MACHINE READABLE TRAVEL DOCUMENTS

TECHNICAL REPORT

VDS-NC

Visible Digital Seal for non-constrained environments

Version – 1.4

Date – May 27, 2022

Published by authority of the Secretary General

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

File	: WG3TF5_N0313 TR - Visible Digital Seal-NC V1.4.doc
Author	: ISO/IEC JTC1 SC17 WG3/TF5

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)
1.1	May 2021	Specified dots/module for the barcode
1.2	Aug 2021	Fixed error in sigvl in JSON schema of signature zone Added option for a sub-CA if the CSCA is an RSA root Added requirement that there can only be a single separate CSCA or subCA per country Specified CRLDP for pointing to ICAO PKD for the separate CSCA or subCA New version of schema for PoV based on latest data set released by WHO Added Proof of Recovery (PoR) based on ICAO (CAPSCA) data set
1.3	Jan 2022	Changes after comment resolution in WG3. Some major changes based on the discussions: • Sub-CA is dropped. In version 2 of PoV, the Signer Certificate may be omitted. A separate trustlist to distribute the Signer Certificate is also defined. • Harmonization of Vaccine code, brand name and disease targeted. Schema published at Github.
1.4	May 2022	Comment resolution from Copenhagen meeting

Table of contents

1. Introduction

Doc 9303-13 defines the Visible Digital Seal for Non-Electronic documents. Doc 9303-7 and Doc 9303-8 also present 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. Three health related use cases are also described in this TR. Further use cases will be added to this TR as the necessity arises.

Note: A profile of VDS-NC for Digital Travel Authorization (DTA) has also been defined as the fourth use case. The details are in the DTA Technical Report.

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].

MUST
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
PoR	Proof of Recovery

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.

It is RECOMMENDED that the barcode is created with at least 3 dots per module sidelength (i.e 9 dots per module at a minimum).

Note: When printing the barcode, a module must have a sidelength of at least 0.254 mm, which translates to 3 dots per module sidelength for 300 dpi printing and 6 dots per module sidelength for 600 dpi printing.

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.

Note: An important consideration in the choice of a barcode symbology is the data carrying capacity. For example, the Aztec and PDF417 have less capacity to store data than the QR code format.

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_PoV_WHO_V2.json"
                              },
                              {
                                    "$ref":
"http://namespaces.icao.int/VDS-NC_message_PoT_ICAO.json"
                              },
                              {
                                    "$ref":
"http://namespaces.icao.int/VDS-NC_message_PoR_ICAO.json"
                              },
]

                        },
                        "additionalProperties": false
                  },
                  "required": ["hdr",
                  "msg"],
                  "additionalProperties": false
            },
            "sig":
{
```

```
                  "oneOf": [{
                        "$ref": "http://namespaces.icao.int/VDS-
NC_signature.json"
                  },
                  {
                        "$ref": "http://namespaces.icao.int/VDS-
NC_signatureV2.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), “icao.rcvy” for PoR (data defined by CAPSCA). 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 (in lowercase) followed by a period followed by the usecase (also in lowercase)
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", "icao.rcvy"
                        ]
                  },
                  "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

There are two versions of the signature zone (Signature Zone and Signature Zone V2). Both versions are valid and current.

In the case of Signature Zone V2, the barcode Signer Certificate can be omitted from the Signature Zone and replaced with a reference to the barcode Signer Certificate.

3.5.1 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 SHA-256 hashing algorithm
ES384 – denotes ECDSA with SHA-384 hashing algorithm
ES512 – denotes ECDSA with SHA-512 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"
            },
            "sigvl": {
                  "type": "string",
                  "description": "Signature value signed over the Data in
base64url encoding"
            }
      },
      "required": ["alg",
      "cer",
      "sigvl"],
      "additionalProperties": false
}
```

3.5.2 Signature Zone V2

The signature zone (V2) consists of the following elements:

Table 4: 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]
`Certificate Reference (cref)`	The identifier for the barcode signer. It is made up of 2 letter country code + serial number of the barcode signer. Maximum size of 42Character (2 for Country Code, 40 for Serial number) (CONDITIONAL) – REQUIRED if Certificate(cer) is

	not provided.
`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_signatureV2.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"
            },
            "cref": {
                  "type": "string",
                  "description": " The identifier for the barcode signer.
It is made up of 2 letter country code + serial number of the barcode
signer."
            },

            "sigvl": {
                  "type": "string",
                  "description": "Signature value signed over the Data in
base64url encoding"
            }
      },
      "required": ["alg",
      "sigvl"],
      "anyOf": [
                        { "required":[ "cer" ] },
                        { "required":[ "cref" ] }
            ],
      "additionalProperties": false
}
```

3.5.3 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”. The EKU MUST be marked as Critical.
- Key-pair MUST be of ECC type.
- A namedCurve in the ECParameters of the Subject Public Key Information Field MAY be used. If a namedCurve is used, it MUST be one of the curves listed in clause 3.6.5

If a link certificate is generated during the rollover of this CA certificate, the Link Certificate MUST comply with the specification of Doc 9303-12 with the restrictions stated here for the CA certificate.

If a different root of trust is used for the issuance of the barcode signers, each issuing State or organization SHALL create only a single such CA.

3.6.3 CRL Distribution Point

In case of a different root of trust, the requirements for the CRL Distribution Point follow the requirements of Doc 9303-12, with the following changes.

The template for the URL values to be defined in the CRLDP is as follows:

https://pkddownload1.icao.int/eHealthCRLs/CountryCode.crl
https://pkddownload2.icao.int/eHealthCRLs/CountryCode.crl

If this country code does not uniquely identify the issuing State or organization, the entry will be created by appending the symbol “_” to the three-letter country code in the MRZ, and then the ICAO assigned three-letter code for the issuing State or organization which uniquely identifies the issuing State or organization.

Singapore PKD example:
https://pkddownload1.icao.int/eHealthCRLs/SGP.crl
https://pkddownload2.icao.int/eHealthCRLs/SGP.crl

Hong Kong example:
https://pkddownload1.icao.int/eHealthCRLs/CHN_HKG.crl
https://pkddownload2.icao.int/eHealthCRLs/CHN_HKG.crl

3.6.4 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.

3.6.5 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.

3.6.6 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.

3.6.7 Trust List

A Trust List is a digitally signed list of signer certificates (E.g. Document signer certificates, barcode signer certificates, master list signer certificates …) that are ‘trusted’ by the Issuing State that signed the Trust List.

The Trust List is a possible distribution mechanism for barcode signer certificates when using Signature Zone V2.

3.6.7.1 Trust List Signer

An entity that digitally signs a Trust List of signer certificates. The Trust List signer is authorized by its national CSCA to perform this function through the issuance of a Trust List Signer certificate.

3.6.7.1.1 Trust List Signer Certificate Profile

The Trust List Signer Certificate MUST comply with the Certificate Fields Profile, which defines the certificate profile requirements common to all certificates for the fields of the certificate, defined in Doc 9303-12.

The Trust List Signer Certificate MUST also comply with the certificate extension profile for Master List Signer defined in Doc 9303-12, with the following restriction:

- The Object Identifier that must be included in the `extendedKeyUsage` extension for Trust List Signer certificates is `2.23.136.1.1.15.2`

3.6.7.1.2 Trust List Signer Validity

The Trust List Signer private key lifetime and the certificate validity period are left to the discretion of the issuing State or organization.

3.6.7.2 Trust List Structure

Trust Lists are implemented as instances of the `ContentInfo` Type, as specified in RFC 5652. The `ContentInfo` MUST contain a single instance of the `SignedData` Type as profiled below. No other data types are included in the `ContentInfo`. All Trust Lists MUST be produced in DER format to preserve the integrity of the signatures within them.

3.6.7.2.1 SignedData Type

The processing rules in RFC 5652 apply.

The specification of Trust List structure uses the following terminology for presence requirements of each field:

m	mandatory — the field MUST be present;
r	recommended — the field SHOULD be present;
x	do not use — the field MUST NOT be present;
o	optional — the field MAY be present.

Table 5. Trust List

Value		Comments
`SignedData`		
`Version`	m	Value = `v3`
`digestAlgorithms`	m	
`encapContentInfo`	m	
`eContentType`	m	`id-icao-trustList`
`eContent`	m	The encoded contents of a `TrustList`
`Certificates`	m	The Trust List Signer certificate MUST be included and the CSCA certificate, which can be used to verify the signature in the `signerInfos` field SHOULD be included.
`Crls`	x	
`signerInfos`	m	It is RECOMMENDED that States only provide 1 `signerinfo` within this field.

Value		Comments
`SignerInfo`	m	
`Version`	m	The value of this field is dictated by the `sid` field. See [RFC 5652] for rules regarding this field.
`Sid`	m	
`subjectKeyIdentifier`	r	It is RECOMMENDED that this field be supported rather than `issuerandSerialNumber`.
`digestAlgorithm`	m	The algorithm identifier of the algorithm used to produce the hash value over `encapsulatedContent` and `SignedAttrs.` See note below.
`signedAttrs`	m	Additional attributes may be included. However these do not have to be processed by Receiving States except to verify the signature value. `signedAttrs` MUST include signing time (see [PKCS #9]).
`signatureAlgorithm`	m	The algorithm identifier of the algorithm used to produce the signature value, and any associated parameters. See note below.
`signature`	m	The result of the signature generation process.
`unsignedAttrs`	o	Although this field MAY be included, Receiving States may choose to ignore it.

Note.— `DigestAlgorithmIdentifiers` MUST omit “`NULL`” parameters, while the `SignatureAlgorithmIdentifier` (as defined in RFC 3447) MUST include `NULL` as the parameter if no parameters are present, even when using SHA2 Algorithms in accordance with RFC 5754. Implementations MUST accept `DigestAlgorithmIdentifiers` with both conditions, absent parameters or with `NULL` parameters.

3.6.7.2.2 ASN.1 Trust List Specification

```
TrustList
{ joint-iso-itu-t(2) international-organizations (23) icao(136)
mrtd(1) security(1) trustList(15) trustList(1)}

DEFINITIONS IMPLICIT TAGS ::=
BEGIN

IMPORTS

 -- Imports from RFC 5280 [PROFILE], Appendix A.1
     Certificate
       FROM PKIX1Explicit88
         { iso(1) identified-organization(3) dod(6)
```

```
           internet(1) security(5) mechanisms(5) pkix(7)
             mod(0) pkix1-explicit(18) };
-- Trust List

TrustListVersion ::= INTEGER {v0(0)}

TrustList ::= SEQUENCE {
  version            TrustListVersion,
  signerCertList           SET OF Certificate }

-- Object Identifiers

-- ICAO security framework
id-icao OBJECT IDENTIFIER::={joint-iso-itu-t(2) international-
organizations (23) icao(136)}
id-icao-mrtd OBJECT IDENTIFIER ::= {id-icao 1}
id-icao-mrtd-security OBJECT IDENTIFIER ::= {id-icao-mrtd 1}

-- Trust list
id-icao-trustListId OBJECT IDENTIFIER ::= {id-icao-mrtd-security 15}
id-icao-trustList OBJECT IDENTIFIER ::= {id-icao-trustListId 1}
id-icao-trustListSigner OBJECT IDENTIFIER ::= {id-icao-trustListId
2}

END
```

3.6.8 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
- PKD; and
- TrustList

Table 6: Distribution of VDS-NC PKI objects

	Barcode	***Bilateral***	***PKD***	***TrustList***	***Notes***
Barcode Signer certificates	Y (Optional if using Signature Zone V2)		Y (secondary)	Y (secondary)	Certificates could be included in the barcode at generation.
CSCA Certificates		Y	Y		For PKD, through ICAO Master List

CRLs (Null and Non-null)		Y	Y		
Trustlist Signer				Y (primary)	Trustlist Signer is included in the Trustlist

4. Use Cases

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

Note: A fourth use case has been defined for Digital Travel Authorization (DTA) and is covered in the TR for DTA.

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 to Doc 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/IEC 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 7: Format of the PoT

{		
Object: **`Message`** {		
Element	Content	Max size
`UTCI(utci)`	Unique Test Certificate Identifier	18
Object: **`PersonalInformation(pid)`** {		
Element	Content	Max size
`Name(n)`	Name of the holder (as specified in Doc 9303-3)	39

	MUST be used.	
`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: 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)	
`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 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).	19

`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
`SpecimenCollection(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",
                  "description": "REQUIRED if document is signed, OPTIONAL
            if document is not signed."
            },
            "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.

Note:

1. *There two versions of the PoV. Both versions are current and supported. PoV Version 2 is the recommended version*

2. *As per the specifications for VDS-NC, there are three fields that identify the vaccine:*

   Vaccine/prophylaxis (ICD-11 extension code) -> encoded as 'des'

   Medicinal Product name -> encoded as 'nam'

   Disease or agent targeted -> encoded as 'dis'

   To ensure interoperability and wider acceptance of VDS-NC, it is necessary to harmonise the values in these fields. To this end, a github site has been created at https://github.com/ICAO-TRIP-ISO-WG3/VDS-NC . It contains a schema definition for all vaccines that are approved as part of the WHO EUL. As more vaccines are approved, the schema will be updated in the github pages.

4.2.1 PoV Signer Certificate Profile

The documentType value for this use-case is NV.

4.2.2 PoV Version 2

The Version Number in the header for this profile is 2 (two).

4.2.2.1 Data Set

The PoV data set is derived from the minimum data set recommended by WHO (WHO-2019-nCoV-Digital-certificates-vaccination-data-dictionary-2021.1-eng.xlsx, 27 AUG 2021)

Section	Data element	Description	Preferred Code System
	UVCI (REQUIRED)	Unique Vaccination Certificate Identifier	
	Certificate valid from (OPTIONAL)	Date in which the certificate for a vaccination event became valid.	Complete date, without time, following the ISO 8601.

Section	**Data element**	**Description**	**Preferred Code System**
	Certificate valid until (OPTIONAL)	Last date in which the certificate for a vaccination event is valid.	Complete date, without time, following the ISO 8601.
Person identification (minimum dataset)	Name (REQUIRED)	Name of the holder (as specified in Doc 9303-3)	
	Unique identifier (RECOMMENDED)	Travel Document Number	
	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	Refer to schema definition at https://github.com/ICAO-TRIP-ISO-WG3/VDS-NC
	Vaccine manufacturer (CONDITIONAL)	Name of the manufacturer of the vaccine received. If vaccine manufacturer is unknown, market authorization holder is REQUIRED.	As defined by Member State
	Vaccine market authorization holder (CONDITIONAL)	Name of the market authorization holder of the vaccine received. If market authorization holder is unknown, vaccine manufacturer is REQUIRED.	As defined by Member State
	Disease or agent targeted (RECOMMENDED)	Disease or agent that the vaccination provides protection against	ICD-11. Must always be 'RA01.0' for Covid-19.

Section		Data element	Description	Preferred Code System
	***Vaccination Details**(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	
		Total Doses (OPTIONAL)	Total expected doses	
		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
		Optional Data Field (OPTIONAL)	Issued at the discretion of the issuing authority	

Note:

The Total Doses is the number of doses that constitute a full vaccination regime for the specific vaccine. For example, if the full vaccination regime is 2 doses for a vaccine, then for each of the doses:

a. The first dose will be encoded with 1 for the Dose Number and 2 for the Total Doses.
b. The second dose will be encoded with 2 for the Dose Number and 2 for the Total Doses.
c. If a booster is given after the two doses, then the Dose Number will be 3 or over and the Total Doses will also be 3 or over.

4.2.2.2 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 8: Format of the PoV

`Object: Message {`

Element	Content	Max size
`UVCI(uvci)`	Unique Vaccination Certificate Identifier	18

Certificate Valid From (cvf)	Date in which the certificate for a vaccination event became valid. ISO8601 YYYY-MM-DD	10
Certificate Valid Until (cvu)	Last date in which the certificate for a vaccination event is valid. ISO8601 YYYY-MM-DD	10

Object: PersonIdentification(pid) {

Element	Content	Max size
Name(n)	Name of the holder	39
Date of birth(dob)	Date of birth of holder. 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 holder (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/164949870)	6
Vaccine brand (nam)	Medicinal product name	Refer to schema definition at https://github.com/ICAO-TRIP-ISO-WG3/VDS-NC
Vaccine manufacturer (mfg)	Name of the manufacturer of the vaccine received. If vaccine manufacturer is unknown, market authorization holder is REQUIRED.	As defined by Member State
Vaccine market authorization holder (mah)	Name of the market authorization holder of the vaccine received. If market authorization holder is unknown, vaccine manufacturer is REQUIRED.	As defined by Member State
Disease or agent targeted (dis)	Disease or agent that the vaccination provides protection against (ICD-11)	6

Array: VaccinationDetails(vd) [{

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
Total Doses(tot)	Total expected doses	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
}]		
}]		

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 PoV is as follows:

```
{
      "$id": "http://namespaces.icao.int/VDS-NC_message_PoV_WHO_V2.json",
      "title": "Message Zone WHO (PoV)",
      "type": "object",
      "description": "PoV Message Schema",
      "type": "object",
      "properties": {
            "uvci": {
                  "type": "string"
            },
            "cvf": {
                  "type": "string",
                  "description": "Certificate valid from.
                        Format YYYY-MM-DD."
                        },
            "cvu": {
                  "type": "string",
                  "description": "Certificate valid until.
                        Format YYYY-MM-DD."
                        },
            "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"
                              },
                              "mfg": {
                                    "type": "string"
                              },
                              "mah": {
                                    "type": "string"
                              },

                              "dis": {
                                    "type": "string"
                              },
                              "vd": {
                                    "type": "array",
                                    "items": [{
                                          "type": "object",
                                          "properties": {

                                          "dvc": {
                                                "type": "string",
                                                "description": "Format
                                                            YYYY-MM-DD"
                                          },
                                          "seq": {
                                                "type": "integer"
                                          },
                                          "tot": {
                                                "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"],
                  "anyOf": [
                        { "required":[ "mfg" ] },
                        { "required":[ "mah" ] }],

            }]
      },
      "opt": {
                  "type": "string"
            }


      },
      "required": ["uvci","pid",
      "ve"]
}
```

4.2.3 PoV Version 1

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

4.2.3.1 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

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

Section		Data element	Description	Preferred Code System
		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

4.2.3.2 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 9: Format of the PoV

`Object: Message {`

Element	Content	Max size
`UVCI(uvci)`	Unique Vaccination Certificate Identifier	18

`Object: PersonIdentification(pid) {`

{

Element	Content	Max size
`Name(n)`	Name of the holder	39
`Date of birth(dob)`	Date of birth of holder 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 holder 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/164949870)	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)`** **[{**

`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"]
}
```

4.3 Proof of Recovery (PoR)

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

For Proof of Recovery the Signature Field MUST be included.

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

4.3.1 PoR Signer Certificate Profile

The documentType value for this use-case is NR.

4.3.2 Data Set

The data set for PoR is derived from the ICAO recommendations for Proof of Recovery certificates.

DATA FIELDS

URCI	Unique Recovery Certificate Identifier (REQUIRED)
Certificate valid from	Date in which the certificate for a test result became valid. (Complete date, without time, following the ISO 8601.) (OPTIONAL)
Certificate valid until	Last date in which the certificate for a test result is valid. (Complete date, without time, following the ISO 8601.) (OPTIONAL)

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)

Test Result:

a) Member state of test (REQUIRED)
b) Date of first positive NAAT test result (Complete date, without time, following the ISO 8601) (REQUIRED)

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 to Doc 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/IEC 18013-1. Mobile Driving Licenses are not included)

4.3.3 Schema Definition

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

Table 10*: Format of the PoR*

Object: Message {

Element	Content	Max size
URCI(urci)	Unique Recovery Certificate Identifier	18
Certificate Valid From (cvf)	Date in which the certificate for a test result became valid. ISO8601 YYYY-MM-DD	10
Certificate Valid Until (cvu)	Last date in which the certificate for a test result is valid. ISO8601 YYYY-MM-DD	10

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:	

	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)	
`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: `TestResult(tr)` {

Element	Content	Max size
`Member state of test (sot)`	Three letter code identifying the country of test.	3
`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	10
}		

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 PoR is as follows:

```
{
      "$id": "http://namespaces.icao.int/VDS-NC_message_PoR_ICAO.json",
      "title": "Message Zone ICAO (PoR)",
      "type": "object",
      "description": "PoR Message Schema",
      "type": "object",
      "properties": {
            "urci": {
                  "type": "string"
            },
            "cvf": {
                  "type": "string",
                  "description": "Certificate valid from.
                        Format YYYY-MM-DD."
                        },
            "cvu": {
                  "type": "string",
                  "description": "Certificate valid until.
                        Format YYYY-MM-DD."
                        },
            "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
            },
            "tr": {
                  "type": "object",
                  "properties": {
                        "sot": {
                              "type": "string",
                              "description": "Three letter code
                        identifying the country of test."
                        },
                        "dnt": {
                              "type": "string",
                              "description": "Date of sample for NAAT test
                              with positive result. Format YYYY-MM-DD."
                        },
                  },
                  "required": ["sot",
                  "dnt"],
                  "additionalProperties": false
            },
            "opt": {
                  "type": "string"
            }
      },
      "required": ["urci","pid",
      "tr"]
}
```

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)

[ISO 8601]] ISO 8601 Date and time — Representations for information interchange

[ISO/IEC 16022] ISO/IEC 16022 Information technology — Automatic identification and data capture techniques — Data Matrix bar code symbology specification

[ISO/IEC 18004] ISO/IEC 18004 Information technology — Automatic identification and data capture techniques — QR Code bar code symbology specification

[ISO/IEC 24778] ISO/IEC 24778 Information technology — Automatic identification and data capture techniques — Aztec Code bar code symbology specification

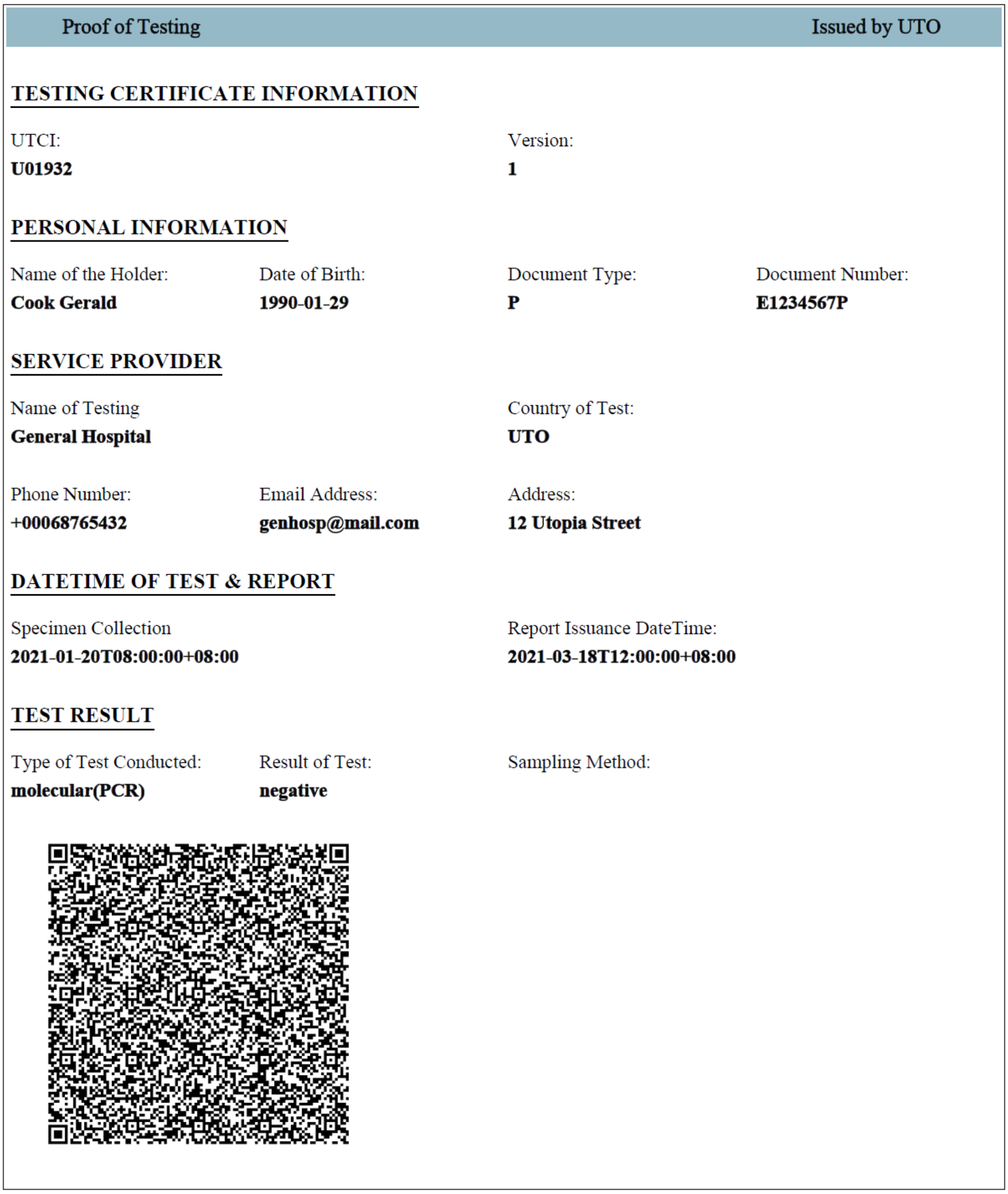
Annex A Abbreviations

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
CRLDP	CRL Distribution Point
ECDSA	Elliptic Curve Digital Signature Algorithm
WHO	World Health Organization
WHO EUL	World Health Organization Emergency Use List

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":"2021-01-20T08:00:00+08:00",
                        "ri":"2021-03-18T12:00:00+08:00"
                  },
                  "tr":{
                        "tc":"molecular(PCR)",
                        "r":"negative"
                  }
            }
      },
      "sig":{
            "alg":"ES256",
            "cer":"MIIBfTCCASCgAwIBAgIBbTAMBggqhkjOPQQ...",
            "sigvl":"-xLZ2iTKzZItWUrq4Dmd4wSfnjkNOn3LG..."
      }
}
```



Proof of Testing — Issued by UTO

TESTING CERTIFICATE INFORMATION

UTCI:	Version:
U01932	**1**

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	Country of Test:
General Hospital	**UTO**

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

DATETIME OF TEST & REPORT

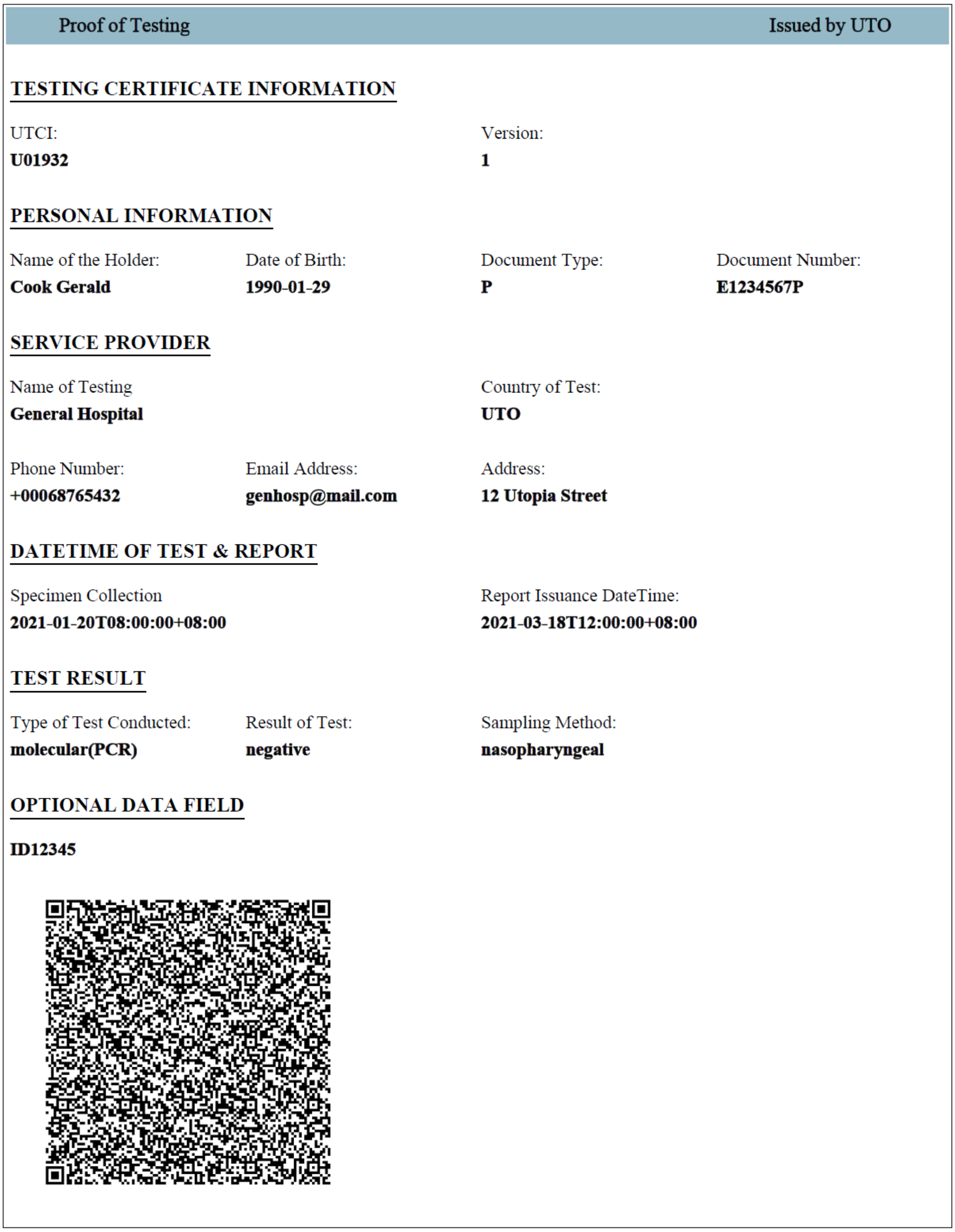
Specimen Collection	Report Issuance DateTime:
2021-01-20T08:00:00+08:00	**2021-03-18T12:00:00+08:00**

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":"2021-01-20T08:00:00+08:00",
                        "ri":"2021-03-18T12:00:00+08:00"
                  },
                  "tr":{
                        "tc":"molecular(PCR)",
                        "r":"negative",
                        "m":"nasopharyngeal"
                  },
                  "opt":"ID12345"
            }
      },
      "sig":{
            "alg":"ES256",
            "cer":"MIIBfTCCASCgAwIBAgIBbTAMBggqhkjOPQQ...",
            "sigvl":"D4xQVxoE2L_xhttv3Tf7sXvo7HG7umOfb..."
      }
}
```



Proof of Testing Issued by UTO

TESTING CERTIFICATE INFORMATION

UTCI:	Version:
U01932	**1**

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	Country of Test:
General Hospital	**UTO**

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

DATETIME OF TEST & REPORT

Specimen Collection	Report Issuance DateTime:
2021-01-20T08:00:00+08:00	**2021-03-18T12:00:00+08:00**

TEST RESULT

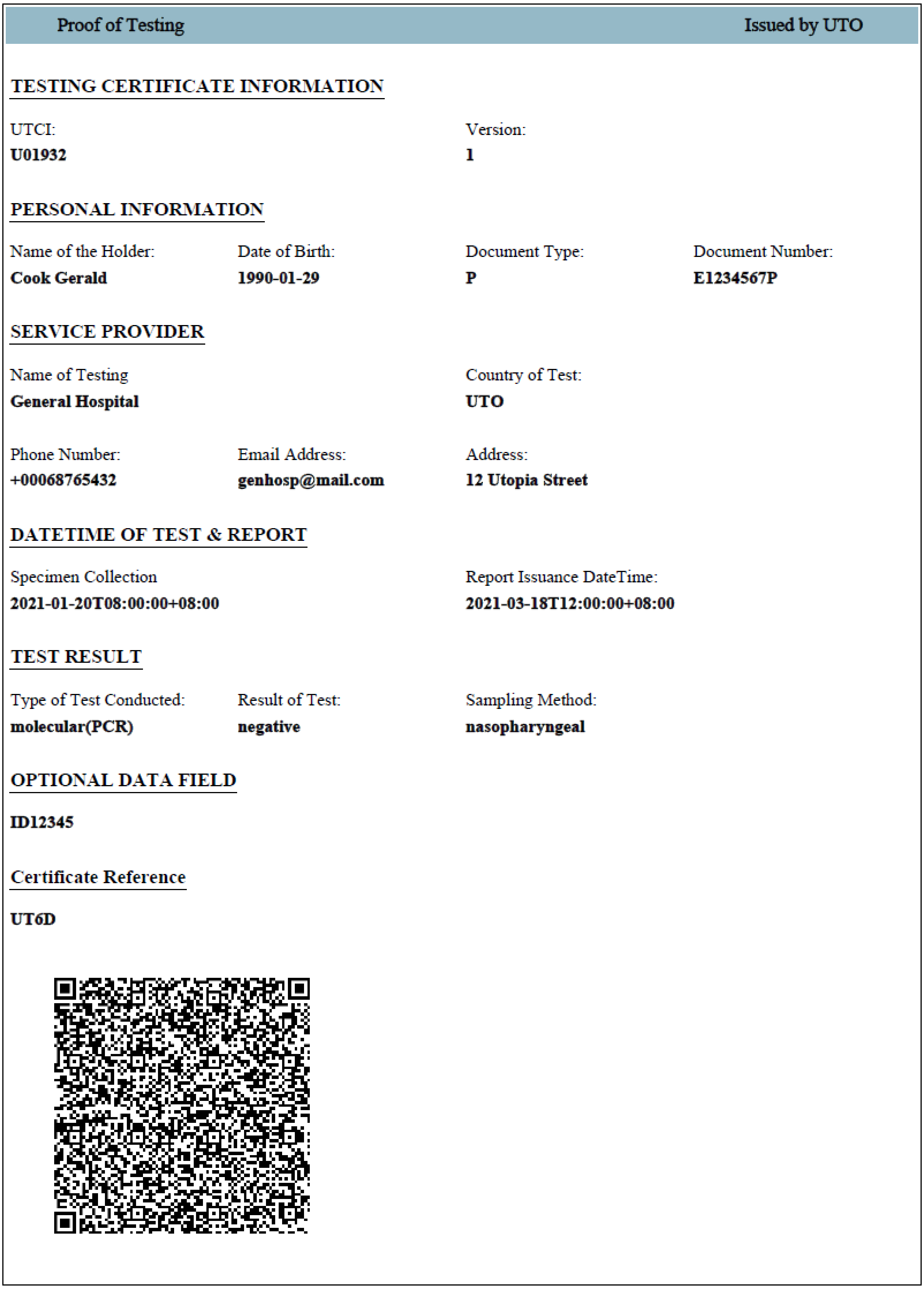
Type of Test Conducted:	Result of Test:	Sampling Method:
molecular(PCR)	**negative**	**nasopharyngeal**

OPTIONAL DATA FIELD

ID12345

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

```
{
      "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":"2021-01-20T08:00:00+08:00",
                        "ri":"2021-03-18T12:00:00+08:00"
                  },
                  "tr":{
                        "tc":"molecular(PCR)",
                        "r":"negative",
                        "m":"nasopharyngeal"
                  },
                  "opt":"ID12345"
            }
      },
      "sig":{
            "alg":"ES256",
            "cref":"UT6D",
            "sigvl":"r714fHdx7t3dkE9oz3cZP8aGbO_OV..."
      }
}
```



Proof of Testing	Issued by UTO

TESTING CERTIFICATE INFORMATION

UTCI:	Version:
U01932	**1**

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		Country of Test:
General Hospital		**UTO**
Phone Number:	Email Address:	Address:
+00068765432	**genhosp@mail.com**	**12 Utopia Street**

DATETIME OF TEST & REPORT

Specimen Collection	Report Issuance DateTime:
2021-01-20T08:00:00+08:00	**2021-03-18T12:00:00+08:00**

TEST RESULT

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

OPTIONAL DATA FIELD

ID12345

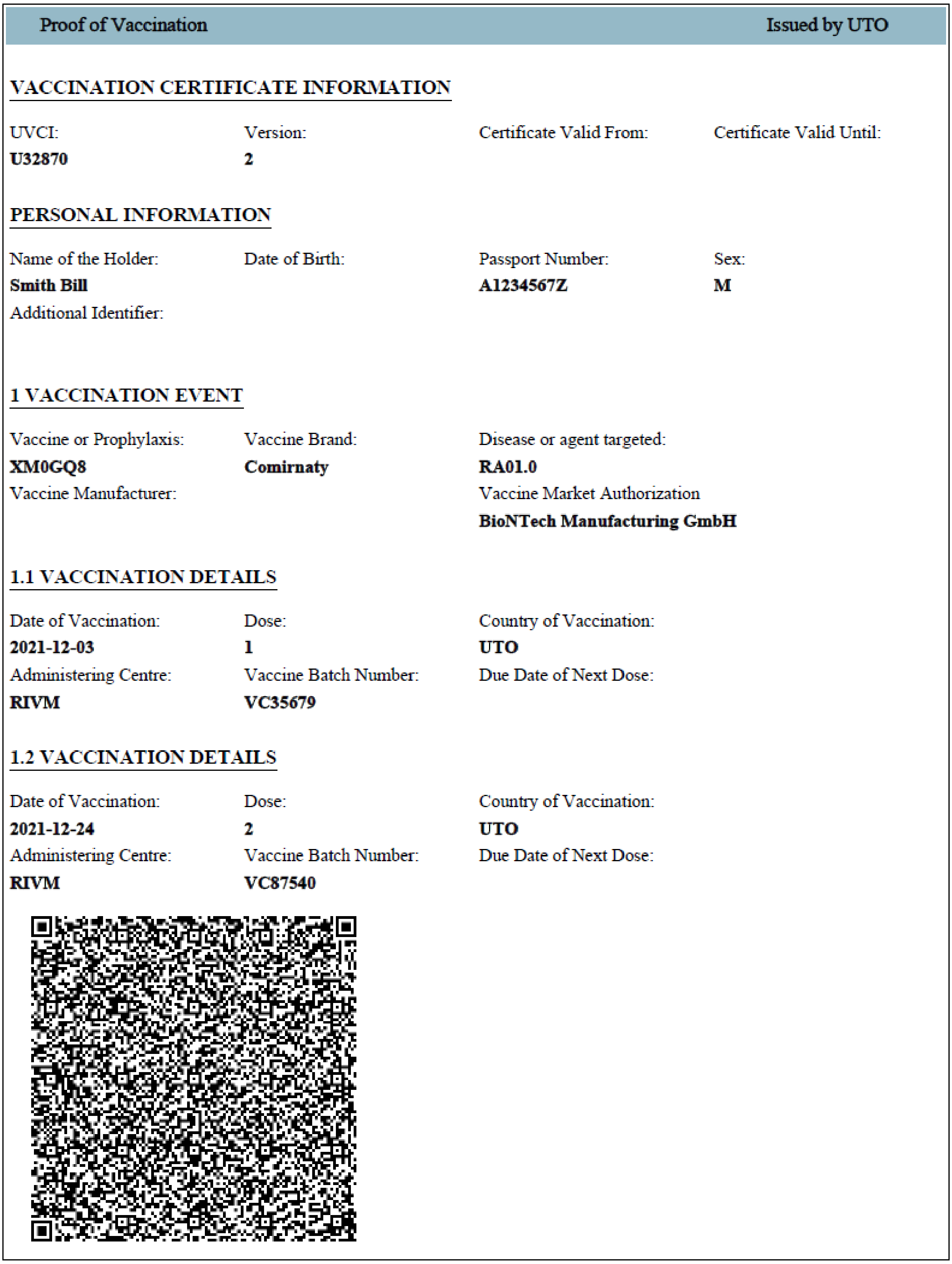
Certificate Reference

UT6D

Annex C Worked Example – PoV Version 2 (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":2,"is":"UTO"
                  },
                  "msg":{
                        "uvci":"U32870",
                        "pid":{
                              "n":"Smith Bill",
                              "sex":"M",
                              "i":"A1234567Z"
                        },
                        "ve":[{
                              "des":"XM0GQ8",
                              "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":"MIIBfTCCASCgAwIBAgIBbDAMBggqhkjOPQQD...",
                  "sigvl":"E89teR1TvGmcV0moFJO9SUZ-xaCUT2wCaV..."
           }
}
```



Proof of Vaccination **Issued by UTO**

VACCINATION CERTIFICATE INFORMATION

UVCI:	Version:	Certificate Valid From:	Certificate Valid Until:
U32870	**2**		

PERSONAL INFORMATION

Name of the Holder:	Date of Birth:	Passport Number:	Sex:
Smith Bill		**A1234567Z**	**M**
Additional Identifier:			

1 VACCINATION EVENT

Vaccine or Prophylaxis:	Vaccine Brand:	Disease or agent targeted:
XM0GQ8	**Comirnaty**	**RA01.0**
Vaccine Manufacturer:		Vaccine Market Authorization
		BioNTech Manufacturing GmbH

1.1 VACCINATION DETAILS

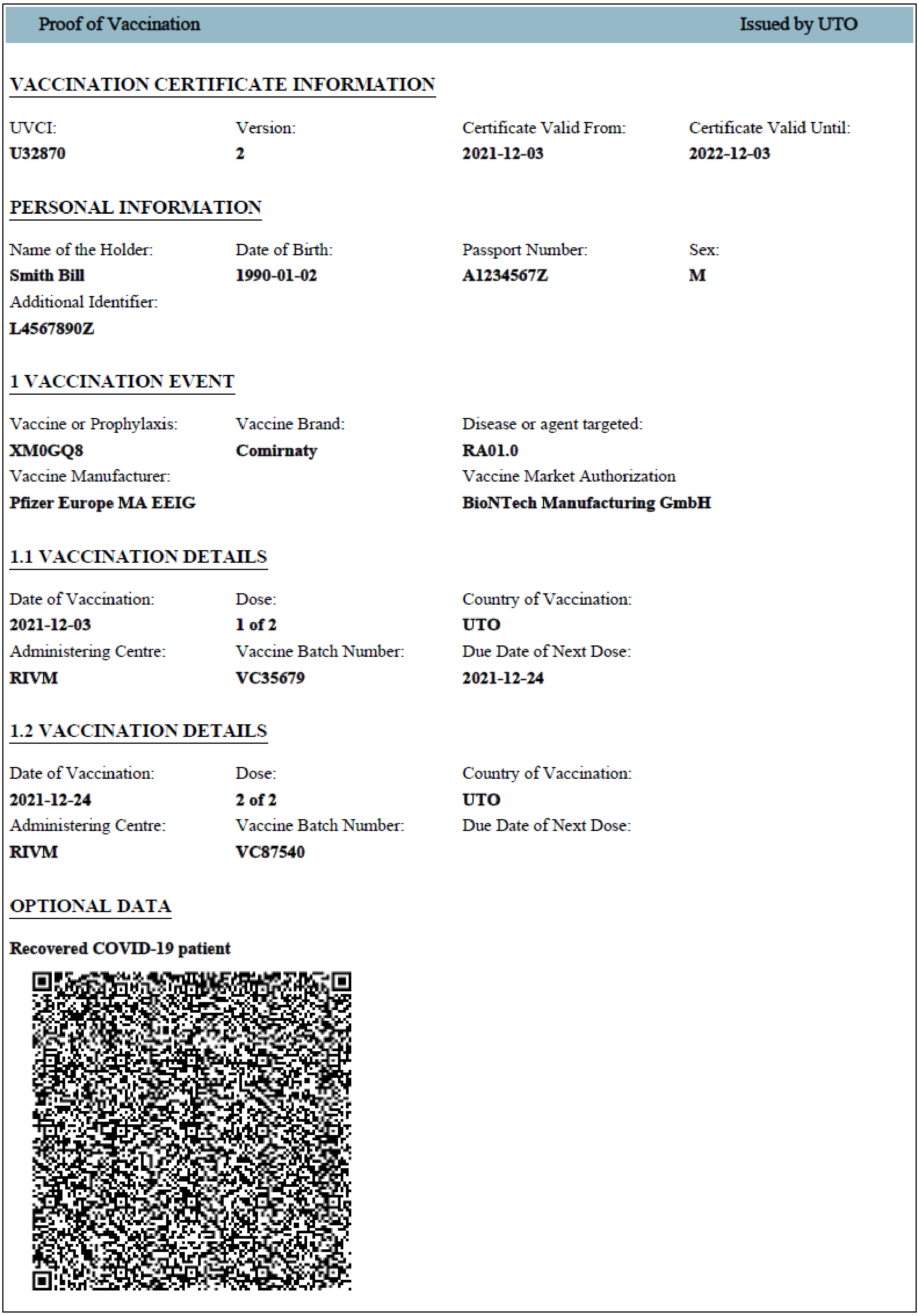
Date of Vaccination:	Dose:	Country of Vaccination:
2021-12-03	**1**	**UTO**
Administering Centre:	Vaccine Batch Number:	Due Date of Next Dose:
RIVM	**VC35679**	

1.2 VACCINATION DETAILS

Date of Vaccination:	Dose:	Country of Vaccination:
2021-12-24	**2**	**UTO**
Administering Centre:	Vaccine Batch Number:	Due Date of Next Dose:
RIVM	**VC87540**	

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":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":"XM0GQ8",
                        "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":"MIIBfTCCASCgAwIBAgIBbDAMBggqhkjOPQQD...",
            "sigvl":"xq1Z8THzT0ilT2GjRPR93mf5lW58Xlo6-F..."
      }
}
```



Proof of Vaccination — Issued by UTO

VACCINATION CERTIFICATE INFORMATION

UVCI: **U32870**	Version: **2**	Certificate Valid From: **2021-12-03**	Certificate Valid Until: **2022-12-03**

PERSONAL INFORMATION

Name of the Holder: **Smith Bill**	Date of Birth: **1990-01-02**	Passport Number: **A1234567Z**	Sex: **M**
Additional Identifier: **L4567890Z**			

1 VACCINATION EVENT

Vaccine or Prophylaxis: **XM0GQ8**	Vaccine Brand: **Comirnaty**	Disease or agent targeted: **RA01.0**
Vaccine Manufacturer: **Pfizer Europe MA EEIG**		Vaccine Market Authorization **BioNTech Manufacturing GmbH**

1.1 VACCINATION DETAILS

Date of Vaccination: **2021-12-03**	Dose: **1 of 2**	Country of Vaccination: **UTO**
Administering Centre: **RIVM**	Vaccine Batch Number: **VC35679**	Due Date of Next Dose: **2021-12-24**

1.2 VACCINATION DETAILS

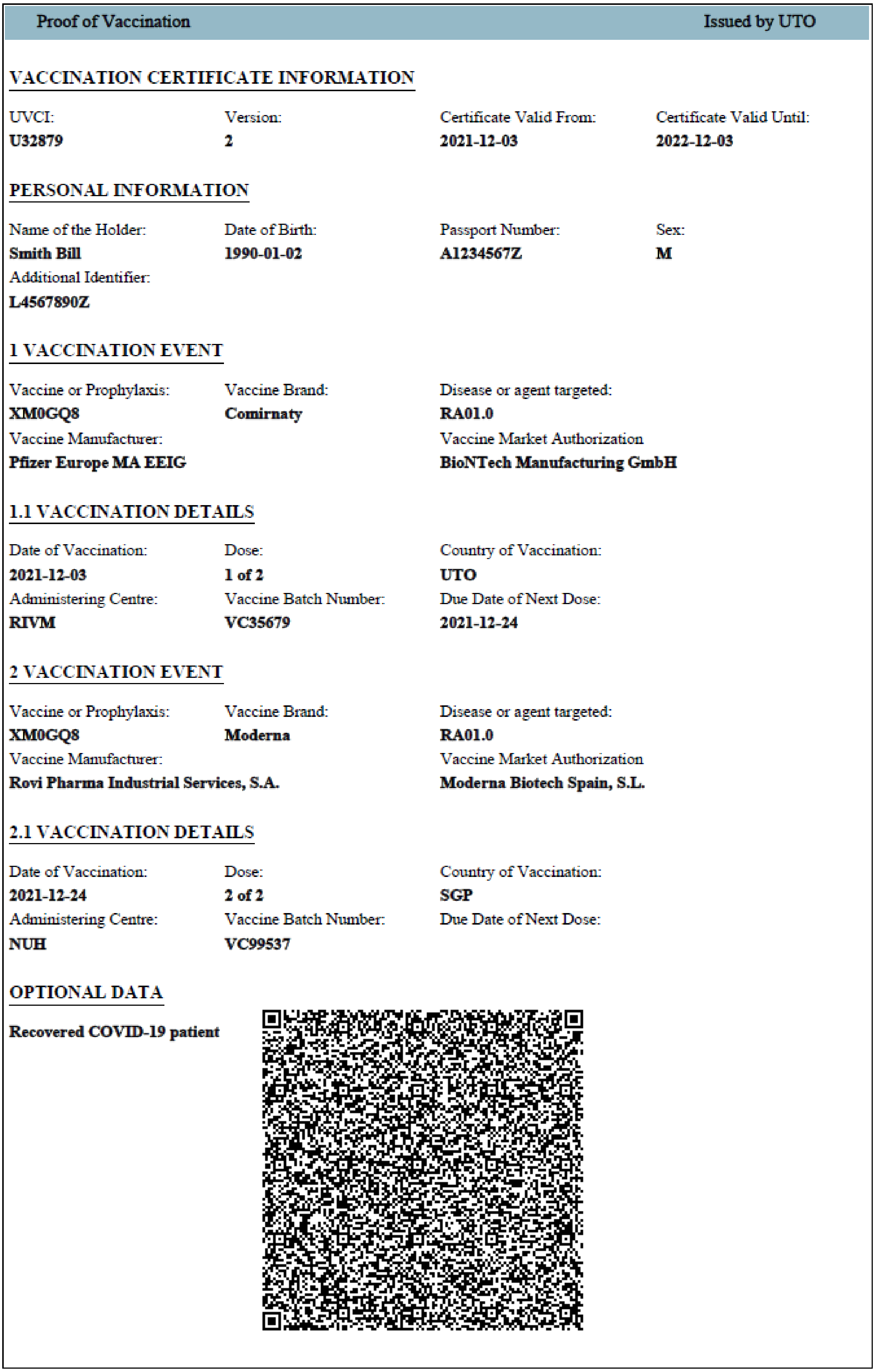
Date of Vaccination: **2021-12-24**	Dose: **2 of 2**	Country of Vaccination: **UTO**
Administering Centre: **RIVM**	Vaccine Batch Number: **VC87540**	Due Date of Next Dose:

OPTIONAL DATA

Recovered COVID-19 patient

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":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":"XM0GQ8",
                              "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":"XM0GQ8",
                              "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":"MIIBfTCCASCgAwIBAgIBbDAMBggqhkjOPQQD...",
                  "sigvl":"gKVP4S-MBL98bTiUciOQt5hYfLi_zy6Wko..."
           }
}
```



Proof of Vaccination Issued by UTO

VACCINATION CERTIFICATE INFORMATION

UVCI:	Version:	Certificate Valid From:	Certificate Valid Until:
U32879	**2**	**2021-12-03**	**2022-12-03**

PERSONAL INFORMATION

Name of the Holder:	Date of Birth:	Passport Number:	Sex:
Smith Bill	**1990-01-02**	**A1234567Z**	**M**
Additional Identifier:			
L4567890Z			

1 VACCINATION EVENT

Vaccine or Prophylaxis:	Vaccine Brand:	Disease or agent targeted:
XM0GQ8	**Comirnaty**	**RA01.0**
Vaccine Manufacturer:		Vaccine Market Authorization
Pfizer Europe MA EEIG		**BioNTech Manufacturing GmbH**

1.1 VACCINATION DETAILS

Date of Vaccination:	Dose:	Country of Vaccination:
2021-12-03	**1 of 2**	**UTO**
Administering Centre:	Vaccine Batch Number:	Due Date of Next Dose:
RIVM	**VC35679**	**2021-12-24**

2 VACCINATION EVENT

Vaccine or Prophylaxis:	Vaccine Brand:	Disease or agent targeted:
XM0GQ8	**Moderna**	**RA01.0**
Vaccine Manufacturer:		Vaccine Market Authorization
Rovi Pharma Industrial Services, S.A.		**Moderna Biotech Spain, S.L.**

2.1 VACCINATION DETAILS

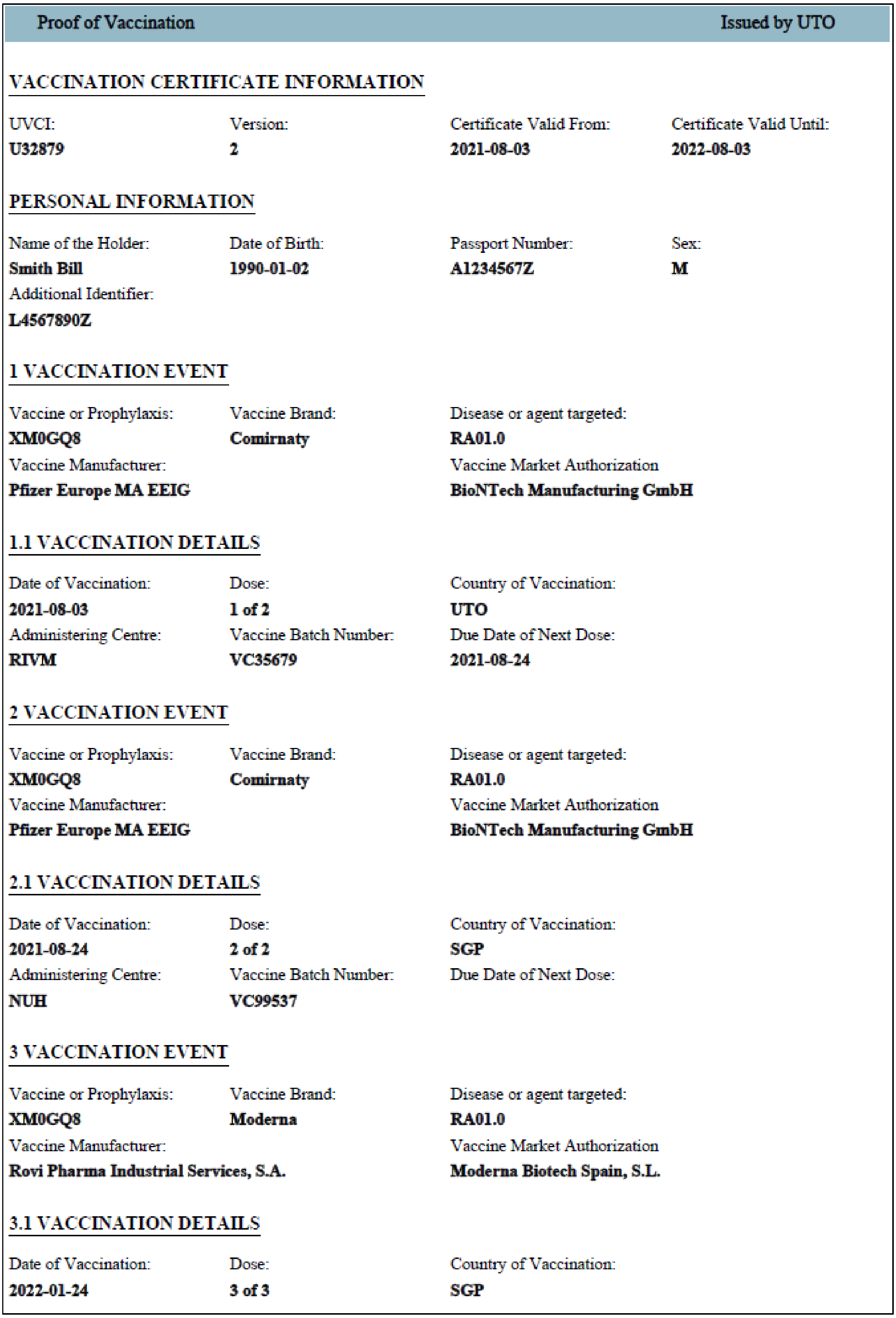
Date of Vaccination:	Dose:	Country of Vaccination:
2021-12-24	**2 of 2**	**SGP**
Administering Centre:	Vaccine Batch Number:	Due Date of Next Dose:
NUH	**VC99537**	

OPTIONAL DATA

Recovered COVID-19 patient

The following is an example of PoV using a different vaccine for booster dose with REQUIRED, RECOMMENDED and OPTIONAL fields.

```
{
           "data":{
                  "hdr":{
                        "t":"icao.vacc",
                        "v":2,
                        "is":"UTO"
                  },
                  "msg":{
                        "uvci":"U32870",
                        "cvf":"2021-08-03",
                        "cvu":"2022-08-03",
                        "pid":{
                              "n":"Smith Bill",
                              "dob":"1990-01-02",
                              "sex":"M",
                              "i":"A1234567Z",
                              "ai":"L4567890Z"
                        },
                        "ve":[{
                              "des":"XM0GQ8",
                              "nam":"Comirnaty",
                              "mfg":"Pfizer Europe MA EEIG",
                              "mah":"BioNTech Manufacturing GmbH",
                              "dis":"RA01.0",
                              "vd":[{
                                    "dvc":"2021-08-03",
                                    "seq":1,
                                    "tot":2,
                                    "ctr":"UTO",
                                    "adm":"RIVM",
                                    "lot":"VC35679",
                                    "dvn":"2021-08-24"
                              }]
                        },
                        {
                              "des":"XM0GQ8",
                              "nam":"Comirnaty",
                              "mfg":"Pfizer Europe MA EEIG",
                              "mah":"BioNTech Manufacturing GmbH",
                              "dis":"RA01.0",
                              "vd":[{
                                    "dvc":"2021-08-24",
                                    "seq":2,
                                    "tot":2,
                                    "ctr":"SGP",
                                    "adm":"NUH",
                                    "lot":"VC99537"
                              }]
                        },
                        {
                              "des":"XM0GQ8",
                              "nam":"Moderna",
                              "mfg":"Rovi Pharma Industrial Services,
S.A.",
                              "mah":"Moderna Biotech Spain, S.L.",
                              "dis":"RA01.0",
                              "vd":[{
                                    "dvc":"2022-01-24",
                                    "seq":3,
                                    "tot":3,
                                    "ctr":"SGP",
                                    "adm":"NUH",
                                    "lot":"VC66498"
                              }]
                        }],
                        "opt":"Recovered COVID-19 patient"
                  }
           },
           "sig":{
                  "alg":"ES256",
                  "cer":"MIIBfTCCASCgAwIBAgIBbDAMBggqhkjOPQQD...",
                  "sigvl":"vusImPobOySS8-QaCSno7J1A_fjipUEVUh..."
           }
}
```



Proof of Vaccination **Issued by UTO**

VACCINATION CERTIFICATE INFORMATION

UVCI:	Version:	Certificate Valid From:	Certificate Valid Until:
U32879	**2**	**2021-08-03**	**2022-08-03**

PERSONAL INFORMATION

Name of the Holder:	Date of Birth:	Passport Number:	Sex:
Smith Bill	**1990-01-02**	**A1234567Z**	**M**
Additional Identifier:			
L4567890Z			

1 VACCINATION EVENT

Vaccine or Prophylaxis:	Vaccine Brand:	Disease or agent targeted:
XM0GQ8	**Comirnaty**	**RA01.0**
Vaccine Manufacturer:		Vaccine Market Authorization
Pfizer Europe MA EEIG		**BioNTech Manufacturing GmbH**

1.1 VACCINATION DETAILS

Date of Vaccination:	Dose:	Country of Vaccination:
2021-08-03	**1 of 2**	**UTO**
Administering Centre:	Vaccine Batch Number:	Due Date of Next Dose:
RIVM	**VC35679**	**2021-08-24**

2 VACCINATION EVENT

Vaccine or Prophylaxis:	Vaccine Brand:	Disease or agent targeted:
XM0GQ8	**Comirnaty**	**RA01.0**
Vaccine Manufacturer:		Vaccine Market Authorization
Pfizer Europe MA EEIG		**BioNTech Manufacturing GmbH**

2.1 VACCINATION DETAILS

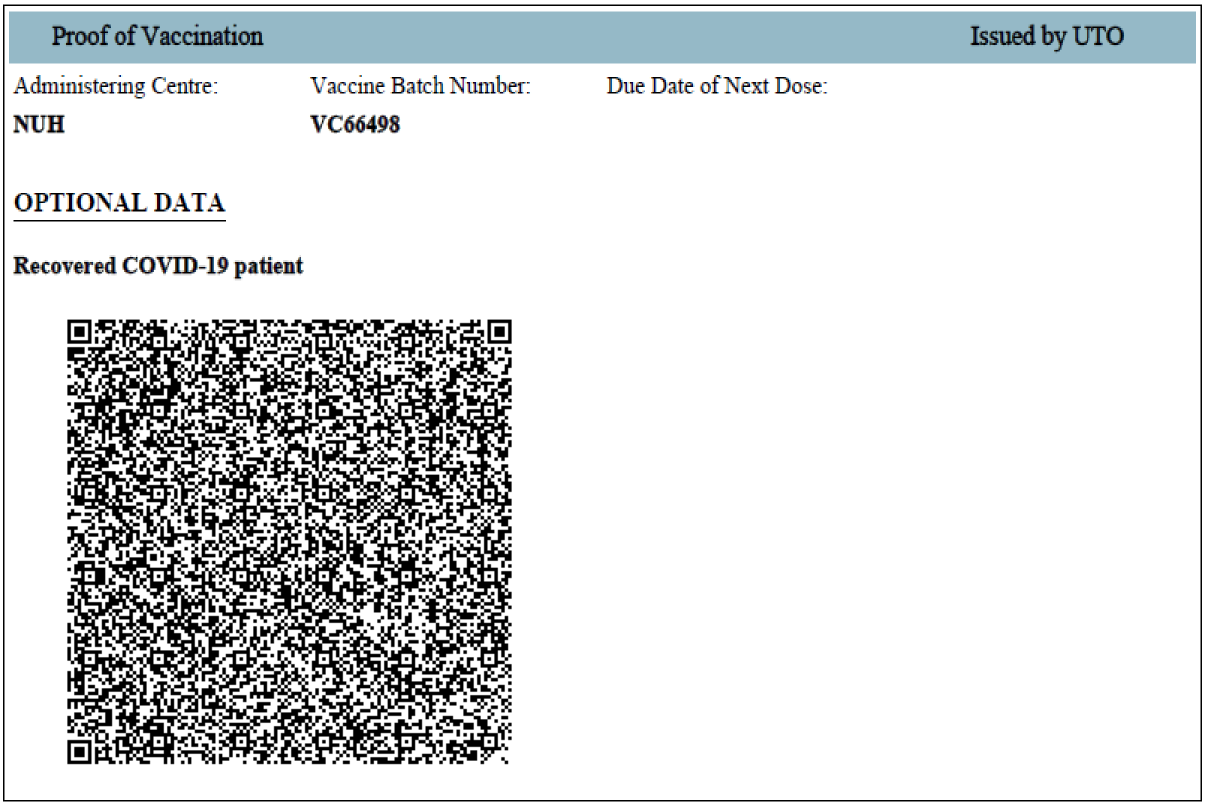
Date of Vaccination:	Dose:	Country of Vaccination:
2021-08-24	**2 of 2**	**SGP**
Administering Centre:	Vaccine Batch Number:	Due Date of Next Dose:
NUH	**VC99537**	

3 VACCINATION EVENT

Vaccine or Prophylaxis:	Vaccine Brand:	Disease or agent targeted:
XM0GQ8	**Moderna**	**RA01.0**
Vaccine Manufacturer:		Vaccine Market Authorization
Rovi Pharma Industrial Services, S.A.		**Moderna Biotech Spain, S.L.**

3.1 VACCINATION DETAILS

Date of Vaccination:	Dose:	Country of Vaccination:
2022-01-24	**3 of 3**	**SGP**



Proof of Vaccination **Issued by UTO**

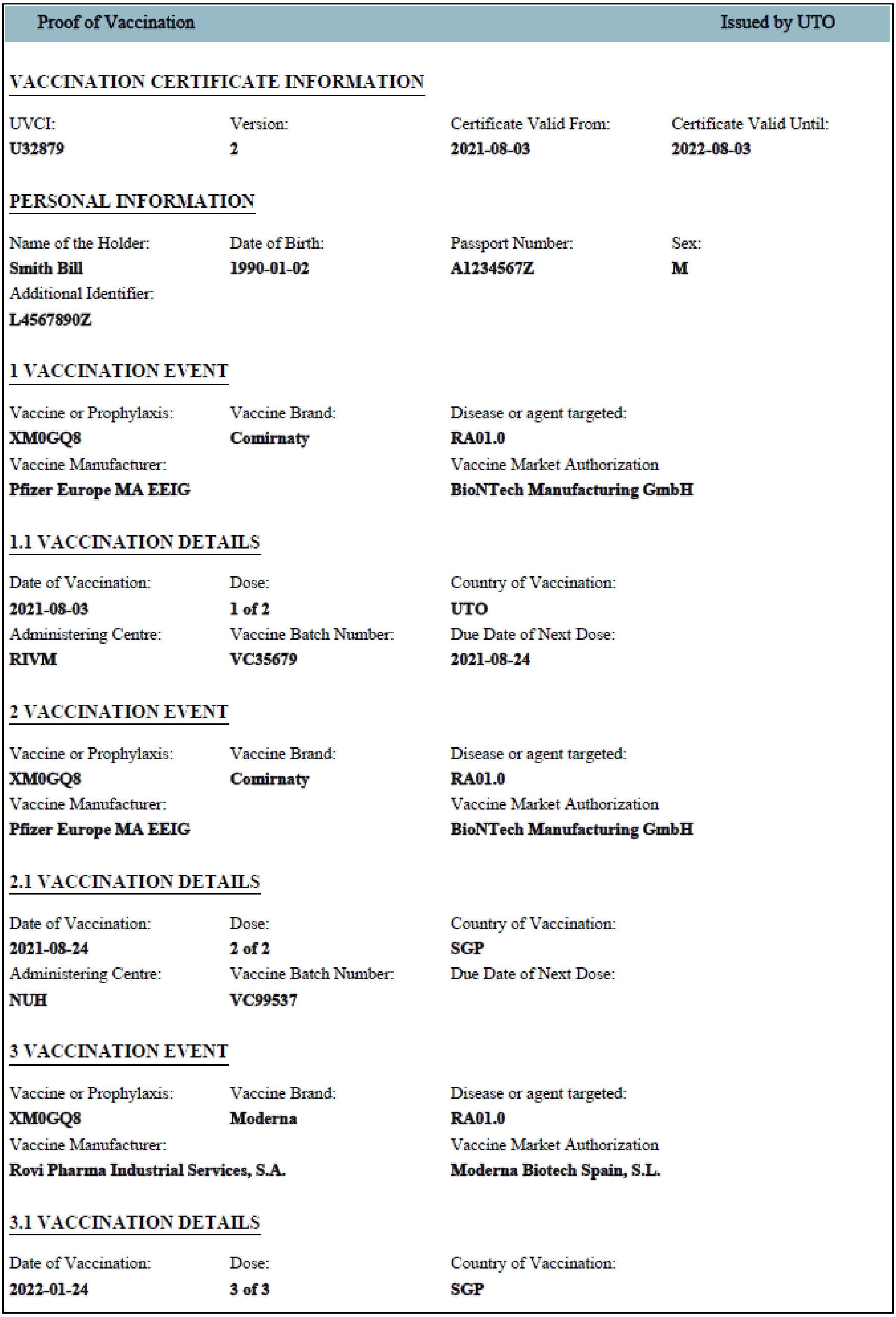
Administering Centre:	Vaccine Batch Number:	Due Date of Next Dose:
NUH	**VC66498**	

OPTIONAL DATA

Recovered COVID-19 patient

The following is an example of PoV using a different vaccine for booster dose with REQUIRED, RECOMMENDED,OPTIONAL fields and Certificate Reference.

```
{
           "data":{
                  "hdr":{
                        "t":"icao.vacc",
                        "v":2,
                        "is":"UTO"
                  },
                  "msg":{
                        "uvci":"U32879",
                        "cvf":"2021-08-03",
                        "cvu":"2022-08-03",
                        "pid":{
                              "n":"Smith Bill",
                              "dob":"1990-01-02",
                              "sex":"M",
                              "i":"A1234567Z",
                              "ai":"L4567890Z"
                        },
                        "ve":[{
                              "des":"XM0GQ8",
                              "nam":"Comirnaty",
                              "mfg":"Pfizer Europe MA EEIG",
                              "mah":"BioNTech Manufacturing GmbH",
                              "dis":"RA01.0",
                              "vd":[{
                                    "dvc":"2021-08-03",
                                    "seq":1,
                                    "tot":2,
                                    "ctr":"UTO",
                                    "adm":"RIVM",
                                    "lot":"VC35679",
                                    "dvn":"2021-08-24"
                              }]
                        },
                        {
                              "des":"XM0GQ8",
                              "nam":"Comirnaty",
                              "mfg":"Pfizer Europe MA EEIG",
                              "mah":"BioNTech Manufacturing GmbH",
                              "dis":"RA01.0",
                              "vd":[{
                                    "dvc":"2021-08-24",
                                    "seq":2,
                                    "tot":2,
                                    "ctr":"SGP",
                                    "adm":"NUH",
                                    "lot":"VC99537"
                              }]
                        },
                        {
                              "des":"XM0GQ8",
                              "nam":"Moderna",
                              "mfg":"Rovi Pharma Industrial Services,
S.A.",
                              "mah":"Moderna Biotech Spain, S.L.",
                              "dis":"RA01.0",
                              "vd":[{
                                    "dvc":"2022-01-24",
                                    "seq":3,
                                    "tot":3,
                                    "ctr":"SGP",
                                    "adm":"NUH",
                                    "lot":"VC66498"
                              }]
                        }],
                        "opt":"Recovered COVID-19 patient"
                  }
           },
           "sig":{
                  "alg":"ES256",
                  "cref":"UT6C",
                  "sigvl":"3gLHjfVKnefbRWtvLcw0dBFsY6hIMbRUCtOT4cDnZWT8..."
           }
}
```



Proof of Vaccination | Issued by UTO

VACCINATION CERTIFICATE INFORMATION

UVCI:	Version:	Certificate Valid From:	Certificate Valid Until:
U32879	**2**	**2021-08-03**	**2022-08-03**

PERSONAL INFORMATION

Name of the Holder:	Date of Birth:	Passport Number:	Sex:
Smith Bill	**1990-01-02**	**A1234567Z**	**M**
Additional Identifier:			
L4567890Z			

1 VACCINATION EVENT

Vaccine or Prophylaxis:	Vaccine Brand:	Disease or agent targeted:
XM0GQ8	**Comirnaty**	**RA01.0**
Vaccine Manufacturer:		Vaccine Market Authorization
Pfizer Europe MA EEIG		**BioNTech Manufacturing GmbH**

1.1 VACCINATION DETAILS

Date of Vaccination:	Dose:	Country of Vaccination:
2021-08-03	**1 of 2**	**UTO**
Administering Centre:	Vaccine Batch Number:	Due Date of Next Dose:
RIVM	**VC35679**	**2021-08-24**

2 VACCINATION EVENT

Vaccine or Prophylaxis:	Vaccine Brand:	Disease or agent targeted:
XM0GQ8	**Comirnaty**	**RA01.0**
Vaccine Manufacturer:		Vaccine Market Authorization
Pfizer Europe MA EEIG		**BioNTech Manufacturing GmbH**

2.1 VACCINATION DETAILS

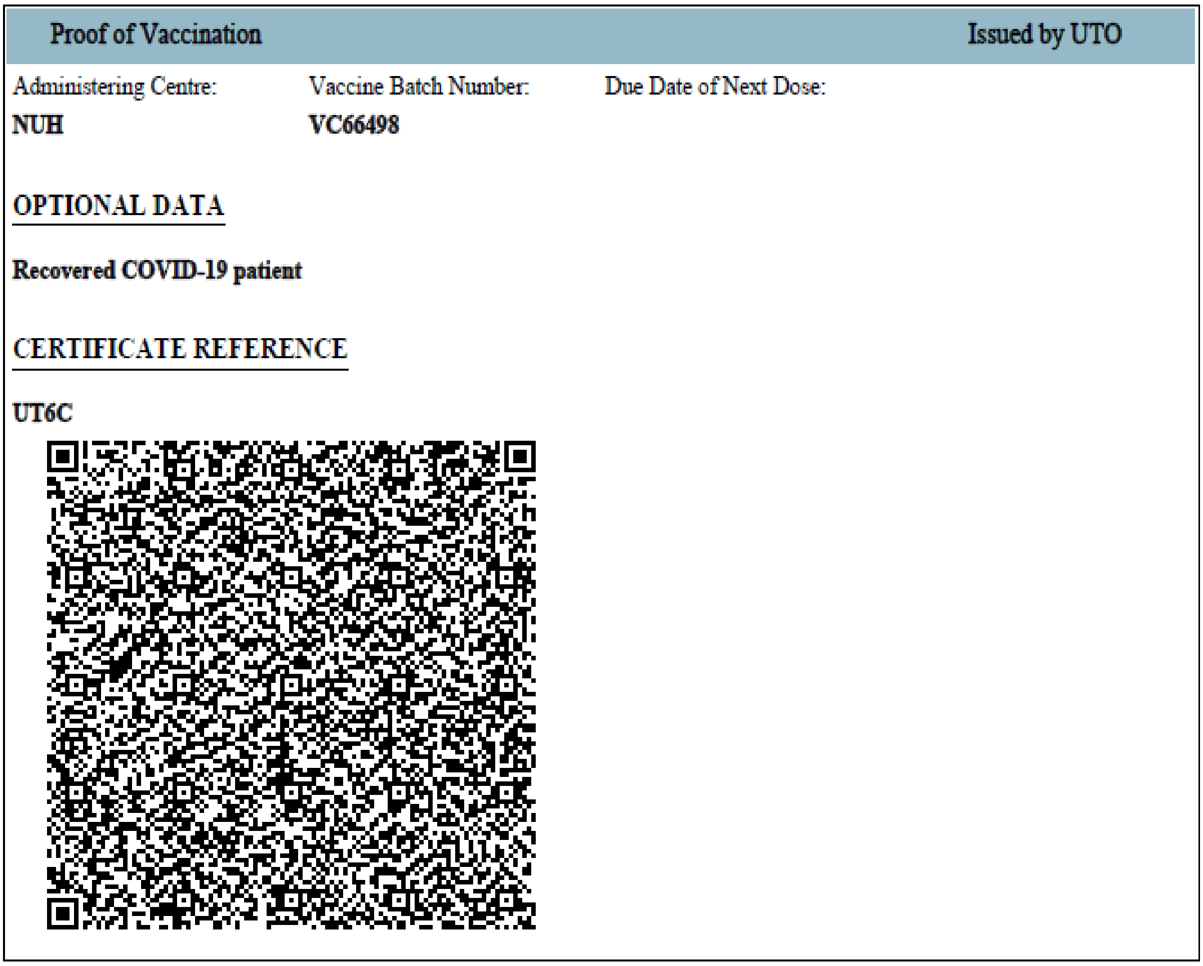
Date of Vaccination:	Dose:	Country of Vaccination:
2021-08-24	**2 of 2**	**SGP**
Administering Centre:	Vaccine Batch Number:	Due Date of Next Dose:
NUH	**VC99537**	

3 VACCINATION EVENT

Vaccine or Prophylaxis:	Vaccine Brand:	Disease or agent targeted:
XM0GQ8	**Moderna**	**RA01.0**
Vaccine Manufacturer:		Vaccine Market Authorization
Rovi Pharma Industrial Services, S.A.		**Moderna Biotech Spain, S.L.**

3.1 VACCINATION DETAILS

Date of Vaccination:	Dose:	Country of Vaccination:
2022-01-24	**3 of 3**	**SGP**



Proof of Vaccination **Issued by UTO**

Administering Centre:	Vaccine Batch Number:	Due Date of Next Dose:
NUH	**VC66498**	

OPTIONAL DATA

Recovered COVID-19 patient

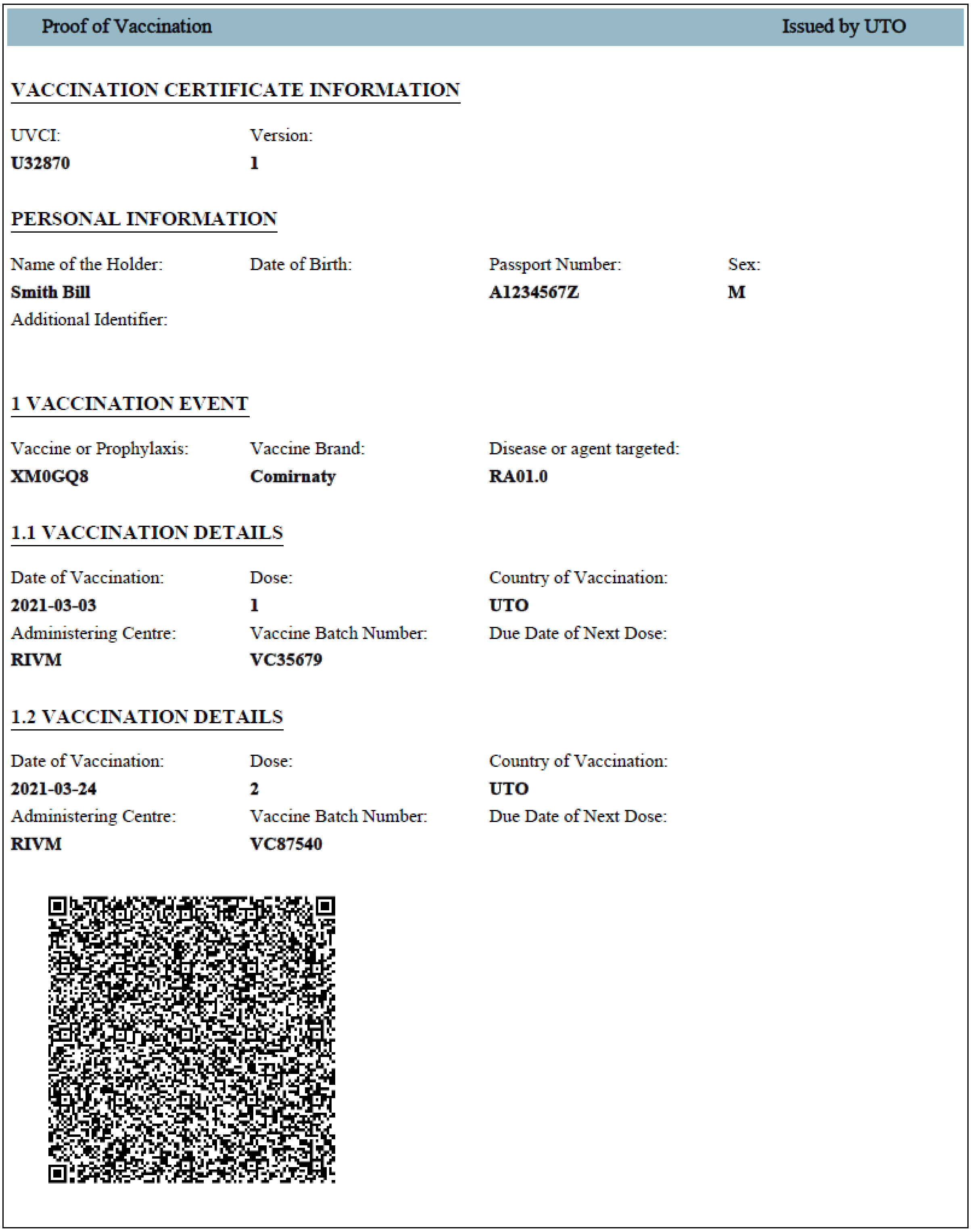
CERTIFICATE REFERENCE

UT6C

Annex D Worked Example – PoV Version 1 (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":"XM0GQ8",
                        "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":"MIIBfTCCASCgAwIBAgIBbDAMBggqhkjOPQQD...",
            "sigvl":"rDSc_TF5-dvccAo1ZHl3-fWHWG311ArPnB..."
      }
}
```



Proof of Vaccination Issued by UTO

VACCINATION CERTIFICATE INFORMATION

UVCI:	Version:
U32870	**1**

PERSONAL INFORMATION

Name of the Holder:	Date of Birth:	Passport Number:	Sex:
Smith Bill		**A1234567Z**	**M**
Additional Identifier:			

1 VACCINATION EVENT

Vaccine or Prophylaxis:	Vaccine Brand:	Disease or agent targeted:
XM0GQ8	**Comirnaty**	**RA01.0**

1.1 VACCINATION DETAILS

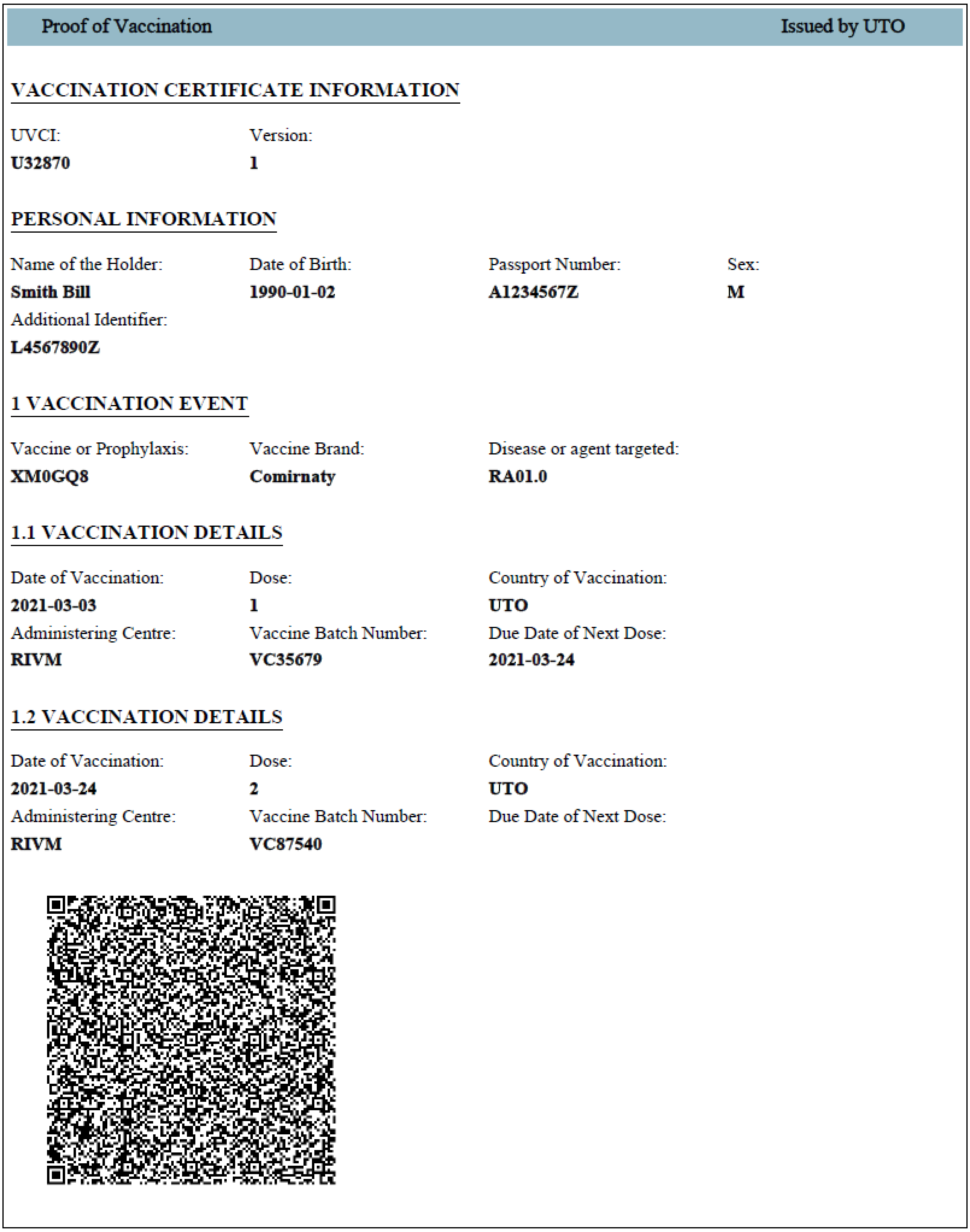
Date of Vaccination:	Dose:	Country of Vaccination:
2021-03-03	**1**	**UTO**
Administering Centre:	Vaccine Batch Number:	Due Date of Next Dose:
RIVM	**VC35679**	

1.2 VACCINATION DETAILS

Date of Vaccination:	Dose:	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 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":"XM0GQ8",
                        "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":"MIIBfTCCASCgAwIBAgIBbDAMBggqhkjOPQQD...",
            "sigvl":"7ewT9cIWDv0M5TzqylIgdnLdllnQ_OEQPt..."
      }
}
```



Proof of Vaccination Issued by UTO

VACCINATION CERTIFICATE INFORMATION

UVCI:	Version:
U32870	**1**

PERSONAL INFORMATION

Name of the Holder:	Date of Birth:	Passport Number:	Sex:
Smith Bill	**1990-01-02**	**A1234567Z**	**M**
Additional Identifier:			
L4567890Z			

1 VACCINATION EVENT

Vaccine or Prophylaxis:	Vaccine Brand:	Disease or agent targeted:
XM0GQ8	**Comirnaty**	**RA01.0**

1.1 VACCINATION DETAILS

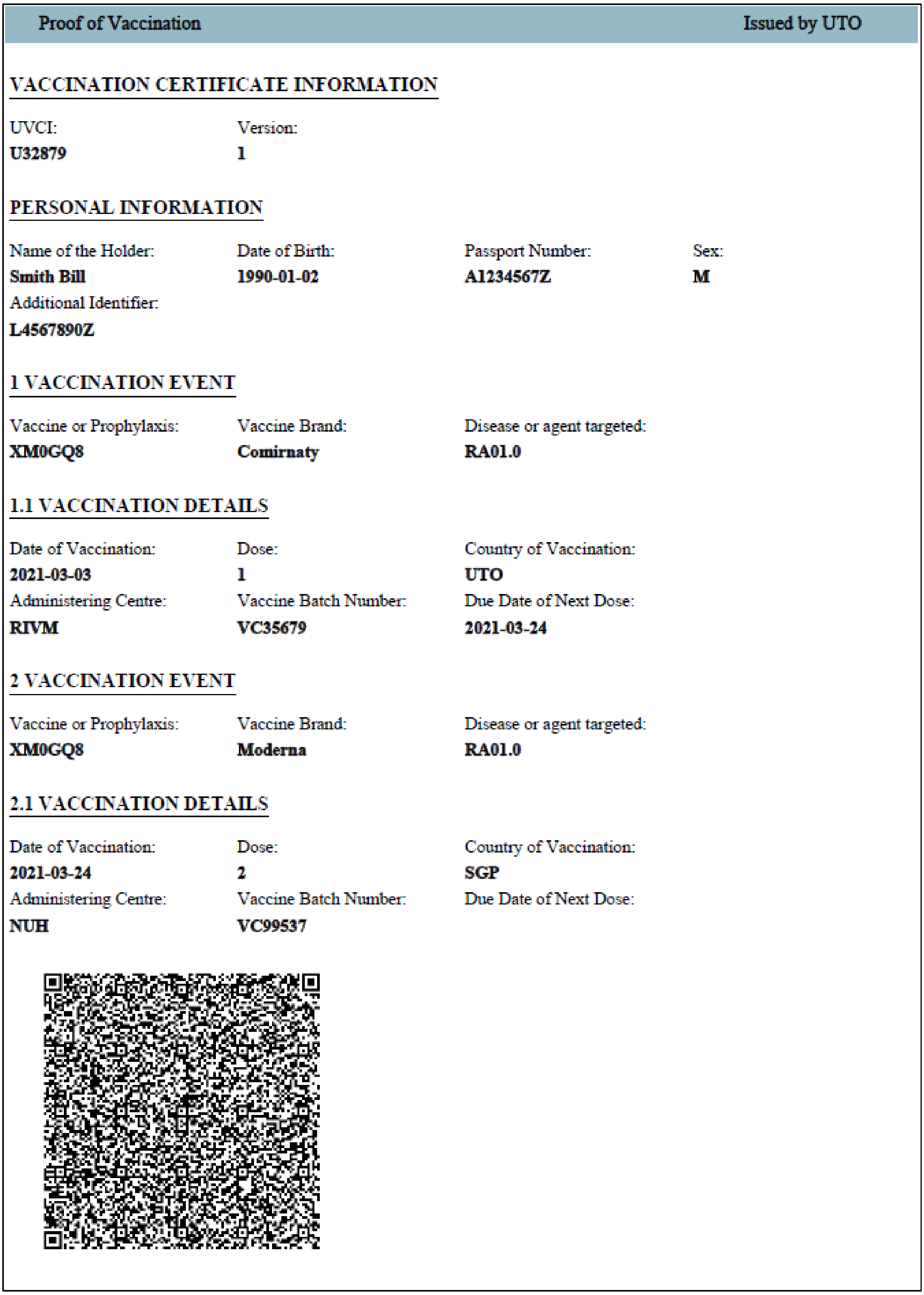
Date of Vaccination:	Dose:	Country of Vaccination:
2021-03-03	**1**	**UTO**
Administering Centre:	Vaccine Batch Number:	Due Date of Next Dose:
RIVM	**VC35679**	**2021-03-24**

1.2 VACCINATION DETAILS

Date of Vaccination:	Dose:	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":"XM0GQ8",
                              "nam":"Comirnaty",
                              "dis":"RA01.0",
                              "vd":[{
                                    "dvc":"2021-03-03",
                                    "seq":1,
                                    "ctr":"UTO",
                                    "adm":"RIVM",
                                    "lot":"VC35679",
                                    "dvn":"2021-03-24"
                              }]
                        },
                        {
                              "des":"XM0GQ8",
                              "nam":"Moderna",
                              "dis":"RA01.0",
                              "vd":[{
                                    "dvc":"2021-03-24",
                                    "seq":2,
                                    "ctr":"SGP",
                                    "adm":"NUH",
                                    "lot":"VC99537"
                              }]
                        }]
                  }
           },
           "sig":{
                  "alg":"ES256",
                  "cer":"MIIBfTCCASCgAwIBAgIBbDAMBggqhkjOPQQD...",
                  "sigvl":"xRgK33HDyIcf-3R5JxVKVQ5tvnlkGNCrJw..."
           }
}
```



Proof of Vaccination **Issued by UTO**

VACCINATION CERTIFICATE INFORMATION

UVCI:	Version:
U32879	**1**

PERSONAL INFORMATION

Name of the Holder:	Date of Birth:	Passport Number:	Sex:
Smith Bill	**1990-01-02**	**A1234567Z**	**M**
Additional Identifier:			
L4567890Z			

1 VACCINATION EVENT

Vaccine or Prophylaxis:	Vaccine Brand:	Disease or agent targeted:
XM0GQ8	**Comirnaty**	**RA01.0**

1.1 VACCINATION DETAILS

Date of Vaccination:	Dose:	Country of Vaccination:
2021-03-03	**1**	**UTO**
Administering Centre:	Vaccine Batch Number:	Due Date of Next Dose:
RIVM	**VC35679**	**2021-03-24**

2 VACCINATION EVENT

Vaccine or Prophylaxis:	Vaccine Brand:	Disease or agent targeted:
XM0GQ8	**Moderna**	**RA01.0**

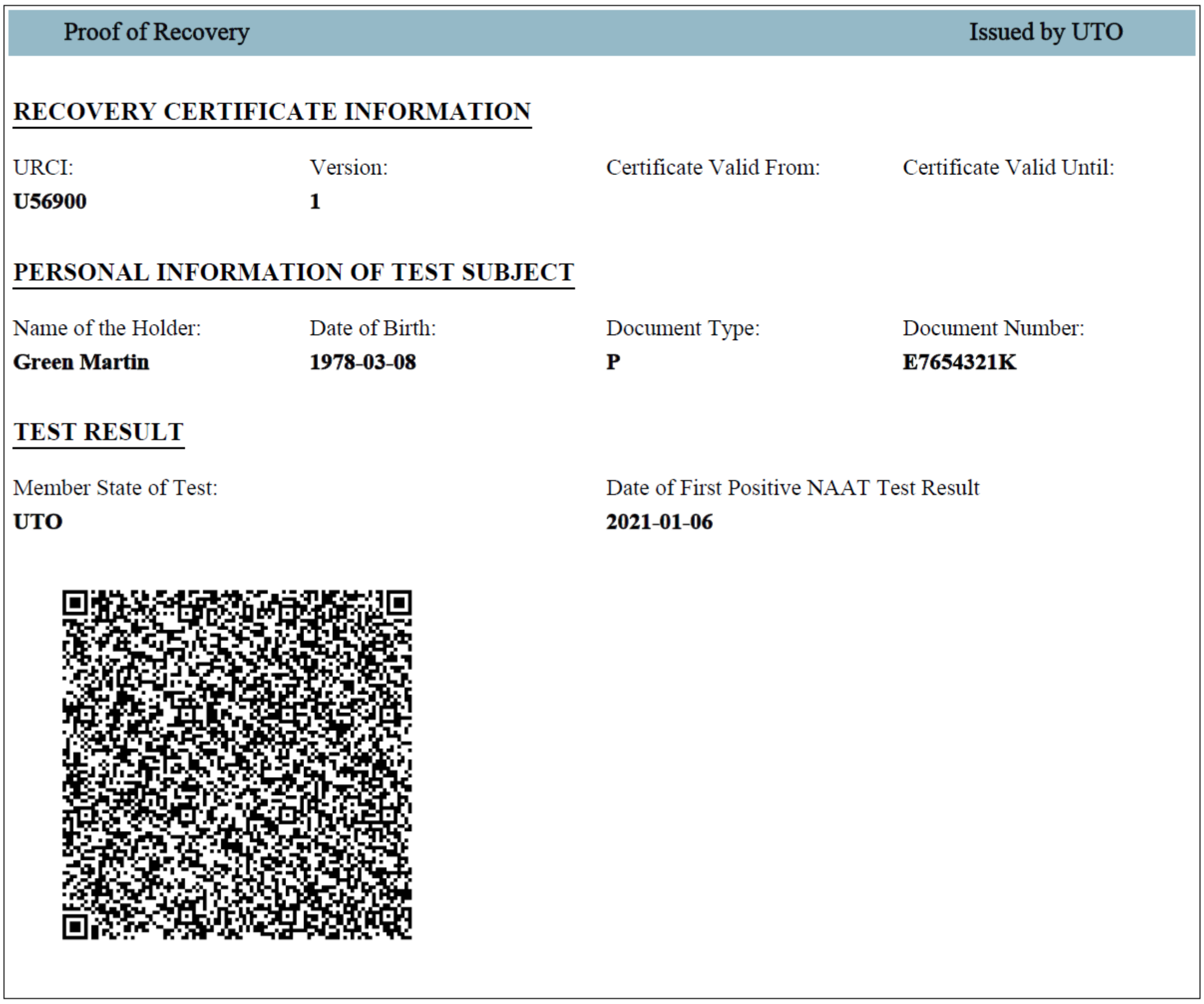
2.1 VACCINATION DETAILS

Date of Vaccination:	Dose:	Country of Vaccination:
2021-03-24	**2**	**SGP**
Administering Centre:	Vaccine Batch Number:	Due Date of Next Dose:
NUH	**VC99537**	

Annex E Worked Example – PoR (Informative)

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

```
{
      "data":{
            "hdr":{
                  "t":"icao.rcvy",
                  "v":1,
                  "is":"UTO"
            },
            "msg":{
                  "urci":"U56900",
                  "pid":{
                        "n":"Green Martin",
                        "dob":"1978-03-08",
                        "dt":"P",
                        "dn":"E7654321K"
                  },
                  "tr":{
                        "sot":"UTO",
                        "dnt":"2021-01-06"
                  }
            }
      },
      "sig":{
            "alg":"ES256",
            "cer":"MIIBfDCCASCgAwIBAgIBbzA...",
            "sigvl":"C97uSfuHz7qH4oqkIBNkA..."
      }
}
```



Proof of Recovery Issued by UTO

RECOVERY CERTIFICATE INFORMATION

URCI:	Version:	Certificate Valid From:	Certificate Valid Until:
U56900	**1**		

PERSONAL INFORMATION OF TEST SUBJECT

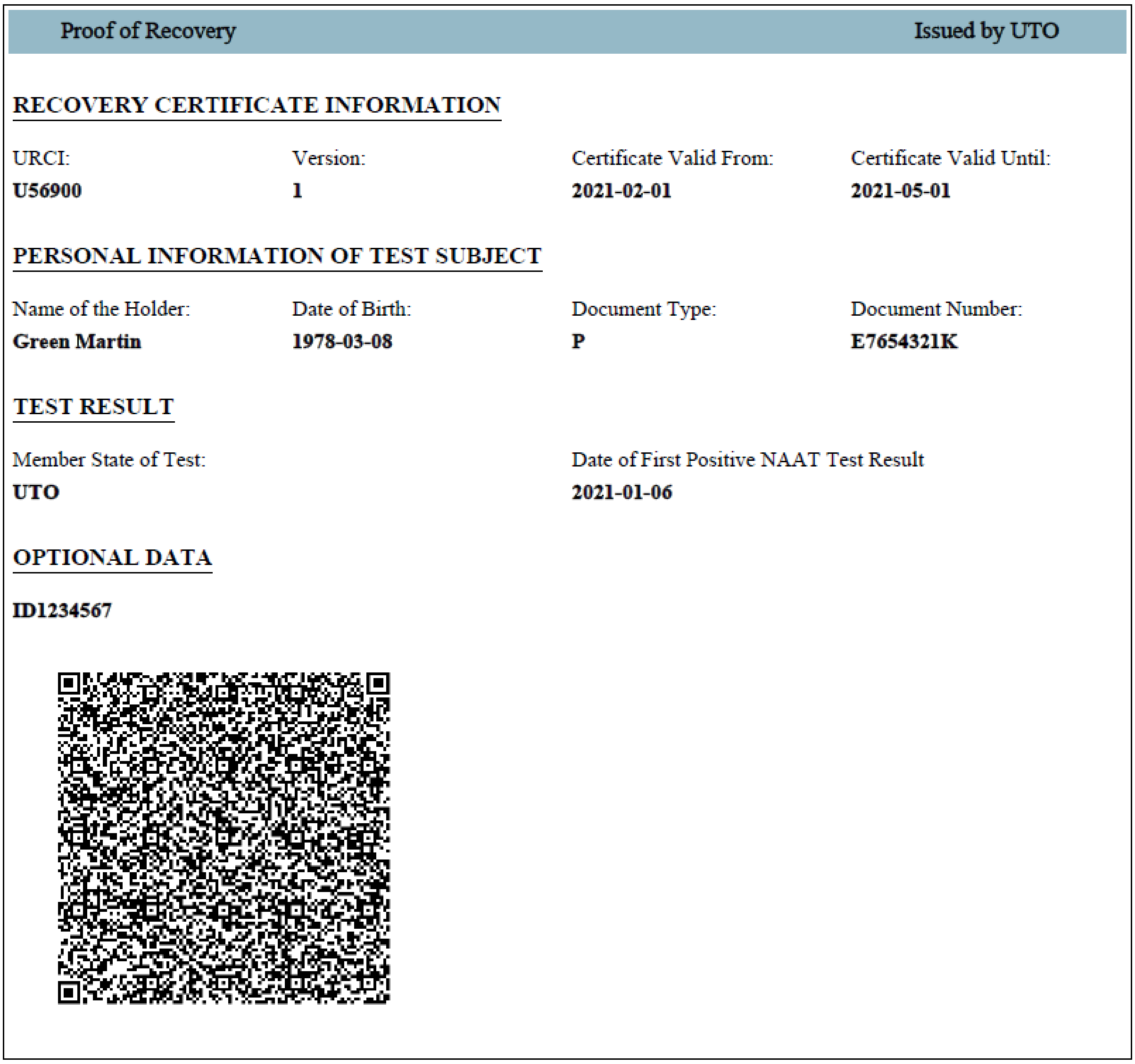
Name of the Holder:	Date of Birth:	Document Type:	Document Number:
Green Martin	**1978-03-08**	**P**	**E7654321K**

TEST RESULT

Member State of Test:	Date of First Positive NAAT Test Result
UTO	**2021-01-06**

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

```
{
      "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",
            "cer":"MIIBfDCCASCgAwIBAgIBbzAMBggqhkjOPQQD...",
            "sigvl":"HBQlHF2bt0snWjSJNIkp4bOaykc46IP8Nc..."
      }
}
```



Proof of Recovery **Issued by UTO**

RECOVERY CERTIFICATE INFORMATION

URCI:	Version:	Certificate Valid From:	Certificate Valid Until:
U56900	**1**	**2021-02-01**	**2021-05-01**

PERSONAL INFORMATION OF TEST SUBJECT

Name of the Holder:	Date of Birth:	Document Type:	Document Number:
Green Martin	**1978-03-08**	**P**	**E7654321K**

TEST RESULT

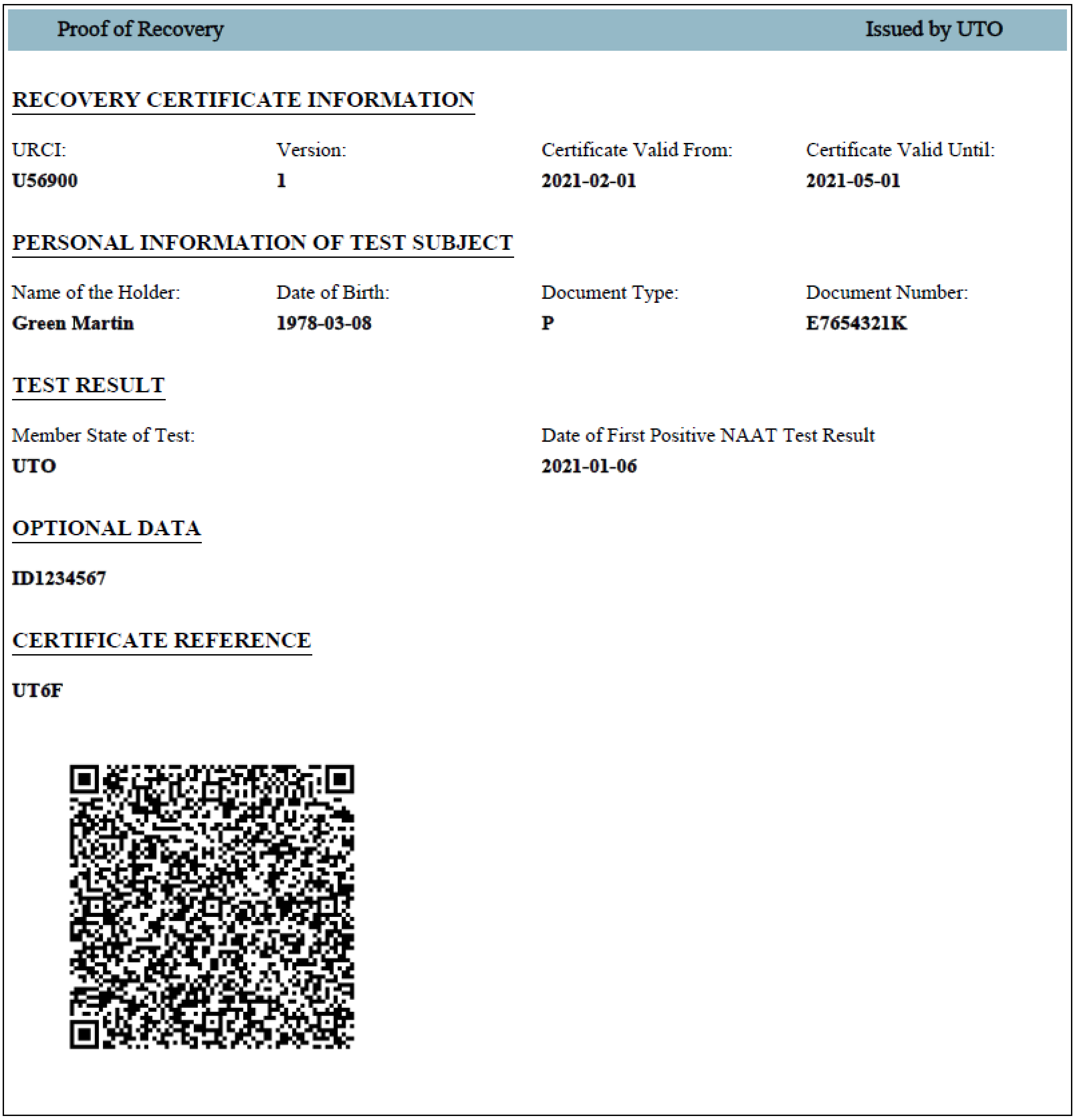
Member State of Test:	Date of First Positive NAAT Test Result
UTO	**2021-01-06**

OPTIONAL DATA

ID1234567

The following is an example of PoR using REQUIRED, RECOMMENDED and OPTIONAL fields with Certificate Reference.

```
{
      "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",
            "sigvl":"0hnZ0ZsjTsY5K39DvVBFxWO73uUHBfY..."
      }
}
```



Proof of Recovery Issued by UTO

RECOVERY CERTIFICATE INFORMATION

URCI:	Version:	Certificate Valid From:	Certificate Valid Until:
U56900	**1**	**2021-02-01**	**2021-05-01**

PERSONAL INFORMATION OF TEST SUBJECT

Name of the Holder:	Date of Birth:	Document Type:	Document Number:
Green Martin	**1978-03-08**	**P**	**E7654321K**

TEST RESULT

Member State of Test:	Date of First Positive NAAT Test Result
UTO	**2021-01-06**

OPTIONAL DATA

ID1234567

CERTIFICATE REFERENCE

UT6F

Annex F 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":2,
            "is":"UTO"
      },
      "msg":{
            "uvci":"U32870",
            "pid":{
                  "n":"Smith Bill",
                  "sex":"M",
                  "i":"A1234567Z"
            },
            "ve":[{
                  "des":"XM0GQ8",
                  "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"
                  }]
            }]
      }
}
```

The same data as a JSON string is as follows :

```
{"hdr":{"t":"icao.vacc","v":2,"is":"UTO"},"msg":{"uvci":"U32870","pid":{"n"
:"Smith
Bill","sex":"M","i":"A1234567Z"},"ve":[{"des":"XM0GQ8","nam":"Comirnaty","m
ah":"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"}]}]}}
```

Output of the JSON Canonicalization [RFC 8785] :

```
{"hdr":{"is":"UTO","t":"icao.vacc","v":2},"msg":{"pid":{"i":"A1234567Z","n"
:"Smith
Bill","sex":"M"},"uvci":"U32870","ve":[{"des":"XM0GQ8","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}]}]}}
```

There are no line breaks in the above text.

Output of the Signature process :

```
"sigvl":"E89teR1TvGmcV0moFJO9SUZ-
xaCUT2wCaV6tW270AGH_JbUe5Nfha1NOENuiY9q8S64ZtlwbXQXszIPLrIt-BA=="
```

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

```
MIIBfTCCASCgAwIBAgIBbDAMBggqhkjOPQQDAgUAMB0xCzAJBgNVBAYTAlVUMQ4wDAYDVQQDDAV
VVCBDQTAeFw0yMDEyMzExNjAwMDBaFw0yOTEyMzExNjAwMDBaMBoxCzAJBgNVBAYTAlVUMQswCQ
YDVQQDEwIwODBZMBMGByqGSM49AgEGCCqGSM49AwEHA0IABI5bRQ3-vabXhHAs2IPi-
k9rP_TS2J8aq5fTtUG1iOwXdBxx2n6c38TJ2MzBWT5PHCKVlq5JOCyJ1nDlCPd1S2yjUjBQMBUG
A1UdJQEB_wQLMAkGB2eBCAEBDgIwHwYDVR0jBBgwFoAUymyksnX8rywn0RH7nDq-
Bs2QOqowFgYHZ4EIAQEGAgQLMAkCAQAxBBMCTlYwDAYIKoZIzj0EAwIFAANJADBGAiEAqw9_Yej
Sj_dU9WOZWrVulY1xhlCOzxO_DiHZLI-PT5wCIQD-mj_W90LN33qZd30ErsLlcTs-
7mFCeYWu44ND84Mmxw==
```

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

```
{"data":{"hdr":{"t":"icao.vacc","v":2,"is":"UTO"},"msg":{"uvci":"U32870","p
id":{"n":"Smith
Bill","sex":"M","i":"A1234567Z"},"ve":[{"des":"XM0GQ8","nam":"Comirnaty","m
ah":"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":"ES
256","cer":"MIIBfTCCASCgAwIBAgIBbDAMBggqhkjOPQQDAgUAMB0xCzAJBgNVBAYTAlVUMQ4
wDAYDVQQDDAVVVCBDQTAeFw0yMDEyMzExNjAwMDBaFw0yOTEyMzExNjAwMDBaMBoxCzAJBgNVBA
YTAlVUMQswCQYDVQQDEwIwODBZMBMGByqGSM49AgEGCCqGSM49AwEHA0IABI5bRQ3-
vabXhHAs2IPi-
k9rP_TS2J8aq5fTtUG1iOwXdBxx2n6c38TJ2MzBWT5PHCKVlq5JOCyJ1nDlCPd1S2yjUjBQMBUG
A1UdJQEB_wQLMAkGB2eBCAEBDgIwHwYDVR0jBBgwFoAUymyksnX8rywn0RH7nDq-
Bs2QOqowFgYHZ4EIAQEGAgQLMAkCAQAxBBMCTlYwDAYIKoZIzj0EAwIFAANJADBGAiEAqw9_Yej
Sj_dU9WOZWrVulY1xhlCOzxO_DiHZLI-PT5wCIQD-mj_W90LN33qZd30ErsLlcTs-
7mFCeYWu44ND84Mmxw==","sigvl":"E89teR1TvGmcV0moFJO9SUZ-
xaCUT2wCaV6tW270AGH_JbUe5Nfha1NOENuiY9q8S64ZtlwbXQXszIPLrIt-BA=="}}
```