eHealth Network

Guidelines on

Technical Specifications

for EU Digital COVID Certificates

Volume 1

V1.1.1

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.

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.

1.1 Versioning Policy

Versions of this specification follow semantic versioning and consist of three different integers describing the *major*, *minor* and *edition* version. A change in the *major* version is an update that includes material changes affecting the decoding of the HCERT or the validation of it. An update of the *minor* version is a feature or maintenance update that maintains backward compatibility with previous versions.

In addition, there is an *edition* version number used for publishing updates to the document itself which has no effect on the HCERT, such as correcting spelling, providing clarifications or addressing ambiguities, et cetera. Hence, the edition number is not indicated in the HCERT. The version numbers are expressed in the title page of the document using a *major.minor.edition* format, where the three parts are separated by decimal dots.

1.2 Version History

Version	Status	Comments
1.0.5	Final	As adopted by the eHN on 2021-04-21.
1.1.1	Minor	As adopted by the eHN on 2022-02-23.

2 Terminology

Organisations adopting this specification for issuing health certificates are called Issuers and organisations accepting health certificates as proof of health status are called Verifiers. Together, these are called Participants. Some aspects in this document must be coordinated between the Participants, such as the management of a namespace and the distribution of cryptographic keys. It is assumed that a party, hereafter referred to as the Secretariat, carries out these tasks. The health certificate container format (HCERT) of this specification is generic, but in this context used to carry the EU Digital COVID Certificate (DCC).

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 (RFC2119, RFC8174) when, and only when, they appear in all capitals, as shown here.

3 Electronic Health Certificate Container Format

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

3.1 Structure of the payload

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

3.2 CWT Claims

3.2.1 CWT Structure Overview

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

3.2.2 Signature Algorithm

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

3.2.3 Key Identifier

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

3.2.4 Issuer

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

3.2.5 Expiration Time

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

3.2.6 Issued At

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

3.2.7 Health Certificate Claim

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

4 Serialisation and creation of the DCC payload

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

5 Transport Encodings

5.1 Raw

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

5.2 Barcode

5.2.1 Payload (CWT) Compression

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

5.2.2 QR 2D Barcode

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

6 Trusted List Format (CSCA and DSC list)

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

6.1 Simplified CSCA/DSC

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

6.2 ICAO eMRTD PKI and Trust Centers

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

7 Security Considerations

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

7.1 HCERT signature validity time

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

7.2 Key Management

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

7.3 Input Data Validation

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

8 Trust management

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

8.1 The Key Identifier (`kids`)

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

8.2 Differences to the ICAO eMRTD PKI trust model

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

8.3 Extended key Usage Identifiers

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