eHealth Network

Guidelines on

Technical Specifications

for EU Digital COVID Certificates

Volume 3

Interoperable 2D Code

Version 1.4

2022-02-23

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 23.02.2022.

TABLE OF CONTENTS

1   Introduction

This document complements normative technical specifications adopted and published as Commission Implementing Decision (EU) 2021/1073 (with any amendments, such as Commission Implementing Decision (EU) 2021/2014). The document should be read together with the legal acts.

Annex I of the Commission Implementing Decision (EU) 2021/1073 of 28 June 2021 describes general rules for interoperable 2D codes.

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 EU Digital COVID Certificates (DCC), Volume 1. In case of discrepancies between this document and the eHN Guidelines on Technical Specifications for DCC, 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 Digital COVID Certificates for all issuers. The aim is to harmonize how Digital COVID Certificates are represented, encoded and signed facilitating interoperability.

1.3   International interoperability

The Digital COVID 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

Also described in the Implementing Decision (EU) 2021/1073, Annex I.

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[1]. The ASCII-encoded personal name should match the name as included in the travel document issued to the holder.

2.2 Compression Algorithm

Fully described in the Implementing Decision (EU) 2021/1073, Annex I.

2.3 2D Code Versioning

Fully described in the Implementing Decision (EU) 2021/1073, Annex I.

2.4 Used Public Key Identification

Fully described in the Implementing Decision (EU) 2021/1073, Annex I.

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[2].

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

Table 1: COSE Format

---

[2] https://tools.ietf.org/html/rfc8152#section-3.1

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
Fully described in the Implementing Decision (EU) 2021/1073, Annex I.

2.6.3   Common Payload Values
Fully described in the Implementing Decision (EU) 2021/1073, Annex I.

2.6.4   Payload
Fully described in the Implementing Decision (EU) 2021/1073, Annex I.

2.7   Optional Data Content

Fully described in the Implementing Decision (EU) 2021/1073, Annex I.

3   Serialization

Fully described in the Implementing Decision (EU) 2021/1073, Annex I.

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 2: Roadmap