# MACHINE READABLE TRAVEL DOCUMENTS



# TECHNICAL REPORT

## VDS-NC

**Visible Digital Seal for non-constrained environments**
Version – 1.0
Date – April 23, 2021

**ISO/IEC JTC1 SC17 WG3/TF5**
**FOR THE**
**INTERNATIONAL CIVIL AVIATION ORGANIZATION**

## Release Control

| Release | Date | Description |
|---------|------|-------------|
| 0.01 | Feb 2021 | Initial Draft capturing the discussions in MDWG and subset of TF5 |
| 0.02 | Feb 2021 | Included Worked examples |
| 0.03 | Feb 2021 | Minor fixes to JSON schema |
| 0.04 | Mar 2021 | Added ID (identifier) for schema |
| 0.05 | Apr 2021 | Changes after Comment Resolution Meeting (March 30) |
| 1.0 | Apr 2021 | Final release after NTWG/WG3 combined meeting (19 April, 2021) |

**TABLE OF CONTENTS**

# 1. Introduction

Doc9303-13 defines the Visible Digital Seal for Non-Electronic documents. Doc 9303-7 and Doc 9303-8 also presents two profiles for Visa Stickers and Emergency Travel documents. Both these use cases have a constraint on the amount of real estate available to print the 2D barcodes and hence, has been defined with a binary format with an emphasis on the size of the resulting 2D barcode. As a result, special scanners with associated software are required to read the barcode and to be able to decode it.

For use cases that do not have the constraint of real estate available for printing the barcode, a new format for Visible Digital Seal for non-constrained environments is presented in this technical report. The approach – VDS-NC – has the following advantages.

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.
3. The data extracted by the barcode reader is human readable except for the signer certificate and the signature value

The VDS-NC is a general definition and can be used for any situation where the size of the barcode is not a serious constraint. The specification details the structure, the trust framework and the signature component. Two health related use cases are also described in this TR. Further use cases will be added to this TR as the necessity arises.

# 2. Terminology and Definitions

## 2.1 Technical report terminology

The key words "MUST", "MUST NOT", "SHALL", "SHALL NOT", "REQUIRED", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC 2119].

1. MUST
2. This word, or the terms "REQUIRED" or "SHALL", means that the definition is an absolute requirement of the specification.

MUST NOT
This phrase, or the phrase "SHALL NOT", means that the definition is an absolute prohibition of the specification.

SHOULD
This word, or the adjective "RECOMMENDED", means that there may exist valid reasons in particular circumstances to ignore a particular item, but the full implications must be understood and carefully weighed before choosing a different course.

SHOULD NOT
This phrase, or the phrase "NOT RECOMMENDED" means that there may exist valid reasons in particular circumstances when the particular behaviour is acceptable or even useful, but the full implications should be understood and the case carefully weighed before implementing any behaviour described with this label.

MAY
This word, or the adjective "OPTIONAL", means that an item is truly optional. One user may choose to include the item because a particular application requires it or because the user feels that it enhances the application while another user may omit the same item. An

implementation which does not include a particular option MUST be prepared to interoperate with another implementation which does include the option, though perhaps with reduced functionality. In the same vein an implementation which does include a particular option MUST be prepared to interoperate with another implementation which does not include the option (except, of course, for the feature the option provides).

CONDITIONAL          The usage of an item is dependent on the usage of other items. It is therefore further qualified under which conditions the item is REQUIRED or RECOMMENDED. This is an additional key word used in Doc 9303 (not part of RFC 2119).

In case OPTIONAL features are implemented, they MUST be implemented as described in this Technical Report.

## 2.2 Terms and Definitions

| Term | Definition |
|------|------------|
| VDS | Visible Digital Seal |
| VDS-NC | Visible Digital Seal for Non Constrained environments |
| PoT | Proof of Testing |
| PoV | Proof of Vaccination |

# 3. Encoding

The VDS-NC is a cryptographically signed data structure containing information encoded as a 2D barcode. It can be printed on a document or issued in the form of a graphic for presentation using a device (e.g. smart phone). The barcode SHOULD be printed in accordance with Doc 9303-13.  This section gives the definitions of the encoding and structure of a VDS-NC.

## 3.1 JSON
The data structure is defined using JSON (JavaScript Object Notation), a lightweight data-interchange format which is easy for humans to read and write. The data MUST be represented as a JSON data Interchange format in accordance with [RFC 7493] which specifies "Internet JSON" (I-JSON).

For date and time fields [RFC 3339] MUST be applied.

Note: In case the date represents a Date of Birth and if parts of the date are not known, refer to Doc 9303-3 for guidance on handling such dates.

## 3.2 Languages and Characters

Latin-alphabet characters SHALL be used to represent data. Latin-based national characters MUST be transliterated according to Doc 9303-3. When data elements are in a language that does not use the Latin alphabet, a transcription or transliteration such as the one defined in Doc 9303-3 MUST be used.

Note: For avoidance of any doubt, only the characters listed below are allowed:
A – Z
a – z
0 - 9
!@#$%&'*+-/=?^_`{|}~.

## 3.3 Barcode Format

Only the following symbologies SHALL be used for 2D barcodes:
- DataMatrix [ISO/IEC 16022]
- Aztec Codes [ISO/IEC 24778]
- QR Codes [ISO/IEC 18004]

Note: Barcodes may be added to this list in the future.

Given the wider availability of scanners that support QR codes, it is RECOMMENDED that the barcode is encoded as a QR code.

The encoded barcode consists of a data zone and a signature zone.

*Table* 1*: Overall Structure*

| | Information |
|---|---|
| { | |
| **Object: `data {`** | Contains `Header` and `Message`; To be signed data |
| **Object: `Header(hdr)`** | Contains information about type of message and issuing State or organization. |
| **Object: `Message(msg)`** | message |
| } | |
| **Object: `Signature(sig)`** | Only REQUIRED if data is signed. If not, this MUST NOT be present |
| } | |

For ICAO's use cases the JSON schema for the VDS-NC MUST be as follows (for national use cases further national messages MAY be used):

```
{
    "$id": "http://namespaces.icao.int/VDS-NC.json",
    "title": "VDS-NC",
    "type": "object",
    "description": "VDS-NC Schema",
    "properties": {
```

```
    "data": {
        "type": "object",
        "properties": {
            "hdr": {
                "$ref": "http://namespaces.icao.int/VDS-
NC_header.json"
            },
            "msg": {
                "oneOf": [{
                    "$ref": "http://namespaces.icao.int/VDS-
NC_message_PoV_WHO.json"
                },
                {
                    "$ref": "http://namespaces.icao.int/VDS-
NC_message_PoT_ICAO.json"
                }]

            },
            "additionalProperties": false
        },
        "required": ["hdr",
        "msg"],
        "additionalProperties": false
    },
    "sig": {
        "$ref": "http://namespaces.icao.int/VDS-NC_signature.json"
    }
  }
}
```

## 3.4 Data Zone

The data zone contains two zones, the header zone and the message zone.

### 3.4.1 Header Zone

The header contains the metadata about the information encoded in the barcode, such as a version number and the type of information encoded.

*Table 2: Format of the Header*

{

**Object: `Header(hdr)` {**

| Element | Content |
|---|---|
| Type(t) | Type is set to "icao.test" for PoT (data defined by CAPSCA), "icao.vacc" for PoV (data defined by WHO). Other Types may be added in the future |
| Version(v) | Each of the use cases will define a version number for the structure. In case of changes in structure, the version number will be incremented. |

| | |
|---|---|
| IssuingCountry(is) | A three letter code identifying the issuing state or organization. The three letter code is according to Doc 9303-3. |

| |
|---|
|     } |

| |
|---|
| } |

Note: The Type field for ICAO use cases will start with "icao" followed by the use case after the ".". If VDS-NC is re-used for use cases not specified by ICAO, i.e. national purposes, the Type (t) element MUST start with the country code according to Doc 9303-3 followed by a period.
Example: "uto.usecase"

The JSON schema for the Header MUST be as follows:

```
{
      "$id": "http://namespaces.icao.int/VDS-NC_header.json",
      "title": "Header",
      "type": "object",
      "description": "Header Schema",
      "properties": {
            "t": {
                  "type": "string",
                  "enum": ["icao.test",
                  "icao.vacc"
                  ]
            },
            "v": {
                  "type": "integer"
            },

            "is": {
                  "type": "string"
            }
      },
"required": ["t",
      "v",
      "is"],
      "additionalProperties": false
}
```

### 3.4.2 Message Zone

The message zone contains the actual data as I-JSON and is defined in the respective profiles.

## 3.5 Signature Zone

The signature zone consists of the following elements:

*Table* 3: *Format of the Signature Zone*

| |
|---|
| { |

| Object: `Signature(sig)` { | |
|---|---|
| Element | Content |
| `SignatureAlgo(alg)` | The signature algorithm used to produce the signature. Signatures MUST be ECDSA. A key length of 256 bit in combination with SHA-256(at the time this document is created) is RECOMMENDED. |
| `Certificate(cer)` | X.509 signer certificate in base64url [RFC 4648] |
| `SignatureValue(sigvl)` | Signature value signed over the Data in base64url [RFC 4648] |
| } | |
| } | |

Note:

The SignatureAlgo field MUST be only one of the following values:
ES256 – denotes ECDSA with Sha256 hashing algorithm
ES384 – denotes ECDSA with Sha384 hashing algorithm
ES512 – denotes ECDSA with Sha512 hashing algorithm


The JSON schema for the Signature Zone MUST be as follows:

```
{
      "$id": "http://namespaces.icao.int/VDS-NC_signature.json",
      "title": "Signature Zone",
      "type": "object",
      "description": "Signature Schema",
      "properties": {
           "alg": {
                "type": "string",
                "description": "The signature algorithm used to produce the
signature"
           },
           "cer": {
                "type": "string",

"description": "X.509 signer certificate in base64url encoding"
           },
           "signvl": {
                "type": "string",
                "description": "Signature value signed over the Data in
base64url encoding"
           }
      },
      "required": ["alg",
      "cer",
      "signvl"],
      "additionalProperties": false
}
```

### 3.5.1 Signature Semantics

The content of the Data Object is the input to the Signature generation process.

To avoid any ambiguity in the data-to-be-signed, the JSON Canonicalization Scheme (JCS) as defined in [RFC 8785] MUST be applied on the JSON data before generating the signature and before validating the signature.

## 3.6 Public Key Infrastructure (PKI) and Certificate Profiles

All Signer certificates used for this specification will fall under the following OID branch:

```
id-icao OBJECT IDENTIFIER ::= {2.23.136}
id-icao-mrtd OBJECT IDENTIFIER ::= {id-icao 1}
id-icao-mrtd-security OBJECT IDENTIFIER ::= {id-icao-mrtd 1}
id-icao-VDS-NC OBJECT IDENTIFIER ::= {id-icao-mrtd-security 14}
```

### 3.6.1 Certificate Authorities (CAs) Hierarchy

It is RECOMMENDED that the CSCA used for issuing document signers for travel documents is also used for issuing the barcode signers for VDS-NC.

### 3.6.2 CSCA Profile

If the barcode signer is issued under the CSCA, there is no change in the CSCA profile.

If a different root of trust is used for the issuance of the barcode signers, then the separate CA MUST comply with the CSCA specifications of Doc 9303-12 with the following restrictions:

EKU extension MUST be included in the separate CA. The validation algorithm MUST ensure that the particular EKU as defined in this document is absent in the CSCA used for travel document. The OID for EKU for the separate CA is "2.23.136.1.1.14.1"

### 3.6.3 Barcode Signer Certificate Profile

The barcode signer MUST comply with the barcode signer certificate profile defined in 9303-12, with the following restriction:

- the VDS-NC signer key-pair MUST be of ECC type
- The EKU OID for VDS-NC Signers is "2.23.136.1.1.14.2".
- DocumentType extension MUST be present. It indicates the document type, which the VDS-NC signer is allowed to produce.
- Value of DocumentType is defined in each use-case in the Use Cases section below. The DocumentType for ICAO use cases as defined currently will start with "N" and be followed by another letter denoting the use case. The letter "U" is reserved for possible future use cases. For National use cases, any letter other than "N" and "U" may be used.

### 3.6.4 ECParameters

The barcode signer certificate SHALL use a namedCurve in the ECParameters of the Subject Public Key Information Field.

Only the following curves MUST be used:
- brainpoolP256r1 [RFC 5639]
- brainpoolP320r1 [RFC 5639]
- brainpoolP384r1 [RFC 5639]
- brainpoolP512r1 [RFC 5639]
- NIST P-256 [FIPS 186-4]
- NIST P-384 [FIPS 186-4]
- NIST P-521 [FIPS 186-4]

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.

Note:
This is a deviation from Doc 9303-12 which requires the parameters to be explicit parameters.

### 3.6.5. Barcode Signer Public Key Validity

## CSCA Certificates (as specified in Doc 9303-12)

Private Key Usage Time: 3 to 5 years
Certificate Validity:Private Key Usage Time + Max. of Key Lifetime (= Certificate
Validity) of bar code Signer Certificates or
other certificates below the CSCA – whichever is
longer

### bar code Signer Certificates
Private Key Usage Time:  As per document profile
Certificate Validity:Private Key Usage Time + document Validity Timeframe

### Example
*Note: The actual validity periods used for the calculation in this example do not imply any recommendations.*
Suppose documents with a validity period of 5 years are issued, and the private key usage time of the bar code Signer Certificate is 1 years. Then validity of the bar code Signer Certificate is 1 + 5 = 6 years. If the usage time of the private key of the CSCA Certificate is 3 years, then the validity of the CSCA Certificate is 3 + 6 = 9 years.

### 3.6.6 Distribution Mechanism

The VDS-NC PKI objects that need to be distributed from issuing states or organizations to receiving states include:

- VDS-NC barcode signer certificate
- Country Signing Certificate Authority certificate
- Certificate Revocation List

The relevant distribution mechanisms for VDS-NC PKI objects include:

- Barcode
- Bilateral; and

- PKD

*Table 4: Distribution of VDS-NC PKI objects*

|  | *Barcode* | *Bilateral* | *PKD* | *Notes* |
|---|---|---|---|---|
| *Barcode Signer certificates* | Y (primary) |  | Y (secondary) | Certificates included in the barcode at generation |
| *CSCA Certificates* |  | Y | Y | For PKD, through ICAO Master List |
| *CRLs (Null and Non-null)* |  | Y | Y |  |

# 4. Use Cases

There are currently two use-cases defined for VDS-NC. In the future, additional use-cases may be defined.

In each use case, maximum number of characters permitted in each field are specified. Blank spaces between words shall count towards the maximum number of characters permitted in the field.

For some fields, maximum number of permitted characters are not explicitly defined. For example, email address. Since the number of characters used has an impact on the size of the barcode and hence its readability, care should be taken to keep the character count as low as possible for fields where restrictions have not been defined.

## 4.1 Proof of Testing (PoT)

The PoT is not a travel document but could be a supporting document used for travel purposes.

For Proof of Testing, the Signature Field is OPTIONAL for the first iteration of the proof, but strongly RECOMMENDED in order to prevent fraud and mis-use.

The Version Number in the header for this profile is 1 (one).

### 4.1.1 POT Signer Certificate Profile

The documentType value for this use-case is NT.

### 4.1.2 Data Set

The data set for PoT is derived from the ICAO recommendations for International COVID-19 Test Report.

**DATA FIELDS (Council approval on March 12, 2021)**

| | |
|---|---|
| UTCI | Unique Test Certificate Identifier (CONDITIONAL) - REQUIRED if document is signed, OPTIONAL if document is not signed. |
| Reporting language: | English REQUIRED (Where the certificate is issued in a language other than English, the certificate SHOULD include an English translation) |

Personal Information of Test Subject:
  a) Name of the Holder (as specified in Doc 9303-3) (REQUIRED)
  b) Date of Birth (YYYY-MM-DD) (REQUIRED)
  c) ID Document Type (REQUIRED)
  d) ID Document Number (REQUIRED)

Service Provider:
  a) Name of testing facility or service provider (REQUIRED)
  b) Country of test (REQUIRED)
  c) Contact details (REQUIRED)

Date and Time of Test and Report:
  a) Date and time of specimen collection (REQUIRED)
  b) Date and time of report issuance (REQUIRED)

Test Result:
  a) Type of test conducted: molecular (PCR); molecular (other); antigen; antibody (REQUIRED)
  b) Result of Test (normal/abnormal or positive/negative) (REQUIRED)
  c) Sampling method (nasopharyngeal, oropharyngeal, saliva, blood, other (OPTIONAL)

Optional Data Field:     Issued at the discretion of the issuing authority (OPTIONAL)

Note: for ID document Type, only the following fields are defined and MUST be used:

P – Passport (conforming toDoc 9303-4)
A – ID Card (conforming to Doc 9303-5)
C – ID Card (conforming to, Doc 9303-5)
I – ID Card (conforming to Doc 9303-5)
AC  - Crew Member Certificate (conforming to Doc 9303-5)
V – Visa (conforming to Doc 9303-7)
D – Driving License (conforming to ISO 18013-1. Mobile Driving Licenses are not included)

### 4.1.3 Schema Definition

The data that will be encoded for the PoT has been defined above. English MUST be used for all data elements. The contents of the Message Zone for PoT MUST be as follows:

*Table 5: Format of the PoT*

```
{

Object: Message {
```

| Element | Content | Max size |
|---|---|---|
| UTCI(utci) | Unique Test Certificate Identifier | 12 |

**Object: PersonalInformation(pid) {**

| Element | Content | Max size |
|---|---|---|
| Name(n) | Name of the holder (as specified in Doc 9303-3) MUST be used. | 39 |
| DOB(dob) | The DOB of the test subject. The [RFC 3339] full date format YYYY-MM-DD MUST be used. | 10 |
| DocType(dt) | The ID Document Type of the identity document MUST be used. Only these values MUST be used:<br>P – Passport (Doc 9303-4)<br>A – ID Card (Doc 9303-5)<br>C – ID Card (Doc 9303-5)<br>I – ID Card Doc 9303-5)<br>AC - Crew Member Certificate (Doc 9303-5)<br>V – Visa (Doc 9303-7)<br>D – Driving License (ISO 18013-1) | |
| 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. | 24 |

**}**

**Object: ServiceProvider(sp) {**

| Element | Content | Max size |
|---|---|---|
| Name(spn) | Name of testing facility or service provider MUST be used. | 20 |
| Country(ctr) | Country of test MUST be used. | 3 |

**Object: ContactDetails(cd) {**

| Element | Content | Max size |
|---|---|---|
| PhoneNumber(p) | Contact number of testing facility or service provider MUST be used. The maximum size of phone number is 19 characters (15 | 19 |

| | characters in accordance with [ITU-T E.123],3 characters for International Country Code and the symbol "+" to indicate that an international prefix is required). | |
| --- | --- | --- |
| Email(e) | Email address of testing facility or service provider MUST be used. | |
| Address(a) | Address of testing facility or service provider MUST be used. | |
| } | | |
| } | | |

**Object: DateTime(dat)** {

| Element | Content | Max size |
| --- | --- | --- |
| SpecimenCollectio n(sc) | Date and time of specimen collection MUST be used. | 25 |
| ReportIssuance(ri ) | Date and time of report issuance MUST be used. | 25 |
| } | | |

**Object: TestResult(tr)** {

| Element | Content | Max size |
| --- | --- | --- |
| TestConducted(tc) | Type of test conducted MUST be used. Only these values MUST be used: molecular(PCR) molecular(other) antigen antibody | |
| Result(r) | Result of Test MUST be used. Only these values MUST be used: normal abnormal positive negative | |
| Method(m) | Sampling method is OPTIONAL. Only these values MUST be used: nasopharyngeal oropharyngeal saliva blood other | |
| } | | |

| Element | Content | Max size |
|---|---|---|
| OptionalDataField (opt) | Optional data issued at the discretion of the issuing authority | 20 |
| } ] | | |
| } | | |
| } | | |

The JSON schema, in accordance with [JSON-SCHEMA], for the message zone for PoT is as follows:

```
{
      "$id": "http://namespaces.icao.int/VDS-NC_message_PoT_ICAO.json",
      "title": "Message Zone ICAO (PoT)",
      "type": "object",
      "description": "PoT Message Schema",
      "properties": {
            "utci": {
                  "type": "string"
            },
            "pid": {
                  "type": "object",
                  "properties": {
                        "n": {
                              "type": "string"
                        },
                        "dob": {
                              "type": "string",
                              "description": "Format YYYY-MM-DD"
                        },
                        "dt": {
                              "type": "string"
                        },
                        "dn": {
                              "type": "string"
                        }
                  },
                  "required": ["n",
                  "dob",
                  "dt",
"dn"],
                  "additionalProperties": false
            },
            "sp": {
                  "type": "object",
                  "properties": {
                        "spn": {
                              "type": "string"
                        },
                        "ctr": {
                              "type": "string",
                              "description": "A three letter code identifying the
country of test."
                        },
```

```
                        "cd": {
                                "type": "object",
                                "properties": {
                                        "p": {
                                                "type": "string"
                                        },
                                        "e": {
                                                "type": "string"
                                        },
                                        "a": {
                                                "type": "string"
                                        }
                                },
                                "required": ["p",
                                "e",
                                "a"]
                        }
                },
                "required": ["spn",
                "ctr",
                "cd"],
                "additionalProperties": false
        },
        "dat": {
                "type": "object",
                "properties": {
                        "sc": {
                                "type": "string",
                                "description": "Refer to rfc3339"
                        },
                        "ri": {
                                "type": "string",
                                "description": "Refer to rfc3339"
                        }
                },
                "required": ["sc",
                "ri"],
                "additionalProperties": false
        },
        "tr": {
                "type": "object",
                "properties": {
                        "tc": {
                                "type": "string",
                                "enum": ["molecular(PCR)",
                                "molecular(other)",
                                "antigen",
                                "antibody"]

        },

                        "r": {
                                "type": "string",
                                "enum": ["normal",
                                "abnormal",
                                "positive",
                                "negative"]
                        },
                        "m": {
```

```
                                "type": "string",
                                "enum": ["nasopharyngeal",
                                "oropharyngeal",
                                "saliva",
                                "blood",
                                "other"]
                        }
                },
                "required": ["tc",
                "r"],
                "additionalProperties": false
        },
        "opt": {
                "type": "string"
        }

},
"required": ["pid",
"sp",
"dat",
"tr"],
"additionalProperties": false
}
```

## 4.2 Proof of Vaccination (PoV)

The PoV is not a travel document but could be a supporting document used for travel purposes.

For Proof of Vaccination the Signature Field MUST be included.

The Version Number in the header for this profile is 1 (one).

### 4.2.1 PoV Signer Certificate Profile

The documentType value for this use-case is NV.

### 4.2.2 Data Set
The PoV data set is derived from the minimum data set recommended by WHO (who-dhi-smart-vaccination-certificate-core-data-set_vrc1.xlsx, 19 March 2021)

| Section | Data element | Description | Preferred Code System |
|---|---|---|---|
| **Person identification** (minimum dataset) | Name (REQUIRED) | Name of the holder (as specified in Doc 9303-3) | |
| | Unique identifier (RECOMMENDED) | Travel Document Number | |

| Section | Data element | Description | Preferred Code System |
|---|---|---|---|
| | Additional identifier (OPTIONAL) | Any other document number at discretion of issuer | |
| | Sex (RECOMMENDED) | Sex of the holder (as specified in Doc 9303-4 Section 4.1.1.1 – Visual Inspection Zone) | |
| | Date of birth (CONDITIONAL) | Vaccinated person's date of birth. REQUIRED if no *Unique identifier* is provided. | Complete date, without time, following the ISO 8601. |
| **\*VaccinationEvent** (minimum dataset) \* means that the whole section may be repeated | Vaccine / prophylaxis (REQUIRED) | ICD-11 Extension codes (http://id.who.int/icd/entity/164949870) | ICD-11 Extension codes (http://id.who.int/icd/entity/164949870) |
| | Vaccine Brand (REQUIRED) | Vaccine medicinal product | As defined by member state |
| | Disease or agent targeted (RECOMMENDED) | Disease or agent that the vaccination provides protection against | ICD-11 |
| **\*VaccinationDetails**(minimum dataset) \* means that the whole section may be repeated | Date of vaccination (REQUIRED) | Date on which the vaccine was administered. The ISO8601 full date format YYYY-MM-DD MUST be used. | Complete date, without time, following ISO 8601 |
| | Dose Number (REQUIRED) | Vaccine dose number | |
| | Country of vaccination (REQUIRED) | The country in which the individual has been vaccinated | Doc 9303-3 Country Codes |
| | Administering centre (REQUIRED) | Name/code of administering centre or a health authority responsible for the vaccination event | |
| | Vaccine batch number (REQUIRED) | A distinctive combination of numbers and/or letters which specifically identifies a batch | |
| | Due date of next dose (OPTIONAL) | Date on which the next vaccination should be administered | Complete date, without time, following ISO 8601 |

## 4.2.3 Schema Definition

The data that will be encoded for the PoV is the data set defined above. The contents of the Message Zone for PoV are as follows

*Table* 6*: Format of the PoV*

**Object: Message {**

| Element | Content | Max size |
|---|---|---|
| UVCI(uvci) | Unique Vaccination Certificate Identifier | 12 |

**Object: PersonIdentification(pid) {**

{

| Element | Content | Max size |
|---|---|---|
| Name(n) | Name of the holder | 39 |
| Date of birth(dob) | Date of birth of test subject. ISO8601 YYYY-MM-DD | 10 |
| UniqueIdentifier(i) | Travel Document Number | 11, Single Unique Identifier only. Identifier should be valid Travel Document number |
| AdditionalIdentifer(ai) | Any other document number at discretion of issuer | 24 |
| Sex(sex) | Sex of the test subject (as specified in Doc 9303-4 Section 4.1.1.1 – Visual Inspection Zone) | 1 |

}

**Array: VaccinationEvent(ve) [{**

| Element | Content | Max size |
|---|---|---|
| Vaccine or Prophylaxis(des) | Vaccine or vaccine sub-type (ICD-11 Extension codes (http://id.who.int/icd/entity/1649498 70) | 6 |
| Vaccine brand (nam) | Medicinal product name | |
| Disease or agent targeted (dis) | Disease or agent that the vaccination provides protection against (ICD-11) | 6 |

**Array: VaccinationDetails(vd) [{**

| Element | Content | Max size |
|---|---|---|
| Date of vaccination(dvc) | Date on which the vaccine was administered. The ISO8601 full date format YYYY-MM-DD MUST be used. | 10 |
| Dose number (seq) | Vaccine dose number. | 2 |
| 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. | 3 |

| Administering centre(adm) | The name or identifier of the vaccination facility responsible for providing the vaccination | 20 |
|---|---|---|
| Vaccine batch number (lot) | A distinctive combination of numbers and/or letters which specifically identifies a batch | 20 |
| 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. | 10 |

        }]

    }]

 }

The JSON schema in accordance with [JSON-SCHEMA] for the message zone for PoV is as follows:

```
{
    "$id": "http://namespaces.icao.int/VDS-NC_message_PoV_WHO.json",
    "title": "Message Zone WHO (PoV)",
    "type": "object",
    "description": "PoV Message Schema",
    "type": "object",
    "properties": {
        "uvci": {
            "type": "string"
        },
        "pid": {
            "type": "object",
            "properties": {
                "n": {
                    "type": "string"
                },
                "dob": {
                    "type": "string",
                    "description": "Format YYYY-MM-DD. Mandatory
                    if no UniqueIdentifier is provided."
                },
                "i": {
                    "type": "string",
                    "description": "Travel Document Number."
                },
                "ai": {
                    "type": "string",
                    "description": "Other document number."
                },
                "sex": {
                    "type": "string",
                    "description": "Specific instance of sex
            information for the vaccinated person."
                }
            },
            "required": ["n"],
```

```
        "anyOf": [
                { "required":[ "i" ] },
                { "required":[ "dob" ] }
        ],
        "additionalProperties": false
},
"ve": {
        "type": "array",
        "items": [{
                "type": "object",
                "properties": {
                        "des": {
                                "type": "string"
                        },
                        "nam": {
                                "type": "string"
                        },
                        "dis ": {
                                "type": "string"
                        },
                        "vd": {
                                "type": "array",
                                "items": [{
                                        "type": "object",
                                        "properties": {

                                        "dvc": {
                                                "type": "string",
                                                "description": "Format
                                                        YYYY-MM-DD"
                                        },
                                        "seq ": {
                                                "type": "integer"
                                        },
                                        "ctr": {
                                                "type": "string",
                                                "description":    "Doc    9303-3
                                                Country Code"
                                        },
                                        "adm": {
                                                "type": "string",
                                                "description": " name or
                                                identifier of the
                                        vaccination facility"
                                        },
                                        "lot": {
                                                "type": "string",
                                                "description": "Batch
                number or lot number of vaccination"
                                        },

                                        "dvn": {
                                                "type": "string",
                                                "description": "Format
                                                        YYYY-MM-DD"
                                        }
                                },
```

```
                    "required": ["dvc", "seq", "ctr",
                    "adm", "lot"],
                    }]
                }
                },
            "required": ["des","nam","vd"],
        }]
    }
    },
    "required": ["uvci","pid",
    "ve"]
}
```

## 5. Reference documentation

The following documentation served as reference for this Technical Report:

| | |
|---|---|
| [RFC 2119] | RFC 2119, S. Bradner, "Key Words for Use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997 |
| [Doc 9303] | ICAO Doc 9303, 8th Edition, "Machine Readable Travel Documents" |
| [RFC 5280] | RFC 5280, D. Cooper, S. Santesson, S. Farrell, S. Boeyen, R. Housley, W. Polk, , "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", May 2008 |
| [JSON-SCHEMA] | https://json-schema.org |
| [RFC 7493] | RFC 7493, T. Bray, "The I-JSON Message Format", March 2015 |
| [RFC 4648] | RFC 4648, Simon Josefsson, "The Base16, Base32, and Base64 Data Encodings", October 2006 |
| [RFC 3339] | RFC 3339, G. Klyne, C. Newman, "Date and Time on the Internet: Timestamps", July 2002 |
| [RFC 8785] | RFC 8785, A. Rundgren, B. Jordan, S. Erdtman, "JSON Canonicalization Scheme (JCS)", June 2020 |
| [ITU-T E.123] | Notation for national and international telephone numbers, e-mail addresses and Web addresses |
| [FIPS 186-4] | NIST FIPS PUB 186-4, Digital Signature Standard (DSS), 2013 |
| [RFC 5480] | RFC 5480, S. Turner, D. Brown, K. Yiu, R. Housley, T. Polk, "Elliptic Curve Cryptography Subject Public Key Information", March 2009 |
| [RFC 5639] | RFC 5639, M. Lochter, J. Merkle, "Elliptic Curve Cryptography (ECC) Brainpool Standard Curves and Curve Generation" March 2010 |
| [ISO 18013-1] | ISO/IEC 18013-1:2018 |

Information technology — Personal identification — ISO-compliant driving licence — Part 1: Physical characteristics and basic data set

[ICD-11]                International Classification of Diseases 11th Revision - https://icd.who.int/en (retrieved April 23,2021)

# **Annex A   Abbreviations**

| Abbreviation | |
|---|---|
| CA | Certificate Authority |
| CAPSCA | Collaborative Arrangement for the Prevention and Management of Public Health Events in Civil Aviation |
| CSCA | Country Signing Certification Authority |
| CRL | Certificate Revocation List |
| DOB | Date of Birth |
| EKU | Extended Key Usage |
| JSON | JavaScript Object Notation |
| JCS | JSON Canonicalization Scheme |
| ICAO | International Civil Aviation Organization |
| OID | Object Identifier |
| PKI | Public Key Infrastructure |

# Annex B    Worked Example – PoT (Informative)

The following is an example of PoT using REQUIRED and RECOMMENDED fields only.

```
{
      "data":{
            "hdr":{
                  "t":"icao.test",
                  "v":1,
                  "is":"UTO"
            },
            "msg":{
                  "utci":"U01932",
                  "pid":{
                        "n":"Cook Gerald",
                        "dob":"1990-01-29",
                        "dt":"P",
                        "dn":"E1234567P"
                  },
                  "sp":{
                        "spn":"General Hospital",
                        "ctr":"UTO",
                        "cd":{
                              "p":"+00068765432",
                              "e":"genhosp@mail.com",
                              "a":"12 Utopia Street"
                        }
                  },
                  "dat":{
                        "sc":"2020-12-12T12:00:00+08:00",
                        "ri":"2021-02-11T14:00:00+08:00"
                  },
                  "tr":{
                        "tc":"molecular(PCR)",
                        "r":"negative"
                  }
            }
      },
      "sig":{
            "alg":"ES256",
            "cer":"MIIBeTCCAR2gAwIBAgIBZzAMBggqhkjOP...",
            "sigvl":"n1d8dbd2omadDys7eh86wvaWbTlFVEv..."
}}
```

| Proof of Testing | Issued by UTO | Version 1 | UTCI: U01932 |
|---|---|---|---|

**PERSONAL INFORMATION**

| Name of the Holder: | Date of Birth: | Document Type: | Document Number: |
|---|---|---|---|
| **Cook Gerald** | **1990-01-29** | **P** | **E1234567P** |

**SERVICE PROVIDER**

| Name of Testing Facility/Service Provider: | | Country of Test: |
|---|---|---|
| **General Hospital** | | **UTO** |

| Phone Number: | Email Address: | Address: |
|---|---|---|
| **+00068765432** | **genhosp@mail.com** | **12 Utopia Street** |

**DATETIME OF TEST & REPORT**

| Specimen Collection DateTime: | Report Issuance DateTime: |
|---|---|
| **2020-12-12T12:00:00+08:00** | **2021-02-11T14:00:00+08:00** |

**TEST RESULT**

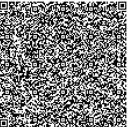| Type of Test Conducted: | Result of Test: | Sampling Method: |
|---|---|---|
| **molecular(PCR)** | **negative** | |

The following is an example of PoT using REQUIRED, RECOMMENDED and OPTIONAL fields.

```
{
    "data":{
        "hdr":{
            "t":"icao.test",
            "v":1,
            "is":"UTO"
        },
        "msg":{
            "utci":"U01932",
            "pid":{
                "n":"Cook Gerald",
                "dob":"1990-01-29",
                "dt":"P",
                "dn":"E1234567P"
            },
            "sp":{
                "spn":"General Hospital",
                "ctr":"UTO",
                "cd":{
                    "p":"+00068765432",
                    "e":"genhosp@mail.com",
                    "a":"12 Utopia Street"
                }
            },
            "dat":{
                "sc":"2020-12-12T12:00:00+08:00",
                "ri":"2021-02-11T14:00:00+08:00"
            },
            "tr":{
```

```
                    "tc":"molecular(PCR)",
                    "r":"negative",
                    "m":"nasopharyngeal"
                },
                "opt":"ID12345"
            }
        },
        "sig":{
            "alg":"ES256",
            "cer":"MIIBeTCCAR2gAwIBAgIBZzAMBggqhkjOPQ...",
            "sigvl":"z_VZDdMvjjRkg06nYLwHt4BP_APEm3MJ..."
        }
}
```
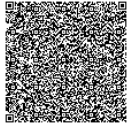
| Proof of Testing | Issued by UTO | Version 1 | UTCI: U01932 |
|---|---|---|---|

**PERSONAL INFORMATION**

| Name of the Holder: | Date of Birth: | Document Type: | Document Number: |
|---|---|---|---|
| **Cook Gerald** | **1990-01-29** | **P** | **E1234567P** |

**SERVICE PROVIDER**

| Name of Testing Facility/Service Provider: | Country of Test: |
|---|---|
| **General Hospital** | **UTO** |

| Phone Number: | Email Address: | Address: |
|---|---|---|
| **+00068765432** | **genhosp@mail.com** | **12 Utopia Street** |

**DATETIME OF TEST & REPORT**

| Specimen Collection DateTime: | Report Issuance DateTime: |
|---|---|
| **2020-12-12T12:00:00+08:00** | **2021-02-11T14:00:00+08:00** |

**TEST RESULT**

| Type of Test Conducted: | Result of Test: | Sampling Method: |
|---|---|---|
| **molecular(PCR)** | **negative** | **nasopharyngeal** |

**OPTIONAL DATA FIELD**

**ID12345**

# Annex C   Worked Example – PoV (Informative)

The following is an example of PoV using the same vaccine being delivered in two doses. It contains REQUIRED and RECOMMENDED fields only.

```
{
      "data":{
            "hdr":{
                  "t":"icao.vacc",
                  "v":1,
                  "is":"UTO"
            },
            "msg":{
                  "uvci":"U32870",
                  "pid":{
                        "n":"Smith Bill",
                        "sex":"M",
                        "i":"A1234567Z"
                  },
                  "ve":[{
                        "des":"XM68M6",
                        "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"
                        }]
                  }]
            }
      },
      "sig":{
            "alg":"ES256",
            "cer":"MIIBeTCCAR2gAwIBAgIBaDAMBggqhkjOPQ...",
            "sigvl":"xgHiDTywgNPZ1AJVQUhPL−mgKvKaxDU5..."
      }
}
```

| Proof of Vaccination | Issued by UTO | Version 1 | UVCI: U32870 |
|---|---|---|---|

**PERSONAL INFORMATION**

| Name of the Holder:<br>**Smith Bill** | Date of Birth: | Passport Number:<br>**A1234567Z** | Sex:<br>**M** |
|---|---|---|---|

Additional Identifier:

**VACCINATION EVENT**

| Vaccine or Prophylaxis:<br>**XM68M6** | Vaccine Brand:<br>**Comirnaty** | Disease or agent targeted:<br>**RA01.0** |
|---|---|---|

**VACCINATION DETAILS 1**

| Date of Vaccination:<br>**2021-03-03** | Dose Number:<br>**1** | Country of Vaccination:<br>**UTO** |
|---|---|---|
| Administering Centre:<br>**RIVM** | Vaccine Batch Number:<br>**VC35679** | Due Date of Next Dose: |

**VACCINATION DETAILS 2**

| Date of Vaccination:<br>**2021-03-24** | Dose Number:<br>**2** | Country of Vaccination:<br>**UTO** |
|---|---|---|
| Administering Centre:<br>**RIVM** | Vaccine Batch Number:<br>**VC87540** | Due Date of Next Dose: |

The following is an example of PoV using the same vaccine being delivered in two doses. It contains REQUIRED, RECOMMENDED and OPTIONAL fields.

```
{
    "data":{
        "hdr":{
            "t":"icao.vacc",
            "v":1,
            "is":"UTO"
        },
        "msg":{
            "uvci":"U32870",
            "pid":{
                "n":"Smith Bill",
                "dob":"1990-01-02",
                "sex":"M",
                "i":"A1234567Z",
                "ai":"L4567890Z"
            },
            "ve":[{
                "des":"XM68M6",
                "nam":"Comirnaty",
                "dis":"RA01.0",
                "vd":[{
                    "dvc":"2021-03-03",
                    "seq":1,
                    "ctr":"UTO",
                    "adm":"RIVM",
                    "lot":"VC35679",
```

```
                        "dvn":"2021-03-24"
                    },
                    {
                        "dvc":"2021-03-24",
                        "seq":2,
                        "ctr":"UTO",
                        "adm":"RIVM",
                        "lot":"VC87540"
                    }]
                }]
            }
        },
        "sig":{
            "alg":"ES256",
            "cer":"MIIBeTCCAR2gAwIBAgIBaDAMBggqhkjOPQ...",
            "sigvl":"cxfyi2vq2XJfZF7ksEkIZJtKbGrRE570..."
        }
    }
}
```

| Proof of Vaccination | Issued by UTO | Version 1 | UVCI: U32870 |
|---|---|---|---|

**PERSONAL INFORMATION**

| Name of the Holder: | Date of Birth: | Passport Number: | Sex: |
|---|---|---|---|
| **Smith Bill** | **1990-01-02** | **A1234567Z** | **M** |

Additional Identifier:
**L4567890Z**

**VACCINATION EVENT**

| Vaccine or Prophylaxis: | Vaccine Brand: | Disease or agent targeted: |
|---|---|---|
| **XM68M6** | **Comirnaty** | **RA01.0** |

**VACCINATION DETAILS 1**

| Date of Vaccination: | Dose Number: | Country of Vaccination: |
|---|---|---|
| **2021-03-03** | **1** | **UTO** |

| Administering Centre: | Vaccine Batch Number: | Due Date of Next Dose: |
|---|---|---|
| **RIVM** | **VC35679** | **2021-03-24** |

**VACCINATION DETAILS 2**

| Date of Vaccination: | Dose Number: | Country of Vaccination: |
|---|---|---|
| **2021-03-24** | **2** | **UTO** |

| Administering Centre: | Vaccine Batch Number: | Due Date of Next Dose: |
|---|---|---|
| **RIVM** | **VC87540** | |

The following is an example of PoV using a different vaccine for each of the two doses with REQUIRED, RECOMMENDED and OPTIONAL fields.
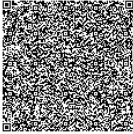
```
{
    "data":{
        "hdr":{
```

```
                    "t":"icao.vacc",
                    "v":1,
                    "is":"UTO"
            },
            "msg":{
                    "uvci":"U32879",
                    "pid":{
                            "n":"Smith Bill",
                            "dob":"1990-01-02",
                            "sex":"M",
                            "i":"A1234567Z",
                            "ai":"L4567890Z"
                    },
                    "ve":[{
                            "des":"XM68M6",
                            "nam":"Comirnaty",
                            "dis":"RA01.0",
                            "vd":[{
                                    "dvc":"2021-03-03",
                                    "seq":1,
                                    "ctr":"UTO",
                                    "adm":"RIVM",
                                    "lot":"VC35679",
                                    "dvn":"2021-03-24"
                            }]
                    },
                    {
                            "des":"XM68M6",
                            "nam":"COVID-19 Vaccine Moderna",
                            "dis":"RA01.0",
                            "vd":[{
                                    "dvc":"2021-03-24",
                                    "seq":2,
                                    "ctr":"SGP",
                                    "adm":"NUH",
                                    "lot":"VC99537"
                            }]
                    }]
            }
    },
    "sig":{
            "alg":"ES256",
            "cer":"MIIBeTCCAR2gAwIBAgIBaDAMBg...",
            "sigvl":"Fwf7zsHVSwEWQ-ExhtLXyIzM..."
    }
}
```

| Proof of Vaccination | Issued by UTO | Version 1 | UVCI: U32870 |
| --- | --- | --- | --- |

### PERSONAL INFORMATION

| Name of the Holder: | Date of Birth: | Passport Number: | Sex: |
| --- | --- | --- | --- |
| **Smith Bill** | **1990-01-02** | **A1234567Z** | **M** |

Additional Identifier:
**L4567890Z**

### VACCINATION EVENT 1

| Vaccine or Prophylaxis: | Vaccine Brand: | Disease or agent targeted: |
| --- | --- | --- |
| **XM68M6** | **Comirnaty** | **RA01.0** |

| Date of Vaccination: | Dose Number: | Country of Vaccination: |
| --- | --- | --- |
| **2021-03-03** | **1** | **UTO** |

| Administering Centre: | Vaccine Batch Number: | Due Date of Next Dose: |
| --- | --- | --- |
| **RIVM** | **VC35679** | **2021-03-24** |

### VACCINATION EVENT 2

| Vaccine or Prophylaxis: | Vaccine Brand: | Disease or agent targeted: |
| --- | --- | --- |
| **XM68M6** | **COVID-19 Vaccine Moderna** | **RA01.0** |

| Date of Vaccination: | Dose Number: | Country of Vaccination: |
| --- | --- | --- |
| **2021-03-24** | **2** | **SGP** |

| Administering Centre: | Vaccine Batch Number: | Due Date of Next Dose: |
| --- | --- | --- |
| **NUH** | **VC99537** | |

# Annex D   Worked Example – Signature Generation (Informative)

The following example uses the PoV given as first example in Annex C.

The signing process of the VDS-NC is as follows:

1. Calculate the message digest
   a. Extract the value from the Data Field, including the braces {}.
   b. Create a Canonical JSON representation [ RFC 8785] of the extracted value
   c. Calculate the message digest of the canonical value using the hashing algorithm extracted from signature algorithm specified in the alg field
2. Signing
   a. The signature generation process includes the result of the message digest calculation process and the VDS-NC signer's private key.
   b. The signature generation above gives the output of r and s. Append r and s and do a base64url encoding, this will be the input to the sigvl field

Extracted value from the Data field:

```
{
     "hdr":{
          "t":"icao.vacc",
          "v":1,
          "is":"UTO"
     },
     "msg":{
          "uvci":"U32870",
          "pid":{
               "n":"Smith Bill",
               "dob":"1990-01-02",
               "sex":"M",
               "i":"A1234567Z",
               "ai":"L4567890Z"
          },
          "ve":[{
               "des":"XM68M6",
               "nam":"Comirnaty",
               "dis":"RA01.0",
               "vd":[{
                    "dvc":"2021-03-03",
                    "seq":1,
                    "ctr":"UTO",
                    "adm":"RIVM",
                    "lot":"VC35679",
                    "dvn":"2021-03-24"
               },
               {
                    "dvc":"2021-03-24",
                    "seq":2,
                    "ctr":"UTO",
                    "adm":"RIVM",
                    "lot":"VC87540"
               }]
```

```
            }]
        }
}
```

The same data as a JSON string is as follows :

{"hdr":{"t":"icao.vacc","v":1,"is":"UTO"},"msg":{"uvci":"U32870","pid":{"n":"Smit
h Bill","dob":"1990-01-
02","sex":"M","i":"A1234567Z","ai":"L4567890Z"},"ve":[{"des":"XM68M6","nam":"Comi
rnaty","dis":"RA01.0","vd":[{"dvc":"2021-03-
03","seq":1,"ctr":"UTO","adm":"RIVM","lot":"VC35679","dvn":"2021-03-
24"},{"dvc":"2021-03-24","seq":2,"ctr":"UTO","adm":"RIVM","lot":"VC87540"}]}]}}}

Output of the JSON Canonicalization [RFC 8785] :

{"hdr":{"is":"UTO","t":"icao.vacc","v":1},"msg":{"pid":{"ai":"L4567890Z","dob":"1
990-01-02","i":"A1234567Z","n":"Smith
Bill","sex":"M"},"uvci":"U32870","ve":[{"des":"XM68M6","dis":"RA01.0","nam":"Comi
rnaty","vd":[{"adm":"RIVM","ctr":"UTO","dvc":"2021-03-03","dvn":"2021-03-
24","lot":"VC35679","seq":1},{"adm":"RIVM","ctr":"UTO","dvc":"2021-03-
24","lot":"VC87540","seq":2}]}]}}}

There are no line breaks in the above text.

Output of the Signature process :

"sigvl":"cxfyi2vq2XJfZF7ksEkIZJtKbGrRE570UZc_rNAlpfRHD_Xjq57r2h-
QLvd_tCQGitsZevFmB0iXzEFdeeZ4zA=="

This signature can be verified using the barcode certificate that is embedded in the VDS-NC and is given below for reference:

MIIBeTCCAR2gAwIBAgIBaDAMBggqhkjOPQQDAgUAMB0xCzAJBgNVBAYTAlVUMQ4wDAYDVQQDDAVVVCBDQ
TAeFw0yMTA0MDcwNDMwMjZaFw0yNjEwMDcwNDMwMjZaMBoxCzAJBgNVBAYTAlVUMQswCQYDVQQDEwIwNj
BZMBMGByqGSM49AgEGCCqGSM49AwEHA0IABI5bRQ3-vabXhHAs2IPi-
k9rP_TS2J8aq5fTtUG1iOwXdBxx2n6c38TJ2MzBWT5PHCKVlq5JOCyJ1nDlCPd1S2yjTzBNMBIGA1UdJQ
QLMAkGB2eBCAEBDgIwHwYDVR0jBBgwFoAUymyksnX8rywn0RH7nDq-
Bs2QOqowFgYHZ4EIAQEGAgQLMAkCAQAxBBMCTlYwDAYIKoZIzj0EAwIFAANIADBFAiBVaaJVHvWLX756y
AGt04C89ZEWGr-BsHDgaRb0EH3d9gIhAO2UNvLNhEoUWT1I_zj_cG5mh2U-lWCMBUQ3zSQqWUcs

The full I-JSON string with certificate and Signature is as follows:

{"data":{"hdr":{"t":"icao.vacc","v":1,"is":"UTO"},"msg":{"uvci":"U32870","pid":{"
n":"Smith Bill","dob":"1990-01-
02","sex":"M","i":"A1234567Z","ai":"L4567890Z"},"ve":[{"des":"XM68M6","nam":"Comi
rnaty","dis":"RA01.0","vd":[{"dvc":"2021-03-
03","seq":1,"ctr":"UTO","adm":"RIVM","lot":"VC35679","dvn":"2021-03-
24"},{"dvc":"2021-03-
24","seq":2,"ctr":"UTO","adm":"RIVM","lot":"VC87540"}]}]}},"sig":{"alg":"ES256","
cer":"MIIBeTCCAR2gAwIBAgIBaDAMBggqhkjOPQQDAgUAMB0xCzAJBgNVBAYTAlVUMQ4wDAYDVQQDDAV
VVCBDQTAeFw0yMTA0MDcwNDMwMjZaFw0yNjEwMDcwNDMwMjZaMBoxCzAJBgNVBAYTAlVUMQswCQYDVQQD
EwIwNjBZMBMGByqGSM49AgEGCCqGSM49AwEHA0IABI5bRQ3-vabXhHAs2IPi-
k9rP_TS2J8aq5fTtUG1iOwXdBxx2n6c38TJ2MzBWT5PHCKVlq5JOCyJ1nDlCPd1S2yjTzBNMBIGA1UdJQ
QLMAkGB2eBCAEBDgIwHwYDVR0jBBgwFoAUymyksnX8rywn0RH7nDq-
Bs2QOqowFgYHZ4EIAQEGAgQLMAkCAQAxBBMCTlYwDAYIKoZIzj0EAwIFAANIADBFAiBVaaJVHvWLX756y

AGt04C89ZEWGr-BsHDgaRb0EH3d9gIhAO2UNvLNhEoUWT1I_zj_cG5mh2U-
lWCMBUQ3zSQqWUcs","sigvl":"cxfyi2vq2XJfZF7ksEkIZJtKbGrRE570UZc_rNAlpfRHD_Xjq57r2h
-QLvd_tCQGitsZevFmB0iXzEFdeeZ4zA=="}}

**— END —**