eHealth Network

Guidelines on

Technical Specifications for Digital Green Certificates Volume 3

Interoperable 2D Code

Version 1.3

2021-04-21

The eHealth Network is a voluntary network, set up under article 14 of Directive 2011/24/EU. It provides a platform of Member States' competent authorities dealing with eHealth.

Adopted by the eHealth Network on 21 April 2021.

TABLE OF CONTENTS

TABLE OF TABLES

TABLE OF FIGURES

1 Introduction

1.1 Context

This document specifies a generic data structure and encoding mechanisms for electronic health certificates. It also specifies a transport encoding mechanism in a machine-readable optical format (QR), which can be displayed on the screen of a mobile device or printed on a piece of paper. This document should be read together with the eHealth Network (eHN) Guidelines on Technical Specifications for Digital Green Certificates (DGC), Volume 1. In case of discrepancies between this document and the eHN Guidelines on Technical Specifications for DGC, Volume 1, the latter prevails.

1.2 Scope of Document

The scope of the document are further definitions of data structures, encodings and formats for the creation of a 2D Code designed to provide a uniform and standardized vehicle for EU green certificates for all issuers. The aim is to harmonize how EU green certificates are represented, encoded and signed facilitating interoperability.

1.3 International interoperability

The Digital Green Certificate technological solutions should seek to ensure interoperability with relevant global initiatives, in particular the World Health Organization (WHO) and the International Civil Aviation Organization (ICAO). This may include interoperability features with 2D barcodes following other recognized international standards/formats, for instance by allowing for adequate conversion between certificate formats.

2 Data Structures and Formats

2.1 CBOR/COSE

To optimize the footprint of the 2D Code, the objects are encoded as CBOR[1] object. To ensure the data integrity, the CBOR Object Signature and Encryption[2] is used. For using CBOR it has to be considered that the recommended serialization rules[3] are considered.

⚠ It's important to ensure during the converting the hints in the CBOR RFC[4].

⚠ It must be ensured that all keys in a JSON Object are UTF-8 encoded.

In addition to the UTF-8 encoded last name(s) and first name(s) of the holder, the 2D barcode must include a second set of the same name fields encoded in ASCII following ICAO Document 9303 part 3[5]. The ASCII-encoded personal name should match the name as included in the travel document issued to the holder.

As described in the DSC-Spec, the CWT format is used to establish a standard container format for the green certificates. It must be ensured that this kind of defined standard claims are not broken by custom claims or retyped by different datatypes.

2.2 Compression Algorithm

To compress the COSE data objects, the zlib compression algorithm is used.

2.3 2D Code Versioning

In productive use cases a lot of different 2D Codes with different assumptions can be scanned by the verifier. To ensure that the context of the scanned code is always clear for processing (e.g. used schema, value sets at this moment, rules etc.) a context prefix is established to represent different versions.

The version field is expressed as string value:

Version Value	Version
HC1	Health Certificate Version 1
HC2	Health Certificate Version 2
..	…

Table 1: Data Context Example

Each context maps to a discovery document, which is provided over the DGCG or national backends. The context can be defined specific by each country or by the eHealth Network.

---

[1] https://tools.ietf.org/html/rfc8949
[2] https://tools.ietf.org/html/rfc8152
[3] https://tools.ietf.org/html/rfc8949#section-4
[4] https://tools.ietf.org/html/rfc8949#section-6
[5] https://www.icao.int/publications/Documents/9303_p3_cons_en.pdf

To provide this context to optical readers it's attached to the encoded barcode before QR Code Generation:

[**version**]Base45 Encoding

The encoding of base45 is described in a IETF draft[6].

2.4 Used Public Key Identification

During the scan of a CBOR object by a code scanner, the verification algorithm must be efficiently matching the used crypto material. For this purpose and the view on the future decentralized scenarios, the used crypto key must be uniquely identifiable by a verifier. This is realized by inserting the field "kid" into the COSE header. The key identifier is defined as the first truncated 8 Bytes of a SHA256 Hash. The "kid" claim can also be used in the JWK concept.

2.5 Data Field Names

To save so much bytes as possible in the 2D Code, each field name must be reduced to acronyms. E.g. Subject to "sub" or Issuer to "iss".

The selected field names should be uniquely over the selected context, otherwise field name translations are much harder to realize.

2.6 COSE/CBOR Content

2.6.1 COSE Structure

A COSE structure contains a protected, unprotected and payload object within one CBOR array defined in the Basic Structure of the RFC8152[7].

Name	CBOR Major Type	Type
protected	2	bstr
payload	2	bstr
signature	2	bstr
unprotected	2	empty

Table 2: COSE Format

The payload "nil" is not allowed for this 2D code and should be rejected. The choice to place the kid in the protected or unprotected header is left to the issuer, all verifiers must accept both.

2.6.2 Signing Header

The header of COSE contains the used algorithm and the key identifier:

Name	CBOR Major Type	Placement In Header	Type	Value	Description
alg	1	protected	nint	-7/-37 (ES256)	Algorithm Field
kid	4	protected	array	First 8 bytes of the hash value	Key Identifier

[6] https://datatracker.ietf.org/doc/draft-faltstrom-base45/
[7] https://tools.ietf.org/html/rfc8152#section-3.1

Table 3: Header Format

More information about the COSE Headers and values of algorithms can be found on the IANA Page[8].

2.6.3 Common Payload Values

The common dataset for all types of CBOR objects are defined as the following table:

Claim Key	Name	CBOR Major Type	Type	Description
1	iss	2	bstr	Issuer of the DGC
6	iat	2	bstr	Issuing Date of the DGC
4	exp	2	bstr	Expiring Date of the DGC
-260	hcert	5	map	Payload of the DGC (Vac,Tst,Rec)

Table 4: Common Values

The syntax is according to the CWT RFC8392[9] and Volume 1 of the Digital Green Certificate technical specifications.

2.6.4 Payload

The claim “HCERT” is defined as container for different types of certificates (e.g. Vaccines, Test and Recovery) by the eHealth Network[10,11] (see eHealth Network Guidelines on Technical Specifications for Digital Green Certificates, Volume 1).

The data contents following the DGC regulation and the schema of the payload for the 2D barcode are defined in the eHealth Network Guidelines on Value Sets for Digital Green Certificates.

2.7 Optional Data Content

Optional national data content is not allowed. The data content is limited to the defined data elements in the minimum data set specified in the Regulation.

[8] https://www.iana.org/assignments/cose/cose.xhtml
[9] https://tools.ietf.org/html/rfc8392
[10] https://ec.europa.eu/health/sites/health/files/ehealth/docs/vaccination-proof_interoperability-guidelines_en.pdf
[11] https://ec.europa.eu/health/sites/health/files/ehealth/docs/citizen_recovery-interoperable-certificates_en.pdf

3 Serialization

As serialization pattern, the following scheme is used:

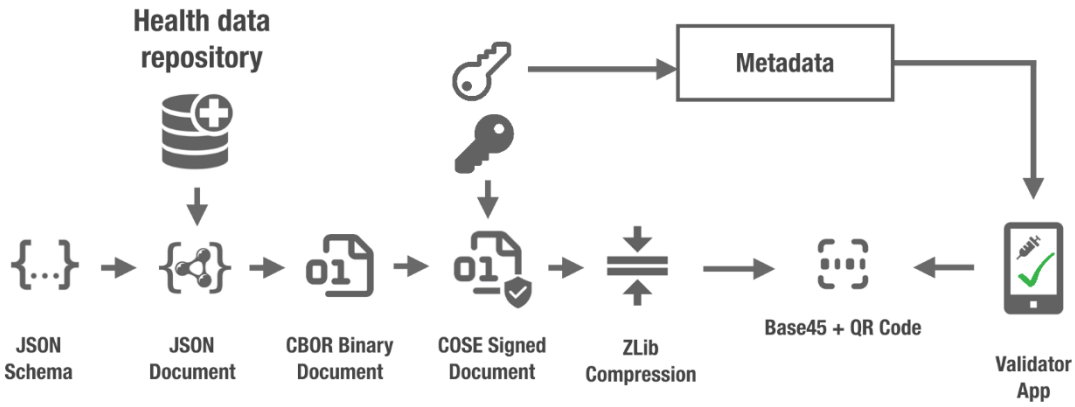

Figure 1: Serialization Process[12]

The process should always start with a JSON file, e.g. from a Health Data Repository (external data sources are optionally), which is matching against the defined DGC Schemas. After this checkup, a transformation of human readability can be processed before the serialization to CBOR starts. During this process it can be decided whether a human readability is useful or not. The acronyms of the claims should be mapped in every case to the display names before serialization and after deserialization.

It should not be considered to replace the field content with metadata information (e.g. 11 for a value) to safe bytes during the compression. There must be always clear defined values.

[12] https://github.com/ehn-digital-green-development/hcert-spec

4 Implementation Roadmap

Feature	Expected Version
CBOR/COSE	1.0
ECDSA Signatures	1.0
QR Code Encoding	1.0
Initial Data Structures	1.0
Aztec Code Encoding	Later versions
Datamatrix Code Encoding	Later versions

Table 5: Roadmap