



ICAO

MACHINE READABLE TRAVEL DOCUMENTS GUIDANCE

Guide for Handling ICAO VDS-NC Health Proofs and EU-DCC

Version – 1.0 | April 2022

FOR THE INTERNATIONAL CIVIL AVIATION ORGANIZATION

Executive Summary

This document has been prepared as part of ICAO's efforts, led by the ICAO Council Aviation Recovery Task Force (CART) and supported by the ICAO Secretariat and its various expert Working Groups, to stimulate restart and sustainable recovery of the aviation and travel sector from the COVID-19 pandemic. It provides guidance to State authorities involved in the processing of health proofs (i.e. proofs of vaccination, testing and/or recovery) to support their verification and use of proofs issued according to ICAO or EU specifications.

CART first discussed the importance of providing robust evidence for COVID-19 testing as part of Phase II of its work that concluded in December 2020. On foot of these initial discussions, ICAO established a multi-disciplinary working group (MDWG) of Member State travel document and PKI experts that had two principal objectives:

1. evaluate the many technical solutions being proposed by industry and international organizations to meet the challenge of testing certification in the air travel continuum, and
2. examine the feasibility of leveraging existing trust models and verification systems established globally for machine-readable travel documents and, specifically, for ePassports, for the COVID-19/health use case.

The MDWG decided that the already-endorsed set of ICAO technical specifications for Visible Digital Seals (VDS) for Non-Electronic Documents should be considered as part of work under the second objective. Together with representatives of the ICAO New Technologies Working Group (NTWG), Public Key Directory (PKD) Board, and ISO/SC17/WG3, a special use case of VDS for "public health proofs" for cross-border travel was elaborated.

As a result, technical requirements for Visible Digital Seals for non-constrained environments (VDS-NC) were developed that provide for the encoding of test, vaccination and recovery data in a digitally-signed barcode. The Technical Report is available at <https://www.icao.int/vdsnc-spec>. The Report has been approved by the Technical Advisory Group on Traveller Identification (TAG/TRIP). It is accompanied by a Guidelines document, also endorsed by TAG/TRIP, approved by ICAO Council and referenced in the CART Take-Off Guidance Document (TOGD), for the use of VDS-NC health proofs in international travel. The Guidelines are available at <https://www.icao.int/vdsnc-guidance>.

CART considered these developments further as part of Phase III of its work, which concluded on 12 March 2021. Recommendation 17 of CART, issued as part of this work, encourages Member States to request evidence of testing (for COVID-19) that is secure, trustworthy, verifiable, convenient to use, compliant with data protection legislation and internationally/globally interoperable. Proof of vaccination could be based upon the World Health Organization (WHO) International Certificate of Vaccination or Prophylaxis (ICVP) and should be issued in an internationally/ globally interoperable format aligned with the technical specifications and guidance outlined by the WHO. Existing solutions should be considered and could incorporate a Visible Digital Seal (VDS-NC) or other interoperable formats from regional or global intergovernmental bodies.

In considering the status of work at this juncture, the prevailing use of different formats of health proof internationally, and the importance of secure and trustworthy verification of these health proofs in international aviation, the ICAO Council requested that ICAO seek interoperability of the ICAO VDS-NC with one of the most commonly-used formats, the EU Digital COVID Certificate. ICAO NTWG, PKD Board and ISO/TF5 experts have engaged in technical discussions with EU eHealth Network experts in describing the differences between the systems and to provide support to actors willing to convert ICAO VDS-NC compliant certificates into EU DCC or vice versa.

This Guidance document is the outcome of these discussions and analysis.

Acknowledgments

This document would not have been possible without the voluntary commitment of many ISO, ICAO and EU experts who participated in this effort.

Special expressions of gratitude have to be given for the exceptional contribution of:

- Mr. R Rajeshkumar (ISO, Auctorizium, Singapore)
- Mr. Andy Hing (Auctorizium, Singapore)
- Mr. Wei-Ren Kwan (Auctorizium, Singapore)
- Ms. Antonia Rana (EU Commission)
- Mr. Konstantin Hyppoenen (EU Commission)

Disclaimers

This document is not binding and only reflects the situation as of end of March, 2022.

Reference should always be made to the most current version of specifications published by ICAO and the EU.

1	Scope.....	6
2	Data sets.....	7
2.1	Proof of Testing.....	7
2.2	Proof of Vaccination.....	11
2.2.1	Comparison of VDS-NC (Version 1) and EU-DCC.....	11
2.2.2	Comparison of VDS-NC (Version 2) and EU-DCC.....	14
2.3	Proof of Recovery.....	18
3	Source of Trust.....	20
3.1	VDS-NC.....	21
3.1.1	Establishing trust anchor.....	21
3.1.2	Signer Certificate Revocation.....	22
3.2	EU-DCC.....	23
3.2.1	Establishing Trust Anchor.....	23
3.2.2	Signer Certificate Revocation.....	23
4	Reading, Decoding and Verification.....	24
4.1	VDS-NC.....	24
4.1.1	Reading and Decoding.....	24
4.1.1.1	Main principles.....	24
4.1.1.2	Reading Steps.....	24
4.1.1.3	Worked Example of a Barcode (Version 1).....	25
4.1.1.4	Worked Example of a Barcode (Version 2).....	28
4.2	EU-DCC.....	31
4.2.1	Reading and Decoding.....	31
4.2.1.1	Main principles.....	31
4.2.1.2	Reading Steps.....	32
4.2.1.3	Worked Example of a Barcode.....	33
4.2.2	Verifying.....	35
5	Revocation.....	35
5.1	VDS-NC.....	35
5.1.1	Revocation of Signer Certificate.....	35
5.1.2	Revocation of the issued proof.....	35
5.2	EU-DCC.....	36

5.2.1	Revocation of Signer Certificate.....	36
5.2.2	Revocation of the issued proof	36
6	Validation by private entities	36
6.1	VDS-NC	36
6.1.1	Main Principles.....	36
6.1.2	Validation Steps	36
6.2	EU-DCC	36
7	Verification of Certificates in the two frameworks.....	36
8	Use one as source document to create the other	37
8.1	Issuance Scenarios	37
8.2	Proof of Vaccination.....	38
8.2.1	Creating a VDS-NC using an EU-DCC	38
8.2.1.1	Prerequisites & Scope	39
8.2.1.2	Mappings.....	39
8.2.1.3	Issuance of Vaccine Certificate	40
8.2.1.4	Issuance Example 1 – two doses of the same vaccine.....	47
8.2.1.5	Issuance Example 2 – 2 doses of different vaccines	50
8.2.2	Creating a EU-DCC using a VDS-NC	53
8.2.2.1	Prerequisites & Scope	53
8.2.2.2	Mappings.....	54
8.2.2.3	Issuance of a Vaccine Certificate	58
8.3	Proof of Recovery.....	66
8.3.1	Creating a VDS-NC using an EU-DCC	66
8.3.1.1	Issuance of Recovery Certificate	66
8.3.1.2	Issuance Example	69
8.3.2	Creating a EU-DCC using a VDS-NC	70
8.3.2.1	Issuance of Recovery Certificate	70
8.3.2.2	Issuance Example	72

1 Scope

COVID-19 related Health Proofs are specified by ICAO using the VDS-NC technical specifications, while the European Union uses a scheme known as EU-DCC (EU Digital Covid Certificate). As a result, verifying

entities might need to validate either of them at their borders. This document is intended for issuing or verifying entities to understand the requirements of being able to issue and verify the VDS-NC and the EU-DCC.

The documents covers the similarities and differences between the two standards, explores the Trust Frameworks required to validate either of them, and attempts to map the information contained in the two specifications.

2 Data sets

COVID-19 Health Proofs are specified for three different use cases: Proof of Testing, Proof of Vaccination and Proof of Recovery. The data sets defined for each of the use cases are different. The following sections outline the information that is contained in each of them and the differences between them (delta). This overview is intended as a guide for receiving entities to decide on the adequacy of the information and the mapping if possible between their own National requirements and the presentation in each of the two specifications.

Note: The data sets are based on the respective design principles adopted by each of the parties, and the following tables do not make any judgement on the suitability or superiority of one over the other, nor do they try to explain their rationale.

2.1 Proof of Testing

The results of a COVID test are encoded in the Proof of Testing. This section attempts to correlate the fields between the two specifications.

Legend	ICAO VDS NC		EU COVID Certificate		Delta
Name	Name	Doc 9303-3 Notation, Full MRZ Name	Name	Name: Surname(s) and Forename(s), including transliterated versions	Different representation of full names. ICAO VDS NC does not include original representations of names (using original charset)
Unique Identifier Name	Unique Identifier Name	Travel Document Number	[Not Present]		VDS-NC recommends the use of the Travel Document Number, this is not specified by DCC

Legend	ICAO VDS NC		EU COVID Certificate		Delta
Additional Identifier	Additional Identifier	Any other document number at discretion of issuer	[Not Present]		VDS-NC recommends the use of the Travel Document Number, this is not specified by DCC
Sex	Sex	Sex of the holder (as specified in Doc 9303-4 Section 4.1.1.1 – Visual Inspection Zone)	[Not Present]		VDS-NC recommends the use of DOC 9303 reference, this is not specified by DCC
Date of Birth	Date of Birth	Tested person's date of birth. REQUIRED if no Unique identifier is provided. Complete date, without time, following the ISO 8601.	Date of Birth	ISO 8601, support for partial dates (YYYY or YYYY-MM)	Partial information on DOB supported by DCC. ICAO VDS NC uses Doc9303 handling of partial dates.
Name of Facility	Facility	Name of the testing facility	Testing centre or facility	Name of the testing facility. Mandatory for NAAT tests, optional for RAT tests.	The field is optional in DCC for RAT tests.
Contact of Testing Facility	Phone Number	ITU-T E.123 Specified Phone Number with Country Code	[Not Present]		Testing facility contact details only present in VDS-NC
Contact E-mail	E-mail	E-mail address of the testing facility	[Not Present]		Testing facility contact details only present in VDS-NC
Disease or agent targeted	[Not Present]		Disease or agent targeted	SNOMED CT, fixed value	VDS-NC Test is specific for

Legend	ICAO VDS NC		EU COVID Certificate		Delta
					COVID-19 and not specified
Facility Address	Address	Address of the testing facility	[Not Present]		Testing facility contact details only present in VDS-NC
Time of Sample Collection	Specimen Collection	Date and Time of the Specimen Collection formatted as RFC3339	Date and time of the test sample collection	Date and Time format of the Sample Collection	No delta
Time of Test Result Production	Report Issuance	Date and Time of the Specimen Collection formatted as RFC3339	Date and time of the test result production. Subsequently removed	Some countries have issued certificates including this value, as it was originally supported.	Currently only present in VDS-NC
Type of Test	Test Conducted	Test Supported are: molecular(PCR) molecular(other) antigen antibody	The type of test	LOINC Code System: Nucleic acid amplification with probe detection Rapid immunoassay	Different Test Coding System. Antibody tests not supported in DCC.
Test Result	Result of The Test	normal abnormal positive negative	Result of the Test	SNOMED CT, only values "detected" and "not detected"	Different Result Coding Systems
Test Method	Sampling Method used	nasopharyngeal oropharyngeal saliva blood other	[Not Present]		The type of test covered by the DCC are the type of Test methods (COVID-19 In Vitro Diagnostic Devices and Test Methods Database)

Legend	ICAO VDS NC		EU COVID Certificate		Delta
					<p>maintained by JRC.</p> <p>Information on the test method is not included in DCC (but may be derived from information on the test device provided in the next field).</p>
Test Name and Manufacturer	[Not Present]		Test name and manufacturer.	<p>NAAT tests: optional text field.</p> <p>RAT tests: mandatory identifier of the test device as defined by the JRC database.</p>	Information not included in VDS-NC Test
Member State of test	[Not Present]		Member State or third country in which the test was carried out	ISO 3166 Country Codes	Only present for DCC. In VDS-NC, it is assumed to be country that is signing the certificate
Certificate issuer	[Not Present]		Certificate issuer	Certificate Issuer Name	Included in the X509 Certificate for VDS-NC
Unique certificate identifier	UTCI		Unique certificate identifier	Certificate Identifier, UVCI	The formats of the UTCI are different, but are unique within their respective space

2.2 Proof of Vaccination

The ICAO VDS-NC specifications detail two versions for the Proof of Vaccination. Both versions are current and valid, with Version 2 being the recommended version.

2.2.1 Comparison of VDS-NC (Version 1) and EU-DCC

Legend	ICAO VDS NC (PoV Version 1)		EU COVID Certificate		Delta
Name	Name	Doc 9303-3 Notation, Full MRZ Name	Name	Name: Surname(s) and Forename(s), including transliterated versions	ICAO VDS NC does not include original representations of names (using original charset). Different representation of full names
Unique Identifier Name	Unique Identifier Name	Travel Document Number	[Not Present]		VDS-NC recommends the use of the Travel Document Number, this is not specified by DCC
Additional Identifier	Additional Identifier	Any other document number at discretion of issuer	[Not Present]		VDS-NC recommends the use of the Additional Document Number, this is not specified by DCC
Sex	Sex	Sex of the holder (as specified in Doc 9303-4 Section 4.1.1.1 – Visual Inspection Zone)	[Not Present]		VDS-NC recommends the use of DOC 9303 reference, this is not specified by DCC

Legend	ICAO VDS NC (PoV Version 1)		EU COVID Certificate		Delta
Date of Birth	Date of Birth	Vaccinated person's date of birth. REQUIRED if no Unique identifier is provided. Complete date, without time, following the ISO 8601.	Date of Birth	ISO 8601, support for partial dates (YYYY or YYYY-MM)	Partial information on DOB supported by DCC. ICAO VDS NC uses Doc9303 handling of partial dates.
Vaccine/Prophylaxis	Vaccine/Prophylaxis	ICD-11 Extension codes (http://id.who.int/icd/entity/164949870)	COVID-19 vaccine or prophylaxis	SNOMED CT or ATC Classification	Different Coding System Register
Vaccine medicinal product	Vaccine Brand	Vaccine medicinal product, as defined per member state	COVID-19 vaccine product name	Union Register of medicinal products or text-based codes for vaccine medicinal products not centrally authorized in the EU	Different use of Brand Register
Vaccine marketing authorization holder or manufacturer ;		[Not Present]	COVID-19 vaccine marketing authorization holder or manufacturer	Organisation code from EMA (SPOR-system for ISO IDMP) or text for vaccine manufacturers not in OMS	Only included in DCC
Disease or agent targeted		Disease or agent that the vaccination provides protection against, ICD-11	Disease or agent targeted	SNOMED CT, fixed value referring to COVID-19 (SARS-CoV or one of its variants)	Different Coding System Register

Legend	ICAO VDS NC (PoV Version 1)		EU COVID Certificate		Delta
Date of vaccination		Date on which the vaccine was administered. The ISO8601 full date format YYYY-MM-DD MUST be used.	Date of vaccination	The date when the described dose was received, in the format YYYY-MM-DD (complete date without time).	Same ISO8601 date format but VDS-NC describes all doses of vaccination where DCC only shows the latest
Dose Number	Dose Number	Vaccine dose number	Number in a series of vaccinations / doses	Defining two fields: Number of dose and the overall number of doses in the series	VDS-NC describes all doses of vaccination where DCC reflects one event per certificate and so only describes one dose and includes its number and the total number of doses
Member State of vaccination	Country of vaccination	The country in which the individual has been vaccinated, Doc9303-3 Country code	Member State or third country in which the vaccine was administered	ISO 3166 Country Codes (2-letter codes)	VDS-NC recommends the use of three letter country code from Doc9303-3 where DCC uses two letter country code from ISO 3166
Administering centre	Administering centre	Name/code of administering centre or a health authority responsible for the vaccination event	[Not Present]		Administering Centre not specified in DCC
Vaccine batch number	Vaccine batch number	A distinctive combination of numbers and/or letters which	[Not Present]		Vaccine batch number not specified in DCC

Legend	ICAO VDS NC (PoV Version 1)		EU COVID Certificate		Delta
		specifically identifies a batch			
Due date of next dose	Due date of next dose	Date on which the next vaccination should be administered	[Not Present]		Next dose not specified in DCC
Certificate issuer	[Not Present]		Certificate issuer	Certificate Issuer Name	Included in the X509 Certificate for VDS-NC
Unique certificate identifier	uvci		Unique certificate identifier	Certificate Identifier, UVCI	The formats of the UVCI are different, but are unique within their respective space

2.2.2 Comparison of VDS-NC (Version 2) and EU-DCC

Legend	ICAO VDS NC (PoV Version 2)		EU COVID Certificate		Delta
Name	Name	Doc 9303-3 Notation, Full MRZ Name	Name	Name: Surname(s) and Forename(s), including transliterated versions	ICAO VDS NC does not include original representations of names (using original charset). Different representation of full names
Unique Identifier Name	Unique Identifier Name	Travel Document Number	[Not Present]		VDS-NC recommends the use of the Travel

Legend	ICAO VDS NC (PoV Version 2)		EU COVID Certificate		Delta
					Document Number, this is not specified by DCC
Additional Identifier	Additional Identifier	Any other document number at discretion of issuer	[Not Present]		VDS-NC recommends the use of the Additional Document Number, this is not specified by DCC
Sex	Sex	Sex of the holder (as specified in Doc 9303-4 Section 4.1.1.1 – Visual Inspection Zone)	[Not Present]		VDS-NC recommends the use of DOC 9303 reference, this is not specified by DCC
Date of Birth	Date of Birth	Vaccinated person's date of birth. REQUIRED if no Unique identifier is provided. Complete date, without time, following the ISO 8601.	Date of Birth	ISO 8601, support for partial dates (YYYY or YYYY-MM)	Partial information on DOB supported by DCC. ICAO VDS NC uses Doc9303 handling of partial dates.
Vaccine/Prophylaxis	Vaccine/Prophylaxis	ICD-11 Extension codes (http://id.who.int/icd/entity/164949870)	COVID-19 vaccine or prophylaxis	SNOMED CT or ATC Classification	Different Coding System Register
Vaccine medicinal product	Vaccine Brand	Vaccine medicinal product, as defined in the Technical Report	COVID-19 vaccine product name	Union Register of medicinal products or text-based codes for vaccine medicinal products not centrally authorized in the EU	Different use of Brand Register

Legend	ICAO VDS NC (PoV Version 2)		EU COVID Certificate		Delta
Vaccine marketing authorization holder or manufacturer ;	Vaccine market authorization holder / Vaccine manufacturer	The names of the market authorization holder and manufacturer are used in two fields	COVID-19 vaccine marketing authorization holder or manufacturer	Organisation code from EMA (SPOR-system for ISO IDMP) or text for vaccine manufacturers not in OMS	VDS-NC describes both values in two separate fields using display names where DCC describes in a single field using code system.
Disease or agent targeted	Disease or agent targeted	Disease or agent that the vaccination provides protection against, ICD-11	Disease or agent targeted	SNOMED CT, fixed value referring to COVID-19 (SARS-CoV or one of its variants)	Different Coding System Register
Date of vaccination	Date of vaccination	Date on which the vaccine was administered. The ISO8601 full date format YYYY-MM-DD MUST be used.	Date of vaccination	The date when the described dose was received, in the format YYYY-MM-DD (complete date without time).	Same ISO8601 date format but VDS-NC describes all doses of vaccination where DCC only shows the latest time).
Dose Number and Total Doses	Dose Number / Total Doses	Vaccine dose number and total expected doses	Number in a series of vaccinations / doses	Defining two fields: Number of dose and the overall number of doses in the series	VDS-NC describes all doses of vaccination and total number of doses where DCC only describes one dose and includes its number and the total number of doses

Legend	ICAO VDS NC (PoV Version 2)		EU COVID Certificate		Delta
Member State of vaccination	Country of vaccination	The country in which the individual has been vaccinated, Doc9303-3 Country code	Member State or third country in which the vaccine was administered	ISO 3166 Country Codes (2-letter codes)	VDS-NC recommends the use of three letter country code from Doc9303-3 where DCC uses two letter country code from ISO 3166
Administering centre	Administering centre	Name/code of administering centre or a health authority responsible for the vaccination event	[Not Present]		Administering Centre not specified in DCC
Vaccine batch number	Vaccine batch number	A distinctive combination of numbers and/or letters which specifically identifies a batch	[Not Present]		Vaccine batch number not specified in DCC
Due date of next dose	Due date of next dose	Date on which the next vaccination should be administered	[Not Present]		Next dose not specified in DCC
Certificate issuer	[Not Present]		Certificate issuer	Certificate Issuer Name	Included in the X509 Certificate for VDS-NC
Unique certificate identifier	uvci		Unique certificate identifier	Certificate Identifier, UVCI	The formats of the UVCI are different, but are unique within their respective space
Vaccination Certificate Validity	Certificate Valid From / Certificate Valid Until	Date in which the certificate for a vaccination event became valid and the last date in which the certificate	Issued At / Expiration Time	Structured and encoded in CBOR Web Token (CWT). Date in which the certificate is issued and	No delta except for coding format

Legend	ICAO VDS NC (PoV Version 2)		EU COVID Certificate		Delta
		for a vaccination event is valid.		date in which the certificate's signature becomes expired.	
Optional Data Field	Optional Data Field	Issued at the discretion of the issuing authority	[Not Present]	-	Optional data field not specified in DCC

2.3 Proof of Recovery

Legend	ICAO VDS NC		EU COVID Certificate		Delta
Name	Name	Doc 9303-3 Notation, Full MRZ Name	Name	Name: Surname(s) and Forename(s), including transliterated versions	ICAO VDS NC does not include original representations of names (using original charset). Different representation of full names
Date of Birth	Date of Birth	Recovered person's date of birth.	Date of birth	ISO 8601, support for partial dates (YYYY or YYYY-MM)	Partial information on DOB supported by DCC. ICAO VDS NC uses Doc9303 handling of partial dates.

Legend	ICAO VDS NC		EU COVID Certificate		Delta
ID Document	ID Document Type / ID Document Number	<p>The ID Document Type and Number of the identity document.</p> <p>Only these values MUST be used for document type:</p> <p>P – Passport (Doc 9303-4)</p> <p>A – ID Card (Doc 9303-5)</p> <p>C – ID Card (Doc 9303-5)</p> <p>I – ID Card Doc 9303-5)</p> <p>AC - Crew Member Certificate (Doc 9303-5)</p> <p>V – Visa (Doc 9303-7)</p> <p>D – Driving License (ISO 18013-1)</p>	[Not Present]	-	ID document not specified in DCC
disease or agent the citizen has recovered from	[Not Present]		disease or agent the citizen has recovered from	SNOMED CT, fixed value referring to COVID-19 (SARS-CoV or one of its variants)	not specified in VDS-NC as it is defined for Covid-19 only
Member State of test	Member state of test	Three letter code identifying the country of test.	Member state of test	ISO 3166 Country Codes (2-letter codes)	VDS-NC recommends the use of three letter country code from Doc9303-3

Legend	ICAO VDS NC		EU COVID Certificate		Delta
					where DCC uses two letter country code from ISO 3166
Date of first positive NAAT test result	Date of first positive NAAT test result	The date when a sample for the NAAT test producing a positive result was collected. ISO8601 YYYY-MM-DD	Date of first positive test result	ISO 8601 complete date of first positive test result	EU DCC supports the issuance of recovery certificates based on rapid antigen tests.
Certificate issuer	[Not Present]		Certificate issuer	Certificate Issuer Name	Included in the X509 Certificate for VDS-NC
Recovery Certificate Validity	Certificate Valid From(df) / Certificate Valid Until(du)	Date in which the recovery certificate is issued and date in which the recovery certificate becomes expired.	Certificate Valid From / Certificate Valid Until	Date in which the certificate for a vaccination event became valid and the last date in which the certificate for a vaccination event is valid.	No delta
Unique certificate identifier	URCI	Unique Recovery Certificate Identifier	Unique certificate identifier	Certificate Identifier, UVCI	The formats of the URCI are different, but are unique within their respective space

3 Source of Trust

Border Control Inspection Systems derive the credentials required to check the authenticity of the information from an established National Trust Anchor. Establishing source of trust and establishing a National Trust Anchor is described for the two schemes in this section

3.1 VDS-NC

Source of trust originates from a single CSCA certificate in a country. CSCA Certificates (CSCA, for short) are long lived certificates that are valid for 5-10 years. To establish the National Trust Anchor, the following steps are required.

CSCAs can be obtained through different means.

1. Diplomatic Exchange
2. Master lists published in ICAO PKD. Apart from the ICAO Master list (which contains the CSCAs of PKD members), the members themselves publish Master lists containing the CSCA of many other countries. The following Master lists are also available from the ICAO PKD.
 - a. Botswana
 - b. Canada
 - c. Switzerland
 - d. Germany
 - e. Ecuador
 - f. Spain
 - g. Finland
 - h. France
 - i. Hungary
 - j. Italy
 - k. Moldova
 - l. Netherlands
 - m. Ukraine
 - n. Uzbekistan
3. German BSI publishes a Master list of CSCAs trusted at their border and can be downloaded from <https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/ElekAusweise/CSCA/GermanMasterList.html>

There are many more such instances of Master Lists published by states, all of which can be used to obtain the CSCAs necessary to validate VDS-NC Health Proofs.

3.1.1 Establishing trust anchor

As specified in [RFC 5280] a Trust Anchor must be established that can be used to anchor the validation procedure for a given Document Signer and Master List Signer.

Each Trust Anchor is comprised of a trusted public key and associated metadata. Trust Anchors MUST include, at a minimum:

- the trusted public key and any associated key parameters;
- the public key algorithm;
- the name of the key owner; and
- the value of the SubjectAltName extension of the CSCA certificate containing the ICAO assigned three-letter code of the issuing authority or organization.

For the initial public key obtained from a CSCA, trust MUST be established through an out-of-band mechanism. For example, if a CSCA certificate was downloaded from a server associated with the CSCA, out-of-band communication (e.g. phone or email) could be used to verify that the downloaded certificate is in fact the authentic certificate for that CSCA. Also, the relying party might analyse the policies, procedures and practices of the issuing CSCA to determine whether they are secure enough to satisfy the local requirements for use of certificates. Once an initial Trust Anchor is established for a given CSCA, the process could be simplified for subsequent keys for that same CSCA. If the CSCA issues a CSCA Link certificate, then out-of-band communication with the CSCA to verify the authenticity of the new certificate could be skipped because the already trusted public key for that same CSCA is used to verify the signature on that CSCA Link certificate.

The Master lists are signed by the current CSCA of the issuing country.

- ➔ The ICAO Master list is signed by the CSCA used to issue the UN laissez passer.
- ➔ The German Masterlist is signed by the CSCA used to issue Passports.
- ➔

Once any of all of the above CSCAs have been established as a Trust Anchor, the Master lists published by these entities can be downloaded on a regular basis and the contents within the master list may be trusted.

According to Doc 9303 requirements, a state must issue a document signer only 2 days after the establishment of the CSCA. Similarly, the document signer can only be used 30 days after issuance. Hence, if a new CSCA is established, it will be at least 32 days before a document signed by this CSCA is issued.

As a consequence, downloading a Master List once a month is sufficient for most purposes.

Barcode Signer Certificates are included in the VDS-NC and may be replaced with a Certificate Reference in Version 2 of the Proof of Vaccination. In case, a certificate reference is used, then the barcode signers must be downloaded at least once every 24 hours.

3.1.2 Signer Certificate Revocation

Barcode signers are issued (signed) by the CSCA and may be revoked. The issuing country must publish a Certificate Revocation List (CRL) when a barcode signer is revoked.

CRLs of ICAO PKD members are available at the URL as defined below:

<https://pkddownload1.icao.int/CRLs/CountryCode.crl>

<https://pkddownload2.icao.int/CRLs/CountryCode.crl>

Where the CountryCode is the 3 letter country code of the issuing country.

For example, a United Nations CRL is published at

<https://pkddownload1.icao.int/CRLs/UNO.crl>

<https://pkddownload2.icao.int/CRLs/UNO.crl>

The German CRL is published at:

<https://pkddownload1.icao.int/CRLs/D.crl>

<https://pkddownload2.icao.int/CRLs/D.crl>

Most of the CSCAs also include a CRL Distribution Point (CRLDP) defined in the CSCA and publish CRLs on their websites. CRLs for countries not part of the PKD can be obtained directly from the CRLDP of the country.

It is recommended that CRLs be downloaded on at least a daily basis.

3.2 EU-DCC

Source of Trust are the CSCAs registered by EU Member States in the DCC Gateway. A single country may have more than one CSCA in case DCCs are managed at regional level. The CSCA can be the CSCA used for electronic machine-readable travel documents (eMRTD CSCA or any other CA.

The CSCA certificate is registered in the DCC Gateway following a well-defined “on boarding” process.

EU Member States are connected to the DCC Gateway through their National Backends via a mutual TLS connection. The certificates corresponding to the keys used to sign the Digital COVID Certificate (called DSC, Document Signer Certificates) are uploaded to the DCC Gateway through this mechanism. EU DCCs are verified against DSCs.

3.2.1 Establishing Trust Anchor

The DCC Gateway validates the DSCs against the respective CSCA certificates registered in the “on boarding” process.

The DCC Gateway generates a “trust list” including all registered DSCs and CSCAs and is responsible for maintaining it. The Trust list is signed by the DCC Gateway.

The trust anchor is the Certificate used by the DCC Gateway to sign this trust list.

DSCs are not included in the EUDCC’s barcode. The identifier (key id, kid) of the DSC is included in the barcode.

As a consequence, in order to check the validity of the signature in the EU DCC, the trust list generated by the DCC gateway must be downloaded on a regular basis to ensure that all barcode signers are available to the inspection system.

3.2.2 Signer Certificate Revocation

The EU-DCC does not require the publishing of CRLs. If a barcode signer (DSC) is to be revoked, it is removed from the trust list provided by the DCC Gateway to the National Backends.

As a consequence, the following needs to be done on a regular basis (at least daily) to maintain the National Trust Anchors:

1. Download the trust list from the DCC Gateway.
2. Verify the signature on the trust list
3. Extract the CSCAs from the trustlist
 - a. If the CSCA exists on the National Trust anchor and is also on the DCC trust list, no action is required.
 - b. If the CSCA exists on the DCC trust list, but not on the National Trust anchor, it should be added to the National trust anchor.
 - c. If the CSCA exists on the National Trust Anchor but is not in the DCC Trust List, **then it is assumed to be revoked and must be removed from the national trust anchor.**
4. Extract the DSCs from the trust list
 - a. Lookup the CSCA corresponding to the DSC. If found, verify the DSC and add to the National trust anchor. If not found, then the DSC must not be added to the National trust anchor.
 - b. After verification,
 - i. If DSC is in both the DCC trust list and the national trust anchor, no action is required.
 - ii. If it is on DCC trust list but not national trust anchor, add it to the National trust anchor.
 - iii. If it is in National trust anchor, but not in DCC trust list, **then it is assumed to be revoked and must be removed from the National trust anchor.**

As the revocation checking is dependent on the presence/absence of the CSCA or the DSCs on the DCC trust list, this process must be done regularly (at least once every day).

4 Reading, Decoding and Verification

This section outline the steps needed to decode the data after scanning the barcode.

4.1 VDS-NC

4.1.1 Reading and Decoding

4.1.1.1 *Main principles*

1. The VDS-NC can be read by most barcode scanners.
2. The Signer Certificate is included in the barcode, which eases the issue of distribution of the barcode signer certificates. For Version 2 of the Proof of Vaccination, the Signer Certificate may be replaced with a Certificate Reference. In this case, the barcode signer certificates must be available through the PKD or published by the country using the trustlist mechanism specified in the Technical Report.
3. The data extracted by the barcode reader is human readable except for the signer certificate and the signature value

4.1.1.2 *Reading Steps*

1. Read the 2D barcode using a reader equipment that is able to read:
 - a. DataMatrix [ISO/IEC 16022]

- b. Aztec Codes [ISO/IEC 24778]
 - c. QR Codes [ISO/IEC 18004]
2. Decoding of the read data
- a. The data structure is defined using I-JSON (JavaScript Object Notation), a lightweight data-interchange format which is easy for humans to read and write.
 - b. The encoded barcode consist of a **data zone** and **signature zone**
3. Verify the **signature** (MUST be present for vaccination certificates V1 and may be replaced with a Certificate Reference for V2)
- a. The signature zone consist of the signature algorithm, certificate and Signature
 - b. The signer certificate SHALL use a named curve of the following list:
 - i. brainpoolP256r1 [RFC 5639]
 - ii. brainpoolP320r1 [RFC 5639]
 - iii. brainpoolP384r1 [RFC 5639]
 - iv. brainpoolP512r1 [RFC 5639]
 - v. NIST P-256 [FIPS 186-4]
 - vi. NIST P-384 [FIPS 186-4]
 - vii. NIST P-521 [FIPS 186-4]
 - c. For the brainpool curves the Object Identifiers specified in [RFC 5639] MUST be used; for the NIST curves the Object Identifiers specified in [RFC 5480] MUST be used.
 - d. Supported Signature algorithms:
 - i. ECDSA with Sha256 hashing algorithm
 - ii. ECDSA with Sha384 hashing algorithm
 - iii. ECDSA with Sha512 hashing algorithm

4.1.1.3 *Worked Example of a Barcode (Version 1)*

This worked example uses the VDS-NC Proof of Vaccination (PoV) Version 1 barcode to illustrate the process:


```
"sigv1":"E29I8LRfFBtpgdXek21qUUpHCFX28B0S91A0OazqNqKJHlwVi6SbEsYBLm05tdKIqnXs  
zAuL-dh05-Az8LeNnA=="
```

The data can also be extracted from the barcode and is as follows:

```
{  
  "hdr": {  
    "t": "icao.vacc",  
    "v": 1,  
    "is": "UTO"  
  },  
  "msg": {  
    "uvci": "U32870",  
    "pid": {  
      "n": "Smith Bill",  
      "sex": "M",  
      "i": "A1234567Z"  
    },  
    "ve": [{  
      "des": "XM8NQ0",  
      "nam": "Comirnaty",  
      "dis": "RA01.0",  
      "vd": [{  
        "dvc": "2021-03-03",  
        "seq": 1,  
        "ctr": "UTO",  
        "adm": "RIVM",  
        "lot": "VC35679"  
      }, {  
        "dvc": "2021-03-24",  
        "seq": 2,  
        "ctr": "UTO",  
        "adm": "RIVM",  
        "lot": "VC87540"  
      }]  
    }  
  }  
}
```

At this point, the data, the certificate used to sign the data and the signature are now available for validation.

4.1.1.3.1 Verifying

The process of validation to establish the authenticity and integrity of the information read from the barcode is described below.

- From the above data, the Signature Algorithm is ES256, which corresponds to an ECDSAwithSHA256.
- The data (which is protected by the signature) is as follows:

```
{"hdr":{"t":"icao.vacc","v":1,"is":"UTO"},"msg":{"uvci":"U32870","pid":{"n":"  
Smith  
Bill","sex":"M","i":"A1234567Z"},"ve":[{"des":"XM8NQ0","nam":"Comirnaty","dis
```

```
": "RA01.0", "vd": [{"dvc": "2021-03-03", "seq": 1, "ctr": "UTO", "adm": "RIVM", "lot": "VC35679"}, {"dvc": "2021-03-24", "seq": 2, "ctr": "UTO", "adm": "RIVM", "lot": "VC87540"}] ] ] }
```

- This data needs to undergo a process of canonicalization using RFC 8785. The output after the canonicalization process is as follows:

```
{ "hdr": { "is": "UTO", "t": "icao.vacc", "v": 1 }, "msg": { "pid": { "i": "A1234567Z", "n": "Smith Bill", "sex": "M" }, "uvci": "U32870", "ve": [ { "des": "XM8NQ0", "dis": "RA01.0", "nam": "Comirnaty", "vd": [ { "adm": "RIVM", "ctr": "UTO", "dvc": "2021-03-03", "lot": "VC35679", "seq": 1 }, { "adm": "RIVM", "ctr": "UTO", "dvc": "2021-03-24", "lot": "VC87540", "seq": 2 } ] ] ] }
```

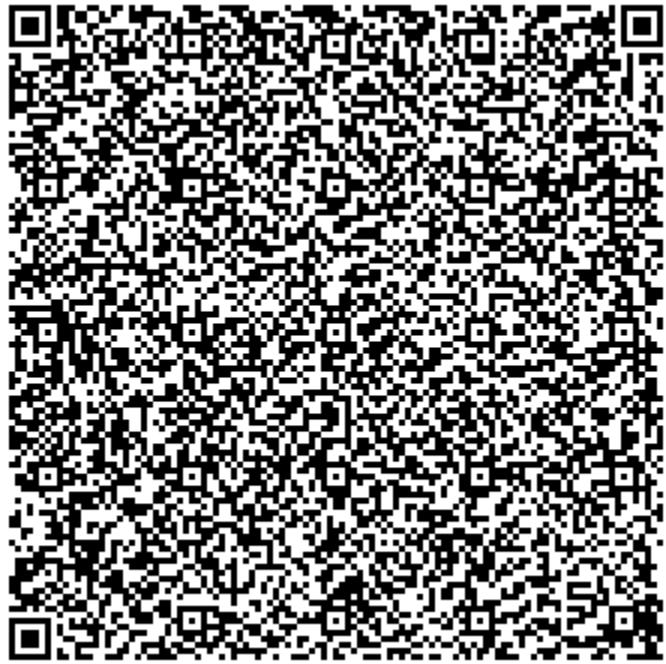
- The hash of the data needs to be calculated. As the Signature Algorithm is a ECDSAwithSHA256, the hashing algorithm to be used is Sha256 and the output is as follows:

tuza6EFBg0/kiLOtBSdpg3t1g/l6h9Tr1QLOITQwGu4=

- Verification of the hash value with the public key should succeed if the data has not been tampered. If verification fails, then the data in the barcode has been tampered with and MUST NOT be trusted.
- Use the Authority Key Identifier of the barcode signer certificate to look up the CSCA in the National Trust Anchor
 - If CSCA is not found, then the barcode signer cannot be verified and the VDS-NC MUST NOT be trusted.
 - If CSCA is found, the barcode signer certificate must be verified using the CSCA. If verification fails, then the data in the barcode MUST NOT be trusted.
- If verification succeeds, then the barcode signer must be checked against the CRL of the country.
 - If barcode signer is in the CRL, then the data in the barcode MUST NOT be trusted.
 - If barcode signer is not in the CRL, then the data in the barcode is AUTHENTIC and can be TRUSTED.

4.1.1.4 *Worked Example of a Barcode (Version 2)*

This worked example uses the VDS-NC Proof of Vaccination (PoV) Version 2 barcode to illustrate the process:



On scanning the barcode, the full I-JSON string with certificate and Signature is as follows:

```
{ "data": { "hdr": { "t": "icao.vacc", "v": 2, "is": "UTO" }, "msg": { "uvci": "U32870", "pid": { "n": "Smith Bill", "sex": "M", "i": "A1234567Z" }, "ve": [ { "des": "XM8NQ0", "nam": "Comirnaty", "mah": "BioNTech Manufacturing GmbH", "dis": "RA01.0", "vd": [ { "dvc": "2021-12-03", "seq": 1, "ctr": "UTO", "adm": "RIVM", "lot": "VC35679" }, { "dvc": "2021-12-24", "seq": 2, "ctr": "UTO", "adm": "RIVM", "lot": "VC87540" } ] } ] }, "sig": { "alg": "ES256", "cer": "MIIBfTCCASCgAwIBAgIBbDAMBggqhkJOPQQDAgUAMB0xCzAJBgNVBAYTAlVUMQ4wDAYDVQQDDAVVVCBDQTAeFw0yMDEyMzExNjAwMDBaFw0yOTEyMzExNjAwMDBaMB0xCzAJBgNVBAYTAlVUMQswCQYDVQDEwIwODBZMBMGBYqGSM49AgEGCCqGSM49AwEHA0IABI5bRQ3-vabXhHAs2IPi-k9rP_TS2J8aq5fTtUG1iOwXdBxx2n6c38TJ2MzBWT5PHCKVlq5JOCyJ1nDlCPd1S2yjUjBQMBUGA1UdJQEB_wQLMAkGB2eBCAEBDgIwHwYDVR0jBBgwFoAUymyksnX8rywn0RH7nDq-Bs2QOqowFgYHZ4EIAQEGAgQLMAkCAQAxBBMCT1YwDAYIKoZIZj0EAWIFAANJADBGAiEAqw9_YejSj_dU9WOZWrVulY1xhlCOzxO_DiHZLI-PT5wCIQD-mj_W90LN33qZd30ErsLlctS-7mFCeYWu44ND84Mmxw==", "sigv1": "6b6Erplj3KgFaCD4h-oG4PK1jISxZhtEZ9vUkj9HRVE4ui3a_RkzmVlS27opCyIIBTEiQ-0azwOHfrDVoCmwSQ==" } }
```

The certificate in Base64 is embedded in the data and is extracted as follows:

```
MIIBfTCCASCgAwIBAgIBbDAMBggqhkJOPQQDAgUAMB0xCzAJBgNVBAYTAlVUMQ4wDAYDVQQDDAVVVCBDQTAeFw0yMDEyMzExNjAwMDBaFw0yOTEyMzExNjAwMDBaMB0xCzAJBgNVBAYTAlVUMQswCQYDVQDEwIwODBZMBMGBYqGSM49AgEGCCqGSM49AwEHA0IABI5bRQ3-vabXhHAs2IPi-k9rP_TS2J8aq5fTtUG1iOwXdBxx2n6c38TJ2MzBWT5PHCKVlq5JOCyJ1nDlCPd1S2yjUjBQMBUGA1UdJQEB_wQLMAkGB2eBCAEBDgIwHwYDVR0jBBgwFoAUymyksnX8rywn0RH7nDq-Bs2QOqowFgYHZ4EIAQEGAgQLMAkCAQAxBBMCT1YwDAYIKoZIZj0EAWIFAANJADBGAiEAqw9_YejSj_dU9WOZWrVulY1xhlCOzxO_DiHZLI-PT5wCIQD-mj_W90LN33qZd30ErsLlctS-7mFCeYWu44ND84Mmxw==
```

The Signature is also embedded as is extracted as follows:

```
"sigv1": "6b6Erplj3KgFaCD4h-  
oG4PK1jISxZhtEZ9vUkj9HRVE4ui3a_RkzmV1S27opCyIIBTEiQ-0azwOHfrDVoCmwSQ=="
```

The data can also be extracted from the barcode and is as follows:

```
{  
  "hdr": {  
    "t": "icao.vacc",  
    "v": 2,  
    "is": "UTO"  
  },  
  "msg": {  
    "uvci": "U32870",  
    "pid": {  
      "n": "Smith Bill",  
      "sex": "M",  
      "i": "A1234567Z"  
    },  
    "ve": [{  
      "des": "XM8NQ0",  
      "nam": "Comirnaty",  
      "mah": "BioNTech Manufacturing GmbH",  
      "dis": "RA01.0",  
      "vd": [{  
        "dvc": "2021-12-03",  
        "seq": 1,  
        "ctr": "UTO",  
        "adm": "RIVM",  
        "lot": "VC35679"  
      }, {  
        "dvc": "2021-12-24",  
        "seq": 2,  
        "ctr": "UTO",  
        "adm": "RIVM",  
        "lot": "VC87540"  
      }]  
    }]  
  }  
}
```

At this point, the data, the certificate used to sign the data and the signature are now available for validation.

4.1.1.4.1 Verifying

The process of validation to establish the authenticity and integrity of the information read from the barcode is described below.

- From the above data, the Signature Algorithm is ES256, which corresponds to an ECDSAwithSHA256.

- The data (which is protected by the signature) is as follows:

```
{"hdr":{"t":"icao.vacc","v":2,"is":"UTO"},"msg":{"uvci":"U32870","pid":{"n":"Smith Bill","sex":"M","i":"A1234567Z"},"ve":[{"des":"XM8NQ0","nam":"Comirnaty","mah":"BioNTech Manufacturing GmbH","dis":"RA01.0","vd":[{"dvc":"2021-12-03","seq":1,"ctr":"UTO","adm":"RIVM","lot":"VC35679"}, {"dvc":"2021-12-24","seq":2,"ctr":"UTO","adm":"RIVM","lot":"VC87540"}]}]}
```

- This data needs to undergo a process of canonicalization using RFC 8785. The output after the canonicalization process is as follows:

```
{"hdr":{"is":"UTO","t":"icao.vacc","v":2},"msg":{"pid":{"i":"A1234567Z","n":"Smith Bill","sex":"M"},"uvci":"U32870","ve":[{"des":"XM8NQ0","dis":"RA01.0","mah":"BioNTech Manufacturing GmbH","nam":"Comirnaty","vd":[{"adm":"RIVM","ctr":"UTO","dvc":"2021-12-03","lot":"VC35679","seq":1}, {"adm":"RIVM","ctr":"UTO","dvc":"2021-12-24","lot":"VC87540","seq":2}]}]}
```

- The hash of the data needs to be calculated. As the Signature Algorithm is a ECDSAwithSHA256, the hashing algorithm to be used is Sha256 and the output in Base64 is as follows:

EWpbQX1TUcrrWJF09UGjR0WYrbYej9EAXdu+X4wxh9Q=

- Verification of the hash value with the public key should succeed if the data has not been tampered. If verification fails, then the data in the barcode has been tampered with and MUST NOT be trusted.
- Use the Authority Key Identifier of the barcode signer certificate to look up the CSCA in the National Trust Anchor
 - If CSCA is not found, then the barcode signer cannot be verified and the VDS-NC MUST NOT be trusted.
 - If CSCA is found, the barcode signer certificate must be verified using the CSCA. If verification fails, then the data in the barcode MUST NOT be trusted.
- If verification succeeds, then the barcode signer must be checked against the CRL of the country.
 - If barcode signer is in the CRL, then the data in the barcode MUST NOT be trusted.

If barcode signer is not in the CRL, then the data in the barcode is AUTHENTIC and can be TRUSTED.

4.2 EU-DCC

4.2.1 Reading and Decoding

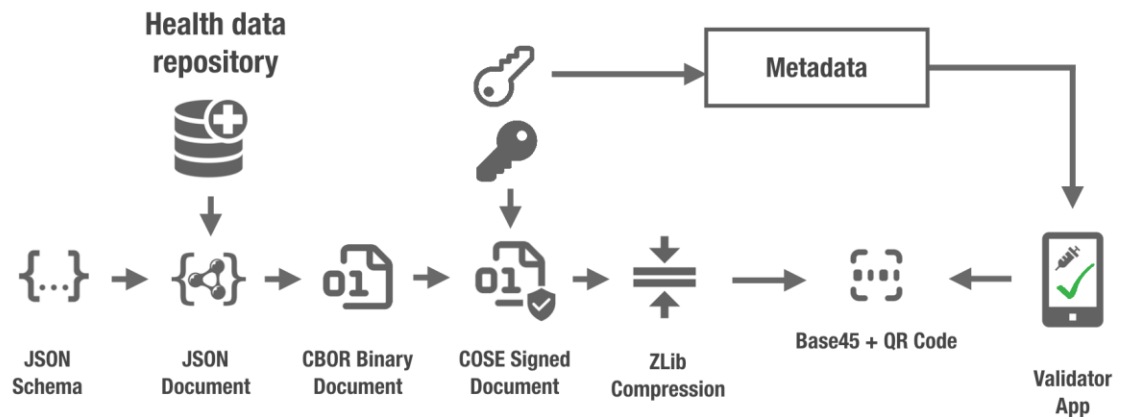
4.2.1.1 Main principles

1. The EU DCC is encoded in Base45 and is expected to be read by all barcode scanners.
2. The Signer Certificate is not included in the barcode, which requires frequent accesses to the EU DCC gateway for the download of certificates required to validate the DCC. This is to facilitate the verification of certificates in suboptimal environments, including by

mobile phones, as the size of the barcode is kept minimal (further supported by the use of CBOR and ZLib compression).

4.2.1.2 Reading Steps

4. Read the 2D barcode using a reader equipment that is able to read:
 - a. QR Codes [ISO/IEC 18004]
5. Decoding of the read data
 - a. The data structure is described in https://ec.europa.eu/health/sites/default/files/ehealth/docs/covid-certificate_json_specification_en.pdf using JSON, authoritative source for the schema being <https://github.com/ehn-dcc-development/ehn-dcc-schema>, however JSON is used for descriptive purposes only, the data in the QR code itself is encoded in CBOR.
 - b. The 2d barcode string consists of a three letter code prefix (currently the only valid value is "HC1"), followed by a ":" and the based45 encoded string, resulting from the following process:



1

- c. The CBOR binary document contains the DCC data (payload), while the COSE signed document contains the signed data.
 - d. The decoding process follows the following steps:
 - i. Base45 decoding
 - ii. Zlib deflating
6. Verification of the **signature** of the COSE object using the public key referenced in the CBOR object ("CBOR Web Token", CWT)

¹ <https://github.com/ehn-dcc-development/hcert-spec/blob/main/overview.png>

7. Supported Signature algorithms:
 - a. ECDSA with Sha256 hashing algorithm (COSE algorithm parameter ES256)
 - b. RSASSA-PSS, 2048 bits with Sha256 hashing algorithm (COSE algorithm parameter PS256)

4.2.1.3 Worked Example of a Barcode

This worked example uses the following barcode to illustrate the process²:



On scanning the barcode, the prefixed Base45 encoded string is as follows:

```
HC1:NCFOXN%TS3DH3ZSUZK+.V0ETD%65NL-AH-
R6IOOK.IR9B+9G4G50PHZF0AT4V22F/8X*G3M9JUPY0BX/KR96R/S09T./0LWTKD33236J3TA3M*4
VV2 73-E3GG396B-43O058YIB73A*G3W19UEBY5:PI0EGSP4*2DN43U*0CEBQ/GXQFY73CIBC:G
7376BxBJBAJ UNFMJCRN0H3PQN*E33H3OA70M3FMJIJN523.K5QZ4A+2XEN QT
QTHC31M3+E32R44$28A9H0D3ZCL4JMYAZ+S-A5$XKX6T2YC 35H/ITX8GL2-
LH/CJTK96L6SR9MU9RFGJA6Q3QR$P2OIC0JVLA8J3ET3:H3A+2+33U
SAAUOT3TPTO4UBZIC0JKQTL*QDKBO.AI9BVYTOCFOPS4IJCOT0$89NT2V457U8+9W2KQ-7LF9-
DF07U$B97JJ1D7WKP/HLIJL8JF8JFHJP7NVDEBU1J*Z222E.GJ457661CFFTWM-
8P2IUE7K*SSW613:9/:TT5IYQBTBU16R4I1A/9VRPJ-TS.7ZEM7MSVOC4RG2L-
TQJROXL2J:52J7F0Q10SMAP3CG3KHF0DWIH
```

² Barcode and associated data used in this section are from <https://github.com/eu-digital-green-certificates/dgc-testdata/tree/main/AT>

The certificate in Base64 for this code is :

```
MIIBVtCCAWOgAwIBAgIKAXk8i880leLsuTAKBggqhkJOPQQDAjA2MRYwFAYDVQQDDA1BVCBER0MgQ1NDQSAxMQswCQYDVQQGEwJBVDEPMA0GA1UECgwGQk1TR1BLMB4XDTIxMDUwNTEyNDEwNl0XDTIzMDUwNTEyNDEwNl0wPTEwMA8GA1UEAwwIQVQgRFNDIDExCzAJBgNVBAYTAkFUMQ8wDQYDVQQKDAZCTVNHUESxCjAIBgNVBAUTATEwWTATBgcqhkJOPQIBBggqhkJOPQMBBwNCAAST1Vz1rRuW1HqObUE9MDe7RzIk1gq4XW5GTyHuHTj5cFEn2Rge37+hINfCZzcozpwQKdyaporPUP1TE7UWl0F3o1IwUDAObgNVHQ8BAf8EBAMCB4AwHQYDVR0OBByEFO49y1ISb6cvXshLcp8UUp9VoGLQMB8GA1UdIwQYMBaAFP7JKEOf1GEvef2iMdtopsetwGGeMAoGCCqGSM49BAMCA0gAMEUCIQDG2opotWG8tJXN84ZZqT6wUBz9KF8D+z9NukYvnUEQ3QIGdBLFSTSiDt0UJaDf6St2bkUQuVHW6fQbONd731/M4nc=
```

The COSE object is:

```
d2844da20448d919375fc1e7b6b20126a0590133a4041a61817ca0061a60942ea001624154390103a101a4617681aa62646e01626d616d4f52472d3130303033303231356276706a313131393334393030376264746a323032312d30322d313862636f624154626369783155524e3a555643493a30313a41543a31303830373834334639344145453045453530393346424332353442443831332342626d706c45552f312f32302f31353238626973781b4d696e6973747279206f66204865616c74682c20417573747269616273640262746769383430353339303036636e616da463666e74754d5553544552465241553c474f455353494e47455262666e754d7573746572667261752d47c3b6c39f696e67657263676e74684741425249454c4562676e684761627269656c656376657265312e302e3063646f626a313939382d30322d323658405812fce67cb84c3911d78e3f61f890d0c80eb9675806aeb66aa2d0d0c91d1fc98d7bcb80bf00e181806a9502e11b071325901bd0d2c1b6438747b8cc50f521
```

The binary CBOR object is:

```
bf6376657265312e302e30636e616dbf62666e754d7573746572667261752d47c3b6c39f696e67657263666e74754d5553544552465241553c474f455353494e47455262676e684761627269656c6563676e74684741425249454c45ff63646f626a313939382d30322d3236617681bf627467693834303533393030366276706a31313139333439303037626d706c45552f312f32302f31353238626d616d4f52472d31303030333032313562646e01627364026264746a323032312d30322d313862636f624154626973781b4d696e6973747279206f66204865616c74682c2041757374726961626369783155524e3a555643493a30313a41543a31303830373834334639344145453045453530393346424332353442443831332342ffff
```

The JSON description of the CBOR encoded payload is the following:

```
"JSON": {
  "ver": "1.0.0",
  "nam": {
    "fn": "Musterfrau-Gößinger",
    "fnt": "MUSTERFRAU<GOESSINGER",
    "gn": "Gabriele",
    "gnt": "GABRIELE"
  },
  "dob": "1998-02-26",
  "v": [
```

```

    {
      "tg": "840539006",
      "vp": "1119349007",
      "mp": "EU/1/20/1528",
      "ma": "ORG-100030215",
      "dn": 1,
      "sd": 2,
      "dt": "2021-02-18",
      "co": "AT",
      "is": "Ministry of Health, Austria",
      "ci": "URN:UVCI:01:AT:10807843F94AEE0EE5093FBC254BD813#B"
    }
  ],
},

```

4.2.2 Verifying

The process of validation to establish the authenticity and integrity of the information read from the barcode follows the schema in the figure above in reverse.

The CWT contains the reference to the public key to be used for validation. The public key is contained in a certificate which is downloaded from the EU DCC gateway. For the purpose of this worked example, the certificate is provided.

Verification of the hash value with the public key should succeed if the data has not been tampered. If verification fails, then the data in the barcode has been tampered with and **MUST NOT** be trusted.

The Authority Key Identifier contained in the DSC can be used to look up the CA in the EU DCCG.

If CA is not found, then the DSC cannot be verified and the EU DCC **MUST NOT** be trusted.

If CA is found, the DSC must be verified using the CA. If verification fails, then the data in the barcode **MUST NOT** be trusted.

5 Revocation

5.1 VDS-NC

5.1.1 Revocation of Signer Certificate

Revocation of Signer Certificate can be handled through CRL as explained in the previous section.

5.1.2 Revocation of the issued proof

Currently, the mechanism to revoke the individual proof has not yet been defined for VDS-NC.

5.2 EU-DCC

5.2.1 Revocation of Signer Certificate

Revocation of the DSC is responsibility of the Member States.

The use of CRLs is recommended and in this case it is recommended that the CRL distribution point is set in the DSC certificate. The use of OSCP is forbidden.

However the primary mechanism to declare a DSC no longer valid is through its removal from the trust list. In other words, as long as a DCS is present in the trust list, it can be considered valid.

5.2.2 Revocation of the issued proof

Individual EU DCCs may be revoked by the issuer by placing them on the revocation list. The revocation lists are published at the EU DCC Gateway. Verifiers may fetch the revocation lists and check EU DCCs against them to detect and reject revoked certificates.

Note: This facility is planned to be implemented and is not available yet as of end March, 2022.

6 Validation by private entities

The health proofs may also need to be verified by private entities. For example, an airline check in counter, a hotel etc. This section details the steps that need to be followed to verify the health proofs.

6.1 VDS-NC

6.1.1 Main Principles

The same principles and steps applies for a private entity as for a public entity to obtain/trust the Masterlist and verify the VDS-NC.

6.1.2 Validation Steps

The ICAO Masterlist and other Masterlists as mentioned in Section 3 of this document are available for public download without any restrictions. Any private entity can follow the steps outlined in Section 3 to set up their own Trust Anchor and validate the VDS-NC using the steps outlined in Section 4.

6.2 EU-DCC

The credentials required for validating the EU-DCC have to be obtained from the EU DCC gateway. Currently, the access is limited to EU and EEA Member States as well as third countries for whom an equivalence decision has been adopted, and the data is not available for public download. Private entities within EU will need to have an arrangement with their National Trust Anchor to get access to these credentials.

For Countries and private entities that are not part of the EU-DCC gateway, there is no current mechanism to obtain the credentials needed to verify EU-DCC. So, verification is not possible.

7 Verification of Certificates in the two frameworks

Credentials (CSCAs, Barcode Signers, CRLs) need to be available for verifying both the EU-DCC and the VDS-NC. Currently, ICAO Master list and the other master lists specified in Section 3 are available for

public download. A similar publication mechanism will be added to the EU DCC system in a near future. The access to the EU-DCC gateway is restricted and public download of the credentials is not possible. The ICAO PKD allows anonymous download of the CSCA master lists through a website. This means that anyone who wishes to validate a VDS-NC could download the master list and verify the VDS.

For EU-DCC, anonymous download is planned to be implemented in the near future. When it is implemented, anyone who wishes to validate an EU DCC could download the DSC list and verify the EU DCC.

The ICAO PKD allows publication of Master Lists that are uploaded by member countries.

ICAO has created a Health Masterlist that contains the CSCAs and barcode signers used to issue health credentials. Members of EU-DCC may submit the CSCAs and barcode signers used by them to ICAO and this would be included in the ICAO Health masterlist. Users of this masterlist can verify both the VDS-NC and EU-DCC, if the issuer of the EU DCC has published the DSC at the ICAO's Health Masterlist.

For verifiers that use only the EU-DCC gateway, there is currently no mechanism to validate VDS-NC by depending on the EU-DCC gateway as the sole source of trust, though this may change in the future.

8 Use one as source document to create the other

8.1 Issuance Scenarios

The facilitation of conversion of VDS-NC from EU-DCC or vice versa is envisaged as happening under for following scenarios.

- Issuance at EU border

The EU-DCC is accepted across the EU. It is possible that when a foreign traveller arrives in the EU, the country may choose to issue an EU-DCC for the convenience of the traveler within the EU. In this case the VDS-NC will be scanned and used as input, speeding up the data entry process. Since the VDS-NC contains the entire vaccination history of the traveler, multiple EU-DCCs will need to be created. This guideline may help EU Member States in such an endeavor.

- Issuance at a Foreign border.

When an EU citizen travels to a country which uses the VDS-NC internally, the country may choose to issue a VDS-NC for use within that country. In this case the EU-DCC could be scanned and used as input, speeding up the data entry process. Since the VDS-NC is a completed history of vaccination, the traveller will need to present all their historical EU-DCCs for each of the doses of the vaccines they have received to enable the conversion to a single VDS-NC.

- A country issues both an EU-DCC and VDS-NC to its citizens.

The EU-DCC may have been issued by the Health Agency within the country using their own CSCA(s). Before the traveller goes overseas, they may approach an agency within their country which may issue a single VDS-NC from the existing EU-DCC(s) for convenience when travelling abroad. The option for scanning the existing EU-DCC will facilitate the process.

A country may wish to implement a conversion service that provides their citizens with a converted VDS NC into EU DCC. The third country would be responsible to digitally sign the certificates.

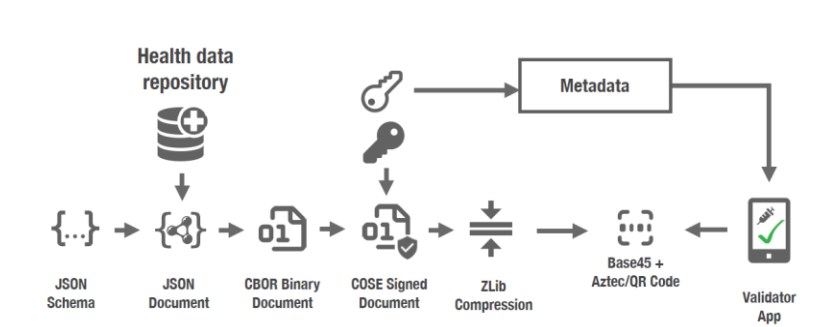
8.2 Proof of Vaccination

The data sets used in the following examples are available at the following locations.

1. For VDS-NC:
 - i. the Technical Report is available at <https://www.icao.int/security/fal/trip/pages/publications.aspx>
 - ii. The JSON files for the Vaccine/Prophylaxis and Vaccine name are available at the github location: <https://github.com/ICAO-TRIP-ISO-WG3>
2. For EU-DCC:
 - i. The DCC value sets are available at https://ec.europa.eu/health/system/files/2022-03/eu-dcc-value-sets_en.pdf
 - ii. The Github location for the same is <https://github.com/ehn-dcc-development/ehn-dcc-valuesets>

8.2.1 Creating a VDS-NC using an EU-DCC

This chapter follows the principles of creating a VDS-NC based on an EU-DCC. This process requires the steps as described in **Error! Reference source not found.** to decrypt, verify (if applicable) and decode the dataset of an EU-DCC. It follows the reversed flow as presented in the EU 'Interoperability of Health Certificates Trust Framework' specifications of the encoding of the JSON Dataset below to retrieve a validated JSON document (containing the dataset):



8.2.1.1 Prerequisites & Scope

- Vaccination, Test and Recovery Health Certificates are only supported for conversion.
- For Vaccination Health Certificates the conversion requires in some examples all vaccination doses (EU-DCC barcodes) verifications to create one VDS-NC. In these cases Vaccine Prophylaxis, Vaccine Medicinal Product and Marketing Authorization Holder is only present on first dose barcode.

8.2.1.2 Mappings

VDS-NC uses WHO ICD-11 codes, while the EU uses SNOMED codes. So a mapping needs to be done between the two systems.

8.2.1.2.1 Vaccine brand (nam)

The Vaccine brand, which is encoded in the VDS-NC as “nam” and “des” is mapped from the value encoded in the field “mp” from the EU-DCC. The mapping of the values is as follows:

EU-DCC “mp” field	VDS-NC “nam” field	VDS-NC “des” field
EU/1/20/1528	Comirnaty	XM8NQ0
EU/1/20/1507	Moderna	XM3DT5
EU/1/21/1529	AstraZeneca	XM4YL8
EU/1/20/1525	Janssen	XM6QV1
CVnCoV	[not included in ICD-11 code]	
Sputnik-V	Gam-Covid-Vac	XM5ZJ4
Convidecia	Convidecia	XM1AG7
EpiVacCorona	EpiVacCorona	XM6SZ8
BBIBP-CorV	BBIBP-CorV	XM8866
Inactivated-SARS-CoV-2-Vero-Cell	Inactivated SARS-CoV-2 (Vero Cell)	XM7HT3
CoronaVac	CoronaVac	XM7HT3
Covaxin	Covaxin (also known as BBV152 A, B, C)	XM1G90
Covishield	Covishield (ChAdOx1_nCoV-19)	XM97T2

Covid-19-recombinant	Recombinant SARS-CoV-2 vaccine	XM3CT4
R-COVI	AstraZeneca	XM4YL8
CoviVac	Covi-Vac	XM85P5
Sputnik-Light	Sputnik-Light	XM5QM6
Hayat-Vax	Hayat-Vax	XM9FQ
Abdala	[not included in ICD-11 code]	
WIBP-CorV	Sinopharm WIBP-CorV	XM1AU2
MVC-COV1901	MVC-COV1901	XM4EC8
NVX-CoV2373	Novavax COVID-19 vaccine	XM9T65
EU/1/21/1618	Novavax COVID-19 vaccine	XM9T65
Covovax	Novavax COVID-19 vaccine	XM9T65
Vidprevtyn	[not included in ICD-11 code]	
VLA2001	[not included in ICD-11 code]	
EpiVacCorona-N	EpiVacCorona-N	XM3SK8
Sputnik-M	[not included in ICD-11 code]	
Covid-19-adsorvidainativada	[not included in ICD-11 code]	
NVSI-06-08	[not included in ICD-11 code]	
YS-SC2-010	[not included in ICD-11 code]	
SCTV01C	[not included in ICD-11 code]	
Covifenz	[not included in ICD-11 code]	
AZD2816	[not included in ICD-11 code]	

8.2.1.3 Issuance of Vaccine Certificate

To create a VDS-NC that consist of two doses of a vaccine, we will need to take two EU-DCC certificate, Certificate 1, which is the first dose and Certificate 2, which is the second dose. For populating each of the data elements, we will refer to the source as being C1 (for Certificate 1) and C2 (for Certificate 2). The VDS-NC consists of a Header Zone, Message Zone and a Signature Zone.

8.2.1.3.1 Message Zone (PoV Version 1)

The table below shows the populating of each data element of the Message Zone for PoV Version 1.

Object: Message {

Element	Content	From EU-DCC
UVCI (uvci)	Unique Vaccination Certificate Identifier	This field has to be uniquely generated from the issuer.

Object: PersonIdentification (pid) {

{

Element	Content	From EU-DCC
Name (n)	Name of the holder	This field is a concatenation of the last name and first name from the EU-DCC. We use the values stored in gnt and fnt, as this is the transliterated name as required by VDS-NC → C1.gnt+” “+C1.fnt

Date of birth(dob)	Date of birth of holder. ISO8601 YYYY-MM-DD	The value in dob can be copied over here. In case of EU-DCC, when month or date is unknown, the field is omitted. For VDS-NC, the handling of unknown portions is as per Doc 9303. The unknown portion is replaced with XX. For example: "1979-04-14" -> "1979-04-14" "1980" -> "1980-XX-XX" "1901-08" -> "1901-08-XX"
--------------------	--	--

→ C1.dob

UniqueIdentifier (i)	Travel Document Number	Travel document number is not included in EU-DCC. The holder of the EU-DCC will have to present his travel document for this field to be registered.
AdditionalIdentifier (ai)	Any other document number at discretion of issuer	Additional identifier is not included in EU-DCC. The holder of the EU-DCC will have to present his additional document for this field to be registered.
Sex (sex)	Sex of the holder (as specified in Doc 9303-4 Section 4.1.1.1 – Visual Inspection Zone)	EU-DCC does not have this field. It will need to be copied from the presented travel document.
}		

Array: VaccinationEvent (ve) [{

If both the doses are using the same vaccine then there is only one Vaccination Event in VDS-NC. If they are different, then it is recorded as two Vaccination events

Element	Content	From EU-DCC
Vaccine or Prophylaxis (des)	Vaccine or vaccine sub-type (ICD-11 Extension codes (http://id.who.int/icd/entity/164949870))	Use the mapping table. → C1.mp or C2.mp
Vaccine brand (nam)	Medicinal product name	Use the mapping table. → C1.mp or C2.mp
Disease or agent targeted (dis)	Disease or agent that the vaccination provides protection against (ICD-11)	Use the mapping table. → C1.tg or C2.tg

Array: VaccinationDetails (vd) [{

One instance of Vaccination Detail will be present for each of the two doses.

Date of vaccination (dvc)	Date on which the vaccine was administered. The ISO8601 full date format YYYY-MM-DD MUST be used.	→ C1.dt or C2.dt
Dose number (seq)	Vaccine dose number.	→ C1.dn or C2.dn
Country of vaccination (ctr)	The country in which the individual has been vaccinated. A three letter code identifying the issuing state or organization. The three letter code is according to Doc 9303-3.	EU-DCC uses two letter code. Conversion to three letter code is required. → C1.co or C2.co
Administering centre (adm)	The name or identifier of the vaccination facility responsible for providing the vaccination	EU-DCC does not have administering centre, but has a certificate issuer field. This may be used to populate this field. → C1.is or C2.is
Vaccine batch number (lot)	A distinctive combination of numbers and/or letters which specifically identifies a batch	EU-DCC does not contain batch number information. Leave it blank. As this field is required, it cannot be removed.
Due date of next dose (dvn)	Date on which the next vaccination should be administered. The ISO8601 full date format YYYY-MM-DD MUST be used.	EU-DCC does not contain this value. This field can be removed.
}}		
}}		
}		

8.2.1.3.2 Message Zone (PoV Version 2)

The table below shows the populating of each data element of the Message Zone for PoV Version 2.

Object: Message {

Element	Content	From EU-DCC
---------	---------	-------------

UVCI (uvci)	Unique Vaccination Certificate Identifier	This field has to be uniquely generated from the issuer.
Certificate Valid From (cvf)	Date in which the certificate for a vaccination event became valid. ISO8601 YYYY-MM-DD	Encoded in the CBOR Web Token (CWT) as "Issued At" (iat, claim key 6). → C1.iat
Certificate Valid Until (cvu)	Last date in which the certificate for a vaccination event is valid. ISO8601 YYYY-MM-DD	Encoded in the CBOR Web Token (CWT) as "Expiration Time" (exp, claim key 4). → C2.exp

Object: PersonIdentification (pid) {

{

Element	Content	From EU-DCC
Name (n)	Name of the holder	This field is a concatenation of the last name and first name from the EU-DCC. We use the value stored in gnt and fnt, as this is the transliterated name as required by VDS-NC → C1.gnt+ " "+C1.fnt
Date of birth (dob)	Date of birth of holder. ISO8601 YYYY-MM-DD	The value in dob can be copied over here. In case of EU-DCC, when month or date is unknown, the field is omitted. For VDS-NC, the handling of unknown portions is as per Doc 9303. The unknown portion is replaced with XX. For example: "1979-04-14" -> "1979-04-14" "1980" -> "1980-XX-XX" "1901-08" -> "1901-08-XX"

→ C1.dob

UniqueIdentifier(i)	Travel Document Number	Travel document number is not included in EU-DCC. The holder of the EU-DCC will have to present his travel document for this field to be registered.
AdditionalIdentifier(ai)	Any other document number at discretion of issuer	Additional identifier is not included in EU-DCC. The holder of the EU-DCC will have to present his additional document for this field to be registered.
Sex (sex)	Sex of the holder (as specified in Doc 9303-4 Section 4.1.1.1 – Visual Inspection Zone)	EU-DCC does not have this field. It will need to be copied from the presented travel document.
}		

Array: VaccinationEvent (ve) [{

If both the doses are using the same vaccine then there is only one Vaccination Event in VDS-NC. If they are different, then it is recorded as two Vaccination events

Element	Content	From EU-DCC
Vaccine or Prophylaxis (des)	Vaccine or vaccine sub-type (ICD-11 Extension codes (http://id.who.int/icd/entity/164949870))	Use the mapping table. → C1.mp or C2.mp
Vaccine brand (nam)	Medicinal product name	Use the mapping table. → C1.mp or C2.mp
Vaccine manufacturer (mfg)	Name of the manufacturer of the vaccine received. If vaccine manufacturer is unknown, market authorization holder is REQUIRED.	→ C1.ma if the value is a manufacturer
Vaccine market authorization holder (mah)	Name of the market authorization holder of the vaccine received. If market authorization holder is	→ C1.ma if the value is a market authorization holder

unknown, vaccine manufacturer is REQUIRED.

Disease or agent targeted (dis)	Disease or agent that the vaccination provides protection against (ICD-11)	Use the mapping table. → C1.tg or C2.tg
Array: VaccinationDetails (vd) [{		One instance of Vaccination Detail will be present for each of the two doses.
Date of vaccination(dvc)	Date on which the vaccine was administered. The ISO8601 full date format YYYY-MM-DD MUST be used.	→ C1.dt or C2.dt
Dose number (seq)	Vaccine dose number.	→ C1.dn or C2.dn
Total Doses(tot)	Total expected doses	→ C1.sd or C2.sd
Country of vaccination (ctr)	The country in which the individual has been vaccinated. A three letter code identifying the issuing state or organization. The three letter code is according to Doc 9303-3.	EU-DDC uses two letter code. Conversion to three letter code is required. → C1.co or C2.co
Administering centre (adm)	The name or identifier of the vaccination facility responsible for providing the vaccination	EU-DCC does not have administering centre, but has a certificate issuer field. This may be used to populate this field. → C1.is or C2.is
Vaccine batch number (lot)	A distinctive combination of numbers and/or letters which specifically identifies a batch	EU-DCC does not contain batch number information. Leave it blank. As this field is required, it cannot be removed.
Due date of next dose (dvn)	Date on which the next vaccination should be administered. The ISO8601 full date format YYYY-MM-DD MUST be used.	EU-DCC does not contain this value. This field can be removed.
}]		
}]		

OptionalDataField
(opt)

Optional data issued at the
discretion of the issuing authority

EU-DCC does not contain this
value. This field can be removed.

}

8.2.1.4 Issuance Example 1 – two doses of the same vaccine

We take the example of an EU-DCC where the two vaccination events of the same vaccine are encoded as two different barcodes.

Second Vaccination (Certificate 2)

```
{
  "JSON": {
    "ver": "1.0.0",
    "nam": {
      "fn": "Achternaam",
      "fnt": "ACHTERNAAM",
      "gn": "Voornaam",
      "gnt": "VOORNAAM"
    },
    "dob": "1964-01-01",
    "v": [
      {
        "tg": "840539006",
        "vp": "1119349007",
        "mp": "EU/1/20/1528",
        "ma": "ORG-100030215",
        "dn": 2,
        "sd": 2,
        "dt": "2021-03-11",
        "co": "AT",
        "is": "Ministry of Health Welfare and Sport",

```

```
        "ci": "urn:uvci:01:NL:ae9b7327ee6e46c68ea056eb25aba624"
    }
}
}
```

First Vaccination (Certificate 1)

```
{
  "JSON": {
    "ver": "1.0.0",
    "nam": {
      "fn": "Achternaam",
      "fnt": "ACHTERNAAM",
      "gn": "Voornaam",
      "gnt": "VOORNAAM"
    },
    "dob": "1964-01-01",
    "v": [
      {
        "tg": "840539006",
        "vp": "1119349007",
        "mp": "EU/1/20/1528",
        "ma": "ORG-100030215",
        "dn": 1,
        "sd": 2,
        "dt": "2021-02-18",
        "co": "AT",
        "is": "Ministry of Health Welfare and Sport",
        "ci": "urn:uvci:01:NL:1135b2fc930845f485d0ef5b35a922e3"
      }
    ]
  }
}
```



```
]
}
}
```

The JSON of VDS-NC PoV version 1 message will look as follows:

```
"msg":{
  "uvci":"U123890",
  "pid":{
    "n":"VOORNAAM ACHTERNAAM",
    "dob":"1964-01-01",
    "i":"A1234567Z",
    "ai":"L4567890Z",
    "sex":"M"
  },
  "ve":[{
    "des":"XM8NQ0",
    "nam":"Comirnaty",
    "dis":"RA01.0",
    "vd":[{
      "dvc":"2021-02-18",
      "seq":1,
      "ctr":"AUT",
      "adm":"Ministry of Health Welfare and Sport",
      "lot":""
    },
    {
      "dvc":"2021-03-11",
      "seq":2,
      "ctr":"AUT",
      "adm":"Ministry of Health Welfare and Sport",
      "lot":""
    }
  ]
}]
}
```

The JSON of VDS-NC PoV version 2 message will look as follows:

```
"msg":{
  "uvci":"U123890",
  "cvf":"2021-02-18",
  "cvu":"2023-02-18",
  "pid":{
    "n":"VOORNAAM ACHTERNAAM",
    "dob":"1964-01-01",
    "i":"A1234567Z",
    "ai":"L4567890Z",
    "sex":"M"
  },
  "ve":[{
    "des":"XM8NQ0",
    "nam":"Comirnaty",
    "mah":"Biontech Manufacturing GmbH",
  ]
}
```

```

        "dis": "RA01.0",
        "vd": [{
            "dvc": "2021-02-18",
            "seq": 1,
            "tot": 2,
            "ctr": "AUT",
            "adm": "Ministry of Health Welfare and Sport",
            "lot": ""
        },
        {
            "dvc": "2021-03-11",
            "seq": 2,
            "tot": 2,
            "ctr": "AUT",
            "adm": "Ministry of Health Welfare and Sport",
            "lot": ""
        }
    ]
}

```

This message can then be used to create the VDS-NC.

8.2.1.5 Issuance Example 2 – 2 doses of different vaccines

We take the example of an EU-DCC where the two vaccination events of different vaccines are encoded as two different barcodes.

Second Vaccination (Certificate 2)

```

{
  "JSON": {
    "ver": "1.0.0",
    "nam": {
      "fn": "Achternaam",
      "fnt": "ACHTERNAAM",
      "gn": "Voornaam",
      "gnt": "VOORNAAM"
    },
    "dob": "1964-01-01",
    "v": [
      {
        "tg": "840539006",
        "vp": "1119349007",
        "mp": "EU/1/20/1507",

```

```
        "ma": "ORG-100031184",
        "dn": 2,
        "sd": 2,
        "dt": "2021-03-11",
        "co": "AT",
        "is": "Ministry of Health Welfare and Sport",
        "ci": "urn:uvci:01:NL:ae9b7327ee6e46c68ea056eb25aba624"
    }
]
}
}
```

First Vaccination (Certificate 1)

```
{
  "JSON": {
    "ver": "1.0.0",
    "nam": {
      "fn": "Achternaam",
      "fnt": "ACHTERNAAM",
      "gn": "Voornaam",
      "gnt": "VOORNAAM"
    },
    "dob": "1964-01-01",
    "v": [
      {
        "tg": "840539006",
        "vp": "1119349007",
        "mp": "EU/1/20/1528",
        "ma": "ORG-100030215",
        "dn": 1,

```

```

        "sd": 2,

        "dt": "2021-02-18",

        "co": "AT",

        "is": "Ministry of Health Welfare and Sport",

        "ci": "urn:uvci:01:NL:1135b2fc930845f485d0ef5b35a922e3"

    }

]

}

}

```

The JSON of VDS-NC PoV version 1 message will look as follows:

```

"msg": {
  "uvci": "U123890",
  "pid": {
    "n": "VOORNAAM ACHTERNAAM",
    "dob": "1964-01-01",
    "sex": "M",
    "i": "A1234567Z",
    "ai": "L4567890Z"
  },
  "ve": [{
    "des": "XM8NQ0",
    "nam": "Comirnaty",
    "dis": "RA01.0",
    "vd": [{
      "dvc": "2021-02-18",
      "seq": 1,
      "ctr": "AUT",
      "adm": "Ministry of Health Welfare and Sport",
      "lot": ""
    }]
  },
  {
    "des": "XM3DT5",
    "nam": "Moderna",
    "dis": "RA01.0",
    "vd": [{
      "dvc": "2021-03-11",
      "seq": 2,
      "ctr": "AUT",
      "adm": "Ministry of Health Welfare and Sport",
      "lot": ""
    }]
  }
]
}

```

```
}
```

The JSON of VDS-NC PoV version 2 message will look as follows:

```
"msg": {
  "uvci": "U123890",
  "cvf": "2021-02-18",
  "cvu": "2023-02-18",
  "pid": {
    "n": "VOORNAAM ACHTERNAAM",
    "dob": "1964-01-01",
    "sex": "M",
    "i": "A1234567Z",
    "ai": "L4567890Z"
  },
  "ve": [{
    "des": "XM8NQ0",
    "nam": "Comirnaty",
    "mah": "Biontech Manufacturing GmbH",
    "dis": "RA01.0",
    "vd": [{
      "dvc": "2021-02-18",
      "seq": 1,
      "tot": 2,
      "ctr": "AUT",
      "adm": "Ministry of Health Welfare and Sport",
      "lot": ""
    }]
  },
  {
    "des": "XM3DT5",
    "nam": "Moderna",
    "mfg": "Rovi Pharma Industrial Services, S.A.",
    "mah": "Moderna Biotech Spain S.L.",
    "dis": "RA01.0",
    "vd": [{
      "dvc": "2021-03-11",
      "seq": 2,
      "tot": 2,
      "ctr": "AUT",
      "adm": "Ministry of Health Welfare and Sport",
      "lot": ""
    }]
  }
]
}
```

8.2.2 Creating a EU-DCC using a VDS-NC

8.2.2.1 Prerequisites & Scope

- Vaccination, Test and Recovery Health Certificates are only supported for conversion.
- For Vaccination Health Certificates the conversion requires to create an EU-DCC for each vaccination dose from a single VDS-NC.

8.2.2.2 Mappings

VDS-NC uses WHO ICD-11 codes, while the EU uses SNOMED codes. So a mapping needs to be done between the two systems.

8.2.2.2.1 Vaccine Product

The Vaccine Product field, which is encoded as “mp” in EU-DCC is populated from the “des” field of the VDS-NC. The following mapping is to be used:

VDS-NC(des field)	EU-DCC(mp field)	EU-DCC(vp field)	Name
XM8NQ0	EU/1/20/1528	1119349007	Comirnaty
XM3DT5	EU/1/20/1507		Moderna
XM4YL8	EU/1/21/1529	J07BX03	Vaxzevria
	R-COVI		AstraZeneca
XM6QV1	EU/1/20/1525		COVID-19 Vaccine Janssen
XM9T65	NVX-CoV2373		NVX-CoV2373
XM1AG7	Convidecia		Convidecia
XM6SZ8	EpiVacCorona		EpiVacCorona
XM3SK8	EpiVacCorona-N		Do not confuse with EpiVacCorona. Also know as Aurora-CoV.
XM8866	BBIBP-CorV		BBIBP-CorV
XM9TQ1	Inactivated-SARS-CoV-2-Vero-Cell		Inactivated SARS-CoV-2 (Vero Cell)

XM7HT3	CoronaVac		CoronaVac
XM1G90	Covaxin		Covaxin (also known as BBV152 A, B, C)
XM97T2	Covishield		Covishield (ChAdOx1_nCoV-19)
XM3CT4	Covid-19-recombinant		Recombinant SARS-CoV-2 vaccine
XM85P5	CoviVac		Covi-Vac
XM5ZJ4	Sputnik-V		Gam-Covid-Vac
XM5QM6	Sputnik-Light		Sputnik-Light
XM9FQ7	Hayat-Vax		Hayat-Vax
XM1AU2	WIBP-CorV		Sinopharm WIBP-CorV
XM4EC8	MVC-COV1901		MVC-COV1901
XM9T65	EU/1/21/1618		Novavax COVID-19 vaccine
	Covovax		Covovax
XM52P3	[Not included in EU-DCC vp list]		ZyCov-D
XM3PG0	[Not included in EU-DCC vp list]		Soberana-02
XM0RV9	[Not included in EU-DCC vp list]		Soberana Plus
XM9P21	[Not included in EU-DCC vp list]		SpikoGen
XM9N08	[Not included in EU-DCC vp list]		Razi COV PARS
XM97N6	[Not included in EU-DCC vp list]		QazVac
XM2YG8	[Not included in EU-DCC vp list]		COVIran Barakat

XM0K39	[Not included in EU-DCC vp list]		Covidful
--------	----------------------------------	--	----------

Before the codification of individual vaccines, some countries have issued a VDS-NC using the generic coding values derived from WHO ICD-11. The following table covers the conversion for such PoVs.

VDS-NC(des field)	VDS-NC(nam field)	EU-DCC(mp field)	EU-DCC(vp field)
XM0GQ8	COMIRNATY	EU/1/20/1528	1119349007
XM0GQ8	COVID-19 Vaccine Moderna	EU/1/20/1507	
XM9QW8	Vaxzevria	EU/1/21/1529	J07BX03

8.2.2.2.2 Vaccine Marketing Authorisation Holder or Manufacturer

The Vaccine market authorization holder or manufacturer, which is encoded in the EU-DCC as “ma”, is populated from the “mah” field of the VDS-NC. Following WHO guidelines, the mah field of the VDS-NC is left to the discretion of the issuing state, as the mechanism to assign a Market Authorization Holder code will be dependent on their own rules and regulations. So, a direct mapping is not possible to define. However, the following table attempts to detail the mapping between different manufacturing entities to the EU-DCC ma value. This is provided as a guide, but is not authoritative or normative in scope:

VDS-NC (mah field)	EU DCC code
AstraZeneca AB	ORG-100001699
Biontech Manufacturing GmbH	ORG-100030215
Janssen-Cilag International	ORG-100001417
Moderna Biotech Spain S.L.	ORG-100031184
Curevac AG	ORG-100006270
CanSino Biologics	ORG-100013793

China Sinopharm International Corp. - Beijing location	ORG-100020693
Sinopharm Weiqida Europe Pharmaceutical s.r.o. - Prague location	ORG-100010771
Sinopharm Zhijun (Shenzhen) Pharmaceutical Co. Ltd. - Shenzhen location	ORG-100024420
Novavax CZ AS	ORG-100032020
Gamaleya Research Institute	Gamaleya-Research-Institute
Vector Institute	Vector-Institute
Sinovac Biotech	Sinovac-Biotech
Bharat Biotech	Bharat-Biotech
Serum Institute Of India Private Limited	ORG-100001981
Fiocruz	Fiocruz
R-Pharm CJSC	ORG-100007893
Chumakov Federal Scientific Center for Research and Development of Immune-andBiological Products	Chumakov-Federal-Scientific-Center
Gulf Pharmaceutical Industries	ORG-100023050
Center for Genetic Engineering and Biotechnology (CIGB)	CIGB
Sinopharm - Wuhan Institute of Biological Products	Sinopharm-WIBP
Medigen Vaccine Biologics Corporation	ORG-100033914
Sanofi Pasteur	ORG-100000788
Valneva France	ORG-100036422
Instituto Butantan	Instituto-Butantan
National Vaccine and Serum Institute, China	NVSI
YishengBiopharma--Yisheng-BiopharmaSinocelltech Ltd	ORG-100026614
Medicago Inc	ORG-100008549

8.2.2.2.3 Country Code Conversion

The EU-DCC uses ISO 3166 2-letter country codes. VDS-NC uses the DOC 9303 3-letter country codes. The Doc 9303 codes are identical to the ISO 3166 codes except for a few extra codes defined in Doc 9303. For the normal codes, ISO 3166 can be used to do the conversion. The following table lists the other codes from Doc 9303.

British Overseas Territories Citizen	GB	GBD
British National (Overseas)	GB	GBN
British Overseas Citizen	GB	GBO
British Subject	GB	GBS
British Protected person	GB	GBP
Republic of Kosovo	KS	RKS
European Union (EU)	EU	EUE
Netherlands Antilles	AN	ANT
Neutral Zone	NT	NTZ

8.2.2.3 Issuance of a Vaccine Certificate

To create an EU DCC based on VDS-NC, the following conversion should be applied.

Target field in EUDCC	Content	Source field in ICAO VDS-NC	Instruction
General contents			
nam/fn	Surname(s)	name (n)	Part of the name until the first space symbol
nam/fnt	Standardised surname(s)	name (n)	Part of the name until the first space symbol, transliterated according to ICAO 9303 Part 3 rules.

			"If the part of the name until the first space symbol" is not a Surname, the convention rule specified in Doc 9303-3, 3.4 is applicable."
nam/gn	Forename(s)	name (n)	Part of the name after the first space symbol "If the part of the name until the first space symbol" is not a Surname, the convention rule specified in Doc 9303-3, 3.4 is applicable."
nam/gnt	Standardised forename(s)	name (n)	Part of the name after the first space symbol, transliterated according to ICAO 9303 Part 3 rules
dob	Date of birth	date of birth (dob)	Copy contents from the dob field, remove any "-XX" substrings
v/tg	Disease or agent targeted: COVID-19 (SARS-CoV or one of its variants)	Disease or agent targeted (dis)	If the value is other than "RA01.0", stop conversion and reject the certificate. Otherwise, use the value "tg": "840539006".
v/vp	COVID-19 vaccine or prophylaxis	Vaccine or Prophylaxis (des)	Use the conversion table "Vaccine type conversion"
v/mp	COVID-19 vaccine product	Vaccine brand (nam)	Use the conversion table "Vaccine name conversion"
v/ma	COVID-19 vaccine marketing authorisation holder or manufacturer	none	Use the conversion table "MAH conversion" table
v/dn	Number in a series of doses	Dose number (seq)	If the VDS-NC certificate includes two or more doses, generate a different EU DCC for each of these, taking the corresponding seq value.

v/sd	The overall number of doses in the series	none	If the VDS-NC certificate includes two or more doses, generate a different EU DCC for each of these, and include the maximum seq value as the overall number of doses. If the VDS-NC certificate total doses includes one dose, use the value indicating the total number of doses needed for a full primary vaccination series, depending on the vaccine product.
v/dt	Date of vaccination	Date of vaccination (dvc)	If the VDS-NC certificate includes two or more doses, generate a different EU DCC for each of these, taking the corresponding dvc value.
v/co	Member State or third country in which the vaccine was administered	Country of vaccination (ctr)	If the VDS-NC certificate includes two or more doses, generate a different EU DCC for each of these, taking the corresponding ctr value. Apply conversion to the two-letter ISO 3166 Part 1 code.
v/is	Certificate issuer	Administering centre (adm)	If the VDS-NC certificate includes two or more doses, generate a different EU DCC for each of these, taking the corresponding adm value.
v/ci	Unique certificate identifier	UVCI (uvci)	Use value "URN:UVCI:01:" + value of hdr/is converted to the two-letter ISO 3166 Part 1 code + uvci + "/1" or "/2" if the VDS-NC certificate includes two or more doses, and a separate EU DCC must be generated for each of these + "#" + checksum. "+" is the concatenation mark.

8.2.2.3.1 Issuance Example 1 – two doses of the same vaccine

We take the example of a VDS-NC where the two same vaccine are encoded in one barcode.

Source: [Visible Digital Seal-NC v1.3 document](#). (Annex C Worked Example – PoV Version 2 (Informative))

```
{
  "data": {
    "hdr": {
      "t": "icao.vacc",
      "v": 2,
      "is": "UTO"
    },
    "msg": {
      "uvci": "U32870",
      "cvf": "2021-12-03",
      "cvu": "2022-12-03",
      "pid": {
        "n": "Smith Bill",
        "dob": "1990-01-02",
        "sex": "M",
        "i": "A1234567Z",
        "ai": "L4567890Z"
      },
      "ve": [
        {
          "des": "XM8NQ0",
          "nam": "Comirnaty",
          "mfg": "Pfizer Europe MA EEIG",
          "mah": "BioNTech Manufacturing GmbH",
          "dis": "RA01.0",
          "vd": [
            {
              "dvc": "2021-12-03",
              "seq": 1,
            }
          ]
        }
      ]
    }
  }
}
```

```

        "tot":2,
        "ctr":"UTO",
        "adm":"RIVM",
        "lot":"VC35679",
        "dvn":"2021-12-24"
    },
    {
        "dvc":"2021-12-24",
        "seq":2,
        "tot":2,
        "ctr":"UTO",
        "adm":"RIVM",
        "lot":"VC87540"
    }
}],
    "opt":"Recovered COVID-19 patient"
}
},
"sig":{
    "alg":"ES256",
    "cer":"MIIBfTCCASCgAwIBAgIBbDAMBggqhkiZOPQD...",
    "sigv1":"xqlZ8THzT0ilT2GjRPR93mf5lW58Xlo6-F..."
}
}

```

The JSON will then look as follows:

Dose 1:

```

{
  "JSON": {
    "ver": "1.0.0",
    "nam": {
      "fn": "Smith",
      "fnt": " SMITH",
      "gn": "Bill",
      "gnt": "BILL"
    }
  }
}

```

```

    },
    "dob": "1990-01-02",
    "v": [
      {
        "tg": "840539006",
        "vp": "1119349007",
        "mp": "EU/1/20/1528",
        "ma": "ORG100030215",
        "dn": 1,
        "sd": 2,
        "dt": "2021-12-03",
        "co": "UT",
        "is": "RIVM",
        "ci": "urn:uvci:01:UT:183464890179545bba1c279f592f2488a"
      }
    ]
  }
}
Dose 2:
{
  "JSON": {
    "ver": "1.0.0",
    "nam": {
      "fn": "Smith",
      "fnt": " SMITH",
      "gn": "Bill",
      "gnt": "BILL"
    },
    "dob": "1990-01-02",
    "v": [
      {
        "tg": "840539006",
        "vp": "1119349007",
        "mp": "EU/1/20/1528",
        "ma": "ORG100030215",
        "dn": 2,
        "sd": 2,
        "dt": "2021-12-24",
        "co": "UT",
        "is": "RIVM",
        "ci": "urn:uvci:01:UT:76482016487215bafa1c279f592f2432a"
      }
    ]
  }
}

```

8.2.2.3.2 Issuance Example 2 – 2 doses of different vaccines

We take the example of a VDS-NC where the two different vaccine are encoded in one barcode.

Source: [Visible Digital Seal-NC v1.3 document. \(Annex C Worked Example – PoV Version 2 \(Informative\)\)](#)

```
{
```

```
"data":{
  "hdr":{
    "t":"icao.vacc",
    "v":2,
    "is":"UTO" },
  "msg":{
    "uvci":"U32879",
    "cvf":"2021-12-03",
    "cvu":"2022-12-03",
    "pid":{
      "n":"Smith Bill",
      "dob":"1990-01-02",
      "sex":"M",
      "i":"A1234567Z",
      "ai":"L4567890Z" },
    "ve":[{"
      "des":"XM8NQ0",
      "nam":"Comirnaty",
      "mfg":"Pfizer Europe MA EEIG",
      "mah":"BioNTech Manufacturing GmbH",
      "dis":"RA01.0",
      "vd":[{"
        "dvc":"2021-12-03",
        "seq":1,
        "tot":2,
        "ctr":"UTO",
        "adm":"RIVM",
        "lot":"VC35679",
        "dvn":"2021-12-24" }]
    }],
  }
```



```
        "des": "XM3DT5",
        "nam": "Moderna",
        "mfg": "Rovi Pharma Industrial Services, S.A.",
        "mah": "Moderna Biotech Spain, S.L.",
        "dis": "RA01.0", "vd": [{
            "dvc": "2021-12-24",
            "seq": 2,
            "tot": 2,
            "ctr": "SGP",
            "adm": "NUH",
            "lot": "VC99537" }]
    }],
    "opt": "Recovered COVID-19 patient" }
},
"sig": {
    "alg": "ES256",
    "cer": "MIIBfTCCASCgAwIBAgIBbDAMBggqhkiZOPQD...",
    "sigv1": "gKVP4S-MBL98bTiUciOQt5hYfLi_zy6Wko..."
}
}
```

The JSON will then look as follows:

Dose 1:

```
{
  "JSON": {
    "ver": "1.0.0",
    "nam": {
      "fn": "Smith",
      "fnt": " SMITH",
      "gn": "Bill",
      "gnt": "BILL"
    },
    "dob": "1990-01-02",
    "v": [
      {
        "tg": "840539006",
```

```

        "vp": "1119349007",
        "mp": "EU/1/20/1528",
        "ma": "ORG100030215",
        "dn": 1,
        "sd": 2,
        "dt": "2021-12-03",
        "co": "UT",
        "is": "RIVM",
        "ci": "urn:uvci:01:UT:87539274518293dba1c273f552f2458a"
    }
  ]
}
}
Dose 2:
{
  "JSON": {
    "ver": "1.0.0",
    "nam": {
      "fn": "Smith",
      "fnt": " SMITH",
      "gn": "Bill",
      "gnt": "BILL"
    },
    "dob": "1990-01-02",
    "v": [
      {
        "tg": "840539006",
        "vp": "1119349007",
        "mp": "EU/1/20/1507",
        "ma": "ORG-100031184",
        "dn": 2,
        "sd": 2,
        "dt": "2021-12-24",
        "co": "SG",
        "is": "NUH",
        "ci": "urn:uvci:01:SG:54371927345642abd1c279f591f2498a"
      }
    ]
  }
}

```

8.3 Proof of Recovery

8.3.1 Creating a VDS-NC using an EU-DCC

8.3.1.1 *Issuance of Recovery Certificate*

A VDS-NC Proof of Recovery (PoR) can be created using an EU-DCC recovery certificate. For populating each of the data elements, we will refer to the EU-DCC recovery certificate as being C.

Object: Message {

Element	Content	From EU-DCC
URCI (urci)	Unique Recovery Certificate Identifier	This field has to be uniquely generated from the issuer.
Certificate Valid From (cvf)	Date in which the certificate for a test result became valid. ISO8601 YYYY-MM-DD	→ C.df
Certificate Valid Until (cvu)	Last date in which the certificate for a test result is valid. ISO8601 YYYY-MM-DD	→ C.du

Object: PersonalInformation(pid) {

Element	Content	
Name (n)	Name of the holder (as specified in Doc 9303-3) MUST be used.	This field is a concatenation of the last name and first name from the EU-DCC. We use the values stored in gnt and fnt, as this is the transliterated name as required by VDS-NC → C.gnt+ " "+C.fnt
DOB (dob)	The DOB of the test subject. The [RFC 3339] full date format YYYY-MM-DD MUST be used.	The value in dob can be copied over here. In case of EU-DCC, when month or date is unknown, the field is omitted. For VDS-NC, the handling of unknown portions is as per Doc 9303. The unknown portion is replaced with XX. For example: "1979-04-14" -> "1979-04-14" "1980" -> "1980-XX-XX" "1901-08" -> "1901-08-XX" → C.dob

DocType (dt)	The ID Document Type of the identity document MUST be used. Only these values MUST be used: P – Passport (Doc 9303-4) A – ID Card (Doc 9303-5) C – ID Card (Doc 9303-5) I – ID Card (Doc 9303-5) AC - Crew Member Certificate (Doc 9303-5) V – Visa (Doc 9303-7) D – Driving License (ISO 18013-1)	Document type is not included in EU-DCC. The holder of the EU-DCC will have to present his document for this field to be registered.
--------------	---	--

DocNum (dn)	The ID Document Number of the identity document MUST be used of the document used in DocType. The ID Document Number is the unique identifier of the test subject.	Document number is not included in EU-DCC. The holder of the EU-DCC will have to present his document for this field to be registered.
-------------	--	--

}

Object: TestResult (tr) {

Element	Content	
Member state of test (sot)	Three letter code identifying the country of test.	EU-DDC uses two letter code. Conversion to three letter code is required. ➔ C.co
Date of first positive NAAT test result (dnt)	The date when a sample for the NAAT test producing a positive result was collected. ISO8601 YYYY-MM-DD	➔ C.fr Note: currently EU-DCC recovery certificates may be issued based on a Rapid Antigen test (ART). ICAO CAPSCA follows WHO specification and recognises only NAAT

tests. Conversion from ART to NAAT is left to the discretion of the issuer.

}

Element	Content	
OptionalDataField (opt)	Optional data issued at the discretion of the issuing authority	EU-DCC does not contain this value. This field can be omitted.

}

8.3.1.2 Issuance Example

We take the example of an EU-DCC recovery certificate.

```
{
  "JSON": {
    "ver": "1.0.0",
    "nam": {
      "fn": "Achternaam",
      "fnt": "ACHTERNAAM",
      "gn": "Voornaam",
      "gnt": "VOORNAAM"
    },
    "dob": "1964-01-01",
    "r": [
      {
        "tg": "840539006",
        "fr": "2021-03-25",
        "co": "GR",
        "is": "Ministry of Health Welfare and Sport",
```

```

        "df": "2021-04-12",

        "du": "2021-07-12",

        "ci": "urn:uvci:01:NL:0b34da1923fa4387a00087feda9bea9f"

    }

]

}

}

```

The JSON of VDS-NC PoR message will look as follows:

```

"msg":{
  "urci":"U56900",
  "cvf":"2021-04-12",
  "cvu":"2021-07-12",
  "pid":{
    "n":"VOORNAAM ACHTERNAAM",
    "dob":"1964-01-01",
    "dt":"P",
    "dn":"E7654321K"
  },
  "tr":{
    "sot":"GRC",
    "dnt":"2021-03-25"
  }
}

```

This message can then be used to create the VDS-NC.

8.3.2 Creating a EU-DCC using a VDS-NC

8.3.2.1 *Issuance of Recovery Certificate*

To create an EU DCC based on VDS-NC, the following conversion should be applied.

Target field in EUDCC	Content	Source field in ICAO VDS-NC	Instruction
General contents			
nam/fn	Surname(s)	name (n)	Part of the name until the first space symbol
nam/fnt	Standardised surname(s)	name (n)	Part of the name until the first space symbol, transliterated

			according to ICAO 9303 Part 3 rules
nam/gn	Forename(s)	name (n)	Part of the name after the first space symbol
nam/gnt	Standardised forename(s)	name (n)	Part of the name after the first space symbol, transliterated according to ICAO 9303 Part 3 rules
dob	Date of birth	date of birth (dob)	Copy contents from the dob field, remove any "-XX" substrings
r/tg	Disease or agent targeted: COVID-19 (SARS-CoV or one of its variants)	[Not Present]	VDS-NC Proof of Recovery is only targeted for COVID-19. Use the value "tg": "840539006".
r/co	Country of test	Member state of test(sot)	Use the conversion table "MAH conversion" table
r/fr	Date of first positive NAAT test result	Date of first positive NAAT test result (dnt)	
r/is	Certificate issuer	[Not Present]	
r/df	Certificate Valid From	Certificate Valid From (cvf)	
r/du	Certificate Valid Until	Certificate Valid Until (cvu)	

r/ci	Unique certificate identifier	UVCI (uvci)	Use value "URN:UVCI:01:" + value of hdr/is converted to the two-letter ISO 3166 Part 1 code + uvci + "/1" or "/2"
------	-------------------------------	-------------	---

8.3.2.2 Issuance Example

We take the example of a VDS-NC proof of recovery.

Source: [Visible Digital Seal-NC v1.3 document. \(Annex E Worked Example – PoR \(Informative\)\)](#)

```
{
  "data": {
    "hdr": {
      "t": "icao.rcvy",
      "v": 1,
      "is": "UTO"
    },
    "msg": {
      "urci": "U56900",
      "cvf": "2021-02-01",
      "cvu": "2021-05-01",
      "pid": {
        "n": "Green Martin",
        "dob": "1978-03-08",
        "dt": "P",
        "dn": "E7654321K"
      },
      "tr": {
        "sot": "UTO",
        "dnt": "2021-01-06"
      }
    }
  }
}
```



```
        "opt": "ID1234567"
    }
},
"sig": {
    "alg": "ES256",
    "cref": "UT6F",
    "sigv1": "0hnZ0ZsjTsY5K39DvVBFxWO73uUHBfY..."
}
}
```

The JSON will then look as follows:

```
{
  "ver": "1.3.1",
  "nam": {
    "fn": "Green",
    "fnt": "GREEN",
    "gn": "Martin",
    "gnt": "MARTIN"
  },
  "dob": "1978-03-08",
  "r": [
    {
      "tg": "840539006",
      "fr": "2021-01-06",
      "co": "UT",
      "is": "", //NOT INCLUDED IN VDS-NC PoR
      "df": "2021-02-01",
      "du": "2021-05-01",
      "ci": "URN:UVCI:01:UT:DEBFCC47C4534E45A906DE81FD859FB6"
    }
  ]
}
```