MINISTRY OF HEALTH
THE GOVERNMENT
REPUBLIC OF INDONESIA

TECHNICAL SPECIFICATIONS INDONESIA INTERNATIONAL VACCINATION CERTIFICATE

Version

1.5 December 2021

Table of Contents

INTRODUCTION

The Indonesian government services in order to prevent further spread of COVID-19 within the country. Aside from the acceleration of the vaccination program and the imposing of multi-level community restrictions, the government also presented PeduliLindungi: a mobile app designed for contact tracing purposes. Relying on data-sharing of its user's, this mobile app will provide color-coded information regarding the COVID-19 status of the users. Black means infected, red means unvaccinated, yellow means vaccinated for the first dose, and green means completely vaccinated. The colors will also help indicate the crowd because the app will provide information regarding the color that dominates in a particular location.

PeduliLindungi mobile app can also store the user's digital COVID-19 vaccination and COVID-19 test certificates, which gives its users convenience since they don't have to prepare physical documents. Furthermore, the app is also integrated with e-HAC or Electronic Health Alert Card, which will help to provide vital documents for the user and prevent unnecessary physical contact if they are planning to travel.

This document specifies a data structure used for the generation of Digitally verifiable credentials from INDONESIA INTERNATIONAL COVID-19 CERTIFICATE. It also specifies a mechanism in a machine-readable optical format (QR), which can be displayed on the screen of a mobile device or printed on a paper.

1   Terminology

Ministry of Health of Republic of Indonesia who adopted DIVOC's INTERNATIONAL COVID-19 CERTIFICATE specifications for issuing COVID-19 vaccine certificates is called as Issuer and organizations accepting these certificates as proof of vaccination are called Verifiers. Issuer will be responsible for sharing the details on the data elements and the Public key with the verifiers. The QR code contains the data set which is aligned with the WHO-DDCC minimal data set.

2   COVID-19 Vaccination Certificate Format

The vaccination certificate container is designed to provide a standardized template for Issuer. The objective is to create digitally verifiable credentials for interoperability within various parties, allowing users to carry the proof of their vaccination digitally and physically. INDONESIA INTERNATIONAL COVID-19 CERTIFICATE provides individuals with a portable and verifiable digital certificate based on W3C open specification, that users can use online and offline. To read and interpret a INDONESIA INTERNATIONAL COVID-19 CERTIFICATE issued by any verifier need to be in line with the JSON schema that establishes the structure of INDONESIA INTERNATIONAL COVID-19 CERTIFICATE vaccination certificate.

2.1   Structure of the payload

The payload is structure follows the JSON Web Token (JWT) digital signature and is defined in (RFC 7519-*https://tools.ietf.org/html/rfc7519*). The payload, as defined below, is transported in a INDONESIA INTERNATIONAL COVID-19 CERTIFICATE. The integrity and authenticity of origin of payload data MUST be verifiable by the Verifier. The payload is compressed before embedding into QR code. To read and verify the payload, verifier app should first unzip the QR code content using *jszip library* (version above -3.5.0). Please refer Annexure A for the sample payload.

2.2   JWT Claims

2.2.1   JWT Structure Overview

*   Header
*   Payload
*   Signature

2.2.2   Header

The header part contains the information about the certificate is based on W3C verifiable credential data model (*https://www.w3.org/TR/vc-data-model/*). The header part will also indicate the type of certificate.

2.2.3   Payload

The payload part will be divided majorly in three parts. First part contains the details on the issuer of the certificate along with the certificate generation timestamp. Second part contains the details on beneficiary to whom the certificate has been issued. Third part contains the details on the event for which the certificate has been generated. The event part included

details on the Inoculation details along with timestamp including information on type of vaccine, dose details and location of inoculation.

2.2.4 Signature Algorithm

It is important to ensure the authenticity of the certificate. The INDONESIA INTERNATIONAL COVID-19 CERTIFICATE is using the self-generated keys and uses the ES256 signature algorithm (Ed25519Signature2018). *https://w3c-ccg.github.io/lds-ed25519-2018/*

The public key along with the method of signing shall be provided to Verifiers for authentication of the certificate. Basis the algorithm used for generation of certificate, verifier can implement the logic to verify the certificate.

3   QR Code Spec

This section specifies a generic data structure and encoding mechanisms for INDONESIA INTERNATIONAL COVID-19 CERTIFICATE certificates. It provided details on mechanism to generate a machine-readable optical format (QR), which can be displayed on the screen of a mobile device or printed on a piece of paper. This section also covers data structures of QR code. The INDONESIA INTERNATIONAL COVID-19 CERTIFICATE follows the DDCC-WHO minimal data set guidelines. The content is maintained in JSON schema.

3.1   Data Structure and Format in JSON Schema

This section provides specific details related to the individual data fields. The authoritative default official JSON schema for DIVOC is located at
https://github.com/egovernments/DIVOC/blob/main/vaccination-context/vaccination-context.js
The upcoming version is to be supported by a defined date by all countries: tagged versions, described more specifically in the Readme file. The schema specific to Indonesia implementation is mentioned Annexure A.

The common structure is outlined below. Detailed information on individual groups and fields is provided in next sections.

```
{
  "@context":[  ],
  "type":[
  ],
```

5

```
"credentialSubject":{
},
"issuer":"",
"issuanceDate":"",
"evidence":[
  {
],
"nonTransferable":"",
"proof":{
}
}
```

The default details of the json schema embedded in QR code is as follows:

#	Field Name	Description
1	context	It provides the details on which data model the certificate is based. Currently it is based on w3c data model
2	type	It provides details on type of certificate. Value is in the form of json array
3	credentialSubject	The section provides the beneficiary details It is of type Object
3.1	Type	This indicates that the certificate has been given to individual or a group. For ex - Person
3.2	Id	This value indicates the event id. It must be unique for each event. Minimum value of length 1 of type alphanumeric.
3.3	refId	This value indicates the beneficiary reference identifier. It should be unique for each beneficiary. Minimum value of length 1 of type alphanumeric.
3.4	name	This value indicates the name of Beneficiary. Minimum value of length 1 of type string.
3.5	gender	This value indicates the gender of Beneficiary. Minimum value of length 1 of type string. For ex : "gender"" : "female"
3.6	Age	This value indicates the age of Beneficiary. Minimum value of length 1 of type string.
3.7	Dob	This value indicates the Date of Birth of Beneficiary. It follows the format of YYYY-MM-DD For ex: "dob" : "1988-04-04"
3.8	nationality	This value indicates the nationality of Beneficiary. Minimum value of length 1 of type string. For ex: "nationality" : "Indonesia"
3.9	address	The section provides the address details of beneficiary It is of type Object
3.9.1	streetAddress	This value indicates the Address of Beneficiary. Minimum value of length 1 of type string
3.9.2	streetAddress2	This value indicates the Address of Beneficiary.
3.9.3	city	This value indicates the City of Beneficiary.
3.9.4	district	This value indicates the District of Beneficiary.

#	Field Name	Description
		Minimum value of length 1 of type string
3.9.5	addressRegion	This value indicates the region of Beneficiary. Minimum value of length 1 of type string
3.9.6	addressCountry	This value indicates the country of Beneficiary. Minimum value of length 2 of type string
3.9.7	postalCode	This value indicates the area code of Beneficiary.
4	issuer	This value indicates the Issuing Authority . Minimum value of length 1 of type string ex : "https://www.pedulilindungi.id/"
5	issuanceDate	This value indicates the Certificate Issuing Date . Minimum value of length 1 of type Date and Time For ex : "2021-06-28T07:21:39.684Z"
6	evidence	The section provides the evidence details of Vaccination event Value is in the form of json array
6.1	icd11Code	This value indicates the ICD11 code of Vaccine Type Value is of type String
6.2	feedbackUrl	This value indicates the feedback Url, if beneficiary is interested to provide feedback of vaccination Value is of type String
6.3	prophylaxis	This value indicates the Vaccine Type Value is of type String
6.4	certificateId	This value indicates the Certificate Id The value is unique for each certificate. If the certificate get updated, new certificate Id will be issued and previous certificate Id will be revoked. Value is of type String
6.5	type	This value indicates the type of event Value is of type String
6.6	batch	This value indicates the batch details of Vaccine Minimum value of length 1 of type string Value is of type String
6.7	vaccine	This value indicates the vaccine details of Vaccine Minimum value of length 1 of type string Value is of type String
6.8	manufacturer	This value indicates the vaccine manufacturer details of Vaccine Minimum value of length 1 of type string Value is of type String
6.9	date	This value indicates the Date of event Value is of type Date It follows the format of YYYY-MM-DD For ex: *"date" : " 2021-11-30T18:26:41.459Z"*
6.10	effectiveStart	This value indicates the effective start date from which the certificate will be considered valid. Value is of type Date It follows the format of YYYY-MM-DD For ex: *"date" : " 2021-11-30T18:26:41.459Z"*
6.11	effectiveUntil	This value indicates the effective end date for the validity of certificate. Value is of type Date It follows the format of YYYY-MM-DD

#	Field Name	Description
		For ex: *"date" : " 2100-11-30T18:26:41.459Z"*
6.12	dose	This value indicates the vaccine dose number taken in this event Minimum value of length 1 of type string. For ex: "dose" : "1" if first dose is taken of vaccine "dose" : "2" if two doses are taken of vaccine
6.13	totalDoses	This value indicates the total number of vaccines required to consider beneficiary fully vaccinated. Minimum value of length 1 of type string For ex: "totalDoses" : "1" for 1 dose vaccine like Sinovac "totalDoses" : "2" for 2 dose vaccine like Sinovac
6.14	verifier	The section provides the verifier of the vaccination event It is of type Object
6.14.1	name	This value indicates the name of verifier Value is of type String
6.15	facility	This value indicates the location details of event It is of type Object
6.15.1	name	This value indicates the name of location Value is of type String
6.15.2	address	The section provides the address details of the vaccination event It is of type Object
6.15.2.1	streetAddress	This value indicates the Address line one of vaccination event. Minimum value of length 1 of type string
6.15.2.2	streetAddress2	This value indicates the Address Line of vaccination event.
6.15.2.3	city	This value indicates the City of Vaccination event.
6.15.2.4	district	This value indicates the District of Vaccination event. Minimum value of length 1 of type string
6.15.2.5	addressRegion	This value indicates the region of Vaccination event. Minimum value of length 1 of type string
6.15.2.6	addressCountry	This value indicates the country of Vaccination event. Minimum value of length 2 of type string
6.15.2.7	postalCode	This value indicates the area code of Vaccination event.
7	nonTransferable	This value indicates that the certificate is nontransferable The value should ne always "true"
8	proof	The section indicates proof section of certificate to check the authenticity of the certificate
8.1	type	This value indicates the algorithm used for signing of the certificate
8.2	created	This value indicates the date and time of signing of the certificate
8.3	verificationMethod	This value indicates the method and public key used for verification of the certificate. The value changes for each implementation. For ex: "verificationMethod":"did:indonesia", will indicate that Indonesia's public key and method to be used for verification
8.4	proofPurpose	This value indicates the method used for every Linked Data Proof For ex: "proofPurpose":"assertionMethod"
8.5	jws	This value indicates the JSON Web Signature (JWS) used to represents content secured with digital signatures

Appendix A - Sample Template of The International Certificate of Vaccination Issued by The Ministry of Health Republic of Indonesia (DIVOC Format)
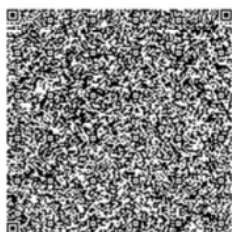
REPUBLIC OF INDONESIA
REPUBLIK INDONESIA

KEMENTERIAN KESEHATAN REPUBLIK INDONESIA

INTERNATIONAL COVID-19 VACCINATION CERTIFICATE

SERTIFIKAT VAKSINASI COVID-19 INTERNASIONAL

Number / Nomor : 633631264

DETAILS / RINCIAN

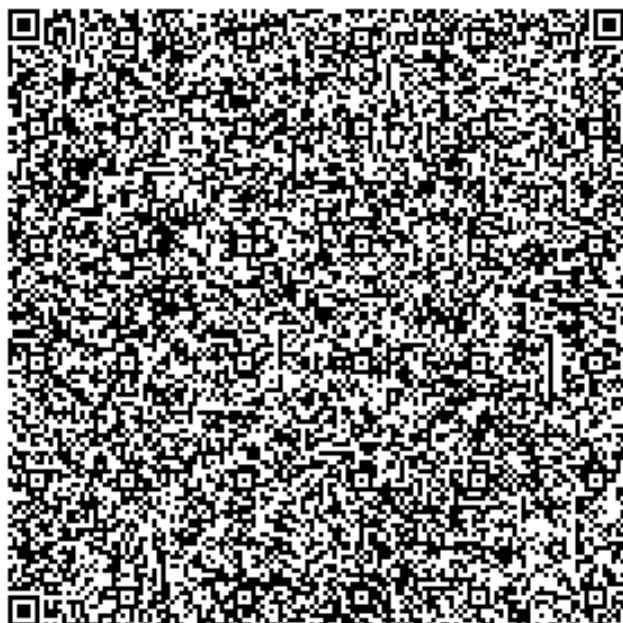|	
Full Name Nama Lengkap	*Ivan*
National Identity Number NIK	123456789ABCD
Passport Number No. Passport	
Date of Birth Tanggal Lahir	2000-05-24

For further details, please visit
https://verify.kemkes.go.id

VACCINATION DETAILS / RINCIAN VAKSINASI

Date of vaccination Tanggal Vaksinasi	Dose Number Dosis ke	Country of Vaccination Negara /Tempat Vaksinasi	Vaccine Manufacturer Jenis Vaksin	Batch ID Batch ID
28-May-2021	*First* / Pertama	Indonesia	sinovac	A0024
28-Jun-2021	*Second* / Kedua	Indonesia	sinovac	A1024

Vaccination is to protect ourselves and our families, neighbors and protect Indonesian people and people worldwide.
Vaksinasi melindungi diri kita, keluarga kita, tetangga dan melindungi rakyat Indonesia dan manusia di seluruh dunia.

World Health Organization Digital Documentation for COVID-19 Certificates Format

Appendix B - Sample Template of The International Certificate of Vaccination Issued by The Ministry of Health Republic of Indonesia (EU Format)

REPUBLIC OF INDONESIA
REPUBLIK INDONESIA

KEMENTERIAN KESEHATAN REPUBLIK INDONESIA

INTERNATIONAL COVID-19 VACCINATION CERTIFICATE

SERTIFIKAT VAKSINASI COVID-19 INTERNASIONAL

Number / Nomor : 788928303

For further details, please visit
https://verify.kemkes.go.id

DETAILS / RINCIAN

Full Name / Nama Lengkap	**Daniel Oscar Baskoro**
National Identity Number / NIK	3404071007920002
Passport Number / No. Passport	
Date of Birth / Tanggal Lahir	1992-07-10

VACCINATION DETAILS / RINCIAN VAKSINASI

Date of vaccination / Tanggal Vaksinasi	Dose Number / Dosis ke	Country of Vaccination / Negara /Tempat Vaksinasi	Vaccine Manufacture / Jenis Vaksin	Batch ID / Batch ID
23-Feb-2021	*First* / Pertama	Indonesia	CoronaVac	24000121
09-Mar-2021	*Second* / Kedua	Indonesia	CoronaVac	24000421

Vaccination is to protect ourselves and our families, neighbors and protect Indonesian people and people worldwide.
Vaksinasi melindungi diri kita, keluarga kita, tetangga dan melindungi rakyat Indonesia dan manusia di seluruh dunia.

World Health Organization Digital Documentation for COVID-19 Certificates Format

EU Payload

```
{
  "6":1638869336,
  "4":1670405336,
  "1":"ID",
  "-260":{
    "1":{
      "ver":"1.0.0",
      "nam":{
        "fn":"",
        "gn":"Daniel Oscar Baskoro"
      },
```

```
        "dob":"1992-07-10",
        "v":[
          {
                                                                            11
            "tg":"840539006",
            "vp":"",
            "mp":"CoronaVac",
            "ma":"",
            "dn":2,
            "sd":2,
            "dt":"2021-03-09",
            "co":"ID",
            "is":"Ministry of health Indonesia",
            "ci":"URN:UVCI:01:ID:788928303"
          }
        ]
      }
    }
}
```
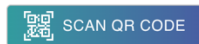
EU QR Example

Appendix C – Verification Mechanism Using Verify.Kemkes.Go.Id

12

Verify a vaccination certificate

The PeduliLindungi vaccination certificate has a digitally signed secure QR code. This can be authenticated online using the verification utility in this portal or using third party verification app using the services outlined below.

Option 1 – Online verification

Steps for online verification:

1. Visit verify.kemkes.go.id/
2. Click on "Scan QR" code.
3. A notification will prompt to activate your device's camera.
4. Point the camera to the QR code on the bottom right of the certificate issued and scan.
5. Please keep the following points in mind while scanning the QR code.
   - QR code should cover at-least 70%-80% of screen.
   - Complete QR code should be part of camera frame.
   - QR code should be parallel to the camera.

Appendix D – Sample JSON (DIVOC)

```
{
  "@context": ["https://www.w3.org/2018/credentials/v1",
"https://www.pedulilindungi.id/credentials/vaccination/v2"],
  "type": ["VerifiableCredential", "ProofOfVaccinationCredential"],
  "credentialSubject": {
   "type": "Person",
   "id": "123456789ABCD",
   "refId": "Test-01",
   "name": "Ivan",
   "gender": "Male",
   "age": "21",
   "nationality": "Indonesian",
   "address": {
    "streetAddress": "JL. SEMEN ROMO",
    "streetAddress2": "",
    "district": "-",
    "city": "",
    "addressRegion": "-",
    "addressCountry": "-",
    "postalCode": "-"
   },
   "dob": "2000-05-24"
  },
  "issuer": "https://www.pedulilindungi.id/",
  "issuanceDate": "2021-12-14T07:49:55.987Z",
  "evidence": [{
   "certificateId": "482823823",
   "type": ["Vaccination"],
   "batch": "A1024",
   "vaccine": "sinovac",
   "manufacturer": "Jenis vaksin",
   "date": "2021-06-28T07:21:39.684Z",
   "effectiveStart": "2021-06-28",
   "effectiveUntil": "2022-06-28",
   "dose": 2,
   "totalDoses": 2,
   "verifier": {
    "name": "vaccinator"
   },
   "facility": {
    "name": "RSUD NGUDI WALUYO",
    "address": {
```

```
        "streetAddress": "Jl. Dokter Sucipto",
        "streetAddress2": "",
        "district": "-",
        "city": "",
        "addressRegion": "-",
        "addressCountry": "IDN",
        "postalCode": "-"
      }
    },
    "feedbackUrl": "https://www.pedulilindungi.id/?482823823",
    "icd11Code": "XM1NL1",
    "prophylaxis": "COVID-19 vaccine, inactivated virus"
  }],
  "nonTransferable": "true",
  "proof": {
    "type": "Ed25519Signature2018",
    "created": "2021-12-14T07:49:55Z",
    "verificationMethod": "did:indonesia",
    "proofPurpose": "assertionMethod",
    "jws":
"eyJhbGciOiJFZERTQSIsImI2NCI6ZmFsc2UsImNyaXQiOlsiYjY0Il19..BtcoPMkzrBv6Tr6ZCenqS
q-nSlQ7bkJmY3oP7Px-eUqgeK_cDEWADVGTj6A8rZZER0S_98f2m8pj1UKE9M4yAw"
  }
}
```

Certificate Public Key (DIVOC):

```
---- BEGIN SSH2 PUBLIC KEY ----
Comment: "eddsa-key-20211210-indonesia"
3sY2pM3VbuN15rZ48hVsC27HmXBRnEAfaRxkhuCjFcxd
L/FF
---- END SSH2 PUBLIC KEY ----
```

HTTP Method: GET

References

https://www.who.int/publications/m/item/interim-guidance-for-developing-a-smart-vaccination-certificate

-

15