ALLEGATO D

Struttura dell'identificativo univoco e caratteristiche e modalità di generazione del codice a barre interoperabile

Sommario

1. Struttura dell'identificativo univoco (art. 9)

Le certificazioni verdi COVID-19 sono identificate attraverso un codice univoco alfanumerico che ha una struttura comune per tutti gli Stati Membri al fine di garantirne l'interoperabilità.

Le specifiche tecniche prese a riferimento e relative a tale struttura sono pubblicate nel documento di eHealth Network "Guidelines on verifiable vaccination certificates, Release 2, 2021-03-12", approvato dalla Commissione europea. In tale documento vengono proposte 3 diverse possibilità di realizzazione del codice univoco.

L'opzione scelta in Italia per il codice univoco delle certificazioni verdi COVID-19, generate dalla PN-DGC, è quella citata nel menzionato documento di eHealth Network come "Option 2 – opaque identifier – no structure".

Il codice univoco è composto:

- da soli caratteri maiuscoli alfanumerici dalla A alla Z e da 0 a 9 più i caratteri speciali {'/','#',':'}

Le componenti del codice univoco sono le seguenti:

- Versione: identifica la versione di codice univoco
- Codice del paese emittente
- Blocco di stringa casuale
- Checksum ovvero codice di controllo per garantire l'integrità del codice stesso

Nella tabella seguente si definiscono i valori da utilizzare per ciascuna delle componenti sopra descritte:

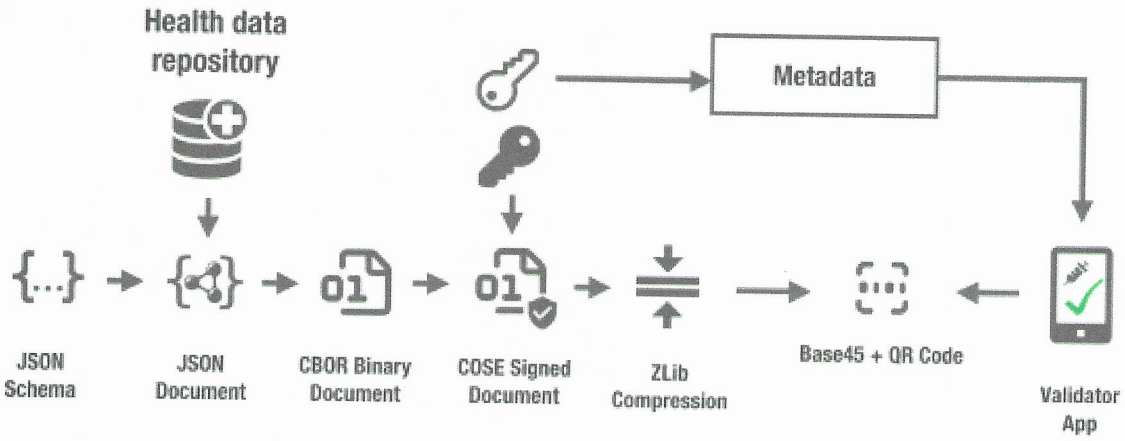
Campo	Lunghezza	Note
Versione	2	Al momento è prevista solo la versione 1 quindi il valore è fisso: 01
Codice paese	2	Valore fisso: IT
Blocco casuale	32	Elemento generato in modo casuale che rende univoco il codice
Checksum	1	Calcolato su tutti i campi precedenti dello standard ISO-7812-1 (LUHN-10)

Di seguito un esempio di codice identificativo secondo lo standard definito:

- 01ITEFCC44D2E72B4BFA9EF9B8A30289F04F#6

2. Caratteristiche e modalità di generazione codice a barre interoperabile

Nella figura di seguito vengono rappresentate le fasi che portano alla generazione del codice QR per l'interoperabilità:



L'algoritmo di generazione del QR si basa sulle seguenti tecnologie:

- **JSON**: (JavaScript Object Notation) è un formato adatto all'interscambio di dati fra applicazioni client/server facilmente leggibile sia da parte di una persona che da parte di un sistema informatico. È basato sul linguaggio JavaScript Standard ECMA-262 3ª edizione (dicembre 1999)
- **CBOR** (Concise Binary Object Representation): è un formato binario di serializzazione dei dati ispirato al formato JSON. Al pari del formato JSON consente la trasmissione di oggetti contenenti informazioni formato a coppie nome-valore, ma in modo più coinciso. Questo incrementa la velocità di elaborazione e di trasferimento al costo di una minore leggibilità da parte di un operatore. È definito secondo lo standard IETF RFC 8949.
- **COSE** (CBOR Object Signing and Encryption): è un protocollo che descrive come creare e gestire i processi di apposizione del sigillo, autenticazione e crittografia basati sul formato CBOR per la serializzazione. È definito secondo lo standard IETF RFC 8152

Nel seguito vengono descritti i passi dell'algoritmo di generazione:

1. Serializzazione in formato JSON: i dati della certificazione (definiti nell'allegato A per le varie tipologie) vengono validati e serializzati in una struttura dati JSON;

2. Trasformazione dei dati in formato CBOR: i dati serializzati in JSON vengono convertiti utilizzando il formato CBOR;
3. Sigillo elettronico qualificato: al fine di garantire l'autenticità, la validità e l'integrità delle informazioni, ai dati è apposto un sigillo con algoritmo di chiave asimmetrica ellittica ECDSA;
4. Incapsulamento secondo il protocollo COSE: i dati serializzati unitamente al sigillo vengono incapsulati in un messaggio "sign1" e nuovamente serializzati in formato CBOR secondo quanto specificato dal protocollo COSE;
5. Compressione dati in formato zLib: il messaggio ottenuto viene compresso al fine di ridurne la dimensione;
6. Codifica dei dati in formato Base45: il messaggio viene serializzato in formato binario;
7. Generazione del QR in formato QRCode: il messaggio finale viene trascritto in formato QR.