COMMISSION IMPLEMENTING DECISION (EU) 2022/483

of 21 March 2022

amending Implementing Decision (EU) 2021/1073 laying down technical specifications and rules for the implementation of the trust framework for the EU Digital COVID Certificate established by Regulation (EU) 2021/953 of the European Parliament and of the Council

(Text with EEA relevance)

THE EUROPEAN COMMISSION,

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

Having regard to Regulation (EU) 2021/953 of the European Parliament and of the Council 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 ([1]), and in particular Article 9(1) thereof,

Whereas:

(1) Regulation (EU) 2021/953 sets out the EU Digital COVID Certificate which provides proof that a person has received a COVID-19 vaccine, a negative test result or has recovered from infection for the purpose of facilitating the holders' exercise of their right to free movement during the COVID-19 pandemic.

(2) Regulation (EU) 2021/954 of the European Parliament and of the Council ([2]) provides that Member States are to apply the rules laid down in Regulation (EU) 2021/953 to third-country nationals who do not fall within the scope of that Regulation, but who are legally staying or residing in their territory and who are entitled to travel to other Member States in accordance with Union law.

(3) Council Recommendation (EU) 2022/290 amending Recommendation (EU) 2020/912 on the temporary restriction on non-essential travel into the EU and the possible lifting of such restriction ([3]) provides that third-country nationals wishing to undertake non-essential travel from a third countries to the Union should be in the possession valid proof of vaccination or recovery, such as a EU Digital COVID Certificate or a COVID-19 certificate issued by a third country covered by an implementing act adopted pursuant to Article 8(2) of Regulation (EU) 2021/953.

(4) In order for the EU Digital COVID Certificate to be operational throughout the Union, the Commission adopted Implementing Decision (EU) 2021/1073 ([4]), laying down technical specifications and rules to populate, securely issue and verify EU Digital COVID Certificates, ensure the protection of personal data, lay down the common structure of the unique certificate identifier and issue a valid, secure and interoperable barcode.

(5) In accordance with Article 4 of Regulation (EU) 2021/953, the Commission and the Member States were to set up and maintain a trust framework for the EU Digital COVID Certificate. That trust framework is able to support the bilateral exchange of certificate revocation lists containing the unique certificate identifiers of revoked certificates.

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

([2]) Regulation (EU) 2021/954 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) with regard to third-country nationals legally staying or residing in the territories of Member States during the COVID-19 pandemic (OJ L 211, 15.6.2021, p. 24).

([3]) Council Recommendation (EU) 2022/290 of 22 February 2022 amending Council Recommendation (EU) 2020/912 on the temporary restriction on non-essential travel into the EU and the possible lifting of such restriction (OJ L 43, 24.2.2022, p. 79).

([4]) 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 (OJ L 230, 30.6.2021, p. 32).

(6) On 1 July 2021, the EU Digital COVID Certificate gateway (the 'gateway'), which is the central part of the trust framework and which allows for the secure and trusted exchange between Member States of public keys used to verify EU Digital COVID Certificates, became operational.

(7) Due to their successful and large-scale rollout, EU Digital COVID Certificates have become a target for fraudsters seeking to find ways to issue fraudulent certificates. Those fraudulent certificates need therefore to be revoked. In addition, certain EU Digital COVID Certificates may be revoked by Member States at national level for medical and public health reasons, for example because a batch of vaccines administered was later found to be defective.

(8) While the EU Digital COVID Certificate system is capable of immediately revealing forged certificates, authentic certificates that are unlawfully issued on the basis of false documentation, unauthorised access or with fraudulent intent cannot be detected in other Member States unless the lists of revoked certificates generated at national level are exchanged between Member States. The same applies for certificates that have been revoked for medical and public health reasons. Failure by Member States' verification applications to detect certificates revoked by other Member States poses a threat to public health and undermines citizens' trust and confidence in the EU Digital COVID Certificate system.

(9) As noted in Recital 19 of Regulation (EU) 2021/953, Member States should, for medical and public health reasons and in the event of fraudulently issued or obtained certificates, be able to establish and exchange with other Member States for the purpose of that Regulation certificate revocation lists in limited cases, in particular as regards certificates that have been issued erroneously, as a result of fraud or following the suspension of a COVID-19 vaccine batch found to be defective. Member States should not be able to revoke certificates issued by other Member States. Certificate revocation lists exchanged should not contain any personal data other than unique certificate identifiers. In particular, they should not include the reason why a certificate has been revoked.

(10) In addition to the general information about the possibility of revocation of certificates and the possible reasons for that, holders of revoked certificates should be promptly informed by the responsible issuing authority about the revocation of their certificates and the reasons for the revocation. However, it may in some cases, and in particular in the case of EU Digital COVID Certificates issued on paper, prove impossible or could involve a disproportionate effort to trace and inform the holder of the revocation. Member States should not collect additional personal data not needed for the issuance process only to be able to inform certificate holders in case their certificates are revoked.

(11) It is thus necessary to enhance the EU Digital COVID Certificate trust framework by supporting the bilateral exchange of certificate revocation lists between Member States.

(12) This Decision does not cover temporary suspension of certificates for national use cases outside the scope of the EU Digital COVID Certificate Regulation, for example because the holder of a vaccination certificate has tested positive for SARS-CoV-2. It is without prejudice to established procedures for checking the business rules for the validity of certificates.

(13) While, from a technical point of view, different architectures for the exchange of revocation lists are feasible, exchanging them via the gateway is the most appropriate one as it limits data exchanges to the trust framework already established and as it minimises the number of both possible points of failure and exchanges between Member States compared to an alternative peer-to-peer system.

(14) Accordingly, the EU Digital COVID Certificate gateway should be enhanced to support the secure exchange of revoked EU Digital COVID Certificates for the purpose of their secure verification via the Gateway. In this regard, appropriate security measures to protect the personal data processed in the gateway should be implemented. To ensure a high level of protection, Member States should pseudonymise certificate attributes by means of an irreversible hash to be included in the revocation lists. Indeed, the unique identifier should be considered as pseudonymised data for the processing operations carried out within the framework of the gateway.

(15) In addition provisions on the role of the Member States and of the Commission as regards the exchange of certificate revocation lists should be laid down.

(16) The processing of personal data of certificate holders, which is done under the responsibility of the Member States or other public organisations or official bodies in the Member States, should be carried out in accordance with Regulation (EU) 2016/679 of the European Parliament and of the Council ([5]). Processing of personal data under the responsibility of the Commission for the purpose of managing and ensuring the security of the EU Digital COVID Certificate Gateway should comply with Regulation (EU) 2018/1725 of the European Parliament and of the Council ([6]).

(17) The Member States, represented by the designated national authorities or official bodies, determine together the purpose and means of processing of personal data through the EU Digital COVID Certificate gateway and are therefore joint controllers. Article 26 of Regulation (EU) 2016/679 places an obligation on joint controllers of personal data processing operations to determine, in a transparent manner, their respective responsibilities for compliance with the obligations under that Regulation. It also provides for the possibility to have those responsibilities determined by Union or Member State law to which the controllers are subject. The arrangement referred to in Article 26 should be included in Annex III to this Decision.

(18) Regulation (EU) 2021/953 assigns a task to the Commission to support such exchanges. The most appropriate way to fulfil that mandate is to collate the submitted certificate revocation lists on behalf of the Member States. Therefore a data processor role should be assigned to the Commission to support these exchanges by facilitating the exchange of lists via the EU Digital COVID Certificate gateway on behalf of the Member States.

(19) The Commission, as a provider of technical and organisational solutions for the EU Digital COVID Certificate gateway, processes the personal data in the revocation lists in the gateway on behalf of the Member States as joint controllers. Therefore, it acts as their processor. Pursuant to Article 28 of Regulation (EU) 2016/679 and Article 29 of Regulation (EU) 2018/1725, the processing by a processor is to be governed by a contract or a legal act under Union or Member State law which is binding on the processor with regard to the controller and which specifies the processing. Therefore it is necessary to lay down rules on processing by the Commission as a data processor.

(20) The Commission's supporting task does not involve the establishment of a central database as referred to in Recital 52 of Regulation (EU) 2021/953. That prohibition is intended to avoid a central repository of all EU Digital COVID Certificates issued and does not preclude the Member States from exchanging revocation lists, which is expressly provided for in Article 4(2) of Regulation (EU) 2021/953.

(21) When processing personal data in the EU Digital COVID Certificate gateway, the Commission is bound by Commission Decision (EU, Euratom) 2017/46 ([7]).

(22) Article 3(10) of Regulation (EU) 2021/953 allows the Commission to adopt implementing acts establishing that COVID-19 certificates issued by a third country with which the Union and the Member States have concluded an agreement on the free movement of persons allowing the contracting parties to restrict such free movement on grounds of public health in a non-discriminatory manner and which does not contain a mechanism of incorporation of Union legal acts are equivalent to those issued in accordance with this Regulation. On that basis, the Commission adopted, on 8 July 2021, Implementing Decision (EU) 2021/1126 ([8]) establishing the equivalence of COVID-19 certificates issued by Switzerland.

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

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

([7]) The Commission publishes further information on Security standards applying to all European Commission information systems on https://ec.europa.eu/info/publications/security-standards-applying-all-european-commission-information-systems_en

([8]) Commission Implementing Decision (EU) 2021/1126 of 8 July 2021 establishing the equivalence of COVID-19 certificates issued by Switzerland to the certificates issued in accordance with Regulation (EU) 2021/953 of the European Parliament and of the Council (OJ L 243, 9.7.2021, p. 49).

(23) Article 8(2) of Regulation (EU) 2021/953 allows the Commission to adopt implementing acts establishing that COVID-19 certificates issued by a third country in accordance with standards and technological systems that are interoperable with the trust framework for the EU Digital COVID Certificate and that allow for the verification of the authenticity, validity and integrity of the certificate, and which contain the data set out in the Annex to the Regulation, are to be considered as equivalent to EU Digital COVID Certificates for the purpose of facilitating the holders' exercise of their right to free movement within the Union. As noted in Recital 28 of Regulation (EU) 2021/953, Article 8(2) of that Regulation concerns the acceptance of certificates issued by third countries to Union citizens and their family members. The Commission has already adopted several such implementing acts.

(24) To avoid gaps in the detection of revoked certificates covered by such implementing acts, it should also be possible for third countries whose COVID-19 certificates have been deemed equivalent pursuant to Article 3(10) and Article 8(2) of Regulation (EU) 2021/953 to submit relevant certificate revocation lists to the EU Digital COVID Certificate gateway.

(25) Some third-country nationals who hold revoked COVID-19 certificates issued by a third country whose COVID-19 certificates have been deemed equivalent pursuant to Regulation (EU) 2021/953 may fall outside the scope of either that Regulation or Regulation (EU) 2021/954 at the moment a revocation list including their certificates is generated by the third country concerned. However, whether all third country nationals holders of revoked certificates fall within the scope of either Regulation cannot be known at the time when a certificate revocation list is generated by a third country concerned. Seeking to exclude persons not covered by the scope of either regulation at the moment when those countries' certificate revocation lists are generated is thus not feasible, and attempting to do so would result in Member States being unable to detect revoked certificates held by third-country nationals travelling to the Union for the first time. However, even the revoked certificates of those third country nationals would be verified by Member States when their holders travel to the Union, and subsequently, when they travel within the Union. The third countries whose certificates have been deemed equivalent pursuant to Regulation (EU) 2021/953 are not involved in the governance of the gateway and thus do not qualify as joint controllers.

(26) In addition, the EU Digital COVID Certificate system has proven to be the only COVID-19 certificate system operational at international level on a large scale. As a result, the EU Digital COVID Certificate has gained increasing global significance and has contributed to addressing the pandemic at the international level by facilitating safe international travel and global recovery. In the process of adopting additional implementing acts pursuant to Article 8(2) of Regulation (EU) 2021/953, new needs regarding populating the EU Digital COVID Certificate arise. According to the rules set out in Implementing Decision (EU) 2021/1073, the surname is a mandatory field in the technical contents of the certificate. It is necessary to amend that requirement to promote inclusion and interoperability with other systems, given that, in some third countries, there are persons without a surname. In cases where the certificate holder's name cannot be divided into two parts, the name should be placed in the same field (surname or forename) of the EU Digital COVID Certificate as would be done the holder's travel or identity document. This change would also better align the technical contents of the certificates with the currently valid specifications on machine-readable travel documents published by the International Civil Aviation Organization.

(27) Implementing Decision (EU) 2021/1073 should therefore be amended accordingly.

(28) The European Data Protection Supervisor was consulted in accordance with Article 42(1) of Regulation (EU) 2018/1725 and delivered an opinion on 11 March 2022.

(29) To allow Member States and the Commission sufficient time to implement the changes needed to enable the exchange of certificate revocation lists via the EU Digital COVID Certificate gateway, this Decision should start to apply four weeks after its entry into force.

(30) The measures provided for in this Decision are in accordance with the opinion of the Committee set up under Article 14 of Regulation (EU) 2021/953,

HAS ADOPTED THIS DECISION:

Article 1

Implementing Decision (EU) 2021/1073 is amended as follows:

(1) the following Articles 5a, 5b and 5c are inserted:

'*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.

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.

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.';

(2) Annex I is amended in accordance with Annex I to this Decision;

(3) Annex V is amended in accordance with Annex II to this Decision;

(4) the text in Annex III to this Decision is added as Annex VI;

(5) the text in Annex IV to this Decision is added as Annex VII.

Article 2

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

It shall apply from four weeks after its entry into force.

Done at Brussels, 21 March 2022.

For the Commission
The President
Ursula VON DER LEYEN

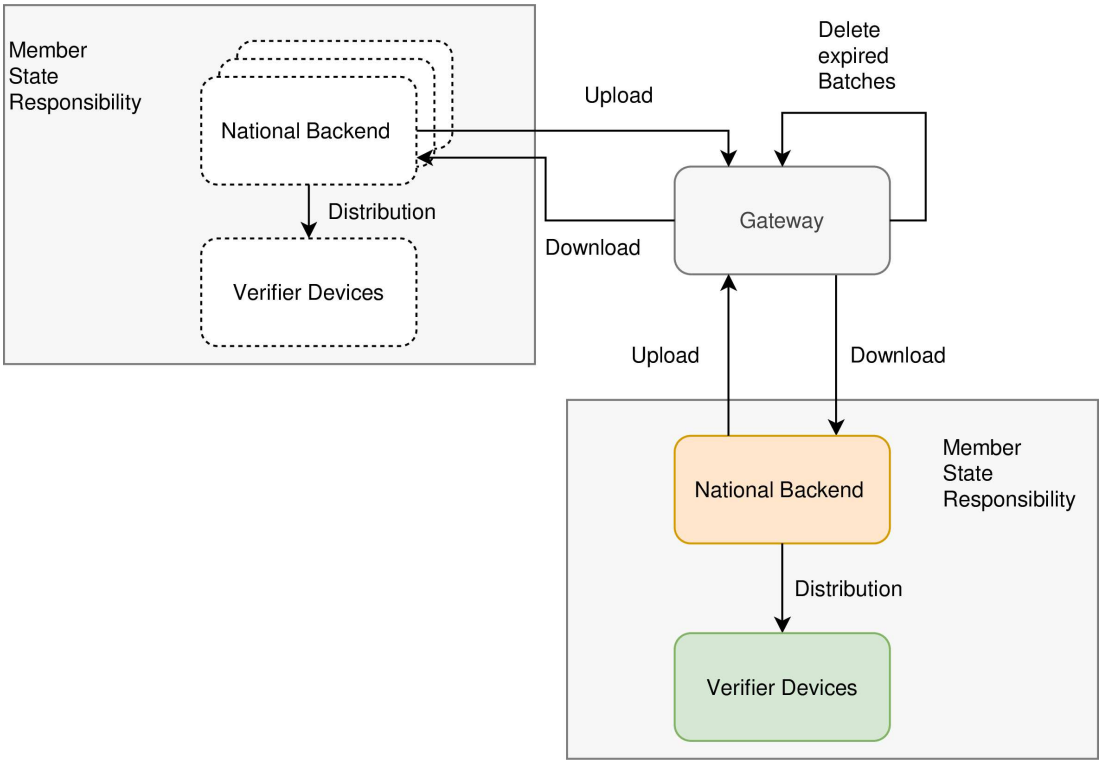
ANNEX I

In Annex I to Implementing Decision (EU) 2021/1073, the following section 9 is added:

'9. **REVOCATION SOLUTION**

9.1. **DCC Revocation List (DRL) Provision**

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



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]).

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 ([2]), 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

([1]) Please also consider 9.5.1.2 for the detailed API descriptions.
([2]) 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.

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
        }, ..
        ]
}
```

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',

'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.

9.5.1.2.2.1. Entries

Field	Mandatory	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.

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

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.'

ANNEX II

Section 3 of Annex V to Implementing Decision 2021/1073 is replaced by the following:

'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.

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”
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.'

ANNEX III

'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.

(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;

(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.'

ANNEX IV

'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;

(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;

(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.

(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.'