This text is meant purely as a documentation tool and has no legal effect. The Union's institutions do not assume any liability for its contents. The authentic versions of the relevant acts, including their preambles, are those published in the Official Journal of the European Union and available in EUR-Lex. Those official texts are directly accessible through the links embedded in this document

►B

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)

(OJ L 230, 30.6.2021, p. 32)

Amended by:

		Official Journal		
		No	page	date
►M1	Commission Implementing Decision (EU) 2021/2014 of 17 November 2021	L 410	180	18.11.2021
►M2	Commission Implementing Decision (EU) 2021/2301 of 21 December 2021	L 458	536	22.12.2021
►M3	Commission Implementing Decision (EU) 2022/483 of 21 March 2022	L 98	84	25.3.2022
►M4	Commission Implementing Decision (EU) 2022/1516 of 8 September 2022	L 235	61	12.9.2022

▼B

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)

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.

▼M1

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.

Article 5

A common coordinated data structure for the data to be included in certificates referred to in Article 3(1) of Regulation (EU) 2021/953, using a JavaScript Object Notation (JSON) schema, is set out in Annex V to this Decision.

▼M3

Article 5a

Exchange of certificate revocation lists

1. The EU Digital COVID Certificate trust framework shall enable the exchange of certificate revocation lists via the central EU Digital COVID Certificate gateway (the ‘gateway’) in accordance with the technical specifications in Annex I.

2. Where Member States revoke EU Digital COVID Certificates they may submit certificate revocation lists to the gateway.

▼M3

3. Where Member States submit certificate revocation lists, the issuing authorities shall keep a list of revoked certificates.

4. Where personal data is exchanged via the gateway, the processing shall be limited to the purpose of supporting the exchange of revocation information. Such personal data shall only be used for the purpose of verifying the revocation status of EU Digital COVID Certificates issued within the scope of Regulation (EU) 2021/953.

5. The information submitted to the gateway shall comprise the following data in accordance with the technical specifications in Annex I:

(a) the pseudonymised unique certificate identifiers of revoked certificates,

(b) an expiry date for the submitted certificate revocation list;

6. Where an issuing authority revokes EU Digital COVID Certificates it has issued pursuant to Regulation (EU) 2021/953 or Regulation (EU) 2021/954 and intends to exchange relevant information through the gateway, it shall transmit the information referred to in paragraph 5 in the form of certificate revocation lists to the gateway in a secure format in accordance with the technical specifications in Annex I.

7. Issuing authorities shall, to the extent possible, provide a solution to inform the holders of revoked certificates about the revocation status of their certificates and the reason for the revocation at the time of revocation.

8. The gateway shall collect the certificate revocation lists received It shall provide tools for distributing the lists to the Member States. It shall automatically delete lists in accordance with the expiry dates indicated for each submitted list by the submitting authority.

9. The designated national authorities or official bodies of the Member States processing personal data in the gateway shall be joint controllers of the data processed. The respective responsibilities of the joint controllers shall be allocated in accordance with Annex VI.

10. The Commission shall be the processor of personal data processed within the gateway. In its capacity as processor on behalf of the Member States, the Commission shall ensure the security of the transmission and of the hosting of personal data within the gateway and shall comply with the obligations of the processor laid down in Annex VII.

11. The effectiveness of the technical and organisational measures for ensuring the security of processing of personal data within the gateway shall be regularly tested, assessed and evaluated by the Commission and by the joint controllers.

▼M3

Article 5b

Submission of certificate revocation lists by third countries

Third countries issuing COVID-19 certificates in respect of which the Commission has adopted an implementing act pursuant to Article 3(10) or Article 8(2) of Regulation (EU) 2021/953 may submit lists of revoked COVID-19 certificates covered by such an implementing act to be processed by the Commission on behalf of the joint controllers in the gateway referred to in Article 5a, in accordance with the technical specifications set out in Annex I.

Article 5c

Governance of the processing of personal data in the central EU Digital COVID Certificate gateway

1. The decision-making process of the joint controllers shall be governed by a working group established under the Committee referred to in Article 14 of Regulation (EU) 2021/953.

2. The designated national authorities or official bodies of the Member States processing personal data in the gateway as joint controllers shall designate representatives to that group.

▼M1

Article 6

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

▼B

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

▼B

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

([1]) rfc8392 (ietf.org)
([2]) rfc8152 (ietf.org)

▼B

— 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

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 ([1])) 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.

([1]) rfc8230 (ietf.org)

▼B

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 ([1]), 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.

3.2.6. Issued At

The Issued At (iat) claim shall hold a timestamp in the integer NumericDate format (as specified in RFC 8392 ([2]), 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 ([3])) 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 ([4])). Application developers may not actually ever decode, or encode to and from the JSON format, but use the in-memory structure.

([1]) rfc8392 (ietf.org)
([2]) rfc8392 (ietf.org)
([3]) rfc7159 (ietf.org)
([4]) rfc7049 (ietf.org)

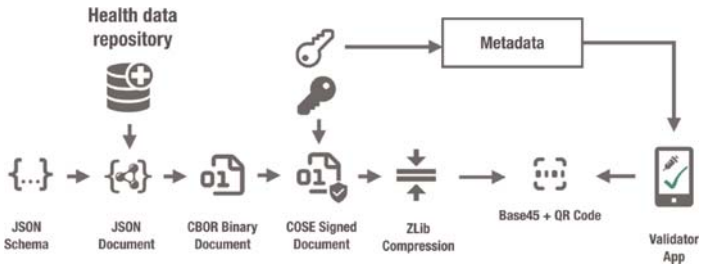
▼B

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 ([1]). The data content is limited to the defined data elements in the minimum data set specified in the Annex to Regulation 2021/953.

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.

([1]) 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.

▼B

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 ([1])) and the Deflate compression mechanism in the format defined in RFC 1951 ([2]).

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.

([1]) rfc1950 (ietf.org)
([2]) rfc1951 (ietf.org)

▼B

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.

▼B

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 ([1]), 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.

([1]) rfc7517 (ietf.org)

▼B

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.

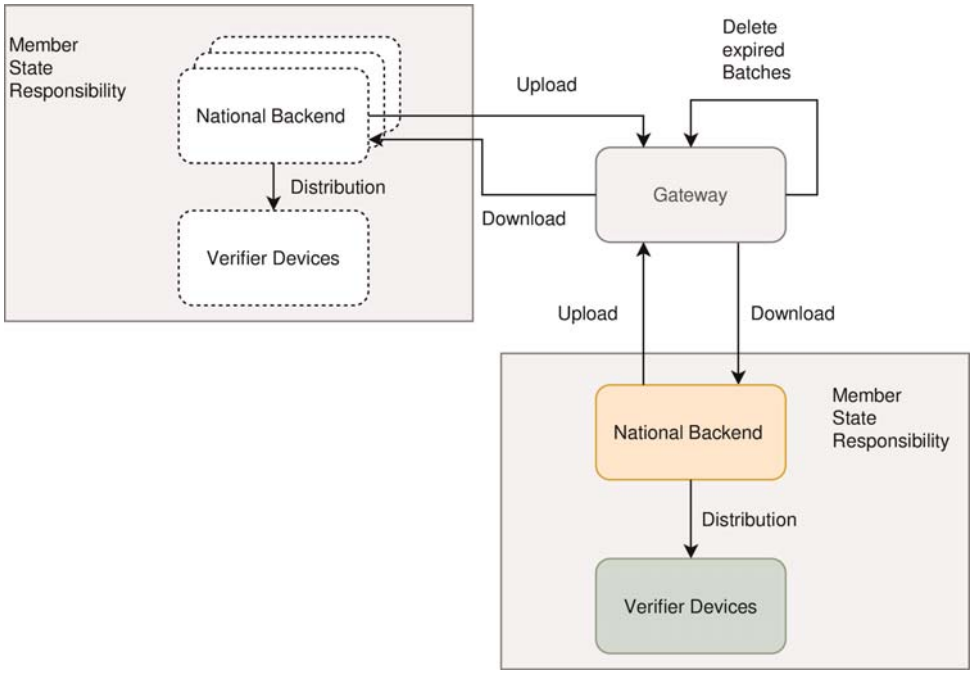
— Member States may choose to never do any verification of published revocations; but instead purely rely on the DSC lists they get daily from the Secretariat or compile themselves.

▼M3

9. **Revocation solution**

9.1. *DCC Revocation List (DRL) Provision*

The Gateway shall provide endpoints and functionality to hold and manage the revocation lists:



▼M3

9.2. *Trust Model*

All connections are established by the standard DCCG trust model by the NB_{TLS} and NB_{UP} certificates (see certificate governance). All information is packed and uploaded by CMS messages to ensure the integrity.

9.3. *Batch Construction*

9.3.1. Batch

Each revocation list shall contain one or multiple entries and shall be packed in batches which contain a set of hashes and their metadata. A batch is immutable and defines an expiration date which indicates when the batch can be deleted. The expiration date of all items in the batch must be exactly the same – meaning that batches must be grouped by expiry date and by signing DSC. Each batch shall contain a maximum of 1 000 entries. If the revocation list consists of more than 1 000 entries, multiple batches shall be created. Any entry may occur in at most one batch. The batch shall be packaged into a CMS structure and signed by the NB_{up} certificate of the uploading country.

9.3.2. Batch Index

When a batch is created it shall be assigned a unique ID by the gateway and shall be automatically added to the index. The index of batches is ordered by the modified date, in ascending chronological order.

9.3.3. Gateway Behaviour

The gateway processes revocation batches without any changes: it can neither update nor remove, nor add any information to the batches. The batches are forwarded to all authorised countries (see chapter 9.6).

The gateway actively observes the expiration dates of batches and removes the expired batches. After the batch is deleted, the gateway returns an "HTTP 410 Gone" response for the deleted batch URL. Therefore, the batch appears in the batch index as "deleted".

9.4. *Hash Types*

The revocation list contains hashes that can represent different revocation types/attributes. These types or attributes shall be indicated in the provisioning of the revocation lists. The current types are:

Type	Attribute	Hash Calculation
SIGNATURE	DCC Signature	SHA256 of DCC Signature
UCI	UCI (Unique Certificate Identifier)	SHA256 of UCI
COUNTRYCODEUCI	Issuing Country Code + UCI	SHA256 of Issuing CountryCode + UCI

Just the first 128 bits of the hashes encoded as base64 strings are put into the batches and used to identify the revoked DCC ([1]).

([1]) Please also consider 9.5.1.2 for the detailed API descriptions.

▼M3

9.4.1. Hash type: SHA256(DCC Signature)

In this case the hash is calculated over the bytes of the COSE_SIGN1 signature from the CWT. For RSA signatures, the entire signature will be used as input. The formula for the EC-DSA signed certificates is using the r value as an input:

SHA256(r)

[required for all new implementations]

9.4.2. Hash type: SHA256(UCI)

In this case the hash is calculated over the UCI string encoded in UTF-8 and converted to a byte array.

[deprecated ([1]), but supported for backwards compatibility]

9.4.3. Hash type: SHA256(Issuing CountryCode+UCI)

In this case CountryCode encoded as a UTF-8 string concatenated with the UCI encoded with a UTF-8 string. This is then converted to a byte array and used as input to the hash function.

[deprecated[2], but supported for backwards compatibility]

9.5. *API Structure*

9.5.1. Revocation Entry Provisioning API

9.5.1.1. Purpose

The API delivers the revocation list entries in batches including a batch index.

9.5.1.2. Endpoints

9.5.1.2.1. Batch List Download Endpoint

The endpoints follow a simple design, returning a list of batches with a small wrapper providing metadata. The batches are sorted by *date* in *ascending (chronological)* order:

/revocation-list

Verb: GET

Content-Type: application/json

Response: JSON Array

```
{
    'more': true|false,
    'batches':
            [{
                'batchId': '{uuid}',
                'country': 'XY',
                'date': '2021-11-01T00:00:00Z'
                'deleted': true | false
            }, ..
            ]
}
```

([1]) Deprecated means that this feature shall not be considered for new implementations but shall be supported for existing implementations for a well-defined period of time.

▼M3

Note: The result is limited by default to 1 000. If the flag ‘more’ is set to true, the response indicates that more batches are available for download. To download more items the client must set the If-Modified-Since header to a date no earlier than the last entry received.

The response contains a JSON array with the following structure:

Field	Definition
more	Boolean Flag which indicates that there are more batches.
batches	Array with the existing batches.
batchId	https://en.wikipedia.org/wiki/Universally_unique_identifier
country	Country Code ISO 3166
date	ISO 8601 Date UTC. Date when the batch was added or deleted.
deleted	boolean. True if deleted. When the deleted flag is set, the entry can be finally removed from the query results after 7 days.

9.5.1.2.1.1. Response *Codes*

Code	Description
200	All ok.
204	No content, if ‘If-Modified-Since’ Header content has no match.

Request Header

Header	Mandatory	Description
If-Modified-Since	Yes	This header contains the last downloaded date to get just the newest results. On the initial call the header should be the set to the ‘2021-06-01T00:00:00Z’

9.5.1.2.2. Batch Download Endpoint

The batches contain a list of certificate identifiers:

/revocation-list/{batchId}

Verb: GET

Accepts: application/cms

Response:CMS with Content

{

‘country’: ‘XY’,

‘expires’: ‘2022-11-01T00:00:00Z’,

▼M3

‘kid’:’23S+33f=’,

‘hashType’:’SIGNATURE’,

‘entries’:[{

‘hash’:’e2e2e2e2e2e2e2e2’

}, ..]

}

The response contains a CMS including a signature which must match to the NB_{UP} certificate of the country. All items in the JSON array contain the following structure:

Field	Mandatory	Type	Definition
expires	Yes	String	Date when the item can be removed. ISO8601 Date/Time UTC
country	Yes	String	Country Code ISO 3166
hashType	Yes	String	Hash Type of the provided entries (see Hash Types)
entries	Yes	JSON Object Array	See Table Entries
kid	Yes	String	base64 encoded KID of the DSC used to sign the DCC. If the KID is not known then the string `UNKNOWN_KID` (excluding the `) can be used.

Notes:

— Batches shall be grouped by expiry date and DSC – all items shall expire at the same time and have been signed by the same key.

— Expiry time is a date/time in UTC because EU-DCC is a global system and we must use an unambiguous time.

— The expiry date of a permanently revoked DCC shall be set at the expiry date of the corresponding DSC used to sign the DCC or at the Expiration Time of the revoked DCC (in which case the used NumericDate/epoch times shall be treated as being in the UTC time zone).

— National Backend (NB) shall remove items from their revocation list when the **expiration** date is reached.

— NB may remove items from their revocation list in the case that the **kid** used to sign the DCC is revoked.

▼**M3**

9.5.1.2.2.1. Entries

Field	Mandat-ory	Type	Definition
hash	Yes	String	First 128 bits of the SHA256 hash encoded as a base64 string

Note: The entries object contains currently just a hash, but to be compatible with changes in the future an object was chosen, instead of a json array.

9.5.1.2.2.2. Response Codes

Code	Description
200	All ok.
410	Batch gone. Batch can be deleted in the national backend.

9.5.1.2.2.3. Response Headers

Header	Description
ETag	Batch ID.

9.5.1.2.3. Batch Upload Endpoint

The upload is done over the same endpoint via POST Verb:

/revocation-list

Verb: POST

Accepts: application/cms

Request: CMS with Content

ContentType: application/cms

Content:

```
{
    'country': 'XY',
    'expires': '2022-11-01T00:00:00Z',
    'kid':'23S+33f=',
    'hashType':'SIGNATURE',
    'entries':[{
        'hash':'e2e2e2e2e2e2e2e2'
        }, ..]
}
```

The batch shall be signed using the NB_{UP} certificate. The Gateway shall verify that the signature was set by the NB_{UP} for the given *country*. If the signature check fails then the upload shall fail.

NOTE: Every batch is immutable and can't be changed after uploading. It can be deleted, though. The ID of every deleted batch is stored, and an upload of a new batch with the same ID is rejected.

▼M3

9.5.1.2.4. Batch Delete Endpoint

A batch can be deleted over the same endpoint via DELETE Verb:

/revocation-list

Verb: DELETE

Accepts: application/cms

ContentType: application/cms

Request: CMS with Content

Content:

{

‘batchId’: ‘...’

}

or, for compatibility reasons, to the following endpoint with the POST verb:

/revocation-list/delete

Verb: POST

Accepts: application/cms

ContentType: application/cms

Request: CMS with Content

Content:

{

‘batchId’: ‘...’

}

9.6. *API Protection/GDPR*

This section specifies measures for the implementation to comply with the provisions of the Regulation 2021/953 as regards to the processing of personal data.

9.6.1. Existing Authentication

The Gateway currently uses the NB_{TLS} certificate to authenticate the countries connecting to the Gateway. This authentication can be used to determine the identity of the country connected to Gateway. That identity can then be used to implement access control.

9.6.2. Access Control

To be able to lawfully process personal data the Gateway shall implement an access control mechanism.

The gateway implements an Access Control List combined with Role Based Security. In that scheme, two tables shall be maintained – one table describing which Roles can apply which Operations to which Resources, the other table describing which Roles are assigned to which Users.

To implement the controls required by this document, three Roles are required, and that is:

RevocationListReader

RevocationUploader

RevocationDeleter

▼**M3**

The following endpoints shall check to see if the User has the Role RevocationListReader; if they do then access shall be granted, if they do not then an HTTP 403 Forbidden shall be returned:

GET/revocation-list/

GET/revocation-list/{batchId}

The following endpoints shall check to see if the User has the Role RevocationUploader; if they do then access shall be granted, if they do not then an HTTP 403 Forbidden shall be returned:

POST/revocation-list

The following endpoints shall check to see if the User has the Role RevocationDeleter; if they do then access shall be granted, if they do not then an HTTP 403 Forbidden shall be returned:

DELETE/revocation-list

POST/revocation-list/delete

The Gateway shall also provide a reliable method whereby the administrators can manage the Roles that are linked to the Users in such a way as to reduce the chance of human errors whilst also not burdening the functional administrators.

▼M1

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 EU Digital COVID Certificate. 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 is described in Annex V.

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 shall 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 shall map such codes to the described value sets. Member States are responsible for any such mappings.

►M4 As some value sets based on the coding systems provided for in this Annex, such as those for vaccine and antigen test coding, are changing often, they shall be published and 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 shall 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)**

   To be used in certificate 1, 2 and 3.

   The following code shall be used:

Code	Display	Code System name	Code System URL	Code System OID	Code System version
840539006	COVID-19	SNOMED CT	http://snomed.info/sct	2.16.840.1.113883.6.96	2021-01-31

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

   Preferred Code System: SNOMED CT or ATC Classification.

   To be used in certificate 1.

   Examples of codes that shall 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).

   A value set setting out the codes to be used pursuant to the code systems established in this section shall be published and regularly updated by the Commission with the support of the eHealth Network. The value set shall be extended when new vaccine types are developed and put into use.

▼M1

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 shall be replaced by a hyphen (-).

Name of the Value Set: Vaccine.

To be used in certificate 1.

An example of a code that shall 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).

A value set setting out the codes to be used pursuant to the code systems established in this section shall be published and regularly updated by the Commission with the support of the eHealth Network.

Vaccines shall be coded using an existing code in the published value set, even if their names are different in different countries. The reason is that there is no global vaccine registry covering all vaccines in current use yet. Example:

— For the vaccine 'COVID-19 Vaccine Moderna Intramuscular Injection', which is the name of the Spikevax vaccine in Japan, use code EU/1/20/1507, as it is the name of this vaccine in the EU.

If this is not possible or advisable in a specific case, a separate code will be provided in the published value set.

▼M4

If a country using the EU Digital COVID Certificate ('EU DCC') decides to issue vaccination certificates to clinical trial participants during ongoing clinical trials, the vaccine medicinal product shall be coded following the pattern

CT_*clinical-trial-identifier*

Where the clinical trial has been registered in the EU Clinical Trials Register (EU-CTR), the clinical trial identifier from this register shall be used. In other cases, identifiers from other registers (such as clinicaltrials.gov or Australian New Zealand Clinical Trials Registry) may be used.

The clinical trial identifier shall include a prefix allowing the identification of the clinical trial register (such as EUCTR for EU Clinical Trials Register, NCT for clinicaltrials.gov, ACTRN for Australian New Zealand Clinical Trials Registry).

Where the Commission has received guidance from the Health Security Committee, the European Centre for Disease Prevention and Control (ECDC) or the European Medicines Agency (EMA) with regard to the acceptance of certificates issued for a COVID-19 vaccine undergoing clinical trials, the guidance shall be published either as part of the value sets document or separately.

▼M1

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 shall be replaced by a hyphen (-).

To be used in certificate 1.

An example of a code that shall 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).

A value set setting out the codes to be used pursuant to the code systems established in this section shall be published and regularly updated by the Commission with the support of the eHealth Network.

Different branches of the same Marketing Authorisation Holder or the same manufacturer shall use an existing code in the published value set.

As a general rule, for the same vaccine product, the code referring to its marketing authorisation holder in the EU shall be used, as there is no internationally agreed vaccine manufacturer or marketing authorisation holder registry yet. Examples:

— For the organisation ‘Pfizer AG’, which is an MAH for vaccine ‘Comirnaty’ used in Switzerland, use code ORG-100030215 referring to BioNTech Manufacturing GmbH, as it is the MAH of Comirnaty in the EU.

— For the organisation ‘Zuellig Pharma’, which is an MAH for vaccine Covid-19 Vaccine Moderna (Spikevax) used in the Philippines, use code ORG-100031184 referring to Moderna Biotech Spain S.L., as it is the MAH of Spikevax in the EU.

If this is not possible or advisable in a specific case, a separate code will be provided in the published value set.

▼M4

If a country using EU DCC decides to issue vaccination certificates to clinical trial participants during ongoing clinical trials, the vaccine marketing authorization holder or manufacturer shall be coded using the value designated to it in the value set, if available. In other cases, the vaccine marketing authorization holder or manufacturer shall be coded using the rule described under Section 3 Vaccine medicinal product (CT_*clinical-trial-identifier*).

▼M1

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 in a series of vaccine doses of a COVID-19 vaccine (N);

(2) Overall number of doses in the vaccination series (C).

5.1. *Primary vaccination series*

Where the person is receiving doses of the primary vaccination series, that is, the vaccination series intended to provide sufficient protection at an initial stage, (C) shall reflect the overall number of doses of the standard primary vaccination series (e.g. 1 or 2, depending on the type of vaccine administered). This includes the option of using a shorter series (C=1) where the vaccination protocol applied by a Member State provides for the administration of a single dose of a 2-dose vaccine to persons having previously been infected with SARS-CoV-2. A completed primary vaccination series shall thus be indicated by N/C = 1. For example:

— 1/1 would indicate the completion of a primary single-dose vaccination course, or the completion of a primary course consisting of one dose of a 2-dose vaccine administered to a recovered person in line with the vaccination protocol applied by a Member State;

— 2/2 would indicate the completion of a primary 2-dose vaccination series.

Where the primary vaccination series is extended, for example for persons with severely weakened immune systems or where the recommended interval between primary doses has not been respected, any such doses shall be encoded as additional doses falling under Section 5.2.

▼M2

5.2. *Booster doses*

Where the person is receiving doses following the primary vaccination series, such booster doses shall be reflected in the corresponding certificates as follows:

— 2/1 indicates the administration of a booster dose following a primary single-dose vaccination course, or the administration of a booster dose following the completion of a primary course consisting of one dose of a 2-dose vaccine administered to a recovered person in line with the vaccination protocol applied by a Member State. After that, doses (X) administered following the first booster dose shall be indicated by (2+X)/(1) > 1 (3/1, for example),

— 3/3 indicates the administration of a booster dose following a primary 2-dose vaccination series. After that, doses (X) administered following the first booster dose shall be indicated by (3+X)/(3+X) = 1 (4/4, for example).

Member States shall implement the encoding rules set out in this Section by 1 February 2022.

Member States shall, automatically or upon request by the persons concerned, re-issue certificates in which the administration of a booster dose following a primary single-dose vaccination course is encoded in such a way that it cannot be distinguished from the completion of the primary vaccination series.

▼M2

For the purposes of this Annex, references to 'booster doses' should be understood as also covering additional doses administered to better protect individuals who mount inadequate immune responses following the completion of the standard primary vaccination series. Within the legal framework established by Regulation (EU) 2021/953, Member States may take measures to address the situation of vulnerable groups who may receive additional doses as a matter of priority. For example, if a Member State decides to administer additional doses only to specific sub-groups of the population, it can choose, in accordance with Article 5(1) of Regulation (EU) 2021/953, to issue vaccination certificates indicating the administration of such additional doses only upon request and not automatically. Where such measures are taken, Member States shall inform the persons concerned accordingly, as well as that they may continue to make use of the certificate received following the completion of the standard primary vaccination series.

▼M1

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). If the vaccination or test was performed by an international organisation (such as UNHCR or WHO) and no information about the country is available, a code for the organisation shall be used. Such additional codes shall be published and regularly updated by the Commission with the support of the eHealth Network.

7. **The type of test**

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 following codes shall be used.

Code	Display	Code System name	Code System URL	Code System OID	Code System version
LP6464-4	Nucleic acid amplification with probe detection	LOINC	http://loinc.org	2.16.840.1.113883.6.1	2.69
LP217198-3	Rapid immunoassay	LOINC	http://loinc.org	2.16.840.1.113883.6.1	2.69

▼M4

The code LP217198-3 (Rapid immunoassay) shall be used to indicate both rapid antigen tests and laboratory-based antigenic assays.

▼M1

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

To be used in certificate 2.

▼M4

The content of the value set shall include the selection of antigen test as listed in the common and updated list of COVID-19 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

▼M1

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**

To be used in certificate 2.

The following codes shall be used:

Code	Display	Code System name	Code System URL	Code System OID	Code System version
260415000	Not detected	SNOMED CT	http://snomed.info/sct	2.16.840.1.113883.6.96	2021-01-31
260373001	Detected	SNOMED CT	http://snomed.info/sct	2.16.840.1.113883.6.96	2021-01-31'

▼B

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.

▼M1

3. **General requirements**

The following overarching requirements shall 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]), namely {'/','#',':'};

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

(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;

([1]) rfc3986 (ietf.org)

([2]) 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.

▼M1

(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 may 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 shall 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 shall be the ISO-7812-1 (LUHN-10) ([1]) summary of the entire UCI in digital/wire transport format. The checksum is separated from the rest of the UCI by a '#' character.

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

▼B

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

The eHealth Network guidelines for verifiable vaccination certificates and basic interoperability elements ([2]) 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.

([1]) 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).

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

▼B

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

▼B

Term	Definition
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
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.

▼B

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.

▼B

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.

▼B

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.

▼B

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.

▼B

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 $DCCG_{TLS}$ certificate or the $DCCG_{TA}$ 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]).

([1]) BSI - Technical Guidelines TR-02102 (bund.de)
([2]) SOG-IS - Supporting documents (sogis.eu)

▼B

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, 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 ([1]).

([1]) rfc5280 (ietf.org)

▼B

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)

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 ([1]))

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.

([1]) rfc5280 (ietf.org)

▼B

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**)

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** [1], **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**)

[1] 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.

▼B

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).

▼M1

ANNEX V

JAVASCRIPT OBJECT NOTATION (JSON) SCHEMA

1. **Introduction**

This Annex establishes the technical data structure for EU Digital COVID Certificates (EUDCC), represented as a JSON schema. The document provides specific instructions related to the individual data fields.

2. **JSON Schema location and versions**

The authoritative official JSON schema for EUDCC is made available at https://github.com/ehn-dcc-development/ehn-dcc-schema. Other locations are not authoritative, but may be used for preparing upcoming revisions.

By default, the current version as set out in this Annex and supported by all countries currently in production is shown under the indicated URL.

Upcoming next version, to be supported by a defined date by all countries, is shown under the indicated URL through version tagging, described more specifically in the Readme file.

▼M3

3. **Common structures and general requirements**

An EU Digital COVID Certificate shall not be issued if not all data fields can be correctly populated in accordance with this specification due to missing information. ***This shall not be understood as affecting the obligation of Member States to issue EU Digital COVID Certificates.***

Information in all fields may be provided using the full set of UNICODE 13.0 characters encoded using UTF-8, unless specifically restricted to value sets or narrower sets of characters.

The common structure shall be as follows:

"JSON":{

"ver":<version information>,

"nam":{

<person name information>

},

"dob":<date of birth>,

"v" or "t" or "r":[

{<vaccination dose or test or recovery information, one entry>}

]

}

Detailed information on individual groups and fields is provided in next sections.

Where the rules indicate that a field shall be skipped, this means that its content shall be empty and that neither the name nor the value of the field are allowed in the contents.

▼M3

3.1. *Version*

Version information shall be provided. Versioning is following Semantic Versioning (semver: https://semver.org). In production, it shall be one of the officially released (current or one of the older officially released) versions. See Section JSON Schema location for more details.

Field id	Field name	Instructions
ver	Schema version	Shall match the identifier of the schema version used for producing the EUDCC. Example: "ver":"1.3.0"

3.2. *Person name and date of birth*

Person name is the official full name of the person, matching the name stated on travel documents. The identifier of the structure is *nam*. Exactly 1 (one) person name shall be provided.

Field id	Field name	Instructions
nam/fn	Surname(s)	Surname(s) of the holder. If the holder has no surnames and has a forename, the field shall be skipped. In all other cases, exactly 1 (one) non-empty field shall be provided, with all surnames included in it. In case of multiple surnames, these shall be separated by a space. Combination names including hyphens or similar characters must however stay the same. Examples: "fn":"Musterfrau-Gößinger" "fn":"Musterfrau-Gößinger Müller"
nam/fnt	Standardised surname(s)	Surname(s) of the holder transliterated using the same convention as the one used in the holder's machine readable travel documents (such as the rules defined in ICAO Doc 9303 Part 3). If the holder has no surnames and has a forename, the field shall be skipped. In all other cases, exactly 1 (one) non-empty field shall be provided, only including characters A-Z and <. Maximum length: 80 characters (as per ICAO 9303 specification). Examples: "fnt":"MUSTERFRAU<GOESSINGER" "fnt":"MUSTERFRAU<GOESSINGER<MUELLER"
nam/gn	Forename(s)	Forename(s), such as given name(s), of the holder. If the holder has no forenames and has a surname, the field shall be skipped. In all other cases, exactly 1 (one) non-empty field shall be provided, with all forenames included in it. In case of multiple forenames, these shall be separated by a space. Example: "gn":"Isolde Erika"

▼M3

Field id	Field name	Instructions
nam/gnt	Standardised forename(s)	Forename(s) of the holder transliterated using the same convention as the one used in the holder's machine-readable travel documents (such as the rules defined in ICAO Doc 9303 Part 3). If the holder has no forenames and has a surname, the field shall be skipped. In all other cases, exactly 1 (one) non-empty field shall be provided, only including characters A-Z and <. Maximum length: 80 characters. Example: "gnt":"ISOLDE<ERIKA"
dob	Date of birth	Date of birth of the DCC holder. Complete or partial date without time restricted to the range from 1900-01-01 to 2099-12-31. Exactly 1 (one) non-empty field shall be provided if the complete or partial date of birth is known. If the date of birth is not known even partially, the field shall be set to an empty string "". This should match the information as provided on travel documents. One of the following ISO 8601 formats shall be used if information on date of birth is available. Other options are not supported. YYYY-MM-DD YYYY-MM YYYY (The verifier app may show missing parts of the date of birth using the XX convention as the one used in machine-readable travel documents, e.g. 1990-XX-XX.) Examples: "dob":"1979-04-14" "dob":"1901-08" "dob":"1939" "dob":""

3.3. *Groups for certificate type specific information*

The JSON Schema supports three groups of entries encompassing certificate type specific information. Each EUDCC shall contain exactly 1 (one) group. Empty groups are not allowed.

Group identifier	Group name	Entries
v	Vaccination group	If present, shall contain exactly 1 (one) entry describing exactly 1 (one) vaccination dose (one dose).
t	Test group	If present, shall contain exactly 1 (one) entry describing exactly 1 (one) test result.
r	Recovery group	If present, shall contain exactly 1 (one) entry describing 1 (one) recovery statement.

▼M1

4. **Certificate type specific information**

4.1. *Vaccination certificate*

Vaccination group, if present, shall contain exactly 1 (one) entry describing exactly one vaccination event (one dose). All elements of the vaccination group are mandatory, empty values are not supported.

▼**M1**

Field id	Field name	Instructions
v/tg	Disease or agent targeted: COVID-19 (SARS-CoV or one of its variants)	A coded value from the value set disease-agent-targeted.json. This value set has a single entry 840539006, which is the code for COVID-19 from SNOMED CT (GPS). Exactly 1 (one) non-empty field shall be provided. Example: "tg": "840539006"
v/vp	COVID-19 vaccine or prophylaxis	Type of the vaccine or prophylaxis used. A coded value from the value set vaccine-prophylaxis.json. The value set is distributed from the EUDCC Gateway. Exactly 1 (one) non-empty field shall be provided. Example: "vp": "1119349007"(a SARS-CoV-2 mRNA vaccine)
v/mp	COVID-19 vaccine product	Medicinal product used for this specific dose of vaccination. ►**M4** A coded value from the value set vaccine-medicinal-product.json. Or a coded value referring to a clinical trial and following the rule defined in Section 3 of Annex II. ◄ The value set is distributed from the EUDCC Gateway. Exactly 1 (one) non-empty field shall be provided. Example: "mp": "EU/1/20/1528" (Comirnaty)
v/ma	COVID-19 vaccine marketing authorisation holder or manufacturer	Marketing authorisation holder or manufacturer, if no marketing authorization holder is present. ►**M4** A coded value from the value set vaccine-mah-manf.json. Or a coded value referring to a clinical trial and following the rule defined in Section 4 of Annex II. ◄ The value set is distributed from the EUDCC Gateway. Exactly 1 (one) non-empty field shall be provided. Example: "ma": "ORG-100030215"(Biontech Manufacturing GmbH)
v/dn	Number in a series of doses	Sequence number (positive integer) of the dose given during this vaccination event. 1 for the first dose, 2 for the second dose etc. More specific rules are provided in Section 5 of Annex II. Exactly 1 (one) non-empty field shall be provided. Examples: "dn": "1"(first dose) "dn": "2"(second dose) "dn": "3"(third dose)
v/sd	The overall number of doses in the series	Overall number of doses (positive integer) in the vaccination series. More specific rules are provided in Section 5 of Annex II. Exactly 1 (one) non-empty field shall be provided. Examples: "sd": "1" (in case of a 1-dose primary vaccination course) "sd": "2" (in case of a 2-dose primary vaccination series or for an additional dose following a 1-dose primary vaccination course) "sd": "3" (e.g. in case of additional doses following a 2-dose primary vaccination series)

▼M1

Field id	Field name	Instructions
v/dt	Date of vaccination	The date when the described dose was received, in the format YYYY-MM-DD (full date without time). Other formats are not supported. Exactly 1 (one) non-empty field shall be provided. Example: "dt": "2021-03-28"
v/co	Member State or third country in which the vaccine was administered	Country expressed as a 2-letter ISO3166 code (RECOMMENDED) or a reference to an international organisation responsible for the vaccination event (such as UNHCR or WHO). A coded value from the value set country-2-codes.json. The value set is distributed from the EUDCC Gateway. Exactly 1 (one) field shall be provided. Example: "co": "CZ" "co": "UNHCR"
v/is	Certificate issuer	Name of the organisation that issued the certificate. Identifiers are allowed as part of the name, but not recommended to be used individually without the name as a text. Max 80 UTF-8 characters. Exactly 1 (one) non-empty field shall be provided. Example: "is": "Ministry of Health of the Czech Republic" "is": "Vaccination Centre South District 3"
v/ci	Unique certificate identifier	Unique certificate identifier (UVCI) as specified in the https://ec.europa.eu/health/sites/default/files/ehealth/docs/vaccination-proof_interoperability-guidelines_en.pdf The inclusion of the checksum is optional. The prefix "URN:UVCI:" may be added. Exactly 1 (one) non-empty field shall be provided. Examples: "ci": "URN:UVCI:01:NL:187/37512422923" "ci": "URN:UVCI:01:AT:10807843F94AEE0EE5093FBC254BD813#B"

4.2. *Test certificate*

Test group, if present, shall contain exactly 1 (one) entry describing exactly one test result.

Field id	Field name	Instructions
t/tg	Disease or agent targeted: COVID-19 (SARS-CoV or one of its variants)	A coded value from the value set disease-agent-targeted.json. This value set has a single entry 840539006, which is the code for COVID-19 from SNOMED CT (GPS). Exactly 1 (one) non-empty field shall be provided. Example: "tg": "840539006"
t/tt	The type of test	The type of the test used, based on the material targeted by the test. A coded value from the value set test-type.json (based on LOINC). Values outside of the value set are not allowed. Exactly 1 (one) non-empty field shall be provided. Example: "tt": "LP6464-4"(Nucleic acid amplification with probe detection) "tt": "LP217198-3"(Rapid immunoassay)

▼M1

Field id	Field name	Instructions
t/nm	Test name (nucleic acid amplification tests only)	The name of the nucleic acid amplification test (NAAT) used. The name should include the name of the test manufacturer and the commercial name of the test, separated by a comma. For NAAT: the field is optional. ►M4 For antigen test: the field shall not be used, as the name of the test is supplied indirectly through the test device identifier (t/ma). ◄ When supplied, the field shall not be empty. Example: "nm": "ELITechGroup, SARS-CoV-2 ELITe MGB® Kit"
▼M4 **t/ma**	Test device identifier (antigen tests only)	Antigen test device identifier from the JRC database. Value set (HSC common list): — All antigen tests in HSC common list (human readable). — https://covid-19-diagnostics.jrc.ec.europa.eu/devices/hsc-common-recognition-rat (machine-readable, values of the field id_device included on the list form the value set). In EU/EEA countries, issuers shall only issue certificates for tests belonging to the currently valid value set. The value set shall be updated every 24 hours. Values outside of the value set may be used in certificates issued by third countries, however the identifiers shall still be from the JRC database. The use of other identifiers such as those provided directly by test manufacturers is not permitted. Verifiers shall detect values not belonging to the up to date value set and display certificates bearing these as invalid. If an identifier is removed from the value set, certificates including it may be accepted for a maximum of 72 hours after the date of removal. The value set is distributed from the EUDCC Gateway. For antigen test: exactly 1 (one) non-empty field shall be provided. For NAAT: the field shall not be used, even if the NAA test identifier is available in the JRC database. Example: “ma”: “344”(SD BIOSENSOR Inc, STANDARD F COVID-19 Ag FIA)
▼M1 **t/sc**	Date and time of the test sample collection	The date and time when the test sample was collected. The time shall include information on the time zone. The value shall not denote the time when the test result was produced. Exactly 1 (one) non-empty field shall be provided. One of the following ISO 8601 formats shall be used. Other options are not supported. YYYY-MM-DDThh:mm:ssZ YYYY-MM-DDThh:mm:ss[+-]hh

▼M1

Field id	Field name	Instructions
		YYYY-MM-DDThh:mm:ss[+-]hhmm YYYY-MM-DDThh:mm:ss[+-]hh:mm Examples: "sc": "2021-08-20T10:03:12Z" (UTC time) "sc": "2021-08-20T12:03:12+02" (CEST time) "sc": "2021-08-20T12:03:12+0200" (CEST time) "sc": "2021-08-20T12:03:12+02:00" (CEST time)
t/tr	Result of the test	The result of the test. A coded value from the value set test-result.json (based on SNOMED CT, GPS). Exactly 1 (one) non-empty field shall be provided. Example: "tr": "260415000" (Not detected)
t/tc	Testing centre or facility	Name of the actor that conducted the test. Identifiers are allowed as part of the name, but not recommended to be used individually without the name as a text. Max 80 UTF-8 characters. Any extra characters should be truncated. The name is not designed for automated verification. For NAAT tests: exactly 1 (one) non-empty field shall be provided. ►M4 For antigen test: the field is optional. If provided, it shall not be empty. ◄ Example: "tc": "Test centre west region 245"
t/co	Member State or third country in which the test was carried out	Country expressed as a 2-letter ISO3166 code (RECOMMENDED) or a reference to an international organisation responsible for carrying out the test (such as UNHCR or WHO). This shall be a coded value from the value set country-2-codes.json. The value set is distributed from the EUDCC Gateway. Exactly 1 (one) field shall be provided. Examples: "co": "CZ" "co": "UNHCR"
t/is	Certificate issuer	Name of the organisation that issued the certificate. Identifiers are allowed as part of the name, but not recommended to be used individually without the name as a text. Max 80 UTF-8 characters. Exactly 1 (one) non-empty field shall be provided. Examples: "is": "Ministry of Health of the Czech Republic" "is": "North-West region health authority"

▼M1

Field id	Field name	Instructions
t/ci	Unique certificate identifier	Unique certificate identifier (UVCI) as specified in the vaccination-proof_interoperability-guidelines_en.pdf (europa.eu) The inclusion of the checksum is optional. The prefix "URN:UVCI:" may be added. Exactly 1 (one) non-empty field shall be provided. Examples: "ci": "URN:UVCI:01:NL:187/37512422923" "ci": " URN:UVCI:01:AT:10807843F94AEE0EE5093FBC254BD813#B"

4.3. *Recovery certificate*

Recovery group, if present, shall contain exactly 1 (one) entry describing exactly one recovery statement. All elements of the recovery group are mandatory, empty values are not supported.

Field id	Field name	Instructions
r/tg	Disease or agent from which the holder has recovered: COVID-19 (SARS-CoV-2 or one of its variants)	A coded value from the value set disease-agent-targeted.json. This value set has a single entry 840539006, which is the code for COVID-19 from SNOMED CT (GPS). Exactly 1 (one) non-empty field shall be provided. Example: "tg": "840539006"
r/fr	Date of the holder's first positive ►M4 ——— ◄ test result	The date when a sample for the ►M4 ——— ◄ test producing a positive result was collected, in the format YYYY-MM-DD (complete date without time). Other formats are not supported. Exactly 1 (one) non-empty field shall be provided. Example: "fr": "2021-05-18"
r/co	Member State or third country in which test was carried out	Country expressed as a 2-letter ISO3166 code (RECOMMENDED) or a reference to an international organisation responsible for carrying out the test (such as UNHCR or WHO). This shall be a coded value from the value set country-2-codes.json. The value set is distributed from the EUDCC Gateway. Exactly 1 (one) field shall be provided. Examples: "co": "CZ" "co": "UNHCR"
r/is	Certificate issuer	Name of the organisation that issued the certificate. Identifiers are allowed as part of the name, but not recommended to be used individually without the name as a text. Max 80 UTF-8 characters. Exactly 1 (one) non-empty field shall be provided. Example: "is": "Ministry of Health of the Czech Republic" "is": "Central University Hospital"

▼M1

Field id	Field name	Instructions
r/df	Certificate valid from	The first date on which the certificate is considered to be valid. The date shall not be earlier than the date calculated as r/fr + 11 days. The date shall be provided in the format YYYY-MM-DD (complete date without time). Other formats are not supported. Exactly 1 (one) non-empty field shall be provided. Example: "df": "2021-05-29"
r/du	Certificate valid until	The last date on which the certificate is considered to be valid, assigned by the certificate issuer. The date shall not be after the date calculated as r/fr + 180 days. The date shall be provided in the format YYYY-MM-DD (complete date without time). Other formats are not supported. Exactly 1 (one) non-empty field shall be provided. Example: "du": "2021-11-14"
r/ci	Unique certificate identifier	Unique certificate identifier (UVCI) as specified in the vaccination-proof_interoperability-guidelines_en.pdf (europa.eu) The inclusion of the checksum is optional. The prefix "URN:UVCI:" may be added. Exactly 1 (one) non-empty field shall be provided. Examples: "ci": "URN:UVCI:01:NL:187/37512422923" "ci": " URN:UVCI:01:AT:10807843F94AEE0EE5093FBC254BD813#B"

▼M3

ANNEX VI

RESPONSIBILITIES OF THE MEMBER STATES AS JOINT CONTROLLERS FOR THE EU DIGITAL COVID CERTIFICATE GATEWAY FOR THE EXCHANGE OF EU DCC REVOCATION LISTS

SECTION 1

Subsection 1

Division of responsibilities

(1) The joint controllers shall process personal data through the trust framework gateway in accordance with the technical specifications in Annex I.

(2) The Member States' issuing authorities remain the sole controller for the collection, use, disclosure and any other processing of revocation information outside the gateway, including for the procedure leading to the revocation of a certificate.

(3) Each controller shall be responsible for the processing of personal data in the trust framework gateway in accordance with Articles 5, 24 and 26 of the General Data Protection Regulation.

(4) Each controller shall set up a contact point with a functional mailbox that will serve for the communication between the joint controllers themselves and between the joint controllers and the processor.

(5) A working group set up by the Committee referred to in Article 14 of Regulation (EU) 2021/953 shall be mandated to decide any issues arising from the exchange of revocation lists and from the joint controllership of related processing of personal data and to facilitate coordinated instructions to the Commission as a processor. The decisions making process of the Joint Controllers is governed by that working group and the rules of procedure to be adopted by it. As a baseline rule, non-participation by any of the joint controllers in a meeting of this working group, that has been announced at least seven (7) days before it has been convened in writing, results in a tacit agreement with the outcomes of that working group meeting. Any of the joint controllers can convene a meeting of this working group.

(6) Instructions to the processor shall be sent by any of the joint controllers' contact points, in agreement with the other joint controllers, as per the working group decision making process outlined in (5) above. The joint controller who provides the instruction should provide them to the processor in writing, and inform all other joint controllers of this. If the matter at hand is sufficiently time-critical that it does not allow for a meeting of the working group as referred to in (5) above, an instruction may be provided nonetheless, but may be rescinded by the working group. This instruction should be given in writing, and all other joint controllers should be informed of this at the time of giving the instruction.

(7) The working group as set up per (5) above does not preclude any of the joint controllers' individual competence to inform their competent supervisory authority in accordance with article 33 and 24 of the General Data Protection Regulation. Such notification does not require the consent of any of the other joint controllers.

▼M3

(8) In the scope of the trust framework gateway only persons authorised by the designated national authorities or official bodies may access the personal data exchanged.

(9) Each issuing authority shall maintain a record of the processing activities under its responsibility. The joint controllership may be indicated in the record.

Subsection 2

Responsibilities and roles for handling requests of and informing data subjects

(1) Each controller in its role as issuing authority shall provide natural persons whose certificate(s) it has revoked ('the data subjects') with information about said revocation and the processing of their personal data in the EU Digital COVID Certificate Gateway for the purposes of supporting the exchange of revocation lists, in accordance with Article 14 of the General Data Protection Regulation, unless this proves impossible or would involve a disproportionate effort.

(2) Each controller shall act as the contact point for natural persons whose certificate it has revoked and shall handle the requests submitted by data subjects or their representatives in the exercise of their rights in accordance with the General Data Protection Regulation. If a joint controller receives a request from a data subject, which relates to a certificate issued by another joint controller, it shall inform the data subject of the identity and contact details of that responsible joint controller. If requested by another joint controller, the joint controllers shall assist each other in handling data subjects' requests and shall reply to each other without undue delay and at the latest within 1 month from receiving a request for assistance. If a request is related to data submitted by a third country, the controller that receives the request shall handle it and inform the data subject of the identity and contact details of the issuing authority in the third country.

(3) Each controller shall make available to the data subjects the content of this Annex including the arrangements laid down in points 1 and 2.

SECTION 2

Management of security incidents, including personal data breaches

(1) The joint controllers shall assist each other in the identification and handling of any security incidents, including personal data breaches, linked to the processing in the EU Digital COVID Certificate Gateway.

(2) In particular, the joint controllers shall notify each other of the following:

(a) any potential or actual risks to the availability, confidentiality and/or integrity of the personal data undergoing processing in the trust framework gateway;

(b) any personal data breach, the likely consequences of the personal data breach and the assessment of the risk to the rights and freedoms of natural persons, and any measures taken to address the personal data breach and mitigate the risk to the rights and freedoms of natural persons;

▼M3

(c) any breach of the technical and/or organisational safeguards of the processing operation in the trust framework gateway.

(3) The joint controllers shall communicate any personal data breaches related to the processing operation in the trust framework gateway to the Commission, to the competent supervisory authorities and, where required so, to data subjects, in accordance with Articles 33 and 34 of the General Data Protection Regulation or following notification by the Commission.

4) Each issuing authority shall implement appropriate technical and organisational measures, designed to:

a) ensure and protect the availability, integrity and confidentiality of the personal data jointly processed;

b) protect against any unauthorised or unlawful processing, loss, use, disclosure or acquisition of or access to any personal data in its possession;

c) ensure that access to the personal data is not disclosed or allowed to anyone other than the recipients or processors.

SECTION 3

Data Protection Impact Assessment

(1) If a controller, in order to comply with its obligations specified in Articles 35 and 36 of Regulation (EU) 2016/679, needs information from another controller, it shall send a specific request to the functional mailbox referred to in Subsection 1(4) of Section 1. The latter shall use its best efforts to provide such information.

▼M3

ANNEX VII

RESPONSIBILITIES OF THE COMMISSION AS DATA PROCESSOR FOR THE EU DIGITAL COVID CERTIFICATE GATEWAY FOR SUPPORTING THE EXCHANGE OF EU DCC REVOCATION LISTS

The Commission shall:

(1) Set up and ensure a secure and reliable communication infrastructure on behalf of the Member States that supports the exchange of revocation lists submitted to the Digital COVID Certificate Gateway.

(2) To fulfil its obligations as data processor of the trust framework gateway for the Member States, the Commission may engage third parties as sub-processors; the Commission shall inform the joint controllers of any intended changes concerning the addition or replacement of other sub-processors thereby giving the controllers the opportunity to jointly object to such changes. The Commission shall ensure that the same data protection obligations as set out in this Decision apply to these sub-processors.

(3) Process the personal data, only based on documented instructions from the controllers, unless required to do so by Union or Member State law; in such a case, the Commission shall inform the joint controllers of that legal requirement before carrying on the processing activity, unless that law prohibits submitting such information on important grounds of public interest.

The processing by the Commission entails the following:

(a) Authentication of national backend servers, based on national backend server certificates;

(b) Reception of the data referred to in Article 5a(3) of the Decision uploaded by national backend servers by providing an application programming interface that allows national backend servers to upload the relevant data;

(c) Storage of the data in the EU Digital COVID certificate gateway;

(d) Making the data available for download by national backend servers;

(e) Deletion of the data at their expiration date or upon instruction of the controller that submitted them;

(f) After the end of the provision of service, delete any remaining data unless Union or Member State law requires storage of the personal data.

(4) Take all state of the art organisational, physical and logical security measures to maintain the EU Digital COVID Certificate Gateway. To this end, the Commission shall:

(a) designate a responsible entity for the security management at the level of the EU Digital COVID Certificate Gateway, communicate to the joint controllers its contact information and ensure its availability to react to security threats;

▼M3

(b) assume the responsibility for the security of the EU Digital COVID Certificate Gateway, including regularly carrying out tests, evaluations and assessments of the security measures;

(c) ensure that all individuals that are granted access to the EU Digital COVID Certificate Gateway are subject to contractual, professional or statutory obligation of confidentiality.

(5) Take all necessary security measures to avoid compromising the smooth operational functioning of the national backend servers. To this end, the Commission shall put in place specific procedures related to the connection from the backend servers to the EU Digital COVID Certificate Gateway. This includes:

(a) risk assessment procedure, to identify and estimate potential threats to the system;

(b) audit and review procedure to:

i. check the correspondence between the implemented security measures and the applicable security policy;

ii. control on a regular basis the integrity of system files, security parameters and granted authorisations;

iii. monitor to detect security breaches and intrusions;

iv. implement changes to mitigate existing security weaknesses;

v. define the conditions under which to authorise, including at the request of controllers, and contribute to, the performance of independent audits, including inspections, and reviews on security measures subject to conditions that respect Protocol (No 7) to the TFEU on the Privileges and Immunities of the European Union;

(c) changing the control procedure to document and measure the impact of a change before its implementation and keep the joint controllers informed of any changes that can affect the communication with and/or the security of their infrastructures;

(d) laying down a maintenance and repair procedure to specify the rules and conditions to be respected when maintenance and/or repair of equipment should be performed;

(e) laying down a security incident procedure to define the reporting and escalation scheme, inform without delay the controllers affected, inform without delay the controllers for them to notify the national data protection supervisory authorities, of any personal data breach and define a disciplinary process to deal with security breaches.

(6) Take state of the art physical and/or logical security measures for the facilities hosting the EU Digital COVID Certificate Gateway equipment and for the controls of logical data and security access. To this end, the Commission shall:

(a) enforce physical security to establish distinct security perimeters and allowing detection of breaches;

▼M3

(b) control access to the facilities and maintain a visitor register for tracing purposes;

(c) ensure that external people granted access to the premises are escorted by duly authorised staff;

(d) ensure that equipment cannot be added, replaced or removed without prior authorisation of the designated responsible bodies;

(e) control access from and to the national backend servers to the trust framework gateway;

(f) ensure that individuals who access the EU Digital COVID Certificate Gateway are identified and authenticated;

(g) review the authorisation rights related to the access to the EU Digital COVID Certificate Gateway in case of a security breach affecting this infrastructure;

(h) keep the integrity of the information transmitted through the EU Digital COVID Certificate Gateway;

(i) implement technical and organisational security measures to prevent unauthorised access to personal data;

(j) implement, whenever necessary, measures to block unauthorised access to the EU Digital COVID Certificate Gateway from the domain of the issuing authorities (i.e.: block a location/IP address).

(7) Take steps to protect its domain, including the severing of connections, in the event of substantial deviation from the principles and concepts for quality or security.

(8) Maintain a risk management plan related to its area of responsibility.

(9) Monitor – in real time – the performance of all the service components of its trust framework gateway services, produce regular statistics and keep records.

(10) Provide support for all trust framework gateway services in English, 24/7 via phone, mail or Web Portal and accept calls from authorised callers: the EU Digital COVID Certificate Gateway's coordinators and their respective helpdesks, Project Officers and designated persons from the Commission.

(11) Assist the joint controllers by appropriate technical and organisational measures, insofar as it is possible in accordance with Article 12 of Regulation (EU) 2018/1725, for the fulfilment of the controller's obligation to respond to requests for exercising the data subject's rights laid down in Chapter III of the General Data Protection Regulation.

▼**M3**

(12) Support the joint controllers by providing information concerning the EU Digital COVID Certificate Gateway, to implement the obligations pursuant to Articles 32, 33, 34, 35 and 36 of the General Data Protection Regulation.

(13) Ensure that data processed within the EU Digital COVID Certificate Gateway is unintelligible to any person who is not authorised to access it.

(14) Take all relevant measures to prevent that the EU Digital COVID Certificate Gateway's operators have unauthorised access to transmitted data.

(15) Take measures in order to facilitate the interoperability and the communication between EU Digital COVID Certificate Gateway's designated controllers.

(16) Maintain a record of processing activities carried out on behalf of the joint controllers in accordance with Article 31(2) of Regulation (EU) 2018/1725.