DECISIONE DI ESECUZIONE (UE) 2021/1073 DELLA COMMISSIONE

del 28 giugno 2021

che stabilisce specifiche tecniche e norme per l'attuazione del quadro di fiducia per il certificato COVID digitale dell'UE istituito dal regolamento (UE) 2021/953 del Parlamento europeo e del Consiglio

(Testo rilevante ai fini del SEE)

LA COMMISSIONE EUROPEA,

visto il trattato sul funzionamento dell'Unione europea,

visto il regolamento (UE) 2021/953 del Parlamento europeo e del Consiglio su un quadro per il rilascio, la verifica e l'accettazione di certificati interoperabili di vaccinazione, di test e di guarigione in relazione alla COVID-19 (certificato COVID digitale dell'UE) per agevolare la libera circolazione delle persone durante la pandemia di COVID-19 ([1]), in particolare l'articolo 9, paragrafi 1 e 3,

considerando quanto segue:

(1) Il regolamento (UE) 2021/953 stabilisce il certificato COVID digitale dell'UE, il cui scopo è fungere da prova del fatto che una persona ha ricevuto un vaccino contro la COVID-19, un risultato negativo a un test o è guarita dall'infezione.

(2) Affinché il certificato COVID digitale dell'UE sia operativo in tutta l'Unione, è necessario stabilire specifiche tecniche e norme per compilare, rilasciare in modo sicuro e verificare i certificati COVID digitali, garantire la protezione dei dati personali, stabilire la struttura comune dell'identificativo univoco del certificato e creare un codice a barre valido, sicuro e interoperabile. Tale quadro di fiducia getta inoltre le basi per cercare di garantire l'interoperabilità con le norme e i sistemi tecnologici internazionali e in quanto tale potrebbe fornire il modello per la cooperazione a livello mondiale.

(3) La capacità di leggere e interpretare il certificato COVID digitale dell'UE richiede una struttura di dati comune e un accordo sul significato voluto di ciascun campo di dati del carico utile e sui suoi possibili valori. Al fine di agevolare tale interoperabilità, è necessario definire una struttura comune coordinata dei dati per il quadro del certificato COVID digitale dell'UE. Gli orientamenti per tale quadro sono stati elaborati dalla rete eHealth istituita sulla base della direttiva 2011/24/UE del Parlamento europeo e del Consiglio ([2]). Tali orientamenti dovrebbero essere presi in considerazione nel definire le specifiche tecniche che stabiliscono il formato e la gestione della fiducia per il certificato COVID digitale dell'UE. Dovrebbero essere specificati meccanismi di codifica e una specifica della struttura dei dati, nonché un meccanismo di codifica di trasporto in un formato ottico leggibile meccanicamente (QR), che possa essere visualizzato sullo schermo di un dispositivo mobile o stampato su carta.

(4) Oltre alle specifiche tecniche per il formato e la gestione della fiducia del certificato COVID digitale dell'UE, dovrebbero essere stabilite norme generali per la compilazione dei certificati da utilizzare per i valori codificati nel contenuto del certificato COVID digitale dell'UE. Le serie di valori che attuano tali norme dovrebbero essere regolarmente aggiornate e pubblicate dalla Commissione, sulla base dei pertinenti lavori della rete eHealth.

(5) A norma del regolamento (UE) 2021/953, i certificati autentici che costituiscono il certificato COVID digitale dell'UE devono essere identificabili singolarmente mediante un identificativo univoco del certificato, tenendo conto del fatto che ai cittadini può essere rilasciato più di un certificato nel periodo in cui il regolamento (UE) 2021/953 rimane in vigore. L'identificativo univoco del certificato dev'essere costituito da una stringa alfanumerica e gli Stati membri dovrebbero garantire che non contenga dati che lo colleghino ad altri documenti o identificativi, come i numeri del passaporto o della carta d'identità, al fine di impedire che il titolare possa essere identificato. Per garantire che l'identificativo del certificato sia univoco, è opportuno stabilire specifiche tecniche e norme per la struttura comune dello stesso.

([1]) GU L 211 del 15.6.2021, pag. 1.

([2]) Direttiva 2011/24/UE del Parlamento europeo e del Consiglio, del 9 marzo 2011, concernente l'applicazione dei diritti dei pazienti relativi all'assistenza sanitaria transfrontaliera (GU L 88 del 4.4.2011, pag. 45).

(6) La sicurezza, l'autenticità, la validità e l'integrità dei certificati che costituiscono il certificato COVID digitale dell'UE e la loro conformità con il diritto dell'Unione in materia di protezione dei dati sono essenziali perché tutti gli Stati membri li accettino. Tali obiettivi sono conseguiti mediante il quadro di fiducia che stabilisce le norme riguardanti il rilascio e la verifica affidabili e sicuri dei certificati COVID digitali dell'UE, e le relative infrastrutture. Il quadro di fiducia dovrebbe essere basato, tra l'altro, su un'infrastruttura a chiave pubblica con una catena di fiducia che va dalle autorità sanitarie o dalle altre autorità designate degli Stati membri alle singole entità che rilasciano i certificati COVID digitali dell'UE. Pertanto, al fine di garantire un sistema di interoperabilità a livello dell'UE, la Commissione ha creato un sistema centrale, il gateway per i certificati COVID digitali dell'UE (il «gateway»), che memorizza le chiavi pubbliche utilizzate per la verifica. Quando il certificato con codice QR è scansionato, la firma digitale è verificata utilizzando la chiave pubblica pertinente, precedentemente memorizzata nel gateway centrale. Le firme digitali possono essere utilizzate per garantire l'integrità e l'autenticità dei dati. Le infrastrutture a chiave pubblica creano fiducia legando le chiavi pubbliche ai soggetti che hanno rilasciato i certificati. Per l'autenticità, nel gateway sono utilizzati diversi certificati a chiave pubblica. Per garantire uno scambio sicuro di dati per il materiale a chiave pubblica tra gli Stati membri e consentire un'ampia interoperabilità, è necessario stabilire i certificati a chiave pubblica che possono essere utilizzati e indicare come dovrebbero essere generati.

(7) La presente decisione consente di rendere operativi i requisiti del regolamento (UE) 2021/953 in modo da ridurre il trattamento dei dati personali al minimo necessario per rendere operativo il certificato COVID digitale dell'UE e contribuisce a un'attuazione da parte dei titolari del trattamento finali che rispetti la protezione dei dati fin dalla progettazione.

(8) Conformemente al regolamento (UE) 2021/953, le autorità competenti o altri organismi designati per il rilascio dei certificati sono titolari del trattamento ai sensi dell'articolo 4, punto 7, del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio ([3]) nel loro ruolo di trattamento dei dati personali nel corso della procedura di rilascio. A seconda del modo in cui gli Stati membri organizzano la procedura di rilascio, possono esserci una o più autorità o organismi designati, ad esempio i servizi sanitari regionali. Conformemente al principio di sussidiarietà, tale scelta spetta agli Stati membri. Pertanto gli Stati membri si trovano nella posizione migliore per garantire, in presenza di più autorità o altri organismi designati, che le rispettive responsabilità siano chiaramente ripartite, indipendentemente dal fatto che si tratti di titolari distinti o di contitolari del trattamento (compresi i servizi sanitari regionali che istituiscono un portale comune per i pazienti per il rilascio dei certificati). Analogamente, per quanto riguarda la verifica dei certificati da parte delle autorità competenti dello Stato membro di destinazione o di transito, o da parte degli operatori di servizi di trasporto passeggeri transfrontalieri tenuti, a norma del diritto nazionale, ad attuare determinate misure di sanità pubblica durante la pandemia di COVID-19, tali verificatori devono rispettare i loro obblighi ai sensi delle norme sulla protezione dei dati.

(9) Non avviene alcun trattamento dei dati personali attraverso il gateway per i certificati COVID digitali dell'UE, in quanto il gateway contiene solo le chiavi pubbliche delle autorità firmatarie. Tali chiavi si riferiscono alle autorità firmatarie e non consentono la reidentificazione diretta o indiretta di una persona fisica cui è stato rilasciato un certificato. Nel suo ruolo di gestore del gateway, la Commissione non dovrebbe pertanto essere né titolare del trattamento né responsabile del trattamento dei dati personali.

(10) Il Garante europeo della protezione dei dati è stato consultato conformemente all'articolo 42, paragrafo 1, del regolamento (UE) 2018/1725 del Parlamento europeo e del Consiglio ([4]) e ha espresso un parere il 22 giugno 2021.

(11) Considerando che le specifiche tecniche e le norme sono necessarie per l'applicazione del regolamento (UE) 2021/953 a decorrere dal 1º luglio 2021, l'applicazione immediata della presente decisione è giustificata.

(12) Pertanto, alla luce della necessità di una rapida attuazione del certificato COVID digitale dell'UE, è opportuno che la presente decisione entri in vigore il giorno della sua pubblicazione,

([3]) Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati) (GU L 119 del 4.5.2016, pag. 1).

([4]) Regolamento (UE) 2018/1725 del Parlamento europeo e del Consiglio, del 23 ottobre 2018, sulla tutela delle persone fisiche in relazione al trattamento dei dati personali da parte delle istituzioni, degli organi e degli organismi dell'Unione e sulla libera circolazione di tali dati, e che abroga il regolamento (CE) n. 45/2001 e la decisione n. 1247/2002/CE (GU L 295 del 21.11.2018, pag. 39).

HA ADOTTATO LA PRESENTE DECISIONE:

Articolo 1

Le specifiche tecniche del certificato COVID digitale dell'UE che stabiliscono la struttura dei dati generici, i meccanismi di codifica e il meccanismo di codifica di trasporto in un formato ottico leggibile meccanicamente sono stabilite nell'allegato I.

Articolo 2

Le norme per la compilazione dei certificati di cui all'articolo 3, paragrafo 1, del regolamento (UE) 2021/953 sono stabilite nell'allegato II della presente decisione.

Articolo 3

I requisiti che stabiliscono la struttura comune dell'identificativo univoco del certificato sono stabiliti nell'allegato III.

Articolo 4

Le norme di governance applicabili ai certificati a chiave pubblica in relazione al gateway per i certificati COVID digitali dell'UE a sostegno degli aspetti di interoperabilità del quadro di fiducia sono stabilite nell'allegato IV.

La presente decisione entra in vigore il giorno della pubblicazione nella *Gazzetta ufficiale dell'Unione europea*.

Fatto a Bruxelles, il 28 giugno 2021

Per la Commissione
La presidente
Ursula VON DER LEYEN

ALLEGATO I

FORMATO E GESTIONE DELLA FIDUCIA

Struttura dei dati generici, meccanismi di codifica e meccanismo di codifica di trasporto in un formato ottico leggibile meccanicamente (di seguito«QR»)

1. Introduzione

Le specifiche tecniche di cui al presente allegato contengono una struttura dei dati generici e meccanismi di codifica per il certificato COVID digitale dell'UE (Digital COVID Certificate — «DCC»). Specificano inoltre un meccanismo di codifica di trasporto in un formato ottico leggibile meccanicamente («QR») che possa essere visualizzato sullo schermo di un dispositivo mobile o stampato. I formati contenitore dei certificati sanitari elettronici delle presenti specifiche sono generici, ma in questo contesto sono utilizzati per trasportare il DCC.

2. Terminologia

Ai fini del presente allegato, per «emittenti» si intendono le organizzazioni che utilizzano le presenti specifiche per rilasciare i certificati sanitari e per «verificatori» si intendono le organizzazioni che accettano i certificati sanitari come prova dello stato sanitario. Per «partecipanti» si intendono gli emittenti e i verificatori. Alcuni aspetti indicati nel presente allegato devono essere coordinati tra i partecipanti, come la gestione di uno spazio dei nomi e la distribuzione delle chiavi crittografiche. Si presume che una parte, in appresso denominata «segretariato», svolga tali compiti.

3. Formato contenitore dei certificati sanitari elettronici

Il formato contenitore dei certificati sanitari elettronici (Electronic Health Certificate Container Format — «HCERT») è concepito per fornire un veicolo uniforme e standardizzato per i certificati sanitari dei diversi emittenti («emittenti»). L'obiettivo delle presenti specifiche è armonizzare il modo in cui tali certificati sanitari sono rappresentati, codificati e firmati allo scopo di agevolare l'interoperabilità.

La capacità di leggere e interpretare un DCC rilasciato da qualsiasi emittente richiede una struttura comune dei dati e un accordo sul significato di ciascun campo di dati del carico utile. Per agevolare tale interoperabilità, è definita una struttura comune coordinata dei dati mediante l'uso di uno schema «JSON» che costituisce il quadro del DCC.

3.1. *Struttura del carico utile*

Il carico utile è strutturato e codificato come CBOR con firma digitale COSE. Questo è comunemente noto come «CBOR Web Token» (CWT) ed è definito in RFC 8392 ([1]). Il carico utile, quale definito nelle sezioni che seguono, è trasportato in una richiesta hcert.

L'integrità e l'autenticità dell'origine dei dati del carico utile devono essere verificabili dal verificatore. Per fornire questo meccanismo, l'emittente deve firmare il CWT utilizzando uno schema di firma elettronica asimmetrica quale definito nella specifica COSE (RFC 8152 ([2])).

3.2. *Richieste CWT*

3.2.1. Panoramica della struttura CWT

Intestazione protetta

— Algoritmo di firma (alg, etichetta 1)

— Identificativo della chiave (kid, etichetta 4)

Carico utile

— Emittente (iss, chiave di richiesta 1, facoltativo, ISO 3166-1 alpha-2 dell'emittente)

— Momento del rilascio (iat, chiave di richiesta 6)

— Termine di scadenza (exp, chiave di richiesta 4)

— Certificato sanitario (hcert, chiave di richiesta -260)

— Certificato COVID digitale dell'UE v1 (eu_DCC_v1, chiave di richiesta 1)

Firma

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

3.2.2. Algoritmo di firma

Il parametro dell'algoritmo di firma (alg) indica l'algoritmo utilizzato per creare la firma. Deve rispettare o superare gli attuali orientamenti del SOGIS sintetizzati nei paragrafi seguenti.

Sono definiti un algoritmo primario e un algoritmo secondario. L'algoritmo secondario dovrebbe essere utilizzato solo se l'algoritmo primario non è accettabile nell'ambito delle norme e dei regolamenti imposti all'emittente.

Al fine di garantire la sicurezza del sistema, tutte le implementazioni devono incorporare l'algoritmo secondario. Per questo motivo, sia l'algoritmo primario che quello secondario devono essere implementati.

I livelli stabiliti dal SOGIS per gli algoritmi primari e secondari sono i seguenti.

— Algoritmo primario: l'algoritmo primario è l'algoritmo di firma digitale su curva ellittica (Elliptic Curve Digital Signature Algorithm — ECDSA) quale definito nella sezione 2.3 (ISO/IEC 14888–3:2006) utilizzando i parametri P–256 definiti nell'appendice D (D.1.2.3) di (FIPS PUB 186-4) in combinazione con l'algoritmo hash SHA–256 quale definito nella funzione 4 (ISO/IEC 10118–3:2004).

Questo corrisponde al parametro dell'algoritmo COSE ES256.

— Algoritmo secondario: l'algoritmo secondario è RSASSA-PSS quale definito in (RFC 8230 ([3])) con un modulo di 2048 bit in combinazione con l'algoritmo hash SHA–256 quale definito nella funzione 4 (ISO/IEC 10118–3:2004).

Questo corrisponde al parametro dell'algoritmo COSE PS256.

3.2.3. Identificativo della chiave

La richiesta Identificativo della chiave (kid) indica il certificato di firma digitale (Document Signer Certificate — DSC) contenente la chiave pubblica che il verificatore deve utilizzare per controllare la correttezza della firma digitale. Nell'allegato IV è descritta la governance dei certificati a chiave pubblica, compresi i requisiti per i DSC.

La richiesta Identificativo della chiave (kid) è utilizzata dai verificatori per selezionare la chiave pubblica corretta da un elenco di chiavi relative all'emittente indicato nella richiesta Emittente (iss). Un emittente può utilizzare diverse chiavi in parallelo per motivi amministrativi e quando effettua i rinnovi delle chiavi. L'identificativo della chiave non è un campo critico per la sicurezza. Per questo motivo, se necessario, può anche essere collocato in un'intestazione non protetta. I verificatori devono accettare entrambe le opzioni. Se entrambe le opzioni sono presenti, deve essere utilizzato l'identificativo della chiave nell'intestazione protetta.

A causa dell'accorciamento dell'identificativo (per motivi di limitazione delle dimensioni) vi è una probabilità molto bassa, ma non inesistente, che l'elenco generale dei DSC accettati da un verificatore possa contenere DSC con kid doppi. Per questo motivo il verificatore deve controllare tutti i DSC con tale kid.

3.2.4. Emittente

La richiesta Emittente (iss) è un valore di stringa che può facoltativamente riportare il codice paese ISO 3166-1 alpha-2 del soggetto che ha rilasciato il certificato sanitario. Tale richiesta può essere utilizzata da un verificatore per individuare la serie di DSC da utilizzare per la verifica. La chiave di richiesta 1 è utilizzata per identificare questa richiesta.

3.2.5. Termine di scadenza

La richiesta Termine di scadenza (exp) deve contenere una marcatura temporale nel formato NumericDate intero (come specificato in RFC 8392 ([4]), sezione 2) che indichi per quanto tempo quella particolare firma sul carico utile è considerata valida e decorso il quale il verificatore deve rifiutare il carico utile come scaduto. Il parametro del termine di scadenza ha lo scopo di imporre un limite al periodo di validità del certificato sanitario. La chiave di richiesta 4 è utilizzata per identificare questa richiesta.

Il termine di scadenza non deve cadere oltre il periodo di validità del DSC.

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

3.2.6. Momento del rilascio

La richiesta Momento del rilascio (iat) deve contenere una marcatura temporale nel formato NumericDate intero (come specificato in RFC 8392 ([5]), sezione 2) indicante il momento in cui è stato creato il certificato sanitario.

Il campo Momento del rilascio non deve indicare una data anteriore al periodo di validità del DSC.

I verificatori possono applicare policy aggiuntive allo scopo di limitare la validità del certificato sanitario in base al momento del rilascio. La chiave di richiesta 6 è utilizzata per identificare questa richiesta.

3.2.7. Richiesta Certificato sanitario

La richiesta Certificato sanitario (hcert) è un oggetto JSON (RFC 7159 ([6])) contenente le informazioni sullo stato sanitario. Nell'ambito della stessa richiesta possono esistere diversi tipi di certificato sanitario, tra cui il DCC.

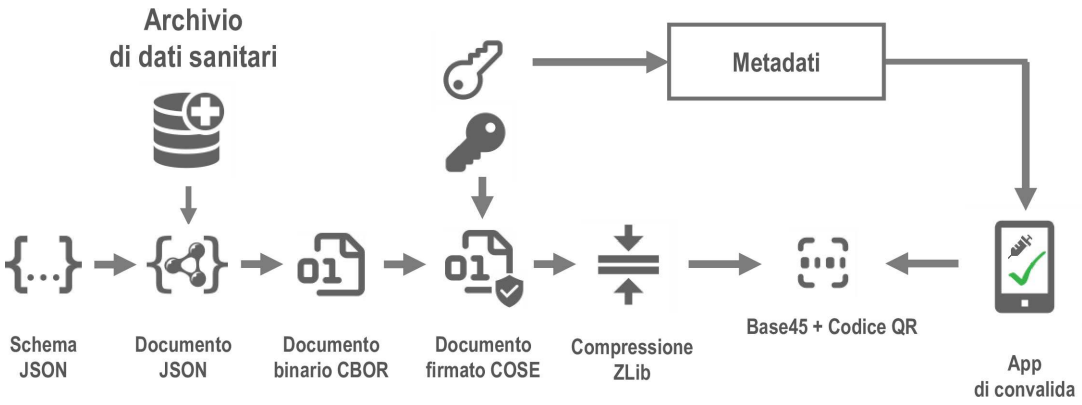
Il formato JSON serve esclusivamente per finalità di schema. Il formato di rappresentazione è CBOR, come definito in (RFC 7049 ([7])). Gli sviluppatori di applicazioni non possono in realtà mai decodificare o codificare da e verso il formato JSON, bensì utilizzano la struttura in-memory.

La chiave di richiesta da utilizzare per identificare questa richiesta è -260.

Le stringhe dell'oggetto JSON dovrebbero essere normalizzate secondo la Normalization Form Canonical Composition (NFC) definita nello standard Unicode. Le applicazioni di decodifica dovrebbero tuttavia essere permissive e solide in relazione a questi aspetti ed è fortemente incoraggiata l'accettazione di qualsiasi tipo di conversione ragionevole. Se durante la decodifica o nelle successive funzioni di confronto si riscontrano dati non normalizzati, le implementazioni dovrebbero comportarsi come se l'immissione fosse normalizzata NFC.

4. Serializzazione e creazione del carico utile DCC

Come modello di serializzazione si utilizza lo schema seguente:



Il processo inizia con l'estrazione dei dati, ad esempio da un archivio di dati sanitari (o da qualche fonte di dati esterna), e con la strutturazione dei dati estratti secondo gli schemi DCC definiti. In questo processo, la conversione nel formato di dati definito e la trasformazione per la leggibilità da parte dell'uomo possono aver luogo prima dell'inizio della serializzazione CBOR. Gli acronimi delle richieste sono in ogni caso mappati ai nomi visualizzati prima della serializzazione e dopo la deserializzazione.

Non sono consentiti contenuti di dati nazionali facoltativi nei certificati rilasciati a norma del regolamento (UE) 2021/953 ([8]). Il contenuto di dati è limitato agli elementi di dati definiti nella serie minima di dati specificata nell'allegato del regolamento (UE) 2021/953.

([5]) rfc8392 (ietf.org).
([6]) rfc7159 (ietf.org).
([7]) rfc7049 (ietf.org).
([8]) Regolamento (UE) 2021/953 del Parlamento europeo e del Consiglio, del 14 giugno 2021, su un quadro per il rilascio, la verifica e l'accettazione di certificati interoperabili di vaccinazione, di test e di guarigione in relazione alla COVID-19 (certificato COVID digitale dell'UE) per agevolare la libera circolazione delle persone durante la pandemia di COVID-19 (GU L 211 del 15.6.2021, pag. 1).

5. **Codifiche di trasporto**

5.1. *Codifica grezza*

Per le interfacce di dati arbitrari, il contenitore HCERT e i suoi carichi utili possono essere trasferiti tal quali, utilizzando qualsiasi trasporto di dati sottostante sicuro e affidabile a 8 bit. Queste interfacce possono comprendere la comunicazione di prossimità (Near-Field Communication — NFC), il Bluetooth o il trasferimento attraverso un protocollo di livello applicazione, ad esempio il trasferimento di un HCERT dall'emittente al dispositivo mobile del titolare.

Se il trasferimento dell'HCERT dall'emittente al titolare si basa su un'interfaccia di sola presentazione (ad esempio SMS, e-mail), la codifica di trasporto grezza non è ovviamente applicabile.

5.2. *Codice a barre*

5.2.1. Compressione del carico utile (CWT)

Per ridurre le dimensioni e migliorare la velocità e l'affidabilità nel processo di lettura dell'HCERT, il CWT è compresso utilizzando ZLIB (RFC 1950 ([9])) e il meccanismo di compressione Deflate nel formato definito in RFC 1951 ([10]).

5.2.2. Codice a barre 2D QR

Ai fini di una migliore gestione delle apparecchiature preesistenti progettate per funzionare sui carichi utili ASCII, il CWT compresso è codificato come ASCII utilizzando Base45 prima di essere codificato in un codice a barre 2D.

Il formato QR quale definito nella norma (ISO/IEC 18004:2015) è utilizzato per la generazione di codici a barre 2D. Si raccomanda un tasso di correzione degli errori di «Q» (circa il 25 %). Poiché si utilizza Base45, il codice QR deve utilizzare la codifica alfanumerica (modalità 2, indicata dai simboli 0010).

Affinché i verificatori siano in grado di rilevare il tipo di dati codificati e di selezionare il sistema adeguato di decodifica e trattamento, i dati codificati Base45 (secondo la presente specifica) hanno come prefisso la stringa dell'identificativo di contesto «HC1:». Le versioni future della presente specifica che incidono sulla retrocompatibilità definiranno un nuovo identificativo di contesto, mentre il carattere che segue «HC» sarà tratto dalla serie di caratteri [1-9 A-Z]. L'ordine degli incrementi è definito in tale ordine, ossia prima [1-9] e successivamente [A-Z].

Si raccomanda di rendere il codice ottico sul supporto di presentazione con dimensioni della diagonale comprese tra 35 mm e 60 mm per i lettori con ottica fissa in cui i supporti di presentazione devono essere collocati sulla superficie del lettore.

Se il codice ottico è stampato su carta con stampanti a bassa risoluzione (< 300 dpi), si deve prestare attenzione a rappresentare ciascun simbolo (punto) del codice QR esattamente quadrato. Se il ridimensionamento non sarà proporzionale, alcune righe o colonne del codice QR avranno simboli rettangolari, il che in molti casi ostacolerà la leggibilità.

6. **Formato dell'elenco di fiducia (elenco di CSCA e DSC)**

Ciascuno Stato membro è tenuto a fornire un elenco di una o più autorità nazionali di certificazione (Country Signing Certificate Authority — CSCA) e un elenco di tutti i certificati di firma digitale (DSC) validi e a mantenere tali elenchi aggiornati.

6.1. *CSCA/DSC semplificati*

A partire da questa versione delle specifiche, gli Stati membri non presumono che siano utilizzate informazioni relative all'elenco dei certificati revocati (Certificate Revocation List — CRL) o che il periodo di utilizzo della chiave privata sia verificato dagli attuatori.

Il meccanismo di validità principale è invece la presenza del certificato nella versione più recente dell'elenco dei certificati.

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

6.2. *Infrastruttura a chiave pubblica eMRTD conforme ICAO e centri protezione*

Gli Stati membri possono ricorrere a una CSCA distinta, ma possono anche presentare i loro certificati CSCA e/o DSC eMRTD esistenti; inoltre possono anche scegliere di procurarseli presso centri protezione (commerciali) e di presentare questi ultimi. Tuttavia qualsiasi DSC deve sempre essere firmato dalla CSCA presentata da tale Stato membro.

7. **Considerazioni in materia di sicurezza**

Nel progettare uno schema basato su questa specifica, gli Stati membri individuano, analizzano e monitorano taluni aspetti legati alla sicurezza.

Dovrebbero essere presi in considerazione almeno gli aspetti seguenti.

7.1. *Periodo di validità della firma HCERT*

L'emittente degli HCERT è tenuto a limitare il periodo di validità della firma specificando un termine di scadenza. Ciò impone al titolare di un certificato sanitario di rinnovarlo periodicamente.

Il periodo di validità accettabile può essere determinato da vincoli pratici. Ad esempio, un viaggiatore potrebbe non avere la possibilità di rinnovare il certificato sanitario durante un viaggio all'estero. Tuttavia può anche accadere che un emittente stia valutando la possibilità di una qualche forma di compromissione della sicurezza che gli impone di ritirare un DSC (invalidando tutti i certificati sanitari rilasciati utilizzando tale chiave ancora entro il loro periodo di validità). Le conseguenze di un tale evento possono essere limitate effettuando una regolare rotazione delle chiavi emittente e richiedendo il rinnovo di tutti i certificati sanitari a intervalli ragionevoli.

7.2. *Gestione delle chiavi*

Questa specifica si basa in larga misura su solidi meccanismi crittografici che garantiscono l'integrità dei dati e l'autenticazione dell'origine dei dati. È pertanto necessario mantenere la riservatezza delle chiavi private.

La riservatezza delle chiavi crittografiche può essere compromessa in vari modi, ad esempio:

— il processo di generazione delle chiavi può essere viziato, con conseguente debolezza delle chiavi;

— le chiavi possono essere rivelate per errore umano;

— le chiavi possono essere rubate da soggetti esterni o interni;

— le chiavi possono essere calcolate mediante crittoanalisi.

Al fine di mitigare i rischi che l'algoritmo di firma sia debole e consenta di compromettere le chiavi private mediante crittoanalisi, questa specifica raccomanda a tutti i partecipanti di implementare un algoritmo di firma secondario di riserva, basato su parametri diversi o su un problema matematico diverso da quello primario.

Per quanto riguarda i rischi menzionati relativi agli ambienti operativi degli emittenti, sono attuate misure di mitigazione per garantire un controllo efficace, in modo da generare, memorizzare e utilizzare le chiavi private nei moduli di sicurezza hardware (Hardware Security Model — HSM). L'uso di HSM per la firma dei certificati sanitari è fortemente incoraggiato.

Indipendentemente dal fatto che un emittente decida di utilizzare gli HSM o no, è opportuno stabilire un calendario dei rinnovi delle chiavi la cui frequenza sia proporzionata all'esposizione delle chiavi a reti esterne, altri sistemi e personale. Un calendario dei rinnovi ben scelto limita inoltre i rischi associati ai certificati sanitari rilasciati erroneamente, consentendo all'emittente di revocare tali certificati in lotti, ritirando una chiave, se necessario.

7.3. *Convalida dei dati immessi*

Queste specifiche possono essere utilizzate in modo da implicare il ricevimento di dati da fonti non fidate in sistemi che possono essere di natura critica. Per ridurre al minimo i rischi associati a questo vettore di attacco, tutti i campi di immissione devono essere debitamente convalidati in termini di tipi di dati, lunghezze e contenuto. Prima di qualsiasi trattamento del contenuto dell'HCERT è verificata anche la firma dell'emittente. Tuttavia la convalida della firma dell'emittente implica innanzitutto l'analisi dell'intestazione protetta dell'emittente, nella quale un potenziale aggressore potrebbe tentare di iniettare informazioni accuratamente preparate per compromettere la sicurezza del sistema.

8. **Gestione della fiducia**

La firma dell'HCERT richiede una chiave pubblica da verificare. Gli Stati membri mettono a disposizione tali chiavi pubbliche. In ultima analisi, ogni verificatore deve disporre di un elenco di tutte le chiavi pubbliche di cui intende fidarsi (dato che la chiave pubblica non fa parte dell'HCERT).

Il sistema è costituito (solo) da due livelli; per ciascuno Stato membro, uno o più certificati di livello nazionale che firmano ognuno uno o più certificati di firma digitale utilizzati nelle operazioni quotidiane.

I certificati degli Stati membri sono denominati certificati dell'autorità nazionale di certificazione (CSCA) e sono (di norma) autofirmati. Gli Stati membri possono averne più di una (ad esempio, in caso di decentramento regionale). Questi certificati CSCA firmano regolarmente i certificati di firma digitale (DSC) utilizzati per firmare gli HCERT.

Il «segretariato» svolge un ruolo funzionale. Esso aggrega e pubblica periodicamente i DSC degli Stati membri, dopo averli verificati sulla base dell'elenco dei certificati CSCA (che sono stati trasmessi e verificati con altri mezzi).

L'elenco risultante dei DSC fornisce quindi la serie aggregata di chiavi pubbliche accettabili (e i relativi identificativi) che i verificatori possono utilizzare per convalidare le firme sugli HCERT. I verificatori devono estrarre e aggiornare regolarmente questo elenco.

Tali elenchi specifici degli Stati membri possono essere adattati nel formato per il proprio contesto nazionale. Pertanto il formato di file di questo elenco di fiducia può variare; ad esempio può trattarsi di un formato JWKS firmato (formato JWK Set per RFC 7517 ([11]), sezione 5) o di qualsiasi altro formato specifico per la tecnologia utilizzata in tale Stato membro.

Al fine di garantire la semplicità, gli Stati membri possono presentare i loro certificati CSCA esistenti generati dai rispettivi sistemi eMRTD conformi ICAO o, come raccomandato dall'OMS, crearne uno specifico per questo settore sanitario.

8.1. *Identificativo della chiave (kid)*

L'identificativo della chiave (kid) è calcolato quando si costruisce l'elenco delle chiavi pubbliche fidate dei DSC ed è costituito da un'impronta digitale SHA-256 troncata (primi 8 byte) del DSC codificato nel formato (grezzo) DER.

I verificatori non sono tenuti a calcolare l'identificativo della chiave sulla base del DSC e possono far collimare direttamente l'identificativo della chiave nel certificato sanitario rilasciato con quello figurante nell'elenco di fiducia.

8.2. *Differenze rispetto al modello di fiducia dell'infrastruttura a chiave pubblica eMRTD conforme ICAO*

Nonostante la modellizzazione sulle migliori pratiche del modello di fiducia dell'infrastruttura a chiave pubblica (Public Key Infrastructure — PKI) eMRTD conforme ICAO, è necessario introdurre una serie di semplificazioni nell'interesse della velocità:

— uno Stato membro può presentare più certificati CSCA;

— il periodo di validità del DSC (utilizzo della chiave) può essere fissato a una durata non superiore a quella del certificato CSCA e può essere assente;

— il DSC può contenere identificativi di policy (utilizzo esteso della chiave) specifici dei certificati sanitari;

— gli Stati membri possono scegliere di non effettuare mai alcuna verifica delle revoche pubblicate e di affidarsi esclusivamente agli elenchi di DSC che ricevono quotidianamente dal segretariato o che compilano essi stessi.

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

ALLEGATO II

NORME PER LA COMPILAZIONE DEL CERTIFICATO COVID DIGITALE DELL'UE

Le norme generali relative alle serie di valori stabilite nel presente allegato mirano a garantire l'interoperabilità a livello semantico e consentono implementazioni tecniche uniformi per il DCC. Gli elementi contenuti nel presente allegato possono essere utilizzati per i tre diversi scenari (vaccinazione/test/guarigione) previsti dal regolamento (UE) 2021/953. Nel presente allegato sono elencati solo gli elementi che richiedono una standardizzazione semantica mediante serie di valori codificati.

La traduzione degli elementi codificati nella lingua nazionale è di competenza degli Stati membri.

Per tutti i campi di dati non menzionati nelle seguenti descrizioni delle serie di valori, si raccomanda la codifica in UTF-8 (nome, centro in cui è stato effettuato il test, soggetto che ha rilasciato il certificato). Si raccomanda di codificare i campi di dati contenenti date (data di nascita, data di vaccinazione, data del prelievo del campione, data del primo risultato positivo al test, date di validità del certificato) secondo la norma ISO 8601.

Se per qualsiasi motivo non è possibile utilizzare i sistemi di codici preferiti elencati di seguito, possono essere utilizzati altri sistemi di codici internazionali ed è opportuno predisporre suggerimenti su come mappare i codici dell'altro sistema di codici al sistema di codici preferito. Il testo (nomi visualizzati) può essere utilizzato in casi eccezionali come meccanismo di backup quando nelle serie di valori definite non è disponibile un codice adeguato.

Gli Stati membri che utilizzano altri codici nei loro sistemi dovrebbero mappare tali codici alle serie di valori descritte. Gli Stati membri sono responsabili di tali mappature.

La Commissione aggiorna regolarmente le serie di valori con il sostegno della rete eHealth e del comitato per la sicurezza sanitaria. Le serie di valori aggiornate sono pubblicate sul pertinente sito web della Commissione e sulla pagina web della rete eHealth. Dovrebbe essere fornita una cronologia delle modifiche.

1. **Malattia o agente in questione/malattia o agente da cui il titolare è guarito: COVID-19 (SARS-CoV-2 o una delle sue varianti)**

   Sistema di codici preferito: SNOMED CT.

   Da utilizzare nei certificati 1, 2 e 3.

   I codici selezionati fanno riferimento alla COVID-19 o, se sono necessarie informazioni più dettagliate sulla variante genetica del SARS-CoV-2, a tali varianti laddove tali informazioni dettagliate siano necessarie per motivi epidemiologici.

   Un esempio di codice da utilizzare è il codice SNOMED CT 840539006 (COVID-19).

2. **Vaccino o profilassi anti COVID-19**

   Sistema di codici preferito: SNOMED CT o classificazione ATC.

   Da utilizzare nel certificato 1.

   Esempi di codici da utilizzare, tratti dai sistemi di codici preferiti, sono il codice SNOMED CT 1119305005 (vaccino antigenico contro il SARS-CoV-2), 1119349007 (vaccino a mRNA contro il SARS-CoV-2) o J07BX03 (vaccini anti COVID-19). La serie di valori dovrebbe essere estesa man mano che vengono sviluppati e messi in uso nuovi tipi di vaccini.

3. **Medicinale vaccinale anti COVID-19**

   Sistemi di codici preferiti (in ordine di preferenza):

   — registro dell'Unione dei medicinali per i vaccini con autorizzazione a livello dell'UE (numeri di autorizzazione);

   — un registro globale dei vaccini come quello che potrebbe essere istituito dall'Organizzazione mondiale della sanità;

   — nome del medicinale vaccinale negli altri casi. Se il nome comprende spazi vuoti, questi devono essere sostituiti da un trattino (-).

Nome della serie di valori: Vaccino.

Da utilizzare nel certificato 1.

Un esempio di codice da utilizzare, tratto dai sistemi di codici preferiti, è EU/1/20/1528 (Comirnaty). Esempio di nome del vaccino da utilizzare come codice: Sputnik-V (che sta per Sputnik V).

4. **Titolare dell'autorizzazione all'immissione in commercio del vaccino anti COVID-19 o fabbricante del vaccino**

Sistema di codici preferito:

— codice organismo dell'EMA (sistema SPOR per ISO IDMP);

— un registro globale dei titolari dell'autorizzazione all'immissione in commercio dei vaccini o dei fabbricanti di vaccini, come quello che potrebbe essere istituito dall'Organizzazione mondiale della sanità;

— nome dell'organismo negli altri casi. Se il nome comprende spazi vuoti, questi devono essere sostituiti da un trattino (-).

Da utilizzare nel certificato 1.

Un esempio di codice da utilizzare, tratto dal sistema di codici preferito, è ORG-100001699 (AstraZeneca AB). Esempio di nome dell'organismo da utilizzare come codice: Sinovac-Biotech (che sta per Sinovac Biotech).

5. **Numero in una serie di dosi e numero complessivo di dosi di una serie**

Da utilizzare nel certificato 1.

Due campi:

1) numero di dosi somministrate in un ciclo;

2) numero di dosi previste per un ciclo completo (specifiche per una persona al momento della somministrazione).

Ad esempio, 1/1 o 2/2 indicherà che il ciclo è stato completato; l'opzione 1/1 si utilizza anche per i vaccini che prevedono due dosi, ma per i quali il protocollo applicato dallo Stato membro prevede di somministrare una dose ai cittadini cui sia stata diagnosticata la COVID-19 prima della vaccinazione. Il numero complessivo di dosi di una serie dovrebbe essere indicato in base alle informazioni disponibili al momento della somministrazione della dose. Ad esempio, se un vaccino specifico richiede un terzo richiamo al momento dell'ultima somministrazione, ciò dovrà essere rispecchiato dal numero nel secondo campo (ad esempio 2/3, 3/3 ecc.).

6. **Stato membro o paese terzo in cui è stato somministrato il vaccino/effettuato il test**

Sistema di codici preferito: codici paese secondo la norma ISO 3166.

Da utilizzare nei certificati 1, 2 e 3.

Contenuto della serie di valori: l'elenco completo dei codici a 2 lettere, disponibile come serie di valori secondo la definizione in FHIR (http://hl7.org/fhir/ValueSet/iso3166-1-2).

7. **Tipo di test**

Sistema di codici preferito: LOINC.

Da utilizzare nel certificato 2, e nel certificato 3 qualora mediante un atto delegato sia introdotto il sostegno per il rilascio di certificati di guarigione basati su tipi di test diversi dai test di amplificazione dell'acido nucleico (NAAT).

I codici di questa serie di valori si riferiscono al metodo di test e sono selezionati almeno per distinguere i test NAAT dai test antigenici rapidi (RAT), come indicato nel regolamento (UE) 2021/953.

Un esempio di codice da utilizzare, tratto dal sistema di codici preferito, è LP217198-3 (immunodosaggio rapido).

8. **Fabbricante e denominazione commerciale del test utilizzato (facoltativo per i test NAAT)**

Sistema di codici preferito: elenco dei test antigenici rapidi del CSS, tenuto dal JRC (banca dati dei dispositivi diagnostici in vitro e dei metodi di test COVID-19).

Da utilizzare nel certificato 2.

Il contenuto della serie di valori comprende la selezione del test antigenico rapido elencato nell'elenco comune e aggiornato dei test antigenici rapidi per la COVID-19, stabilito sulla base della raccomandazione 2021/C 24/01 del Consiglio e approvato dal comitato per la sicurezza sanitaria. L'elenco è tenuto dal JRC nella banca dati dei dispositivi diagnostici in vitro e dei metodi di test COVID-19 all'indirizzo seguente: https://covid-19-diagnostics.jrc.ec.europa.eu/devices/hsc-common-recognition-rat.

Per questo sistema di codici devono essere utilizzati campi pertinenti quali l'identificativo del dispositivo diagnostico, il nome del test e il fabbricante, secondo il formato strutturato del JRC disponibile all'indirizzo https://covid-19-diagnostics.jrc.ec.europa.eu/devices.

9. **Risultato del test**

Sistema di codici preferito: SNOMED CT.

Da utilizzare nel certificato 2.

I codici selezionati consentono di distinguere tra risultati positivi e negativi al test (rilevato o non rilevato). Se i casi d'uso lo richiedono, possono essere aggiunti altri valori (ad esempio, indeterminato).

Esempi di codici da utilizzare, tratti dal sistema di codici preferito, sono 260415000 (non rilevato) e 260373001 (rilevato).

ALLEGATO III

STRUTTURA COMUNE DELL'IDENTIFICATIVO UNIVOCO DEL CERTIFICATO

1. **Introduzione**

Ciascun certificato COVID digitale dell'UE (DCC) include un identificativo univoco del certificato (Unique Certificate Identifier — UCI) che sostiene l'interoperabilità dei DCC. L'UCI può essere utilizzato per verificare il certificato. Gli Stati membri sono responsabili della sua attuazione. L'UCI è un mezzo per verificare la veridicità del certificato e, se del caso, per collegarsi a un sistema di registrazione (ad esempio, un sistema informativo sulla vaccinazione). Questi identificativi consentono inoltre agli Stati membri di affermare (su supporto cartaceo e digitale) che le persone sono state vaccinate o sottoposte a test.

2. **Composizione dell'identificativo univoco del certificato**

L'UCI segue una struttura e un formato comuni che agevolano l'interpretazione delle informazioni da parte dell'uomo e/o della macchina e può riguardare elementi quali lo Stato membro di vaccinazione, il vaccino stesso e l'identificativo specifico di uno Stato membro. Garantisce agli Stati membri la flessibilità necessaria per la sua formattazione, nel pieno rispetto della legislazione in materia di protezione dei dati. L'ordine dei distinti elementi segue una gerarchia definita che può consentire future modifiche dei blocchi, mantenendone nel contempo l'integrità strutturale.

Le possibili soluzioni per la composizione dell'UCI formano uno spettro in cui la modularità e l'interpretabilità da parte dell'uomo costituiscono i due principali parametri di diversificazione e una caratteristica fondamentale:

— modularità: la misura in cui il codice è composto da blocchi costitutivi distinti che contengono informazioni semanticamente diverse;

— interpretabilità da parte dell'uomo: la misura in cui il codice è significativo o può essere interpretato da un lettore umano;

— univocità a livello mondiale: l'identificativo del paese o dell'autorità è ben gestito e ogni paese (autorità) è tenuto a gestire adeguatamente il proprio segmento nello spazio dei nomi senza riciclare o riemettere gli identificativi. Questa combinazione garantisce che ciascun identificativo sia univoco a livello mondiale.

3. **Requisiti generali**

In relazione all'UCI dovrebbero essere soddisfatti i requisiti generali seguenti:

1) serie di caratteri: sono ammessi solo caratteri alfanumerici US-ASCII maiuscoli (da «A» a «Z», da «0» a «9»), con caratteri speciali aggiuntivi per la separazione da RFC 3986 ([1]), ([2]), vale a dire {«/», «#», «:»};

2) lunghezza massima: i programmatori dovrebbero cercare di rispettare una lunghezza di 27-30 caratteri ([3]);

3) prefisso della versione: si riferisce alla versione dello schema UCI. Il prefisso della versione è «01» per questa versione del documento ed è composto da due cifre;

4) prefisso del paese: il codice paese è specificato dalla norma ISO 3166-1. Codici più lunghi (ad esempio 3 e più caratteri come nel caso di «UNHCR») sono riservati all'uso futuro;

5) suffisso del codice/somma di controllo.

5.1. Gli Stati membri dovrebbero utilizzare una somma di controllo quando è probabile che si verifichino la trasmissione, la trascrizione (umana) o altre forme di corruzione (vale a dire l'utilizzo in forma stampata).

5.2. La somma di controllo non deve essere utilizzata per convalidare il certificato e non fa tecnicamente parte dell'identificativo, bensì è utilizzata per verificare l'integrità del codice. Tale somma di controllo deve essere la sintesi secondo la norma ISO 7812-1 (LUHN-10) ([4]) dell'intero UCI in formato di trasporto digitale/elettronico. La somma di controllo è separata dal resto dell'UCI da un carattere «#».

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

([2]) Campi quali il genere, il numero di lotto, il centro di somministrazione, l'identificazione dell'operatore sanitario, la data della prossima vaccinazione possono non essere necessari per scopi diversi dall'uso medico.

([3]) Per l'implementazione con codici QR, gli Stati membri potrebbero prendere in considerazione la possibilità di utilizzare una serie supplementare di caratteri fino a una lunghezza totale di 72 caratteri (compresi i 27-30 caratteri dell'identificativo stesso) per trasmettere altre informazioni. Spetta agli Stati membri definire la specifica di tali informazioni.

([4]) L'algoritmo di Luhn mod N è un'estensione dell'algoritmo di Luhn (noto anche come algoritmo mod 10) che funziona per i codici numerici ed è utilizzato ad esempio per calcolare la somma di controllo delle carte di credito. L'estensione consente all'algoritmo di funzionare con sequenze di valori su qualsiasi base (nel nostro caso caratteri alfa).

Occorre garantire la retrocompatibilità: gli Stati membri che nel corso del tempo modificano la struttura dei loro identificativi (nella versione principale, attualmente fissata a v1) sono tenuti a garantire che due identificativi identici rappresentino la stessa dichiarazione/lo stesso certificato di vaccinazione. In altre parole, gli Stati membri non possono riciclare gli identificativi.

4. **Opzioni per gli identificativi univoci dei certificati per i certificati di vaccinazione**

Gli orientamenti della rete eHealth per i certificati di vaccinazione verificabili e gli elementi fondamentali di interoperabilità ([5]) prevedono diverse opzioni a disposizione degli Stati membri e di altre parti che possono coesistere tra i diversi Stati membri. Gli Stati membri possono utilizzare tali diverse opzioni in versioni diverse dello schema UCI.

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

ALLEGATO IV

GOVERNANCE DEI CERTIFICATI A CHIAVE PUBBLICA

1. Introduzione

Lo scambio sicuro e fidato delle chiavi di firma per i certificati COVID digitali dell'UE (DCC) tra gli Stati membri è realizzato dal gateway per i certificati COVID digitali dell'UE (Digital COVID Certificate Gateway — DCCG), che funge da archivio centrale per le chiavi pubbliche. Con il DCCG, gli Stati membri sono abilitati a pubblicare le chiavi pubbliche corrispondenti alle chiavi private che utilizzano per firmare i certificati COVID digitali. Gli Stati membri che se ne avvalgono possono utilizzare il DCCG per estrarre in tempo utile materiale aggiornato relativo alle chiavi pubbliche. Successivamente, il DCCG potrà essere esteso allo scambio di informazioni supplementari affidabili fornite dagli Stati membri, come le norme di convalida per i DCC. Il modello di fiducia del quadro DCC è un'infrastruttura a chiave pubblica (PKI). Ciascuno Stato membro mantiene una o più autorità nazionali di certificazione (CSCA) i cui certificati hanno una durata di vita relativamente lunga. A seguito della decisione dello Stato membro, la CSCA può essere uguale o diversa dalla CSCA utilizzata per i documenti di viaggio leggibili a macchina. La CSCA rilascia certificati a chiave pubblica per i firmatari di documenti nazionali di breve durata (ossia i firmatari dei DCC), denominati certificati di firma digitale (DSC). La CSCA agisce come un'ancora di fiducia in modo che gli Stati membri che se ne avvalgono possano utilizzare il certificato CSCA per convalidare l'autenticità e l'integrità dei DSC che cambiano regolarmente. Una volta effettuata la convalida, gli Stati membri possono fornire tali certificati (o solo le chiavi pubbliche in essi contenute) alle loro applicazioni di convalida dei DCC. Oltre alle CSCA e ai DSC, il DCCG si avvale anche della PKI per autenticare le transazioni, firmare i dati, come base per l'autenticazione e come mezzo per garantire l'integrità dei canali di comunicazione tra gli Stati membri e il DCCG.

Le firme digitali possono essere utilizzate per garantire l'integrità e l'autenticità dei dati. Le infrastrutture a chiave pubblica creano fiducia legando le chiavi pubbliche a identità verificate (o emittenti). Ciò è necessario per consentire agli altri partecipanti di verificare l'origine dei dati e l'identità del partner della comunicazione e di decidere in merito alla fiducia. Per l'autenticità, nel DCCG sono utilizzati diversi certificati a chiave pubblica. Il presente allegato definisce quali certificati a chiave pubblica sono utilizzati e come devono essere concepiti al fine di consentire un'ampia interoperabilità tra gli Stati membri. Esso fornisce maggiori dettagli sui necessari certificati a chiave pubblica, nonché orientamenti sui modelli di certificato e sui periodi di validità per gli Stati membri che intendono gestire una propria CSCA. Poiché i DCC devono essere verificabili per un periodo di tempo definito (a partire dal rilascio, scadono dopo un determinato periodo di tempo), è necessario definire un modello di verifica per tutte le firme applicate sui certificati a chiave pubblica e sui DCC.

2. Terminologia

La tabella seguente riporta le abbreviazioni e la terminologia utilizzate in tutto il presente allegato.

Termine	Definizione
Certificato	O certificato a chiave pubblica. Un certificato X.509 v3 contenente la chiave pubblica di un'entità.
CSCA	Autorità nazionale di certificazione
DCC	Certificato COVID digitale dell'UE. Un documento digitale firmato contenente informazioni sulla vaccinazione, sul test o sulla guarigione.
DCCG	Gateway per i certificati COVID digitali dell'UE. Questo sistema è utilizzato per scambiare DSC tra gli Stati membri.
$DCCG_{TA}$	Il certificato dell'ancora di fiducia del DCCG. La chiave privata corrispondente è utilizzata per firmare l'elenco di tutti i certificati CSCA off-line.
$DCCG_{TLS}$	Il certificato del server TLS del DCCG
DSC	Certificato di firma digitale. Il certificato a chiave pubblica dell'autorità preposta alla firma dei documenti di uno Stato membro (ad esempio un sistema autorizzato a firmare i DCC). Tale certificato è rilasciato dalla CSCA dello Stato membro.
EC-DSA	Algoritmo di firma digitale su curva ellittica. Un algoritmo di firma crittografica basato su curve ellittiche.
Stato membro	Stato membro dell'Unione europea

Termine	Definizione
mTLS	TLS reciproco. Il protocollo Transport Layer Security con autenticazione reciproca.
NB:	Back-end nazionale di uno Stato membro
NB_{CSCA}	Il certificato CSCA di uno Stato membro (potrebbe essere più di uno)
NB_{TLS}	Il certificato di autenticazione del client TLS di un back-end nazionale
NB_{UP}	Il certificato utilizzato da un back-end nazionale per firmare pacchetti di dati caricati sul DCCG
PKI	Infrastruttura a chiave pubblica. Modello di fiducia basato su certificati a chiave pubblica e autorità di certificazione.
RSA	Algoritmo crittografico asimmetrico basato sulla fattorizzazione dei numeri interi utilizzato per le firme digitali o per la cifratura asimmetrica

3. **Flussi di comunicazione e servizi di sicurezza DCCG**

Questa sezione fornisce una panoramica dei flussi di comunicazione e dei servizi di sicurezza nel sistema DCCG. Definisce inoltre quali chiavi e certificati sono utilizzati per proteggere la comunicazione, le informazioni caricate, i DCC e un elenco di fiducia firmato contenente tutti i certificati CSCA di cui è stato effettuato l'on-boarding. Il DCCG funge da hub di dati che consente lo scambio di pacchetti di dati firmati per gli Stati membri.

I pacchetti di dati caricati sono forniti dal DCCG «tal quali», il che significa che il DCCG non aggiunge né cancella i DSC dai pacchetti ricevuti. Il back-end nazionale (NB) degli Stati membri è abilitato a verificare l'integrità e l'autenticità end-to-end dei dati caricati. Inoltre i back-end nazionali e il DCCG utilizzeranno l'autenticazione TLS reciproca per stabilire una connessione sicura in aggiunta alle firme contenute nei dati scambiati.

3.1. *Autenticazione e creazione di connessioni*

Il DCCG utilizza il protocollo Transport Layer Security (TLS) con autenticazione reciproca per stabilire un canale criptato autenticato tra il back-end nazionale (NB) dello Stato membro e l'ambiente gateway. Pertanto il DCCG detiene un certificato del server TLS, abbreviato $DCCG_{TLS}$, mentre i back-end nazionali detengono un certificato del client TLS, abbreviato NB_{TLS}. I modelli di certificato sono forniti nella *sezione 5*. Ogni back-end nazionale può fornire il proprio certificato TLS. Tale certificato sarà esplicitamente inserito in una lista bianca e potrà quindi essere rilasciato da un'autorità di certificazione pubblicamente riconosciuta (ad esempio un'autorità di certificazione che segue i requisiti di base del CA/Browser Forum), da un'autorità nazionale di certificazione o potrà essere autofirmato. Ciascuno Stato membro è responsabile dei propri dati nazionali e della protezione della chiave privata utilizzata per stabilire la connessione con il DCCG. L'approccio «presenta il tuo certificato» richiede una procedura ben definita di registrazione e identificazione, nonché procedure di revoca e rinnovo come descritto nelle *sezioni 4.1*, *4.2* e *4.3*. Il DCCG utilizza una lista bianca in cui vengono aggiunti i certificati TLS dei back-end nazionali dopo l'avvenuta registrazione. Solo i back-end nazionali che si autenticano con una chiave privata corrispondente a un certificato della lista bianca possono stabilire una connessione sicura con il DCCG. Il DCCG utilizzerà anche un certificato TLS che consenta ai back-end nazionali di verificare che stiano effettivamente stabilendo una connessione con il «vero» DCCG e non con qualche entità malevola che si fa passare per il DCCG. Il certificato del DCCG sarà fornito ai back-end nazionali una volta effettuata la registrazione. Il certificato $DCCG_{TLS}$ sarà rilasciato da un'autorità di certificazione pubblicamente riconosciuta (anche in tutti i principali browser). Spetta agli Stati membri verificare che la loro connessione al DCCG sia sicura (ad esempio, controllando l'impronta digitale del certificato $DCCG_{TLS}$ del server collegato rispetto a quella fornita dopo la registrazione).

3.2. *Autorità nazionali di certificazione e modello di convalida*

Gli Stati membri che partecipano al quadro DCCG sono tenuti ad avvalersi di una CSCA per il rilascio dei DSC. Gli Stati membri possono avere più di una CSCA, ad esempio in caso di decentramento regionale. Ciascuno Stato membro può avvalersi delle autorità di certificazione esistenti oppure istituire un'apposita autorità di certificazione (eventualmente autofirmata) per il sistema DCC.

Gli Stati membri devono presentare il certificato o i certificati CSCA all'operatore del DCCG durante la procedura ufficiale di on-boarding. Dopo l'avvenuta registrazione dello Stato membro (*cfr. la sezione 4.1 per maggiori dettagli*), l'operatore del DCCG aggiornerà un elenco di fiducia firmato contenente tutti i certificati CSCA attivi nel quadro del DCC. L'operatore del DCCG utilizzerà un'apposita coppia di chiavi asimmetriche per firmare l'elenco di fiducia e i certificati in ambiente off-line. La chiave privata non sarà memorizzata nel sistema DCCG on line per evitare che una compromissione del sistema on line consenta a un aggressore di compromettere l'elenco di fiducia. Il corrispondente certificato dell'ancora di fiducia $DCCG_{TA}$ sarà fornito ai back-end nazionali durante la procedura di on-boarding.

Gli Stati membri possono recuperare l'elenco di fiducia dal DCCG per le loro procedure di verifica. La CSCA è definita come l'autorità di certificazione che rilascia i DSC, per cui gli Stati membri che utilizzano una gerarchia di autorità di certificazione a più livelli (ad esempio, autorità di certificazione radice -> CSCA -> DSC) devono indicare l'autorità di certificazione subordinata che rilascia i DSC. In questo caso, se uno Stato membro si avvale di un'autorità di certificazione esistente, il sistema DCC ignorerà tutto ciò che è al di sopra della CSCA e inserirà nella lista bianca solo la CSCA come ancora di fiducia (anche se si tratta di un'autorità di certificazione subordinata). Ciò è dovuto al fatto che nel modello ICAO sono consentiti solo 2 livelli: una CSCA «radice» e un DSC «foglia» firmato solo da tale CSCA.

Nel caso in cui uno Stato membro gestisca la propria CSCA, tale Stato membro è responsabile del funzionamento sicuro e della gestione delle chiavi di tale autorità. La CSCA funge da ancora di fiducia per i DSC e pertanto la protezione della chiave privata della CSCA è essenziale per l'integrità dell'ambiente DCC. Il modello di verifica nella PKI DCC è il modello a strati, in base al quale tutti i certificati nella convalida del percorso del certificato devono essere validi in un determinato momento (ossia al momento della convalida della firma). Si applicano pertanto le restrizioni seguenti:

— la CSCA non rilascia certificati con periodo di validità superiore a quello del certificato dell'autorità di certificazione stesso;

— il firmatario del documento non firma documenti con periodo di validità superiore a quello del DSC stesso;

— gli Stati membri che gestiscono la propria CSCA sono tenuti a definire i periodi di validità della loro CSCA e di tutti i certificati rilasciati e devono provvedere al loro rinnovo.

La *sezione 4.2* contiene raccomandazioni per i periodi di validità.

3.3. *Integrità e autenticità dei dati caricati*

I back-end nazionali possono utilizzare il DCCG per caricare e scaricare pacchetti di dati firmati digitalmente dopo l'avvenuta autenticazione reciproca. All'inizio, questi pacchetti di dati contengono i DSC degli Stati membri. La coppia di chiavi utilizzata dal back-end nazionale per la firma digitale dei pacchetti di dati caricati nel sistema DCCG è denominata coppia di chiavi di firma per il caricamento da parte del back-end nazionale e il corrispondente certificato a chiave pubblica è abbreviato con certificato NB_{UP}. Ciascuno Stato membro presenta il proprio certificato NB_{UP}, che può essere autofirmato o rilasciato da un'autorità di certificazione esistente, come un'autorità pubblica di certificazione (ossia un'autorità di certificazione che rilascia certificati conformemente ai requisiti di base del CA/Browser Forum). Il certificato NB_{UP} è diverso da qualsiasi altro certificato utilizzato dallo Stato membro (ossia CSCA, client TLS o DSC).

Gli Stati membri devono fornire il certificato di caricamento all'operatore del DCCG durante la procedura di registrazione iniziale (*cfr. la sezione 4.1 per maggiori dettagli*). Ciascuno Stato membro è responsabile dei propri dati nazionali ed è tenuto a proteggere la chiave privata utilizzata per firmare i caricamenti.

Gli altri Stati membri possono verificare i pacchetti di dati firmati utilizzando i certificati di caricamento forniti dal DCCG. Il DCCG verifica l'autenticità e l'integrità dei dati caricati con il certificato di caricamento del back-end nazionale prima che siano forniti agli altri Stati membri.

3.4. *Requisiti relativi all'architettura tecnica del DCCG*

I requisiti relativi all'architettura tecnica del DCCG sono i seguenti:

— il DCCG utilizza l'autenticazione TLS reciproca per stabilire una connessione criptata autenticata con i back-end nazionali. Pertanto il DCCG tiene una lista bianca dei certificati del client NB_{TLS} registrati;

— il DCCG utilizza due certificati digitali ($DCCG_{TLS}$ e $DCCG_{TA}$) con due coppie di chiavi distinte. La chiave privata della coppia di chiavi $DCCG_{TA}$ è mantenuta off-line (non sulle componenti on line del DCCG);

— il DCCG tiene un elenco di fiducia dei certificati NB_{CSCA} firmati con la chiave privata $DCCG_{TA}$;

— le cifrature utilizzate devono soddisfare i requisiti della *sezione 5.1*.

4. Gestione del ciclo di vita del certificato

4.1. *Registrazione dei back-end nazionali*

Per partecipare al sistema DCCG, gli Stati membri devono registrarsi presso l'operatore del DCCG. Questa sezione descrive la procedura tecnica e operativa da seguire per registrare un back-end nazionale.

L'operatore del DCCG e lo Stato membro devono scambiarsi informazioni sui referenti tecnici per la procedura di on-boarding. Si presume che i referenti tecnici siano legittimati dai rispettivi Stati membri e che l'identificazione/autenticazione avvenga attraverso altri canali. Ad esempio, l'autenticazione può essere ottenuta quando il referente tecnico di uno Stato membro fornisce i certificati sotto forma di file criptati con password via e-mail e condivide la password corrispondente con l'operatore del DCCG per telefono. Possono essere utilizzati anche altri canali sicuri definiti dall'operatore del DCCG.

Lo Stato membro deve fornire tre certificati digitali durante il processo di registrazione e identificazione:

— il certificato TLS dello Stato membro NB_{TLS};

— il certificato di caricamento dello Stato membro NB_{UP};

— il certificato o i certificati CSCA dello Stato membro NB_{CSCA}.

Tutti i certificati forniti devono soddisfare i requisiti definiti nella *sezione 5*. L'operatore del DCCG verificherà che il certificato fornito sia conforme ai requisiti della *sezione 5*. Dopo l'identificazione e la registrazione, l'operatore del DCCG:

— aggiunge il certificato o i certificati NB_{CSCA} all'elenco di fiducia firmato con la chiave privata che corrisponde alla chiave pubblica $DCCG_{TA}$;

— aggiunge il certificato NB_{TLS} alla lista bianca dell'endpoint TLS del DCCG;

— aggiunge il certificato NB_{UP} al sistema DCCG;

— fornisce allo Stato membro il certificato a chiave pubblica $DCCG_{TA}$ e $DCCG_{TLS}$.

4.2. *Autorità di certificazione, periodi di validità e rinnovo*

Nel caso in cui uno Stato membro intenda gestire la propria CSCA, i certificati CSCA possono essere autofirmati. Essi fungono da ancora di fiducia dello Stato membro e pertanto lo Stato membro deve proteggere con forza la chiave privata corrispondente alla chiave pubblica del certificato CSCA. Si raccomanda agli Stati membri di utilizzare un sistema off-line per la loro CSCA, ossia un sistema informatico non connesso ad alcuna rete. Per accedere al sistema si utilizza un controllo multi-persona (ad esempio, secondo il principio del doppio controllo). Dopo la firma dei DSC sono effettuati controlli operativi e il sistema che detiene la chiave CSCA privata è conservato in condizioni di sicurezza con forti controlli d'accesso. Per proteggere ulteriormente la chiave CSCA privata si possono utilizzare moduli di sicurezza hardware o carte intelligenti. I certificati digitali contengono un periodo di validità che impone il rinnovo del certificato. Il rinnovo è necessario per utilizzare nuove chiavi crittografiche e per adattare le dimensioni delle chiavi nel caso di nuovi miglioramenti nel calcolo o quando nuovi attacchi minacciano la sicurezza dell'algoritmo crittografico utilizzato. Si applica il modello a strati (cfr. la *sezione 3.2*).

Data la validità di un anno dei certificati COVID digitali, si raccomandano i periodi di validità seguenti:

— CSCA: 4 anni

— DSC: 2 anni

— Caricamento: 1-2 anni

— Autenticazione del client TLS: 1-2 anni

Ai fini di un rinnovo tempestivo, si raccomandano i periodi di utilizzo seguenti per le chiavi private:

— CSCA: 1 anno

— DSC: 6 mesi

Gli Stati membri devono creare tempestivamente nuovi certificati di caricamento e certificati TLS, ad esempio un mese prima della scadenza, al fine di consentire il corretto funzionamento. I certificati CSCA e i DSC dovrebbero essere rinnovati almeno un mese prima della fine dell'utilizzo della chiave privata (tenendo conto delle necessarie procedure operative). Gli Stati membri devono fornire certificati CSCA, certificati di caricamento e TLS aggiornati all'operatore del DCCG. I certificati scaduti sono rimossi dalla lista bianca e dall'elenco di fiducia.

Gli Stati membri e l'operatore del DCCG devono tenere traccia della validità dei propri certificati. Non esiste un'entità centrale che tenga traccia della validità dei certificati e che informi i partecipanti.

4.3. *Revoca dei certificati*

In generale, i certificati digitali possono essere revocati dall'autorità di certificazione che li ha rilasciati utilizzando elenchi dei certificati revocati o il responder Online Certificate Status Protocol (OCSP). Le CSCA per il sistema DCC dovrebbero fornire elenchi dei certificati revocati (CRL). Anche se tali CRL non sono attualmente utilizzati da altri Stati membri, essi dovrebbero essere integrati per le applicazioni future. Se una CSCA decide di non fornire CRL, i DSC di tale CSCA dovranno essere rinnovati quando i CRL diventeranno obbligatori. Per la convalida dei DSC, i verificatori non dovrebbero utilizzare l'OCSP ma i CRL. Si raccomanda che il back-end nazionale esegua la necessaria convalida dei DSC scaricati dal DCCG e che trasmetta ai validatori DCC nazionali solo una serie di DSC fidati e convalidati. I validatori DCC non dovrebbero effettuare alcun controllo delle revoche dei DSC nel loro processo di convalida. Uno dei motivi è proteggere la vita privata dei titolari di DCC evitando ogni possibilità che l'uso di un determinato DSC possa essere monitorato dal suo responder OCSP associato.

Gli Stati membri possono rimuovere autonomamente i propri DSC dal DCCG utilizzando certificati di caricamento e TLS validi. Rimuovendo un DSC, tutti i DCC rilasciati con tale DSC non saranno più validi quando gli Stati membri estrarranno gli elenchi di DSC aggiornati. La protezione del materiale relativo alle chiavi private corrispondenti ai DSC è fondamentale. Gli Stati membri sono tenuti a informare l'operatore del DCCG quando devono revocare i certificati di caricamento o TLS, ad esempio a causa della compromissione del back-end nazionale. L'operatore del DCCG può quindi togliere la fiducia per il certificato in questione, ad esempio rimuovendolo dalla lista bianca TLS. L'operatore del DCCG può rimuovere i certificati di caricamento dalla banca dati del DCCG. I pacchetti firmati con la chiave privata corrispondente a questo certificato di caricamento non saranno più validi quando i back-end nazionali toglieranno la fiducia per il certificato di caricamento revocato. Qualora un certificato CSCA debba essere revocato, gli Stati membri informano l'operatore del DCCG e gli altri Stati membri con cui hanno rapporti di fiducia. L'operatore del DCCG rilascerà un nuovo elenco di fiducia in cui il certificato in questione non sarà più presente. Tutti i DSC rilasciati da tale CSCA non saranno più validi nel momento in cui gli Stati membri aggiorneranno il trust store del loro back-end nazionale. Nel caso in cui il certificato $DCCG_{TLS}$ o il certificato $DCCG_{TA}$ debba essere revocato, l'operatore del DCCG e gli Stati membri devono collaborare per stabilire una nuova connessione TLS fidata e un nuovo elenco di fiducia.

5. **Modelli di certificato**

Questa sezione stabilisce i requisiti crittografici, i relativi orientamenti e i requisiti dei modelli di certificato. Per i certificati del DCCG, questa sezione definisce i modelli di certificato.

5.1. *Requisiti crittografici*

Gli algoritmi crittografici e le suite di cifratura TLS sono scelti sulla base delle attuali raccomandazioni dell'Ufficio federale tedesco per la sicurezza delle informazioni (BSI) o del SOGIS. Tali raccomandazioni e le raccomandazioni di altre istituzioni e organismi di normazione sono simili. Le raccomandazioni sono contenute negli orientamenti tecnici TR 02102-1 e TR 02102-2 ([1]) o nei meccanismi crittografici concordati dal SOGIS ([2]).

5.1.1. Requisiti relativi al DSC

Si applicano i requisiti di cui all'*allegato I, sezione 3.2.2*. Si raccomanda pertanto vivamente ai firmatari dei documenti di utilizzare l'algoritmo di firma digitale su curva ellittica (ECDSA) con NIST-p-256 (come definito nell'appendice D di FIPS PUB 186-4). Altre curve ellittiche non sono supportate. A causa dei limiti di spazio del DCC, gli Stati membri non dovrebbero utilizzare l'algoritmo RSA-PSS, anche se consentito come algoritmo di riserva. Nel caso in cui gli

([1]) BSI - Technical Guidelines TR-02102 (bund.de).
([2]) SOGIS - Supporting documents (sogis.eu).

Stati membri utilizzino l'algoritmo RSA-PSS, dovrebbero utilizzare un modulo di dimensioni pari a 2048 o al massimo 3072 bit. L'algoritmo SHA-2 con una lunghezza di output ≥ 256 bit è utilizzato come funzione di hash crittografico (cfr. ISO/IEC 10118-3:2004) per la firma del DSC.

5.1.2. Requisiti per certificati TLS, di caricamento e CSCA

Per i certificati digitali e le firme crittografiche nel contesto del DCCG, i principali requisiti relativi agli algoritmi crittografici e alla lunghezza della chiave sono riassunti nella tabella seguente (a partire dal 2021):

Algoritmo di firma	Dimensioni della chiave	Funzione di hash
EC-DSA	Min. 250 bit	SHA-2 con lunghezza di output ≥ 256 bit
RSA-PSS (riempimento raccomandato) RSA-PKCS#1 v1.5 (riempimento preesistente)	Modulo RSA (N) da min. 3000 bit con esponente pubblico e > 2^16	SHA-2 con lunghezza di output ≥ 256 bit
DSA	Numero primo p da min. 3000 bit, chiave q da 250 bit	SHA-2 con lunghezza di output ≥ 256 bit

La curva ellittica raccomandata per l'algoritmo EC-DSA è NIST-p-256 a causa della sua applicazione diffusa.

5.2. *Certificato CSCA (NB_{CSCA})*

La tabella seguente fornisce indicazioni sul modello di certificato NB_{CSCA} se uno Stato membro decide di gestire la propria CSCA per il sistema DCC.

Le voci **in grassetto** sono obbligatorie (devono essere inserite nel certificato), quelle *in corsivo* son raccomandate (dovrebbero essere inserite). Per i campi mancanti non sono definite raccomandazioni.

Campo	Valore
Subject (Soggetto)	**cn=<nome comune univoco e non vuoto>,***o=<fornitore>,* **c=<Stato membro che gestisce la CSCA>**
Key usage (Utilizzo della chiave)	**certificate signing** (firma del certificato), *CRL signing* (firma del CRL) (come minimo)
Basic Constraints (Limitazioni di base)	**CA = true (vero), path length constraints (limiti di lunghezza del percorso) = 0**

Il nome del soggetto deve essere univoco e non vuoto all'interno dello Stato membro specificato. Il codice paese (c) deve corrispondere allo Stato membro che si avvarrà di questo certificato CSCA. Il certificato deve contenere un identificativo della chiave del soggetto (Subject Key Identifier — SKI) univoco conformemente a RFC 5280 ([3]).

5.3. *Certificato di firma digitale (DSC)*

La tabella seguente fornisce indicazioni sul DSC. Le voci **in grassetto** sono obbligatorie (devono essere inserite nel certificato), quelle *in corsivo* son raccomandate (dovrebbero essere inserite). Per i campi mancanti non sono definite raccomandazioni.

Campo	Valore
Serial Number (Numero di serie)	**numero di serie univoco**
Subject (Soggetto)	**cn=<nome comune univoco e non vuoto>,***o=<fornitore>,* **c=<Stato membro che utilizza il DSC>**
Key Usage (Utilizzo della chiave)	**digital signature** (firma digitale) (come minimo)

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

Il DSC deve essere firmato con la chiave privata corrispondente a un certificato CSCA utilizzato dallo Stato membro.

Devono essere utilizzate le estensioni seguenti:

— il certificato deve contenere un identificativo della chiave dell'autorità (Authority Key Identifier — AKI) corrispondente all'identificativo della chiave del soggetto (SKI) del certificato della CSCA emittente;

— il certificato dovrebbe contenere un identificativo della chiave del soggetto univoco (conformemente a RFC 5280 ([4])).

Inoltre il certificato dovrebbe contenere l'estensione del punto di distribuzione del CRL che indica l'elenco dei certificati revocati (CRL) fornito dalla CSCA che ha rilasciato il DSC.

Il DSC può contenere un'estensione dell'utilizzo esteso della chiave con zero o più identificativi di policy sull'utilizzo della chiave che limitano i tipi di HCERT che il certificato è autorizzato a verificare. In presenza di una o più estensioni, i verificatori verificano l'utilizzo della chiave confrontandola con l'HCERT memorizzato. A tal fine sono definiti i valori extendedKeyUsage (utilizzo esteso della chiave) seguenti:

Campo	Valore
extendedKeyUsage (utilizzo esteso della chiave)	1.3.6.1.4.1.1847.2021.1.1 per i soggetti che rilasciano certificati di test
extendedKeyUsage (utilizzo esteso della chiave)	1.3.6.1.4.1.1847.2021.1.2 per i soggetti che rilasciano certificati di vaccinazione
extendedKeyUsage (utilizzo esteso della chiave)	1.3.6.1.4.1.1847.2021.1.3 per i soggetti che rilasciano certificati di guarigione

In mancanza di un'estensione dell'utilizzo della chiave (ossia nessuna estensione o zero estensioni), questo certificato può essere utilizzato per convalidare qualsiasi tipo di HCERT. Altri documenti possono definire ulteriori identificativi di policy sull'utilizzo esteso della chiave utilizzati per la convalida degli HCERT.

5.4. *Certificati di caricamento (NBUP)*

La tabella seguente fornisce indicazioni per il certificato di caricamento del back-end nazionale. Le voci **in grassetto** sono obbligatorie (devono essere inserite nel certificato), quelle *in corsivo* son raccomandate (dovrebbero essere inserite). Per i campi mancanti non sono definite raccomandazioni.

Campo	Valore
Subject (Soggetto)	**cn=<nome comune univoco e non vuoto>,***o=<fornitore>,* **c=<Stato membro che utilizza il certificato di caricamento>**
Key Usage (Utilizzo della chiave)	**digital signature** (firma digitale) (come minimo)

5.5. *Autenticazione del client TLS del back-end nazionale (NB_{TLS})*

La tabella seguente fornisce indicazioni per il certificato di autenticazione del client TLS del back-end nazionale. Le voci **in grassetto** sono obbligatorie (devono essere inserite nel certificato), quelle *in corsivo* son raccomandate (dovrebbero essere inserite). Per i campi mancanti non sono definite raccomandazioni.

Campo	Valore
Subject (Soggetto)	**cn=<nome comune univoco e non vuoto>,***o=<fornitore>,* **c=<Stato membro sul back-end nazionale>**
Key Usage (Utilizzo della chiave)	**digital signature** (firma digitale) (come minimo)
Extended key usage (Utilizzo esteso della chiave)	**client authentication** (autenticazione del client) **(1.3.6.1.5.5.7.3.2)**

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

Il certificato può, ma non necessariamente deve, contenere anche *server authentication* (autenticazione del server) *(1.3.6.1.5.5.7.3.1)* per l'utilizzo esteso della chiave.

5.6. *Certificato di firma dell'elenco di fiducia ($DCCG_{TA}$)*

La tabella seguente definisce il certificato dell'ancora di fiducia del DCCG.

Campo	Valore
Subject (Soggetto)	**cn = Digital Green Certificate Gateway** (gateway per i certificati verdi digitali) ([5])**, o=<fornitore>, c=<paese>**
Key Usage (Utilizzo della chiave)	**digital signature** (firma digitale) (come minimo)

5.7. *Certificati del server TLS del DCCG ($DCCG_{TLS}$)*

La tabella seguente definisce il certificato TLS del DCCG.

Campo	Valore
Subject (Soggetto)	cn=<FQDN o indirizzo IP del DCCG>, o=<fornitore>, c=<paese>
SubjectAltName (Nome alternativo del soggetto)	dNSName: <nome DNS del DCCG> o iPAddress: <indirizzo IP del DCCG>
Key Usage (Utilizzo della chiave)	**digital signature** (firma digitale) (come minimo)
Extended Key usage (Utilizzo esteso della chiave)	**server authentication** (autenticazione del server) **(1.3.6.1.5.5.7.3.1)**

Il certificato può, ma non necessariamente deve, contenere anche *client authentication* (autenticazione del client) *(1.3.6.1.5.5.7.3.2)* per l'utilizzo esteso della chiave.

Il certificato TLS del DCCG è rilasciato da un'autorità di certificazione pubblicamente riconosciuta (anche in tutti i principali browser e sistemi operativi, conformemente ai requisiti di base del CA/Browser Forum).

([5]) La terminologia «certificato verde digitale» anziché «certificato COVID digitale dell'UE» è stata mantenuta in questo contesto perché è questa la terminologia che è stata codificata in modo fisso e utilizzata nel certificato prima che i colegislatori decidessero di modificarla.