specifikován v příloze nařízení 2021/953.

([5]) rfc8392 (ietf.org)
([6]) rfc7159 (ietf.org)
([7]) rfc7049 (ietf.org)
([8]) Nařízení Evropského parlamentu a Rady (EU) 2021/953 ze dne 14. června 2021 o rámci pro vydávání, ověřování a uznávání interoperabilních certifikátů o očkování, o testu a o zotavení v souvislosti s onemocněním COVID-19 (digitální certifikát EU COVID) za účelem usnadnění volného pohybu během pandemie COVID-19 (Úř. věst. L 211, 15.6.2021, s. 1).

5. **Kódování při přenosu**

5.1. *Nezpracovaná data (raw)*

Kontejner HCERT a jeho informační obsahy lze přes blíže neupřesněná datová rozhraní přenášet bez jakékoli změny, přičemž lze využít jakéhokoli podkladového spolehlivého přenosu dat, který bez poškození přenese 8bitové hodnoty. Tato rozhraní mohou zahrnovat NFC (Near-Field Communication), Bluetooth nebo přenos přes protokol aplikační vrstvy, například přenos HCERT od vydavatele do mobilního zařízení držitele.

Je-li přenos HCERT od vydavatele k držiteli založen na výlučně prezentačním rozhraní (např. SMS, e-mail), pak se kódování při přenosu ve formě nezpracovaných dat samozřejmě nepoužije.

5.2. *Čárový kód*

5.2.1. Komprimace informačního obsahu (CWT)

Za účelem zmenšení velikosti a zvýšení rychlosti a spolehlivosti procesu čtení HCERT se CWT zkomprimuje pomocí ZLIB (RFC 1950 ([9])) a kompresního mechanismu Deflate ve formátu definovaném v RFC 1951 ([10]).

5.2.2. 2D čárový kód QR

Z důvodu lepší podpory starších zařízení, která jsou navržena pro informační obsah typu ASCII, je komprimovaný CWT před kódováním do 2D čárového kódu kódován jako ASCII s využitím Base45.

Pro generování 2D čárových kódů se použije formát QR definovaný v (ISO/IEC 18004:2015). Doporučuje se nastavit určitou míru korekce chyb „Q“ (kolem 25 %). Vzhledem k použití kódu Base45 musí kód QR používat alfanumerické kódování (režim 2 označený symboly 0010).

Aby mohli ověřovatelé detekovat typ kódovaných dat a vybrat správné schéma dekódování a zpracování, obsahují data v kódování Base45 (v souladu s touto specifikací) předponu v podobě řetězce identifikátoru kontextu „HC1:“. Budoucí verze této specifikace, které budou mít dopad na zpětnou kompatibilitu, definují nový identifikátor kontextu, přičemž znak následující po „HC“ se vybírá ze sady znaků [1-9 A-Z]. Pořadí přírůstků je definováno v tomto pořadí, tj. nejprve [1–9] a poté [A–Z].

Doporučuje se, aby byl optický kód na prezentačním médiu vyobrazen s úhlopříčkou 35 mm až 60 mm, aby bylo možné používat čtečky s pevnou optikou, kdy musí být prezentační médium položeno na povrch čtečky.

Je-li optický kód vytištěn na papíře tiskárnou s nízkým rozlišením (< 300 dpi), je třeba dbát na to, aby každý symbol (tečka) kódu QR byl přesně čtvercový. Neproporční změna měřítka povede k tomu, že v některých řádcích nebo sloupcích kódu QR budou obdélníkové symboly, což v mnoha případech omezí čitelnost.

6. **Formát seznamu vytvářejícího důvěru (seznam CSCA a DSC)**

Každý členský stát je povinen poskytnout seznam jedné nebo více národních certifikačních autorit (CSCA) a seznam všech platných certifikátů signatářů dokumentů (DSC) a je povinen tyto seznamy aktualizovat.

6.1. *Zjednodušené CSCA/DSC*

Počínaje touto verzí specifikací nemohou členské státy předpokládat, že se používají jakékoli informace ze seznamu zneplatněných certifikátů nebo že implementátoři ověřují dobu používání soukromých klíčů.

Primárním mechanismem ověření platnosti je místo toho přítomnost certifikátu na nejnovější verzi tohoto seznamu certifikátů.

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

6.2. *Certifikáty ICAO eMRTD PKI a centra důvěry*

Členské státy mohou používat samostatnou CSCA, ale mohou rovněž předložit své stávající certifikáty eMRTD CSCA nebo DSC a mohou se dokonce rozhodnout, že si je opatří od (komerčních) center důvěry a následně předloží. Každý DSC však musí být vždy podepsán certifikátem CSCA předloženým příslušným členským státem.

7. **Bezpečnostní aspekty**

Členské státy při vytváření koncepce schématu na základě této specifikace určují, analyzují a sledují některé bezpečnostní aspekty.

Zohledněny by měly být přinejmenším tyto aspekty:

7.1. *Doba platnosti podpisu HCERT*

Vydavatel HCERT je povinen omezit dobu platnosti podpisu tím, že uvede datum a čas skončení platnosti podpisu. Pro držitele zdravotního certifikátu z toho vyplývá nutnost pravidelně jej obnovovat.

Na to, jaká doba platnosti je přijatelná, mohou mít určující vliv praktická omezení. Cestující například nemusí mít možnost obnovit si zdravotní certifikát v průběhu cesty do zámoří. Může se však také stát, že vydavatel uvažuje o možnosti určitého narušení bezpečnosti, které vyžaduje, aby vydavatel stáhl určitý DSC (čímž zneplatní všechny zdravotní certifikáty vydané s použitím tohoto klíče ještě v době jejich platnosti). Důsledky takové události lze omezit pravidelnou obměnou klíčů vydavatele a vyžadováním obnovy všech zdravotních certifikátů v určitém přiměřeném intervalu.

7.2. *Správa klíčů*

Tato specifikace se do značné míry opírá o silné kryptografické mechanismy pro zabezpečení integrity dat a ověřování původu dat. Zachování důvěrnosti soukromých klíčů je proto nezbytné.

Důvěrnost kryptografických klíčů může být ohrožena mnoha různými způsoby, například:

— proces generování klíčů může být chybný, takže výsledné klíče jsou slabé,

— klíče mohu být vyzrazeny lidskou chybou,

— klíče mohou být odcizeny externími nebo interními narušiteli,

— klíče mohou být vypočteny kryptoanalýzou.

V zájmu zmírnění rizika, že v algoritmu podpisu budou objeveny slabiny, které umožní pomocí kryptoanalýzy kompromitovat soukromé klíče, doporučuje tato specifikace všem účastníkům implementovat sekundární záložní podpisový algoritmus založený na odlišných parametrech nebo na jiném matematickém problému než primární algoritmus.

Pokud jde o zmíněná rizika související s operačním prostředím vydavatelů, musí být implementována zmírňující opatření k zajištění účinné kontroly, například generování, ukládání a používání soukromých klíčů v hardwarových bezpečnostních modulech (Hardware Security Module, HSM). Používání HSM pro podepisování zdravotních certifikátů je důrazně doporučováno.

Bez ohledu na to, zda se vydavatel rozhodne HSM používat, by měl být stanoven harmonogram obměny klíčů, přičemž četnost obměn by měla být úměrná tomu, v jaké míře jsou klíče exponované vůči externím sítím, jiným systémům a zaměstnancům. Dobře zvolený harmonogram obměny rovněž omezuje rizika spojená s chybně vydanými zdravotními certifikáty, protože vydavatel může v případě potřeby stáhnout určitý klíč a tím tyto certifikáty hromadně zneplatnit.

7.3. *Ověřování platnosti vstupních dat*

Tyto specifikace mohou být použity způsobem vedoucím k tomu, že do systémů, které mohou být kriticky důležité, budou přijímána data z nedůvěryhodných zdrojů. V zájmu minimalizace rizik spojených s tímto vektorem útoku musí být všechna vstupní pole řádně validována z hlediska typu dat, délky a obsahu. Před jakýmkoli zpracováním obsahu HCERT se rovněž ověří podpis vydavatele. Ověření platnosti podpisu vydavatele však předpokládá, že se nejprve zanalyzuje chráněné záhlaví vydavatele, do něhož se potenciální útočník může pokusit vložit speciálně vytvořené informace ve snaze narušit bezpečnost systému.

8. **Řízení důvěry**

K ověření podpisu HCERT je nutný veřejný klíč. Členské státy zajistí přístup k těmto veřejným klíčům. V konečném důsledku každý ověřovatel potřebuje mít seznam všech veřejných klíčů, kterým je ochoten důvěřovat (protože veřejný klíč není součástí HCERT).

Systém má (pouze) dvě vrstvy: pro každý členský stát jeden nebo více vnitrostátních certifikátů, z nichž se každým podepíše jeden nebo více certifikátů signatářů dokumentů, které se pak používají při každodenních činnostech.

Certifikáty členských států se nazývají certifikáty národních certifikačních autorit (Country Signing Certificate Authority, CSCA) a jedná se (zpravidla) o samopodepsané certifikáty. Členské státy jich mohou mít více (například v případě regionální decentralizace). Pomocí těchto certifikátů CSCA se pravidelně podepisují certifikáty signatářů dokumentů (DSC) používané k podepisování zdravotních certifikátů.

„Sekretariát" je funkční role. Pravidelně shromažďuje DSC členských států a poté, co je ověří podle seznamu certifikátů CSCA (které byly předány a ověřeny jinými prostředky), je zveřejňuje.

Výsledný seznam DSC pak poskytuje souhrnný soubor akceptovatelných veřejných klíčů (a odpovídajících identifikátorů klíče), které mohou ověřovatelé používat k ověřování podpisů zdravotních certifikátů. Ověřovatelé si musí tento seznam pravidelně stahovat a aktualizovat.

Tyto seznamy specifické pro jednotlivé členské státy mohou být ve formátu přizpůsobeném jejich vnitrostátnímu prostředí. Souborový formát tohoto seznamu vytvářejícího důvěru se tak může různit: může se například jednat o podepsaný JWKS (formát JWK Set podle oddílu 5 dokumentu RFC 7517 ([11])) nebo o jakýkoli jiný formát specifický pro technologii používanou v daném členském státě.

V zájmu zajištění jednoduchosti mohou členské státy předložit své stávající certifikáty CSCA ze svých systémů ICAO eMRTD nebo v souladu s doporučením WHO vytvořit certifikát specifický pro tuto oblast zdravotnictví.

8.1. *Identifikátor klíče (kid)*

Identifikátor klíče (kid) se vypočítá při sestavování seznamu důvěryhodných veřejných klíčů na základě DSC a skládá se ze zkráceného (prvních 8 bajtů) otisku SHA-256 certifikátu DSC, který je kódován ve formátu DER (raw).

Ověřovatelé nemusí vypočítávat identifikátor klíče na základě DSC a mohou přímo porovnat identifikátor klíče ve vydaném zdravotním certifikátu s identifikátorem klíče uvedeným na seznamu vytvářejícím důvěru.

8.2. *Rozdíly oproti modelu důvěry ICAO eMRTD PKI*

Ačkoli se vychází z osvědčených postupů v rámci modelu důvěry ICAO eMRTD PKI, kvůli urychlení se provádí řada zjednodušení:

— Členský stát může předložit více certifikátů CSCA.

— Doba platnosti (použitelnosti klíče) DSC může být nastavena na libovolnou dobu nepřekračující dobu platnosti CSCA a nemusí být stanovena.

— DSC může obsahovat identifikátory zásad (rozšířených použití klíče), které jsou specifické pro zdravotní certifikáty.

— Členské státy se mohou rozhodnout, že nebudou vůbec ověřovat zveřejněná zneplatnění, a že se místo toho spolehnou pouze na seznamy DSC, které každý den obdrží od sekretariátu nebo které si samy sestaví.

([11]) rfc7517 (ietf.org)

PŘÍLOHA II

PRAVIDLA TÝKAJÍCÍ SE ÚČELU VYPLŇOVÁNÍ DIGITÁLNÍHO CERTIFIKÁTU EU COVID

Cílem obecných pravidel týkajících se souborů hodnot stanovených v této příloze je zajistit interoperabilitu na sémantické úrovni a umožnit jednotnou technickou implementaci digitálních certifikátů EU COVID. Prvky obsažené v této příloze mohou být použity pro tři různé scénáře (očkování/testování/zotavení), jak je stanoveno v nařízení (EU) 2021/953. V této příloze jsou uvedeny pouze prvky, u kterých je potřebná sémantická normalizace prostřednictvím kódovaných souborů hodnot.

Za překlad kódovaných prvků do národního jazyka odpovídají členské státy.

U všech datových polí, která nejsou uvedena v následujících popisech souborů hodnot, se doporučuje kódování UTF-8 (jméno, testovací středisko, vydavatel certifikátu). Datová pole obsahující kalendářní data (datum narození, datum očkování, datum odběru vzorku pro účel testu, datum prvního pozitivního výsledku testu, data platnosti certifikátu) se doporučuje kódovat podle normy ISO 8601.

Pokud z nějakého důvodu nelze použít upřednostňované systémy kódování uvedené níže, mohou být použity jiné mezinárodní systémy kódování a mělo by být vydáno doporučení, jak mají být kódy tohoto jiného systému kódování mapovány na upřednostňovaný systém kódování. Ve výjimečných případech, kdy definované soubory hodnot neobsahují vhodný kód, lze jako záložní mechanismus použít text (zobrazované názvy).

Členské státy, které ve svých systémech používají jiné kódování, by měly tyto kódy mapovat na popsané soubory hodnot. Za veškerá taková mapování odpovídají členské státy.

Komise tyto soubory hodnot s podporou sítě pro elektronické zdravotnictví a Výboru pro zdravotní bezpečnost pravidelně aktualizuje. Aktualizované soubory hodnot se zveřejňují na příslušných internetových stránkách Komise, jakož i na internetových stránkách sítě pro elektronické zdravotnictví. Měla by být poskytována historie změn.

1. **Onemocnění nebo původce onemocnění, jehož se certifikát týká/Onemocnění, z něhož se držitel uzdravil, nebo původce onemocnění: COVID-19 (SARS-CoV-2 nebo jedna z jeho variant)**

   Upřednostňovaný systém kódování: SNOMED CT.

   Použije se v certifikátu 1, 2 a 3.

   Vybrané kódy odkazují na COVID-19 nebo, jsou-li zapotřebí podrobnější informace o genetické variantě SARS-CoV-2, na tyto varianty, pokud jsou tyto podrobné informace z epidemiologických důvodů nezbytné.

   Příkladem kódu, který by se měl použít, je kód SNOMED CT 840539006 (COVID-19).

2. **Očkovací látka nebo profylaxe proti onemocnění COVID-19**

   Upřednostňovaný systém kódování: SNOMED CT nebo klasifikace ATC.

   Použije se v certifikátu 1.

   Příkladem kódů z preferovaných systémů kódování, které by se měly použít, jsou kódy SNOMED CT 1119305005 (antigenní očkovací látka proti SARS-CoV-2), 1119349007 (očkovací látka proti SARS-CoV-2 na bázi mRNA) nebo J07BX03 (očkovací látky proti COVID-19). Tento soubor hodnot by měl být po vyvinutí a zavedení nových typů očkovacích látek rozšířen.

3. **Léčivý přípravek – očkovací látka proti COVID-19**

   Preferované systémy kódování (v pořadí podle preference):

   — Rejstřík léčivých přípravků Unie pro očkovací látky s celounijní registrací (čísla registrace)

   — Celosvětový rejstřík očkovacích látek, například rejstřík, který by mohla zřídit Světová zdravotnická organizace

   — Název léčivého přípravku – očkovací látky v ostatních případech. Pokud název obsahuje prázdné znaky, měly by být nahrazeny spojovníkem (-).

Název souboru hodnot: Očkovací látka.

Použije se v certifikátu 1.

Příkladem kódu z upřednostňovaných systémů kódování, který by se měl použít, je EU/1/20/1528 (Comirnaty). Příklad názvu očkovací látky, který se použije jako kód: Sputnik-V (pro Sputnik V).

4. **Držitel rozhodnutí o registraci očkovací látky proti onemocnění COVID-19 nebo výrobce očkovací látky proti onemocnění COVID-19**

Upřednostňovaný systém kódování:

— Kód organizace udělený agenturou EMA (systém SPOR pro ISO IDMP)

— Celosvětový rejstřík držitelů rozhodnutí o registraci nebo výrobců očkovacích látek, například rejstřík, který by mohla zřídit Světová zdravotnická organizace

— Název organizace v ostatních případech. Pokud název obsahuje prázdné znaky, měly by být nahrazeny spojovníkem (-).

Použije se v certifikátu 1.

Příkladem kódu z upřednostňovaného systému kódování, který by se měl použít, je ORG-100001699 (AstraZeneca AB). Příklad názvu organizace, který se použije jako kód: Sinovac-Biotech (pro Sinovac Biotech).

5. **Pořadí v rámci řady dávek, jakož i celkový počet dávek v této řadě**

Použije se v certifikátu 1.

Dvě pole:

1) Pořadí dávky podané v rámci jednoho cyklu

2) Počet očekávaných dávek v rámci úplného cyklu (specifické pro osobu v době podání)

Například 1/1, 2/2 budou představovat dokončený cyklus, včetně možnosti 1/1 pro očkovací látky, které sice předpokládají dvě dávky, ale podle protokolu uplatňovaného daným členským státem má být občanům, u nichž bylo před očkováním diagnostikováno onemocnění COVID-19, podávána pouze jedna dávka. Celkový počet dávek v řadě by měl být uveden podle informací dostupných v době podání dávky. Pokud například určitá očkovací látka v době podání naposledy podané dávky vyžaduje třetí dávku (přeočkování), uvede se to ve druhém číselném poli (například 2/3, 3/3 atd.).

6. **Členský stát nebo třetí země, v nichž byla očkovací látka podána/byl test proveden**

Upřednostňovaný systém kódování: kódy zemí podle ISO 3166.

Použije se v certifikátech 1, 2 a 3.

Obsah souboru hodnot: úplný seznam dvoupísmenných kódů, který je k dispozici jako soubor hodnot definovaných ve standardu FHIR (http://hl7.org/fhir/ValueSet/iso3166-1-2).

7. **Druh testu**

Upřednostňovaný systém kódování: LOINC.

Použije se v certifikátu 2, a dále v certifikátu 3, pokud je prostřednictvím aktu v přenesené pravomoci zavedena podpora pro vydávání certifikátů o zotavení založených na jiných druzích testu než NAAT.

Kódy v tomto souboru hodnot odkazují na metodu testu a musí být zvoleny tak, aby umožnily přinejmenším odlišit testy NAAT od testů RAT, jak je uvedeno v nařízení (EU) 2021/953.

Příkladem kódu z upřednostňovaného systému kódování, který by se měl použít, je LP217198-3 (rychlý imunologický test).

8. **Výrobce a obchodní název použitého testu (pro test NAAT nepovinné)**

Upřednostňovaný systém kódování: seznam rychlých testů na antigen, který vydává Výbor pro zdravotní bezpečnost (HSC) a spravuje Společné výzkumné středisko (databáze diagnostických prostředků in vitro a metod testování pro onemocnění COVID-19).

Použije se v certifikátu 2.

Obsah souboru hodnot zahrnuje výběr rychlých testů na antigen uvedených ve společném a aktualizovaném seznamu rychlých testů na antigen pro diagnostiku onemocnění COVID-19, který byl sestaven na základě doporučení Rady 2021/C 24/01 a schválen Výborem pro zdravotní bezpečnost. Tento seznam spravuje Společné výzkumné středisko v rámci databáze diagnostických prostředků in vitro a metod testování pro onemocnění COVID-19, která je na adrese: https://covid-19-diagnostics.jrc.ec.europa.eu/devices/hsc-common-recognition-rat

Pro tento systém kódování se použijí relevantní pole, jako je identifikátor testovacího prostředku, název testu a výrobce, podle strukturovaného formátu Společného výzkumného střediska, který je k dispozici na adrese https://covid-19-diagnostics.jrc.ec.europa.eu/devices

9. **Výsledek testu**

Upřednostňovaný systém kódování: SNOMED CT.

Použije se v certifikátu 2.

Vybrané kódy musí umožňovat rozlišení mezi pozitivními a negativními výsledky testu (detekováno/nedetekováno). Je-li to v jednotlivých případech užití potřebné, lze přidat i další hodnoty (například „neplatný výsledek“).

Příklady kódů z upřednostňovaného systému kódování, které by se měly použít, jsou 260415000 (nedetekováno) a 260373001 (detekováno).

PŘÍLOHA III

SPOLEČNÁ STRUKTURA JEDINEČNÉHO IDENTIFIKÁTORU CERTIFIKÁTU

1. **Úvod**

Každý digitální certifikát EU COVID (DCC) obsahuje jedinečný identifikátor certifikátu (UCI), který podporuje interoperabilitu digitálních certifikátů EU COVID. Identifikátor UCI lze používat k ověření certifikátu. Implementace UCI je odpovědností členských států. UCI je prostředkem k ověření pravdivosti certifikátu a případně k propojení s registračním systémem (například IIS). Tyto identifikátory rovněž umožní členským státům vydávat (papírová a digitální) potvrzení pro jednotlivé osoby, že byly očkovány nebo testovány.

2. **Součásti jedinečného identifikátoru certifikátu**

Identifikátor UCI se řídí společnou strukturou a formátem usnadňujícím interpretaci informací člověkem nebo strojem a může se týkat prvků, jako je členský stát očkování, samotná očkovací látka a identifikátor specifický pro členský stát. Členským státům zajišťuje flexibilní možnosti stanovení formátu při plném souladu s právními předpisy v oblasti ochrany údajů. Pořadí jednotlivých prvků se řídí definovanou hierarchií, která může umožnit budoucí úpravy bloků při zachování strukturální integrity.

Různé možnosti složení UCI tvoří spektrum, v němž modularita a možnost interpretace člověkem představují dva hlavní rozlišující parametry a tvoří jednu základní charakteristiku:

— modularita: míra, do jaké je kód složen ze samostatných stavebních bloků, které obsahují sémanticky odlišné informace,

— možnost interpretace člověkem: míra, do jaké je kód smysluplný nebo může být interpretován lidským čtenářem,

— globálně jedinečný; identifikátor země nebo orgánu je řádně spravován; očekává se, že každá země (orgán) bude svůj segment jmenného prostoru řádně spravovat, a to tak, že nikdy nebude identifikátory recyklovat nebo opakovaně vydávat. Tato kombinace umožňuje zajistit, aby každý identifikátor byl globálně jedinečný.

3. **Všeobecné požadavky**

V souvislosti s UCI by měly být splněny tyto zastřešující požadavky:

1) Znaková sada: povoleny jsou pouze velká písmena a číslice US-ASCII („A“ až „Z“, „0“ až „9“), dále pak zvláštní oddělovací znaky podle RFC3986 ([1]) ([2]), jmenovitě {„/“, „#“, „:“}.

2) Maximální délka: při konstrukci by se mělo cílit na délku v rozmezí 27–30 znaků ([3]).

3) Předpona verze: jedná se o verzi schématu UCI. Předpona verze je pro tuto verzi dokumentu „01“; předpona verze se skládá ze dvou číslic.

4) Předpona země: kód země je specifikován podle normy ISO 3166-1. Delší kódy, např. 3 znaky a více (například „UNHCR“), jsou vyhrazeny pro budoucí použití.

5) Přípona kódu/kontrolní součet:

5.1. Členské státy by měly použít kontrolní součet, pokud je pravděpodobné, že může dojít k poškození při přenosu, přepisu (člověkem) nebo jiným způsobem (například při použití v tištěné podobě).

5.2. Kontrolní součet se nesmí používat k ověřování platnosti certifikátu a technicky vzato není součástí identifikátoru, nýbrž slouží pouze k ověření integrity kódu. Tento kontrolní součet by měl být souhrnem celého UCI ve formátu pro digitální přenos podle normy ISO-7812-1 (LUHN-10) ([4]). Od ostatních částí UCI je kontrolní součet oddělen znakem „#“.

([1]) rfc3986 (ietf.org)

([2]) Pole, jako je pohlaví, číslo šarže, očkovací středisko, identifikace zdravotnického pracovníka či datum příštího očkování, nemusí být potřebná pro jiné než lékařské účely.

([3]) Při implementaci s kódy QR by členské státy mohly uvažovat o další sadě znaků až do celkové délky 72 znaků (včetně 27–30 znaků samotného identifikátoru), která by umožnila předávání dalších informací. Specifikace těchto informací je věcí členských států.

([4]) Algoritmus Luhn mod N je rozšířením algoritmu Luhn (který je znám rovněž jako algoritmus mod 10), který pracuje s číselnými kódy a používá se například pro výpočet kontrolního součtu čísel kreditních karet. Uvedené rozšíření umožňuje algoritmu pracovat se sekvencemi hodnot v libovolné bázi (v našem případě s písmeny).

Měla by být zajištěna zpětná kompatibilita: členské státy, které v průběhu času mění strukturu svých identifikátorů (v rámci hlavní verze, v současné době stanovené jako v1), musejí zajistit, aby kterékoli dva identifikátory, které jsou totožné, reprezentovaly tentýž certifikát o očkování/totéž potvrzení. Jinými slovy, členské státy nemohou identifikátory recyklovat.

4. **Možnosti jednoznačných identifikátorů certifikátů, pokud jde o certifikáty o očkování**

Pokyny pro ověřitelné certifikáty o očkování a základní prvky interoperability ([5]), které vydala síť pro elektronické zdravotnictví, poskytují členským státům a dalším stranám různé možnosti, které mohou mezi různými členskými státy existovat souběžně. Členské státy mohou tyto různé možnosti uplatňovat v různých verzích schématu UCI.

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

PŘÍLOHA IV

SPRÁVA CERTIFIKÁTŮ VEŘEJNÝCH KLÍČŮ

1. Úvod

Bezpečnou a důvěryhodnou výměnu podpisových klíčů pro digitální certifikáty EU COVID (DCC) mezi členskými státy zajišťuje brána pro digitální certifikát EU COVID (DCCG), která slouží jako centrální úložiště veřejných klíčů. DCCG umožňuje členským státům zveřejňovat veřejné klíče odpovídající soukromým klíčům, které používají k podepisování digitálních certifikátů COVID. Členské státy, které bránu DCCG využívají, ji mohou použít ke včasnému získávání aktuálních veřejných klíčů. Později může být brána DCCG rozšířena, aby umožňovala i výměnu doplňujících důvěryhodných informací, které členské státy poskytují, jako jsou pravidla pro ověřování platnosti DCC. Modelem důvěry, který se pro rámec DCC používá, je infrastruktura veřejných klíčů (PKI). Každý členský provozuje jednu nebo více národních certifikačních autorit (CSCA), jejichž certifikáty mají relativně dlouhou životnost. Podle rozhodnutí daného členského státu může být autorita CSCA stejná či odlišná od CSCA využívané pro strojově čitelné cestovní doklady. CSCA vydává certifikáty veřejných klíčů pro vnitrostátní signatáře dokumentů (tj. pro signatáře DCC), které mají krátkou životnost a označují se jako certifikáty signatářů dokumentů (DSC). CSCA funguje jako zdroj důvěry, takže členské státy, které ji využívají, mohou certifikát CSCA použít k ověřování pravosti a integrity pravidelně se měnících DSC. Po ověření jejich platnosti mohou členské státy tyto certifikáty (nebo pouze veřejné klíče v nich obsažené) použít ve svých aplikacích pro ověřování platnosti DCC. Kromě CSCA a DSC využívá brána DCCG infrastrukturu veřejných klíčů také k ověřování pravosti transakcí, podepisování dat, jako základ pro autentizaci a jako prostředek k zajištění integrity komunikačních kanálů mezi členskými státy a bránou DCCG.

K zajištění integrity a pravosti dat lze používat digitální podpisy. Infrastruktury veřejných klíčů vytvářejí důvěru tím, že vytvářejí vazbu mezi veřejnými klíči a ověřenými identitami (nebo vydavateli). To je nutné k tomu, aby ostatní účastníci mohli ověřit původ dat a totožnost komunikačního partnera a rozhodnout se o jejich důvěryhodnosti. V rámci brány DCCG se pro zajištění pravosti používá více certifikátů veřejných klíčů. V této příloze je definováno, jaké certifikáty veřejných klíčů se používají a jak mají být koncipovány, aby umožňovaly širokou interoperabilitu mezi členskými státy. Jsou v ní uvedeny podrobnější informace o nezbytných certifikátech veřejných klíčů a pokyny k šablonám certifikátů a dobám platnosti pro členské státy, které chtějí provozovat vlastní CSCA. Vzhledem k tomu, že digitální certifikáty EU COVID musí být ověřitelné v určitém stanoveném časovém rozmezí (od vydání do skončení platnosti po uplynutí určité doby), je nezbytné definovat ověřovací model pro všechny podpisy použité na certifikátech veřejných klíčů a digitálních certifikátech EU COVID.

2. Terminologie

Následující tabulka obsahuje zkratky a terminologii používané v této příloze.

Pojem	Definice
Certifikát	Též certifikát veřejného klíče. Certifikát X.509 v3, který obsahuje veřejný klíč určitého subjektu.
CSCA	Národní certifikační autorita (Country Signing Certificate Authority)
DCC	Digitální certifikát EU COVID. Podepsaný digitální dokument, který obsahuje informace o očkování, testu nebo zotavení.
DCCG	Brána pro digitální certifikát EU COVID (EU Digital COVID Certificate Gateway). Tento systém se používá k výměně DSC mezi členskými státy.
$DCCG_{TA}$	Certifikát zdroje důvěry (Trust Anchor) brány DCCG. Příslušným soukromým klíčem se off-line podepisuje seznam všech certifikátů CSCA.
$DCCG_{TLS}$	Serverový certifikát TLS brány DCCG
DSC	Certifikát signatáře dokumentu (Document Signer Certificate). Certifikát veřejného klíče autority členského státu pro podepisování dokumentů (například systému, který je oprávněn podepisovat DCC). Tento certifikát vydává CSCA členského státu.
EC-DSA	Elliptic Curve Digital Signature Algorithm. Kryptografický algoritmus podpisu založený na eliptických křivkách.
Členský stát	Členský stát Evropské unie

Pojem	Definice
mTLS	Mutual TLS. Protokol zabezpečení na transportní vrstvě včetně vzájemné autentizace.
NB	Vnitrostátní backendový systém (National Backend) členského státu
NB_{CSCA}	Certifikát CSCA členského státu (může být více než jeden)
NB_{TLS}	Autentizační klientský certifikát TLS vnitrostátního backendového systému
NB_{UP}	Certifikát používaný vnitrostátním backendovým systémem k podepisování datových balíčků, které jsou nahrávány do DCCG
PKI	Infrastruktura veřejných klíčů (Public Key Infrastructure). Model důvěry založený na certifikátech veřejných klíčů a certifikačních autoritách.
RSA	Asymetrický kryptografický algoritmus založený na rozkladu na prvočinitele, používaný pro digitální podpisy nebo asymetrické šifrování

3. **Komunikační toky a bezpečnostní služby brány DCCG**

Tento oddíl poskytuje přehled komunikačních toků a bezpečnostních služeb v systému DCCG. Definuje také, které klíče a certifikáty se používají k ochraně komunikace, nahrávaných informací, digitálních certifikátů EU COVID a podepsaného seznamu vytvářejícího důvěru, který obsahuje veškeré přijaté certifikáty CSCA. DCCG funguje jako datový uzel, který členským státům umožňuje předávání podepsaných datových balíčků.

Nahrané datové balíčky poskytuje brána DCCG ve stejné podobě, v jaké je obdržela, což znamená, že do balíčků, které obdrží, DCCG nepřidává žádné DSC ani je z nich neodebírá. Vnitrostátní backendový systém (NB) členských států musí být schopen ověřit *end-to-end* integritu a pravost nahraných dat. Kromě toho budou vnitrostátní backendové systémy a brána DCCG používat i vzájemné ověřování totožnosti prostřednictvím TLS k navázání bezpečného spojení. To je nad rámec podpisů obsažených v předávaných datech.

3.1. *Ověření totožnosti a navázání spojení*

Brána DCCG používá protokol TLS (Transport Layer Security) se vzájemnou autentizací k vytvoření autentizovaného šifrovaného kanálu mezi vnitrostátním backendovým systémem (NB) členského státu a prostředím brány. DCCG je proto držitelem serverového certifikátu TLS, označovaného zkratkou $DCCG_{TLS}$, a vnitrostátní backendové systémy jsou držiteli klientského certifikátu TLS, označovaného zkratkou NB_{TLS}. Šablony certifikátů jsou uvedeny v *oddíle 5*. Každý vnitrostátní backendový systém může poskytnout svůj vlastní certifikát TLS. Tento certifikát bude zařazen na seznam výslovně povolených certifikátů, a může být tudíž vydán důvěryhodnou veřejnou certifikační autoritou (například certifikační autoritou, která se řídí základními požadavky fóra CA Browser Forum), národní certifikační autoritou nebo může být samopodepsaný. Každý členský stát odpovídá za svá vnitrostátní data a za ochranu soukromého klíče používaného k navázání spojení s bránou DCCG. Přístup založený na tom, že každý z účastníků poskytuje svůj vlastní certifikát, vyžaduje dobře definovaný postup registrace a identifikace, jakož i postupy zneplatnění a obnovení platnosti certifikátů, které jsou popsány v *oddílech 4.1, 4.2* a *4.3*. Brána DCCG používá seznam povolených certifikátů, na který jsou po úspěšné registraci přidány certifikáty TLS vnitrostátních backendových systémů. Bezpečné připojení k bráně DCCG mohou navázat pouze vnitrostátní backendové systémy, které prokáží svou totožnost s použitím soukromého klíče, jenž odpovídá některému z certifikátů v seznamu povolených certifikátů. Brána DCCG také použije certifikát TLS, který umožní vnitrostátním backendovým systémům ověřit, že navazují spojení se „skutečnou" bránou DCCG, a nikoli s nějakým zlovolným subjektem, který se za bránu DCCG pouze vydává. Certifikát brány DCCG bude vnitrostátním backendovým systémům poskytnut po úspěšné registraci. Certifikát $DCCG_{TLS}$ bude vydán důvěryhodnou veřejnou certifikační autoritou (která je uznávána všemi nejpoužívanějšími prohlížeči). Je na členských státech, aby ověřily, zda je jejich připojení k bráně DCCG bezpečné (například kontrolou otisku certifikátu $DCCG_{TLS}$ serveru, k němuž se připojují, vůči certifikátu, který jim byl poskytnut po registraci).

3.2. *Národní certifikační autority a model ověřování platnosti*

Členské státy zapojené do rámce DCCG musí k vydávání DSC používat CSCA. Členské státy mohou mít více než jednu CSCA, například v případě regionální decentralizace. Každý členský stát může buď použít stávající certifikační autority, nebo může vytvořit certifikační autoritu (případně samopodepsanou) vyhrazenou pro systém digitálních certifikátů EU COVID.

Během oficiálního postupu onboardingu musí členské státy předložit svůj certifikát (certifikáty) CSCA provozovateli brány DCCG. Po úspěšné registraci členského státu (*bližší informace jsou uvedeny v oddíle 4.1*) aktualizuje provozovatel brány DCCG podepsaný seznam vytvářející důvěru, který obsahuje všechny certifikáty CSCA, jež jsou v rámci systému DCC aktivní. Provozovatel DCCG podepíše seznam vytvářející důvěru a certifikáty v off-line prostředí s použitím vyhrazeného páru asymetrických klíčů. Soukromý klíč nebude uložen v on-line systému DCCG, aby narušením zabezpečení on-line systému nezískal útočník možnost ohrozit zabezpečení seznamu vytvářejícího důvěru. Během postupu onboardingu bude vnitrostátním backendovým systémům předán odpovídající certifikát zdroje důvěry $DCCG_{TA}$.

Členské státy mohou získat seznam vytvářející důvěru z brány DCCG pro své postupy ověřování. CSCA je definována jako certifikační autorita, která vydává DSC, takže členské státy, které používají víceúrovňovou hierarchii certifikačních autorit (například kořenová certifikační autorita -> CSCA -> DSC), musí poskytnout podřízenou certifikační autoritu, která vydává DSC. Používá-li v takovém případě členský stát stávající certifikační autoritu, pak bude systém DCC ignorovat vše nad úrovní CSCA a na seznam povolených certifikátů zahrne jako zdroj důvěry pouze CSCA (i když se jedná o podřízenou certifikační autoritu). Jde o model ICAO, až na to, že se připouští právě 2 úrovně – kořenová CSCA a podřízené DSC podepsané právě touto CSCA.

V případě, že členský stát provozuje svou vlastní CSCA, je tento členský stát odpovědný za bezpečný provoz a správu klíčů této certifikační autority. CSCA slouží jako zdroj důvěry pro DSC, ochrana soukromého klíče CSCA je proto zcela zásadní podmínkou integrity prostředí DCC. Modelem ověřování platnosti v rámci DCC PKI je model „shell", podle kterého musí být při ověřování posloupnosti certifikátů všechny certifikáty platné v daném okamžiku (tj. v době ověřování podpisu). Proto platí tato omezení:

— CSCA nevydává certifikáty, které mají delší platnost než certifikát certifikační autority,

— signatář dokumentu nepodepisuje dokumenty, které mají delší platnost než DSC,

— členské státy, které provozují svou vlastní CSCA, musí pro svou CSCA a pro všechny vydané certifikáty stanovit příslušné doby platnosti a musí se postarat o obnovování certifikátů.

Oddíl 4.2 obsahuje doporučení týkající se dob platnosti.

3.3. *Integrita a pravost nahrávaných dat*

Vnitrostátní backendové systémy mohou pomocí brány DCCG po úspěšné vzájemné autentizaci nahrávat a stahovat digitálně podepsané datové balíčky. Zprvu tyto datové balíčky obsahují DSC členských států. Pár klíčů, který vnitrostátní backendový systém používá pro digitální podpis datových balíčků nahrávaných do systému DCCG, se nazývá nahrávací pár podpisových klíčů vnitrostátního backendového systému a odpovídající certifikát veřejného klíče se označuje zkratkou NB_{UP}. Každý členský stát předkládá svůj vlastní certifikát NB_{UP}, který může samopodepsán nebo vystaven stávající certifikační autoritou, například veřejnou certifikační autoritou (tj. certifikační autoritou, která vydává certifikáty v souladu se základními požadavky fóra CAB). Certifikát NB_{UP} se musí lišit od všech ostatních certifikátů používaných daným členským státem (tj. certifikátu CSCA, klientského certifikátu TLS nebo certifikátů DSC).

Členské státy musí poskytnout nahrávací certifikát provozovateli brány DCCG při počáteční registraci (*bližší informace jsou uvedeny v oddíle 4.1*). Každý členský stát odpovídá za svá vnitrostátní data a musí chránit soukromý klíč, který používá k podepisování nahraných dat.

Ostatní členské státy mohou ověřovat podepsané datové balíčky pomocí nahrávacích certifikátů, které poskytuje brána DCCG. Před poskytnutím nahraných dat jiným členským státům ověřuje brána DCCG pravost a integritu nahraných dat s použitím nahrávacího certifikátu příslušného vnitrostátního backendového systému.

3.4. *Požadavky na technickou architekturu DCCG*

Na technickou architekturu brány DCCG se vztahují následující požadavky:

— K navázání autentizovaného šifrovaného spojení s vnitrostátními backendovými systémy používá brána DCCG vzájemnou autentizaci pomocí TLS. DCCG proto vede seznam povolených registrovaných klientských certifikátů NB_{TLS}.

— DCCG používá dva digitální certifikáty ($DCCG_{TLS}$ a $DCCG_{TA}$) se dvěma odlišnými páry klíčů. Soukromý klíč z páru klíčů k $DCCG_{TA}$ je uchováván off-line (tj. mimo on-line součásti DCCG).

— DCCG vede seznam vytvářející důvěru s certifikáty NB_{CSCA}, který je podepsán soukromým klíčem $DCGG_{TA}$.

— Použité šifry musí splňovat požadavky uvedené v *oddíle 5.1*.

4. **Řízení životního cyklu certifikátů**

4.1. *Registrace vnitrostátních backendových systémů*

Členské státy se musí zaregistrovat u provozovatele brány DCCG, aby se mohly účastnit systému DCCG. Tento oddíl popisuje technický a provozní postup, který je při registraci vnitrostátního backendového systému třeba dodržet.

Provozovatel DCCG a členský stát si musejí pro účely procesu onboardingu předat informace o technických kontaktních osobách. Předpokládá se, že technické kontaktní osoby mají od svých členských států příslušné oprávnění a že identifikace/autentizace se provádí prostřednictvím jiných kanálů. Autentizaci lze například zajistit tak, že technická kontaktní osoba členského státu poskytne certifikáty e-mailem jako soubory zašifrované heslem a příslušné heslo sdělí provozovateli DCCG telefonicky. Lze využít i jiné bezpečné kanály definované provozovatelem DCCG.

Během procesu registrace a identifikace musí členský stát poskytnout tři digitální certifikáty:

— certifikát TLS členského státu NB_{TLS}

— nahrávací certifikát členského státu NB_{UP},

— certifikát(y) CSCA členského státu NB_{CSCA}.

Všechny poskytnuté certifikáty musí vyhovovat požadavkům stanoveným v *oddíle 5*. To, zda daný certifikát požadavky *oddílu 5* splňuje, ověří provozovatel DCCG. Po identifikaci a registraci provozovatel DCCG:

— přidá certifikát(y) NB_{CSCA} do seznamu vytvářejícího důvěru, který je podepsán soukromým klíčem odpovídajícím veřejnému klíči $DCCG_{TA}$,

— přidá certifikát NB_{TLS} na seznam povolených certifikátů v koncovém bodě TLS systému DCCG,

— přidá certifikát NB_{UP} do systému DCCG,

— poskytne členskému státu certifikát veřejného klíče $DCCG_{TA}$ a $DCCG_{TLS}$.

4.2. *Certifikační autority, doby platnosti a obnovení*

V případě, že členský stát chce provozovat vlastní autoritu CSCA, mohou být certifikáty CSCA samopodepsané. Fungují jako zdroj důvěry členského státu, a členský stát proto musí důsledně chránit soukromý klíč odpovídající veřejnému klíči v certifikátu CSCA. Doporučuje se, aby členské státy pro své autority CSCA používaly off-line systém, tj. počítačový systém, který není připojen k žádné síti. K přístupu do tohoto systému by měla být zapotřebí součinnost více osob (například podle principu čtyř očí). Po podepsání certifikátů DSC se zavedou provozní kontroly a systém, ve kterém je uchováván soukromý klíč CSCA, musí být umístěn na bezpečném místě s přísným řízením přístupu. K další ochraně soukromého klíče CSCA lze použít hardwarové bezpečnostní moduly nebo čipové karty. Digitální certifikáty obsahují údaj o době platnosti, který nutí k obnovování certifikátů. Obnovování je nezbytné k tomu, aby se v případě, kdy je v důsledku nových vylepšení v oblasti výpočetních technologií nebo nových útoků ohrožena bezpečnost použitého kryptografického algoritmu, mohly použít nové kryptografické klíče a upravit délky klíčů. Použije se model „shell“ (viz *oddíl 3.2*).

S ohledem na roční platnost digitálních certifikátů COVID se doporučují následující doby platnosti:

— CSCA: 4 roky,

— DSC: 2 roky,

— nahrávací certifikát: 1–2 roky,

— autentizační klientský certifikát TLS: 1–2 roky.

Pro účely včasného obnovení se doporučují následující doby používání soukromých klíčů:

— CSCA: 1 rok,

— DSC: 6 měsíců.

Členské státy musí vytvořit nové nahrávací certifikáty a certifikáty TLS včas, například měsíc před skončením platnosti, aby byl zajištěn bezproblémový provoz. Certifikáty CSCA a DSC by měly být obnoveny nejméně jeden měsíc před ukončením používání příslušného soukromého klíče (s přihlédnutím k nezbytným provozním postupům). Členské státy musí poskytnout aktualizované certifikáty CSCA, nahrávací certifikáty a certifikáty TLS provozovateli DCCG. Certifikáty, kterým skončila platnost, se odstraní ze seznamu povolených certifikátů i ze seznamu vytvářejícího důvěru.

Členské státy a provozovatel DCCG musejí sledovat platnost svých vlastních certifikátů. Neexistuje žádný ústřední subjekt, který by vedl záznamy o platnosti certifikátů a informoval o ní účastníky.

4.3. *Zneplatnění certifikátů*

Obecně platí, že digitální certifikáty mohou být zneplatněny certifikační autoritou, která je vydala, a to pomocí seznamů zneplatněných certifikátů nebo prostřednictvím respondéru OCSP (Online Certificate Status Protocol). Autority CSCA pro systém DCC by měly poskytovat seznamy zneplatněných certifikátů (CRL). I když tyto seznamy zneplatněných certifikátů v současné době jiné členské státy nevyužívají, měly by být integrovány pro účely budoucích aplikací. V případě, že se CSCA rozhodne neposkytovat seznamy zneplatněných certifikátů, musí být certifikáty DSC od této CSCA obnoveny hned poté, co seznamy zneplatněných certifikátů začnou být povinné. Ověřovatelé by k ověřování platnosti certifikátů DSC neměli používat OCSP a měli by používat seznamy zneplatněných certifikátů. Doporučuje se, aby vnitrostátní backendový systém provedl nezbytné ověření platnosti DSC stažených z brány DCCG a vnitrostátním ověřovatelům platnosti DCC předal pouze sadu důvěryhodných a ověřených DSC. Ověřovatelé platnosti DCC by neměli v rámci svého postupu ověřování platnosti ověřovat, zda je nebo není zneplatněn DSC. Jedním z důvodů je ochrana soukromí držitelů digitálních certifikátů EU COVID, protože se tak vyloučí možnost, že by používání kteréhokoli konkrétního DSC mohlo být sledováno příslušným respondérem OCSP.

Členské státy mohou své certifikáty DSC z brány DCCG samy odstraňovat za použití platných nahrávacích certifikátů a certifikátů TLS. Odstranění DSC znamená, že všechny digitální certifikáty EU COVID vydané s použitím tohoto DSC pozbydou platnosti, jakmile si členské státy stáhnou aktualizované seznamy DSC. Zásadní význam má ochrana obsahu soukromých klíčů odpovídajících certifikátům DSC. V případě, že jsou členské státy nuceny zneplatnit nahrávací certifikát nebo certifikát TLS, například z důvodu narušení bezpečnosti vnitrostátního backendového systému, musí o tom informovat provozovatele DCCG. Provozovatel DCCG pak může zbavit dotčený certifikát důvěryhodnosti, například tak, že jej odstraní ze seznamu povolených certifikátů TLS. Provozovatel DCCG může odebrat nahrávací certifikáty z databáze DCCG. Balíčky podepsané soukromým klíčem, který odpovídá tomuto nahrávacímu certifikátu, se stanou neplatnými, jakmile vnitrostátní backendové systémy přestanou považovat zneplatněný nahrávací certifikát za důvěryhodný. V případě, že musí být zneplatněn certifikát CSCA, informují o tom členské státy provozovatele DCCG i ostatní členské státy, s nimiž udržují vztah důvěry. Provozovatel DCCG vydá nový seznam vytvářející důvěru, ve kterém již dotčený certifikát nebude obsažen. Všechny certifikáty DSC vydané touto autoritou CSCA se stanou neplatnými, jakmile členské státy aktualizují úložiště důvěry ve svém vnitrostátním backendovém systému. V případě, že musí být zneplatněn certifikát $DCCG_{TLS}$ nebo $DCCG_{TA}$, musí provozovatel DCCG a členské státy spolupracovat na navázání nového důvěryhodného spojení TLS a vytvoření nového seznamu vytvářejícího důvěru.

5. **Šablony certifikátů**

V tomto oddíle jsou stanoveny kryptografické požadavky a pokyny, jakož i požadavky na šablony certifikátů. Pro certifikáty DCCG jsou v tomto oddíle definovány šablony certifikátů.

5.1. *Kryptografické požadavky*

Kryptografické algoritmy a sady šifer TLS se volí na základě stávajícího doporučení německého Spolkového úřadu pro bezpečnost informací (BSI) nebo Poradního výboru pro bezpečnost informačních systémů (SOG-IS). Tato doporučení a doporučení jiných institucí a normalizačních organizací jsou si podobná. Tato doporučení lze najít v technických pokynech TR 02102-1 a TR 02102-2 ([1]) nebo v dokumentu SOG-IS Agreed Cryptographic Mechanisms (Dohodnuté kryptografické mechanismy výboru SOG-IS) ([2]).

5.1.1. Požadavky na DSC

Použijí se požadavky stanovené v *oddíle 3.2.2 přílohy I*. Důrazně se proto doporučuje, aby signatáři dokumentů používali algoritmus ECDSA s křivkou NIST-p-256 (podle definice uvedené v dodatku D dokumentu FIPS PUB 186-4). Jiné eliptické křivky nejsou podporovány. Vzhledem k omezenému množství místa v digitálních

([1]) BSI – technické pokyny TR-02102 (bund.de)
([2]) SOG-IS – podpůrné dokumenty (sogis.eu)

certifikátech EU COVID by členské státy neměly používat RSA-PSS, i když je tento algoritmus přípustný jako záložní možnost. V případě, že členské státy RSA-PSS využívají, měly by použít 2048bitový nebo maximálně 3072bitový modulus. Jako kryptografická hašovací funkce pro podpis DSC se použije SHA-2 s délkou výstupu ≥ 256 bitů (viz ISO/IEC 10118-3:2004).

5.1.2. Požadavky na certifikáty TLS, nahrávací certifikáty a certifikáty CSCA

Pokud jde o digitální certifikáty a kryptografické podpisy používané v kontextu DCCG, hlavní požadavky na kryptografické algoritmy a délku klíče jsou shrnuty v následující tabulce (stav v roce 2021):

Algoritmus podpisu	Délka klíče	Hašovací funkce
EC-DSA	min. 250 bitů	SHA-2 s délkou výstupu ≥ 256 bitů
RSA-PSS (doporučená výplň) RSA-PKCS#1 v1.5 (starší výplň)	min. 3000bitový modulus RSA (N) s veřejným exponentem e > 2^16	SHA-2 s délkou výstupu ≥ 256 bitů
DSA	min. 3000bitové prvočíslo p, 250bitový klíč q	SHA-2 s délkou výstupu ≥ 256 bitů

Eliptickou křivkou doporučenou pro EC-DSA je NIST-p-256 vzhledem k širokému rozšíření této implementace.

5.2. *Certifikát CSCA (NB_{CSCA})*

Následující tabulka obsahuje pokyny k šabloně certifikátu NB_{CSCA} pro případ, že se členský stát rozhodne provozovat pro systém DCC svou vlastní CSCA.

Tučně vyznačené údaje jsou povinné (musí být v certifikátu obsaženy), údaje vyznačené *kurzívou* jsou doporučené (certifikát by je měl obsahovat). Na chybějící pole se nevztahují žádná doporučení.

Pole	Hodnota
Subject (subjekt)	**cn=<neprázdný a jedinečný běžný název>,***o=<Poskytovatel>*, **c=<členský stát provozující CSCA>**
Key usage (použití klíče)	**certificate signing** (podepisování certifikátů), *CRL signing* (podepisování CRL) (minimálně)
Basic Constraints (základní omezení)	**CA = true, path length constraints = 0**

Název subjektu musí neprázdný a v daném členském státě jedinečný. Kód země (c) musí odpovídat členskému státu, který bude tento certifikát CSCA využívat. Certifikát musí obsahovat jedinečný identifikátor klíče subjektu (SKI) podle RFC 5280 ([3]).

5.3. *Certifikát signatáře dokumentu (DSC)*

Následující tabulka obsahuje pokyny pro DSC. **Tučně** vyznačené údaje jsou povinné (musí být v certifikátu obsaženy), údaje vyznačené *kurzívou* jsou doporučené (certifikát by je měl obsahovat). Na chybějící pole se nevztahují žádná doporučení.

Pole	Hodnota
Serial Number (sériové číslo)	**jedinečné sériové číslo**
Subject (subjekt)	**cn=<neprázdný a jedinečný běžný název>,***o=<Poskytovatel>*, **c=<členský stát používající tento DSC>**
Key Usage (použití klíče)	**digital signature** (digitální podpis) (minimálně)

([3]) rfc5280 (ietf.org)

Certifikát DSC musí být podepsán soukromým klíčem odpovídajícím certifikátu CSCA, který členský stát používá.

Používat se mají tato rozšíření:

— certifikát musí obsahovat identifikátor klíče autority (AKI) odpovídající identifikátoru klíče subjektu (SKI) v certifikátu autority CSCA, která jej vydala,

— certifikát by měl obsahovat jedinečný identifikátor klíče subjektu (SKI, v souladu s RFC 5280 ([4])).

Certifikát by měl navíc obsahovat rozšíření CRL Distribution Point (distribuční místo seznamu zneplatněných certifikátů) s odkazem na seznam zneplatněných certifikátů (CRL) poskytnutý autoritou CSCA, která tento DSC vydala.

DSC může obsahovat rozšíření Extended Key Usage (rozšířené použití klíče), které může obsahovat nula nebo více identifikátorů zásad používání klíče, které stanoví omezení pro typy certifikátů HCERT, které lze prostřednictvím tohoto certifikátu ověřovat. Pokud je alespoň jeden takový identifikátor přítomen, ověřovatelé ověří použití klíče podle uloženého HCERT. Pro tento účel jsou definovány tyto hodnoty extendedKeyUsage (rozšířené použití klíče):

Pole	Hodnota
extendedKeyUsage	1.3.6.1.4.1.1847.2021.1.1 pro vydavatele certifikátů o testu
extendedKeyUsage	1.3.6.1.4.1.1847.2021.1.2 pro vydavatele certifikátů o očkování
extendedKeyUsage	1.3.6.1.4.1.1847.2021.1.3 pro vydavatele certifikátů o zotavení

Pokud certifikát žádné takové rozšíření použití klíče neobsahuje, lze jej použít k ověření jakéhokoli typu HCERT. Příslušné doplňující identifikátory zásad rozšířeného používání klíče používané pro ověřování platnosti certifikátů HCERT mohou být definovány v jiných dokumentech.

5.4. *Nahrávací certifikáty (NB_{UP})*

Následující tabulka obsahuje pokyny pro nahrávací certifikát vnitrostátního backendového systému. **Tučně** vyznačené údaje jsou povinné (musí být v certifikátu obsaženy), údaje vyznačené *kurzívou* jsou doporučené (certifikát by je měl obsahovat). Na chybějící pole se nevztahují žádná doporučení.

Pole	Hodnota
Subject (subjekt)	**cn=<neprázdný a jedinečný běžný název>**, *o=<Poskytovatel>*,**c=<členský stát používající tento nahrávací certifikát>**
Key Usage (použití klíče)	**digital signature** (digitální podpis) (minimálně)

5.5. *Autentizační klientský certifikát TLS vnitrostátního backendového systému (NB_{TLS})*

Následující tabulka obsahuje pokyny pro autentizační klientský certifikát TLS vnitrostátního backendového systému. **Tučně** vyznačené údaje jsou povinné (musí být v certifikátu obsaženy), údaje vyznačené *kurzívou* jsou doporučené (certifikát by je měl obsahovat). Na chybějící pole se nevztahují žádná doporučení.

Pole	Hodnota
Subject (subjekt)	**cn=<neprázdný a jedinečný běžný název>,** *o=<Poskytovatel>*,**c=<členský stát provozující vnitrostátní koncový bod>**
Key Usage (použití klíče)	**digital signature** (digitální podpis) (minimálně)
Extended key usage (rozšířené použití klíče)	**client authentication** (autentizace klienta) **(1.3.6.1.5.5.7.3.2)**

([4]) rfc5280 (ietf.org)

Certifikát může také obsahovat rozšířené použití klíče *server authentication (1.3.6.1.5.5.7.3.1)*, ale není to povinné.

5.6. *Certifikát pro podepisování seznamu vytvářejícího důvěru ($DCCG_{TA}$)*

Následující tabulka definuje certifikát zdroje důvěry DCCG.

Pole	Hodnota
Subject (subjekt)	**cn = Digital Green Certificate Gateway** ([5]), **o=<Poskytovatel>, c=<země>**
Key Usage (použití klíče)	**digital signature** (digitální podpis) (minimálně)

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

Následující tabulka definuje certifikát TLS pro DCCG.

Pole	Hodnota
Subject (subjekt)	cn=<plně kvalifikovaný název domény nebo IP adresa DCCG>, o=<Poskytovatel>, c= <země>
SubjectAltName (alternativní název subjektu)	dNSName: <DNS název DCCG> nebo iPAddress: <IP adresa DCCG>
Key Usage (použití klíče)	**digital signature** (digitální podpis) (minimálně)
Extended Key usage (rozšířené použití klíče)	**server authentication** (autentizace serveru) **(1.3.6.1.5.5.7.3.1)**

Certifikát může také obsahovat rozšířené použití klíče *client authentication (1.3.6.1.5.5.7.3.2)*, ale není to povinné.

Certifikát DCCG pro TLS je vydán důvěryhodnou veřejnou certifikační autoritou (která je uznávána všemi nejpoužívanějšími prohlížeči a operačními systémy v souladu se základními požadavky fóra CAB).

([5]) Název „Digital Green Certificate“ (digitální zelený certifikát) namísto „digitální certifikát EU COVID“ je v této souvislosti zachován, protože jde o název, který byl napevno nastaven a zaveden v daném certifikátu předtím, než se spolunormotvůrci dohodli na novém termínu.