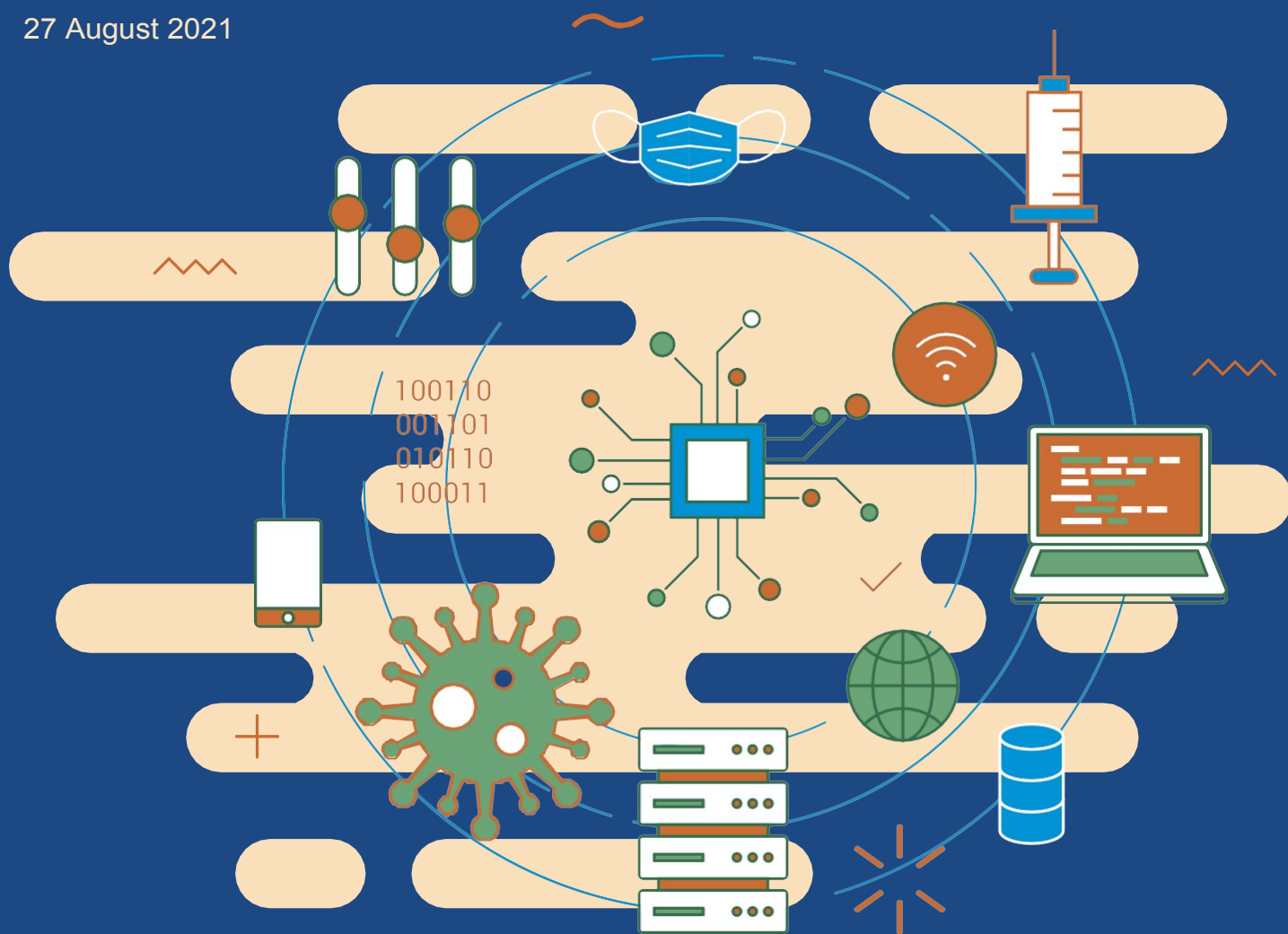


Digital Documentation of COVID-19 Certificates: Vaccination Status

TECHNICAL SPECIFICATIONS AND IMPLEMENTATION GUIDANCE

27 August 2021



Digital Documentation of COVID-19 Certificates: **Vaccination Status**

TECHNICAL SPECIFICATIONS AND IMPLEMENTATION GUIDANCE

Digital Documentation of COVID-19 Certificates: Vaccination Status — Technical Specifications and Implementation Guidance, 27 August 2021.

WHO/2019-nCoV/Digital_certificates/vaccination/2021.1

© World Health Organization 2021

Some rights reserved. This work is available under the Creative Commons Attribution-NonCommercial-ShareAlike

3.0 IGO licence (CC BY-NC-SA 3.0 IGO; <https://creativecommons.org/licenses/by-nc-sa/3.0/igo>).

Under the terms of this licence, you may copy, redistribute and adapt the work for non-commercial purposes, provided the work is appropriately cited, as indicated below. In any use of this work, there should be no suggestion that WHO endorses any specific organization, products or services. The use of the WHO logo is not permitted. If you adapt the work, then you must license your work under the same or equivalent Creative Commons licence. If you create a translation of this work, you should add the following disclaimer along with the suggested citation: “This translation was not created by the World Health Organization (WHO). WHO is not responsible for the content or accuracy of this translation. The original English edition shall be the binding and authentic edition”.

Any mediation relating to disputes arising under the licence shall be conducted in accordance with the mediation rules of the World Intellectual Property Organization (<http://www.wipo.int/amc/en/mediation/rules/>).

Suggested citation. Digital Documentation of COVID-19 Certificates: Vaccination Status — Technical Specifications and Implementation Guidance, 27 August 2021. Geneva: World Health Organization; 2021 (WHO/2019-nCoV/Digital_certificates/vaccination/2021.1). Licence [CC BY-NC-SA 3.0 IGO](https://creativecommons.org/licenses/by-nc-sa/3.0/igo).

Cataloguing-in-Publication (CIP) data. CIP data are available at <http://apps.who.int/iris>.

Sales, rights and licensing. To purchase WHO publications, see <http://apps.who.int/bookorders>. To submit requests for commercial use and queries on rights and licensing, see <http://www.who.int/about/licensing>.

Third-party materials. If you wish to reuse material from this work that is attributed to a third party, such as tables, figures or images, it is your responsibility to determine whether permission is needed for that reuse and to obtain permission from the copyright holder. The risk of claims resulting from infringement of any third-party-owned component in the work rests solely with the user.

General disclaimers. The designations employed and the presentation of the material in this publication do not imply the expression of any opinion whatsoever on the part of WHO concerning the legal status of any country, territory, city or area, or of its authorities, or concerning the delimitation of its frontiers or boundaries. Dotted and dashed lines on maps represent approximate border lines, for which there may not yet be full agreement.

The mention of specific companies or of certain manufacturers' products does not imply that they are endorsed or recommended by WHO in preference to others of a similar nature that are not mentioned. Errors and omissions excepted; the names of proprietary products are distinguished by initial capital letters.

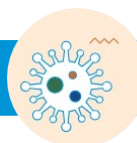
All reasonable precautions have been taken by WHO to verify the information contained in this publication. However, the published material is being distributed without warranty of any kind, either expressed or implied. The responsibility for the interpretation and use of the material lies with the reader. In no event shall WHO be liable for damages arising from its use.

Editing: Green Ink Publishing Services Ltd.

Design and layout: RRD Design LLC

Contents

Acknowledgements	v
Abbreviations	vii
Glossary	viii

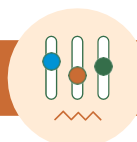


Executive Summary xi



SECTION 1 Introduction 1

1.1. Purpose of this document	1
1.2. Target audience	2
1.3. Scope	2
1.4. Assumptions	3
1.5. Methods	5
1.6. Additional WHO guidance documents	5
1.7. Other initiatives	5



SECTION 2 Ethical considerations and data protection principles 6

2.1. Ethical considerations for a DDCC:VS	6
2.2. Data protection principles for a DDCC:VS	12
2.3. DDCC:VS design criteria	15








SECTION 3 Continuity of Care scenario 16

3.1. Key settings, personas and digital services	16
3.2. Continuity of Care workflows and use cases	18
3.3. Functional requirements for Continuity of Care scenario	24



SECTION 4 Proof of Vaccination scenario 27

4.1. Key settings, personas and digital services	27
4.2. Proof of Vaccination workflows and use cases	29
4.3. Functional requirements for Proof of Vaccination scenario	37

	SECTION 5 DDCC:VS core data set	40
	5.1. Core data set principles	40
	5.2. Core data elements	42
	SECTION 6 National Trust Architecture	46
	6.1. Signing a DDCC:VS	48
	6.2. Verifying a DDCC:VS signature	49
	6.3. Trusting a DDCC:VS signature	50
	SECTION 7 National governance considerations	51
	SECTION 8 Implementation considerations	53
	8.1. Considerations before deploying	54
	8.2. Key factors to consider with solution developers	56
	8.3. Cost category considerations	57
	8.4. Additional resources to support implementation	59
	References	60
	Annexes	62
	Annex 1 Illustrative example of Digital Documentation of COVID-19 Certificates: Vaccination Status (DDCC:VS)	63
	Annex 2 Business process symbols used in workflows	64
	Annex 3 Guiding principles for mapping the WHO Family of International Classifications (WHO-FIC) and other classifications	65
	Annex 4 What is public key infrastructure (PKI)?	68
	Annex 5 Non-functional requirements	72
	Annex 6 Open Health Information Exchange (OpenHIE)-based architectural blueprint	77
	Web Annex A DDCC:VS Core data dictionary https://apps.who.int/iris/bitstream/handle/10665/343264/WHO-2019-nCoV-Digital-certificates-vaccination-data-dictionary-2021.1-eng.xlsx	
	Web Annex B Technical Briefing https://apps.who.int/iris/bitstream/handle/10665/344456/WHO-2019-nCoV-Digital_certificates-vaccination-technical_briefing-2021.1-eng.pdf	

Acknowledgements

The World Health Organization (WHO) is grateful for the contribution that many individuals and organizations have made to the development of this document.

This document was coordinated by Garrett Mehl, Natschja Ratanaprayul, Derek Ritz, Philippe Veltsos, and Bernardo Mariano Junior of the WHO Department of Digital Health and Innovations, in collaboration with individuals in departments across WHO and other organizations, who include: Marta Gacic-Dobo and Jan Grevendonk of the WHO Department of Immunization, Vaccines and Biologicals; Carmen Dolea and Thomas Hofmann of the International Health Regulations Secretariat; Sara Barragan Montes and Ninglan Wang of the WHO Department of Country Readiness Strengthening; Andreas Reis and Katherine Littler of the WHO Department of Health Ethics and Governance; Ayman Badr and Kevin Crampton of the WHO Department of Information Management and Technology; Thomas Grein and Abdi Rahman Mahamud of Strategic Health Operations WHO Emergency Response; Wouter 'T Hoen of the WHO Department of Human Resources and Talent Management; Carl Leitner, Jenny Thompson and Luke Duncan from PATH; Voo Teck Chuan from National University of Singapore; and Robert Jakob and Nenad Kostanjsek of the WHO Department of Data and Analytics.

The following individuals (listed in alphabetical order) reviewed, provided feedback and contributed to this document at various stages: Aasim Ahmad (Aga Khan University), Onyema Ajuebor (WHO), Shada Alsalamah (WHO), Thalia Arawi (American University), Joaquin Andres Blaya (World Bank), Emily Carnahan (PATH), Ciaran Carolan (International Civil Aviation Organization (ICAO), Gabriel Catan (World Bank), Jim Case (SNOMED International), Vladimir Choi (WHO), Adam Cooper (World Bank consultant), Angus Dawson (University of Sydney), Christiane Demarkar (ICAO), Vyjayanti T Desai (World Bank), Edward Simon Dunstone (World Bank consultant), Marie Eichholtzer (World Bank), Ezekiel J Emanuel (University of Pennsylvania), Ioana-Maria Gligor (European Commission Directorate-General for Health and Food Safety), Marelize Gorgens (World Bank), Clayton Hamilton (WHO), Monica Harry (SNOMED International), Christopher Hornek (ICAO), Matthew Thomas Hulse (World Bank), Konstantin Hyppönen (European Commission Directorate-General for Health and Food Safety), Sharon Kaur (University of Malaya), Alastair Kenworthy (New Zealand Ministry of Health – Manatū Hauora), Tarek Khorshed (WHO), Edmund Kienast (Australian Digital Health Agency), Mark Landry (WHO), Christos Maramis (European Commission Directorate-General for Communications Networks, Content and Technology), Marco Marsella (European Commission Directorate-General for Communications Networks, Content and Technology), Jonathan Marskell (World Bank), Ignacio Mastroleo (Facultad Latinoamericana de Ciencias Sociales), Rajeesh Menon (Ernst & Young), Jane Millar (SNOMED International), Anita Mittal (World Bank consultant), Toni Morrison (SNOMED International), Richard Morton (International Port Community Systems Association), James L Neumann (World Bank), Beth Newcombe (Immigration, Refugees and Citizenship Canada), Mohamed Nour (WHO), Vanja Pajic (WHO), Roberta Pastore (WHO), Maria Paz Canales (Derechos Digitales), Alexandrine Pirlot de Corbion (Privacy International), R Rajeshkumar (Auctorizium Pte Ltd), Eric Ramirez (El Salvador Secretaría de Innovación de la Presidencia), Suzy Roy (SNOMED International), Carla Saenz (WHO Regional Office for the Americas), David Satola (World Bank), Ester Sikare (United States Centers for Disease Control and Prevention), Maxwell J Smith (University of Toronto), Vincent van Pelt (Nictiz), Pramod Varma (EkStep Foundation), Gillan Ward (World Bank consultant), Stefanie Weber (Federal Institute for Drugs and Medical Devices, Germany), and Stephen Wilson (Lockstep Group).

The WHO extends sincere thanks to the following individuals (listed in alphabetical order), who contributed to the technical consultation process: Roberta Andraghetti (WHO), Housseynou Ba (WHO), Madhava Balakrishnan (WHO), Andre Arsene Bitu Fouda (WHO), Stuart Campo (United Nations Office for the Coordination of Humanitarian Affairs, Centre for Humanitarian Data), Marcela Contreas (WHO), Jun Gao (WHO), Fernando Gonzalez-Martin (WHO), Christopher Haskew (WHO), Jennifer Horton (WHO), Beverly Knight (ISO TC215 Health Informatics Canadian Mirror Committee), Kathleen Krupinski (WHO), Ephrem Lemango (WHO), Ann Linstrand (WHO), Jason Mwenda Mathiu (WHO), Ngum Meh Zang (WHO),

(Center for Implementation and Innovation in Health Policies), Buenos Aires, Argentina), Elizabeth Peloso (Liz Peloso Consulting Inc.), Alain Poy (WHO), Magdalena Rabini (WHO), Maria Soc (PATH), Soumya Swaminathan (WHO), Martha Velandia (WHO), Petra Wilson (Health Connect Partners), and all members and observers of the Smart Vaccination Certificate Working Group.

This work was funded by the Bill and Melinda Gates Foundation, the Government of Estonia, Fondation Botnar, the State of Kuwait, and the Rockefeller Foundation. The views of the funding bodies have not influenced the content of this document.

Abbreviations

1D	one-dimensional
2D	two-dimensional
AEFI	adverse event(s) following immunization
API	application programming interface
COVID-19	coronavirus disease 2019
DDCC	Digital Documentation of COVID-19 Certificates
DDCC:VS	Digital Documentation of COVID-19 Certificates: Vaccination Status
DSC	document signer certificate
EIR	electronic immunization registry
FHIR	Fast Healthcare Interoperability Resources
HCID	health certificate identifier
HL7	Health Level Seven
HPV	human papillomavirus
ICD	International Classification of Diseases
ICT	information and communications technology
ID	identifier
IHR	International Health Regulations (2005)
IPS	International Patient Summary
ISO	International Organization for Standardization
OPENHIE	Open Health Information Exchange
PHA	public health authority
PHSMS	public health and social measures
PKI	public key infrastructure
QA	quality assurance
SHR	shared health record
SLA	service level agreement
SNOMED CT GPS	Systematized Nomenclature of Medicine Clinical Terms Global Patient Set
WHO-FIC	WHO Family of International Classifications

Glossary

CERTIFICATE: A document attesting a fact. In the context of the vaccination certificate, it attests to the fact that a vaccine has been administered to an individual.

CERTIFICATE AUTHORITY (CA): Also known as a “certification authority” in the context of a public key infrastructure, is an entity or organization that issues digital certificates.

COVAX: The vaccines pillar of the Access to COVID-19 Tools (ACT) Accelerator. It aims to accelerate the development and manufacture of COVID-19 vaccines, and to guarantee fair and equitable access for every country in the world.

DATA CONTROLLER: The person or entity that, alone or jointly with others, determines the purposes and means of the processing of personal data. A data controller has primary responsibility for the protection of personal data.

DATA PROCESSING: “Processing” means any operation or set of operations performed on personal data or on sets of personal data, whether by automated means or not, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

DATA PROCESSOR: A person or entity that processes personal data on behalf of, or under instruction from, the data controller.

DATA SUBJECT: The Subject of Care or the DDCC:VS Holder if the DDCC:VS Holder represents the Subject of Care, such as a minor, or represents a person who is physically or legally incapable of giving consent for the processing of their personal data.

DDCC:VS GENERATION SERVICE: The service that is responsible for generating a digitally signed representation, the DDCC, of the information concerning a COVID-19 vaccination.

DDCC:VS REGISTRY SERVICE: The service that can be used to request and receive the digitally signed COVID-19 vaccination information.

DDCC:VS REPOSITORY SERVICE: A potentially federated service that has a repository, or database, of DDCC:VS.

DIGITAL DIVIDE: The gap between demographic groups and regions that have access to modern ICT and those that do not, or that have restricted access.

DIGITAL DOCUMENTATION OF COVID-19 CERTIFICATE(S) (DDCC): A digitally signed FHIR document that represents the core data set for the relevant COVID-19 certificate using the JavaScript Object Notation (JSON) representation.

DIGITAL DOCUMENTATION OF COVID-19 CERTIFICATE(S): VACCINATION STATUS (DDCC:VS): A type of DDCC

that is used to represent the COVID-19 vaccination status of an individual. Specifically, the DDCC:VS is a digitally signed Health Level Seven (HL7) Fast Healthcare Interoperability Resources (FHIR) document containing the data elements included in the DDCC:VS core data set.

DIGITAL REPRESENTATION: A virtual representation of a physical object or system. In this context, the digital representation must be a digitally signed FHIR document or a digitally signed two-dimensional (2D) barcode (e.g. a QR code).

DIGITAL SIGNATURE: In the context of this guidance document, it is a hash generated from the HL7 FHIR data concerning a vaccination signed with a private key.

DIGITALLY SIGNED: A digital document is digitally signed when plain-text health content is “hashed” with an algorithm, and that hash is encrypted, or “signed”, with a private key.

ENCRYPTION: A security procedure that translates electronic data in plain text into a cipher code, by means of either a code or a cryptographic system, to render it incomprehensible without the aid of the original code or cryptographic system.

HEALTH CERTIFICATE IDENTIFIER (HCID): A unique alphanumeric identifier (ID) for a physical and/or digital health document which contains one or more vaccination events. It is the key identifier, present within the DDCC:VS and retained in the DDCC:VS registry.

HEALTH DATA: Personal data related to the physical or mental health of a natural person, including the provision of health services, which reveal information about his or her health status. These include personal data derived from the testing or examination of a body part or bodily substance, including from genetic data and biological samples.

IDENTIFICATION DOCUMENT: A document that attests the identity of or a linkage to someone, for example, a passport or a national identity card.

IDENTIFIER: A name that labels the identity of an object or individual. Usually, it is a unique alphanumeric string that is associated with an individual, for example, a passport number or medical record ID.

ONE-DIMENSIONAL (1D) BARCODE: A visual black and white pattern using variable-width lines and spaces for encoding information in a machine-readable form. It is also known as a linear code.

MAY: MAY is used to describe technical features and functions that are optional, and it is the implementer’s decision whether to include that feature or function based on the implementation context.¹

PASS: A document that gives an individual the authorization to have access to something, such as public spaces, events and modes of transport.

¹ This definition is based on the definition published by the Internet Engineering Task Force (IETF) (<https://www.ietf.org/rfc/rfc2119.txt>, accessed 30 June 2021).

PERSONAL DATA: Any information relating to an individual who is or can be identified, directly or indirectly, from that information. Personal data include: biographical data (biodata), such as name, sex, civil status, date and place of birth, country of origin, country of residence, individual registration number, occupation, religion and ethnicity; biometric data, such as a photograph, fingerprint, facial or iris image; health data; as well as any expression of opinion about the individual, such as assessments of his or her health status and/or specific needs.

PUBLIC KEY: The part of a private–public key pair used for digital encryption that is designed to be freely distributed.

PUBLIC KEY INFRASTRUCTURE (PKI): The policies, roles, software and hardware components and their governance that facilitate digital signing of documents and issuance/distribution/exchange of keys.

PRIVATE KEY: The part of a private–public key pair used for digital encryption that is kept secret and held by the individual/organization signing a digital document.

SHALL: SHALL is used to describe technical features and functions that are mandatory for this specification.¹

SHOULD: SHOULD is used to describe technical features and functions that are recommended, but are not mandatory. It is the implementer's decision whether to include that feature or function based on the implementation context. However, it is highly recommended that the implementer review the reasons for not following the recommendations before deviating from the technical specifications outlined²

SUBJECT OF CARE: The vaccinated person.

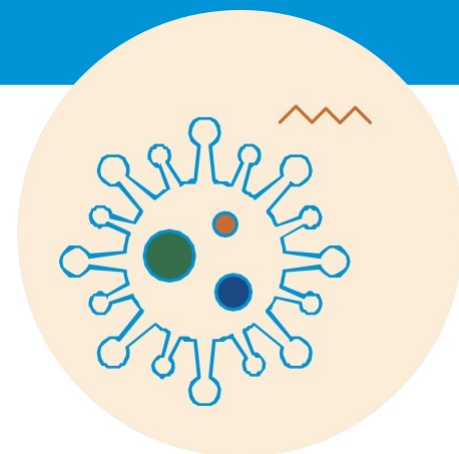
THIRD PARTY USE: Use by a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorized to process personal data.

TWO-DIMENSIONAL (2D) BARCODE: Also called a matrix code. A 2D way to represent information using individual black dots within a square or rectangle. For example, a QR code is a type of 2D barcode. It is similar to a linear (1D) barcode, but it can represent more data per unit area. There are different types, defined by standards such as ISO/IEC 16022, 24778, 18004, etc.

VERIFIER: A natural person or legal person, either private or public, who is formally authorized (under national law, decree, regulation or other official act or order) to verify the vaccination status presented on the DDCC.

¹ This definition is based on the definition published by the Internet Engineering Task Force (IETF) (<https://www.ietf.org/rfc/rfc2119.txt>, accessed 30 June 2021).

Executive summary



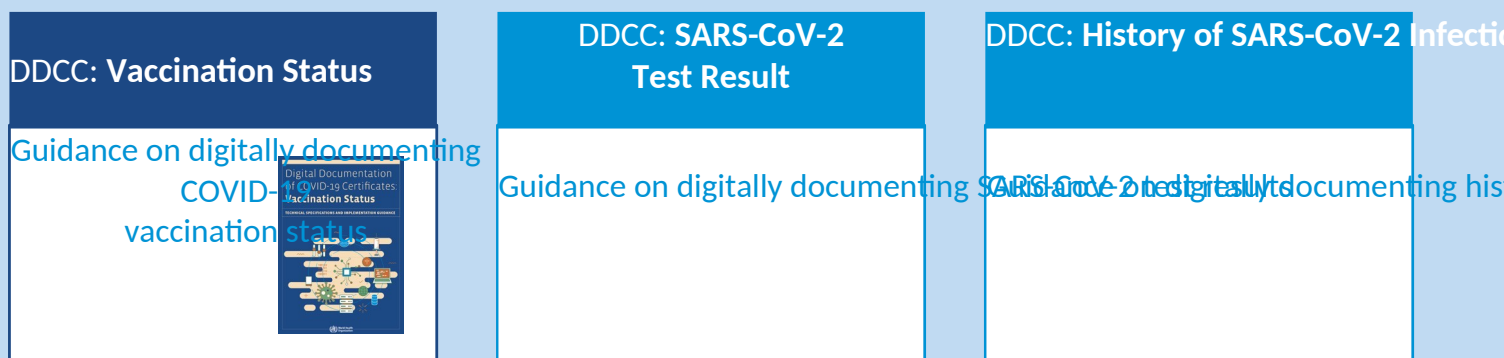
In the context of the coronavirus disease (COVID-19) pandemic, the concept of Digital Documentation of COVID-19 Certificates (DDCC) is proposed as a mechanism by which a person's COVID-19-related health data can be digitally documented via an electronic certificate. A digital vaccination certificate that documents a person's current vaccination status to protect against COVID-19 can then be used for continuity of care or as proof of vaccination for purposes other than health care. The resulting artefact of this approach is referred to as the Digital Documentation of COVID-19 Certificates: Vaccination Status (DDCC:VS).

The current document is written for the ongoing global COVID-19 pandemic; thus, the approach is architected to respond to the evolving science and to the immediate needs of countries in this rapidly changing context; for this reason, the document is issued as interim guidance. The approach could eventually be extended to capture vaccination status to protect against other diseases.

The document is part of a series of guidance documents (see Fig. 1) on digital documentation of COVID-19-related data of interest: vaccination status (this document), laboratory test results, and history of SARS-CoV-2 infection.

The World Health Organization (WHO) has developed this guidance and accompanying technical specifications, in collaboration with a multidisciplinary group of partners and experts, in order to support WHO Member States in adopting interoperable standards for recording vaccination status. The audience of this document is therefore Member States and their implementing partners that want to put in place digitally signed vaccination records.

Figure 1
Guidance documents for DDCC



What is the DDCC:VS?

A vaccination certificate is a health document that records a vaccination service received by an individual, traditionally as a paper card noting key details about the vaccinated individual, vaccine administered, date administered, and other data in the core data set (see [section 5.2](#)). Digital vaccination certificates are immunization records in an electronic format that are accessible by both the vaccinated person and authorized health workers, and which can be used in the same way as the paper card: to ensure continuity of care or provide proof of vaccination. These are the two scenarios considered in this document (see Table 1).

A vaccination certificate can be purely digital (e.g. stored in a smartphone application or on a cloud-based server) and replace the need for a paper card, or it can be a digital representation of the traditional paper-based record (see Fig. 2). A digital certificate should never require individuals to have a smartphone or computer. The link between the paper record and the digital record can be established using a one-dimensional (1D) or two-dimensional (2D) barcode, for example, printed on or affixed to the paper vaccination card. References to the “paper” record in this document mean a physical document (printed on paper, plastic card, cardboard, etc.). An illustrative example of a paper-based DDCC:VS is given in [Annex 1](#).

The DDCC:VS is a digitally signed representation of data content that describes a vaccination event. DDCC:VS data content respects the specified core data set and follows the Health Level Seven (HL7) Fast Healthcare Interoperability Resources (FHIR) standard detailed in the FHIR Implementation Guide.

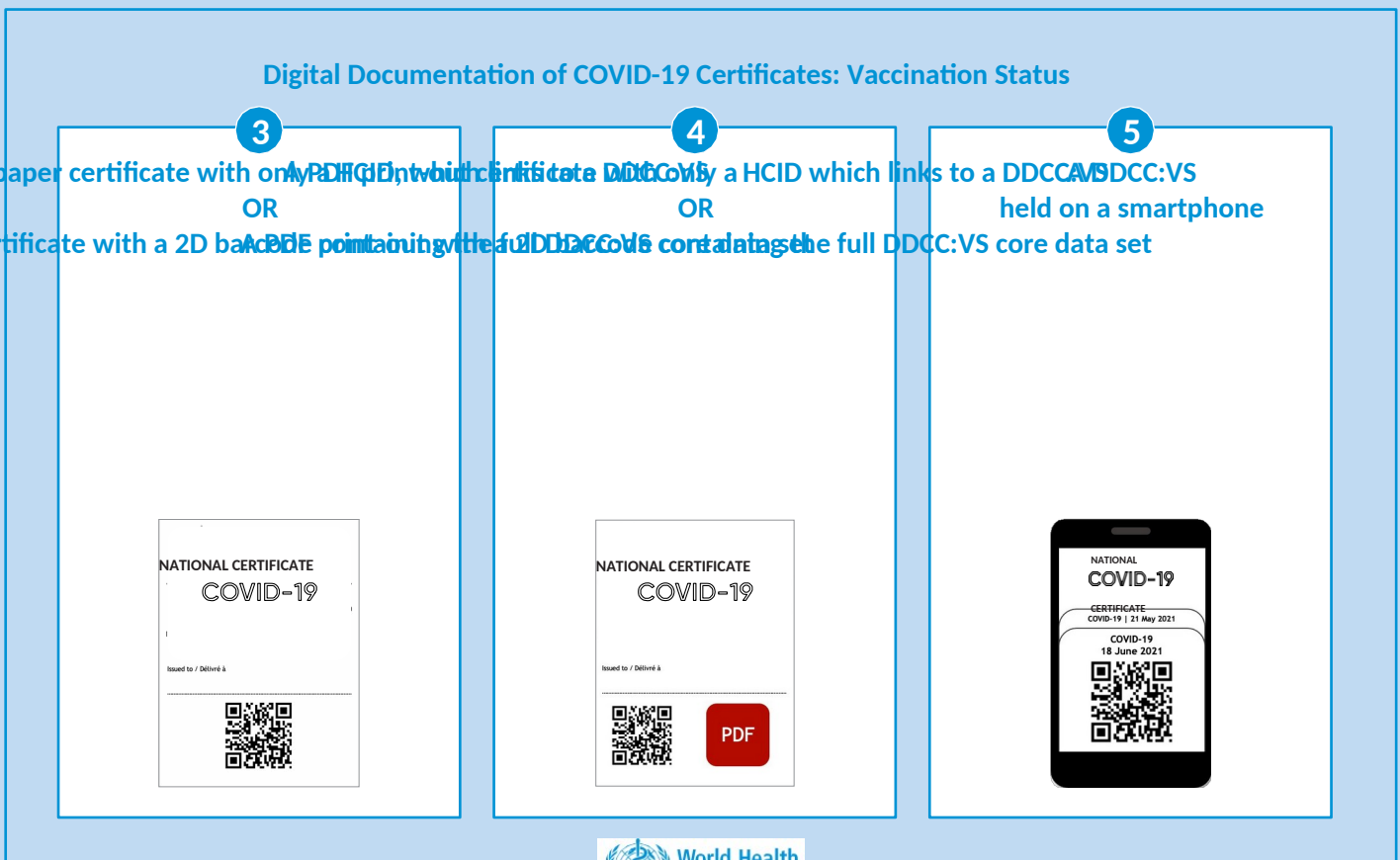
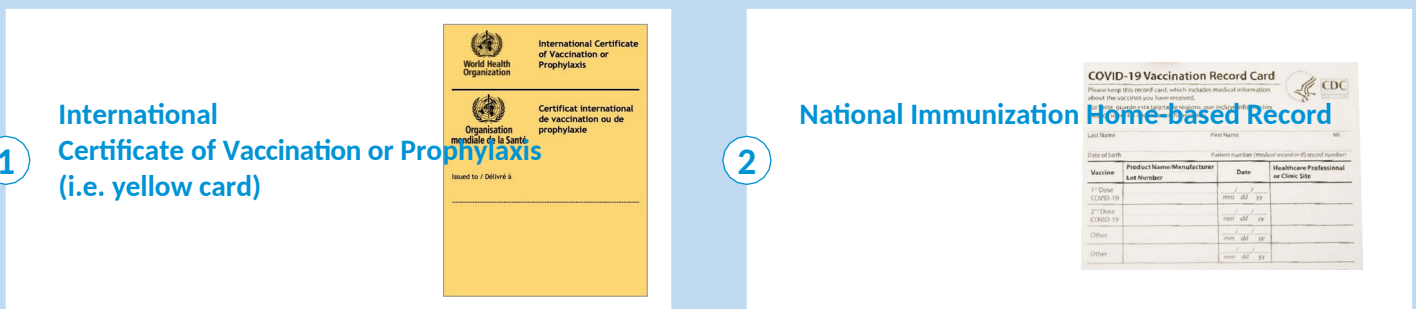
The guidance in this document is for a digital record that only shows that a vaccination has occurred. The digital record is not intended to serve as an immunity passport or provide a judgement or decision on what that vaccination means or permits.

This guidance is consistent with advice provided to the WHO secretariat at the eighth meeting of the International Health Regulations (2005) Emergency Committee (IHR EC) regarding the coronavirus disease (COVID-19), “advocating for WHO to expedite the work to establish updated means for

documenting COVID-19 status of travellers, including vaccination, history of SARS-CoV-2 infection, and SARS-CoV-2 test results.”¹ In the absence of a mechanism to digitally document COVID-19 vaccination status, it may be recorded in the International Certificate of Vaccination and Prophylaxis (ICVP). The ICVP format and data set would suffice as a valid health document for any future digitization efforts. Furthermore, in response to the IHR EC advice to the Secretariat, WHO is actively working to update the design of the ICVP to accommodate the COVID-19 status of travelers, including vaccination, history of infection, and test results consistent with the DDCC:VS specifications. In relation to the ICVP, The IHR EC furthermore recommends States Parties “recognition of all COVID-19 vaccines that have received [WHO Emergency Use Listing](#) in the context of international travel. In addition, States Parties are encouraged to include information on COVID-19 status, in accordance with WHO guidance, within the WHO booklet containing the International Certificate of Vaccination and Prophylaxis; and to use the digitized version when available.”

1 [Statement on the eighth meeting of the International Health Regulations \(2005\) Emergency Committee regarding the coronavirus disease \(COVID-19\) pandemic](#)

Figure 2
Different illustrative formats of DDCC:VS



Scenarios of use of the DDCC:VS

The scope of this document covers two scenarios of use for the DDCC:VS (see Table 1).

1. **CONTINUITY OF CARE:** Vaccination records are an important part of an individual's medical records, starting at birth. The Continuity of Care scenario describes the primary purpose of a vaccination certificate. The vaccination record shows individuals and caregivers which vaccinations an individual has received, as part of that individual's medical history; it therefore supports informed decision-making on any future health service provision.
2. **PROOF OF VACCINATION:** Vaccination records can also provide proof of vaccination status for purposes not related to health care.

Table 1
Some possible uses of DDCC:VS

Continuity of Care	Proof of Vaccination
<ul style="list-style-type: none"> → Provides a basis for health workers to offer a subsequent coverage dose and/or appropriate health services → Provides schedule information for an individual to know test, whether another dose, and of which vaccine, is needed, and when the next dose is due → Enables investigation into adverse events by health workers, as per existing guidance on adverse events following immunization (AEFI) (vaccine safety) 	<ul style="list-style-type: none"> → Establishes the vaccination status of individuals in monitoring surveys → Establishes vaccination status after a positive COVID-19 to understand vaccine effectiveness → For work → For university education → For international travel*
<p>* In the context of international travel, in accordance with advice from the 8th meeting of the International Health Regulations (2005) Emergency Committee on COVID-19, held on 14 July 2021, countries should not require proof of COVID-19 vaccination as a condition for travel.</p>	

The use cases within the two scenarios will vary depending on the digital maturity and local context of the country in which a DDCC:VS solution is implemented.

What are the minimum requirements to implement a DDCC:VS?

Digital vaccination certificates should meet the public health needs of each WHO Member State, as well as the needs of individuals around the world. They should never create inequity due to lack of access to specific software or technologies (i.e. a digital divide). The recommendations for the implementation of DDCC:VS must therefore be applicable to the widest range of use cases, catering to many different levels of digital maturity between implementing countries. The minimum requirements were developed accordingly, to allow the greatest possible flexibility for Member States and their implementer(s) to build a solution that is fit for purpose in the context of their overall health information systems.

The minimum requirements for a DDCC:VS are as follows.

- The potential benefits, risks and costs of implementing a DDCC:VS solution should be assessed before introducing a DDCC:VS system and its associated infrastructure. This includes an impact assessment of the ethical and privacy implications and potential risks that may arise with the implementation of a DDCC:VS.
- Member States must establish the appropriate policies for appropriate use, data protection and governance of the DDCC:VS to reduce the potential harms, while achieving the public health benefits involved in deploying such a solution.
- A digitally signed electronic version of the data about a vaccination event, called a DDCC:VS, must exist. As a minimum, both the required data elements in the core data set and the metadata should be recorded, as described in [section 5.2](#).
- An individual who has received a vaccination should have access to proof of this – either as a traditional paper card or a version of the electronic DDCC:VS.
- Where a paper vaccination card is used, it should be associated with a health certificate identifier (HCID). A DDCC:VS should be associated, as a digital representation, with the paper vaccination card via the HCID. Multiple forms of digital representations of the DDCC:VS may be associated with the paper vaccination card via the HCID.
- The HCID should appear on any paper card in both a human-readable and a machine-readable format (i.e. alphanumeric characters that are printed, as well as rendered as a 1D or 2D barcode).
- A DDCC:VS Generation Service should exist. The DDCC:VS Generation Service is responsible for taking data about a vaccination event, converting it to use the FHIR standard, and then digitally signing the FHIR document and returning it to the DDCC:VS Holder. This signed FHIR document is the DDCC:VS.
- A DDCC:VS Registry Service should exist. The DDCC:VS Registry Service is responsible for storing an index that associates an HCID with metadata about the DDCC:VS. As a minimum, the Registry Service stores the core metadata described in [section 5.2](#). One or more DDCC:VS Repository Service(s) *may* exist, which can be used to retrieve a DDCC:VS; in which case the location of the DDCC:VS may also be included in the metadata within the DDCC:VS Registry Service.

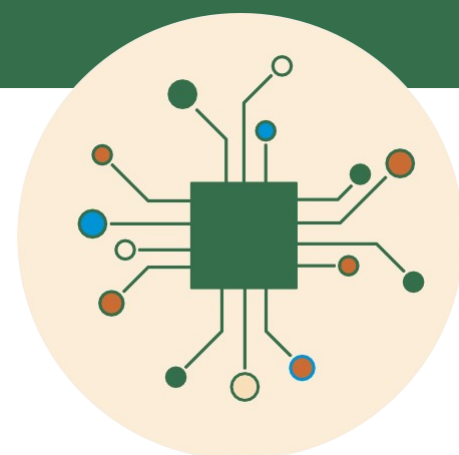
The different services are discussed in more detail in [sections 3](#) and [4](#), and are shown in Fig. 7.

These components are minimum requirements; Member States may adopt and develop additional components for their deployed DDCC:VS system.

SECTION

1

Introduction



Coronavirus disease (COVID-19), caused by the severe acute respiratory syndrome coronavirus 2 (SARS-CoV-2), was first identified in December 2019 and has spread to become a global pandemic. The outbreak has forced curtailment of movement, curfews and adoption of preventative measures to try to halt transmission, lower the burden on health systems, and reduce morbidity and loss of life. COVID-19 vaccines are being delivered at record speed, and countries need a way to give individuals a record of their vaccination status. Ideally, digital technology can be leveraged to facilitate large-scale vaccination campaigns and augment paper-based vaccination cards, which are easily lost and prone to fraud (1–4). There are a wide range of digital solutions that can be used to document COVID-19 vaccination, and choices on design and implementation should be guided by balancing various values and contextual considerations. To ensure respect for human rights and protection of values such as equity and public trust, the technical specifications and implementation guidance outlined in this document have been built on the basis of the ethical considerations and data protection principles described in [section 2](#) of this document.

1.1. Purpose of this document

This document lays out an approach for creating a signed digital version of a vaccination record for COVID-19 based on a core data set of key information to be recorded, and an approach for the digital signature. The document leverages existing free and open standards, and is driven by the ethics, use cases and requirements for Digital Documentation of COVID-19 Certificates: Vaccination Status (DDCC:VS).

As Member States are increasingly looking to adopt digital solutions for a vaccination certificate for COVID-19, this document provides a baseline set of requirements for a compliant DDCC:VS solution that is interoperable with other standards-based solutions. With the baseline requirements met, it is also anticipated that Member States will further adapt and extend these specifications to suit their needs, most likely working with a local technology partner of their choice to implement a digital solution.

This document is therefore software-agnostic and provides a starting point for Member States to design, develop and deploy a DDCC:VS solution for national use in whichever format best suits their needs (e.g. a paper card with a one-dimensional [1D] barcode or QR code stickers, or a fully functioning smartphone application developed internationally or locally).

1.2. Target audience

The primary target audience of this document is national authorities tasked with creating or overseeing the development of a digital vaccination certificate solution for COVID-19. The document may also be useful to government partners such as local businesses, international organizations, non-governmental organizations and trade associations, that may be required to support Member States in developing or deploying a DDCC:VS solution.

1.3. Scope

1.3.1. In scope

This document specifically focuses on how to digitally document COVID-19 vaccination status and attest that an individual has received a vaccine (i.e. how to provide a signed digital vaccination certificate). Two priority scenarios are described in Table 1: Continuity of Care and Proof of Vaccination. This document describes a specification for a signed digital vaccination certificate, including:

- ethical and legal considerations, and privacy and data protection principles for the design, implementation and use of a DDCC:VS;
- use cases arising from the two scenarios for the operation of a DDCC:VS, including the sequence of steps involved in executing the scenarios;
- a core data set with the data elements that must be handled for a DDCC:VS describing vaccination status, as described in the use cases;
- a Health Level Seven (HL7) Fast Healthcare Interoperability Resources (FHIR) implementation guide based on the content outlined in this guidance document, to support the adoption of open standards for interoperability; and
- approaches for implementing a DDCC:VS, including considerations for setting up a national trust framework to enable digital signing of a vaccination certificate.

1.3.2. Out of scope

Aspects that are considered out of the scope of this work are:

- digital documentation of COVID-19 laboratory test results (which will be covered in a separate guidance document);
- digital documentation of history of SARS-CoV-2 infection (which will be covered in a separate guidance document);
- digital documentation of COVID-19 recovery status because of the uncertainty around any immunity status arising from recovery;
- any governance, judgement or decision based on the information provided in a DDCC:VS for any purpose (e.g. its use as a vaccine passport);
- recording and handling of adverse event reporting;
- considerations for monitoring and evaluation of DDCC:VS roll-out and use;
- the choice of algorithm for generating any two-dimensional (2D) barcodes, which is at the discretion of the Member State. A Member State may augment the core data set with additional information (e.g. a passport number) to provide a stronger identity binding than is presumed in this document, for use cases that require it under existing Member State policies and regulations. Identity binding would enable utilization of existing 2D barcode algorithms such as those set out by the International Civil Aviation Organization (ICAO) and the European Union. The HL7 FHIR implementation guide (at <https://WorldHealthOrganization.github.io/ddcc>) provides an algorithm for generating 2D barcodes that may be used in the absence of identifying information beyond that found within the core data set; and
- technical functionality to support selective disclosure of information contained in DDCC:VS.

1.4. Assumptions

The technological specification for a DDCC:VS is intended to be flexible and adaptable for each Member State to meet its diverse public health needs as well as the diverse needs of individuals around the world. It is assumed that there is no one-size-fits-all solution, and so the specification must remain flexible and software-agnostic, while minimizing the amount of digital infrastructure required.

The requirements outlined are intended to allow for DDCC:VS solutions to meet the needs of a country's holistic public health preparedness and response plan, while still being usable in other national and local contexts. An overarching assumption is that multiple digital health products and solutions will be implemented to operationalize the requirements described in this document. This allows for support of local and sustainable development so that Member States have a broad choice of appropriate solutions without excluding compliant products from any source.

The following assumptions are made about Member States' responsibilities as foundational aspects of setting up and running a DDCC:VS solution.

- Member States will be responsible for **implementing the policies** necessary to support the DDCC:VS workflows, complying with their legal obligations under national and international law, including any applicable obligations related to respecting human rights and data protection policies.

- Member States will adhere to **ethical principles** and act to prevent new inequities from being created by a DDCC:VS solution.
- The DDCC:VS is a **health document** associated with an individual who has proved that they are who they claim to be, based on the policies established by the Member State; it is not, itself, an identity card or identification document.
- It will be up to the Member State to determine the **mechanism for unique identification** of the Subject of Care. For continuity of care, a health worker is able to ascertain the identity of a Subject of Care as per the norms and policies of the Public Health Authority (PHA) and based on existing national laws and policies.
- It will be up to the Member State to determine the **format in which to implement the DDCC:VS**. To avoid digital exclusion, the recommendations and requirements in the current document are designed to support the use of paper augmented with 1D or 2D barcodes or a smartphone application, or in another format.
- If a Member State decides to implement the DDCC:VS in paper format, any paper vaccination card issued will have a **health certificate identifier (HCID)** in both a human-readable and, additionally, a machine-readable (1D or 2D barcode) format to link it to a digital record. The HCID will be used as an index for the DDCC:VS.
- Respecting the data protection principles (see [section 2.2](#)), Members States will **adhere to data protection and privacy laws and regulations** established under national law or adopted through bilateral or multilateral agreements.
- The PHA of a Member State will need to have access to a national public key infrastructure (PKI) for **digitally signing the DDCC:VS**. This document does not describe the PKI in detail, but key assumptions are that the PHA will need to:
 - » establish and maintain a root certificate authority that anchors the country's PKI for the purposes of supporting DDCC:VS;
 - » generate and cryptographically sign document signer certificates (DSCs);
 - » authorize document signer private keys to cryptographically sign digital DDCC:VS;
 - » broadly disseminate public keys if there is a desire to allow others to validate issued DDCC:VS;
 - » allow for the health content contained within a traditional paper vaccination card to be digitized and verifiable by one or more digital representations, including, as a minimum, a DDCC:VS identified through the HCID; a Member State may choose to also generate and distribute to the DDCC:VS Holder a signed 2D barcode as a digital representation, containing, as a minimum, the core data set content (e.g. printed on or attached to the paper record, sent by email, loaded into a smartphone app or downloaded from website);
 - » keep the signature-verification processes manageable; the number of private keys used by the PHA to sign DDCC:VS should be no more than a small proportion relative to the number of digital health solutions used to capture health events; and
 - » ensure private keys used to sign DDCC:VS will not be associated with individual health workers.
- The PHA will need to **operate a DDCC:VS Generation Service** to create DDCC:VS, and a DDCC:VS Registry Service to record their issuance. Optionally, the PHA may also decide to provide a DDCC:VS Repository Service to allow requesters to search for, and retrieve, a DDCC:VS using the HCID (for the purposes of verification or continuity of care).
- Subsequent vaccinations recorded on a paper card may be added to the Subject of Care's digital record associated to the HCID on the paper card, resulting in a **new instance of a DDCC:VS**.

1.5. Methods

Since the COVID-19 pandemic began, and as vaccines have shown signs of efficacy, the number of digital solutions for vaccination certificates has increased. For the WHO to remain software-agnostic, the Smart Vaccination Certificate Working Group was created, with the intention of being a multisectoral working group focused on supporting development of key standards for digital vaccination certificates, sharing joint learnings, and supporting development of a governance model with a national trust framework architecture to support the roll-out of COVID-19 vaccines nationally (5).

Furthermore, the WHO has developed this guidance in consultation with Member States and partner organizations to ensure it is implementable in all contexts.

1.6. Additional WHO guidance documents

Specific guidance on how or when DDCC:VS should be used can be found in the following WHO guidance documents.

- [Technical considerations for implementing a risk-based approach to international travel in the context of COVID-19: Interim guidance, 2 July 2021](#) (6)
- [Policy considerations for implementing a risk-based approach to international travel in the context of COVID-19](#) (7)
- [Interim guidance on considerations for implementing and adjusting public health and social measures in the context of COVID-19](#) (8)

The following WHO guidance documents also served as a baseline for this work.

- [Statement of the eighth meeting of the International Health Regulations \(2005\) Emergency Committee regarding the coronavirus disease \(COVID-19\) pandemic](#) (40)
- [Statement of the seventh meeting of the International Health Regulations \(2005\) Emergency Committee regarding the coronavirus disease \(COVID-19\) pandemic](#) (9)
- [Statement on the sixth meeting of the International Health Regulations \(2005\) Emergency Committee regarding the coronavirus disease \(COVID-19\) pandemic](#) (10)
- [Interim position paper: considerations regarding proof of COVID-19 vaccination for international travellers \(as of 5 February 2021\)](#) (11)
- [Monitoring COVID-19 vaccination: considerations for the collection and use of vaccination data](#) (12)
- [Practical guide for the design, use and promotion of home-based records in immunization programmes](#) (13)
- [Guidance on developing a national deployment and vaccination plan for COVID-19 vaccines](#) (14)
- [International Health Regulations \(2005\), third edition](#) (15)

1.7. Other initiatives

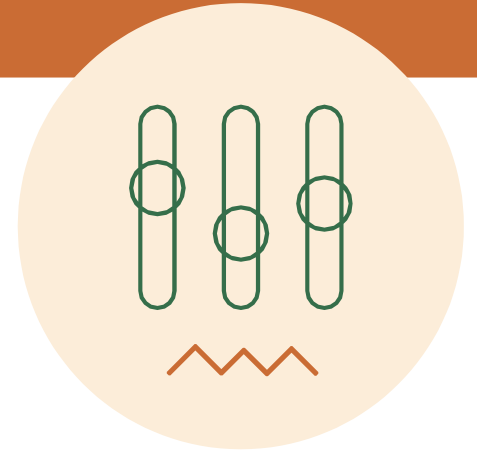
DDCC:VS core data set guidance laid out in this document may be leveraged to generate artefacts conformant with other initiatives such as the International Civil Aviation Organization (ICAO) *Guidelines on visible digital seals (“VDS-NC”) for travel-related health proofs* (16) and the European Union (EU) EU Digital COVID Certificate (17). Additional technical details can be found on

the DDCC vaccination certificate implementation guide available at:
WorldHealthOrganization.github.io/ddcc.

SECTION

2

Ethical considerations and data protection principles



As with any digital solution, there are ethical considerations, such as potential impacts on equity and on equitable access, and data protection principles that need to inform the design of the technical specifications, as well as provide guidance on how resulting solutions can be ethically implemented. The following sections discuss some key ethical considerations and data protection principles that Member States are encouraged to – and, where they have legal obligations, must – include in their respective deployments of any DDCC:VS. These ethical considerations and data protection principles have also informed the design criteria for a DDCC:VS outlined in the following section.

2.1. Ethical considerations for a DDCC:VS

This section presents ethical considerations to take into account when designing, developing and deploying a DDCC:VS as part of the response to the COVID-19 pandemic (which may be extended to other diseases). This document covers two priority scenarios of use for a DDCC:VS, which are:

1. as a record to serve as the basis for continuing healthcare for that individual (Continuity of Care); and
2. as a record documenting that an individual has received a vaccination (Proof of Vaccination).

This section therefore focuses on the ethical considerations relevant to these two use cases in a national or local setting and provides some recommendations for their ethical implementation. It also briefly mentions some further considerations that may be important if further domestic uses for DDCC:VS are developed. Such potential uses include public health surveillance, pharmacovigilance, research, and exemptions to public health and social measures (8).

Requiring proof of vaccination to protect against COVID-19 for international travel as a condition for entry to or exit from a country will not be discussed here, as it is a legal matter that is captured in the WHO's interim position paper on considerations regarding proof of COVID-19 vaccination

for international travellers specifying “proof of COVID-19 vaccination should not be required as a condition of entry to, or exit from a country.”(11)

2.1.1. Key ethical considerations for current proposed uses of DDCC:VS

Ethics should be an integral part of the design and deployment of a DDCC:VS solution. However, policy decisions are often complex and difficult. Many different considerations will need to be made and weighed against each other. Often, the evidence is uncertain and there are many different competing ethical perspectives and positions. Evidence alone will not provide the right answer, nor will a simple set of ethical rules. Public health action requires careful judgement and acceptance of responsibility for the outcomes. A number of different ethical considerations should be taken into account, including both objectives and processes.

2.1.1.1 Objectives

A good starting point is to identify how the use of a DDCC:VS can contribute to important general duties of any government through public health activity in response to infectious diseases such as COVID-19. Three key objectives of public health action are:

1. to protect and promote the welfare of individuals, communities and the population as a whole;
2. to ensure equal treatment for all individuals and prevent or mitigate, as far as possible, avoidable and unfair health inequalities (i.e. health inequities) within the boundaries of the state; and
3. to create and maintain trust in public health activities as part of the health-care system.

The creation and use of a DDCC:VS can contribute to each of these objectives. For example, in relation to objective 1, a DDCC:VS can promote welfare through proof of vaccination and continuity of care

by ensuring that individuals do not receive an inappropriate mix of vaccine types, and also allow for appropriate follow-up in the unlikely event of any adverse events. Promotion of this objective also contributes to confidence in the vaccination programme, benefitting the whole population.

Such

an outcome is an important common good – that is, a good for all that cannot be created by each individual alone. Such goods require the coordinated actions of, and support from, governments. In addition, other benefits will follow from the use of a DDCC:VS, because of improved health and subsequent increased opportunities for individuals and communities to make their own choices and pursue their own economic and social goals.

In relation to objective 2, equal treatment requires respecting and protecting all persons equally and acting to ensure, as far as possible, that there is no discrimination against anyone. An example of how to work towards this objective is to ensure that appropriate personal data protection safeguards are implemented. Individual vaccination status is private information, and protections need to be in place to ensure that no individual is forced to disclose or publicly display a DDCC:VS to access any public area or activity (18). Such a practice and/or the lack of a DDCC:VS itself may result in the stigmatization of individuals without a DDCC:VS and may exacerbate the risk of harms.

Another example of working towards objective 2 is to think about ways to try and achieve

equity through the distribution of health resources. While DDCC:VS may offer a more reliable, accurate and trusted mechanism to record an individual vaccination history, they risk exacerbating health inequities, for the following reasons.

- While COVID-19 vaccines may eventually be widely accessible, current global distribution is inequitable and there are populations that vaccination programmes may struggle to reach due to, for example, geography, terrain, transient or nomadic movement, war and conflict, or illegal or insecure residency status (19). These hard-to-reach populations (e.g. refugees, asylum seekers, internally displaced persons) are disproportionately less likely to have an opportunity to be vaccinated and obtain a DDCC:VS.
- A DDCC:VS may increase digital exclusion if its application and use requires that individuals have access to a digital infrastructure or if that digital infrastructure is too burdensome for all Member States to deploy.
- Vaccinated individuals with geographical, financial or disability barriers may also be excluded from obtaining and using a DDCC:VS, depending on the administration process, cost and design. Ensuring an equitable and inclusive approach to the implementation of DDCC:VS will mean that those with greater barriers to obtaining and using a DDCC:VS are supported to a greater extent than others.

In relation to objective 3, trust is vital to ensuring the benefits of DDCC:VS for individuals, communities and the whole population. For example, the provision of robust data protection measures and the use of procedural considerations, outlined in [section 2.2](#), may contribute to the maintenance of trust in public health systems. This in turn contributes to the delivery of objective 1. Another example might be that a DDCC:VS should only be used for its intended purpose, as inappropriate uses may result in legitimate ones being undermined.

2.1.1.2 Processes

The pursuit of the objectives above can create ethical problems. One way to mitigate this risk is by ensuring that various processes uphold important procedural values. These values, in turn, also contribute to the pursuit of the objectives above. Such values include:

- **TRANSPARENCY:** providing clear, accurate and publicly accessible information about the basis for the policy and the process by which it is made, from the onset – i.e. notifying the public that such a process is underway. Such a process disciplines decision-making and ensures accountability by providing a sound basis for an eventual decision that reasonable members of the public may agree with.
- **INCLUSIVENESS IN DECISION-MAKING:** providing opportunities for all relevant stakeholders to participate in policy formulation and design, in particular those affected, and advocates for these individuals and groups.
- **ACCOUNTABILITY:** providing a clear framework for who is responsible for what, and how responsibilities will be regulated and enforced.
- **RESPONSIVENESS:** providing mechanisms and opportunities to review and revise decisions and policies based on evolving scientific evidence and other relevant data. This may include public consultation or engagement with a wide range of experts, industries and other stakeholders so that the policies are responsive to real and perceived ethical issues and concerns. Particularly important stakeholders are those who are likely to be disadvantaged or face distinct or heightened risks with the creation of a DDCC:VS, such as individuals who are unable or unwilling to be vaccinated, individuals with insecure or invalid citizenship or residency status, and vaccinated individuals who may face other barriers in obtaining or using a DDCC:VS (20).

2.1.2. Ethical considerations related to further potential uses of DDCC:VS

The two currently proposed uses of DDCC:VS, proof of vaccination and continuity of care, are features of traditional clinical uses. However, a number of other possible uses for a DDCC:VS raise ethical issues. In the context of COVID-19, a DDCC:VS might play a role in achieving various public health purposes such as determining vaccination coverage in a given population, which may help to determine when to lift or relax public health and social measures (PHSMs) at a population level. A DDCC:VS might also be used to facilitate individualized exemption from, or, reduction of PHSMs (e.g. reduced quarantine time post exposure) or individual access to an activity based on proof of vaccination (if such uses are held to be ethical), which we can term a “health pass” function. The potential deployment of a DDCC:VS for these purposes, particularly as a health pass, engenders a number of potential ethical problems for individuals and communities, and human rights challenges (21,22).

First, use of a DDCC:VS as a health pass raises a distinct set of risks because of current scientific uncertainties regarding COVID-19 vaccines. While COVID-19 vaccines have demonstrated efficacy and effectiveness in preventing severe disease and death, the extent to which each vaccine prevents transmission of SARS-CoV-2 to susceptible individuals remains to be assessed. How long each vaccine confers protection against severe disease and against infection, and how well each protects against current and future variants of SARS-CoV-2 needs to be regularly assessed. In this context of scientific uncertainty, use of a DDCC:VS as a health pass based solely on individual vaccination status may increase the risk of disease spread. This is particularly the case if individuals with a DDCC:VS are completely exempted from PHSMs or if it is hard to enforce individuals’ compliance with required

PHSMs during an activity (e.g. mask wearing and physical distancing during a concert) to which they are allowed access based on their DDCC:VS.

Second, some potential behavioural responses to a DDCC:VS in its role as a health pass could undermine individual and public health. These include the following.

- Where the benefits of a health pass are significant, it may result in vaccination certification fraud. This may increase COVID-19 risks if a non-vaccinated person is potentially in contact with vulnerable people.
- Individuals may be less willing to disclose their medical history and (potential) contraindications to a COVID-19 vaccine in order to be vaccinated and to obtain a DDCC:VS, which increases the risk of adverse events.
- The creation of a DDCC:VS following vaccination for each individual may incentivize more people to receive a vaccine to access the benefits of a DDCC:VS. However, it may also increase vaccine hesitancy because of privacy and other concerns that the vaccination record could be linked to personal data and be used for functions other than those originally intended (e.g. surveillance of individual health status), or be used by unintended third parties (e.g. immigration, commercial entities, researchers) (23).

Third, a DDCC:VS in its use as a health pass risks introducing unfair disadvantages and injustices. The limited supply of COVID-19 vaccine within some countries has been distributed to prioritize those at greatest risk of infection (such as health-care workers) or severe outcomes (such as the elderly). There is a danger that those who are willing to be vaccinated but have not yet been offered a vaccine, or those who are unable to be vaccinated for medical reasons, would be unfairly disadvantaged if a DDCC:VS incorporated health pass functions. Consideration should be given to whether unvaccinated

individuals could use other proofs of health status to allow them similar access to the same services while mitigating the risk of disease spread. These other proofs may include a negative COVID-19 test or proof of post-infection-acquired immunity based on tests that are reliable and accurate (which have been called immunity certificates), although this also raises considerable scientific and ethical concerns (24).

2.1.3. Recommendations

The design, development and implementation of a DDCC:VS for domestic use raises many ethical issues. The following series of recommendations focuses on the two proposed priority uses of DDCC:VS for Proof of Vaccination and Continuity of Care.

1. THE SCOPE OF USE OF A DDCC:VS SHOULD BE CLEARLY DEFINED.

A DDCC:VS can be used for a number of purposes. Each Member State that introduces one should be clear about which uses are proposed and that a DDCC:VS should not be used for other purposes.

The current proposed uses are for proof of vaccination and continuity of care only. To prevent any potential misuse, any DDCC:VS policy should set out clear and specific policies, and laws if needed, on the limits to legitimate uses of a DDCC:VS. Use of a DDCC:VS to restrict the right to freedom to movement and other human rights is only justified when it supports the pursuit of a legitimate aim during a public health emergency and is provided for by law, proportionate, of limited duration, based on scientific evidence, and not imposed in an arbitrary, unreasonable or discriminatory manner.

2. POTENTIAL BENEFITS, RISKS AND COSTS SHOULD BE ASSESSED BEFORE INTRODUCTION OF A DDCC:VS.

The creation or development of a DDCC:VS should be based on an assessment of the benefits and costs of its uses, and the advantages and disadvantages of the proposed infrastructure, in comparison with other potential or existing ways to record, validate and verify vaccination records. Benefit and cost assessment – as a function of stewardship of scarce public health resources – should take short-, medium- and long-term views. A short-term view would consider the utility and opportunity cost of investing in a DDCC:VS infrastructure over other measures for responding to COVID-19 and meeting other public health needs during a public health crisis. Consideration should be given to whether the DDCC:VS infrastructure could hinder vaccination rates or reduce access to vaccines because of the potential inefficiencies it may introduce for processing vaccination registration and certification. A long-term view would consider the potential advantages of a DDCC:VS for strengthening the health system, such as enhancing the immunization information system and its interoperability across jurisdictions. In addition, the ethical issues and risks raised by a DDCC:VS, and the impact of trade-offs between the benefits and burdens accrued to individuals, families, businesses and other relevant stakeholders should be assessed prior to implementation. Community engagement, particularly with representatives of groups who are likely to face increased disadvantages or risks, should also be conducted.

3. OBTAINING AND USING A DDCC:VS SHOULD BE AS INCLUSIVE AND FAIR AS POSSIBLE.

DDCC:VS solutions should be as inclusive as possible and should not create disadvantage. To achieve this, it may be necessary to provide alternative, cost-effective DDCC:VS solutions, including paper-based certificates, for individuals and groups with existing disadvantages, such as those with digital skill or disability barriers, those living in areas with poorer digital connectivity, and undocumented or irregular migrants. No one should be excluded through a requirement for individual payment to obtain and use a DDCC:VS.

4. ALL NECESSARY MEASURES SHOULD BE PUT IN PLACE TO PROTECT PARTICIPANTS FOR CONTINUITY OF CARE.

A DDCC:VS will include potentially sensitive data relating to the health of individuals, and this data should therefore be protected by appropriate medical confidentiality and privacy safeguards. Access to or use of the data for continuity of care should be based on the appropriate consent standard (e.g. implied or explicit) in a given health-care system and should be sufficient for the receiving health-care provider or team to continue providing good medical care. These ethical standards will also apply to international transfer of DDCC:VS data for continuity of care (such as when a patient accesses medical services abroad).

For adults without decisional capacity, use of their DDCC:VS vaccination record for decisions relating to their health care may be based on their advance decisions or, in the absence of an advance decision, be made in the adult's best interest by a health-care proxy or an authorized surrogate. Minors with sufficient intelligence and maturity should be able to allow the use of their DDCC:VS data for continuity of care, where consent is required.

5. ALL COMMUNICATION SHOULD BE CLEAR AND TRANSPARENT.

Implementation details of a DDCC:VS relevant to users should be communicated in a transparent manner, which may contribute to the promotion of public trust and acceptance of a DDCC:VS. This communication includes how a DDCC:VS would work to benefit individuals and public health, the policies and mechanisms in place to limit access to and use of a DDCC:VS by third parties, whether DDCC:VS data are linked to other types of data and the purposes of any data linkage.

If, in the future, the uses of DDCC:VS are extended into other scientific or public health purposes (e.g. programme monitoring or research), data subjects and other members of the public should be informed of the nature and occurrences of these activities in advance, the ethics oversight

or governance structure in place (including for surveillance activities (25), and options for controlling or limiting DDCC:VS data for these uses. DDCC:VS data are sensitive and should, in general, be anonymized (or pseudonymized, or de-identified) for scientific or public health purposes, to minimize risks to the data subjects. Where DDCC:VS data need to be retained in an identifiable form for these purposes, consideration should be given to whether consent is required or should be waived based on satisfaction of appropriate ethical criteria (e.g. minimal risk, impracticability of obtaining consent, no adverse effects on the rights and welfare of the data subjects, and serving a public health good).

6. THE DDCC:VS SHOULD BE CONSTANTLY MONITORED FOR IMPACT AND ADJUSTED AS NECESSARY.

Post implementation, it is important to monitor the effects of DDCC:VS in terms of positive and negative outcomes (e.g. impact on equity) and to consider potential interventions to mitigate

negative outcomes. Such monitoring should also review uses that do not fit neatly into legitimate and illegitimate use categories set by policies, to consider whether these uses should be continued, modified or stopped.

2.2. Data protection principles for a DDCC:VS

This section presents fundamental data protection principles for the DDCC:VS as a prerequisite for continuity of care and proof of vaccination. The principles are designed to provide guidance to the national authorities tasked with creating or overseeing the development of the DDCC:VS. The objectives are to encourage Member States to adopt or adapt their national laws and regulations, as necessary, respect personal data protection principles, and ensure respect for the human rights and fundamental freedoms of individuals, in particular the right to privacy, in order to build trust in the implementation of the DDCC:VS.

The data protection principles are as follows.

1. **LAWFUL BASIS, LEGITIMATE USE AND FAIR PROCESSING**

The personal data collected in the interest of the application of the DDCC:VS should be processed in a fair and non-discriminatory manner, based on the consent of the data subject, the necessity to protect the vital interests of the data subject or of another data subject, or explicitly justified by legitimate public health objectives.

The processing of personal data in the interest of the application of the DDCC:VS should have a lawful basis; it should comply with applicable laws, including broader human rights standards and data privacy and data protection laws, as well as respecting the highest standards of confidentiality, and moral and ethical conduct.

Personal data collected for the application of the DDCC:VS should only be accessed, analysed or otherwise used while respecting the legitimate interests of the data subjects concerned. Specifically, to ensure that data use is fair, data should not be used in a way that violates human rights or in any other ways that are likely to cause unjustified or adverse effects on any individual(s) or group(s) of individuals.

Any retention of personal data processed in the interest of the application of the DDCC:VS should have a legitimate and fair basis. Before any data are retained, the potential risks, harms and benefits should be considered. Personal data should be permanently deleted after the time needed to fulfil their purpose, unless their extended retention is justified for specified purposes.

2. **TRANSPARENCY**

The processing of personal data in the interest of the application of the DDCC:VS should be carried out to be transparent to the data subjects. Data subjects should be provided with easily accessible, concise, comprehensible and reader-friendly information in clear and unambiguous language regarding: the purpose of the data processing; the type of data processed; how data will be retained, stored and shared, or made otherwise accessible; who will be the recipients of the data and how long the data will be retained. Information should also be provided to data subjects on applicable data retention schedules, and on how to exercise their data subject rights. A list of entities authorized to process personal data in the interest of the application of the DDCC:VS should be made public.

3. PURPOSE LIMITATION AND SPECIFICATION

As the personal data collected in the interest of the DDCC:VS may only be used for continuity of care and proof of verification, they should not be processed in ways that are incompatible with such purposes. The use of this data for any other purpose, including the sale and use of personal data for commercial purposes, should be prohibited, except with the explicit, unambiguous and freely given prior consent of the data subject.

The purposes for which personal data are processed in the interest of the application of the DDCC:VS should be specified no later than at the time of data collection. The subsequent use of the personal data should be limited to the fulfilment of those specified purposes.

When a health worker or verifier of the DDCC:VS is carrying out their mandated activities for continuity of care or proof of vaccination; transferring personal data processed in the interest of the application of the DDCC:VS to a third party or allowing access by a third party should only be permitted if the principles underlying the lawful basis, as referred to above, are met; and the third party affords appropriate protection that is equal to or higher than those protections provided by the data controller, for the personal data.

Personal data processed in the interest of the application of the DDCC:VS should be relevant to the purposes for which they are to be used and, to the extent necessary for those purposes, be accurate, complete, and kept up to date.

4. PROPORTIONALITY, NECESSITY AND DATA MINIMIZATION

The processing of personal data should be relevant (have a rational link to specified purposes), adequate (sufficient to properly fulfil the specified purposes) and limited to what is required to fulfil the specified purposes. The processing of personal data should not be excessive for the purposes for which those personal data are collected. Data collected and retained on the DDCC:VS should be as limited as possible, respecting proportionality and necessity. Data access, analysis or other use should be kept to the minimum necessary to fulfil their purpose. The amount of data, including their granularity, should be limited to the minimum necessary. Selective disclosure mechanisms should be used to support proportionate data access.

Data use should be monitored to ensure that it does not exceed the legitimate use. Personal data retained in the interest of the application of the DDCC:VS should only be retained and stored for the time that is necessary for specified purposes. Personal data accessed at the point of verification of the DDCC:VS should not be retained and stored in a repository, database or otherwise.

5. CONFIDENTIALITY AND SECURITY

Personal data processed in the interest of the application of the DDCC:VS should be kept confidential and not disclosed to unauthorized parties; personal data should only be accessible to the data subject or to other explicitly authorized parties.

With regard to the nature and sensitivity of the personal data processed in the interest of the application of the DDCC:VS, appropriate organizational, physical and technical security measures should be implemented for both electronic and paper-based data in order to protect the security and integrity of personal data. This protection includes measures to protect against personal-data breach, and measures to ensure the continued availability of that personal data for the purposes for which it is processed; this applies regardless of whether the data are stored on devices, applications, servers or networks, or if they are sent through services involved in collection, transmission, processing, retention or storage.

Taking into account the available technology and cost of implementation, robust technical and organizational safeguards and procedures (e.g. efficient monitoring of data access, data breach notification procedures) should be implemented to ensure proper data management throughout the data life-cycle. Such measures are to prevent any accidental loss, destruction, damage, unauthorized use, falsification, tampering, fraud, forgery, unauthorized disclosure or breach of personal data.

In case of a security breach leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or access to personal data transmitted, stored or otherwise processed, DDCC:VS Holders should be notified in an appropriate and timely manner. DDCC:VS Holders should be notified of: any data breach; the nature of the data breach, which may affect their rights as data subjects; and recommendations to mitigate potential adverse effects.

6. DATA SUBJECT RIGHTS, COMPLAINT AND LEGAL REDRESS

DDCC:VS Holders, if they have provided sufficient evidence of being the DDCC:VS Holder, should be able to exercise data subject rights. These data subject rights include the right of access, correction, deletion, objection and restriction of personal data, subject to conditions regulated by national law, decree, regulation or other official act or order. Data subjects have the right to seek redress by a complaint procedure if they suffer harm or loss as a result of misused DDCC:VS data or incorrect or incomplete data. Data subjects should be provided with easily accessible, concise, comprehensible and reader-friendly information about how they might exercise their data subject rights and how to seek legal redress, including how they can exercise any rights in the case of alleged fraud.

7. INDEPENDENT OVERSIGHT AND ACCOUNTABILITY

An independent public authority should be responsible for monitoring whether any data controller and data processor involved in the processing of personal data in the interest of the DDCC:VS adhere to the principles, and may recommend revoking the authorization to collect or otherwise process DDCC:VS data. Such a public authority should have access to all information necessary to fulfil its task. Adequate policies and mechanisms should be in place to ensure adherence to these principles.

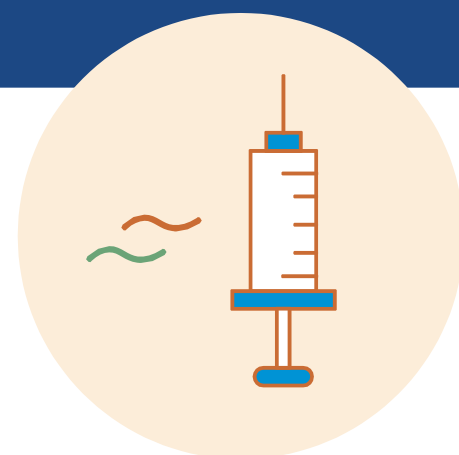
2.3. DDCC:VS design criteria

Due to the ethical considerations and data protection principles outlined above, the following design criteria were considered when formulating the requirements for implementing a DDCC:VS for the Continuity of Care scenario and for the Proof of Vaccination scenario.

1. Implementation of the DDCC:VS should not increase health inequities or increase the digital divide.
2. Everyone who has been vaccinated to protect against COVID-19 has the right to obtain and hold a DDCC:VS.
3. The DDCC:VS needs to be in a format that can be accessible to all, for example, in paper and digital formats. Any solution should also work in online and offline environments across multiple platforms – paper and digital.
4. Individuals should not be treated differently or given different levels of trust due to the format of the DDCC:VS they are using (e.g. there should be no discrimination based on whether someone is presenting a DDCC:VS on a smartphone or a paper card).
5. Any solution should not be at an additional cost to the vaccinated person. The interoperability specifications used in DDCC:VS solutions should be based on open standards to ensure equitable access to a range of non-proprietary digital tools.
6. The infrastructure that the DDCC:VS solution is built on should ensure that individuals and Member States are not locked into a commitment with only one vendor.
7. Any solution should be as environmentally friendly as possible. The most environmentally sustainable options should be pursued to reduce any additional undue harm to the environment.
8. Any solution should be designed to augment and work within the context of existing health information systems, as appropriate.
9. Any solution should not share or store more data than is needed to successfully execute its tasks. Minimization of health content for purposes not related to health care, and privacy-protecting features, should be built into the system and be respected accordingly.
10. Anti-fraud mechanisms should be built into any approach.
11. Digital technology should not be the only mechanism available for verification. There should always be possible ways to revert to a paper-only manual verification of vaccination certificates. For example, a paper representation may be printed from the DDCC:VS or captured in the International Certificate of Vaccination and Prophylaxis (ICVP) and combined with an identity verification as outlined within the policy set by the public health authority.

It is important to note that despite the technological design criteria outlined here, it will be essential for Member States to ensure that the legal and policy frameworks are in place to support responsible use of the DDCC:VS as defined by the Member State.

Continuity of Care scenario



This section describes the use cases and actors involved in using a DDCC:VS for Continuity of Care, as well as functional requirements for a digital solution. In the context of COVID-19, the use of a vaccination record for Continuity of Care is primarily to: ensure that individuals know if, and when, they will need a subsequent dose; for health workers to use the proof of COVID-19 vaccination to decide on provision of health services based on medical history; and for ensuring health workers have access to accurate vaccination history when an adverse event follows immunization. It will be up to Member States to define how this scenario is applied and adapted to their own context and level of digital maturity, in compliance with their legal and policy frameworks.

3.1. Key settings, personas and digital services

The Continuity of Care scenario is expected to involve the following settings, which can be in the same physical location.

1. **CARE SITE:** where the vaccination event takes place. Some examples of this include at a primary health-care facility, a temporary vaccination site, or a pharmacy, as determined by the Member State's vaccine delivery plan.
2. **DATA ENTRY SITE:** where the vaccination record is digitized. The record can be digitized at the care site if the digital solution is available, or it can be done retroactively under the auspices of the public health authority or health service provider.

The key personas, or relevant stakeholders, involved in the provision of a DDCC:VS are outlined in Table 2. These key personas are anticipated to interact with the digital services outlined in Table 3, including digital services that might not have a user interface that the key personas interact with, but are critical building blocks of the reference architecture.

Table 2
Key personas for Continuity of Care

	The person who receives the vaccination.
	The person who has the Subject of Care's vaccination certificate. The person is usually the Subject of Care but does not have to be. For example, a caregiver may hold the DDCC:VS for a child or other dependant.
	The person who administers the vaccine. Depending on national policies, the person who administers the vaccine might not be a formal health-care worker. Examples of vaccinators could include physicians, nurse practitioners, community health workers or other trained volunteers.
	The person who enters the information about the Subject of Care (as outlined in the data set) that has been manually recorded at care sites into a digital system. Health workers can also be the Data Entry Personnel if a point-of-care system is in place that allows workers to digitally document a vaccination event right away.
	An entity or organization under whose auspices the vaccination is performed and the DDCC:VS is issued.

Table 3
Digital services for Continuity of Care

	A secure system that is used at the point of care or health facility, such as an electronic immunization registry (EIR), an electronic medical record or a shared health record (SHR).
	The service that is responsible for taking data about a vaccination event, converting that data to use the FHIR standard, signing that HL7 FHIR document, returning it to the Digital Health Solution, and making the digital artefact available to serve Continuity of Care and Proof of Vaccination use cases.
	The signed HL7 FHIR document is the DDCC:VS. The Digital Health Solution is, in turn, responsible for distributing the DDCC:VS and any associated representation of the data (such as a QR code) to the DDCC:VS Holder, based on PHA policy.
	This service also registers this signed document in a location available to the DDCC:VS Registry Service and potentially generates extra artefacts, such as QR code representations.

3.2. Continuity of Care workflows and use cases

The Continuity of Care scenario is summarized in Fig. 3. The workflow's actors and settings, and its related high-level requirements, may be described as follows.

1. A Subject of Care presents at a care site. The identity of the Subject of Care is established as per Member State processes and norms. The Subject of Care MAY present an existing DDCC:VS card to inform the care delivery process. The Vaccinator MAY retrieve existing health history data about the Subject of Care if authorized to do so.
2. A Vaccinator administers a COVID-19 vaccination.
3. Elements of the DDCC:VS core data set content SHALL be entered onto the DDCC:VS paper card, which SHALL have an HCID. The DDCC:VS paper card SHALL be provided to the DDCC:VS Holder at Point A. The HCID SHALL be used to establish a globally unique identifier (ID) for the DDCC:VS or to reference the ID of a previously established DDCC:VS.
4. The care site MAY have a local Digital Health Solution with data entered at the point of care. If so, the Vaccinator and/or Data Entry Personnel directly record details of the vaccination event, which SHALL be persisted based on the DDCC:VS core data set.
5. The care site MAY have a local Digital Health Solution with data entered after the vaccine administration event. If so, Data Entry Personnel can record details of the vaccination event, which SHALL be persisted according to the DDCC:VS core data set.

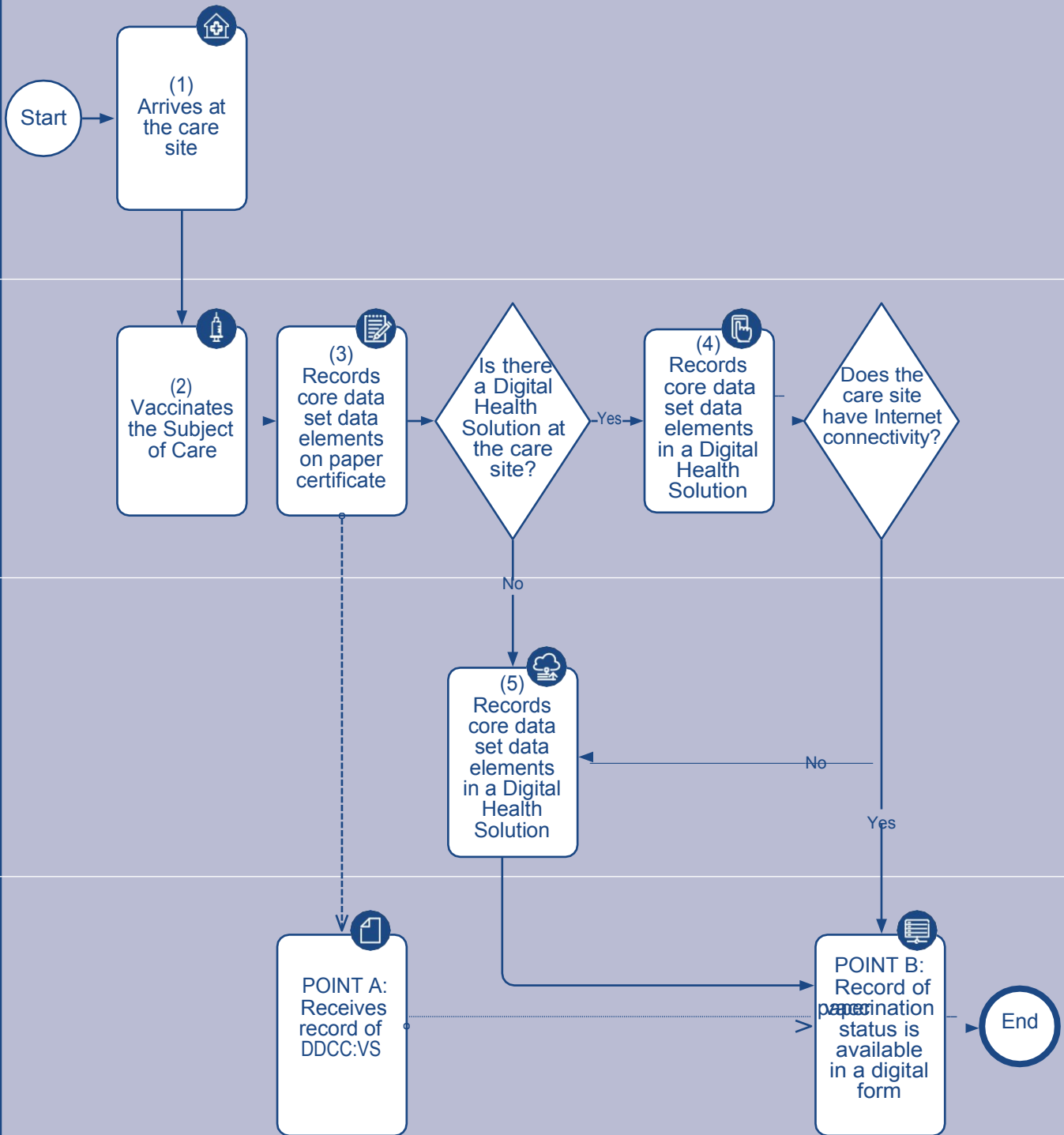
If a Digital Health Solution does not exist at the care site, details of the vaccination event SHALL be recorded and persisted in a paper record (e.g. immunization registry book), according to the required DDCC:VS core data set. Details of the vaccination event can then be electronically recorded into a Digital Health Solution available at another site, by Data Entry Personnel.

Health data captured during the vaccination event SHALL be recorded as coded content using the FHIR standard. If the data represent a subsequent vaccination event (e.g. second dose), this content SHALL be added as another event to the Subject of Care's existing FHIR composition.

Once the DDCC:VS content is digitally recorded and persisted, either by the Vaccinator or Data Entry Personnel at the point of care or after the vaccination has been administered, and the DDCC:VS has been digitally signed using PKI technology and created by the DDCC Generation Service, the record of the vaccination event is available in a digital format, as a DDCC:VS, to the DDCC:VS Holder at Point B.

Figure 3 Continuity of Care scenario¹

The vaccine is administered, the core data set is recorded on the DDCC paper certificate, and the record is then made available in digital form.



¹The business process symbols used in the workflows are explained in [Annex 2](#).

3.2.1. Continuity of Care use cases

Navigating through the workflow diagram shown in Fig. 3, there are three pathways for the Continuity of Care scenario, which are illustrated through the three workflow navigation paths in Fig. 4, Fig. 5 and Fig. 6. These three different pathways can be described as use cases, as outlined in Table 4.

Table 4
Continuity of Care use cases

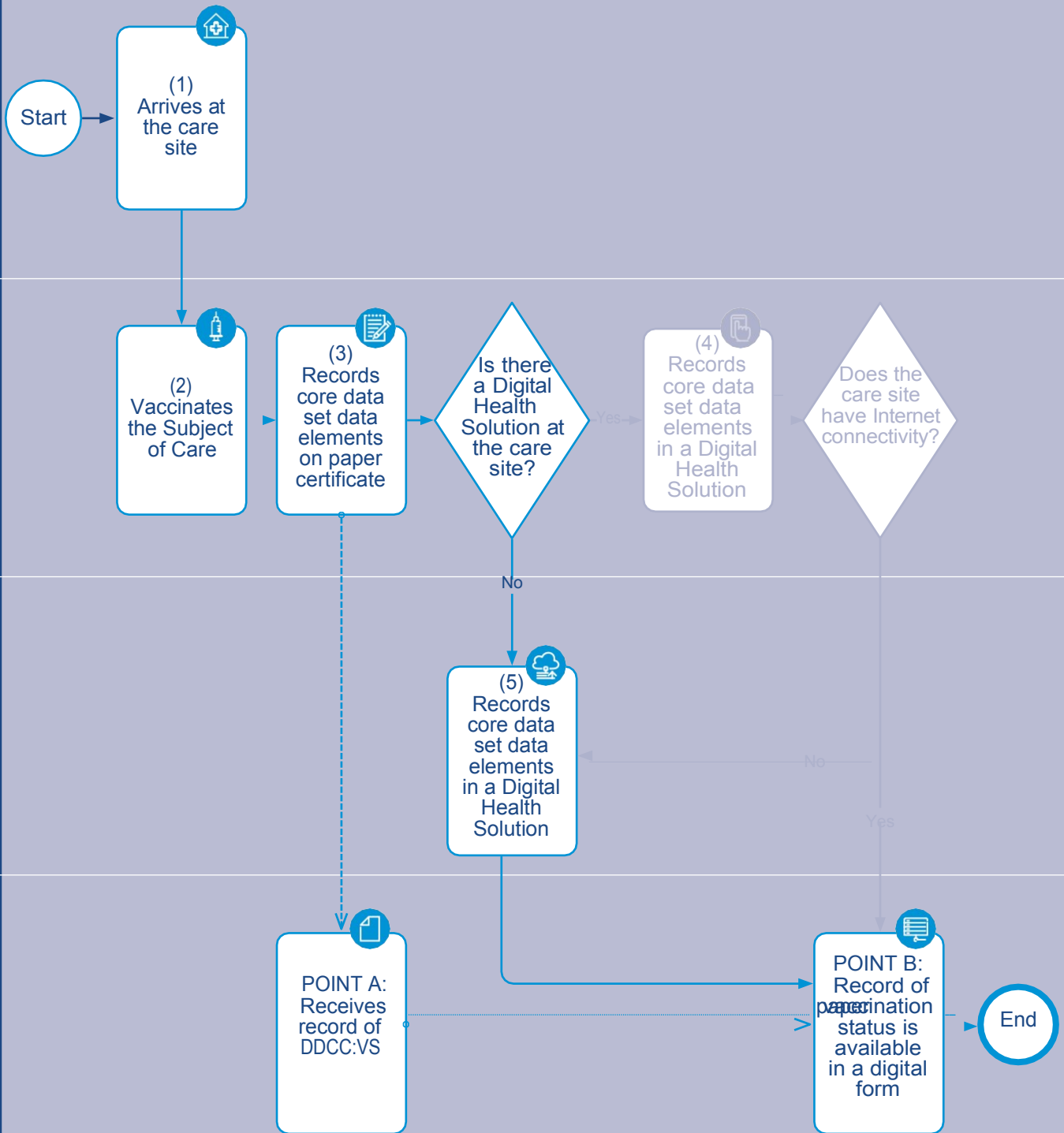
	Figure 4	Figure 5	Figure 6
	A guideline-based vaccine administration is recorded on paper. After the vaccination Digital event, data about it can be	A guideline-based vaccine administration is recorded using an offline secure Health Solution that updates with the content uploaded, subsequently, to an online Digital Health Solution.	A guideline-based vaccine administration is recorded using an online secure Digital Health Solution, the content in real time.
Solution.			
	Time delay until digital format is available.	Time delay until digital format is available.	No delay if digital system is available.
t	Vaccination event data are recorded in paper register and/or patient file.	Some steps are executed in the Digital Health Solution, rather than in the paper immunization register or patient file.	Some steps are executed in the Digital Health Solution rather than in the paper immunization register or patient file.
S	Relies on the HCID barcode being pre-printed on the card or pre-printed on a sticker to affix to the paper card.	HCID barcode must be pre-printed on the card or pre-printed on a sticker to affix to the paper card.	It is possible to print the HCID barcode on the DDCC:VS card at the time of the event.
r	Content other than the HCID barcode is expected to be handwritten.	If a printer is available, it is possible to print the core data set content onto the card; or else the content can be handwritten.	If a printer is available, it is possible to print the core data set content onto the card; or else the content can be handwritten.

DDCC:VS: Digital Documentation of COVID-19 Certificates: Vaccination Status; HCID: health certificate identifier; ID: identifier.

Figure 4

Continuity of Care scenario: Paper First use case (UC001)¹

The vaccine is administered, the core data set is recorded on the DDCC paper certificate, and the record is then made available in digital form.

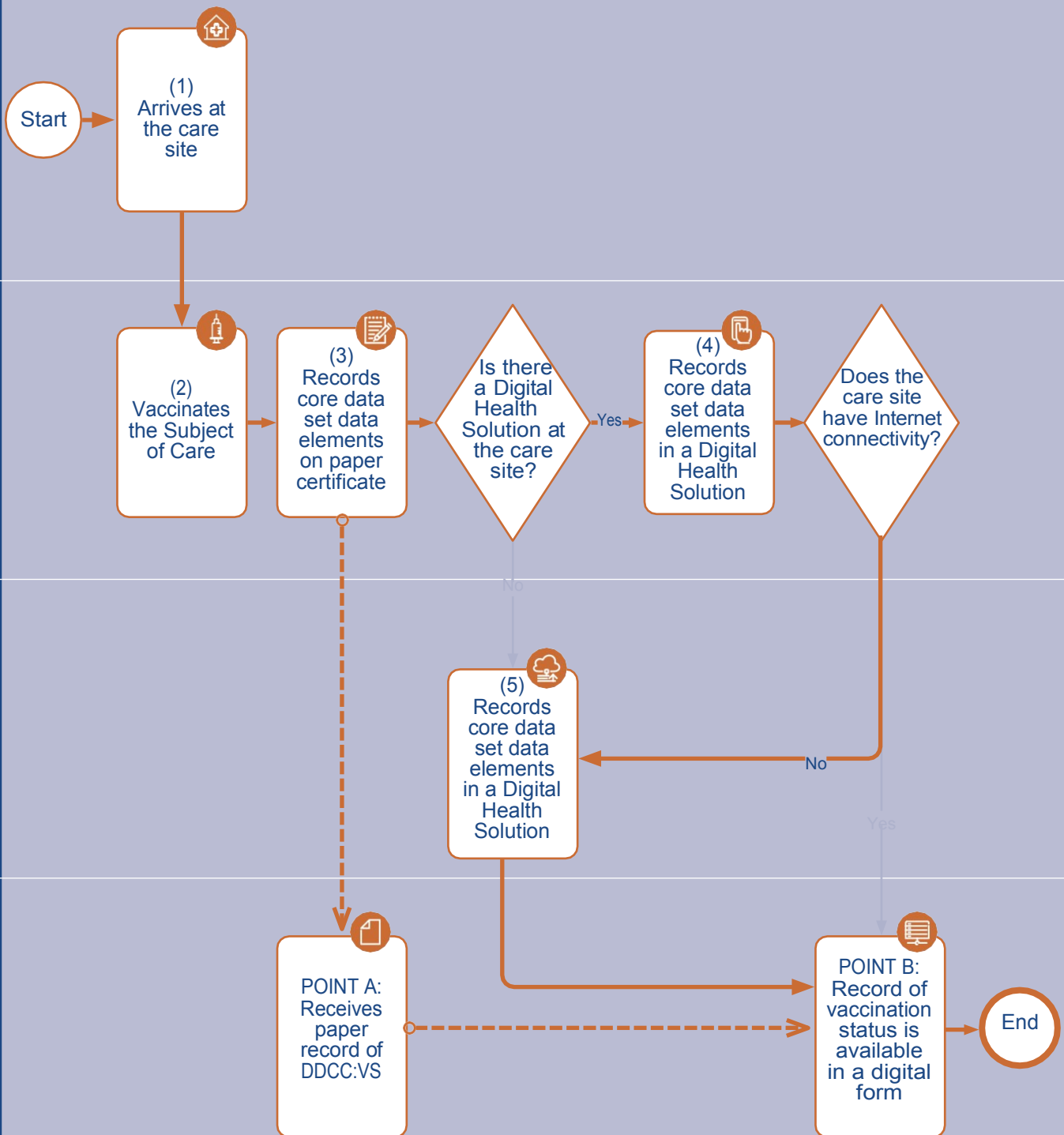


¹The business process symbols used in the workflows are explained in [Annex 2](#).

Figure 5

Continuity of Care scenario: Offline Digital use case (UC002)¹

The vaccine is administered, the core data set is recorded on the DDCC paper certificate, and the record is then made available in digital form.

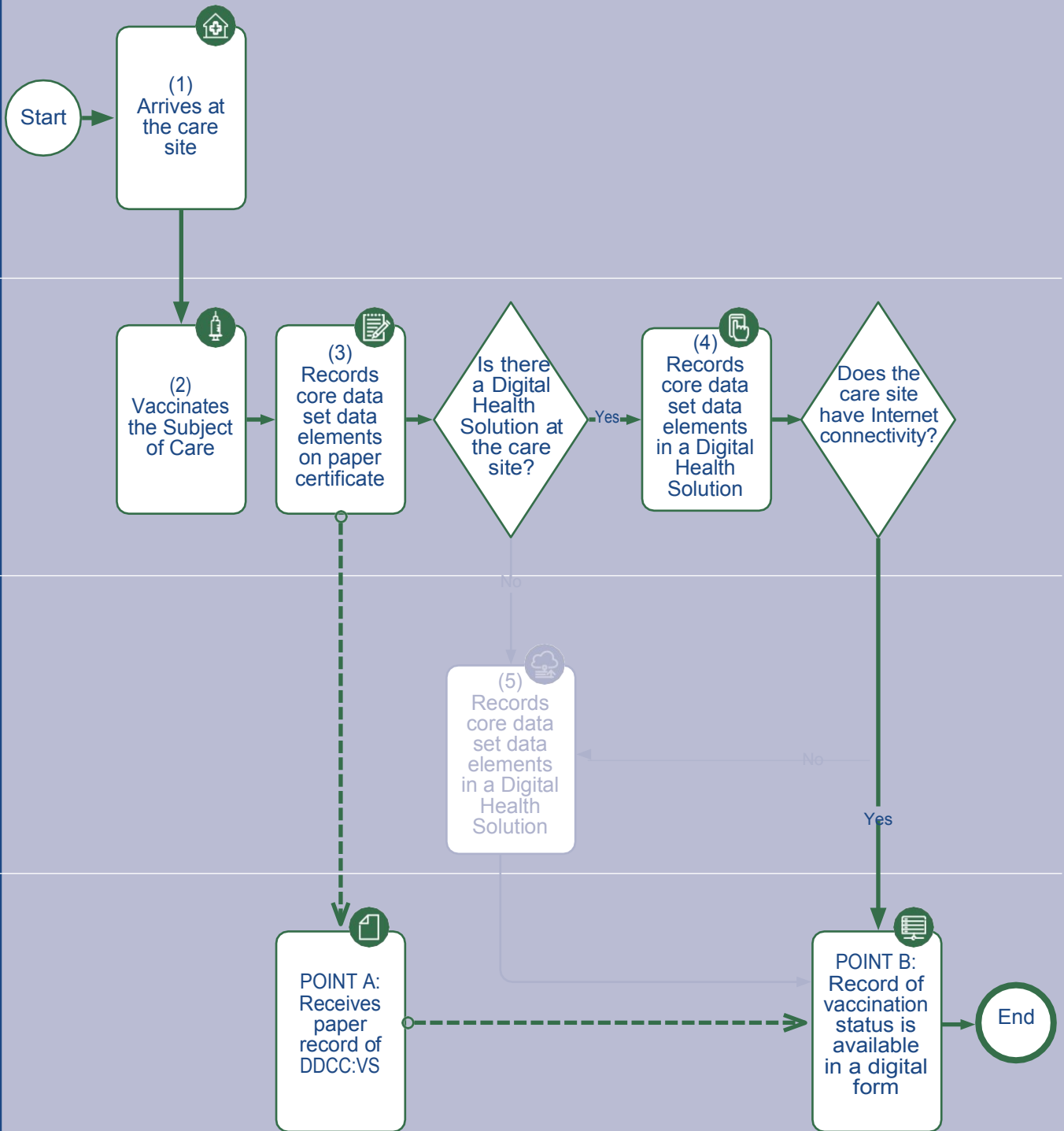


¹The business process symbols used in the workflows are explained in [Annex 2](#).

Figure 6

Continuity of Care scenario: Online Digital use case (UC003)¹

The vaccine is administered, the core data set is recorded on the DDCC paper certificate, and the record is then made available in digital form.



¹The business process symbols used in the workflows are explained in [Annex 2](#).

3.2.2. Operationalizing the Continuity of Care use cases

In order to operationalize the Continuity of Care use cases, as the specification is intended to be implementable, an HL7 FHIR implementation guide has been created (available at: <https://WorldHealthOrganization.github.io/ddcc>). HL7 FHIR is a free and open data exchange

standard that can be used to establish interoperability across systems. The implementation guide is to ensure that data for the DDCC:VS is captured in a consistent and interoperable way. The HL7

FHIR implementation guide for DDCC:VS contains a standards-compliant specification that explicitly encodes computer-interoperable logic, including data models, terminologies and logic expressions, in a computable language sufficient for implementation of the Continuity of Care use cases.

3.3. Functional requirements for Continuity of Care scenario

High-level functional requirements for the elements described in Fig. 3 are presented in Table 5 as suggested features that any digital solutions that would facilitate DDCC:VS issue or usage may have. These are written as guidance requirements only, to be used as a starting point for Member States or other interested parties who need to develop their own specifications for a DDCC:VS to take and adapt.

Non-functional requirements are applicable to both scenarios of use (Continuity of Care and Proof of Vaccination) and are included in *Annex 5*.

Table 5
Functional requirements for the Continuity of Care scenario¹

✓	✓	✓
✓	✓	✓
✓	✓	✓
✓	✓	✓
✓	✓	✓
✓	✓	✓
✓	✓	✓



Requirement ID	Functional requirement	UC001 Paper First	UC002 Offline Digital	UC003 Online Digital
DDCC.FXNREQ.007	It SHALL be possible for the Vaccinator to identify the Subject of Care as per the norms and policies of the PHA under whose authority the vaccination is administered.			
	It SHOULD be possible to verify the identity of the Subject of Care against existing records, if such a check is mandated by local procedures, and to retrieve any pertinent health history.			
	It SHALL be possible to register a new Subject of Care if the person is presenting for the first time.			
	It SHALL be possible to issue a new paper card to the Subject of Care for the purpose of recording the vaccination.			
	It SHALL be possible to update an existing paper card held by the Subject of Care if the card is presented during the vaccination and there is space available on the card.			
	Where paper cards are used, a PHA SHALL put in place a process to replace lost or damaged cards with the necessary supporting technology.			
	It SHALL be possible to associate a globally unique HCID with a paper vaccination card recording each			

SECTION 3

Continuity of Care scenario

Requirement ID	Functional requirement	UC001 Paper First	UC002 Offline Digital	UC003 Online Digital
	It SHALL be possible to enter or attach the HCID as a 1D barcode to any paper vaccination card issued to the Subject of Care (or the HCID card holder).	✓	✓	✓
	It SHOULD be possible to prepare pre-printed cards with a previously generated HCID that is encoded in (at minimum) a 1D barcode.	✓	✓	✓
	It SHALL be possible to record the core data set content on a paper vaccination card issued to the Subject of Care (or the DDCC:VS card holder).	✓	✓	✓
	It SHALL be possible to manually sign the paper card and include the official stamp of the administering centre as a non-digital means of certifying that the content has been recorded by an approved authority.	✓	✓	✓
	The data concerning the vaccination (at minimum, the HCID and the core data set content) SHOULD be entered into an electronic format as soon as reasonably possible after the vaccine is administered. This will most likely be into a Digital Health Solution, if one exists, at the point of care.	✓	✓	✓
	It SHALL be possible to retrieve information about the vaccination(s) administered to the Subject of Care from the content in the DDCC:VS.	✓	✓	✓
	All data concerning the vaccination SHALL be handled in a secure manner to respect confidentiality between the health worker and Subject of Care.	✓	✓	✓
	Digital technology SHALL NOT be needed for any aspect of paper card issue/update – the process SHALL function in an entirely offline and non-electronic manner.	✓		
	Paper cards and the validation markings they bear SHALL be designed to combat fraud and misuse.	✓	✓	✓
	Where an offline (disconnected) Digital Health Solution exists, the Data Entry Personnel SHALL securely log in to record all pertinent information about the vaccination.		✓	
	Any offline Digital Health Solution for vaccination registration SHALL include required content defined in the DDCC:VS core data set.		✓	
	Any offline Digital Health Solution for vaccination registration SHOULD be designed for quality data capture, including enforcement of data validation rules at the point of data entry.		✓	
	If patients' records are held in an offline Digital Health Solution available at the time of vaccination, then it SHOULD be possible for an authorized user to view the record for the Subject of Care, including pertinent medical history, per PHA policies.		✓	
	If an offline Digital Health Solution for vaccination registration is available, then it SHOULD be possible to search, list, filter, reorder and export the history of vaccinations administered.		✓	
	If an offline Digital Health Solution for vaccination registration is available, then it MAY be possible to schedule a regular, recurring export/dispatch of data, based on availability of a connection, to send them to another public health record system.		✓	
DDCC.FXNREQ.023	If an offline Digital Health Solution for vaccination registration is available, then it SHALL validate that HCIDs entered are confirmed to be unique, based on its own data set.		✓	

Requirement ID	Functional requirement	UC001 Paper First	UC002 Offline Digital	UC003 Online Digital
	If an offline Digital Health Solution for vaccination registration is available, then it MAY be responsible for outputting the vaccination data using the FHIR standard.		✓	
	If an offline Digital Health Solution for vaccine registration is available, and is part of the national PKI trust framework, and is authorized by the PHA to sign vaccination content as a DDCC:VS, then it SHALL register the DDCC:VS through the DDCC:VS Registry Service.		✓	
	For each care delivery session, the facility, organization and care delivery health worker context of the vaccine administration event SHALL be established.		✓	✓
	If an online/connected public health DDCC:VS Generation Service is available at the time of vaccination, then it SHALL be possible to register the vaccination as soon as possible after it is administered.			✓
	The DDCC:VS Generation Service involved in the vaccination SHALL ensure encryption of data, in transit and at rest, to provide end-to-end security of personal data.			✓
	The DDCC:VS Generation Service MAY be the agent responsible for issuing the HCID, provided that the HCID can be associated at the time of vaccination in a timely manner. If the DDCC:VS Generation Service is responsible for issuing HCsIDs, it SHALL only issue unique HCsIDs, i.e. the same HCID should never appear on two different paper vaccination cards.			✓
	If pre-generated HCsIDs and pre-printed vaccination cards are used, the generation of the HCsIDs, along with any supporting technology to ensure HCsIDs will not be duplicated within or across care sites, SHALL be managed by PHA policy.			✓
	It SHALL be possible for the DDCC:VS Generation Service to accept data from an authorized, connected point-of-care system, where such a system exists, i.e. to be able to accept data transferred from local data stores at sites where vaccinations are administered.			✓
	It SHALL be possible for the DDCC:VS Generation Service to represent vaccination data using the FHIR format.			✓
	It SHALL be possible for the DDCC:VS Generation Service to perform digital signing of vaccination data.			✓
	It MAY be possible for the solution to generate a machine- readable 2D barcode that, in addition to the HCID, contains further useful technical information, such as a web end-- point for validating the HCID, or a public key.			✓
	It MAY be possible for the DDCC:VS Generation Service to generate a 2D barcode that includes the unencrypted minimum core data set content (in FHIR standard) of the			✓

1D: one-dimensional; 2D: two-dimensional; DDCC: Digital Documentation of COVID-19 Certificates; DDCC:VS: Digital Documentation of COVID-19 Certificates: Vaccination Status; HCID: health certificate identifier; ID: identifier; PHA: public health authority.

¹ The use case(s) to which each functional requirement applies are indicated with a ✓.



This section describes the use cases and actors involved in using a DDCC:VS for Proof of Vaccination, as well as functional requirements for a digital solution. The Proof of Vaccination scenario relies on the PHA having access to a trusted means of digitally signing an HL7 FHIR document, which represents the core data set for the DDCC:VS. It will be up to Member States to define the purposes for which this scenario is applied and adapted to their own contexts and levels of digital maturity, in compliance with their legal and policy frameworks.

4.1. Key settings, personas and digital services

For the Proof of Vaccination scenario, there is one additional setting to consider: the **verification site**, where it is necessary for people to prove their COVID-19 vaccination status (such as a care site, a school, or an airport). How, when, where, and by whom the DDCC:VS can be verified should be defined by the Member State. The relevant policies, including data protection policies, should be put in place accordingly.

These key personas (see Table 6) are anticipated to interact with digital services (see Table 7). Not all of these digital services will have a user interface that the key personas directly interact with, but they are still critical building blocks of the reference architecture.

Table 6
Key personas for Proof of Vaccination

	In the context of Proof of Vaccination, the DDCC:VS Holder is the person who wants to assert a claim related to a COVID-19 vaccination status. This person could be the same as the Subject of Care or, for example, could be a caregiver who may hold the DDCC:VS for a child or other dependant.
	The person or entity that wants to verify the vaccination status claim, i.e. verify the vaccination status shown on a DDCC:VS.
	The entity that has overall responsibility for vaccinating the country's population. The National PHA is also responsible for the DDCC:VS Generation Service and the DDCC:VS Registry Service.
	Any external PHA to which the National PHA might defer to verify certificates not issued by the National PHA. This could be a PHA in another country, but it could also be any regional- level or international organization.

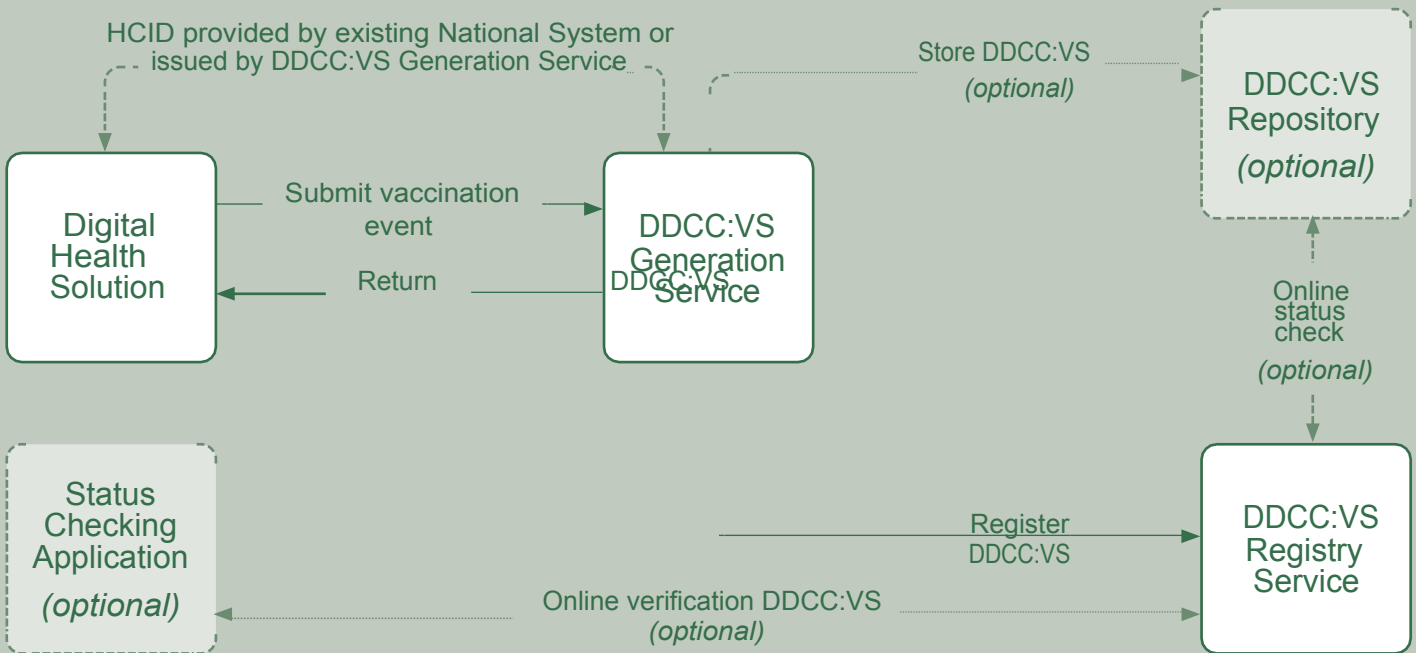
Table 7
Digital services for Proof of Vaccination

	HCID is the key identifier which is present in the DDCC:VS. The HCID may be provided by an existing national system or alternatively, it could also be issued directly by the DDCC:VS Generation Service which will then encode the ID in the DDCC:VS. An index that associates the HCID with metadata about the DDCC:VS is stored in the DDCC:VS Registry Service.
	A digital solution that can inspect and cryptographically verify the validity of the DDCC:VS. This can be an application on a mobile phone or another device.
	The service that is responsible for taking data about a vaccination event, converting that data to use the FHIR standard, signing that HL7 FHIR document, and returning it to the Digital Health Solution. The signed HL7 FHIR document is the DDCC:VS. The Digital Health Solution is in turn responsible for distributing the DDCC:VS and any associated representation of the data, such as a QR code, to the DDCC:VS Holder based on PHA policy.
	A service that is an index that is able to return metadata related to the DDCC:VS (the signed FHIR document), such as its signature. This metadata may include the location from which the DDCC:VS may be retrieved from the DDCC:VS Repository, if one exists. The DDCC:VS Registry Service can be utilized to determine whether a DDCC:VS has been revoked, for example, due to revocation of a key within the PKI, a compromised batch of vaccinations, or issues within the supply chain. It is important to note that a DDCC:VS Registry Service is not the same as an electronic immunization registry, which is commonly used for routine immunization programmes.
	The optional service that has a repository, or database, of all the DDCC:VS and which is able to return a copy of the DDCC:VS (the signed FHIR document) and potentially the one dimensional or two dimensional barcode representation (such as a QR code) of the signed FHIR document. This can be architected in a centralized or decentralized manner. Regardless, it is a mechanism that stores and persists the DDCC:VS information.

The digital services for Proof of Vaccination and the relationships between them are shown in Fig. 7.

Figure 7

The relationships between digital services for Proof of Vaccination



Note the use of the HCID throughout these services. As the unique identifier included in a DDCC:VS, it can be provided by an existing national system, generated at the point of care or issued by DDCC:VS Generation Service (as illustrated in Figure 7). Subsequent vaccinations may also be added to the digital record associated to the HCID. HCID can allow verifiers to search for, and retrieve a DDCC:VS for the purposes of verification.

4.2. Proof of Vaccination workflows and use cases

In order to sign a digital document, PKI technology is required. Each Member State would be responsible for managing its own PKI through its PHA or another national delegated authority. PKI is described in further detail in [section 6](#) and [Annex 4](#). This document assumes that a PKI has already been deployed or is available within a country to support the DDCC:VS workflows described in this section. This PKI supports the sharing of public keys that correspond to the private keys that have been used to cryptographically sign DDCC:VS and may support the sharing of public keys from trusted International PHAs so that signed DDCC:VS issued by these parties may be cryptographically verified.

The verification of a claim of vaccination is illustrated in Fig. 8. The workflow's actors and settings, and its related high-level requirements, may be described as follows.

1. A DDCC:VS Holder presents a DDCC:VS to a Verifier in support of a claim of vaccination status.
2. To verify the COVID-19 vaccination claim of a *verifiable* DDCC:VS Holder, there are four separate pathways (Manual Verification, Offline Cryptographic Verification, Online Status Check [national DDCC:VS] and Online Status Check [international DDCC:VS]) that a Verifier could take to check the COVID-19 vaccination claim at Point C, elaborated as Proof of Vaccination use cases in Table 8. A Verifier may visually verify a DDCC:VS, or scan a machine-readable version of the DDCC:VS's HCID and use that when accessing a verification service or verify using a digitally signed, machine-readable representation of the core data set content (e.g. as a 2D barcode).

Note that, regardless of the use case, a DDCC:VS Generation Service is **required**. The DDCC:VS Registry Service is also **required**. However, the DDCC:VS Repository Service is **optional** depending on which

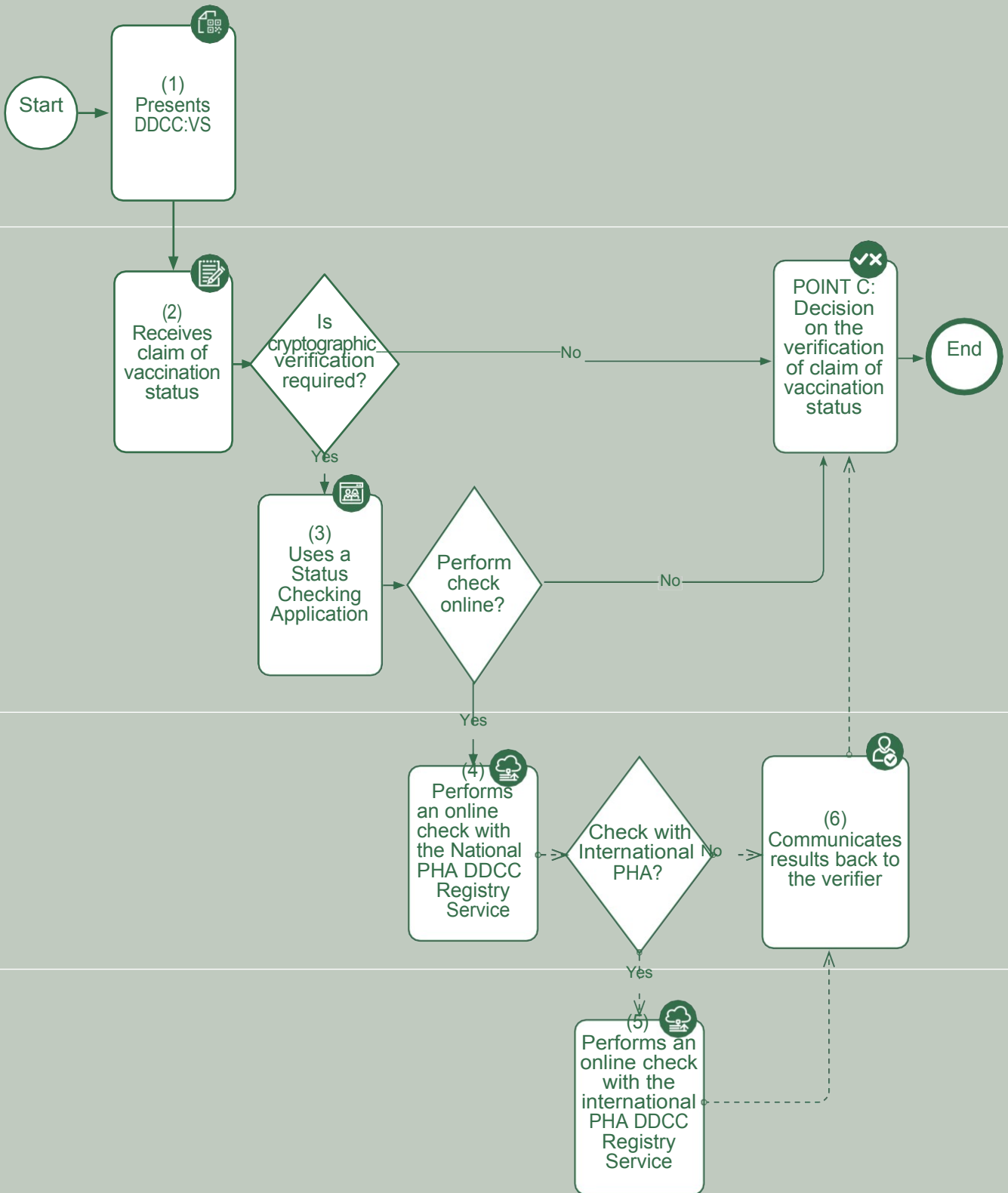
use case is being implemented, but it is **required** for the online verification use cases. See Table 7 for descriptions of the DDCC:VS services noted; the DDCC:VS Registry Service is not equivalent to a registry.

4.2.1. Proof of Vaccination use cases

Navigating through the workflow diagram shown in Fig. 8, there are four possible verification pathways (illustrated separately in Fig. 9, Fig. 10, Fig. 11 and Fig. 12), which are the use cases of the Proof of Vaccination scenario listed in Table 8.

Figure 8
Proof of Vaccination scenario¹

Verification of a claim of vaccination



DDCC:VS: Digital Documentation of COVID-19 Certificates: Vaccination Status; PHA: public health authority.

¹The business process symbols used in the workflows are explained in *Annex 2*.

Table 8
Proof of Vaccination use cases

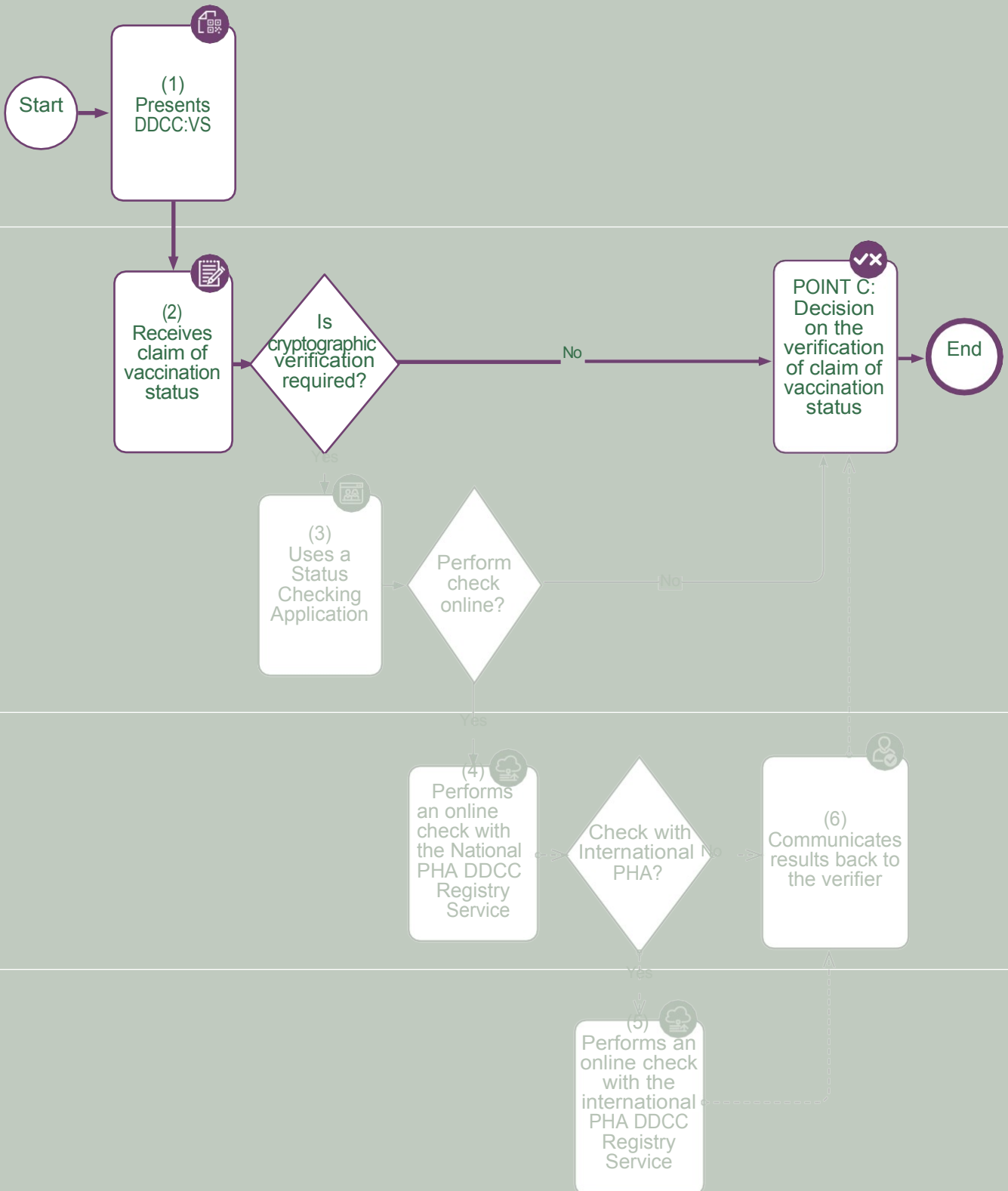
	A Verifier verifies a DDCC:VS using a purely visual means, based on his or her subjective judgement, as is currently done with International Vaccination or Prophylaxis. This type of check is currently well access accepted, is quick and easy to do, and requires no digital technology.	A Verifier verifies a DDCC:VS using digital cryptographic processes in an offline mode.	This pathway is used when the DDCC:VS is being verified in the same jurisdiction as it was issued. A Verifier verifies a DDCC:VS using digital cryptographic processes in an online mode that includes a status check against the PHA's DDCC:VS Registry Service and, optionally, the DDCC:VS Repository.
	Offline	Offline	Online
	→ Verification is visually performed by the Verifier. As judgement can be subjective, it relies on policies to protect against discrimination. DDCC:VS card matches the DDCC:VS	→ Can confirm that the HCID barcode on the paper card is valid and has not been altered. → Can confirm whether DDCC:VS has been issued by an authorized PHA. → Can confirm that the hash of any signed 2D barcodes matches therein.	→ Can confirm that the HCID barcode on the paper card is valid and has not been altered. → Can confirm whether the DDCC:VS has been issued by an authorized PHA. → If authorized to do so, can confirm that the content on a paper card matches the DDCC:VS digital content. → Can check whether signed 2D barcodes containing DDCC:VS content have been revoked or updated.
	→ Can confirm that the HCID barcode on the paper card is valid and has not been altered. → Can confirm whether the DDCC:VS has been issued by an authorized PHA. → If authorized to do so, can confirm that the content on a digital content. → Can confirm that the hash of any signed 2D barcodes content represented therein. → Can check whether signed 2D barcodes containing DDCC:VS content have been revoked or updated.		
	Not possible	Possible if a cache of revoked certificates is maintained by the Verifier	Possible
	Not required	Required	Required
	Optional	Optional	Required

DDCC:VS: Digital Documentation of COVID-19 Certificates: Vaccination Status; HCID: health certificate identifier; ID: identifier; PHA: public health authority.

Figure 9

Proof of Vaccination scenario: Manual Verification use case (UC004)¹

Verification of a claim of vaccination



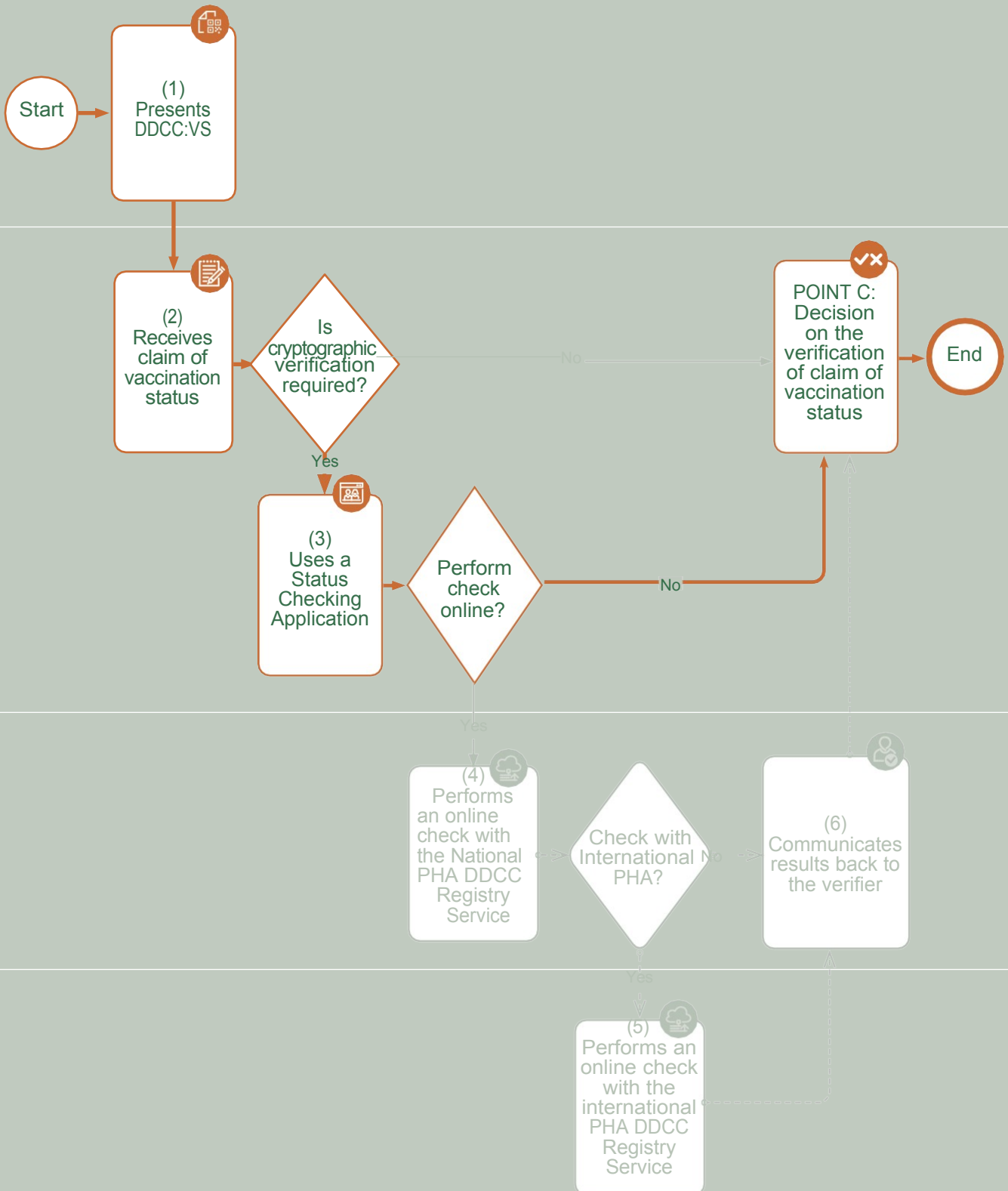
DDCC:VS: Digital Documentation of COVID-19 Certificates: Vaccination Status; PHA: public health authority.

¹The business process symbols used in the workflows are explained in *Annex 2*.

Figure 10

Proof of Vaccination scenario: Offline Cryptographic Verification use case (UC005)¹

Verification of a claim of vaccination



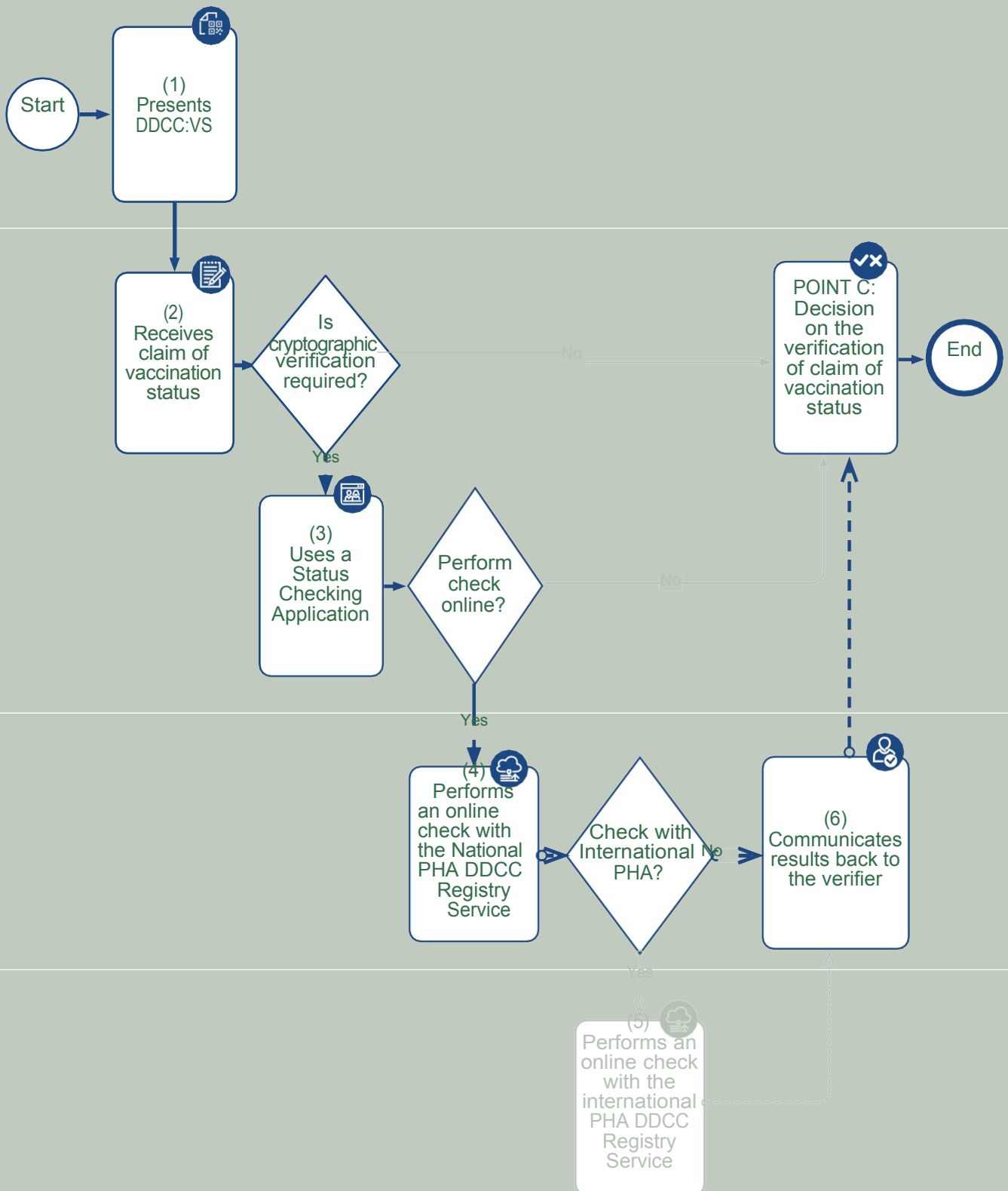
DDCC:VS: Digital Documentation of COVID-19 Certificates: Vaccination Status; PHA: public health authority.

¹The business process symbols used in the workflows are explained in [Annex 2](#).

Figure 11

Proof of Vaccination scenario: Online Status Check (National DDCC:VS) use case (UC006)¹

Verification of a claim of vaccination



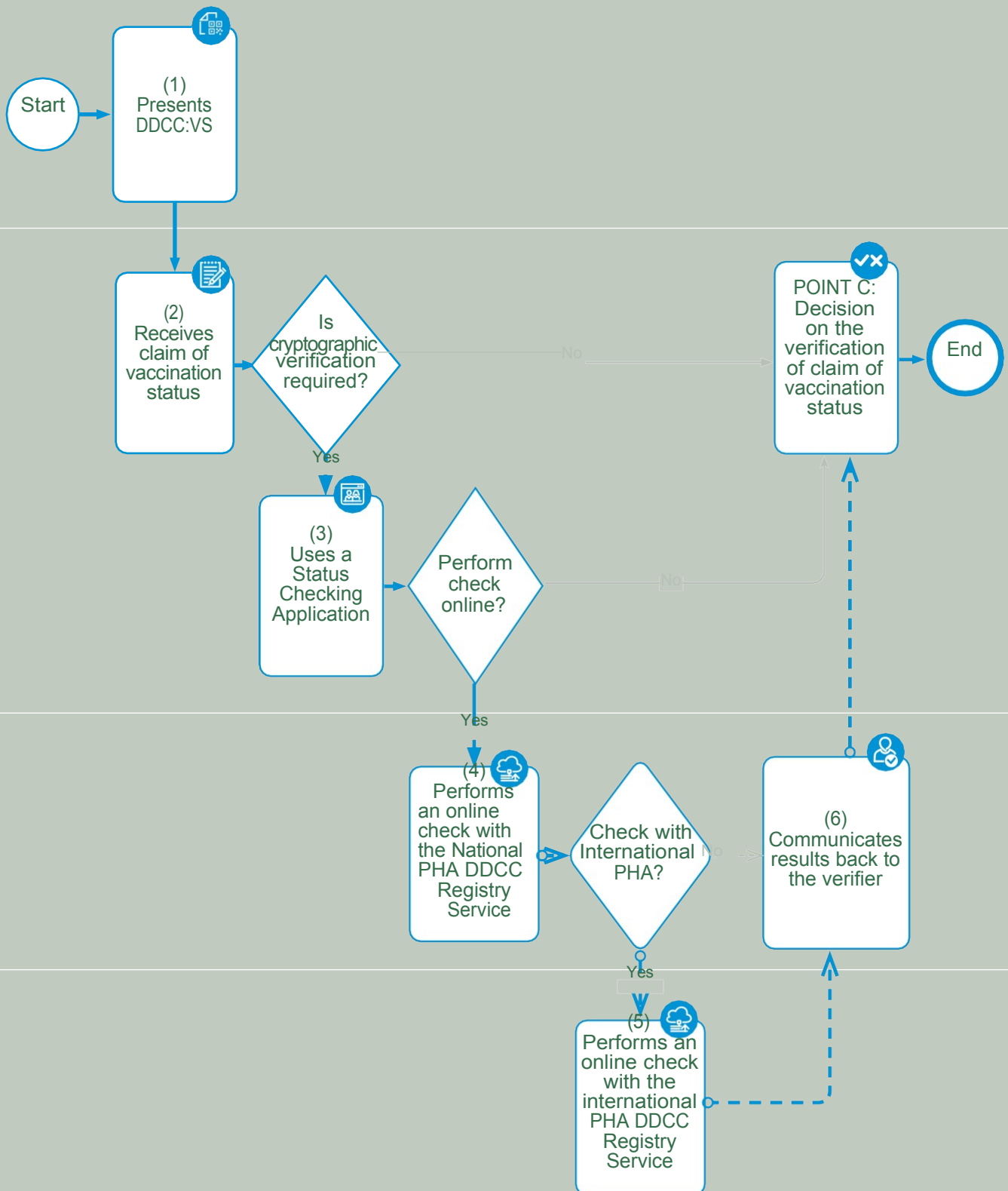
DDCC:VS: Digital Documentation of COVID-19 Certificates: Vaccination Status; PHA: public health authority.

¹The business process symbols used in the workflows are explained in *Annex 2*.

Figure 12

Proof of Vaccination scenario: Online Status Check (International DDCC:VS) use case (UC007)¹

Verification of a claim of vaccination



DDCC:VS: Digital Documentation of COVID-19 Certificates: Vaccination Status; PHA: public health authority.

¹The business process symbols used in the workflows are explained in *Annex 2*.

4.2.2. Operationalizing the Proof of Vaccination use cases

Similar to supporting operationalization of the Continuity of Care use cases, the FHIR implementation guide includes implementable specifications for the Proof of Vaccination use cases described in this document, (available at <https://WorldHealthOrganization.github.io/ddcc>). The FHIR implementation guide for DDCC:VS contains a standards-compliant specification that explicitly encodes computer- interoperable logic, including data models, terminologies and logic expressions, in a computable language sufficient for implementation of Proof of Vaccination use cases.

4.3. Functional requirements for Proof of Vaccination scenario

High-level functional requirements for the activities described in Fig. 8 are presented in Table 9 as suggested features that any digital solutions that would facilitate DDCC:VS verification may have. These are written as guidance requirements only to be used as a starting point for Member States or other interested parties that need to develop their own specifications for a digital solution for DDCC:VS to take and adapt.

Given non-functional requirements are common to both scenarios (Continuity of Care and Proof of Vaccination) (see [Annex 5](#)).

Table 9

Functional requirements for the Proof of Vaccination scenario¹

Requirement ID	Functional requirement	UC004 Manual	UC005 Offline	UC006 National	UC007 International
	Paper cards and the validation markings they bear SHOULD be designed to combat fraud and misuse. Any process that generates a paper vaccination card SHALL include elements on the card that support the Verifier in visually checking that the card is genuine (e.g. water marks, holographic seals etc.) without the use of any digital technology.	✓	✓	✓	✓
	Paper vaccination cards SHALL display an HCID.	✓	✓	✓	✓
	Where paper cards are used, an authority SHALL put in place a process for the replacement of lost or damaged cards with the necessary supporting technology.	✓	✓	✓	✓
	If a paper vaccination card or electronic vaccination document bearing a 1D or 2D barcode is presented to a Verifier, then it SHALL be possible for the Verifier to scan the code and, as a minimum, read the HCID encoded in the barcode, to visually compare it with the HCID written on the paper card, if present.		✓	✓	

Requirement ID	Functional requirement	UC004 Manual	UC005 Offline	UC006 National	UC007 International	
DDCC.FXNREQ.049	If a paper vaccination card or electronic vaccination document bears a QR code and that 2D barcode includes a digital signature, then it MAY be possible for the Verifier to check the signature, using information downloaded from a DDCC:VS Registry Service, to ensure it is genuine.			✓	✓	
	It MAY be possible to log all offline verification operations so that, at a later stage, when an online connection is available, verification decisions can be reviewed and reconfirmed against data provided by the online DDCC:VS Registry Service. For example, this may be done to confirm that a certificate checked offline in the morning using public key and revocation data downloaded from the DDCC:VS Registry Service the day before has not been added to a public key revocation list issued that same day.		✓			
	It SHALL always be possible to perform some form of offline verification of vaccination cards; any solution should be designed so that a loss of connectivity to online components of the solution cannot force the verification work to stop.		✓	✓	✓	
	If, at the time of verification, a Verifier has online access/connectivity to a DDCC:VS Registry Service managed by a National PHA, then it SHALL be possible to query whether the HCID present in the barcode (and the public key, if also present) of the paper vaccination card are currently valid.				✓	✓
	When making the verification check, any solution SHALL send only the minimum information required for the verification to complete. The minimum information comprises the metadata (see section 5.2) and signature of the DDCC:VS.				✓	✓
	When receiving a request for validation, a National PHA SHALL consult its DDCC:VS Registry Service and respond with a status to indicate that the signing key has not been revoked, that the key was issued by a certified authority, and that the DDCC has not otherwise been revoked.				✓	✓
	A PHA servicing a validation request MAY respond with basic details of the vaccination card holder (name, date of birth, sex, etc.), in accordance with PHA policies, so the Verifier can confirm that the vaccination card corresponds to the DDCC:VS Holder who has presented himself or herself for validation.				✓	✓
	A PHA SHALL maintain a PKI to underpin the signing and verification process. Lists of valid public keys and revocation lists will be held in such a system and be linked to the DDCC:VS Generation Service to associate public keys with HCIDs.				✓	✓
	A PHA MAY log the requests it receives for verification (even if rendered anonymous), so that it has a searchable history for the purposes of audit and fighting fraud, provided				✓	✓

	that such logging respects data protection principles.				
--	--	--	--	--	--

SECTION 4

Proof of Vaccination scenario

Requirement ID	Functional requirement	UC004 Manual	UC005 Offline	UC006 National	UC007 International
DDCC.FXNREQ.061	A PHA SHALL be able to return a verification status, as defined by the implementer, to a requester, based on the information provided.			✓	✓
	A PHA MAY be able to service individual verification requests (i.e. details relating to one vaccination certificate) or requests sent in bulk (details of multiple certificates sent in one request).			✓	✓
	A PHA SHOULD be able to validate that the requestor making a verification request is an authorized agent, but MAY also allow anonymous verification requests.			✓	✓
	The certificate authority (or authorities) in each country SHALL maintain records of the DSCs issued for the purpose of signing vaccination certificates and expose any service(s) that allow a public key to be looked up and checked against its records to check for validity.			✓	✓
	Any communication between a Verifier and a DDCC:VS Registry Service or other data service managed by a PHA SHALL be secured to prevent interference with the data in transit and at rest.			✓	✓
	SMS-based verification of alphanumeric HCIDs MAY be provided by a PHA as a means of sending a verification request or receiving a response with a status code.			✓	
	If a verification request is made in country A for a certificate that was issued by country B or a supranational entity, then country A's PHA SHOULD have a means of transferring the request/ querying the data held by that authority.				✓
	A Member State SHOULD put in place bilateral or multilateral agreements with other countries or with a supranational entity or regional body for access to those entities' vaccination certificate data and digital signatures.				✓
	Communications between one country's and another's PHA or a supranational DDCC:VS Registry Service SHALL be secure and prevent interference with the data in transit and at rest.				✓
	It SHALL be the ultimate responsibility of the country where verification is taking place to decide whether a vaccination claim is valid or not.				✓
There SHOULD be a mechanism for country A to notify country B if a suspected fraudulent					

1D: one-dimensional; 2D: two-dimensional; DDCC: Digital Documentation of COVID-19 Certificates; DDCC:VS: Digital Documentation of COVID-19 Certificates: Vaccination Status; DSC: document signer certificate; HCID: health certificate identifier; ID: identifier; PHA: public health authority.

¹ The use case(s) to which each functional requirement applies are indicated with a ✓.

SECTION

5

DDCC:VS core data set



The DDCC:VS core data set includes data elements about the Subject of Care and vaccine administration events that are required for the two core scenarios of Continuity of Care and Proof of Vaccination. Stakeholders and systems may use the DDCC:VS core data set as defined, or they may continue to use their existing terminology with a map to the DDCC:VS core data set, so long as it contains the required data elements in the DDCC:VS core data set. The recommended core data set is intended to include the critical data required for interoperability, specific to the scenarios of use defined and driven by the public health need. A comprehensive data dictionary in spreadsheet format can be found in Web Annex A.

5.1. Core data set principles

To develop the core data set, data requirements under the International Health Regulations (15), WHO home-based records guidance (13), WHO adverse events following immunization (AEFI) reporting requirements (26) and WHO immunization programme monitoring guidance are considered (12). The core data set has been further informed by analysis of existing digital vaccination certificates deployed in some countries and by pre-existing standards for digital vaccination certificates.

The following key principles were used to guide the formulation of the core data set.

- **DATA MINIMIZATION.** Aligned with the principle of data privacy protection, only the minimum set of data elements necessary for documenting a vaccination event for the purposes of a DDCC:VS should be included. Each data element must have a purpose in accordance with the predefined use cases. This is especially important for personal data.
- **OPEN STANDARDS.** Aligned with the principle of open access, proprietary terminology code systems or proprietary standards cannot be recommended to Member States.
- **IMPLEMENTABLE ON DIGITAL AND PAPER.** Aligned with the principle of equity, data requirements should not increase inequities or put individuals at risk. Additionally, data input requirements should be feasible on paper but take advantage of the benefits of digital

technology.

→ **NOT ALL DATA ELEMENTS NEED TO BE IN THE VACCINATION CERTIFICATE.** Aligned with the principle of capability, flexibility and sustainability, the vaccination certificate is intended to be part of a much larger ecosystem of immunization information systems which include:

- » EIRs (such as OpenSRP [27]);
- » reporting systems for vaccine coverage monitoring (such as District Health Information Software 2; DHIS2 [28]); and
- » AEFI reporting systems (such as Vigiflow [29]).

To underscore the importance of the ability to implement, the data content model for the DDCC:VS core data set has been developed as an HL7 FHIR implementation guide. The [DDCC vaccination certificate implementation guide](#)¹ is based on the widely adopted HL7 FHIR International Patient Summary (IPS) health data content model (30).

International Classification of Diseases (ICD) is the preferred data standard for DDCC:VS. The 11th revision of ICD (ICD-11) (31), which comes into effect for recording and reporting in January 2022, is recommended as the most suitable and future-proof value set for use in the DDCC:VS data dictionary. ICD-11 is:

- a global public good that is completely free and available for all to use in its entirety; no payment will be required to access any additional parts of the code system;
- kept clinically updated through an open, public and transparent maintenance process;
- able to provide comprehensive content coverage and the granularity required for data fields in individual-level systems, including the DDCC:VS;
- easy to integrate into software systems via a public API for use in all settings, without additional tooling; this is due to ICD-11's digital and multilingual structure; and
- human-readable and machine-readable.

For countries with legacy ICD systems (e.g. the 10th revision of ICD, ICD-10), WHO will provide ICD-10- based value sets for use in the DDCC:VS data dictionary, as well as mappings to other freely available classifications and terminologies (e.g. Anatomical Therapeutic Chemical [ATC], SNOMED CT GPS [32], etc.). For guiding principles of the WHO Family of International Classifications (WHO-FIC) and other classifications, and terminology mapping in the context of the WHO DDCC:VS, see [Annex 3](#).

¹ The DDCC implementation guide can be found here: <https://worldhealthorganization.github.io/ddcc/>

5.2. Core data elements

The three key sections of the core data set are:

1. the header
2. data elements for each vaccination event
3. vaccination certificate metadata.

The **header** section data elements include the Subject of Care's ID information (see Table 10). The header section is intended to capture information about the vaccinated individual to allow for information on the vaccination event to be linked to a specific person. This data should remain the same regardless of which vaccination a person has received; thus, it should only be collected once.

Table 10
Header section of the DDCC:VS with preferred code system

	The full name of the vaccinated person.	String	Not applicable	
	The vaccinated person's date of birth (DOB), if known. If unknown, use assigned DOB for administrative purposes.	Date	Complete date, following ISO 8601 (YYYYMMDD or YYYY-MM-DD)	
	Unique ID for the vaccinated person, according to the policies applicable to each country. There can be more than one unique ID used to link records (e.g. national ID, health ID, immunization information system ID, medical record ID).	ID	Not applicable	
	Documentation of a specific instance of sex information for the vaccinated person.	Coding ¹	As defined by Member State	

ID: identifier; ISO: International Organization for Standardization.

¹Coding data elements are multiple choice and the input options, or values, are data elements taken from a set of predefined options (e.g. sex, vaccine or prophylaxis, vaccine brand).

The **data elements for each vaccination event** section outlines data that need to have been collected for each vaccination the vaccinated person received (see Table 11). For each dose, all the data elements in Table 11 are required to have been recorded. In paper form, this is equivalent to a separate row on a vaccination certificate that is then repeated for each vaccination received.

Table 11
Data for each vaccination event, with preferred code system

Generic description of the vaccine or vaccine sub-type (e.g. COVID-19 mRNA vaccine, HPV vaccine).	Coding	ICD-11	
The brand or trade name used to refer to the vaccine received.	Coding	As defined by Member State	
Name of the manufacturer of the vaccine received (e.g. Serum Institute of India, AstraZeneca). If vaccine manufacturer is unknown, market authorization holder is REQUIRED.	Coding	As defined by Member State	
Name of the market authorization holder of the vaccine received. If market authorization holder is unknown, vaccine manufacturer is REQUIRED.	Coding	As defined by Member State	
Batch number or lot number of the vaccine.	String	Not applicable	
Date on which the vaccine was provided.	Date	Complete date, following ISO 8601	
Date upon which provided vaccination is considered valid This data should only be considered valid at the time of issuance, as guidance is likely to evolve with further scientific evidence. Any user of this data (Vaccinator, Verifier) should validate this date according to their national policy. In the case of repeated doses, the data field for a subsequent dose should override the data field for a predecessor dose.	Date	Complete date, following ISO 8601	
Vaccine dose number.	Quantity	Not applicable	

Total expected doses as defined by Member State care plan and immunization programme policies.	Quantity	Not applicable	
The country in which the individual has been vaccinated.	Coding	ISO 3166-1 alpha-3 (numeric)	
The name or ID of the vaccination facility responsible for providing the vaccination.	String	As defined by Member State	
The health worker who provided the vaccination or the supervising clinician's handwritten signature. REQUIRED for PAPER vaccination certificates that have been filled out with handwriting ONLY. A printed paper vaccination certificate does not require the handwritten signature of a health worker.	Signature	Not applicable	
OPTIONAL for DIGITAL and PAPER vaccination certificates. The unique ID for the health worker as determined by the Member State. There can be more than one unique ID used (e.g. system-generated ID, health profession number, cryptographic signature, or any other form of unique ID for a health worker). This can be used in lieu of a paper-based signature.	ID	Not applicable	
Name of disease that vaccine given to protect against (such as COVID-19).	Coding	ICD-11	
Date on which the next vaccination should be administered, if a second dose is required.	Date	Complete date, following ISO 8601	

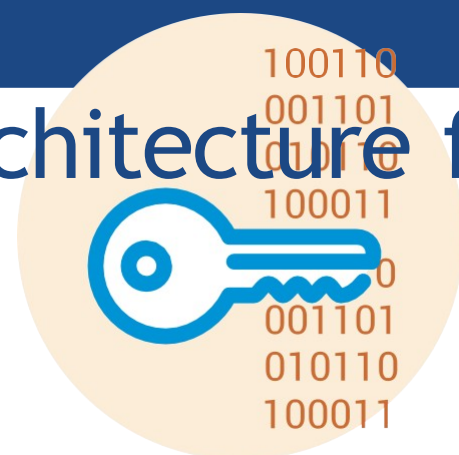
HPV: human papilloma virus; ICD-11: International Classification of Diseases 11th Revision; ID: identifier; ISO: International Organization for Standardization; mRNA: messenger ribonucleic acid.

The **vaccination certificate metadata** contain data elements that are not typically visible to the user, but that are required to be linked to the certificate itself (see Table 12). It is anticipated that additional metadata elements will be added by Member States at the time of certificate generation to support specific use case implementations.

Table 12
Vaccination certificate metadata

The authority or authorized organization that issued the vaccination certificate.	String	Not applicable
Unique ID used to associate the vaccination status represented in a paper vaccination card to its digital representation(s).	ID	Not applicable
Date in which the certificate for a vaccination event became valid. No health or clinical inferences should be made from this date.	Date	Complete date, following ISO 8601
Last date in which the certificate for a vaccination event is valid. No health or clinical inferences should be made from this date.	Date	Complete date, following ISO 8601
Version of the core data set and HL7 FHIR implementation guide that the certificate is using.	String	Not applicable

FHIR: Fast Healthcare Interoperability Resources; HL7: Health Level Seven; ID: identifier; ISO: International Organization for Standardization.

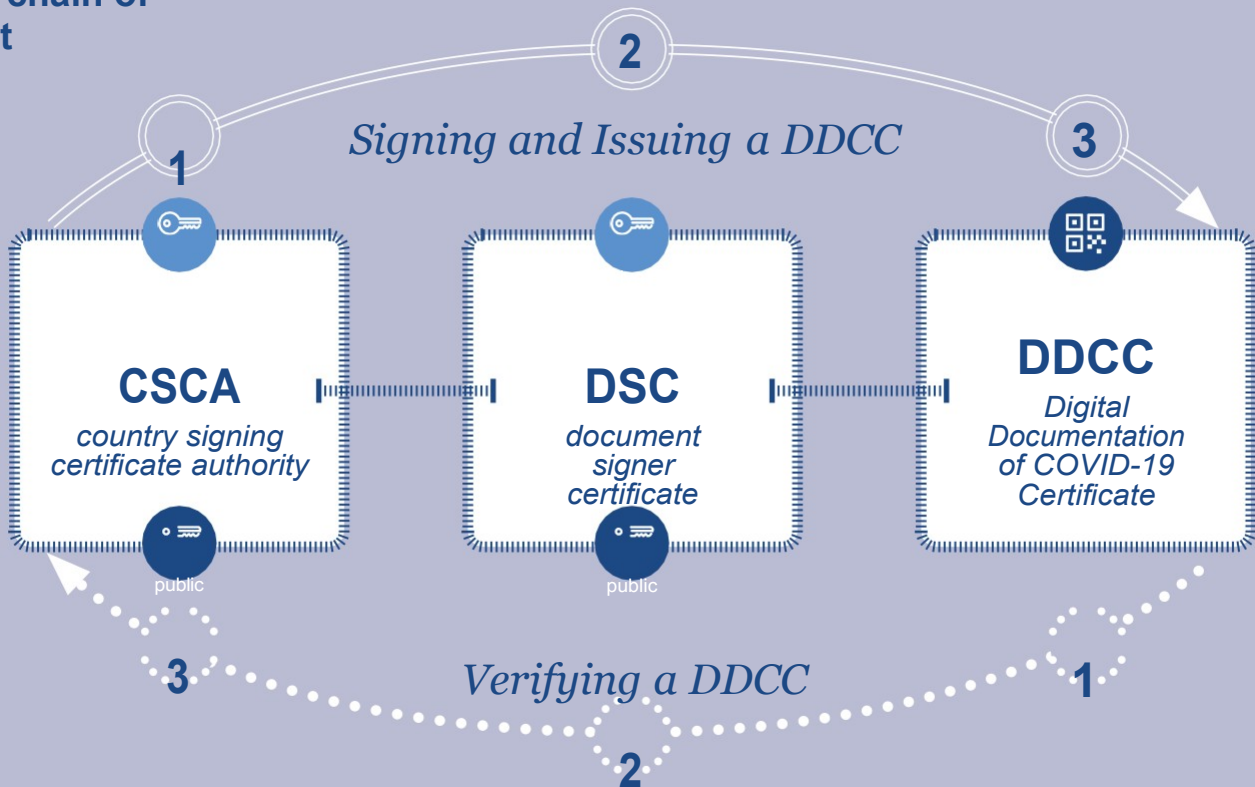


The scenarios presented in earlier chapters, and the data associated with them, suggest the need for a digital ecosystem within a country for the issuance, updating and verification of the DDCC:VS. This ecosystem would comprise a suite of digital tools for the management of DDCC:VS data and the processes and governance rules for using these systems. It could be as simple as a server for storing and managing the data or as extensive as an entire health information exchange infrastructure.

In [Annex 6](#), considerations for such a national architecture of digital components are presented as a generic design for a set of interconnected components that would facilitate the successful operation of a national DDCC:VS system. Member States are at different levels of digital health maturity and investment, and have different local contexts. The architecture is presented as general guidance with the expectation that this guidance will be adapted and tailored to suit the specific real-world needs of each Member State.

In order to sign a digital document, PKI technology is required. PKI uses private and public key pairs to operationalize digital signing and cryptographic verification. Content that is signed by a private key can be verified by the corresponding public key of the key pair. This sign–verify mechanism is leveraged to establish the trust framework (chain of trust; see Fig. 13). There are many different mechanisms/technologies to implement this approach. PKI is described in further detail in [Annex 4](#).

Figure 13

The chain of trust

Member States will need to establish or utilize a domestic PKI that can be leveraged to issue and to verify DDCC:VS. An existing PKI framework may be used, provided it meets the requirements outlined in this document. This document assumes that a PKI has already been deployed or is available within a country to support the DDCC:VS workflows described in [sections 3](#) and [4](#). The PKI can be maintained and managed by another government entity (e.g. ministry of ICT, ministry of interior, ministry of foreign affairs) or by a contractor that the PHA has selected. Regardless, PHAs will have the signing authority. The two key steps for establishing a PKI framework are:

1. The **PHA** will need to generate at least one **document signer certificate (DSC)** – a private–public key pair that can be used by the trusted agents of the PHA to sign the DDCC:VS.
2. The **Member State** will need to establish a mechanism to assert that a DSC from a PHA has been authorized to sign health documents. Two approaches are outlined in [section 7](#).

There are many ways in which a PKI can be implemented. An example implementation of digital signing is provided in the implementation guide available at:

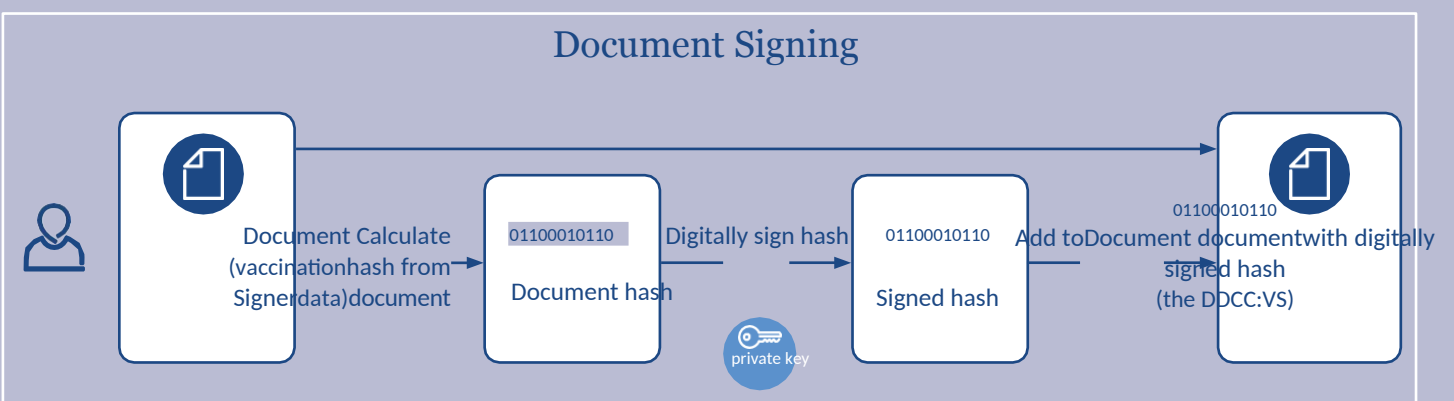
<https://WorldHealthOrganization.github.io/ddcc>. The precise algorithms used for the implementation – for example, for hashing and for signature generation – are at the discretion of the Member State.

6.1. Signing a DDCC:VS

The process of signing a DDCC:VS is shown in the top row of Fig. 13 and involves three steps.

1. The PHA generates a private and public key pair that serve as the “root certificate”. The private key is kept highly secure (never revealed to another party, maintained in a disconnected location, stored on media that is itself password-protected, etc.); the public key will be widely disseminated.
2. The PHA generates one or more DSC key pairs. DSC private keys are kept highly secure, and public keys are widely disseminated. The DSC key pair is digitally signed by the root certificate’s private key.
3. A DDCC:VS is digitally signed using the DSC’s private key. A barcode representation (e.g. QR code) of the signed content can be generated if required. The process of signing is illustrated in Fig. 14 and works as follows.
 - a. A human-readable plain text description of the vaccination data is transformed into a non-human-readable “document hash” using a hashing algorithm, which is a mathematical function that performs a one-way transformation of data of any size to data of a fixed size in a manner that is impossible to unambiguously reverse.
 - b. The DSC’s private key is used to sign the hash in a process in which the digital information of the private key further transforms the digital hash to produce a “signed hash”.
 - c. This signed hash now effectively contains information about the private key and the data contained on the DDCC:VS in a non-human-readable and cryptographically secure format.

Figure 14
How digital signatures work



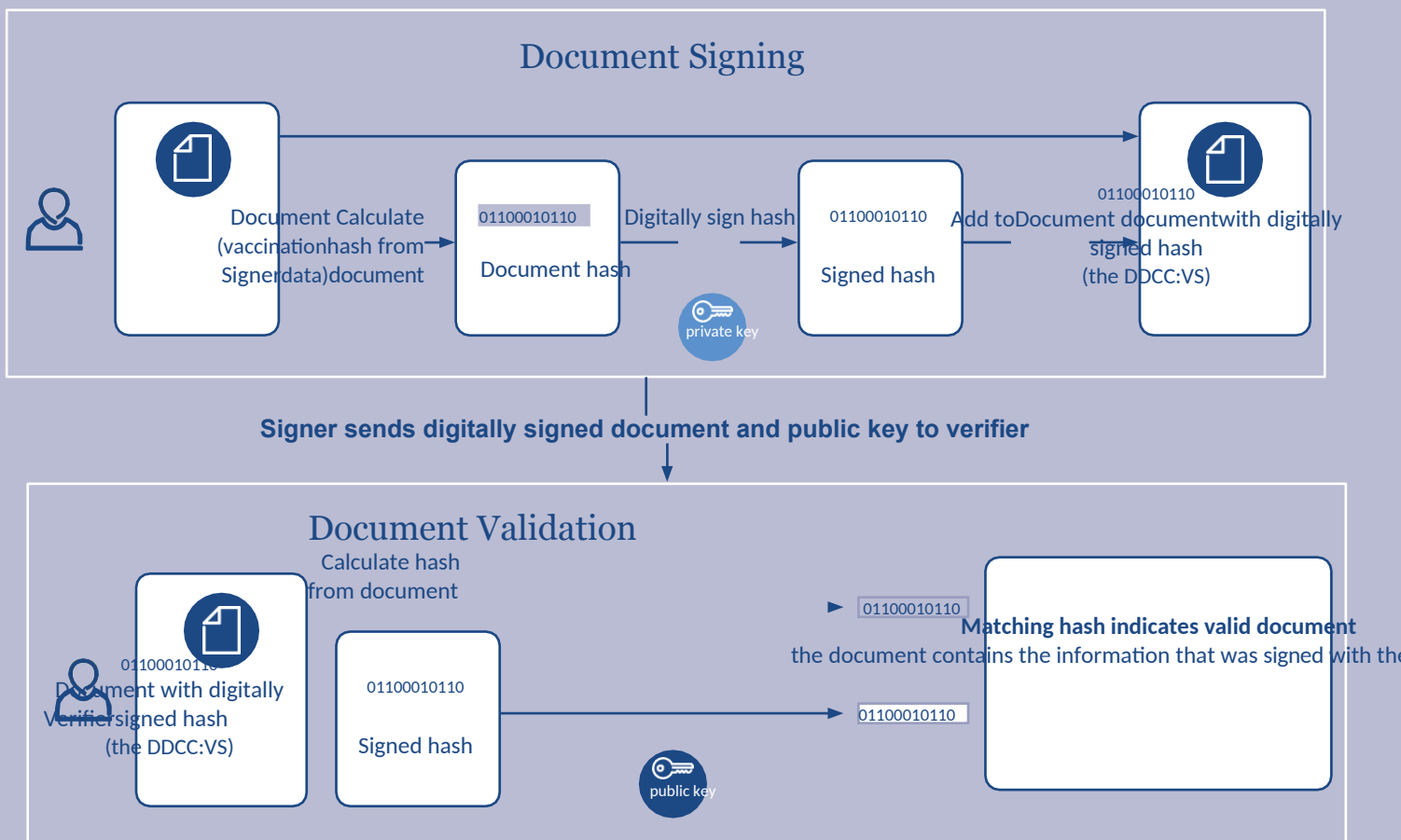
6.2. Verifying a DDCC:VS signature

The verification process, shown in the bottom row of Fig. 13 and further detailed in Fig. 15, reverses the signing process to verify content in the signed DDCC:VS.

1. A Verifier calculates its own hash (i.e. “calculated hash”) from the information in the DDCC:VS using the same hashing algorithm as was used by the document signer.
2. The DDCC:VS’s signed hash is read by a digital solution.
3. The document signer’s **public** key is used to cryptographically transform the signed hash back to the document hash. The Verifier can compare the document hash from step 2 to its own calculated hash from step 1. If they match, the Verifier is confident that:
 - a. only someone with access to the DSC’s private key could have signed the document, because the public key was able to decrypt the document hash; and
 - b. the data that was signed is the same as the data read from the DDCC:VS, because the calculated hash matches the document hash.
4. The PHA’s root certificate **public** key is used to cryptographically verify that the document signer’s signature was issued under the responsibility of the PHA.

Figure 15

How digital signature verification works



6.3. Trusting a DDCC:VS signature

The cryptographic strength of private–public key pairs is based on the mathematics of asymmetric cryptography, a process involving “one-way” mathematical functions, which are operations that are easy to compute in one direction but extremely hard to reverse. They provide a high level of security provided the private key is not compromised and remains available only to the entity performing the signing. Operationally, private keys are kept highly secure and public keys are broadly shared. Provided that a private key is not compromised and unintentionally revealed to another party, content that is “signed” by (i.e. encoded with) a private key may be readily verified by (i.e. decrypted by) anyone who has the corresponding public key. Anyone using the public key associated with the private key can be confident that:

1. material they decrypt with a public key can only have been signed by the holder of the corresponding private key; and
2. the holder of the private key cannot deny that they signed the material.

PKI is the mechanism whereby the public key is circulated to all who need it and the receiver is assured that the public key comes from a trusted source. Furthermore, a PKI also includes means for revoking keys, so that if a private key is compromised, the public keys can be flagged as no longer valid.

SECTION

7

National governance considerations



Governance in the health sector is “a wide range of steering and rule-making related functions carried out by governments/decisions makers as they seek to achieve national health policy objectives that are conducive to universal health coverage” (33). A national framework to govern the complex and dynamic health policy for implementing DDCC:VS should be tailored to meet the Member State’s needs, which vary. This section provides an overview of some key governance considerations for Member States implementing DDCC:VS solutions. However, it will be the responsibility of the Member State to determine the most appropriate governance mechanisms for its context.

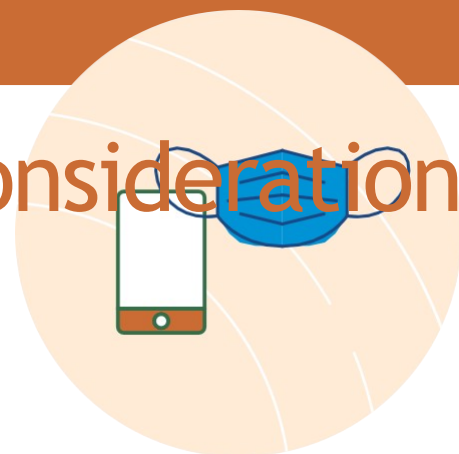
Fundamentally, trust in the system should derive from the security-by-design of a PKI and the governance rules put in place by the Member State to operate it. The Proof of Vaccination scenario of use requires governance to be established at two levels: 1. the PHA; and 2. the Member State. At PHA level, at least one DSC needs to be utilized to sign the DDCC:VS. At Member State level, an authorized DSC-sharing mechanism needs to be established to indicate which DSCs are currently permitted to sign the DDCC:VS. There are two recommended approaches.

1. **ROOT CERTIFICATE AUTHORITY:** The Member State establishes a root certificate authority, which holds a root certificate for the DDCC:VS. The private key of the Root Certificate managed by the Member State may be used by the Member State to sign a PHA’s DSC that has been authorized for use. The public key of the root certificate can be used to validate that the DSC is authorized. Note that the term “root” does not imply hierarchy or that the root certificate authority is at the top of that hierarchy. Rather, it is used to denote that a root certificate authority may be trusted directly (34).
2. **MASTER LIST:** The Member State establishes a mechanism to manage and distribute, as appropriate, a master list of DSCs that have been authorized for PHAs to use to sign the DDCC:VS.

Member States can leverage an existing PKI or create a new one specifically for DDCC:VS. Regardless, depending on how a Member State’s health systems are organized, there are several PKI options that the national-level ministry of health could consider, depending on the governance context in the Member State.

To ensure that national governing bodies can establish mutual trust with other Member States through bilateral or multilateral agreements, governance mechanisms should be in place for the digital signing infrastructure based on each Member State's governance context. In addition to the authorized DSC- sharing mechanism, the following components should be addressed, with clear policies in place for each Member State.

- **ISSUING DDCC:VS:** There should be clear and transparent processes in place for issuing DDCC:VS in order to establish trust in the system. Transparently acknowledging which entities are eligible to issue a DDCC:VS reduces the potential for fraudulent issuance of DDCC:VS and provides accountable entities when possible fraud has occurred.
- **VERIFYING DDCC:VS:** Member States need to define the requirements for what it means to have a "valid" DDCC:VS. Furthermore, Member States will need to decide whether the DDCC:VS can be verified by anyone with the means to verify a DDCC:VS; alternatively, they may decide on a list of trusted Verifiers, in which case only trusted Verifiers would be able to verify a DDCC:VS. The appropriate privacy mechanisms should be built into the implementation based on this decision.
- **REVOCAION OF DDCC:VS:** There should be clear and transparent processes for revocation of a DDCC:VS in case fraud has occurred, incorrect information needs to be rectified, faulty vaccine batches have been discovered or issues have been detected within the vaccine supply chain. These revocation processes should also include standard operating procedures for:
 - » **INFORMING INDIVIDUALS:** Individuals will need to be informed if their DDCC:VS has been revoked and for what reason. Enforcing revocation without clearly communicated justification may lead to erosion of trust in governing bodies.
 - » **INFORMING VERIFIERS:** Verifiers will need to be informed if DDCC:VS have been revoked in order to be able to continuously trust that DDCC:VS issued by a specific entity are still valid. For example, if there are reports of counterfeit DDCC:VS, Verifiers should be informed about the possibility of encountering counterfeit DDCC:VS. This allows for continued trust in the system.
 - » **REMEDY PROVISION:** If a DDCC:VS is revoked, Member States should apply measures to rectify the situation, for example, by providing the option of a new vaccination, if advisable. Alternatively, there might be processes to obtain a new, verifiable DDCC:VS.
- **DATA MANAGEMENT AND PRIVACY PROTECTION:** Member States are responsible for data timeliness and completeness, and for the accuracy of DDCC:VS issued by their PHAs. Personal data about individuals with DDCC:VS from other countries need to be processed according to a set of principles and processes agreed upon by Member States, in order to establish trust between Member States.



Since COVID-19 was declared a Public Health Emergency of International Concern under the IHR in January 2020, there has been a clear and urgent need for all Member States to effectively address the COVID-19 pandemic. In the digital age, there has also been immediate acknowledgement that digital health solutions can effectively and immediately be leveraged to support the public health response to the pandemic (35). However, there are two distinct approaches that Member States can use to pursue the implementation of DDCC:VS, both of which have different implications for implementation strategy.

1. **SHORT-TERM DDCC:VS SOLUTION:** Deploy a short-term DDCC:VS solution to address the immediate need of the pandemic that includes a clearly established end date and a roadmap towards discontinuing the DDCC:VS solution once COVID-19 is no longer considered a Public Health Emergency of International Concern under the IHR.
2. **LONG-TERM DDCC:VS SOLUTION:** Deploy a DDCC:VS solution to address the immediate needs of the pandemic but also to build digital health infrastructure that can be a foundation for digital vaccination certificates beyond COVID-19 (e.g. digital home-based records for childhood immunizations) and support other digital health initiatives.

Both approaches are valid and will depend on the available resources, the pandemic response plan, the overall public health strategy and the digital health roadmap of the Member State. However, it is critical for Member States to determine whether their DDCC:VS is intended only to be in response to the COVID-19 pandemic, or if it is intended to be a sustainable solution that can address other existing health systems challenges and future pandemics. The chosen approach will greatly inform critical DDCC:VS implementation decisions, some of which are outlined in sections 8.1 and 8.2. Regardless of the direction, some key implementation considerations need to be taken into account.

8.1. Considerations before deploying

Using the framework of essential components of a digital health implementation presented in the [WHO/ITU's National eHealth Strategy Toolkit](#) (36), and the guidance provided in the [Digital implementation investment guide \(DIIG\)](#) (37), the following considerations and key questions should be examined prior to deployment of a DDCC:VS solution.

STRATEGY AND INVESTMENT

- Is the DDCC:VS solution intended to be a short-term solution or a long-term digital vaccination certificate solution?
- What are the potential benefits, risks and costs of implementing a DDCC:VS solution? These should be assessed before introducing a DDCC:VS system and its associated infrastructure. An impact assessment should include ethical and privacy implications and potential risks that may arise with the implementation of DDCC:VS.
- What is the potential impact on individuals, families, businesses, health workers, vaccinators and other relevant stakeholders?
- What is the potential impact on public health and on the economy?
- What is the additional value added beyond using the paper system only?

INFRASTRUCTURE

- How can existing digital health investments be leveraged? Due to the need for pandemic response, existing digital health investments should be leveraged as much as possible.
- If there is an intention to pre-print DDCC:VS, then is high-volume printing capacity for paper forms available domestically?
- Consider the coverage of mobile phone adoption before pursuing a mobile-only solution. Is there broad mobile phone adoption and high coverage of mobile phone networks outside the major urban areas? Among those with mobile phones, is there broad adoption of smartphones?
- Is a PKI in place that can also be leveraged to support digitally signing DDCC:VS digital documents?

LEGISLATION, POLICY AND COMPLIANCE

- Are policies for appropriate use and data protection in place to address the ethical considerations and data protection principles of DDCC:VS?
- How will it be assured that individuals are not treated differently, or given different levels of trust, due to the format of the DDCC:VS they are using (e.g. smartphone application or paper certificate)?
- For continuity of care, are digital health data sharing and consent management policies in place?
- What technical and organizational safeguards exist to ensure proper data management throughout the data life-cycle? Will additional processes (e.g. monitoring of data access, data breach notification) need to be implemented?
- What review processes are needed for any newly developed policies or procedures?

LEADERSHIP AND GOVERNANCE

- Is there an existing department within the ministry of health that will be accountable for this work? There needs to be a clear accountable entity, whether it is a single department or a formalized cross-cutting group or committee, that is responsible for operationalizing DDCC:VS.
- Is there a clear governance mechanism and are standard operating procedures in place to support the use and maintenance of the DDCC:VS?
- What agency will be responsible for independent oversight for use of the DDCC:VS, and what level of authority will it be given? How will the impact of DDCC:VS use on public health, the economy, the environment and individuals be assessed? Are mechanisms in place to course-correct as needed?
- What agreements or formal collaborations will need to be established in a memorandum of understanding?
- Will there need to be agreements established bilaterally, multilaterally or at a regional level to establish trusted recognition between DDCC:VS of different provenance? Are bilateral or regional agreements in place that can be leveraged?

WORKFORCE

- Is the value added by the digital representation clearly communicated? Health workers, health facility managers and vaccinators may face the additional burden of operating a dual system of both paper-based and digital solutions.
- Are change management processes and support in place when implementing a DDCC:VS?
- Is there a ready domestic supply of digital health workers? Does this workforce have the skillsets needed or, if not, what level of effort would be needed to conduct training?
- Are there health informatics programmes at national universities that can help fill the requirements for technical support to health workers who are taking up new digital health solutions?
- Given the ever-changing context of the COVID-19 pandemic, how will continuous training and updating of health workers, vaccinators, health facility managers, and public health officials take place to ensure continued relevance of the DDCC:VS?

SERVICES AND APPLICATIONS

- Are point-of-care applications used presently to support routine immunization (e.g. electronic immunization registries)? If yes, could these also be leveraged to support COVID19 vaccine administration?
- Do point-of-service applications exist that are used for other workflows not related to vaccination, but which could be leveraged to collect the DDCC:VS core data set and associate these data with an HCID? Examples may include existing supply chain or HMIS solutions that can be readily extended to support new workflows.
- Are there existing products in the marketplace that would fit your needs and adhere to international specifications and guidance?
- Are there different types of software models, including: custom-developed software, commercial off-the-shelf (COTS) software, free packaged software, open source software, and software as a service (SaaS)? The benefits and risks of these different software models should be considered.

- If deciding to use open source products, is there a responsive established user community that will provide support and help add features at no cost?
- Which services and applications would be the most environmentally sustainable?

STANDARDS AND INTEROPERABILITY

- Is there an existing interoperability framework to guide how a DDCC:VS can interoperate with other existing solutions? Are there solutions in the marketplace that have operationalized standards for interoperability?
- Is conformance-testing capacity available domestically to test whether DDCC:VS solutions adhere to national (and/or international) specifications?
- Are there reusable components, such as terminology services, that could be incorporated? An example of how to leverage the OpenHIE framework is given in [Annex 6](#).

HEALTH CONTENT

- What is the process to account for the constantly changing context of COVID-19? As the evidence base increases and relevant clinical and/or public health guidelines are updated, there may be new health content requirements. Implementation of the DDCC:VS should change in accordance with the changing health context and remain evidence based.

8.2. Key factors to consider with solution developers

If a PHA that is responsible for the delivery of a digital solution does not have the appropriate technology skills in-house, then it may want to look for one or more partners to provide that service. The choice of a digital partner will ideally be subject to a competitive process. Multiple potential suppliers will be considered to identify partners that represent the best fit for the work at the optimal price, with consideration of the total cost of ownership, timeline and sustainability of the solution. The approach to inviting tenders for the work, assessing tenders, awarding a contract and then working with a partner should consider the following high-level key factors.

- The terms of reference for the work that needs to be performed should be clearly expressed and at a level of detail that allows solution developers to respond with a high degree of confidence in their bids.
- An early decision is needed as to whether work will be performed under a fixed price or a time-and-materials arrangement (or a mixture of the two in which, for example, a core product is delivered but additional work paid on a prorata basis).
- The timeline for work should be realistically set. The realization of a digital solution is a technology project, and projects are subject to the triple constraints of scope, cost and time, with the quality of the work affected by all three. The engaging authority should have a realistic understanding of the likely effort of the project and the effects on scope and cost if the timeline is set to be too short.
A phased approach to deliver a minimum viable product first and iterate further enhancements is often recommended.

- A decision is needed as to whether a single supplier (with sub-contractors) or a consortium of suppliers is permitted. Working with a consortium brings the advantage that multiple best-in-class vendors can collaborate, but also involves the complication of extra communication and coordination between these actors.
- The metrics for success of the work should be defined early, so that the goals and outcomes of the project are clear to all involved. Ideally, these metrics should be measurable key performance indicators (number of vaccination records stored, speed of operation, compliance with regulations, etc.). Contracts (and payment schedules) can be tied to performance indicators to incentivize vendors and keep the focus clearly on the desired outcome.
- Suppliers should demonstrate solid expertise in the area of work for which they are being engaged; they should have a portfolio of previous experience and be able to provide references. A demonstration of relevant previous work can be requested to gain confidence in the vendor's expertise.
- Suppliers should also demonstrate a solid track record of project management for delivering digital solutions. This will include establishing a clear communication plan so that the regularity of and format for reporting on project progress is understood and the procedure for escalation of problems is agreed.
- The working hours, location and corporate culture (including working language) of any supplier should be considered, to ensure that teams will work together well and that the risk of miscommunication is reduced.
- As noted at the start of the section, if the strategy is to build a digital solution as part of a longer-term investment in public health technology that will outlive the COVID-19 pandemic, then the choice of a supplier that can potentially become a long-term partner in that journey is advisable.
- It should be clear where the intellectual property for any work delivered by the digital supplier will reside, particularly if the supplier is creating new assets. The same applies to the purchase and use of any software licences needed to execute the project and the operation of the product created.

A successful partnership with a digital solution developer rests on clear, binding contracts, a shared understanding of the goals and desired outcomes of the work, and a working relationship that aligns all parties behind these goals.

8.3. Cost category considerations

Regardless of whether the intended DDCC:VS solution will be a short-term solution or a long-term digital vaccination certificate solution, specific cost categories and related cost drivers will affect the budget for this work. However, whether they will be incurred as a sunk cost of the pandemic (for short-term solutions) or an investment for future digital health systems (long-term solutions) will depend on the Member State's implementation strategy. Table 13 provides a non-exhaustive list of possible cost drivers for implementing a DDCC:VS solution.

Table 13
Illustrative costs for a DDCC:VS

	<ul style="list-style-type: none"> → Coordination of personnel to develop and maintain relevant partnerships → Conducting an impact assessment and developing new policies, processes and standard operating procedures for ongoing monitoring of use and impact → Independent oversight and monitoring
	<ul style="list-style-type: none"> → Personnel to oversee the overall programme until planned end (if there is one), including project management – and vendor management, if applicable → System set-up and end-user support → Monitoring feedback and taking corrective action → Handling complaints and exercising data subject rights, including legal redress
	<ul style="list-style-type: none"> → Building completely new COVID-19 systems or leveraging existing software systems (e.g. adapting EIR systems) → Subscriptions, licensing fees and implementation costs associated with the software model → Custom configurations or any enhancements, if needed, or any custom-developed software → Translations and localizations, if needed
	<ul style="list-style-type: none"> → Data storage (e.g. costs for storage in the cloud, or on local servers or individual devices) → Devices (e.g. printers and scanners) needed at the vaccination site or in the back office → Quality assurance, end-user testing and testing of conformity with standards and interoperability with other systems (if part of the design); ensure costs are allocated for collecting end-user feedback and updating the digital system according to feedback received → Training vaccinators, health facility managers and data entry personnel, which may involve travel or other logistical costs → Training materials for verifiers of DDCC:VS → Transport of any necessary hardware, software or materials (including paper cards) to the vaccination sites or certificate-issuance sites → Increased technical support required during the roll-out phase → Communications on when, where and how people can obtain a DDCC:VS → Communication of what DDCC:VS can and cannot be used for → Battling “infodemics” (too much information, misinformation and disinformation) associated with DDCC:VS → Meeting accessibility requirements of individuals and reaching groups with disadvantages, such as individuals with digital skill barriers or disability barriers
	<ul style="list-style-type: none"> → Adapting content, depending on acceptance agreements between Member States → Coordination for establishing agreements between Member States
	<ul style="list-style-type: none"> → Undertaking mapping exercises and adopting standards agreed upon through the establishment of trust frameworks → Any licensing fees associated with use of standards (note that the standards proposed by WHO in this guidance document have no licensing fees)
	<ul style="list-style-type: none"> → With the Paper First approach: printing, which will increase as more people are vaccinated and, subsequently, more people receive a physical vaccination certificate

- As people are vaccinated: the additional personnel to support use of the systems, including training, management, etc.
 - Depending on the licensing model associated with any digital solution, the additional licences that may need to be purchased as the number of operators or amount of data increases, or additional IT infrastructure is needed
 - As data volume and number of system users grows, the scaling up of the capacity of the digital solution to provide the necessary storage and processing power
-
- Consistent training of new staff when staff leave, and refresher training for existing staff – with content updates made as the context changes
 - Monitoring and evaluation of DDCC:VS implementation practices and processes, with application of learnings
 - Continued messaging, with consideration of accessibility needs
 - Continued help desk or customer service technology support for users of the DDCC:VS
 - Fixing bugs, adding features, maintaining customizations, releasing updates, and hardware maintenance and replacement

8.4. Additional resources to support implementation

Additional resources that can be leveraged to support the implementation of DDCC:VS include examples of implementations already deployed, additional technical specifications for specific use cases, and general guidance on implementing digital health solutions. Note that the following is a non-exhaustive list of examples. WHO will be documenting in a clearinghouse software solutions that are consistent with the DDCC:VS specifications.

WHO INTEROPERABILITY STANDARD FOR DDCC:VS

- [DDCC:VS HL7 FHIR Implementation Guide](#)
- [DDCC:VS core data dictionary, 27 July 2021](#)

EXAMPLE DDCC:VS IMPLEMENTATIONS

- [EU Digital COVID Certificate \(17\)](#)
- [OpenSRP FHIR Core Smart Vaccination Certificates](#)

SOFTWARE CONSISTENT WITH DDCC:VS SPECIFICATIONS' DATASET AND ARCHITECTURE

- [EU Digital COVID Certificate Gateway](#)
- [DIVOC \(Digital Infrastructure for Vaccination Open Credentialing\) in India \(39\)](#)
- [Open SRP FHIR Core Smart Vaccination Certificates for Android](#)
- [OpenHIE DDCC Transactions Mediator](#)

EXAMPLE SPECIFICATIONS THAT CAN BE USED TO GUIDE IMPLEMENTATION

- [ICAO Guidelines: visible digital seals \(“VDS-NC”\) for travel-related health proofs \(16\)](#)
- [OpenHIE DDCC FHIR Implementation Guide](#)

GENERAL IMPLEMENTATION GUIDANCE FOR DIGITAL HEALTH SOLUTIONS

- [Digital implementation investment guide \(DIIG\): integrating digital interventions into health programmes \(37\)](#) – provides a generic systematic process for countries to develop a costed implementation plan for digital health, which can be leveraged to specifically guide implementation of the DDCC:VS.

WHO INTERNATIONAL TRAVEL GUIDANCE

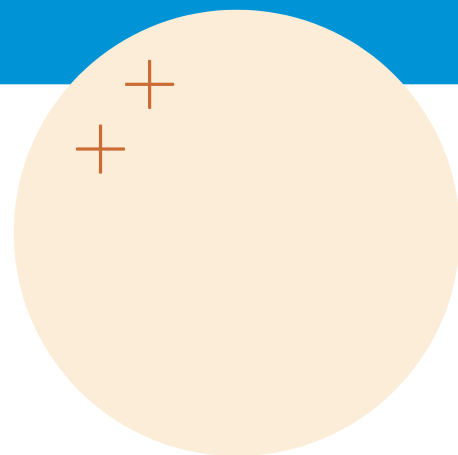
- [International Health Regulations](#)
- [Travel Guidance](#)

References

1. Diamond, D. 'Ripe for fraud': Coronavirus vaccination cards support burgeoning scams. In: The Washington Post [website]. USA: The Washington Post; 18 April 2021 (<https://www.washingtonpost.com/health/2021/04/18/scams-coronavirus-vaccination-cards/>, accessed 9 August 2021).
2. Siringi, S. Fake health certificate racket rife in Kenya. *Lancet Infect Dis.* 2002;2(8):454. doi:10.1016/s1473-3099(02)00357-2.
3. Deguma MC, Deguma JJ. The possible threat of faking Covid-19 diagnostic tests and vaccination certifications: a call to an immediate action. *J Public Health (Oxf).* 2021;43(2):e340–1. doi:10.1093/pubmed/fdab054.
4. Grierson J. Fake Covid vaccine and test certificate market is growing, researchers say. In: The Guardian [website]. Guardian News & Media Limited; 16 May 2021 (<https://www.theguardian.com/world/2021/may/16/fake-covid-vaccine-and-test-certificate-market-is-growing-researchers-say>, accessed 27 June 2021).
5. World Health Organization open call for nomination of experts to contribute to the Smart Vaccination Certificate technical specifications and standards. In: World Health Organization/Newsroom [website]. Geneva: World Health Organization; 2 December 2020 (<https://www.who.int/news-room/articles-detail/world-health-organization-open-call-for-nomination-of-experts-to-contribute-to-the-smart-vaccination-certificate-technical-specifications-and-standards-application-deadline-14-december-2020>, accessed 27 June 2021).
6. Technical considerations for implementing a risk-based approach to international travel in the context of COVID-19: Interim guidance, 2 July 2021. In: World Health Organization/Newsroom [website]. Geneva: World Health Organization; 2 July 2021 (<https://www.who.int/publications/i/item/WHO-2019-nCoV-Risk-based-international-travel-2021.1>, accessed 27 July 2021).
7. Policy considerations for implementing a risk-based approach to international travel in the context of COVID-19. Geneva: World Health Organization; 2 July 2021 (<https://apps.who.int/iris/handle/10665/342235>, accessed 6 July 2021).
8. Considerations for implementing and adjusting public health and social measures in the context of COVID-19. Interim guidance. Geneva: World Health Organization; 14 June 2021 (<https://www.who.int/publications/i/item/considerations-in-adjusting-public-health-and-social-measures-in-the-context-of-covid-19-interim-guidance>, accessed 27 June 2021).
9. Statement on the seventh meeting of the International Health Regulations (2005) Emergency Committee regarding the coronavirus disease (COVID-19) pandemic. In: World Health Organization/News [website]; 19 April 2021 ([https://www.who.int/news/item/19-04-2021-statement-on-the-seventh-meeting-of-the-international-health-regulations-\(2005\)-emergency-committee-regarding-the-coronavirus-disease-\(covid-19\)-pandemic](https://www.who.int/news/item/19-04-2021-statement-on-the-seventh-meeting-of-the-international-health-regulations-(2005)-emergency-committee-regarding-the-coronavirus-disease-(covid-19)-pandemic), accessed 27 June 2021).
10. Statement on the sixth meeting of the International Health Regulations (2005) Emergency Committee regarding the coronavirus disease (COVID-19) pandemic. In: World Health Organization/News [website]; 15 January 2021 ([https://www.who.int/news/item/15-01-2021-statement-on-the-sixth-meeting-of-the-international-health-regulations-\(2005\)-emergency-committee-regarding-the-coronavirus-disease-\(covid-19\)-pandemic](https://www.who.int/news/item/15-01-2021-statement-on-the-sixth-meeting-of-the-international-health-regulations-(2005)-emergency-committee-regarding-the-coronavirus-disease-(covid-19)-pandemic), accessed 27 June 2021).
11. Technical considerations for implementing a risk-based approach to international travel in the context of COVID-19: Interim guidance. Geneva: World Health Organization; 2 July 2021 (<https://www.who.int/publications/i/item/WHO-2019-nCoV-Risk-based-international-travel-2021.1>, accessed 20 July 2021).
12. Monitoring COVID-19 vaccination: considerations for the collection and use of vaccination data. Interim guidance. Geneva: World Health Organization; 3 March 2021 (<https://www.who.int/publications/i/item/monitoring-covid-19-vaccination-interim-guidance>, accessed 27 June 2021).
13. Practical guide for the design, use and promotion of home-based records in immunization programmes. Geneva: World Health Organization; 1 June 2015 (<https://www.who.int/publications/i/item/WHO-IVB-15.05>, accessed 27 June 2021).
14. Guidance on developing a national deployment and vaccination plan for COVID-19 vaccines. Geneva: World Health Organization; 1 June 2021 (<https://www.who.int/publications/i/item/WHO-2019-nCoV-Vaccine-deployment-2021.1-eng>, accessed 27 June 2021).
15. International Health Regulations (2005), third edition. Geneva: World Health Organization; 1 January 2016 (<https://www.who.int/publications/i/item/9789241580496>, accessed 27 June 2021).
16. Guidelines: visible digital seals ("VDS-NC") for travel-related health proofs. International Civil Aviation Organization (ICAO) Technical Advisory Group (TAG) on the Traveler Identification Group (TRIP); no date (<https://www.icao.int/Security/FAL/TRIP/PublishingImages/Pages/Publications/Guidelines%20-%20VDS%20for%20Travel-Related%20Public%20Health%20Proofs.pdf>, accessed 27 June 2021).
17. EU Digital COVID certificate. In: European Commission [website]; no date (https://ec.europa.eu/info/live-work-travel-eu/coronavirus-response/safe-covid-19-vaccines-europeans/eu-digital-covid-certificate_en#what-is-the-eu-digital-covid-

18. Requiring proof of Covid-19 vaccination (vaccine “passports”/“certificates”): Key ethical, legal, and social issues. Policy brief. In: Swiss National COVID-19 Science Task Force [website]. Zurich: ETH Board; 19 February 2021 (<https://scienctaskforce.ch/en/policy-brief/requiring-proof-of-covid-19-vaccination-vaccine-passports-certificates-key-ethical-legal-and-social-issues>, accessed 27 June 2021).
19. Ozawa S, Yemeke TT, Evans DR, Pallas SE, Wallace AS, Lee BY. Defining hard-to-reach populations for vaccination. *Vaccine*. 2019;37(37):5525–34. doi:10.1016/j.vaccine.2019.06.081.
20. What place should COVID-19 vaccine passports have in society? Ada Lovelace Institute; 17 February 2021 (<https://www.adalovelaceinstitute.org/wp-content/uploads/2021/02/COVID-19-vaccine-passports-rapid-expert-deliberation.pdf>, accessed 27 June 2021).
21. Committee on Bioethics. Statement on human rights considerations relevant to “vaccine pass” and similar documents. Strasbourg: Council of Europe; 4 May 2021 (<https://rm.coe.int/dh-bio-2021-7-final-statement-vaccines-e/1680a259dd>, accessed 27 June 2021).
22. COVID-19 Vaccination certificates and lifting public health and social measures: ethical considerations. Geneva: World Health Organization; forthcoming.
23. Twelve criteria for the development and use of COVID-19 vaccine passports. Pre-print paper. London: The Royal Society The Royal Society SET-C (Science in Emergencies Tasking – COVID); 14 February 2021 (<https://royalsociety.org/-/media/policy/projects/set-c/set-c-vaccine-passports.pdf>, accessed 27 June 2021).
24. Voo TC, Reis AA, Thomé B, Ho CW, Tam CC, Kelly-Cirino C, et al. Immunity certification for COVID-19: ethical considerations. *Bulletin of the World Health Organization*. 2021;99(2):155–61. doi:10.2471/BLT.20.280701.
25. Guidelines on ethical issues in public health surveillance. Geneva: World Health Organization, 2017 (<https://www.who.int/publications/i/item/who-guidelines-on-ethical-issues-in-public-health-surveillance>, accessed 27 June 2021).
26. Global manual on surveillance of adverse events following immunization. Geneva: World Health Organization, 2016, (<https://apps.who.int/iris/handle/10665/206144>, accessed 27 June 2021).
27. OpenSRP. In: OpenSRP [website]. OpenSRP; no date (<https://smartregister.org/>, accessed 29 June 2021).
28. About DHIS2. In: DHIS2 [website]. University of Oslo; no date (<https://dhis2.org/about>, accessed 27 June 2021).
29. VigiFlow: Supporting national and regional pharmacovigilance and vaccine surveillance processes. In: Uppsala Monitoring Centre [website]; no date (<https://www.who-umc.org/global-pharmacovigilance/vigiflow>, accessed 27 June 2021).
30. International Patient Summary Implementation Guide: 1.0.0 – Continuous Integration Build [website]. Health Level Seven International – Patient Care Work Group; 2021 (<https://build.fhir.org/ig/HL7/fhir-ips>, accessed 27 June 2021).
31. ICD-11: International Classification of Diseases 11th Revision. In: World Health Organization International Classification of Diseases [website]. Geneva: World Health Organization; 2021 (<https://icd.who.int/en>, accessed 27 June 2021).
32. Global Patient Set. In: SNOMED International [website]. London: SNOMED International; 2021 (<https://www.snomed.org/snomed-international/learn-more/global-patient-set>, accessed 27 June 2021).
33. Health system governance. In: World Health Organization/Health topics [website]. Geneva: World Health Organization; no date (https://www.who.int/health-topics/health-systems-governance#tab=tab_1, accessed 27 June 2021).
34. Adams C, Farrell S, Kause T, Mononen T. Internet X.509 Public Key Infrastructure Certificate Management Protocol (CMP), section 3.1.1.2 Certification Authority. Reston (VA) and Geneva: The Internet Society Network Working Group; 2005 (<https://datatracker.ietf.org/doc/html/rfc4210#section-3.1.1.2>, accessed 27 June 2021).
35. Budd J, Miller BS, Manning EM, Lamos V, Zhuang M, Edelstein M, et al. Digital technologies in the public-health response to COVID-19. *Nat Med*. 2020;26(8):1183–92. doi:10.1038/s41591-020-1011-4.
36. National eHealth Strategy Toolkit: overview. Geneva: World Health Organization and International Telecommunication Union; 2012 (<https://www.who.int/ehealth/publications/overview.pdf>, accessed 28 June 2021).
37. Digital implementation investment guide (DIIG): integrating digital interventions into health programmes. Geneva: World Health Organization; 15 September 2020 (<https://www.who.int/publications/i/item/9789240010567>, accessed 28 June 2021).
38. Rwanda uses DHIS2 as an interactive system for rapid and paperless COVID-19 vaccination. In: dhis2 [website]. University of Oslo; no date (<https://dhis2.org/rwanda-covid-vaccination>, accessed 28 June 2021).
39. DIVOC - Digital Infrastructure for Vaccination Open Credentialing. In: DIVOC [website]. India: eGov Foundation; no date (<https://divoc.egov.org.in>, accessed 28 June 2021).
40. Statement on the eighth meeting of the International Health Regulations (2005) Emergency Committee regarding the coronavirus disease (COVID-19) pandemic. In: World Health Organization/News [website]; 15 July 2021 ([https://www.who.int/news/item/15-07-2021-statement-on-the-eighth-meeting-of-the-international-health-regulations-\(2005\)-emergency-committee-regarding-the-coronavirus-disease-\(covid-19\)-pandemic](https://www.who.int/news/item/15-07-2021-statement-on-the-eighth-meeting-of-the-international-health-regulations-(2005)-emergency-committee-regarding-the-coronavirus-disease-(covid-19)-pandemic), accessed 26 July 2021)

Annexes



Annex 1

Illustrative example of Digital Documentation of COVID-19 Certificates: Vaccination Status (DDCC:VS)

Below is an illustrative example of a DDCC:VS intended to be printed on A6 paper and folded like a booklet. This is not a template, nor are Member States required to adopt this design. Member States are encouraged to design a vaccination certificate (paper and/or digital) with the core data set requirements, fraud prevention mechanisms and scenarios of use in mind.¹

Figure A1.1
The outside of the vaccination certificate

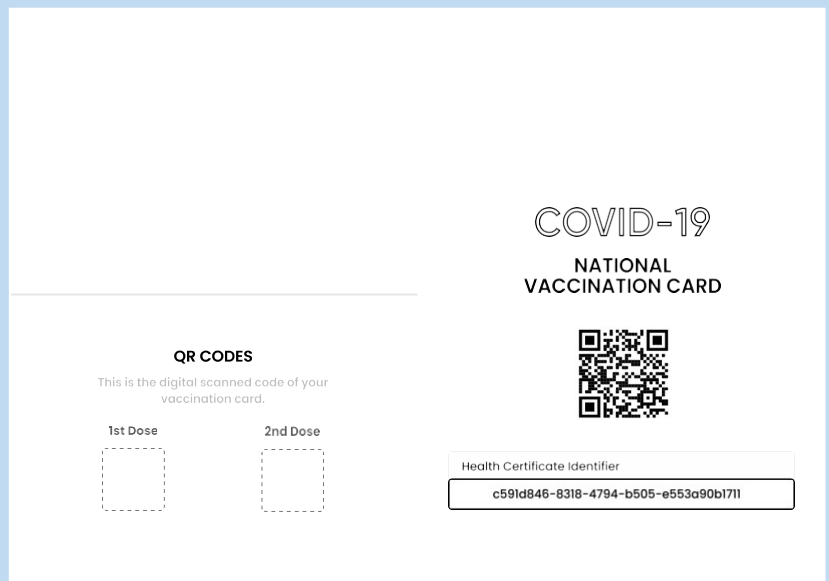


Figure A1.2
The inside of the vaccination certificate

A Your Background Information		C Your Second Dose <small>If Required</small>	
Name <input type="text"/>		ID Number <input type="text"/>	
Date of Birth (Day / Month / Year) <input type="text"/>		Sex <input type="checkbox"/> Male <input type="checkbox"/> Female	
B Your First Dose		Date of Vaccination <input type="text"/> Vaccine <input type="text"/>	
Date of Vaccination <input type="text"/> Vaccine <input type="text"/>		Date of Vaccination <input type="text"/> Vaccine <input type="text"/>	
Vaccine Brand <input type="text"/>		Vaccine Brand <input type="text"/>	
Batch Number <input type="text"/>		Batch Number <input type="text"/>	
Vaccine Manufacturer <input type="text"/>		Vaccine Manufacturer <input type="text"/>	
Administering centre <input type="text"/>		Administering centre <input type="text"/>	
Health Worker Signature <input type="text"/>		Health Worker Signature <input type="text"/>	
Country of vaccination <input type="text"/>		Country of vaccination <input type="text"/>	
Total Doses <input type="text"/>		Total Doses <input type="text"/>	
Due date of next dose <input type="text"/>			

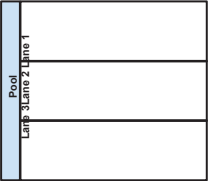
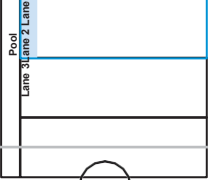



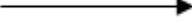


¹ This illustrative example is adapted from the COVID-19 Paper Based Information System designed and developed by Sonder Design, which can be accessed here: <https://www.notion.so/COVID-19-Paper-Based-Information-System-a1fc3840e904142b775f1e9c92711c8>.

Annex 2

Business process symbols used in workflows

Table A2.1 provides an overview of the standardized notation for business process mapping that is used to depict the Continuity of Care use cases and Proof of Vaccination use cases.

Table A2.1
Business process symbols used in workflows

Symbol	Symbol name	Description
	Pool	A pool consists of multiple “swim lanes” that depict all the individuals or types of users that are involved in carrying out the business process or workflow.
	Swim lane	Each persona is assigned to a swim lane, a designated area for noting the activities performed or expected by that specific actor.
	Start event or trigger event	The start event notes the beginning of the process.
	End event	The end event notes the end of a business process.
	Activity, process, step or task	Each activity notes the successive actions performed by the actor for that swim lane.
	Sequence flow	This denotes the flow direction from one process to the next.
	Message flow	This denotes the flow of data or information from one process to another.
	Gateway	This symbol is used to depict a fork, or decision point, in the workflow, which may be a simple binary (e.g. yes/no) filter with two corresponding output arrows, or a different set of outputs.

Annex 3

Guiding principles for mapping the WHO Family of International Classifications (WHO-FIC) and other classifications

Mapping from classifications and terminologies used in existing systems to the International Classification of Diseases, 11th revision (ICD-11), and other WHO-FIC classifications should follow the principles listed below.¹

1. Establish use case(s) prior to developing the map – this involves identifying and formulating the purpose(s) for which the map will be used and describing the different types of users and how they will process data using the map.
2. Clearly define the purpose, scope and directionality of the map.
3. Maps should be unidirectional and single-purpose. Separate unidirectional maps should be used in place of bidirectional maps (to support both a forward and a backward map table). Such unidirectional maps can support data continuity for epidemiological and longitudinal studies. Maps should not be reversed.
4. Develop clear and transparent documentation that is freely available to all and that describes the purpose, scope, limitations and methodology of the map.
5. Ideally, the producers of both terminologies in any map should participate in the mapping effort to ensure that the result accurately reflects the meaning and usage of their terminologies. As a minimum, both terminology producers should participate in defining the basic purpose and parameters of the mapping task, reviewing and verifying the map, developing the plan for testing and validation, and devising a cost-effective strategy for building, maintaining and enhancing the map over time.
6. Map developers should agree on the competencies, knowledge and skills required of team members at the onset of the project. Ideally, target users of the map should also participate in its design and testing to ensure that it is fit for its intended purpose.
7. Establish quality assurance (QA) and usage validation protocols at the beginning of the project and apply them throughout the mapping process. QA and usage validation involve ensuring the reproducibility, traceability, usability and comparability of the maps. Factors that may be involved in QA include quality-assurance rules, testing (test protocols, pilot testing) and quality metrics (such as computational metrics or precisely defined cardinality, equivalence and conditionality). Clear documentation of the QA process and validation procedures is an important component of this step in the mapping process. If it is feasible to conduct a pilot test, doing so will improve the QA and validation process. Mapping is an iterative process that will improve over time as it is used in real settings. Usage validation of maps is an independent process involving users of the maps (not developers of the maps) in order to determine whether the maps are fit for purpose (e.g. whether end-users reach the correct code in the target terminology when using manual and automated maps, etc.).

¹ Further mapping guidance details are provided in the forthcoming white paper on WHO-FIC classifications and terminology mapping produced in collaboration with the WHO-FIC Network, available at: www.who.int/classifications.

Key principles for usage validation of maps include:

- a. Use a “gold standard” (i.e. a statement in the original source data – e.g. a diagnosis as written in the medical record) as the reference point.
 - b. Compare the original source data with the end results of the following two processes.
 - » Coding of original source data with a source terminology – map code(s) of source terminology to code(s) of target terminology; and
 - » Coding of original source data with target terminology.
 - c. Use a statistically significant sample size that is representative of the target terminology and its prototypical use case settings.
 - d. When performing usage validation of automated maps, always include human (i.e. manual) validation.
8. Upon publication and release, include information about release mechanisms, release cycle, versioning, source/target and licence agreement requirements, and provide a feedback mechanism for users. Dissemination of maps should also include documentation as stated above, describing the purpose, scope, limitations and methodology used to create the maps.
 9. Establish an ongoing maintenance mechanism, release cycle, types and drivers of changes, and versioning of maps. The maintenance phase should include an outline of the overall life-cycle plan for the map, conflict resolution mechanism, continuous improvement process, and decision process around when an update is required. Whenever maps are updated, the cycle of QA and validation must be repeated.
 10. When map specialists are conducting mapping manually, it is recommended to provide the necessary tools and documentation to drive consistency. Such items include: the tooling environment (workflow details and resources related to both source and target schemes); source and target browsers, if available; technical specifications (use case, scope, definitions); editorial mapping principles or rules to ensure consistency of the maps, particularly where human judgement is required; and implementation guidance. Additionally, it is best practice to provide an environment that supports dual independent authoring of maps, as this is thought to reduce bias among human map specialists. Development of a consensus management process to aid in the resolution of discrepancies and complex issues is also beneficial.
 11. In computational mapping, it is advisable to include resources to ensure consistency when building a map using a computational approach, including a description of the tooling environment, when human intervention would occur, documentation (e.g. the rules used in computerized algorithms), and implementation guidance. It is also advisable to always compute the accuracy and error rate of maps. It is important to manually verify and validate the computer-generated mapping lists. Such manual checking is necessary in the QA process, as maps that are generated automatically often contain errors. Such manually verified maps can also assist in the training of the machine-learning model when maps for different sections of terminologies are being generated sequentially.
 12. The level of equivalence between source and target entities – such as equivalent, broader, narrower – should be specified.

13. If the mapping uses cardinality as a metric, then it must be clearly defined in terms of what is being linked between source and target, how the cardinalities are counted, and the direction of the map. The cardinality of a map (one-to-one, one-to-many, many-to-one, and many-to-many), without a clear definition, however, has a very weak semantic definition, being nothing more than the numbers of source entities and target entities that are linked in the map.
14. Maps should be machine-readable to optimize their utility.
15. When creating maps using ICD-11, map into the foundation component first, then generate maps to mortality and morbidity statistics through linearization aggregation.

Annex 4

What is public key infrastructure (PKI)?

The solution discussed in this document involves applying digital signatures to information to provide a guarantee that the information has been validated by an accredited authority. The proposed method is to employ a digital certificate using a private–public key pair, a common mathematical approach for encryption and digital trust. The processes, systems, software and rules around the management of these certificates form a PKI – essentially, all the components that need to be in place for a trusted solution to work.

WHY IS A PKI NEEDED?

Various individuals and organizations, when presented with a vaccination certificate, will need to be able to verify that the certificate has come from an approved authority, and that what the document purports to be is indeed true.

For paper-based records, verification has been achieved historically by means of signatures and unique seals (e.g. stamps, holographic images, special paper), but these can be copied or forged. The electronic equivalent, making use of technology, is a digital certificate. At its simplest, the electronic equivalent can be a pair of keys: a private key and a public key. Either key can be used to digitally encrypt information in such a way that it can only be decrypted by its twin key. The private key is kept secret and protected, as the name suggests, but the public key is widely disseminated.

WHAT IS A PKI?

A system is needed to distribute public keys and to reassure the recipient that the public key has come from an accredited source (i.e. the certificate authority). This is one job of a PKI, which is a mechanism for disseminating the public keys and for following up with any revocation notices if a public key is found to be compromised. Revocation may happen, for example, if the private key is obtained by an unintended party.

In essence, the PKI binds a certificate to the identity of a particular individual or organization, so that a recipient can trust that the public key provided does reliably resolve back to the individual or organization in question.

HOW IS A PKI USED?

This property of the pair of keys for encryption or decryption (based on a one-way mathematical operation involving the factorization of large numbers) has many useful applications. Examples are:

Example 1: If I want to send a confidential message to a friend, then I can encrypt the message with his or her public key and send it out confident that only the person with the private key (my friend) will be able to read it.

Example 2: Likewise, if I want to send a message to the same friend and give him or her confidence that it could only have come from me, I can encrypt it with my private key, and my friend can then decrypt it with my public key, knowing that only someone with the private key (i.e. me) could have written it.

This second scenario is of interest for signing DDCC:VS data. It can be guaranteed that data has been approved and signed by a trusted authority if certificates are signed using private keys held by that authority and the person checking is in possession of the public key.

The keys are long alphanumeric sequences (see Fig. A4.1). There are various software tools for generating public–private key pairs.

Figure A4.1
An example key

```

---- BEGIN SSH2 PUBLIC KEY ----
    Comment: "RSA-KEY-20210528"
AAAAB3NzaC1yc2EAAAABJQAAAQEARK462NWt2/JshVHGyCIU2HzV083IHYEKeLTL
G+7EWHCK26XRRE8F/WsG7qnlWShBvbcKDTARcM8jQS4qSG1KUC09s6ZLRUT1mYF
JSB6BVBgGU/dDnsalKMMN4HR0outluzMTXnDypHrzDjXG3nqFrzFR0AtARf5aYNA1
SSZMH2Jl3BF9M29JGLV411WbMQZMMEBNRMYWMM3WCIZ826N/0LLEEFuYP8q6TBMN
msRIOalpGsTEYI2GKU/oRTxzYcP2GLY0VLE/UGoYSIEYLI3ME6DSJbMUHTxQKsCM
13GgQVewREYSLX6oL0uaUYyFHTTFF2kzCH8MWIB1IQP2z4izQw==
---- END SSH2 PUBLIC KEY ----

```

Figure A4.2
An example of a key generation tool

The screenshot shows the PuTTY Key Generator window. The 'Key' section displays a public key for pasting into an OpenSSH authorized_keys file. The key is highlighted in blue. Below the key, the key fingerprint is shown as 'ssh-rsa 2048 f6:39:2e:e6:2b:75:61:a6:10:07:4c:fa:cd:cd:af:19'. The key comment is 'rsa-key-20210701'. The 'Actions' section includes buttons for 'Generate', 'Load', 'Save public key', and 'Save private key'. The 'Parameters' section shows 'Type of key to generate' set to 'RSA' and 'Number of bits in a generated key' set to '2048'.

A digital certificate (or public key certificate) is a file that contains a public key along with extra information such as the name of the issuer and the validity dates for using the key. A standard such as X509 is used to describe the elements in such a file.

HOW DOES A PKI WORK FOR VACCINATION CERTIFICATES?

For the purposes of the DDCC:VS, the PKI is used to establish data provenance, as per example 2 above, which works as follows.

- A. A certificate authority, such as a public health authority, is nominated within a particular country, region or jurisdiction, and that certificate authority becomes the “trust anchor” responsible for issuing certificates. Trust begins at this point, and this entity has to be a recognized and authorized actor.
- B. The certificate authority doesn’t sign vaccination documents and data. The signing of vaccination documents and data is handled by other agencies, such as public health actors and other stakeholders.
- C. Therefore, the certificate authority issues private–public key pairs to these other actors in the form of document signer certificates (DSCs), providing them with the information needed to digitally sign documents.
- D. These different agencies then use the private key in their DSC to perform this signing activity. Signing involves encrypting the information using the private key so it is rendered into a format that is not human-readable.
- E. Any electronic information can be signed in this way. The health certificate identifier (HCID) could be signed, a representation of the whole vaccination record could be signed, or some other combination of information, as determined by the certificate authority, could be signed.
- F. An interested party (i.e. a Verifier) who wants to decrypt the encrypted information for the vaccination certificate must have two key things.
 - » The public key corresponding to the private key in the DSC; and
 - » Trust that the public key, from the DSC, came from a certificate authority that the interested party trusts.
- G. To facilitate the two points in (F), a certificate authority usually sets up an online service for this purpose. The Verifier can interrogate the service and:
 - » Ask for the public key if it does not have it. The Verifier can provide the HCID and check that the authority has that HCID in its records and that the HCID is linked to a valid public key. This is the role of the DDCC:VS Registry Service in this paper.
 - » Once the Verifier has the public key, it can also check with the authority that the public key is valid and has not been revoked.

- H. Finally, now that the Verifier knows that the public key came from a trusted source, the Verifier can decrypt whatever information has been provided for the vaccination certificate. If the decryption reveals the data, the Verifier can be confident that:
- » the information could only have been encrypted by someone with the private key, therefore it must have come from someone in possession of the DSC;
 - » the information has not been altered or tampered with after it was signed, otherwise the decryption would not work; and
 - » the information can be trusted, because the Verifier trusts the certificate authority, and trusts the certificate authority to have issued the DSC, which must have been used to encrypt the information.
- I. If the public key decrypts the encrypted information so that it looks identical to the unencrypted version provided, the Verifier can be confident that only the entity in possession of the private key sent these data, and that it has not been altered since by any other party.
- » For the vaccination certificates, the HCID must resolve back to a digital record that is digitally signed in the manner described.
 - » Optionally, the DDCC:VS core data set could also be encoded into a barcode to enable the Verifier to perform an offline check, but the Verifier would still need to be able to validate that the public key was a valid one.

A PKI is only as secure as the IT infrastructure on which it is implemented; although PKI gives a high degree of trust, care must be taken to design and run the system in a manner that maintains security.

Annex 5

Non-functional requirements

This section contains a suggested set of generic non-functional requirements (see Table A5.1). Along with the functional requirements in [sections 3.3](#) and [4.3](#), these non-functional requirements can be adapted when specifying a digital solution for the scenarios in this paper. Non-functional requirements explain the conditions under which any digital solution must remain effective and are organized into the following categories.

- **ACCESSIBILITY:** The provision of flexibility to accommodate each user's needs and preferences, along with appropriate measures to ensure access to persons with disabilities on an equal basis with others; for example, the solution should still be accessible to those with visual impairment.
- **AVAILABILITY (SERVICE LEVEL AGREEMENTS; SLAs):** The definition of when the system will be available to the user community, how such metrics will be measured, and the functionality in the tool for managing planned downtime.
- **CAPACITY – CURRENT AND FORECAST:** The number of concurrent users that can interact with the system without an unacceptable degradation in performance, speed or responsiveness. User populations are never static, and so the ability to handle current typical and peak volumes of usage and predicted future states, and the strategy for handling a traffic surge, must be considered.
- **UPTIME SLAs – DISASTER RECOVERY, BUSINESS CONTINUITY, RESILIENCE:** The requirements for the system in terms of how it recovers from critical, unexpected failure and the support for business continuity. This includes time to recovery, how recovery is established, and at what levels resilience and redundancy are built into the system to minimize any data loss.
- **PERFORMANCE/RESPONSE TIME:** The speed with which the system is expected to respond under normal and exceptional loads, with a definition of what those terms mean.
- **PLATFORM COMPATIBILITY:** The different operating systems, machines and configuration on which the solution is expected to run.
- **SECURITY AND PRIVACY:** The levels of security that the solution must provide in terms of user authentication and data protection.
- **REGULATION AND COMPLIANCE:** Any regulatory/legal constraints with which the system must comply, such as data protection policies, WHO cloud policies, and information management and retention rules of the jurisdiction(s) in which the solution will run.
- **RELIABILITY:** A measure of the reliability of the tool, for example the acceptable mean time between failures of the solution (both hardware and software components).
- **SCALABILITY (HORIZONTAL, VERTICAL):** The ability to, and strategy for, handling an increasing load on the solution (in terms of increased number of users it can support, higher volumes of data it can handle, quicker performance and response, etc.). A solution can be scaled either horizontally (adding more elements to the solution, such as extra load-balanced servers) or vertically (adding extra capacity in existing elements, such as upgrading an existing server).
- **SUPPORTABILITY:** The requirements for engineers to detect, diagnose, resolve and monitor any issues and faults that arise while the solution is being used. This covers the features/functions that will be built into the system to facilitate technical support work.

- **USABILITY BY TARGET USER COMMUNITY:** The extent to which a product can be used by specified users to achieve specified goals with effectiveness, efficiency and satisfaction in a specified context of use. This includes optimization of the interface for clarity and efficiency, and ensuring that the solution is appropriate to the needs and the experience level and expectations of the target users.
- **DATA RETENTION/ARCHIVING:** Requirements relating to how information will be archived from its normal location and then retained, including the frequency, the approval process and any process for restoring information from the archive.

Table A5.1
Non-functional requirements for the DDCC:VS

Requirement ID	Category	Non-functional requirement
DDCC.NFXNREQ.001	Accessibility	Any solution SHALL provide optimization for delivery to users with low bandwidth, as in a low digital maturity setting users will often have limited (or intermittent) Internet connectivity.
DDCC.NFXNREQ.002	Accessibility	Any solution SHOULD provide offline availability that permits a user to continue to work with data while offline, such as by creating a set of requests to be sent when next online.
DDCC.NFXNREQ.003	Accessibility	Any solution SHALL provide a mechanism for the resynchronization/dispatch of data created offline when the solution is reconnected.
DDCC.NFXNREQ.004	Accessibility	Any solution SHOULD follow best practice to deliver interfaces that are clear, intuitive and consistent (standardized colour schemes, icons, placement of visual elements – titles, buttons, filters, navigation, etc.)
DDCC.NFXNREQ.005	Accessibility	Any solution SHOULD follow best practice to deliver interfaces that are accessible by the widest range of users, including considerations for different cultures (e.g. left-to-right and right-to-left scripts), visual impairment (e.g. colour blindness) and physical disability (e.g. the need to interact using one hand).
DDCC.NFXNREQ.006	Accessibility	Any solution SHOULD automatically optimize its interface (layout of elements, organization of information, etc.) to adapt to the device on which it is being used, so that it is accessible on personal computers (desktops, laptops), tablets and smartphones using principles of adaptive design.
DDCC.NFXNREQ.007	Availability	Any solution developed SHOULD NOT be able to accept more than 10 minutes of outage during normal usage and cannot accept more than 1 minute of data loss of queries and responses.
DDCC.NFXNREQ.008	Availability	It MAY be possible to provide an indication of the availability status of any solution so that users can check the system's "health". The same functionality MAY also notify of any planned downtime, retired functionality, release notes, etc.
DDCC.NFXNREQ.009	Capacity – current and forecast	The system SHALL be able to support the potentially large number of concurrent users performing read and write operations during normal operation. This metric will vary significantly between different country contexts and will depend on the design, but should be used as the anticipated capacity standard.
DDCC.NFXNREQ.010	Capacity, current and forecast	During periods of peak usage, system traffic MAY surge the number of concurrent users performing read and write operations.
DDCC.NFXNREQ.011	Capacity, current and forecast	Forecast growth of the user base is anticipated to be high. As a safety contingency, the system SHOULD support, or have scaling plans to support, growth of 25% per year.
DDCC.NFXNREQ.012	Disaster recovery, business continuity, resilience	All data and derived analysis SHALL be stored within an appropriate data architecture to ensure redundancy and rapid disaster recovery, to eliminate the risk of data loss.
DDCC.NFXNREQ.013	Disaster recovery, business continuity,	The system SHOULD provide near-instantaneous switch-over if any one component of the system architecture fails critically (database server, web server, system

resilience

monitoring job, service bus, etc.).

Requirement ID	Category	Non-functional requirement
DDCC.NFXNREQ.014	Disaster recovery, business continuity, resilience	The system SHOULD provide near-instantaneous switch-over if any one component of the physical architecture fails critically (data centre destroyed, server destroyed, etc.)
DDCC.NFXNREQ.015	Disaster recovery, business continuity, resilience	All components of the solution SHOULD be underpinned by robust monitoring tools that track usage across space and time, so that system load and source can be queried.
DDCC.NFXNREQ.016	Disaster recovery, business continuity, resilience	Data concerning system usage SHOULD be available to system administrators via a dashboard to show current load, and recent load (last week, last month), and be able to perform custom queries by place and time. It SHOULD be possible to export this data.
DDCC.NFXNREQ.017	Disaster recovery, business continuity, resilience	It SHALL be possible to automatically log any periods of outage of the system and to supplement and update this record manually.
DDCC.NFXNREQ.018	Disaster recovery, business continuity, resilience	It SHALL be possible to trigger system alerts based on uptime and performance.
DDCC.NFXNREQ.019	Disaster recovery, business continuity, resilience	It SHOULD be possible to use system alerts to perform actions such as dispatch of a warning email/SMS to a system administrator or to execute a script that (for example) spins up a new virtual machine for load balancing.
DDCC.NFXNREQ.020	Performance/ response time	The solution SHALL follow best practices to deliver a responsive interface in which typical requests can be served (end-to-end interaction) in a maximum time specified in a number of seconds to be determined based on typical bandwidths. Degradation to a greater maximum time in number of seconds for limited-bandwidth scenarios is acceptable.
DDCC.NFXNREQ.021	Performance/ response time	The solution SHOULD be designed so that degradation of performance due to increased load (surge of users) is minimized.
DDCC.NFXNREQ.022	Performance/ response time	Where appropriate, long-running processes such as complex queries MAY be available for asynchronous execution, to allow a user to continue to interact with the system while the job executes and to receive a notification when the work is complete.
DDCC.NFXNREQ.023	Performance/ response time	The system MAY implement detection of a frozen (“hung”) interface to give the user the option to cancel a current request.
DDCC.NFXNREQ.024	Performance/ response time	The system SHOULD collect metrics on performance and response time to allow a system administrator to monitor system behaviour, identify bottlenecks or issues, and pro-actively address any risk of unacceptable degradation of speed.
DDCC.NFXNREQ.025	Performance/ response time	As with system availability, the solution SHALL provide dashboards of performance metrics, allow querying of the performance log and export of performance data for reports.
DDCC.NFXNREQ.026	Performance/ response time	As with system availability, the solution SHALL have the ability to set thresholds on performance and use the breach of those thresholds to raise alerts that can trigger email notifications or automated system actions (bring an extra server into a load- balanced set, for example).
DDCC.NFXNREQ.027	Security and privacy	Tools to request an account, log in, log out, set and change passwords, and receive password reminders SHALL be provided.
DDCC.NFXNREQ.028	Security and privacy	All interactions between a client and a server component of the solution SHALL be securely encrypted to prevent “man in the middle” interference with data in transit.
DDCC.NFXNREQ.029	Security and privacy	Any cloud components of the solution SHALL store their cloud data-at-rest in an encrypted format.
DDCC.NFXNREQ.030	Security and privacy	The solution SHALL have a security model that is robust and flexible and controls both access to data and the operations that can be executed against data.

Requirement ID	Category	Non-functional requirement
DDCC.NFXNREQ.031	Security and privacy	Information about the governance and restricted use of data SHOULD be available within any solution alongside the data concerned, so that users have a clear and consistent reminder of the level of confidentiality, sensitivity and the permitted use of the data they are currently viewing.
DDCC.NFXNREQ.032	Security and privacy	Dashboards, reports, standard queries and exports of security information SHOULD be provided to assist system administrators in the management of access permissions. Queries to highlight conflicting permissions SHOULD be available.
DDCC.NFXNREQ.033	Security and privacy	The confidentiality of data must be managed with utmost care. In shared data environments, there SHALL be a clear separation of between the system's data and any other hosted clients' information. Dedicated hosting and data sources are preferred.
DDCC.NFXNREQ.034	Regulation and compliance	Any solution SHOULD be designed to be mindful of existing reference architecture guidelines and standards for distributed trust framework solutions and tools for exchanging vaccination data.
DDCC.NFXNREQ.035	Regulation and compliance	Any solution SHALL be compliant with any data policies and legal requirements identified by the country in whose jurisdiction the solution will operate.
DDCC.NFXNREQ.036	Regulation and compliance	It MAY be possible to tag data sets with any regulation and compliance information relevant to them so that this is readily available with the data set. Such information might include the data provider, intended purpose of the data, restrictions on the use of the data, and restrictions on where data can be stored.
DDCC.NFXNREQ.037	Regulation and compliance	Any solution SHALL be compliant with any data storage, retention and destruction laws mandated by the data policies and data laws of the countries in which data are located.
DDCC.NFXNREQ.038	Reliability	Any solution SHOULD be designed to maximize the mean time between failures, with appropriate best practice to deliver a robust, well-tested and reliable platform.
DDCC.NFXNREQ.039	Reliability	Any solution SHOULD provide a log, in which failures in any part of the system are logged, so that mean time between failures can be calculated and tracked.
DDCC.NFXNREQ.040	Scalability	Any solution SHOULD be designed so that elements can be scaled horizontally by, for example, adding extra resources (more servers, extra virtual machines, etc.) and the mechanisms for coordinating their activity (load balancing, session management, etc.)
DDCC.NFXNREQ.041	Scalability	Any solution SHOULD be designed so that elements can be scaled vertically by, for example, adding extra capacity to solution elements (increased CPU, increased RAM, etc.)
DDCC.NFXNREQ.042	Scalability	It MAY be possible to configure rules for automatic horizontal scaling of the system to respond to increased load (e.g. spinning up a new virtual machine and adding it to a load-balanced pool of resources). Rules will be based on thresholds for system load and performance.
DDCC.NFXNREQ.043	Scalability	Any solution SHOULD log sufficient information about performance and load so that technical staff can refine the system's scaling strategy based on actual usage.
DDCC.NFXNREQ.044	Supportability	Any solution SHOULD provide a feedback channel as described in functional requirements for collecting information and support requests.
DDCC.NFXNREQ.045	Supportability	Any solution MAY provide access to learning material to support a user's understanding of how to use the tool and achieve specific aims.
DDCC.NFXNREQ.046	Supportability	The solution SHALL include a system log of activity in which events of interest, the time and date when they occur, their categorization, and the user (if appropriate) who triggered the event are recorded. The log must be of sufficient detail to assist technical staff with debugging issues.

Requirement ID	Category	Non-functional requirement
DDCC.NFXNREQ.047	Supportability	It MAY be possible to configure system logging in a verbose and a standard format. Verbose format will be used for periods of testing or bug fixing, and standard for production use of a stable system in which smaller log size is prioritized over a high level of detail.
DDCC.NFXNREQ.048	Supportability	It SHOULD be possible for technical support staff to filter and query system logs to quickly identify sections of interest.
DDCC.NFXNREQ.049	Supportability	It MAY be possible to trigger alerts from the creation of predefined log entries (e.g. an error, warning, failure). Alerts can be used to take actions such as email dispatch.
DDCC.NFXNREQ.050	Supportability	Any solution SHALL have a published strategy for the release of patches, maintenance releases and version upgrades.
DDCC.NFXNREQ.051	Usability	Any interface created SHOULD be mindful of best practices for user design/adaptive design to ensure the best chance of presenting a clear and concise, and intuitive user experience. This is particularly important for any interface dealing with data entry.
DDCC.NFXNREQ.052	Usability	It SHOULD be possible to deliver definition/explanation text in the language currently selected for the interface via the solution, so that acronyms, jargon, technical terms, etc. can be clarified where necessary.
DDCC.NFXNREQ.053	Usability	The user interface MAY be designed so that navigation via keyboard (tab movement between fields, use of shortcut keys) is possible if the user does not have access to a pointer device.
DDCC.NFXNREQ.054	Usability	When the solution adapts for display on a smartphone/tablet, the interface SHALL be designed mindful of touch-screen interaction.
DDCC.NFXNREQ.055	Usability	The solution MAY provide an efficient and easy way to manage taxonomy (for administrator-users) to record standard definitions, relationships between terms, etc.
DDCC.NFXNREQ.056	Data retention/archiving	It SHOULD be possible to manually request an archive of a selected subset of information.
DDCC.NFXNREQ.057	Data retention/archiving	It MAY be possible to schedule the archiving of a selected subset of information and to set a recurrence for this operation. The archive operation will execute when the scheduled date and time arrives.
DDCC.NFXNREQ.058	Data retention/archiving	It MAY be possible to trigger a notification alert when an archive operation completes (including success and failure reports).
DDCC.NFXNREQ.059	Data retention/archiving	Any archive function SHALL not affect the performance of the system.
DDCC.NFXNREQ.060	Data retention/archiving	Any archive material SHOULD be labelled with metadata about the information it contains and the date and time it was created, to facilitate quick navigation of all archived material.
DDCC.NFXNREQ.061	Data retention/archiving	It SHOULD be possible, with the necessary authority and permissions, to restore information from a chosen archive back into the operational set of information.
DDCC.NFXNREQ.062	Data retention/archiving	All archival operations SHALL be logged.
DDCC.NFXNREQ.063	Data retention/archiving	It SHOULD be possible, with the necessary authority and permissions, to perform a limited search of the contents of archives to identify information of interest.
DDCC.NFXNREQ.064	Data retention/archiving	All information written to archives SHALL be in an encrypted format to prevent misuse if accessed by an unauthorized system or person.

CPU, central processing unit; RAM, random-access memory.

Annex 6

Open Health Information Exchange (OpenHIE)-based architectural blueprint

This section illustrates how a standards-based health-data-sharing infrastructure could support point-of-care digital health solutions. If digital health solutions are employed in real time during the vaccine administration event, it is anticipated that complementary digital health infrastructure, such as the architectural elements described by the OpenHIE specification, could be leveraged.

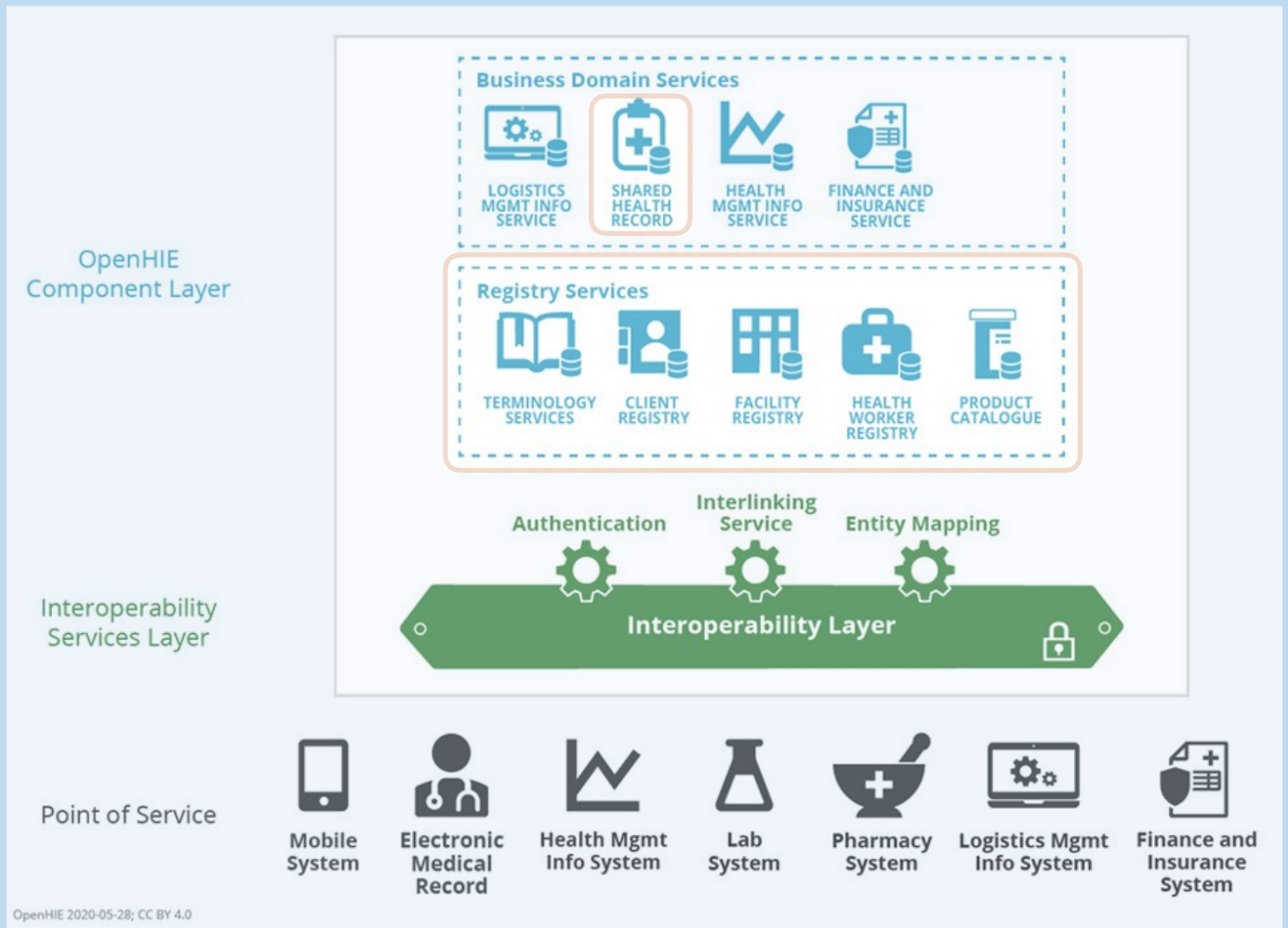
OpenHIE describes a reusable architectural framework that leverages health information standards, enables flexible implementation by country partners, and supports exchange of individual components. OpenHIE also serves as a global community of practice to support countries towards “open and collaborative development and support of country-driven, large-scale health information sharing architectures”¹

The OpenHIE high-level architecture² is shown in Fig. A6.1. To show how a health-data-sharing infrastructure could support point-of-care digital health solutions to issue Digital Documentation of COVID-19 Certificates: Vaccination Status (DDCC:VS), a set of digital health interactions are described in terms of the conformance-testable Integrating the Healthcare Enterprise (IHE) specifications referenced by the OpenHIE specification.

1 OpenHIE. In: OpenHIE [website]. OpenHIE; no date (<https://ohie.org/about>, accessed 29 June 2021)²

2 OpenHIE Architecture Specification. OpenHIE; September 2020 (<https://ohie.org/wp-content/uploads/2020/12/OpenHIE-Specification-Release-3.0.pdf>, accessed 29 June 2021).

Figure A6.1
OpenHIE architecture¹



¹ Orange boxes indicate registries and repositories relevant to DDCC:VS.

The registries and repositories defined in the OpenHIE architecture (see Fig. A6.1) may play a role in providing data that are part of the DDCC:VS core data set defined in [section 5](#). These registries and repositories include the following:

TERMINOLOGY SERVICES: A registry service used to manage clinical and health system terminologies, which health applications can use for mapping to other standard or non-standard code systems to support semantic interoperability. For example, a terminology service can be used to manage terminology mappings of existing code systems to the International Classification of Diseases, 11th revision (ICD-11).

CLIENT REGISTRY: Also referred to as a patient registry, a demographic database that contains definitive information about each Subject of Care. This database can include a Subject of Care's name, date of birth, sex, address, phone number, email address, as well as other person-specific information such as parent-child relationships, caregiver relationships, family-clinician relationships and consent directives. It is also in the client registry that the list of unique identifiers (IDs; e.g. national ID, national health ID, health insurance ID) for a particular Subject of Care can be found. The data elements in the DDCC:VS core data set that may be populated with data from the client registry include:

- name
- date of birth
- sex
- unique IDs.

FACILITY REGISTRY: A database of facility information, including data such as the facility name, a Public Health Authority (PHA)-issued unique ID, the organization under whose responsibility the facility operates, location (by address and/or Global Positioning System [GPS] coordinates), facility type, hours of operation, and the health services offered. The data elements in the DDCC:VS core data set that may be populated with data from the facility registry include:

- administering centre: facility name or unique ID can be used to represent this
- country of vaccination.

HEALTH WORKER REGISTRY: A database of health worker information that contains information such as name, date of birth, and qualifications of health workers (including cadre, accreditations and authorizations of practice). The health worker registry also references unique health worker IDs that may have been issued by a PHA, care delivery organizations or individual health facilities. The data element in the DDCC:VS core data set that may be provided with information from the health worker registry is:

- health worker ID.

PRODUCT CATALOGUE: A system used to manage the metadata and multiple IDs for medical commodities. Depending on whether the product catalogue includes vaccine products, the data elements in the DDCC:VS core data set that could be obtained from the product catalogue are:

- vaccine or prophylaxis
- vaccine brand
- vaccine manufacturer
- vaccine market authorization holder
- vaccine batch number
- disease or agent targeted.

SHARED HEALTH RECORD (SHR): A repository that may be used to maintain longitudinal health information about a Subject of Care and to support continuity of care over time, across different care delivery sites. Health data in the SHR can include content such as the Subject of Care's medication list, allergies, current problem list, immunization records, history of procedures, medical devices, diagnostic results, vital sign observation record, history of illness, history of pregnancies and current pregnancy status, care plan and advance directives. Such health data may be expressed using health data content standards such as the Health Level Seven (HL7) Fast Healthcare Interoperability Resources (FHIR) International Patient Summary (IPS) specification. Data in the SHR can be important for delivering guideline-based care during vaccine administration. Furthermore, data generated during vaccination administration could be added to the SHR, if in use, in order to support future provision of health services.

