COMMISSION IMPLEMENTING DECISION (EU) 2021/1073

of 28 June 2021

laying down technical specifications and rules for the implementation of the trust framework for the EU Digital COVID Certificate established by Regulation (EU) 2021/953 of the European Parliament and of the Council

(Text with EEA relevance)

THE EUROPEAN COMMISSION,

Having regard to the Treaty on the Functioning of the European Union,

Having regard to Regulation (EU) 2021/953 of the European Parliament and of the Council on a framework for the issuance, verification and acceptance of interoperable COVID-19 vaccination, test and recovery certificates (EU Digital COVID Certificate) to facilitate free movement during the COVID-19 pandemic ([1]), and in particular Article 9(1) and (3) thereof,

Whereas:

(1) Regulation (EU) 2021/953 sets out the EU Digital COVID Certificate the purpose of which is to serve as a proof that a person has received a COVID-19 vaccine, a negative test result or recovered from infection.

(2) In order for the EU Digital COVID Certificate to be operational throughout the Union, it is necessary to establish technical specifications and rules to populate, securely issue and verify the digital COVID certificates, ensure the protection of personal data, lay down the common structure of the unique certificate identifier and issue a valid, secure and interoperable barcode. That trust framework also sets the premises for seeking to ensure interoperability with international standards and technological systems, and, as such, could provide the model for cooperation at global level.

(3) The ability to read and interpret the EU Digital COVID Certificate requires a common data structure and agreement on the intended meaning of each data field of the payload and its possible values. In order to facilitate such interoperability, it is necessary to define a common coordinated data structure for the framework of the EU Digital COVID Certificate. The guidelines for this framework have been developed by the eHealth Network established on the basis of Directive 2011/24/EU of the European Parliament and of the Council ([2]). Those guidelines should be taken into account in laying down the technical specifications setting out the format and trust management for the EU Digital COVID Certificate. A data structure specification and encoding mechanisms should be specified, as well as 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.

(4) In addition to the technical specifications for format and trust management of the EU Digital COVID Certificate, general rules for the purpose of populating the certificates should be established in order to be used for coded values in the content of the EU Digital COVID Certificate. The value sets implementing those rules should be regularly updated and published by the Commission, drawing upon the relevant work of the eHealth Network.

(5) Pursuant to Regulation (EU) 2021/953, authentic certificates making up the EU Digital COVID Certificate are to be individually identifiable by means of a unique certificate identifier, taking into account that citizens may be issued more than one certificate during the time Regulation (EU) 2021/953 remains in force. The unique certificate identifier is to be composed of an alphanumeric string, and Member States should ensure that it does not contain any data linking it to other documents or identifiers, such as to passport or identity card numbers, in order to prevent that the holder can be identified. For the purpose of ensuring that the certificate identifier is unique, technical specifications and rules for the common structure thereof should be established.

[1] OJ L 211, 15.6.2021, p. 1.

[2] Directive 2011/24/EU of the European Parliament and of the Council of 9 March 2011 on the application of patients' rights in cross-border healthcare (OJ L 88, 4.4.2011, p. 45).

(6) The security, authenticity, validity and integrity of the certificates comprising the EU Digital COVID Certificate and their compliance with Union data protection law are key to their acceptance in all Member States. Those objectives are achieved by the trust framework laying out the rules on and infrastructure for the reliable and secure issuance and verification of the EU Digital COVID certificates. Among others, the trust framework should be based on a public-key infrastructure with a trust chain from Member States' health authorities or other trusted authorities to the individual entities issuing the EU Digital COVID certificates. Therefore, with a view to ensuring an EU-wide interoperability system, the Commission has built a central system – the EU Digital COVID Certificate gateway (the 'gateway') – that stores public keys used for verification. When the QR code certificate is scanned, the digital signature is verified using the relevant public key, previously stored in that central gateway. Digital signatures can be used to ensure data integrity and authenticity. Public Key Infrastructures establish trust by binding public keys to certificate issuers. In the gateway, multiple public key certificates are used for authenticity. To ensure a secure data exchange for public key material between Member States and allow broad interoperability, it is necessary to establish the public key certificates that may be used and provide how they should be generated.

(7) This Decision allows to make the requirements of Regulation (EU) 2021/953 operational in a way that minimises the processing of personal data to what is necessary to make the EU Digital COVID Certificate operational and contributes to an implementation by the final controllers that respects data protection by design.

(8) In accordance with Regulation (EU) 2021/953, the authorities or other designated bodies responsible for issuing the certificates are controllers referred to in Article 4(7) of Regulation (EU) 2016/679 of the European Parliament and of the Council [3] in their role of processing personal data in the course of the issuance process. Depending on how Member States organise the issuance process, there may be one or more authorities or designated bodies, for example regional health services. In accordance with the principle of subsidiarity, that is a choice for Member States. Therefore, Member States are best placed to ensure, where there are multiple authorities or other designated bodies, that their respective responsibilities are clearly allocated, independently of whether they are separate or joint controllers (including regional health services establishing a joint patient portal for issuing the certificates). Similarly, regarding verification of certificates by the competent authorities of the Member State of destination or transit, or by the cross-border passenger transport services operators required by national law to implement certain public health measures during the COVID-19 pandemic, those verifiers have to comply with their obligations under data protection rules.

(9) There is no processing of personal data through the EU Digital COVID Certificate gateway, as the gateway only contains the public keys of the signing authorities. Those keys relate to the signing authorities and do not allow either direct or indirect re-identification of a natural person to whom a certificate has been issued. In its role as the manager of the gateway, the Commission should thus be neither a controller nor processor of personal data.

(10) The European Data Protection Supervisor was consulted in accordance with Article 42(1) of Regulation (EU) 2018/1725 of the European Parliament and of the Council [4] and delivered an opinion on 22 June 2021.

(11) Considering that technical specifications and rules are necessary for the application of Regulation (EU) 2021/953 from 1 July 2021, the immediate application of this Decision is justified.

(12) Therefore, in the light of the need for rapid implementation of the EU Digital COVID Certificate, this Decision should enter into force on the day of its publication,

[3] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119, 4.5.2016, p. 1).

[4] Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39).

HAS ADOPTED THIS DECISION:

Article 1

The technical specifications for the EU Digital COVID Certificate laying down the generic data structure, the encoding mechanisms, and the transport encoding mechanism in a machine-readable optical format are set out in Annex I.

Article 2

The rules for populating the certificates referred to in Article 3(1) of Regulation (EU) 2021/953 are set out in Annex II to this Decision.

Article 3

The requirements laying down the common structure of the unique certificate identifier are set out in Annex III.

Article 4

The governance rules applicable to public key certificates in relation to the EU Digital COVID Certificate gateway supporting the interoperability aspects of the trust framework are set out in Annex IV.

This Decision shall enter into force on the day of its publication in the *Official Journal of the European Union*.

Done at Brussels, 28 June 2021.

For the Commission
The President
Ursula VON DER LEYEN

ANNEX I

FORMAT AND TRUST MANAGEMENT

Generic data structure, encoding mechanisms and transport encoding mechanism in a machine-readable optical format (hereinafter called 'QR')

1. Introduction

The technical specifications set out in this Annex contain a generic data structure and encoding mechanisms for the EU Digital COVID Certificate ('DCC'). They also specify a transport encoding mechanism in a machine-readable optical format ('QR'), which can be displayed on the screen of a mobile device or printed out. The electronic health certificate container formats of these specifications are generic, but in this context used to carry the DCC.

2. Terminology

For the purpose of this Annex, 'issuers' means organisations using these specifications for issuing health certificates and 'verifiers' means organisations accepting health certificates as proof of health status. 'Participants' means issuers and verifiers. Some aspects set out in this Annex 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.

3. Electronic Health Certificate Container Format

The Electronic Health Certificate Container Format ('HCERT') is designed to provide a uniform and standardised vehicle for health certificates from their different issuers ('issuers'). The objective of these specifications is to harmonise how those health certificates are represented, encoded and signed with the goal of facilitating interoperability.

The ability to read and interpret a DCC issued by any issuer requires a common data structure and agreement on the significance of each data field of the payload. To facilitate such interoperability, a common coordinated data structure is defined through the use of a 'JSON' schema that constitutes the framing of the DCC.

3.1. *Structure of the payload*

The payload is structured and encoded as a CBOR with a COSE digital signature. This is commonly known as a "CBOR Web Token" (CWT), and is defined in RFC 8392 [1]. The payload, as defined in the following sections, is transported in a hcert claim.

The integrity and authenticity of origin of payload data must be verifiable by the verifier. To provide this mechanism, the issuer must sign the CWT using an asymmetric electronic signature scheme as defined in the COSE specification (RFC 8152 [2]).

3.2. *CWT Claims*

3.2.1. CWT Structure Overview

Protected Header

— Signature Algorithm (alg, label 1)

— Key Identifier (kid, label 4)

Payload

— Issuer (iss, claim key 1, optional, ISO 3166-1 alpha-2 of issuer)

— Issued At (iat, claim key 6)

— Expiration Time (exp, claim key 4)

— Health Certificate (hcert, claim key -260)

— EU Digital COVID Certificate v1 (eu_DCC_v1, claim key 1)

Signature

[1] rfc8392 (ietf.org)

[2] rfc8152 (ietf.org)

3.2.2. Signature Algorithm

The Signature Algorithm (alg) parameter indicates what algorithm is used for the creating the signature. It must meet or exceed current SOG-IS guidelines as summarised in the following paragraphs.

One primary and one secondary algorithm is defined. The secondary algorithm should only be used if the primary algorithm is not acceptable within the rules and regulations imposed on the issuer.

In order to ensure the security of the system, all implementations have to incorporate the secondary algorithm. For this reason, both the primary and the secondary algorithm must be implemented.

The SOG-IS set levels for the primary and secondary algorithms are:

— Primary Algorithm: The primary algorithm is Elliptic Curve Digital Signature Algorithm (ECDSA) as defined in (ISO/IEC 14888–3:2006) section 2.3, using the P–256 parameters as defined in appendix D (D.1.2.3) of (FIPS PUB 186–4) in combination with the SHA–256 hash algorithm as defined in (ISO/IEC 10118–3:2004) function 4.

This corresponds to the COSE algorithm parameter ES256.

— Secondary Algorithm: The secondary algorithm is RSASSA-PSS as defined in (RFC 8230 [3]) with a modulus of 2048 bits in combination with the SHA–256 hash algorithm as defined in (ISO/IEC 10118–3:2004) function 4.

This corresponds to the COSE algorithm parameter: PS256.

3.2.3. Key Identifier

The Key Identifier (kid) claim indicates the Document Signer Certificate (DSC) containing the public key to be used by the verifier for checking the correctness of the digital signature. Public key certificate governance, including requirements for DSCs, is described in Annex IV.

The Key Identifier (kid) claim is used by verifiers for selecting the correct public key from a list of keys pertaining to the issuer indicated in the Issuer (iss) Claim. Several keys may be used in parallel by an issuer for administrative reasons and when performing key rollovers. The Key Identifier is not a security-critical field. For this reason, it may also be placed in an unprotected header if required. Verifiers must accept both options. If both options are present, the Key Identifier in the protected header must be used.

Due to the shortening of the identifier (for size limitation reasons) there is a slim but non-zero chance that the overall list of DSCs accepted by a verifier may contain DSCs with duplicate kids. For this reason, a verifier must check all DSCs with that kid.

3.2.4. Issuer

The Issuer (iss) claim is a string value that may optionally hold the ISO 3166-1 alpha-2 Country Code of the entity issuing the health certificate. This claim can be used by a verifier to identify which set of DSCs to use for verification. The Claim Key 1 is used to identify this claim.

3.2.5. Expiration Time

The Expiration Time (exp) claim shall hold a timestamp in the integer NumericDate format (as specified in RFC 8392 [4], section 2) indicating for how long this particular signature over the payload shall be considered valid, after which a verifier must reject the payload as expired. The purpose of the expiry parameter is to force a limit of the validity period of the health certificate. The Claim Key 4 is used to identify this claim.

The Expiration Time must not exceed the validity period of the DSC.

[3] rfc8230 (ietf.org)

[4] rfc8392 (ietf.org)

3.2.6. Issued At

The Issued At (iat) claim shall hold a timestamp in the integer NumericDate format (as specified in RFC 8392 [5], section 2) indicating the time when the health certificate was created.

The Issued At field must not predate the validity period of the DSC.

Verifiers may apply additional policies with the purpose of restricting the validity of the health certificate based on the time of issue. The Claim Key 6 is used to identify this claim.

3.2.7. Health Certificate Claim

The Health Certificate (hcert) claim is a JSON (RFC 7159 [6]) object containing the health status information. Several different types of health certificate may exist under the same claim, of which the DCC is one.

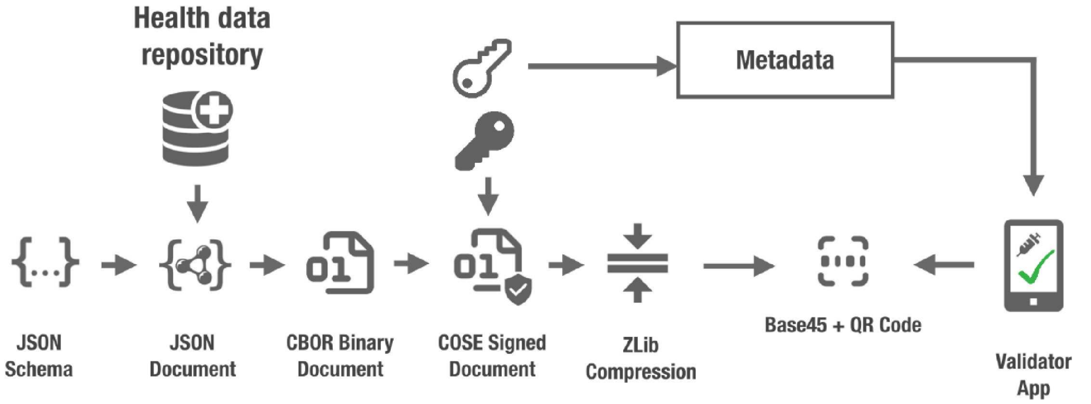
The JSON is purely for schema purposes. The representation format is CBOR, as defined in (RFC 7049 [7]). Application developers may not actually ever decode, or encode to and from the JSON format, but use the in-memory structure.

The Claim Key to be used to identify this claim is -260.

Strings in the JSON object should be normalized according to the Normalization Form Canonical Composition (NFC) defined in the Unicode standard. Decoding applications should however be permissive and robust in these aspects, and acceptance of any reasonable type conversion is strongly encouraged. If non-normalised data is found during decoding, or in subsequent comparison functions, implementations should behave as if the input is normalised to NFC.

4. Serialisation and creation of the DCC payload

As serialization pattern, the following scheme is used:



The process starts with extraction of data, for example, from a Health Data Repository (or some external data source), structuring the extracted data according to the defined DCC Schemas. In this process, conversion to the defined data format and transformation for human readability may take place before the serialization to CBOR starts. The acronyms of the claims shall be mapped in every case to the display names before serialization and after deserialization.

Optional national data content is not allowed in certificates issued following the Regulation (EU) 2021/953 [8]. The data content is limited to the defined data elements in the minimum data set specified in the Annex to Regulation 2021/953.

[5] rfc8392 (ietf.org)

[6] rfc7159 (ietf.org)

[7] rfc7049 (ietf.org)

[8] Regulation (EU) 2021/953 of the European Parliament and of the Council of 14 June 2021 on a framework for the issuance, verification and acceptance of interoperable COVID-19 vaccination, test and recovery certificates (EU Digital COVID Certificate) to facilitate free movement during the COVID-19 pandemic, OJ L 211, 15.6.2021, p. 1.

5. **Transport Encodings**

5.1. *Raw*

For arbitrary data interfaces, the HCERT container and its payloads may be transferred as-is, utilising any underlying, 8 bit safe, reliable data transport. These interfaces may include Near-Field Communication (NFC), Bluetooth or transfer over an application layer protocol, for example transfer of an HCERT from the Issuer to a holder's mobile device.

If the transfer of the HCERT from the Issuer to the holder is based on a presentation-only interface (for example, SMS, email), the raw transport encoding is obviously not applicable.

5.2. *Barcode*

5.2.1. Payload (CWT) Compression

To lower size and to improve speed and reliability in the reading process of the HCERT, the CWT shall be compressed using ZLIB (RFC 1950 [9]) and the Deflate compression mechanism in the format defined in RFC 1951 [10].

5.2.2. QR 2D Barcode

In order to better handle legacy equipment designed to operate on ASCII payloads, the compressed CWT is encoded as ASCII using Base45 before being encoded into a 2D barcode.

The QR format as defined in (ISO/IEC 18004:2015) shall be used for 2D barcode generation. An error correction rate of 'Q' (around 25 %) is recommended. Because Base45 is used, the QR code has to use Alphanumeric encoding (Mode 2, indicated by the symbols 0010).

In order for verifiers to be able to detect the type of data encoded and to select the proper decoding and processing scheme, the Base45 encoded data (as per this specification) shall be prefixed by the Context Identifier string "HC1:". Future versions of this specification that impact backwards-compatibility shall define a new Context Identifier, whereas the character following "HC" shall be taken from the character set [1-9A-Z]. The order of increments is defined to be in that order, i.e., first [1-9] and then [A-Z].

The optical code is recommended to be rendered on the presentation media with a diagonal size between 35 mm and 60 mm to accommodate readers with fixed optics where the presentation media is required to be placed on the surface of the reader.

If the optical code is printed on paper using low-resolution (< 300 dpi) printers, care must be taken to represent each symbol (dot) of the QR code exactly square. Non-proportional scaling will result in some rows or columns in the QR having rectangular symbols, which will hamper readability in many cases.

6. **Trust List Format (CSCA and DSC list)**

Each Member State is required to provide a list of one or more Country Signing Certificate Authorities (CSCAs) and a list of all valid Document Signer Certificates (DSCs), and keep these lists current.

6.1. *Simplified CSCA/DSC*

As of this version of the specifications, Member States shall not assume that any Certificate Revocation List (CRL) information is used; or that the Private Key Usage Period is verified by implementors.

Instead, the primary validity mechanism is the presence of the certificate on the most recent version of that certificate list.

[9] rfc1950 (ietf.org)
[10] rfc1951 (ietf.org)

6.2. *ICAO eMRTD PKI and Trust Centers*

Member States can use a separate CSCA – but may also submit their existing eMRTD CSCA certificates and/or DSCs; and may even chose to procure these from (commercial) trust centres – and submit these. However, any DSC must always be signed by the CSCA submitted by that Member State.

7. **Security Considerations**

When designing a scheme using this specification, Member States shall identify, analyse and monitor certain security aspects.

The following aspects should be taken into account as a minimum:

7.1. *HCERT signature validity time*

The issuer of HCERTs is required to limit the validity period of the signature by specifying a signature expiry time. This requires the holder of a health certificate to renew it at periodic intervals.

The acceptable validity period may be determined by practical constraints. For example, a traveller may not have the possibility to renew the health certificate during a trip overseas. However, it may also be the case that an issuer is considering the possibility of a security compromise of some sort, which requires the issuer to withdraw a DSC (invalidating all health certificates issued using that key which is still within their validity period). The consequences of such an event may be limited by regularly rolling Issuer keys and requiring renewal of all health certificates, on some reasonable interval.

7.2. *Key management*

This specification relies heavily on strong cryptographic mechanisms to secure data integrity and data origin authentication. Maintaining the confidentiality of the private keys is therefore necessary.

The confidentiality of cryptographic keys can be compromised in a number of different ways, for instance:

- The key generation process may be flawed, resulting in weak keys.
- The keys may be exposed by human error.
- The keys may be stolen by external or internal perpetrators.
- The keys may be calculated using cryptanalysis.

In order to mitigate against the risks that the signing algorithm is found to be weak, allowing the private keys to be compromised through cryptanalysis, this specification recommends all participants to implement a secondary fallback signature algorithm based on different parameters or a different mathematical problem than the primary.

As regards the risks mentioned related to the issuers' operating environments, mitigations measures to ensure effective control shall be implemented such as to generate, store and use the private keys in Hardware Security Modules (HSMs). Use of HSMs for signing health certificates is highly encouraged.

Regardless of whether an issuer decides to use HSMs or not, a key roll-over schedule should be established where the frequency of the key roll-overs is proportionate to the exposure of keys to external networks, other systems and personnel. A well-chosen roll-over schedule also limits the risks associated with erroneously issued health certificates, enabling an issuer to revoke such health certificates in batches, by withdrawing a key, if required.

7.3. *Input data validation*

These specifications may be used in a way that implies receiving data from untrusted sources into systems that may be of mission-critical nature. To minimise the risks associated with this attack vector, all input fields must be properly validated by data types, lengths and contents. The issuer signature shall also be verified before any processing of the contents of the HCERT takes place. However, the validation of the issuer Signature implies parsing the Protected Issuer Header first, in which a potential attacker may attempt to inject carefully crafted information designed to compromise the security of the system.

8. Trust Management

The signature of the HCERT requires a public key to verify. Member States shall make these public keys available. Ultimately, every verifier needs to have a list of all public keys it is willing to trust (as the public key is not part of the HCERT).

The system consists of (only) two layers; for each Member State one or more country level certificates that each signs one or more Document Signer Certificates that are used in day to day operations.

The Member State certificates are called Country Signing Certificate Authority (CSCA) certificates and are (typically) self-signed. Member States may have more than one (for example, in case of regional devolution). These CSCA certificates regularly sign the Document Signer Certificates (DSCs) used for signing HCERTs.

The "Secretariat" is a functional role. It shall regularly aggregate and publish the Member States' DSCs, after having verified these against the list of CSCA certificates (which have been conveyed and verified by other means).

The resulting list of DSCs shall then provide the aggregated set of acceptable public keys (and the corresponding kids) that verifiers can use to validate the signatures over the HCERTs. Verifiers must fetch and update this list regularly.

Such Member State-specific lists may be adapted in the format for their own national setting. As such, the file format of this trust list may vary, for example, it can be a signed JWKS (JWK set format per RFC 7517 ([11]), section 5) or any other format specific to the technology used in that Member State.

In order to ensure simplicity, Member States may both submit their existing CSCA certificates from their ICAO eMRTD systems or, as recommended by the WHO, create one specifically for this health domain.

8.1. *The Key Identifier (kids)*

The key identifier (kid) is calculated when constructing the list of trusted public keys from DSCs and consists of a truncated (first 8 bytes) SHA-256 fingerprint of the DSC encoded in DER (raw) format.

Verifiers do not need to calculate the kid based on the DSC and can directly match the key identifier in issued health certificate with the kid on the trust list.

8.2. *Differences to the ICAO eMRTD PKI trust model*

While patterned on best practices of the ICAO eMRTD PKI trust model, a number of simplifications shall be made in the interest of speed:

- A Member State may submit multiple CSCA certificates.
- The DSC (key usage) validity period may be set to any length not exceeding that of the CSCA certificate and may be absent.
- The DSC may contain policy identifiers (Extended Key Usage) that are specific to health certificates.
- Member States may choose to never do any verification of published revocations; but instead purely rely on the DSC lists they get daily from the Secretariat or compile themselves.

[11] rfc7517 (ietf.org)

ANNEX II

RULES FOR THE PURPOSE OF POPULATING THE EU DIGITAL COVID CERTIFICATE

The general rules concerning the value sets established in this Annex aim to ensure interoperability on semantic level and shall allow uniform technical implementations for the DCC. Elements contained in this Annex may be used for the three different settings (vaccination/testing/recovery), as provided for in Regulation (EU) 2021/953. Only elements with the necessity of semantic standardisation through coded value sets are listed in this Annex.

Translation of the coded elements into the national language are under the responsibility of the Member States.

For all data fields not mentioned in the following value set descriptions, encoding in UTF-8 is recommended (name, testing centre, certificate issuer). Data fields containing calendar dates (date of birth, date of vaccination, date of test sample collection, date of first positive test result, certificate validity dates) are recommended to be encoded following the ISO 8601.

If for any reason the preferred code systems listed below cannot be used, other international code systems may be used and advice on how to map the codes from the other code system to the preferred code system should be put in place. Text (display names) may be used in exceptional cases as a backup mechanism when a suitable code is not available in the defined value sets.

Member States using other coding in their systems should map such codes to the described value sets. Member States are responsible for any such mappings.

The value sets shall be regularly updated by the Commission with the support of the eHealth Network and the Health Security Committee. The updated value sets shall be published on the relevant website of the Commission, as well as on the webpage of the eHealth Network. A history of changes should be provided.

1. **Disease or agent targeted/Disease or agent from which the holder has recovered: COVID-19 (SARS-CoV-2 or one of its variants)**

Preferred Code System: SNOMED CT.

To be used in certificate 1, 2 and 3.

The selected codes shall refer to COVID-19 or, if more detailed information on the genetic variant of SARS-CoV-2 is needed, to these variants if such detailed information is needed due to epidemiological reasons.

Example of a code that should be used is the SNOMED CT code 840539006 (COVID-19).

2. **COVID-19 vaccine or prophylaxis**

Preferred Code System: SNOMED CT or ATC Classification.

To be used in certificate 1.

Examples of codes that should be used from the preferred code systems are the SNOMED CT code 1119305005 (SARS-CoV-2 antigen vaccine), 1119349007 (SARS-CoV-2 mRNA vaccine) or J07BX03 (covid-19 vaccines). The value set should be extended when new vaccine types are developed and put into use.

3. **COVID-19 vaccine medicinal product**

Preferred Code Systems (in the order of preference):

— Union Register of medicinal products for vaccines with EU-wide authorisation (authorisation numbers)

— A global vaccine register such as one that could be established by the World Health Organisation

— Name of the vaccine medicinal product in other cases. If the name includes whitespaces, these should be replaced by a hyphen (-).

Name of the Value Set: Vaccine.

To be used in certificate 1.

An example of a code that should be used from the preferred code systems is EU/1/20/1528 (Comirnaty). An example of the name of the vaccine to be used as a code: Sputnik-V (standing for Sputnik V).

4. **COVID-19 vaccine marketing authorisation holder or manufacturer**

Preferred Code System:

— Organisation code from EMA (SPOR system for ISO IDMP)

— A global vaccine marketing authorisation holder or manufacturer register, such as one that could be established by the World Health Organisation

— Name of the organisation in other cases. If the name includes whitespaces, these should be replaced by a hyphen (-).

To be used in certificate 1.

Example of a code that should be used from the preferred code system is ORG-100001699 (AstraZeneca AB). An example of the name of the organisation to be used as a code: Sinovac-Biotech (standing for Sinovac Biotech).

5. **Number in a series of doses as well as the overall number of doses in the series**

To be used in certificate 1.

Two fields:

(1) Number of dose administered in a cycle

(2) Number of expected doses for a complete cycle (specific for a person at the time of administration)

For example, 1/1, 2/2 will be presented as completed; including the option 1/1 for vaccines including two doses, but for which the protocol applied by the Member State is to administer one dose to citizens that were diagnosed with COVID-19 prior to the vaccination. The overall number of doses in the series should be indicated as per information available at the time when the dose is administered. For example, if a specific vaccine requires a third shot (booster) at the time of the latest administered shot, the second field number shall reflect this (for example 2/3, 3/3 etc.).

6. **Member State or third country in which the vaccine was administered/test was carried out**

Preferred Code System: ISO 3166 Country Codes.

To be used in certificates 1, 2 and 3.

Value set content: the complete list of 2-letter codes, available as a value set defined in FHIR (http://hl7.org/fhir/ValueSet/iso3166-1-2)

7. **The type of test**

Preferred Code System: LOINC.

To be used in certificate 2, and certificate 3 if support for the issuance of recovery certificates based on types of test other than NAAT is introduced through a delegated act.

The codes in this value set shall refer to the method of the test and shall be selected at least to separate the NAAT tests from RAT tests as expressed in Regulation (EU) 2021/953.

An example of a code that should be used from the preferred code system is LP217198-3 (Rapid immunoassay).

8. **Manufacturer and commercial name of the test used (optional for NAAT test)**

Preferred Code System: List from the HSC of Rapid Antigen Tests as maintained by the JRC (COVID-19 In Vitro Diagnostic Devices and Test Methods Database.

To be used in certificate 2.

The content of the Value Set shall include the selection of rapid antigen test as listed in the common and updated list of COVID-19 rapid antigen tests, established on the basis of Council Recommendation 2021/C 24/01 and agreed by the Health Security Committee. The list is maintained by the JRC in the COVID-19 In Vitro Diagnostic Devices and Test Methods Database at: https://covid-19-diagnostics.jrc.ec.europa.eu/devices/hsc-common-recognition-rat

For this code system, relevant fields such as the identifier of the test device, name of the test and manufacturer shall be used, following the JRC structured format available at https://covid-19-diagnostics.jrc.ec.europa.eu/devices

9. **Result of the test**

Preferred Code System: SNOMED CT.

To be used in certificate 2.

The codes selected shall allow distinguishing between positive and negative test results (detected or not detected). Additional values (like undetermined) may be added if the use cases do require this.

Examples of codes that should be used from the preferred code system are 260415000 (Not detected) and 260373001 (Detected).

ANNEX III

COMMON STRUCTURE OF THE UNIQUE CERTIFICATE IDENTIFIER

1. **Introduction**

Each EU Digital COVID Certificate (DCC) shall include a unique certificate identifier (UCI) which supports the interoperability of the DCCs. The UCI may be used to verify the certificate. Member States shall be responsible for implementing the UCI. The UCI is a means to verify the veracity of the certificate and, where applicable, to link to a registration system (for example, an IIS). These identifiers shall also enable (paper and digital) assertions by the Member States that individuals have been vaccinated or tested.

2. **Composition of the unique certificate identifier**

The UCI shall follow a common structure and format easing human- and/or machine-interpretability of information and may relate to elements such as Member State of vaccination, the vaccine itself and a Member State specific identifier. It ensures flexibility to Member States to format it, in full respect of data protection legislation. The order of the separate elements follows a defined hierarchy that can enable future modifications of the blocks while maintaining its structural integrity.

The possible solutions for the composition of the UCI form a spectrum wherein the modularity and human-interpretability are the two main diversifying parameters and one fundamental characteristic:

— Modularity: the degree to which the code is composed of distinct building blocks that contain semantically different information

— Human-interpretability: the degree to which the code is meaningful or can be interpreted by the human reader

— Globally unique; the Country or Authority identifier is well-managed; and each country (authority) is expected to manage its segment of the namespace well by never recycling or re-issuing identifiers. The combination of this ensures that each identifier is globally unique.

3. **General requirements**

The following overarching requirements should be satisfied in relation to the UCI:

(1) Charset: only uppercase US-ASCII alpha numerical characters ('A' to 'Z', '0' to '9') are allowed; with additional special characters for separation from RFC3986 [1] [2], namely {'/','#',':'};

(2) Maximum length: designers should try to aim for a length of 27-30 characters [3];

(3) Version prefix: this refers to the version of the UCI schema. The version prefix is '01' for this version of the document; the version prefix is composed of two digits;

(4) Country prefix: the country code is specified by ISO 3166-1. Longer codes (e.g. 3 characters and up (for example, 'UNHCR') are reserved for future use;

(5) Code suffix/Checksum:

5.1. Member States should use a checksum when it is likely that transmission, (human) transcription or other corruptions may occur (that is to say when used in print).

5.2. The checksum must not be relied upon for validating the certificate and is not technically part of the identifier but is used to verify the integrity of the code. This checksum should be the ISO-7812-1 (LUHN-10) [4] summary of the entire UCI in digital/wire transport format. The checksum is separated from the rest of the UCI by a '#' character.

[1] rfc3986 (ietf.org)

[2] Fields such as Sex, Batch/lot number, Administering centre, Health Professional identification, Next vaccination date may not be needed for purposes other than medical use.

[3] For implementation with QR codes, Member States could consider an extra set of characters up to a total length of 72 characters (including the 27-30 of the identifier itself) may be used to convey other information. The specification of this information is up to the Member States to define.

[4] The Luhn mod N algorithm is an extension to the Luhn algorithm (also known as mod 10 algorithm) which works for numeric codes and is used for example for calculating the checksum of credit cards. The extension allows the algorithm to work with sequences of values in any base (in our case alpha characters).

Backwards-compatibility should be ensured: Member States that over time change the structure of their identifiers (within the main version, currently set at v1) must ensure that any two identifiers that are identical represent the same vaccination certificate/assertion. Or, in other words, Member States cannot recycle identifiers.

4. **Options for unique certificate identifiers for vaccination certificates**

The eHealth Network guidelines for verifiable vaccination certificates and basic interoperability elements [5] provide for different options available to Member States and other parties that may co-exist among different Member States. Member States may deploy such different options in different version of the UCI schema.

[5] https://ec.europa.eu/health/sites/default/files/ehealth/docs/vaccination-proof_interoperability-guidelines_en.pdf

ANNEX IV

PUBLIC KEY CERTIFICATE GOVERNANCE

1. Introduction

The secure and trusted exchange of signature keys for EU digital COVID certificates (DCCs) between Member States is realised by the EU Digital COVID Certificate Gateway (DCCG), which acts as a central repository for the public keys. With the DCCG, Member States are empowered to publish the public keys corresponding to the private keys that they use to sign digital COVID certificates. Relying Member States can use the DCCG to fetch up-to-date public key material on a timely basis. Later, the DCCG can be extended to exchange trustworthy supplementary information that the Member States provide, like validation rules for DCCs. The trust model of the DCC framework is a Public Key Infrastructure (PKI). Each Member State maintains one or more Country Signing Certificate Authority (CSCA), certificates of which are relatively long lived. Following the Member State's decision, the CSCA may be the same or different than the CSCA used for machine-readable travel documents. The CSCA issues public key certificates for the national, short lived, Document Signers (i.e. signers for DCCs), which are called Document Signer Certificates (DSCs). The CSCA acts as a trust anchor such that relying Member States can use the CSCA certificate to validate the authenticity and integrity of the regularly changing DSCs. Once validated, Member States can provide these certificates (or just the public keys contained therein) to their DCC validation applications. Besides CSCAs and DSCs, the DCCG also relies on PKI to authenticate transactions, sign data, as the basis for authentication and as a means to ensure integrity of the communication channels between Member States and the DCCG.

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 Annex defines which public key certificates are used and how they shall be designed in order to allow broad interoperability among Member States. It provides more details on the necessary public key certificates and it gives guidance on certificate templates and validity periods for Member States 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 DCCs.

2. Terminology

The following table contains abbreviations and terminology used throughout this Annex.

Term	Definition
Certificate	Or public key certificate. An X.509 v3 certificate that contains the public key of an entity
CSCA	Country Signing Certificate Authority
DCC	EU Digital COVID Certificate. A signed digital document that contains vaccination, test or recovery information
DCCG	EU Digital COVID Certificate Gateway. This system is used to exchange DSCs between the Member States
DCCG_{TA}	The Trust Anchor certificate of the DCCG. The corresponding private key is used to sign the list of all CSCA certificates offline
DCCG_{TLS}	The TLS server certificate of the DCCG
DSC	Document Signer Certificate. The Public Key Certificate of a Member State's document signing authority (for example, a system that is allowed to sign DCCs). This certificate is issued by the CSCA of the Member State
EC-DSA	Elliptic Curve Digital Signature Algorithm. A cryptographic signature algorithm based on elliptic curves
Member State	Member State of the European Union

Term	Definition
mTLS	Mutual TLS. The Transport Layer Security Protocol with mutual authentication
NB	National backend of a Member State
NB_{CSCA}	The CSCA certificate of a Member State (could be more than one)
NB_{TLS}	The TLS client authentication certificate of a national backend
NB_{UP}	The certificate that a national backend uses to sign data packages that are uploaded to the DCCG
PKI	Public Key Infrastructure. Trust model based on public key certificates and certificate authorities
RSA	Asymmetric cryptographic algorithm based on integer factorization used for digital signatures or asymmetric encryption

3. DCCG communication flows and security services

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 DCCs, and a signed trust list that contains all onboarded CSCA certificates. The DCCG works as a data hub that allows the exchange of signed data packages for Member States.

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. In addition to this, national backends and the DCCG will use mutual TLS authentication to establish a secure connection. This is in addition to the signatures in the data exchanged.

3.1. *Authentication and connection establishment*

The DCCG uses Transport Layer Security (TLS) with mutual authentication to establish an authenticated encrypted channel between the Member State’s national backend (NB) and the Gateway environment. Therefore, the DCCG holds a TLS server certificate, abbreviated $DCCG_{TLS}$, and the national backends hold a TLS client certificate – abbreviated NB_{TLS}. Certificate templates are provided in *Section 5*. Every national backend can provide their own TLS certificate. This certificate will be whitelisted explicitly and thus may be issued by a publicly trusted certificate authority (for example, a certificate authority that follows the baseline requirements of the CA Browser Forum), by a national certificate authority or it can be self-signed. Every Member State is responsible for their national data and the protection of the private key used to establish the connection to the DCCG. The “bring your own certificate” approach requires a well-defined registration and identification process, as well as revocation and renewal procedures as described in *sections 4.1, 4.2* and *4.3*. The DCCG uses a whitelist where the TLS certificates of NBs are added after their successful registration. Only NBs that authenticate themselves with a private key that corresponds to a certificate from the whitelist can establish a secure connection to the DCCG. The DCCG will also use a TLS certificate that allows the NBs to verify that they are indeed establishing a connection to the “real” DCCG and not some malevolent entity posing as DCCG. The certificate of the DCCG will be provided to the NBs after successful registration. The $DCCG_{TLS}$ certificate will be issued from a publicly trusted CA (included in all major browsers). It is the responsibility of the Member States to verify that their connection to the DCCG is secure (for example, by checking the fingerprint of the $DCCG_{TLS}$ certificate of the server connected to against the one provided post registration).

3.2. *Country Signing Certificate Authorities and Validation Model*

Member States taking part in the DCCG framework must use a CSCA to issue the DSCs. Member States may have more than one CSCA, for example, in case of regional devolution. Each Member State can either use existing certificate authorities or they can set up a dedicated (possibly self-signed) certificate authority for the DCC system.

Member States must present their CSCA certificate(s) to the DCCG operator during the official onboarding procedure. After successful registration of the Member State (*see section 4.1 for more details*), the DCCG operator will update a signed trust list that contains all CSCA certificates that are active in the DCC framework. The DCCG operator will use a dedicated asymmetric key pair to sign the trust list and the certificates in an offline environment. The private key will not be stored on the online DCCG system, such that a compromise of the online system does not enable an attacker to compromise the trust list. The corresponding trust anchor certificate $DCCG_{TA}$, will be provided to the national backends during the onboarding process.

Member States can retrieve the trust list from the DCCG for their verification procedures. The CSCA is defined as the certificate authority that issues DSCs, hence Member States that use a multi-tier CA hierarchy (for example, Root CA -> CSCA -> DSCs) must provide the subordinary certificate authority that issues the DSCs. In this case, if a Member State uses an existing certificate authority, then the DCC system will ignore anything above the CSCA and whitelist only the CSCA as the trust anchor (even though it is a sub-ordinate CA). This is as the ICAO model, only allows for exactly 2 levels – a 'root' CSCA and a 'leaf' DSC signed by just that CSCA.

In case a Member State operates its own CSCA, the Member State is responsible for the secure operation and key management of this CA. The CSCA acts as the trust anchor for DSCs, and therefore protecting the private key of the CSCA is essential for the integrity of the DCC environment. The verification model in the DCC PKI is the shell model, which states that all certificates in the certificate path validation must be valid at a given time (i.e. the time of signature validation). Therefore, the following restrictions apply:

— The CSCA shall not issue certificates that are longer valid than the CA certificate itself;

— The document signer shall not sign documents that are longer valid than the DSC itself;

— Member States that operate their own CSCA must define validity periods for their CSCA and all issued certificates and they must take care of certificate renewal.

Section 4.2 contains recommendations for validity periods.

3.3. *Integrity and authenticity of uploaded data*

National backends can use the DCCG to upload and download digitally signed data packages after successful mutual authentication. In the beginning, these data packages contain the DSCs of the Member States. The key pair that is used by the national backend for the digital signature of uploaded data packages in the DCCG system is called national backend upload signature key pair and the corresponding public key certificate is abbreviated by NB_{UP} certificate. Each Member State brings its own NB_{UP} certificate, which can be self-signed, or issued by an existing certificate authority, such as a public certificate authority (i.e. a certificate authority that issues certificate in accordance with the CAB-Forum baseline requirements). The NB_{UP} certificate shall be different from any other certificates used by the Member State (i.e. CSCA, TLS client or DSCs).

The Member States must provide the upload certificate to the DCCG operator during the initial registration procedure (*see Section 4.1 for more details*). Every Member State is responsible for their national data and it must protect the private key that is used for signing the uploads.

Other Member States can verify the signed data packages using the upload certificates that are provided by the DCCG. The DCCG verifies the authenticity and integrity of the uploaded data with the NB upload certificate before they are provided to other Member States.

3.4. *Requirements on the technical DCCG architecture*

The requirements on the technical DCCG architecture are as follows:

— The DCCG uses mutual TLS authentication to establish an authenticated encrypted connection with the NBs. Therefore, the DCCG maintains a whitelist of registered NB_{TLS} client certificates;

— The DCCG uses two digital certificates ($DCCG_{TLS}$ and $DCCG_{TA}$) with two distinct key pairs. The private key of the $DCCG_{TA}$ key pair is maintained offline (not on the online components of the DCCG);

— The DCCG maintains a trust list of the NB_{CSCA} certificates that is signed with the $DCCG_{TA}$ private key;

— The ciphers used must meet the requirements from *Section 5.1*.

4. Certificate Lifecycle Management

4.1. *Registration of National Backends*

Member States must register with the DCCG operator to take part in the DCCG system. This section describes the technical and operational procedure that must be followed to register a national backend.

The DCCG operator and the Member State must exchange information on technical contact persons for the onboarding process. It is assumed that the technical contact persons are legitimated by their Member States and identification/authentication is performed over other channels. For example, the authentication can be achieved when a Member State's technical contact provides the certificates as password-encrypted files via email and shares the corresponding password with the DCCG operator via telephone. Also other secure channels defined by the DCCG operator may be used.

The Member State must provide three digital certificates during the registration and identification process:

— The Member State's TLS certificate NB_{TLS}

— The Member State's upload certificate NB_{UP}

— The Member State's CSCA certificate(s) NB_{CSCA}

All provided certificates must adhere to the requirements defined in *Section 5*. The DCCG operator will verify that the provided certificate adheres to the requirements of *Section 5*. After the identification and registration, the DCCG operator:

— adds the NB_{CSCA} certificate(s) to the trust list signed with the private key that corresponds to the $DCCG_{TA}$ public key;

— adds the NB_{TLS} certificate to the whitelist of the DCCG TLS endpoint;

— adds the NB_{UP} certificate to the DCCG system;

— provides the $DCCG_{TA}$ and $DCCG_{TLS}$ public key certificate to the Member State.

4.2. *Certificate authorities, validity periods and renewal*

In case that a Member State wants to operate its own CSCA, the CSCA certificates may be self-signed certificates. They act as the trust anchor of the Member State and therefore the Member State must strongly protect the private key corresponding to the CSCA certificate's public key. It is recommended that the Member States use an offline system for their CSCA, i.e. a computer system that is not connected to any network. Multi person control shall be used to access the system (for example, following the four eyes principle). After signing DSCs, operational controls shall be applied and the system that holds the private CSCA key shall be stored safely with strong access controls. Hardware Security Modules or Smart Cards can be used to further protect the CSCA private key. Digital certificates contain a validity period that enforces certificate renewal. Renewal is necessary to use fresh cryptographic keys and to adapt the key sizes when new improvements in computation or new attacks threaten the security of the cryptographic algorithm that is used. The shell model applies (see *Section 3.2*).

The following validity periods are recommended, given the one-year validity for digital COVID certificates:

— CSCA: 4 years

— DSC: 2 years

— Upload: 1-2 years

— TLS Client authentication: 1-2 years

For a timely renewal, the following usage periods for the private keys are recommended:

— CSCA: 1 year

— DSC: 6 months

Member States must create new upload certificates and TLS certificates timely, for example, one month, before expiration in order to allow smooth operation. CSCA certificates and DSCs should be renewed at least one month before the private key usage ends (considering the necessary operational procedures). Member States must provide updated CSCA certificates, upload and TLS certificates to the DCCG operator. Expired certificates shall be removed from the whitelist and trust list.

Member States and the DCCG operator must keep track of the validity of their own certificates. There is no central entity that keeps record of the certificate validity and informs the participants.

4.3. *Revocation of certificates*

In general, digital certificates can be revoked by their issuing CA using certificate revocation lists or Online Certificate Status Protocol Responder (OCSP). CSCAs for the DCC system should provide certificate revocation lists (CRLs). Even if these CRLs are currently not used by other Member States, they should be integrated for future applications. In case a CSCA decides not to provide CRLs, the DSCs of this CSCA must be renewed when CRLs become mandatory. Verifiers should not use OCSP for validation of the DSCs and should use CRLs. It is recommended that the national backend performs necessary validation of DSCs downloaded from the DCC Gateway and only forwards a set of trusted and validated DSC to national DCC validators. DCC validators should not perform any revocation checking on DSC in their validation process. One reason for this is to protect the privacy of DCC holders by avoiding any chance that the use of any particular DSC can be monitored by its associated OCSP responder.

Member States can remove their DSCs from the DCCG on their own using valid upload and TLS certificates. Removing a DSC means that all DCCs issued with this DSC will become invalid when Member States fetch the updated DSC lists. The protection of private key material corresponding to DSCs is crucial. Member States must inform the DCCG operator when they must revoke upload or TLS certificates, for example due to compromise of the national backend. The DCCG operator can then remove the trust for the affected certificate, for example by removing it from the TLS whitelist. The DCCG operator can remove the upload certificates from the DCCG database. Packages signed with the private key corresponding to this upload certificate will become invalid when national backends remove the trust of the revoked upload certificate. In case that a CSCA certificate must be revoked, Member States shall inform the DCCG operator as well as other Member States that they have trust relationships with. The DCCG operator will issue a new trust list where the affected certificate is not contained anymore. All DSCs issued by this CSCA will become invalid when Member States update their national backend trust store. In case that the $\mathrm{DCCG}_{\mathrm{TLS}}$ certificate or the $\mathrm{DCCG}_{\mathrm{TA}}$ certificate must be revoked, the DCCG operator and the Member States must work together to establish a new trusted TLS connection and trust list.

5. **Certificate Templates**

This section sets out cryptographic requirements and guidance as well as requirements on certificate templates. For the DCCG certificates, this section defines the certificate templates.

5.1. *Cryptographic requirements*

Cryptographic algorithms and TLS cipher suites shall be chosen based on the current recommendation from the German Federal Office for Information Security (BSI) or SOG-IS. These recommendations and the recommendations of other institutions and standardization organization are similar. The recommendations can be found in the technical guidelines TR 02102-1 and TR 02102-2 [1] or SOG-IS Agreed Cryptographic Mechanisms [2].

5.1.1. Requirements on the DSC

The requirements provided for in *Annex I, Section 3.2.2* shall apply. Hence, it is strongly recommended that Document Signers use the Elliptic Curve Digital Signature Algorithm (ECDSA) with NIST-p-256 (as defined in appendix D of FIPS PUB 186-4). Other elliptic curves are not supported. Due to the space restrictions of the DCC,

[1] BSI - Technical Guidelines TR-02102 (bund.de)

[2] SOG-IS - Supporting documents (sogis.eu)

Member States should not use RSA-PSS, even if it is allowed as a fall back algorithm. In case that Member States use RSA-PSS, they should use a modulus size of 2048 or max. 3072 bit. SHA-2 with an output length of ≥ 256 bits shall be used as cryptographic hash function (see ISO/IEC 10118-3:2004) for the DSC signature.

5.1.2. Requirements on TLS, Upload and CSCA certificates

For digital certificates and cryptographic signatures in the DCCG context, the major requirements on cryptographic algorithms and key length are summarized in the following table (as of 2021):

Signature Algorithm	Key size	Hash function
EC-DSA	Min. 250 Bit	SHA-2 with an output length ≥ 256 Bit
RSA-PSS (recommended padding) RSA-PKCS#1 v1.5 (legacy padding)	Min. 3000 Bit RSA Modulus (N) with a public exponent e > 2^16	SHA-2 with an output length ≥ 256 Bit
DSA	Min. 3000 Bit prime p, 250 Bit key q	SHA-2 with an output length ≥ 256 Bit

The recommended elliptic curve for EC-DSA is NIST-p-256 due to its widespread implementation.

5.2. *CSCA certificate (NB$_{CSCA}$)*

The following table gives guidance on the NB$_{CSCA}$ certificate template if a Member State decides to operate its own CSCA for the DCC system.

Bold entries are required (must be included in the certificate), *italic* entries are recommended (should be included). For absent fields, no recommendations are defined.

Field	Value
Subject	**cn=<non-empty and unique common name>,** *o=<Provider>,* **c=<Member State operating the CSCA>**
Key usage	**certificate signing,** *CRL signing* (at minimum)
Basic Constraints	**CA = true, path length constraints = 0**

The subject name must be non-empty and unique within the specified Member State. The country code (c) must match the Member State that will use this CSCA certificate. The certificate must contain a unique subject key identifier (SKI) according to RFC 5280 [3].

5.3. *Document Signer Certificate (DSC)*

The following table provides guidance on the DSC. **Bold** entries are required (must be included in the certificate), *italic* entries are recommended (should be included). For absent fields, no recommendations are defined.

Field	Value
Serial Number	**unique serial number**
Subject	**cn=<non-empty and unique common name>**, *o=<Provider>,* **c=<Member State that uses this DSC>**
Key Usage	**digital signature** (at minimum)

[3] rfc5280 (ietf.org)

The DSC must be signed with the private key corresponding to a CSCA certificate that is used by the Member State.

The following extensions are to be used:

— The certificate must contain a Authority Key Identifier (AKI) matching the Subject Key Identifier (SKI) of the issuing CSCA certificate

— The certificate should contain a unique Subject Key Identifier (in accordance to RFC 5280 [4])

In addition, the certificate should contain the CRL distribution point extension pointing to the certificate revocation list (CRL) that is provided by the CSCA that issued the DSC.

The DSC may contain an extended key usage extension with zero or more key usage policy identifiers that constrain the types of HCERTs this certificate is allowed to verify. If one or more are present, the verifiers shall verify the key usage against the stored HCERT. The following extendedKeyUsage values are defined for this:

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 Vaccination Issuers
extendedKeyUsage	1.3.6.1.4.1.1847.2021.1.3 for Recovery Issuers

In absence of any key usage extension (i.e. no extensions or zero extensions), this certificate can be used to validate any type of HCERT. Other documents may define relevant additional extended key usage policy identifiers used with validation of HCERTs.

5.4. *Upload Certificates (NBUP)*

The following table provides guidance for the national backend upload certificate. **Bold** entries are required (must be included in the certificate), *italic* entries are recommended (should be included). For absent fields, no recommendations are defined.

Field	Value
Subject	**cn=<non-empty and unique common name>**, *o=<Provider>*, **c=<Member State that uses this upload certificate>**
Key Usage	**digital signature** (at minimum)

5.5. *National Backend TLS Client Authentication (NB$_{TLS}$)*

The following table provides guidance for the national backend TLS client authentication certificate. **Bold** entries are required (must be included in the certificate), *italic* entries are recommended (should be included). For absent fields, no recommendations are defined.

Field	Value
Subject	**cn=<non-empty and unique common name>**, *o=<Provider>*, **c=<Member State on the NB>**
Key Usage	**digital signature** (at minimum)
Extended key usage	**client authentication (1.3.6.1.5.5.7.3.2**)

[4] rfc5280 (ietf.org)

The certificate may also contain the extended key usage *server authentication (1.3.6.1.5.5.7.3.1)*, but it is not required.

5.6. *Trust list signature certificate (DCCG$_{TA}$)*

The following table defines the DCCG Trust Anchor certificate.

Field	Value
Subject	**cn = Digital Green Certificate Gateway** [5]**, o=<Provider>, c=<country>**
Key Usage	**digital signature** (at minimum)

5.7. *DCCG TLS Server certificates (DCCG$_{TLS}$)*

The following table defines the DCCG TLS certificate.

Field	Value
Subject	**cn=<FQDN or IP address of the DCCG>, o=<Provider>, c= <country>**
SubjectAltName	**dNSName: <DCCG DNS name> or iPAddress: <DCCG IP address>**
Key Usage	**digital signature** (at minimum)
Extended Key usage	**server authentication (1.3.6.1.5.5.7.3.1**)

The certificate may also contain the extended key usage *client authentication (1.3.6.1.5.5.7.3.2)*, but it is not required.

The TLS certificate of the DCCG shall be issued by a publicly trusted certificate authority (included in all major browsers and operating systems, following the CAB Forum baseline requirements).

[5] The terminology of 'Digital Green Certificate' instead of 'EU Digital COVID Certificate' has been maintained in this context because this is the terminology which has been hardcoded and deployed in the certificate before the co-legislators decided on a new terminology.