eHealth Network

Guidelines on

Technical Specifications

for EU Digital COVID Certificates

Volume 5

Public Key Certificate Governance

V1.2

2022-02-23

eHealth Network

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

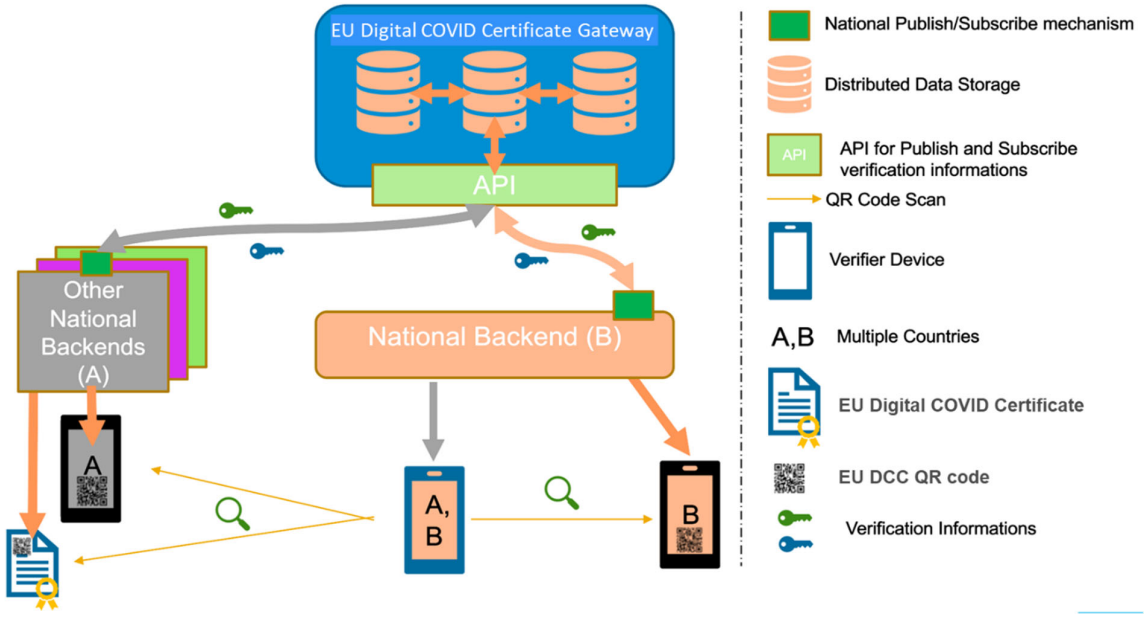
This document complements normative technical specifications adopted and published as Commission Implementing Decision (EU) 2021/1073 (with any amendments, such as Commission Implementing Decision (EU) 2021/2014). The document should be read together with the legal acts.

Annex IV of the Commission Implementing Decision (EU) 2021/1073 of 28 June 2021 describes general rules for the public key certificate governance.

1.1 Context

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

The following picture presents a high-level overview of the system.



1.2 Scope of Document

Digital signatures can be used to achieve data integrity and authenticity. Public Key Infrastructures establish trust by binding public keys to verified identities (or issuers). This is necessary to allow other participants to verify the data origin and the identity of the communication partner and decide about trust. In the DCCG, multiple public key certificates are used for authenticity. This document defines which public key certificates are used and how they should be designed in order to allow broad interoperability between the different Member States. This document is based on [1] and [2]. It provides more details on the necessary public key certificates and it gives guidance on certificate templates and validity periods for countries that want to operate their own CSCA. Since DCCs shall be verifiable for a defined timeframe (starting from the issuing, expire after a given time), it is necessary to define a verification model for all signatures applied on the public key certificates and the digital COVID certificates. Legal and administrative procedures are not in the scope of this document, they must be defined separately.

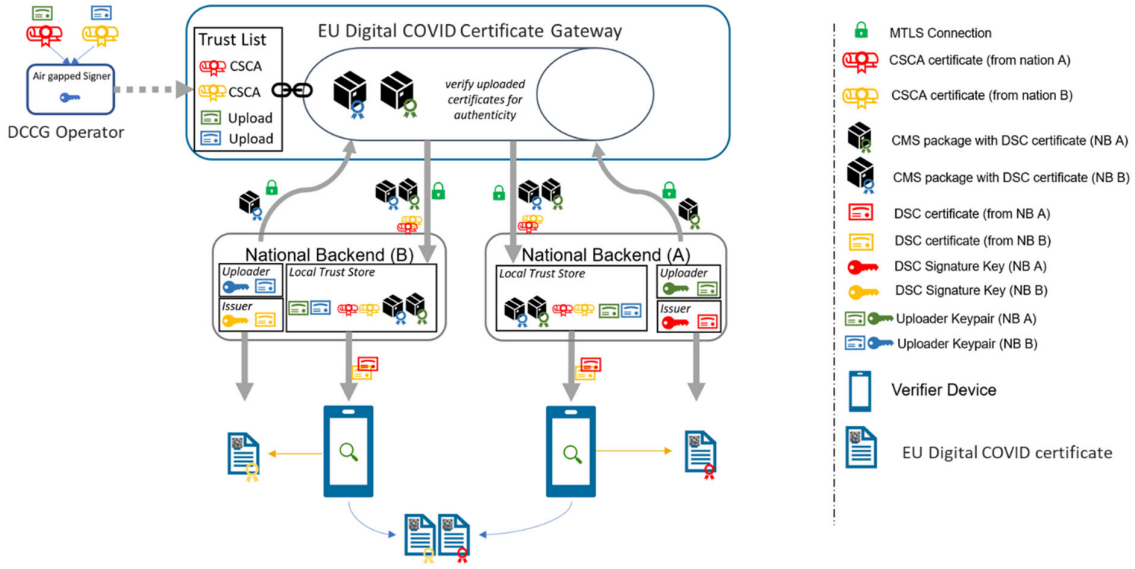
2 Terminology

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

3 DCCG communication flows and security services

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

This section gives an overview of the communication flows and security services in the DCCG system. It also defines which keys and certificates are used to protect the communication, the uploaded information, the digital COVID certificates, and a signed trust list that contains all onboarded CSCA certificates. The following figure gives a high-level overview of the DCCG communication flow and security services. The following sub-sections will explain the design in more detail.



The DCCG works as a data hub that allows the exchange of signed data packages for registered EU Member States. In the current phase, the signed data packages contain the Document Signer Certificates that are used by the Member States. This allows other national backends to fetch them and distribute the information to their validation apps. Even if the DSCs are already signed by the CSCA, this approach allows to extend the system later to allow national backends the upload of different, generally unsigned, content (like validation rules).

Uploaded data packages are provided by the DCCG “as is”, meaning that the DCCG does not add or delete DSCs from the packages it receives. The national backend (NB) of the Member States shall be enabled to verify the end-to-end integrity and authenticity of the uploaded data (see Section 3.4).

In addition to this - National Backends and the DCCG will use mutual TLS authentication to establish a secure connection (see Section 3.2). So this is in *addition* to the signatures in the data exchanged.

3.1 Authentication and connection establishment

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

3.2 Country Signing Certificate Authorities and Validation Model

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

3.3 Integrity and authenticity of uploaded data

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

3.4 Requirements on the technical DCCG architecture

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

4 Certificate Lifecycle Management

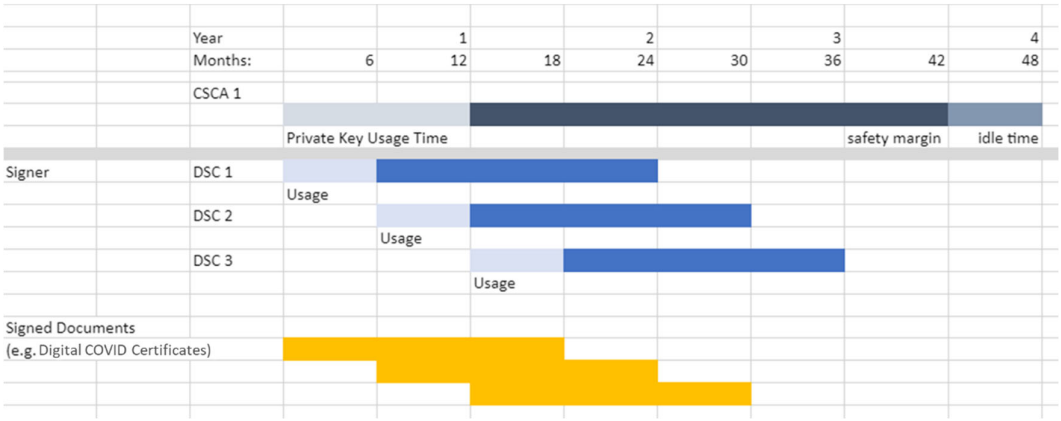
4.1 Registration of National Backends

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

4.2 Certificate authorities, validity periods and renewal

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

The following picture shows the private key usage periods and certificate lifetimes for the recommended times in case that Member States want to operate their own CSCA (assuming one-year maximum lifetime of signed documents).



Member States might define different validity periods for their public key certificates.

4.3 Revocation of certificates

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

4.4 Certificates for Staging Environments

The member states and the DCC operator will use non-production environments (development, acceptance, testing, etc.) to test the system before they move to production or when new features are released. It is mandatory that public key certificates and the related key material is not reused between the production and the non-production environments. Hence, member states MUST use different public key certificates and private keys for the production and all the non-production environments. This applies to the NB_{TLS}, NB_{UP} certificates of the member states and all DSCs. The $DCCG_{TA}$ certificates will be different for production and non-production environments.

There are multiple reasons why certificates should not be reused across different environments. One reason is that the corresponding private keys must be copied from one system to the other and typically non-production environments do not enjoy the same level of protection as production environments. This puts the security of the private keys at risk. In the scope of the DCC system there is an additional risk that DSCs issued for testing purpose are published on the production DCCG and these DSCs could be used to issue valid DCCs.

5 Certificate Templates

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

5.1 Cryptographic requirements

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

5.1.1 Requirements on the DSC

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

5.1.2 Requirements on TLS, Upload and CSCA

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

5.2 CSCA certificate (NB_{CSCA})

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

5.3 Document Signer (DSC)

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

The following extensions are to be used as defined in [2, Appendix A4]. Countries MAY also include an extendedKeyUsage entry with *zero* or more (i.e. up to 3) entries from:

Field	Value
extendedKeyUsage	1.3.6.1.4.1.1847.2021.1.1 for Test Issuers
extendedKeyUsage	1.3.6.1.4.1.1847.2021.1.2 for Vacination Issuers
extendedKeyUsage	1.3.6.1.4.1.1847.2021.1.3 for Recovery Issuers

These values are defined as non critical, therefore all applications should handle new and/or unknown OIDs gracefully.

5.4 Upload Certificates (NB_{UP})

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

5.5 National Backend TLS Client Authentication (NB_{TLS})

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

Be aware that self-signed certificates should also contain the key usage *Certificate signing* (`keyCertSign`), such that the (self) signature of the certificate can be validated.

5.6 Trust list signature certificate ($DCCG_{TA}$)

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

5.7 DGCG TLS Server certificates ($DCCG_{TLS}$)

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

6 REFERENCES

[1] Interoperability of health certificates – Trust Framework – v. 1.0 – 12.03.2021 – eHealth Network – available at https://ec.europa.eu/health/sites/health/files/ehealth/docs/trust-framework_interoperability_certificates_en.pdf - last accessed 27.04.2021

[2] Technical Specifications for Digital COVID Certificates Volume 1 V1.0.5 - eHealth Network – available at https://ec.europa.eu/health/sites/health/files/ehealth/docs/digital-green-certificates_v1_en.pdf - last accessed 27.04.2021

[3] ETSI EN 319 102-1: Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part 1: Creation and Validation – version 1.1.1, 2016 – available at https://www.etsi.org/deliver/etsi_en/319100_319199/31910201/01.01.01_60/en_31910201v010101p.pdf – last accessed 23.04.2021