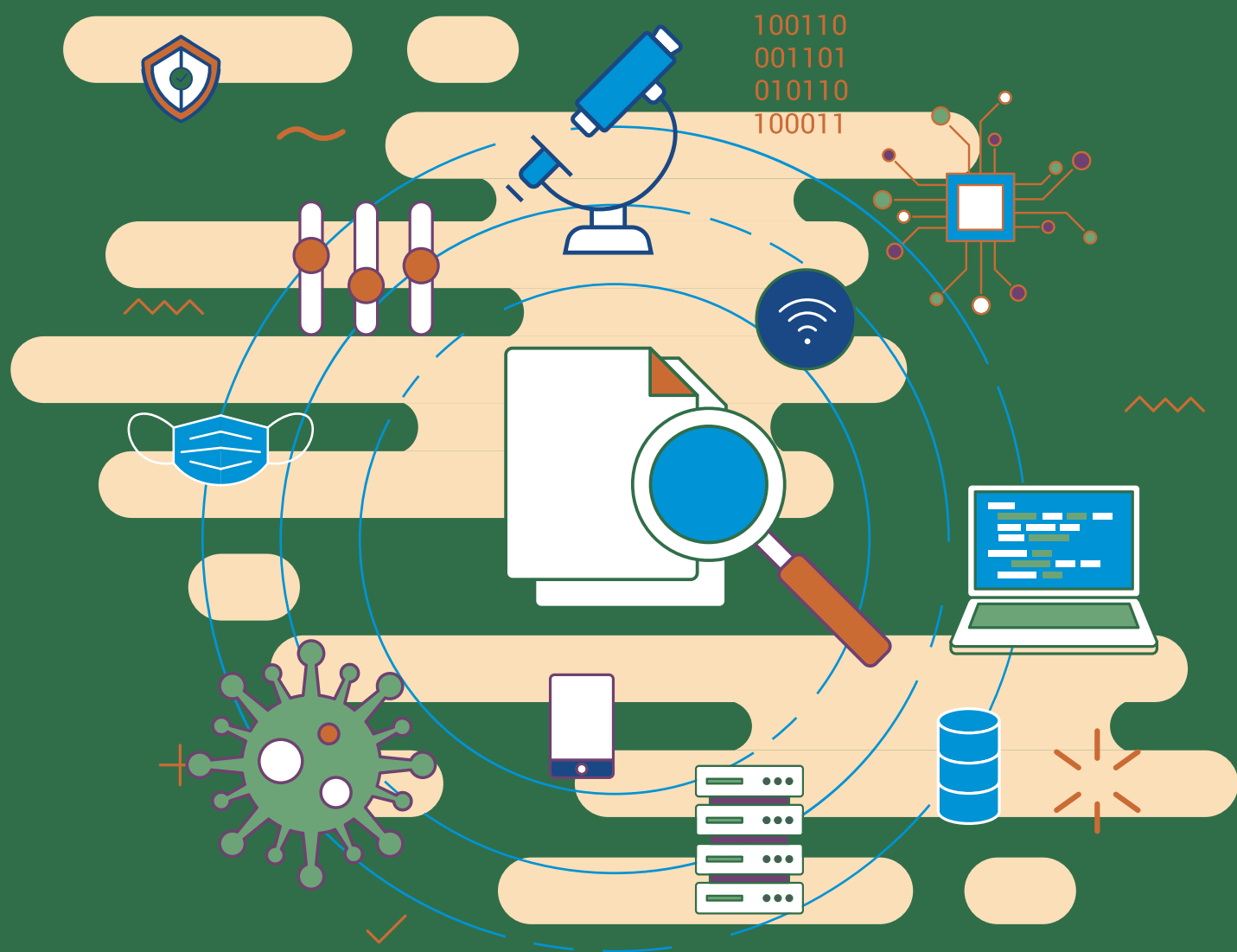


# Digital Documentation of COVID-19 Certificates: Test Result

## TECHNICAL SPECIFICATIONS AND IMPLEMENTATION GUIDANCE

31 March 2022





# Digital Documentation of COVID-19 Certificates: **Test Result**

## **TECHNICAL SPECIFICATIONS AND IMPLEMENTATION GUIDANCE**

31 March 2022

**Digital Documentation of COVID-19 Certificates: Test Result - Technical Specifications and Implementation Guidance, 31 March 2022.**

WHO/2019-nCoV/Digital\_certificates\_diagnostic\_test\_results/2022.1

© World Health Organization 2022

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: Test Result - Technical Specifications and Implementation Guidance, 31 March 2022. Geneva: World Health Organization; 2022 (WHO/2019-nCoV/Digital\_certificates\_diagnostic\_test\_results/2022.1). 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.

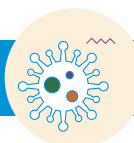
The mention of specific companies or of certain manufacturers' products does not imply that they are endorsed or recommended by WHO in preference to others of a similar nature that are not mentioned. Errors and omissions excepted; the names of proprietary products are distinguished by initial capital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

Design and layout: RRD Design LLC

# Contents

Acknowledgements	iii
Abbreviations	iv
Glossary	v



## Executive summary

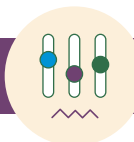
ix



## 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	6



## SECTION 2 Ethical considerations and data protection principles

7

2.1. Ethical considerations for a DDCC:TR	7
2.2. Data protection principles for a DDCC:TR	12
2.3. DDCC:TR design criteria	15



## SECTION 3 Test result certificate generation

17




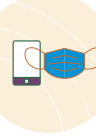

3.1. Key settings, personas and digital services	18
3.2. Certificate generation workflow	19
3.3. Functional requirements for certificate generation	21



## SECTION 4 Test result certificate verification and validation

24

4.1. Proof scenarios	24
4.2. Key settings, personas and digital services	25
4.3. Test result certificate verification and validation workflows and use cases	26
4.4. Functional requirements for test result certificate verification and validation	35

	<b>SECTION 5 DDCC:TR core data set</b>	<b>38</b>
	5.1. Core data set principles	38
	5.2. Core data elements	40
	<b>SECTION 6 Public key infrastructure for signing and verifying a DDCC:TR</b>	<b>43</b>
	6.1. Signing a DDCC:TR	45
	6.2. Verifying a DDCC:TR signature	46
	6.3. Trusting a DDCC:TR signature	47
	<b>SECTION 7 National governance considerations</b>	<b>48</b>
	<b>SECTION 8 Implementation considerations for a DDCC:TR solution</b>	<b>51</b>
	8.1. Considerations before deploying	51
	8.2. Key factors to consider with solution developers	54
	8.3. Cost category considerations	55
	8.4. Additional resources to support implementation	57
	References	58
	<b>Annexes</b>	<b>61</b>
	Annex 1 Business process symbols used in workflows	62
	Annex 2 Guiding principles for mapping the WHO Family of International Classifications (WHO-FIC) and other classifications	63
	Annex 3 Public key infrastructure	66
	Annex 4 Non-functional requirements	70
	Annex 5 Open Health Information Exchange (OpenHIE)-based architectural blueprint	75
	Web Annex A DDCC:TR Core data dictionary	
	<a href="https://apps.who.int/iris/bitstream/handle/10665/352585/WHO-2019-nCoV-Digital-certificates-diagnostic-test-results-data-dictionary-2022.1-enq.xlsx">https://apps.who.int/iris/bitstream/handle/10665/352585/WHO-2019-nCoV-Digital-certificates-diagnostic-test-results-data-dictionary-2022.1-enq.xlsx</a>	

## 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 Carl Leitner, Garrett Mehl, Akshita Palliwal, Natschja Ratanaprayul and Derek Ritz of the WHO Department of Digital Health and Innovation, in collaboration with individuals in departments across WHO and other organizations, who include: Carmen Dolea, Fernando Gonzalez-Martin and Magdalena Rabini of the International Health Regulations Secretariat; Sara Barragan Montes, Ninglan Wang and Anne Dlugosz of the WHO Department of Country Readiness Strengthening; Mark Perkins and Karin Von Eije of the WHO Department of Emerging Diseases and Zoonoses; 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; Ute Ströher of the WHO Department of Regulation and Prequalification; Wouter 'T Hoen of the WHO Department of Human Resources and Talent Management; Robert Jakob and Nenad Kostanjsek of the WHO Department of Data and Analytics; Jenny Thompson and Luke Duncan of PATH; and Voo Teck Chuan of the National University of Singapore.

The following individuals (listed in alphabetical order) reviewed, provided feedback on and contributed to this document at various stages: Joseph Amlung (Regenstrief Institute), Roberta Andraghetti (Pan American Health Organization [PAHO]), David Baorto (Regenstrief Institute), Joaquin Andres Blaya (World Bank), Jim Case (SNOMED International), Gabriel Catan (World Bank), Adam Cooper (World Bank), Angus Dawson (University of Sydney), Christiane DerMarkar (International Civil Aviation Organization [ICAO]), Vyjayanti T Desai (World Bank), Marie Eichholtzer (World Bank), Ioana-Maria Gligor (European Commission, Directorate-General for Health and Food Safety), Marelize Gorgens (World Bank), Lionel Gresh (PAHO), Monica Harry (SNOMED International), Mathew Thomas Hulse (World Bank), Konstantin Hyppönen (European Commission, Directorate-General for Health and Food Safety), Carlos Machado (European Commission, Directorate-General for Health and Food Safety), Jonathan Marskell (World Bank), Riki Merrick (Association of Public Health Laboratories), Jane Miller (SNOMED International), Toni Morrison (SNOMED International), R Rajeshkumar (ICAO), Eric Ramirez (The Palladium Group), Suzy Roy (SNOMED International), David Satola (World Bank), Maxwell J Smith (University of Toronto), Lorenzo Subissi (WHO), and Nina Rehn-Mendoza (Public Health Agency of Sweden).

WHO extends sincere thanks to the following individuals (listed in alphabetical order), who contributed to the technical consultation process: Brian Anderson (MITRE), Rabe Elshesheny (WHO), Adi V Gundlapalli (United States Centers for Disease Control and Prevention), Alexander Klosovsky (International Organization for Migration), Barry Lim (Singapore Government Technology Agency, Digital Services), Jairo Mendez-Rico (PAHO), Rajeesh Menon (eGovernments Foundation, India), Mohamed Nour (WHO), Vanja Pacic (WHO Regional Office for Europe), Ester Sikare (United States Centers for Disease Control and Prevention), and Stefanie Weber (Federal Institute for Drugs and Medical Devices, Germany).

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

## Abbreviations

<b>1D</b>	one-dimensional
<b>2D</b>	two-dimensional
<b>AG-RDT</b>	antigen detection rapid diagnostic test
<b>COVID-19</b>	coronavirus disease caused by SARS-CoV-2 virus
<b>DDCC</b>	Digital Documentation of COVID-19 Certificates
<b>DDCC:TR</b>	Digital Documentation of COVID-19 Certificates: Test Result
<b>DDCC:VS</b>	Digital Documentation of COVID-19 Certificates: Vaccination Status
<b>DSC</b>	document signer certificate
<b>EU</b>	European Union
<b>FHIR</b>	Fast Healthcare Interoperability Resources
<b>HCID</b>	health certificate identifier
<b>HL7</b>	Health Level Seven
<b>ICAO</b>	International Civil Aviation Organization
<b>ICD</b>	International Classification of Diseases
<b>ICHI</b>	International Classification of Health Interventions
<b>ID</b>	identifier
<b>IHR</b>	International Health Regulations (2005)
<b>IPS</b>	international patient summary
<b>ISO</b>	International Organization for Standardization
<b>LIS</b>	laboratory information system
<b>NAAT</b>	nucleic acid amplification test
<b>OPENHIE</b>	Open Health Information Exchange
<b>PHA</b>	public health authority
<b>PKD</b>	public key directory
<b>PKI</b>	public key infrastructure
<b>QA</b>	quality assurance
<b>SARS-CoV-2</b>	severe acute respiratory syndrome coronavirus 2
<b>SLA</b>	service-level agreement
<b>VDS-NC</b>	visible digital seals for non-constrained environments
<b>WHO</b>	World Health Organization
<b>WHO-FIC</b>	WHO Family of International Classifications



## Glossary

**ANTIGEN DETECTION RAPID DIAGNOSTIC TEST (AG-RDT):** Directly detects viral protein antigens of SARS-CoV-2, the virus that causes COVID-19, in respiratory samples using a lateral flow immunoassay.

**CERTIFICATE:** A document attesting a fact. In the context of the test result certificate, it attests to the fact that a SARS-CoV-2 diagnostic test has been conducted and the test result has been provided to an individual.

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

**DATA CONTROLLER:** The person or entity that, alone or jointly with others, determines the purposes and means of 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 or not by automated means, 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 Tested Person or the DDCC:TR Holder if the DDCC:TR Holder represents a Tested Person such as a minor child, or represents a person who is physically or legally incapable of giving consent for the processing of personal data.

**DDCC GENERATION SERVICE:** The service that is responsible for generating a digitally signed representation, the DDCC, of the information concerning a test for SARS-CoV-2. This service can be used to generate both vaccination status (DDCC:VS) and test result (DDCC:TR) certificates.

**DDCC REGISTRY SERVICE:** The service that can be used to request and receive metadata associated with a DDCC. This service can be used for both vaccination status and test result certificates.

**DDCC REPOSITORY SERVICE:** A potentially federated service that serves as a repository, or database, of the health content associated with DDCC. This service can be used as a repository for both vaccination status and test result certificates.

**DIGITAL DIVIDE:** The gap between demographic groups and regions that have access to modern information and communications technology (ICT) and those that do not or that have restricted access.

**DIGITAL DOCUMENTATION OF COVID-19 CERTIFICATES (DDCC):** A digitally signed Health Level Seven (HL7) Fast Healthcare Interoperability Resources (FHIR) document that contains the core data set content for the relevant COVID-19 certificate.

**DIGITAL DOCUMENTATION OF COVID-19 CERTIFICATES: TEST RESULT (DDCC:TR):** A type of DDCC that is used to represent the SARS-CoV-2 diagnostic test result(s) of an individual. Specifically, the DDCC:TR is a digitally signed HL7 FHIR document containing the data elements included in the DDCC:TR core data set.

**DIGITAL HEALTH SOLUTION:** A secure system that is used to capture and/or manage a digital record of the DDCC:TR core data elements, such as a laboratory information system (LIS).

**DIGITAL REPRESENTATION:** A virtual representation of a physical object or system. In this context, the digital representation must be a digitally signed HL7 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 test, signed with a private key from a public-private key pair using standard encryption techniques.

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

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

**HEALTH CERTIFICATE IDENTIFIER (HCID):** An alphanumeric identifier (ID) for a physical paper and/or digital health folder that contains one or more test or vaccination events and associated certificates for a person. Each test event corresponds to a DDCC:TR. Each vaccination event corresponds to a DDCC:VS. It is at the discretion of the Member State to determine whether the HCID will be associated with a single event or multiple events. A Member State may determine, as per its policy, that there may be only one DDCC that corresponds to an HCID.

**HEALTH DATA:** Personal data related to the physical or mental health of a natural, or legal, person, including about the provision of health services, which reveal information about that person’s 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 a person, for example a passport or a national identity card.

**IDENTIFIER (ID):** A name that labels the identity of an object or individual. For example, it can be a unique alphanumeric string that is associated with an individual, such as a passport number or medical record ID. Other types of identifier include a document identifier, a facility identifier and a health worker identifier.

**LABORATORY INFORMATION SYSTEM (LIS):** Sometimes also referred to as a laboratory information management system, this is a software system that supports laboratory activities. Key functionality includes receiving and storing test results and requests for tests. Test results can be made available via paper reports and/or electronic formats, both to human users and to other health information systems (e.g. electronic medical record systems, billing systems).

**MAY:** MAY (in upper case) is used to describe technical features and functions that are optional. It is the implementer's decision whether to include that feature or function based on the implementation context.<sup>1</sup>

**NUCLEIC ACID AMPLIFICATION TEST (NAAT):** A type of viral diagnostic test for SARS-CoV-2. NAATs detect genetic material (i.e. nucleic acids) with high sensitivity and specificity and are usually the reference method (i.e. gold standard) for SARS-CoV-2 detection. There are multiple NAATs available to detect SARS-CoV-2 that have small variances in performance and larger variances in the ease of use of the test system.

**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.

**PAPER TEST RESULT CERTIFICATE:** A test result certificate that is either handwritten or printed on paper, with a barcode. This barcode can be generated in real time or preprinted directly onto the certificate or on a barcode sticker.

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

**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; and any expression of opinion about the individual, such as assessments of that person's health status and/or specific needs.

**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.

**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 and exchange of keys.

**SHALL:** SHALL (in upper case) is used to describe technical features and functions that are mandatory for this specification.<sup>2</sup>

**SHOULD:** SHOULD (in upper case) is used to describe technical features and functions that are recommended but are not mandatory. It is the implementer's decision on whether to include that feature or function based on the implementation context and policies of the implementing Member State. However, the implementer is strongly recommended to review the reasons for not following the recommendations before deviating from the technical specifications outlined.<sup>2</sup>

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).

2 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).

**TEST REPORT:** The record, or report, of a SARS-CoV-2 diagnostic test result. A test report contains key demographic information about the Tested Person, the laboratory or testing centre that conducted the test, the test results, and other details needed for clinical use. Test reports differ from “test certificates” in that test reports do not contain means of cryptographically verifying the contents of the report.

**TEST RESULT CERTIFICATE:** A document that attests to the fact that an individual has been tested for SARS-CoV-2, and attests to the result of that SARS-CoV-2 diagnostic test.

**TESTED PERSON:** The person who is tested for SARS-CoV-2.

**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.

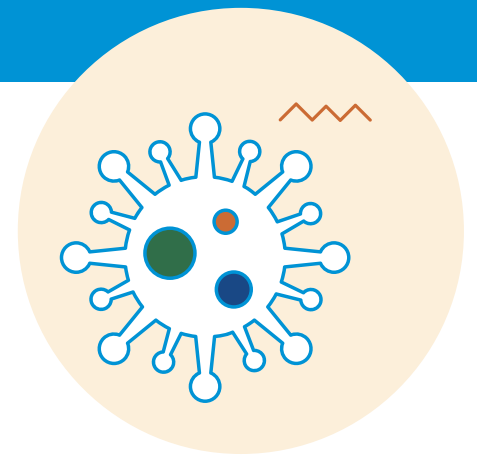
**TWO-DIMENSIONAL (2D) BARCODE:** Also called a matrix code. A 2D representation of information using individual black dots within a square or rectangle. For example, a QR code is a 2D barcode. A 2D barcode is similar to a 1D barcode, but it can represent more data per unit area.

**VALIDATION:** A process that relies on the Verifier validating and accepting the test result certificate based on the acceptance criteria and associated validity period, as determined by the policies of the Member States in which the certificate will be used – i.e. validation answers the question, “With the data I am provided with, do I accept this certificate based on existing policies?”

**VERIFICATION:** A process that relies on the Verifier confirming the status of a test result certificate and ensuring that it is a true and unaltered certificate that has been signed and issued under the authority of a public health authority of a Member State – i.e. verification answers the question, “Is this from a trusted source?”

**VERIFIER:** A natural, or legal, person, either private or public, formally authorized (under national law, decree, regulation or other official act or order) to verify and validate the SARS-CoV-2 diagnostic test result presented in the DDCC.

**VERIFIER APPLICATION:** Also sometimes referred to as a certificate check application. It is a secure application used to verify and validate the SARS-CoV-2 diagnostic test result presented on the DDCC:TR. A Verifier can use the Verifier Application to scan the barcode, display the data held within the DDCC:TR and validate the DDCC:TR using a predefined set of acceptance criteria. The Verifier Application does not store or transmit any personal data, such as name and date of birth.



# 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 health data can be digitally documented via an electronic certificate. A test report that documents a person's severe acute respiratory syndrome coronavirus 2 (SARS-CoV-2) diagnostic test result can be used to generate a certificate as proof of that SARS-CoV-2 diagnostic test result. The resulting artefact of this approach is referred to as the **Digital Documentation of COVID-19 Certificates: Test Result (DDCC:TR)**.*

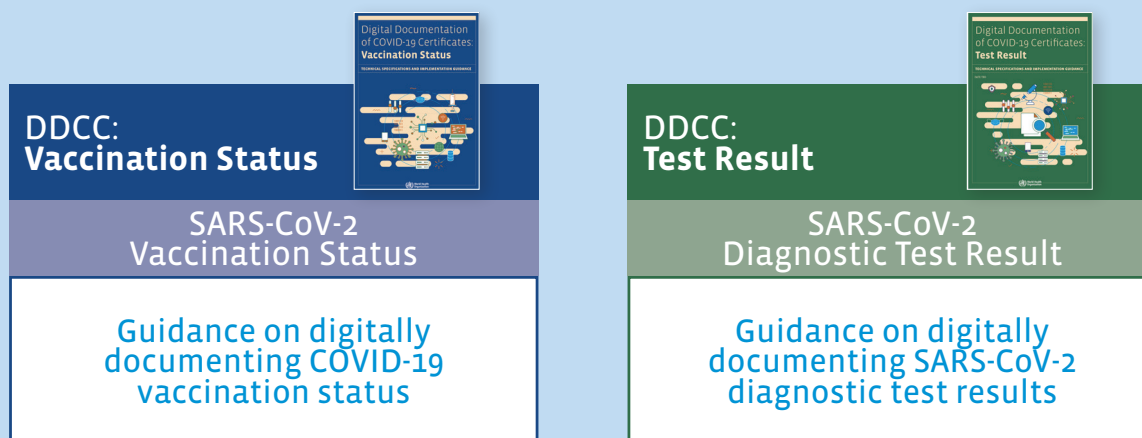
The document is the second of two guidance documents (see Fig. 1) on digital documentation of COVID-19 related data of interest: vaccination status<sup>3</sup> and test result (this document). Technical specifications and implementation guidance for two scenarios for a test result certificate, "proof of negative SARS-CoV-2 test result" and "proof of previous SARS-CoV-2 infection", are combined in a single DDCC:TR document, because, for both scenarios, some form of diagnostic testing is required before a test result certificate is issued.

The World Health Organization (WHO) has developed this guidance and accompanying technical specifications in collaboration with a multidisciplinary group of partners and experts, to support WHO Member States in adopting interoperable standards for recording SARS-CoV-2 diagnostic test results. The intended audience of this document is Member States and their implementing partners that want to put in place digitally signed test result certificates for SARS-CoV-2.

The current document is written for the ongoing global pandemic of COVID-19; 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.

<sup>3</sup> Digital documentation of COVID-19 certificates: vaccination status – technical specifications and implementation guidance. Geneva: World Health Organization; 2021 ([https://www.who.int/publications/i/item/WHO-2019-nCoV-Digital\\_certificates-vaccination-2021.1](https://www.who.int/publications/i/item/WHO-2019-nCoV-Digital_certificates-vaccination-2021.1), accessed 11 February 2022).

Figure 1  
Guidance documents for DDCC



## What is the DDCC:TR?

The DDCC:TR is a test result certificate that attests: (a) to the fact that an individual has been tested for SARS-CoV-2, and (b) to the result of that SARS-CoV-2 diagnostic test.

Some government authorities, following technical and ethical considerations, require a test result certificate that may be used as proof of a negative SARS-CoV-2 test result or proof of previous SARS-CoV-2 infection<sup>4</sup> for individualized exemptions from public health and social measures and/or accessing certain socioeconomic activities.<sup>5</sup>

A test result certificate includes minimal data about the individual who has been tested, the type of test conducted, the sample collection date and time, the test result, and other data in the core data set (see [section 5.2](#)). A test result certificate is a health document, and it is not intended for use as an identity document. It is at the discretion of Member States to determine the policies and procedures for binding a test result certificate to an individual's identity.

A "test report" differs from a "test result certificate". A test report contains a clinical interpretation of the test and relevant detailed medical information for use by authorized health workers for ongoing clinical care, early detection and infection containment measures (e.g. contact tracing and case reporting). A test report does not have an expiration date, and it may not necessarily be verifiable by a third party.

A test result certificate requires the information contained in a SARS-CoV-2 test report in order to generate a DDCC:TR. The test result certificate describes the SARS-CoV-2 diagnostic test result for a Tested Person, and often has a time-bound period of validity. Furthermore, unlike a test report, the test result certificate is digitally signed and can be verified and validated online or offline.

<sup>4</sup> Technical considerations for implementing a risk-based approach to international travel in the context of COVID-19: interim guidance. Geneva: World Health Organization; 2021 (<https://apps.who.int/iris/handle/10665/342212>, accessed 11 February 2022).

<sup>5</sup> Considerations for implementing and adjusting public health and social measures in the context of COVID-19: interim guidance. Geneva: World Health Organization; 2021 (<https://apps.who.int/iris/handle/10665/341811>, accessed 11 February 2022).

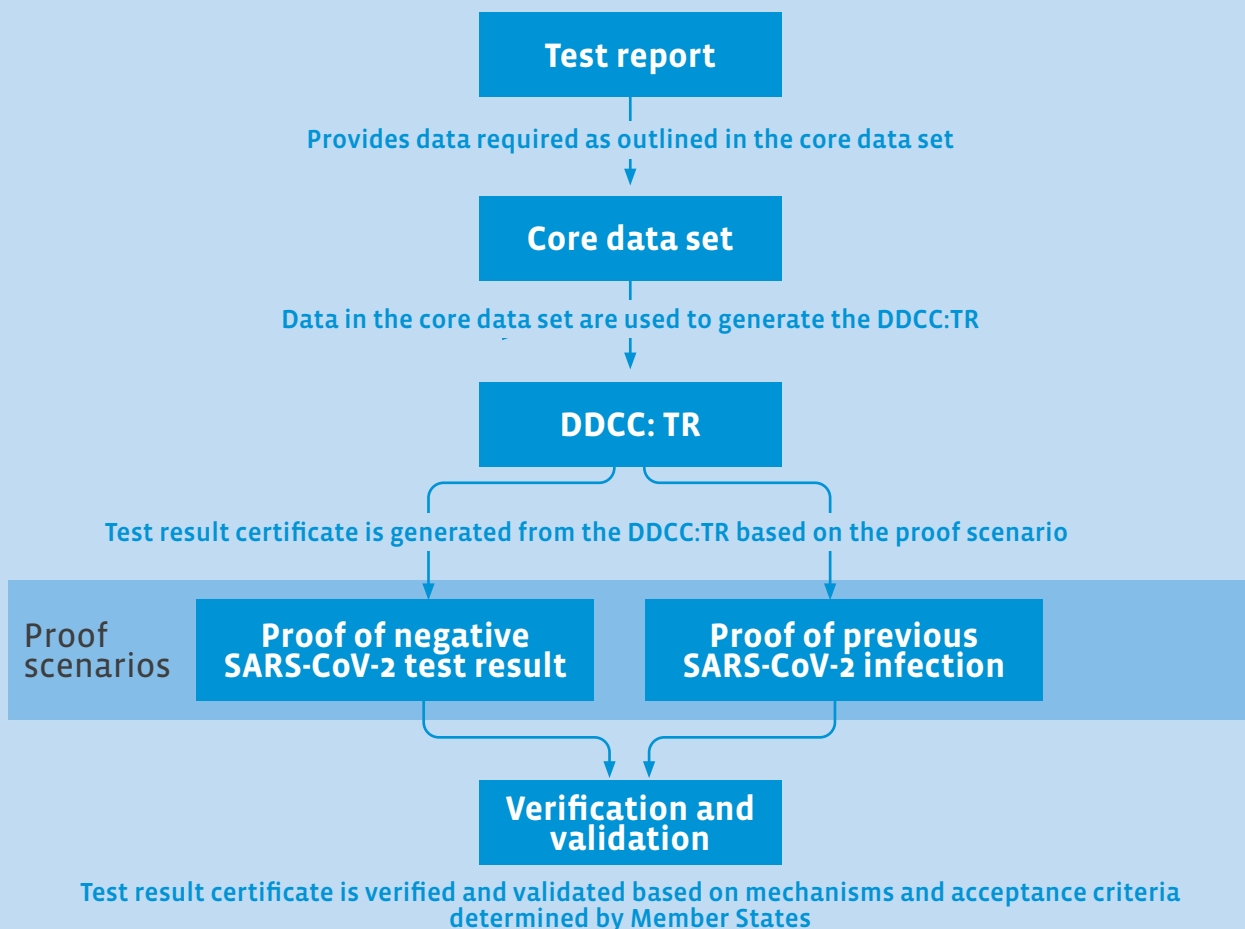
Table 1 provides a non-exhaustive list of uses of a test report compared with a test result certificate.<sup>6</sup>

**Table 1**  
**Different uses for test reports and test result certificates**

Test reports	Test result certificates
<p>Test reports are widely known and accepted. There is no additional need to verify these reports.</p> <p>Test reports are commonly used in:</p> <ul style="list-style-type: none"> <li>→ clinical care</li> <li>→ contact tracing</li> <li>→ case reporting</li> <li>→ screening and early detection of cases.</li> </ul>	<p>The uses of test result certificates should be determined by Member States, based on their existing legal frameworks and risk-based approach to pandemic control and mitigation. They may be used domestically or internationally. Some possible scenarios where a test result certificate may be used include:</p> <ul style="list-style-type: none"> <li>→ international travel</li> <li>→ access to socioeconomic activities (e.g. restaurants, sporting events).</li> </ul>

A test report can be used to generate a test result certificate. Fig. 2 depicts the overall steps of how a test report is leveraged to create a verifiable test result certificate.

**Figure 2**  
**DDCC:TR process**



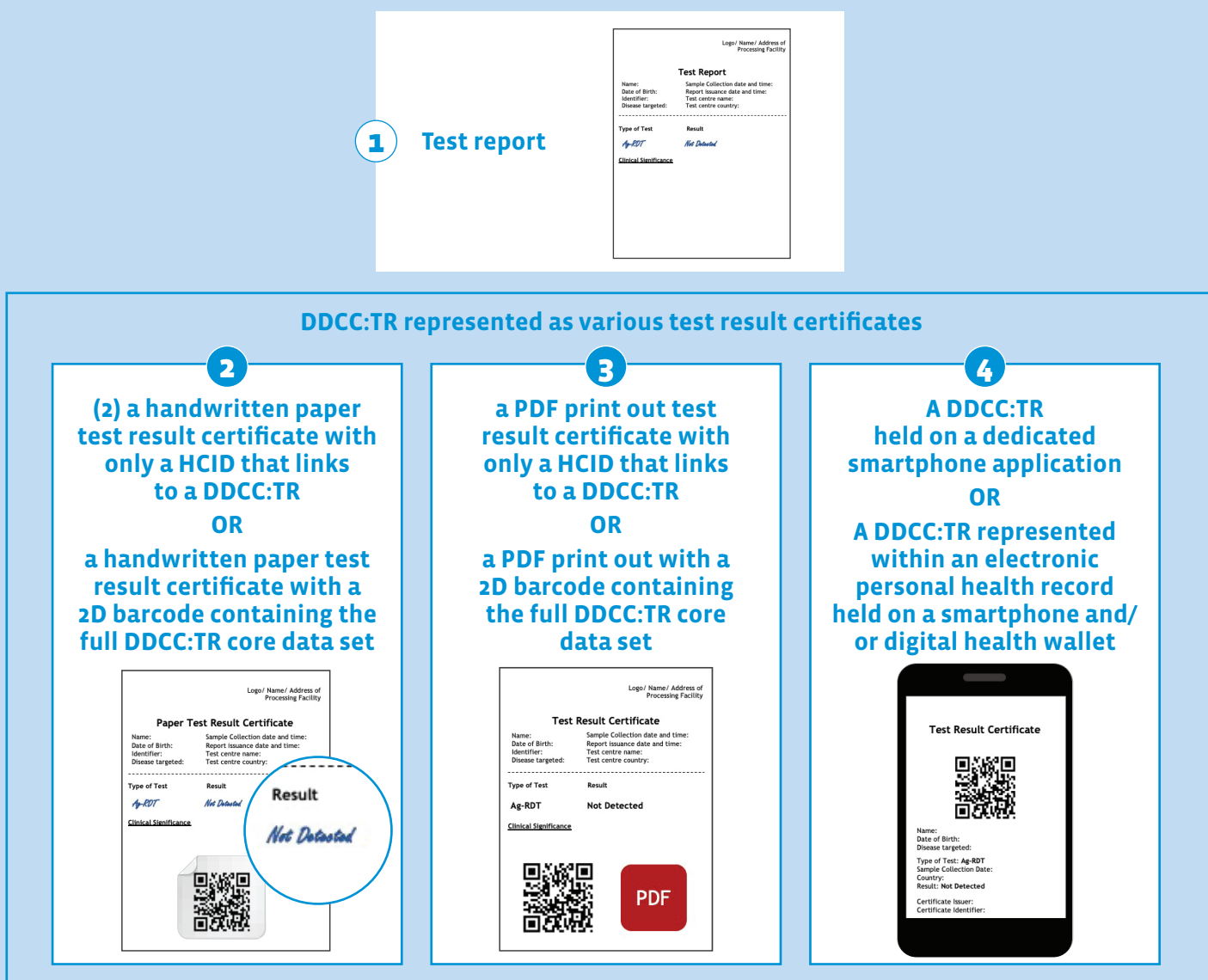
<sup>6</sup> Requirements and scope of digital certificates. Switzerland: National COVID-19 Science Task Force (NCS-TF); 2021 (<https://scienctaskforce.ch/en/policy-brief/requirements-and-scope-of-digital-certificates>, accessed 23 February 2022).

A DDCC:TR can be purely digital (e.g. stored in a smartphone application or on a cloud-based server), or it can be a computable representation of a test report rendered as a paper test result certificate (see Fig. 3). A DDCC:TR should never require individuals to have access to a smartphone or computer.

The link between the paper test result certificate and the digital certificate can be established through a health certificate identifier (HCID) using a one-dimensional (1D) or two-dimensional (2D) barcode that is printed on, or affixed to, the paper. References to a “paper test result” in this document refer to a physical paper document.

The DDCC:TR is a digitally signed representation of data content that describes the result of a SARS-CoV-2 diagnostic test that has been conducted. That data content respects the specified core data set and follows the Health Level Seven (HL7) Fast Healthcare Interoperability Resources (FHIR) standard. Many representations of a test result certificate can then be produced from a DDCC:TR.

Figure 3  
Different representations of a SARS-CoV-2 diagnostic test result





## Proof scenarios of the DDCC:TR

The scope of this document covers two proof scenarios of use for the DDCC:TR:

1. **PROOF OF NEGATIVE SARS-COV-2 TEST RESULT:** Test result certificates can be used as documented evidence of a negative test result when SARS-CoV-2 is not detected by a SARS-CoV-2 diagnostic test for viral detection (e.g. a nucleic acid amplification test [NAAT] or an antigen detection rapid diagnostic test [Ag-RDT]).<sup>7</sup>
2. **PROOF OF PREVIOUS SARS-COV-2 INFECTION:** Test result certificates can also be used as documented evidence of a previous SARS-CoV-2 infection with a positive result from a SARS-CoV-2 diagnostic test for viral detection (e.g. a NAAT or an Ag-RDT).<sup>7</sup> Note that proof of previous SARS-CoV-2 infection does not provide information on infectiousness, transmission risk or recovery from SARS-CoV-2 infection, as a proof of recovery status requires both proof of previous SARS-CoV-2 infection and proof that the individual is no longer infectious per WHO's criteria for releasing COVID-19 patients from isolation.<sup>7-9</sup>

Member States can use WHO guidance to determine which type(s) of SARS-CoV-2 diagnostic tests (e.g. NAAT, Ag-RDT) are appropriate for their target population and the setting where each test result certificate will be used. A risk assessment on the impact of the use of diagnostic testing for the DDCC is recommended. Key considerations for this risk assessment may include:

- considerations related to sensitivity, specificity and predictive value of SARS-CoV-2 diagnostic tests; previously infected individuals may have detectable RNA for over 100 days while being no longer infectious;
- access to and availability of testing services, and costs of SARS-CoV-2 diagnostic tests; if SARS-CoV-2 diagnostic testing is expensive and not widely available, low-income individuals might inadvertently be excluded from activities requiring proof of test results,<sup>10-14</sup>
- and the Member State's epidemiological situation (e.g. SARS-CoV-2 prevalence).<sup>15</sup>

7 Technical considerations for implementing a risk-based approach to international travel in the context of COVID-19: interim guidance. Geneva: World Health Organization; 2021 (<https://apps.who.int/iris/handle/10665/342212>, accessed 11 February 2022).

8 Criteria for releasing COVID-19 patients from isolation. Geneva: World Health Organization; 2020 (<https://www.who.int/news-room/commentaries/detail/criteria-for-releasing-covid-19-patients-from-isolation>, accessed 11 February 2022).

9 Living guidance for clinical management of COVID-19. Geneva: World Health Organization; 2021 (<https://www.who.int/publications/i/item/WHO-2019-nCoV-clinical-2021-2>, accessed 11 February 2022).

10 Diagnostic testing for SARS-CoV-2. Geneva: World Health Organization; 2020 (<https://www.who.int/publications/i/item/diagnostic-testing-for-sars-cov-2>, accessed 11 February 2022).

11 COVID-19 diagnostic testing in the context of international travel: scientific brief. Geneva: World Health Organization; 2020 (<https://apps.who.int/iris/handle/10665/337832>, accessed 11 February 2022).

12 SARS-CoV-2 antigen-detecting rapid diagnostic tests: an implementation guide. Geneva: World Health Organization; 2020 (<https://www.who.int/publications/i/item/9789240017740>, accessed 11 February 2022).

13 Recommendations for national SARS-CoV-2 testing strategies and diagnostic capacities: interim guidance. Geneva: World Health Organization; 2021 (<https://www.who.int/publications/i/item/WHO-2019-nCoV-lab-testing-2021.1-eng>, accessed 11 February 2022).

14 Antigen-detection in the diagnosis of SARS-CoV-2 infection. Geneva: World Health Organization; 2021 (<https://www.who.int/publications/i/item/antigen-detection-in-the-diagnosis-of-sars-cov-2-infection-using-rapid-immunoassays>, accessed 11 February 2022).

15 Technical considerations for implementing a risk-based approach to international travel in the context of COVID-19: interim guidance. Geneva: World Health Organization; 2021 (<https://apps.who.int/iris/handle/10665/342212>, accessed 11 February 2022).

The level of reliability of the content within a test result certificate should be interpreted by Member States according to the sensitivity and specificity of the SARS-CoV-2 diagnostic test that was used and noted in the test report.<sup>10-17</sup>

Furthermore, how the two proof scenarios will be implemented, and for what purpose, will depend on the legal frameworks and public health policies determined by the Member State. The use of the HL7 FHIR specification is intended to facilitate the application of different acceptance criteria to verify the test result certificates in cross-border use cases. The corresponding WHO Digital Documentation of COVID-19 Certificates (DDCC) implementation guide (available at <https://worldhealthorganization.github.io/ddcc>) provides details on how to use HL7 FHIR for operationalizing cross-border data-exchange use cases. The use cases within the two proof scenarios will further vary depending on the digital maturity and local context of the country in which a DDCC:TR solution is implemented.

---

## Minimum requirements to implement a DDCC:TR solution

---

DDCC:TR solutions 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. due to a digital divide) or to lack of access to diagnostic testing. The recommendations for the implementation of a DDCC:TR solution must therefore be applicable to the widest range of use cases, catering to many different levels of digital maturity within and between implementing countries.

The minimum requirements were developed 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:TR implementation are as follows.

- The potential benefits, risks and costs of implementing a DDCC:TR solution should be assessed before introducing a DDCC:TR 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:TR solution.
- Member States must establish policies for the appropriate use, data protection and governance of the DDCC:TR solution to reduce the potential harms while achieving the public health benefits involved in deploying such a solution.
- An individual who has been tested for SARS-CoV-2 should have access to proof of the test result in a paper and/or digital format.
- A digitally signed electronic version of the test report data, expressed using the HL7 FHIR specification, must exist, as this is the DDCC:TR. As a minimum, both the required data elements in the core data set and metadata should be recorded, as described in [section 5.2](#).
- A Public Health Authority (PHA) must operate a DDCC Generation Service to digitally sign an electronic version of the required data elements in the core data set (including metadata), to

---

16 Advice on the use of point-of-care immunodiagnostic tests for COVID-19: scientific brief. Geneva: World Health Organization; 2020 (<https://www.who.int/news-room/commentaries/detail/advice-on-the-use-of-point-of-care-immunodiagnostic-tests-for-covid-19>, accessed 11 February 2022).

17 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>, accessed 11 February 2022).

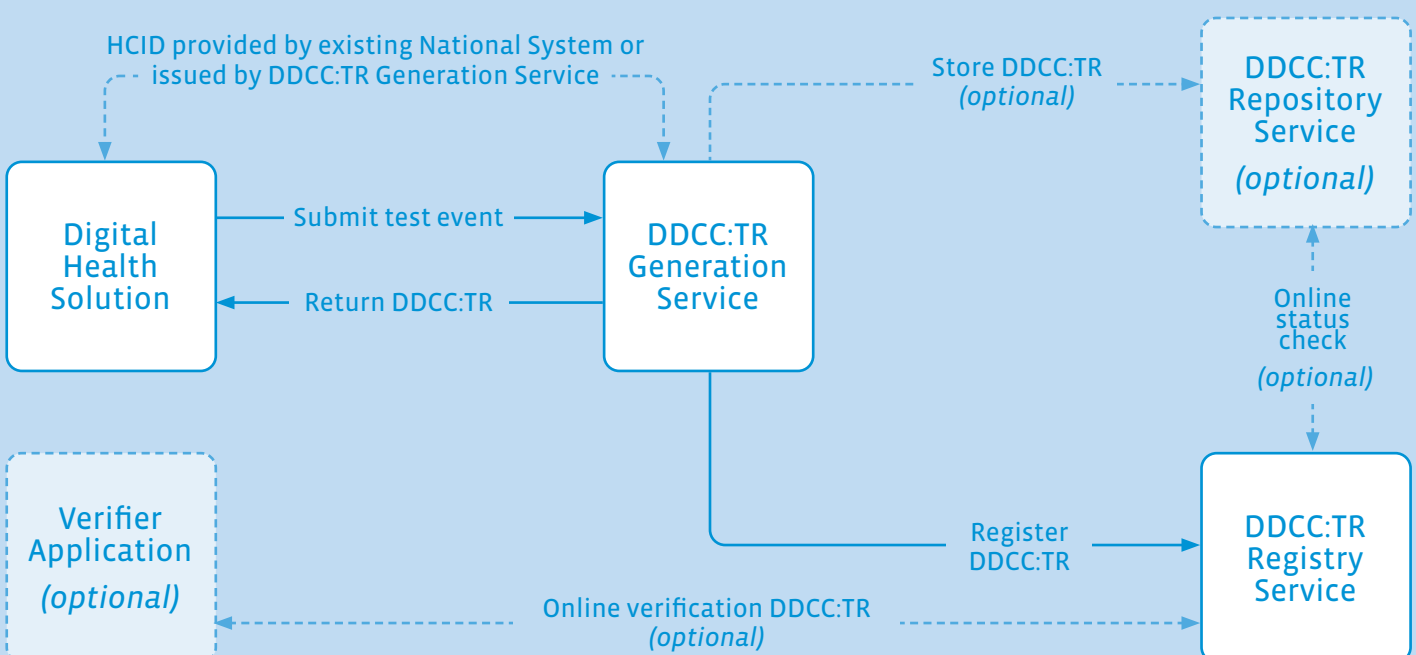
produce a DDCC:TR. The DDCC Generation Service is responsible for taking the test result data, representing it using the HL7 FHIR standard, digitally signing the HL7 FHIR document, and updating the DDCC:TR Registry Service (see below).

- It is at the discretion of the Member State to determine whether an HCID is associated with a single test result certificate or multiple test result certificates. One or more DDCC:TR (i.e. one or more test results) may also be associated with a single HCID, and each test result certificate may have its own identifier. If the DDCC:TR (i.e. a digitally signed electronic version of test report data) is to be represented as a paper test result certificate, it must be associated with an HCID. Multiple representations of the DDCC:TR (i.e. multiple 2D barcode formats) may be associated with a paper test result certificate via the HCID.
- For any paper test result certificate, the HCID must appear in a human-readable and a machine-readable format (i.e. alphanumeric characters printed on the paper as well as rendered within a 1D or 2D barcode).
- A DDCC Registry Service must exist, to store metadata about the DDCC:TR that are retrievable with the HCID. As a minimum, the DDCC Registry Service stores the core metadata described in [section 5.2](#).
- One or more DDCC Repository Service(s) may exist, which can be used to retrieve a DDCC:TR; if a DDCC Repository Service exists, the location from where the DDCC:TR may be retrieved may also be included in the metadata within the DDCC Registry Service.

Fig. 4 shows the relationships between digital services. The different services are discussed in more detail in [section 3](#) and [section 4](#).

These components are minimum requirements. Member States may adopt and develop additional components for their deployed DDCC:TR solution.

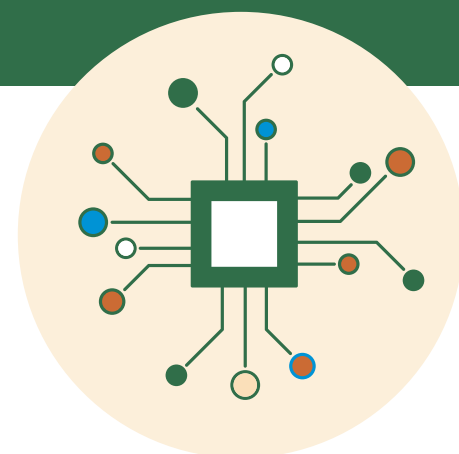
Figure 4  
**Relationships between digital services**



HCID: health certificate identifier; DDCC:TR: Digital Documentation of COVID-19 Certificates: Test Result.

Note the use of the HCID throughout these services. As the unique identifier included in a DDCC:TR, it can be provided by an existing national system, generated at the point of care or issued by DDCC:TR Generation Service (as illustrated in [Figure 7](#)). HCID can allow verifiers to search for, and retrieve a DDCC:TR for the purposes of verification.

# 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 pandemic has had a negative impact on all societies and economies across the globe. COVID-19 vaccines are being delivered at record speed, but they are currently not equitably distributed globally. As countries reopen their economies, infection control and mitigation measures still need to be in place due to continued transmission in all countries. As part of an overall package of interventions, some countries require proof of SARS-CoV-2 diagnostic test results to facilitate movement of citizens, including access to socioeconomic activities and mass gatherings.*

Digital technology can be leveraged to augment paper-based SARS-CoV-2 diagnostic test results, which are easily lost and prone to fraud (1–4). A wide range of digital solutions can be used to digitally document SARS-CoV-2 diagnostic test results; 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 [Chapter 2](#).

## 1.1 Purpose of this document

This document lays out an approach for creating a signed digital version of a SARS-CoV-2 test result certificate based on the required data and an approach for the digital signature. This certificate of a SARS-CoV-2 diagnostic test result, or “test result certificate”, can be used as proof of a negative SARS-CoV-2 test result or proof of previous SARS-CoV-2 infection. The document leverages existing free and open standards, and is driven by ethical considerations, use cases, and requirements for the Digital Documentation of COVID-19 Certificates: Test Result (DDCC:TR).

As Member States are increasingly looking to adopt digital solutions for COVID-19 certificates, this document provides a baseline set of requirements for a DDCC:TR solution that is interoperable with other standards-based solutions. With the baseline requirements met, it is 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.

---

## 1.2 Target audience

---

The primary audience of this document is national authorities tasked with creating or overseeing the development of digital certificates that would provide proof of SARS-CoV-2 diagnostic test results. The document may also be useful to government partners such as local businesses, international organizations, nongovernmental organizations, trade associations, and any other organization tasked with supporting Member States in developing or deploying a DDCC:TR solution.

---

## 1.3 Scope

---

### 1.3.1 In scope

This document specifically focuses on how to provide signed digital certificates for SARS-CoV-2 diagnostic test results, including:

- ethical and legal considerations, including privacy and data protection principles, for the design, implementation and use of DDCC:TR solution;
- proof scenarios of a negative SARS-CoV-2 test result and of previous SARS-CoV-2 infection, and use cases arising from the operation of a DDCC:TR solution, including the sequence of steps in executing the scenarios;
- a core data set of data elements to be included in a DDCC:TR solution based on the use case;
- 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:TR solution, including considerations for setting up a national trust framework to enable digital signing of a test result certificate.

### 1.3.2 Out of scope

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

- policy guidance regarding the use of a test result certificate or DDCC:TR;
- any guidance regarding interpretation of the information provided in a DDCC:TR, or decision-making based on that information, for any purpose;
- issuance, verification and validation of test result certificates for self-administered tests, at-home tests and antibody tests;
- digital documentation of COVID-19 vaccination status certificates (which is covered in a separate guidance document) (5);

- digital documentation of COVID-19 certificates for proof of recovery status to exempt individuals from testing or quarantine requirements for travelling internationally. There is uncertainty around immunity status arising from recovery from previous infection, and additional data are required to provide proof that an individual has met the World Health Organization (WHO) criteria for releasing COVID-19 patients from isolation (6–8);
- processes for specimen collection, data collection and sample analysis. WHO guidance on diagnostic testing for SARS-CoV-2 can be found in separate reference documents (9–16);
- processes for generation, verification and validation of test reports (which will be at the discretion of Member States);
- verification and associated processes related to identification of a Tested Person, and association of a Tested Person's identity to a test result certificate. Processes and mechanisms for identification of a Tested Person should be based on Member States' policies;
- guidance on how to implement and manage a public key infrastructure (PKI) for the purpose of electronically signing the digital certificate;
- any requirements regarding quality assurance of laboratories, medical devices and diagnostic tests used to perform the test and provide a test report. These requirements should be guided by existing national and international standards and regulations for diagnostic laboratories, medical devices and diagnostic tests as defined by the mandated authorities of Member States;
- monitoring and evaluation considerations for the roll-out and use of a DDCC:TR solution;
- the choice of algorithm for generating any two-dimensional (2D) barcodes, which is at the discretion of the Member State. Member States may augment the core data set with additional information to provide stronger identity binding than is presumed in this document, if required by existing 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 (EU); and
- technical functionality to support selective disclosure of information in a DDCC:TR.

---

## 1.4 Assumptions

---

The technological specification for a DDCC:TR solution 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 are common requirements across all Member States and that a common approach to addressing these could support economies of scale and broad interoperability between solutions.

The requirements outlined are intended to allow for DDCC:TR 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 Member States to support the local, sustainable development of a DDCC:TR solution through a broad choice of appropriate compliant solutions.

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

- Member States will be responsible for implementing the policies necessary to support the DDCC:TR workflows, complying with their legal obligations under national and international law, including any applicable obligations related to respecting human rights and data protection policies (see [section 2.2](#)).
- Member States will adhere to ethical principles, as outlined within this document, and act to prevent new inequities from being created by a DDCC:TR solution.
- The DDCC:TR is a health document associated with an individual who has proved to be who they claim they are, based on the policies established by the Member State. The DDCC:TR is not an identity card or identification document. It will be at the discretion of the Member State to determine the mechanism for identification of the Tested Person.
- It is at the discretion of the Member States to establish policies that clearly outline the criteria for acceptance of a DDCC:TR, including, for example, the certificate validity period for each proof scenario for domestic and/or international use cases.
- It is at the discretion of the Member States to determine the format in which to implement the DDCC:TR. 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, a smartphone application or another easily accessible format.
- The Public Health Authority (PHA) of a Member State needs access to a PKI for digitally signing each DDCC:TR. This document does not describe the PKI in detail, but key assumptions are that the PHA needs to:
  - » utilize an existing root certificate authority or establish and maintain a root certificate authority that anchors the country's PKI for the purposes of supporting the DDCC:TR solution;
  - » generate and cryptographically sign document signer certificates (DSCs);
  - » authorize document signer private keys to cryptographically sign the digital DDCC:TR;
  - » ensure private keys used to sign the DDCC:TR will not be associated with individual health workers;
  - » broadly disseminate public keys if there is a desire to allow others to cryptographically validate an issued DDCC:TR;
  - » allow for the health content contained within a traditional paper test report to be digitized and verifiable, by one or more digital representations. For example, Member States may choose to generate a signed 2D barcode as a digital representation of the core data set content, which is then printed onto or affixed to the paper record, sent by email to the DDCC:TR Holder, loaded into a smartphone application, or made downloadable on a website; and
  - » keep the signature-verification processes manageable. The number of private keys used by the PHA to sign DDCC:TRs should not be more than a small proportion of the number of Digital Health Solutions used to capture test results.
- The PHA of a Member State will need to operate a DDCC Generation Service to create DDCC:TRs, and a DDCC Registry Service to record the issuance of a DDCC:TR. Optionally, the PHA may also decide to provide a DDCC Repository Service to allow Verifiers to search for and retrieve a DDCC:TR using the health certificate identifier (HCID).

## 1.5 Methods

Since the COVID-19 pandemic began, the number of digital solutions for test result certificates has increased. WHO intends to remain software agnostic and has consulted multisectoral experts focused on supporting the development of key standards for digital test result certificates, sharing lessons learned, and supporting the development of a trust framework architecture.

Furthermore, WHO 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 when, where and how DDCC:TRs can be used can be found in the following WHO guidance documents:

- Policy considerations for implementing a risk-based approach to international travel in the context of COVID-19 (18)
- Technical considerations for implementing a risk-based approach to international travel in the context of COVID-19: interim guidance (6)
- Considerations for implementing and adjusting public health and social measures in the context of COVID-19: interim guidance (19)
- Statements on meetings of the International Health Regulations (2005) Emergency Committee regarding the COVID-19 pandemic:
  - » Statement on the tenth meeting of the International Health Regulations (2005) Emergency Committee regarding the coronavirus disease (COVID-19) pandemic (20)
  - » Statement on the ninth meeting of the International Health Regulations (2005) Emergency Committee regarding the coronavirus disease (COVID-19) pandemic (21)
  - » Statement on the eighth meeting of the International Health Regulations (2005) Emergency Committee regarding the coronavirus disease (COVID-19) pandemic (22)
  - » Statement on the seventh meeting of the International Health Regulations (2005) Emergency Committee regarding the coronavirus disease (COVID-19) pandemic (23)
  - » Statement on the sixth meeting of the International Health Regulations (2005) Emergency Committee regarding the coronavirus disease (COVID-19) pandemic (24)
- Key planning recommendations for mass gatherings in the context of COVID-19 (25)

Specific guidance and recommendations on SARS-CoV-2 diagnostic testing and related strategies can be found in the following WHO guidance documents:

- Diagnostic testing for SARS-CoV-2 (9)
- COVID-19 diagnostic testing in the context of international travel: scientific brief (10)
- SARS-CoV-2 antigen-detecting rapid diagnostic tests: an implementation guide (11)
- COVID-19 natural immunity (26)
- Recommendations for national SARS-CoV-2 testing strategies and diagnostic capacities (12)
- Antigen-detection in the diagnosis of SARS-CoV-2 infection (13)



- Assessment tool for laboratories implementing SARS-CoV-2 testing: interim guidance (27)
- Laboratory biosafety guidance related to COVID-19: interim guidance (14)
- Advice on the use of point-of-care immunodiagnostic tests for COVID-19 scientific brief (15)

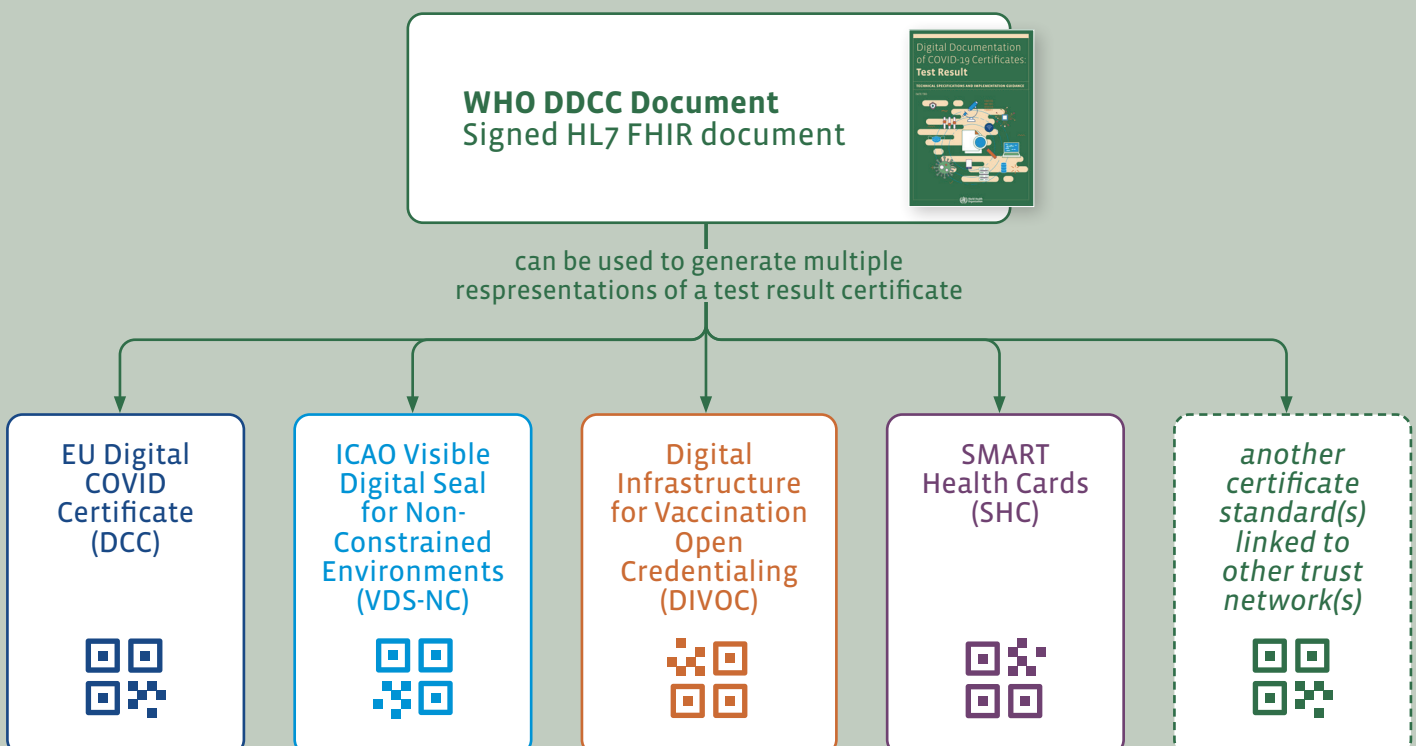
## 1.7 Other initiatives

The data captured about the test that was conducted (i.e. test event content) in the DDCC:TR core data set guidance laid out in this document may be leveraged to generate the test event content for artefacts conformant with other initiatives, such as the ICAO guidelines on visible digital seals (VDS-NC) for travel-related public health proofs (28), the EU Digital COVID Certificate (DCC) (29), the Digital Infrastructure for Vaccination Open Credentialing (DIVOC) (30) and SMART Health Cards (31) (see Fig. 5).

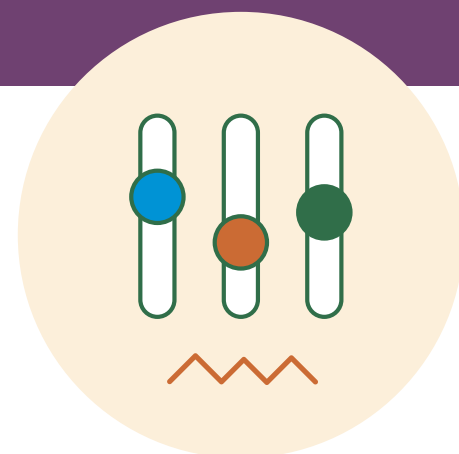
There may be a need to extend the core data set to include additional metadata to generate artefacts conformant with other specifications, such as “Date and Time of Report Issuance” for conformance with ICAO VDS-NC (28). Additional technical details can be found in the WHO DDCC HL7 FHIR implementation guide (available at <https://worldhealthorganization.github.io/ddcc>) (17).

This DDCC:TR specification document does not provide QR code or 2D barcode specifications. QR code specifications are outlined in other initiatives and can be rendered from the WHO DDCC HL7 FHIR implementation guide.

Figure 5  
Relationship between DDCC document and other initiatives



# Ethical considerations and data protection principles



*As with any digital solution, for DDCC:TR there are both ethical considerations, such as potential impacts on equality, human rights and public trust, and data protection principles that need to inform the design of DDCC:TR technical specifications and provide guidance on how resulting solutions can be implemented ethically (32). The following sections discuss key ethical considerations and data protection principles that Member States ethically ought to – and, where they have legal obligations, must – include in their respective deployments of a DDCC:TR solution. These ethical considerations and data protection principles informed the design criteria for a DDCC:TR solution outlined in the following chapters.*

## 2.1 Ethical considerations for a DDCC:TR

SARS-CoV-2 diagnostic test results may be documented for individual health purposes, such as diagnosis and continuity of care, and for public health uses for infection detection and containment (e.g. surveillance, population screening to detect unknown cases of infection, and contact tracing) (12). A DDCC:TR, as proof of a negative SARS-CoV-2 test result or proof of previous SARS-CoV-2 infection, could be issued to an individual based on test results initially recorded for individual health purposes or public health reasons, or an individual could undergo testing specifically to obtain a DDCC:TR. The functions of a DDCC:TR are distinct from the above-mentioned individual health purposes or public health purposes, because a DDCC:TR is a test certificate (as opposed to a test report) issued to an individual that may be used for individualized exemptions from public health and social measures (e.g. post-exposure quarantine), or to facilitate movement or regulation of access to socioeconomic activities during the COVID-19 pandemic as required or permitted by legitimate authorities.

This section presents the ethical considerations for designing, developing and deploying a DDCC:TR solution and provides some recommendations for ethical implementation.

### 2.1.1 Key ethical considerations for current proposed uses of a DDCC:TR

Ethics should be an integral part of the design and deployment of a DDCC:TR solution. 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 and accountability for the outcomes. Several different ethical considerations should be considered, taking into account relevant national and international contextual factors, including the ethical aims of public health action and procedural values for governing the decision-making process.

#### 2.1.1.1 Ethical aims

A starting point is to identify how the use of a DDCC:TR can contribute to important general duties of any government through public health activity in response to the COVID-19 pandemic. Three key ethical aims of public health action are:

1. protecting and promoting the welfare of individuals and communities;
2. ensuring equitable treatment of individuals and communities, and preventing or mitigating, as far as possible, avoidable and unfair disadvantages in health opportunities and other relevant considerations within the boundaries of the state; and
3. engendering and maintaining public trust in public health activities as part of the health system.

**1. PROTECTING AND PROMOTING WELFARE:** The primary function of a DDCC:TR is to digitally document, issue and verify proof of SARS-CoV-2 diagnostic test results for individuals in a reliable and accurate manner that can be used to: exempt holders from certain public health and social measures; or to facilitate their movement and access to socioeconomic activities in lieu of, or in addition to, a Digital Documentation of COVID-19 Certificates: Vaccination Status (DDCC:VS), as required or permitted by legitimate authorities as part of the overall public health response to the COVID-19 pandemic.

Such a function contributes to the achievement of welfare promotion, by increasing opportunities for individuals and communities to pursue their own economic and social goals through greater access to areas of life that would otherwise be curtailed during the pandemic, while at the same time mitigating risks of disease spread and its negative consequences due to increased movement and congregation during the pandemic.

**2. ENSURING EQUITABLE TREATMENT:** Equitable treatment requires respecting and protecting all persons equally and acting to ensure, as far as possible, no wrongful or unfair discrimination that may amount to a violation of human rights. In contexts that require or permit the use of a SARS-CoV-2 test result certificate for individualized exemptions from public health and social measures, or individualized access to certain activities and services, a DDCC:TR helps mitigate disadvantages in opportunities for participation in civil, social and economic life. For example, a DDCC:TR could be especially useful to: those who lack access to, or are not prioritized to receive, a COVID-19 vaccine (e.g. children and young adults); those who are unable to be vaccinated due to medical reasons (e.g. individuals who are at risk of a severe allergic reaction); those who choose not to be vaccinated despite vaccine being available; those who are vaccinated but cannot obtain or provide proof of valid vaccination status (e.g. when an individual obtains a COVID-19 vaccine from an illicit source or of a vaccine brand not recognized or accepted by the recipient's country); and those who are waiting to receive a subsequent

dose according to recommended vaccination schedules. Depending on the epidemiological situation and other reasons, a DDCC:TR may also be required as an additional certificate for individuals with a DDCC:VS to facilitate movement and gatherings, especially in environments that pose higher risks.

Like the introduction of a DDCC:VS, the use of a DDCC:TR as a “health pass” for access to socioeconomic activities (e.g. work; domestic and international travel; cultural, entertainment, leisure and sporting events; and conferences and industry trade shows) may exacerbate inequalities highlighted or created by the pandemic and increase prior disadvantages of particular groups, for the following reasons.

- Members of certain populations (e.g. refugees, individuals with illegal or insecure residency status, the homeless, and those who live at or below poverty levels) are disproportionately less likely to have opportunities for SARS-CoV-2 testing and certification due to lack of availability, accessibility, affordability (where testing is not free) and other issues.
- Individuals who rely on a DDCC:TR for facilitated movement may face more burdens than those who have a DDCC:VS. For example, individuals for whom a DDCC:TR is a requirement to perform their work, to travel or to access other socioeconomic activities may need to undergo more frequent testing, which requires time and expense and may place substantial burdens on particular groups. In addition, individuals with a DDCC:TR may be required to comply with additional public health and social measures (e.g. travel quarantine, which incurs additional costs) that do not apply to those with a DDCC:VS. Such measures and their burdens may deter participation in the activities that require a COVID-19 certificate and increase the disadvantages of those without access to vaccinations.
- A DDCC:TR may increase digital exclusion if individuals lack access to the digital infrastructure or to the knowledge and skills to utilize it, or if there is disparity in the establishment or support of the digital infrastructure across or within Member States.
- Individuals with disabilities may face barriers, depending on the administration process and design, in obtaining and using a DDCC:TR.

An equitable approach to the use of DDCC:TRs will ensure that the burdens for individuals who depend on a DDCC:TR to facilitate movement, for work and for social gatherings are not disproportionate. Ensuring an equitable approach also means that those with greater barriers to obtaining and using a DDCC:TR are supported to a greater extent than others.

**3. ENGENDERING PUBLIC TRUST:** Trust is vital to ensure the benefits of DDCC:TR 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 delivering the aim of protecting and promoting welfare. To enhance trust, a DDCC:TR should be used only for its intended purpose, as illegitimate uses (e.g. unjustified exclusion from a socioeconomic activity) may result in legitimate uses (e.g. facilitation of movement) being undermined.

#### 2.1.1.2 *Procedural values*

Disagreements about how to weight the different ethical aims, or conflicts between those aims, may require procedural values that govern the decision-making process, to arrive at ethical decisions in the deployment of a DDCC:TR. In turn, these procedural values also contribute to the effective pursuit of the aims. Such values include the following.

- **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 under way). Such a process disciplines decision-making and ensures accountability by providing clear and sound rationale.
- **INCLUSIVENESS:** Providing opportunities for all relevant stakeholders to participate in policy formulation and design. This may be achieved through public consultation or engagement with a wide range of experts, industries and members of the public to address real and perceived issues. Particularly important stakeholders are those who are likely to be disadvantaged or who face distinct or heightened risks with the implementation of a DDCC:TR (e.g. individuals who have concerns about SARS-CoV-2 testing because of, for example, the burden of isolation if they test positive for an active infection; individuals with insecure or invalid citizenship or residency status; and individuals who may face barriers in obtaining or using a DDCC:TR).
- **ACCOUNTABILITY:** Providing a clear description 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.

### 2.1.1.3 Recommendations

The design, development and implementation of a DDCC:TR raises many ethical issues and human rights challenges. The following eight recommendations are for the two proof scenarios: proof of negative SARS-CoV-2 test result and proof of previous SARS-CoV-2 infection.

#### 1. CERTIFICATION SHOULD BE AS ACCURATE AS POSSIBLE.

Use of a DDCC:TR is intended to facilitate exemptions from public health and social measures, movement and/or access to socioeconomic activities. Therefore, certification should be reliable and accurate (6,11,18,25,26). It is for Member States to determine the requirements for proof of a previous SARS-CoV-2 infection in order to obtain a DDCC:TR, based on relevant scientific information and risk assessment (9,11–13,24–26,33).

#### 2. THE SCOPE OF USE OF A DDCC:TR SHOULD BE CLEARLY DEFINED.

A DDCC:TR can be used for several purposes. To prevent potential misuse, clear and specific policies, and laws if needed, should be set on permitted and prohibited uses of a DDCC:TR. Use of a DDCC:TR in response to a public health emergency such as the COVID-19 pandemic is justified only when it: supports the pursuit of a legitimate aim during the emergency and is provided for by policy, regulations or law; is proportionate; is of limited duration; is based on scientific evidence; and is not imposed in an arbitrary, unreasonable or discriminatory manner.

#### 3. A DDCC:TR SHOULD NOT BE REQUIRED TO ACCESS BASIC SERVICES.

To protect welfare, ensure equal respect for persons and ensure public trust, a DDCC:TR should not be a requirement to access goods and services that support the basic necessities of daily life (e.g. accessing health and social services, buying groceries and using public transport). Exclusion of those without a COVID-19 certificate from access to goods and services that meet basic needs would violate human rights. In addition, any public health benefits of restricting such access would likely be outweighed by the harms to individuals and communities. Any potential increased risk that those without a COVID-19 certificate might pose to others through their use of such services

could be mitigated by everyone in the population complying with public health and social measures (e.g. wearing a mask, physical distancing) as well as through broader measures such as contact tracing and isolation.

#### 4. **POTENTIAL BENEFITS, RISKS AND COSTS SHOULD BE ASSESSED BEFORE INTRODUCTION OF A DDCC:TR SOLUTION.**

A DDCC:TR solution 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, certify and verify test result records and certificates. A cost-benefit 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:TR infrastructure over other measures for responding to COVID-19 and meeting other public health needs during a public health crisis. A long-term view would consider the potential advantages of a DDCC:TR for strengthening the public health system, such as creating a system for health certification that could be leveraged to facilitate individuals' movement for future epidemics and pandemics.

In addition, the ethical issues and risks raised by a DDCC:TR, and the impact of trade-offs between the benefits and burdens accrued on 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.

#### 5. **OBTAINING AND USING A DDCC:TR SHOULD BE AS INCLUSIVE AND FAIR AS POSSIBLE.**

DDCC:TR solutions should be as inclusive as possible and should not create or exacerbate disadvantages. To achieve this, tests should be made generally available, accessible and affordable and/or free of charge where feasible and consistent with public health goals (34). It is necessary to provide cost-effective DDCC:TR solutions that include paper-based certificates, and meaningful opportunities to obtain them, for individuals and groups with existing disadvantages, such as those without digital skills, those with disability barriers, those living in areas with poorer digital connectivity and those who are undocumented migrants or who are homeless.

#### 6. **ALL COMMUNICATION SHOULD BE CLEAR AND TRANSPARENT.**

Relevant information about the implementation of a DDCC:TR should be communicated in a transparent and accessible manner (including in language that those affected can easily understand). Such communication helps promote public trust and acceptance of a DDCC:TR solution. This communication includes: how a DDCC:TR would benefit individuals, public health and society as a whole; the justification or criteria for why a DDCC:TR is used in certain contexts and not others, and when its use may be removed; the policies and mechanisms in place to limit access to and use of a DDCC:TR by third parties; and whether DDCC:TR data are linked to other types of data, and the purposes of any data linkage. Relevant information also includes: specific requirements of the testing process (e.g. recognized tests and providers, number of tests); costs; validity period of the certificate given its specified use; the locations where or activities for which a DDCC:TR is used; the restrictions that would be removed or would remain for a DDCC:TR Holder in a given context; and the implications of testing positive for active infection, and the required or recommended actions (e.g. the need to self-isolate and physically distance from others).

## 7. THE DDCC:TR SOLUTION SHOULD BE CONSTANTLY MONITORED FOR IMPACT AND ADJUSTED AS NECESSARY.

After implementation, it is important to monitor and evaluate the effects of a DDCC:TR regularly in terms of positive and negative outcomes (e.g. impact on public health, equality and human rights) and to consider potential interventions to mitigate negative outcomes. Such monitoring and evaluation should also review uses that do not fit neatly into categories of legitimate and illegitimate use set by policies, to consider whether these uses should be continued, modified or stopped. Adequate resources should be provided to support monitoring and evaluation activities. The information resulting from those activities should be made publicly available to promote transparency and trust.

## 8. THERE SHOULD BE ETHICAL SAFEGUARDS WHEN DDCC:TR DATA ARE USED FOR SCIENTIFIC PURPOSES.

Use of DDCC:TR data for scientific purposes (e.g. research) is ethically justifiable when those purposes aim to provide information and evidence to support public health responses to the pandemic, and when ethical safeguards are in place to protect public and individual interests and promote public trust in, and the gain of social value from, the scientific uses. In this regard, appropriate ethical oversight and governance of such data uses – including for non-research activities such as surveillance (35) – should be implemented. Data subjects and other members of the public should be informed, in advance, of the nature and occurrence of these activities, and of any options they have for controlling or limiting DDCC:TR data for these uses.

DDCC:TR data are sensitive and should, in general, be anonymized (or pseudonymized, or de-identified) for scientific purposes, to minimize risks to data subjects. Where DDCC:TR data need to be retained in an identifiable form for scientific purposes, consideration should be given to whether consent is required or should be waived based on appropriate ethical criteria being met (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).

## 2.2 Data protection principles for a DDCC:TR solution

The previous section highlights the importance of data protection to the fostering of public trust in the implementation of DDCC:TR solution. This section presents specific and fundamental data protection principles for the deployment of a DDCC:TR solution as a response to the COVID-19 pandemic. The principles are designed to provide guidance to the national authorities tasked with creating or overseeing the development of a DDCC:TR solution. To build trust in the implementation of the DDCC:TR, the objectives are to: encourage Member States to adopt or adapt 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.

The data protection principles are as follows.

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

Personal data collected in the interest of the application of the DDCC:TR should be processed in a fair and non-discriminatory manner with the consent of the data subject, and protecting the vital interests of the data subject or another data subject, or as explicitly justified by legitimate public health objectives.

The processing of personal data in the interest of the application of the DDCC:TR 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:TR should be accessed, analysed or otherwise used only 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:TR 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:TR should 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:TR should be made public.

## 3. **PURPOSE LIMITATION AND SPECIFICATION**

Personal data collected in the interest of the DDCC:TR should not be processed in ways that are incompatible with specified legitimate purposes. The use of these 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:TR 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.

Transfer of personal data processed in the interest of the application of the DDCC:TR to a third party, or allowing access by a third party, should be permitted only if: the principles underlying the lawful basis, as referred to above, are met; and the third party affords the personal data appropriate protection that is equal to or higher than those protections provided by the data controller.



Personal data processed in the interest of the application of the DDCC:TR 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 in the DDCC:TR 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 its 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 legitimate use. Personal data retained in the interest of the application of the DDCC:TR should be retained and stored only for the time that is necessary for specified purposes. Personal data accessed at the point of verification of the DDCC:TR should not be retained, for example stored in a repository, database or otherwise.

#### 5. **CONFIDENTIALITY AND SECURITY**

Personal data processed in the interest of the application of the DDCC:TR should be kept confidential and not disclosed to unauthorized parties; personal data should be accessible only 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:TR, appropriate organizational, physical and technical security measures should be implemented for both electronic and paper-based data 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, in applications, on servers or on networks, or if they are sent through services involved in collection, transmission, processing, retention or storage.

Considering 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 of the following in the context of personal data: accidental loss, destruction, damage, unauthorized use, falsification, tampering, fraud, forgery, unauthorized disclosure or breach.

In the event of a security breach leading to the accidental or unlawful destruction, loss, alteration, or unauthorized disclosure of or access to personal data transmitted, stored or otherwise processed, DDCC:TR Holders should be notified in an appropriate and timely manner. DDCC:TR 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:TR Holders, if they have provided sufficient evidence of being the DDCC:TR Holder, should be able to exercise data subject rights. These data subject rights include the right of access to, correction of, deletion of, objection to and restriction of personal data, subject to conditions determined 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:TR 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:TR adhere to the principles, and may recommend revoking the authorization to collect or otherwise process DDCC:TR 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:TR design criteria

---

Due to the ethical considerations and data protection principles outlined above, the following design criteria were determined to inform the requirements and technical specifications for implementing a DDCC:TR as part of a holistic package of interventions to address the COVID-19 pandemic.

1. Implementation of the DDCC:TR should not increase health inequities or increase the digital divide.
2. Everyone who has a valid negative SARS-CoV-2 test result for active infection or a valid positive test result for proof of previous SARS-CoV-2 infection, within the window period recognized by relevant competent authorities, has the ethical right to obtain and hold a DDCC:TR where it is a prerequisite for access to socioeconomic activities.
3. The DDCC:TR needs to be in a format that can be accessible to all (e.g. in paper and digital formats). Any solution should also work in online and offline environments across multiple platforms – paper and digital. For example, digital technology should not be the only mechanism available for verification. There should always be possible ways to revert to paper-only manual verification of test result certificates.
4. DDCC:TR users should not be treated differently due to the format of the DDCC:TR they are using (e.g. there should be no discrimination based on whether someone is presenting a DDCC:TR on a smartphone or a representation on a paper card).
5. Any DDCC:TR solution should not be at an additional cost to the person who has taken the relevant diagnostic test(s) to evidence their SARS-CoV-2 diagnostic test result (negative SARS-CoV-2 infection or proof of previous SARS-CoV-2 infection within a predetermined time period).
6. The interoperability specifications used in DDCC:TR solutions should utilize open standards to ensure equitable access to a range of non-proprietary digital tools.

7. The infrastructure that the DDCC:TR solution is built on should ensure that individuals and Member States are not locked into a commitment with only one vendor.
8. Any DDCC:TR 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.
9. Any DDCC:TR solution should be designed to augment and work within the context of existing health information systems, as appropriate.
10. Any DDCC:TR solution should not share or store more data than is needed to successfully execute its tasks. The DDCC:TR should contain only the minimum data necessary to achieve the facilitation of individuals' movement and access to socioeconomic activities. Privacy-protecting features should be built into the system and be respected accordingly.
11. Anti-fraud mechanisms should be built into any approach.

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:TR as defined by the Member State.

# Test result certificate generation



*This section broadly describes the actors involved in generating a test result certificate. In the context of COVID-19, a DDCC:TR solution can be employed to generate a test result certificate for either proof of a negative SARS-CoV-2 test result or proof of previous SARS-CoV-2 infection.*

Processes for specimen collection, data collection, sample analysis and the generation of test reports (if required) will be defined by Member States and are outside the scope of this document. These activities will be preconditions for generating a test result certificate. Furthermore, Member States will need to define how a certificate will be generated, issued and adapted to their own contexts and levels of digital maturity, in compliance with their legal and policy frameworks.

Note that a test report and a test result certificate (DDCC:TR) serve different purposes (Table 2).

**Table 2**  
**Differences between a test report and a test result certificate**

	Test report	Test result certificate
Features	<ul style="list-style-type: none"> <li>→ Contains all relevant medical information</li> <li>→ Encodes detailed information for use by authorized health professionals</li> <li>→ Has no expiry date</li> <li>→ In combination with clinical symptoms, can aid diagnosis or evaluation of disease status</li> <li>→ May not be verified by a third party</li> </ul>	<ul style="list-style-type: none"> <li>→ Requires information contained in a test report in order to generate a DDCC:TR</li> <li>→ Provides a claim about the SARS-CoV-2 diagnostic test result of a Tested Person</li> <li>→ Contains the minimum information necessary for verifying the validity of the claim</li> <li>→ Has a time-bound validity period</li> <li>→ Is digitally signed and can be verified offline or online</li> </ul>
Possible uses	<ul style="list-style-type: none"> <li>→ Individual health purposes and clinical care</li> <li>→ Early detection and containment measures (e.g. contact tracing, case reporting, surveillance, screening)</li> <li>→ Depending on Member State policies, to inform vaccination requirements</li> </ul>	<ul style="list-style-type: none"> <li>→ Individualized exemptions from public health and social measures (e.g. post-exposure quarantine)</li> <li>→ To facilitate movement and access to socioeconomic activities (e.g. national and/or international travel, participation in mass gatherings) in the context of the COVID-19 pandemic</li> </ul>

## 3.1 Key settings, personas and digital services

Certificate generation is expected to involve the following settings.

1. **CERTIFICATE GENERATION SITE:** Where the certificate is generated. This site may be the same as where preconditions for the certificate generation process take place (i.e. where the testing takes place), but it does not have to be. The site would operate under the auspices of the Public Health Authority (PHA). This site could be a laboratory, temporary pop-up clinic or other type of facility, as determined by the Member State.
2. **CERTIFICATE ISSUANCE SITE:** Where the certificate is issued to the DDCC:TR Holder. This may be the same as the certificate generation site or could be an online website and/or application.

The key personas, or relevant stakeholders, involved in the provision of a DDCC:TR are outlined in Table 3. These key personas are anticipated to interact with the digital services outlined in Table 4, including digital services that might not have a user interface with which the key personas interact, but are critical building blocks of the reference architecture.

**Table 3**  
**Key personas for certificate generation**

Role	Description
Tested Person	The person who is tested for SARS-CoV-2 infection.
DDCC:TR Holder	The person who has the Tested Person's test result certificate. This person is usually, but not necessarily, the Tested Person. For example, a caregiver may hold the DDCC:TR for a child or other dependant.
Data Entry Personnel	The people who enter into a digital system the information about the Tested Person (as outlined in the core data set) that was manually recorded at a sample collection site. If a Digital Health Solution, such as an LIS, is in place, laboratory technicians may also be considered Data Entry Personnel, as they would be able to digitally document a test result through the LIS immediately.
Public Health Authority (PHA)	An entity or organization under whose auspices the test is performed and the DDCC:TR is issued.

LIS: laboratory information system.

**Table 4**  
**Digital services for certificate generation**

Digital service	Description
Digital Health Solution	A secure system that is used to record and/or manage a digital record of the DDCC:TR core data elements (e.g. an LIS). The Digital Health Solution is responsible for distribution of the DDCC:TR and any associated representations (such as a QR code) to the DDCC:TR Holder, based on the PHA's policy.
DDCC Generation Service <sup>a</sup>	The service responsible for taking data about a SARS-CoV-2 diagnostic test result, converting that data to use the HL7 FHIR standard, signing that HL7 FHIR document, and returning it to the Digital Health Solution. The signed HL7 FHIR document is the DDCC:TR. This service also registers the signed document in a location available to the DDCC Registry Service, (optionally) persists the signed HL7 FHIR document to the DDCC Repository Service, and potentially generates extra representations, such as QR code representations.
DDCC Registry Service <sup>b</sup>	The service that persists a record of the DDCC:TR certificate metadata and (optionally) the location of the DDCC Repository Service end point, which can be leveraged for online verification.
DDCC Repository Service <sup>c</sup>	An optional digital service that has a repository, or database, of the health content associated with each DDCC:TR. This service is able to return a copy of the DDCC:TR (the signed HL7 FHIR document) and potentially the barcode representation (e.g. a QR code) of the signed HL7 FHIR document.

FHIR: Fast Healthcare Interoperability Resources; HL7: Health Level Seven; LIS: laboratory information system; PHA: Public Health Authority.

<sup>a</sup> DDCC Generation Service can be used for generating both vaccination status and test result certificates.

<sup>b</sup> DDCC Registry Service can be used for persisting the records of vaccination status and test result certificates.

<sup>c</sup> DDCC Repository Service can be used as a repository for both vaccination status and test result certificates.

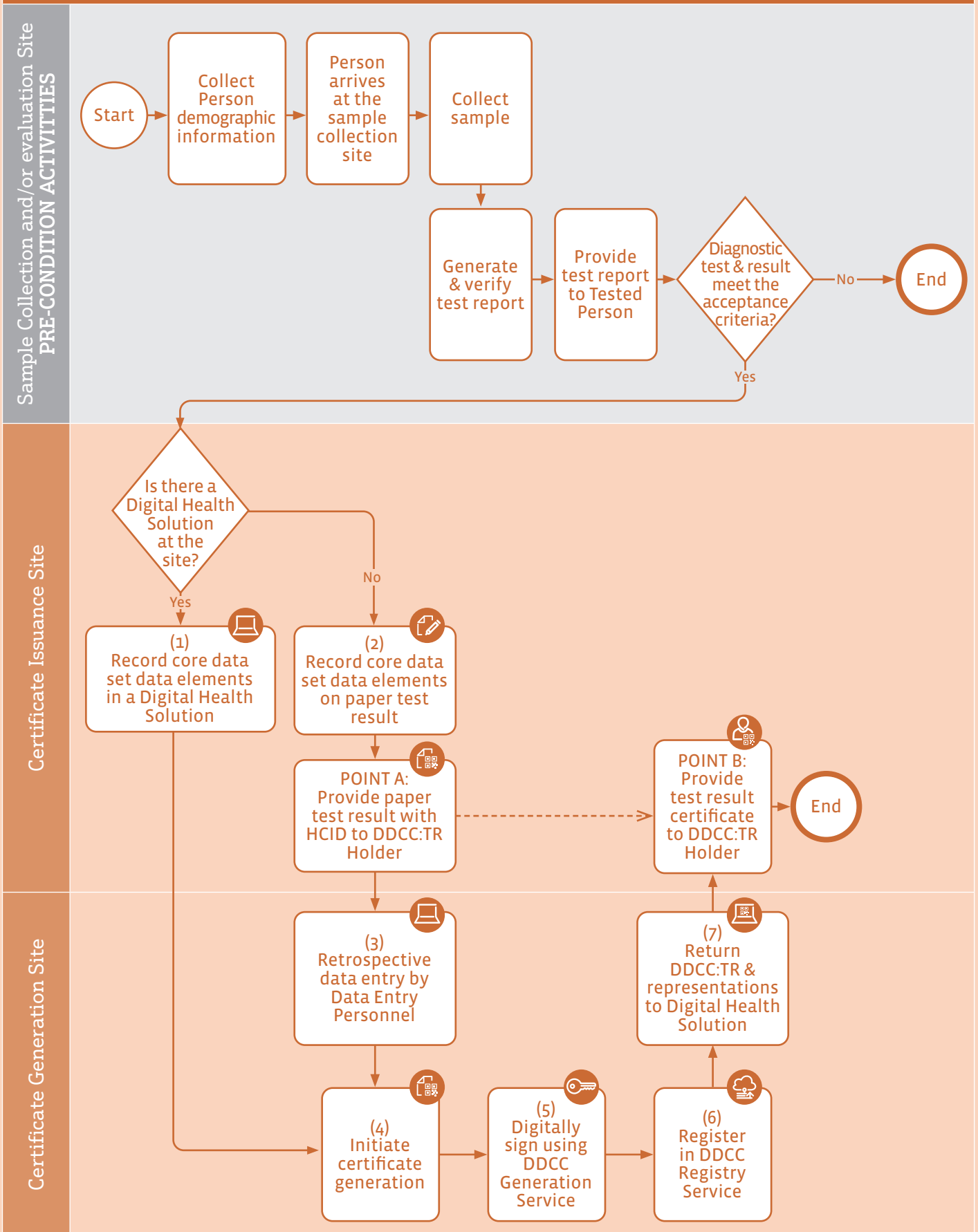
## 3.2 Certificate generation workflow

The process for certificate generation is summarized in Fig. 6. For a test result certificate to be generated, it is assumed that the following activities have already taken place as per the norms and processes of the Member State:

1. Demographic data about the person have been captured in accordance with the Member State's policies.
2. The person has arrived at the sample collection site to be tested for SARS-CoV-2.
3. The specimen has been collected and analysed.
4. A test report has been generated and verified by authorized personnel.
5. A test report has been given to the Tested Person.
6. The test type and corresponding result meet the acceptance criteria, as determined by the Member State, to generate a DDCC:TR.

Figure 6

### Certificate generation workflow



HCID: health certificate identifier

The workflow's actors and settings (Fig. 6) may be described as follows.<sup>1</sup>

1. The certificate issuance site MAY have a local Digital Health Solution. The Data Entry Personnel record details of the test event, which SHALL be recorded based on the DDCC:TR core data.
2. If a Digital Health Solution is not available at the certificate issuance site, details of the test event SHALL be initially recorded and persisted in a paper format that contains a health certificate identifier (HCID), according to the required DDCC:TR core data set. The paper test result SHALL have an HCID in a human-readable format and in a one-dimensional (1D) or two-dimensional (2D) barcode format. The HCID SHALL be used to establish a globally unique identifier (ID) for the DDCC:TR or to reference the ID of a previously established DDCC:TR. The paper test result with an HCID SHALL be provided to the DDCC:TR Holder at point A.
3. If a Digital Health Solution is not available at the certificate issuance site, details of the test event, in accordance with the DDCC:TR core data set, SHALL be retrospectively and electronically entered by Data Entry Personnel into a Digital Health Solution at the certificate generation site. The resulting test result certificate and/or its representations MAY be provided to the DDCC:TR Holder at point B. The paper test result with HCID issued at point A can now be used as a paper test result certificate.
4. The DDCC:TR core data set content is submitted to the DDCC Generation Service, and the certificate generation process is initiated.
5. The DDCC Generation Service SHALL generate a digitally signed Health Level Seven (HL7) Fast Healthcare Interoperability Resources (FHIR) document using a private key.
6. The signed HL7 FHIR document SHALL be registered in the DDCC Registry Service.
7. A digitally signed HL7 FHIR test result certificate (DDCC:TR) SHALL be generated, and a signed 2D barcode representation of the DDCC:TR MAY be generated by the DDCC Generation Service and returned to the Digital Health Solution. The resulting artefact SHALL be provided to the DDCC:TR Holder (who MAY be the Tested Person), as per the Member State's existing norms and practices, in a digital format at point B.

### 3.3 Functional requirements for certificate generation

To sign a digital document, public key infrastructure (PKI) technology is required. PKI supports the sharing of public keys that correspond to the private keys that have been used to cryptographically sign DDCC:TRs. The PKI may support the sharing of public keys from trusted international PHAs so that signed DDCC:TR representations issued by PHAs may be cryptographically verified. PKI is described in further detail in [Chapter 6](#) and [Annex 3](#).

Each Member State would be responsible for managing its own PKI through its PHA or another delegated authority. This document assumes that a PKI has already been deployed or is available within a country to support the DDCC:TR workflows described in this section.

<sup>1</sup> For definitions of "MAY", "SHALL" and "SHOULD", see the glossary.



High-level functional requirements for the activities described in Fig. 6 are presented in Table 5 as suggested features that any digital solution used to support DDCC:TR generation should 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:TR to take and adapt.

Non-functional requirements for certificate generation are included in [Annex 4](#).

**Table 5**  
**Functional requirements for certificate generation<sup>a</sup>**

Requirement ID	Functional requirement
DDCCTR.FXNREQ.001	It <b>SHALL</b> be possible to issue a new paper test result certificate to the Tested Person or DDCC:TR Holder for the purpose of recording the test event.
DDCCTR.FXNREQ.002	A PHA <b>SHALL</b> put in place a process to replace or reissue a lost or damaged paper test result certificate, with the necessary supporting technology.
DDCCTR.FXNREQ.003	It <b>SHALL</b> be possible to associate a globally unique HCID with a Tested Person's registered test result certificate(s).
DDCCTR.FXNREQ.004	It <b>SHALL</b> be possible to enter or attach the HCID as a 1D or 2D barcode to any paper test result certificate issued to the Tested Person (or DDCC:TR Holder).
DDCCTR.FXNREQ.005	It <b>SHALL</b> be possible to manually record the core data set content on a paper test result certificate issued to the Tested Person (or to the DDCC:TR Holder).
DDCCTR.FXNREQ.006	It <b>SHALL</b> be possible to manually sign the paper test result certificate 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.
DDCCTR.FXNREQ.007	It <b>SHALL</b> be possible to retrieve information about the diagnostic test event of the Tested Person from the content in the DDCC:TR or one of its representations.
DDCCTR.FXNREQ.008	All data concerning the test result <b>SHALL</b> be handled in a secure manner to respect the confidentiality of the Tested Person's health data.
DDCCTR.FXNREQ.009	Digital technology <b>SHALL NOT</b> be needed for any aspect of issuing a paper test result with HCID – the process <b>SHALL</b> function in an entirely offline and non-electronic manner.
DDCCTR.FXNREQ.010	Paper test result certificates and the validation markings they bear <b>SHALL</b> be designed to combat fraud and misuse.
DDCCTR.FXNREQ.011	If an offline Digital Health Solution is used to capture and manage SARS-CoV-2 diagnostic test results, and related content is available, then it <b>MAY</b> be responsible for outputting the test data using the HL7 FHIR standard.
DDCCTR.FXNREQ.012	If an offline Digital Health Solution is used to capture and manage SARS-CoV-2 diagnostic test results, has related content available, is part of the national PKI trust framework, and is authorized by the PHA to sign test result content as a DDCC:TR, then it <b>SHALL</b> register the DDCC:TR through the DDCC Registry Service.
DDCCTR.FXNREQ.013	If an online or connected DDCC Generation Service is available at the time of recording SARS-CoV-2 test results, then it <b>SHALL</b> be possible to register the test report as soon as possible after the result is available.
DDCCTR.FXNREQ.014	The DDCC Generation Service involved in the test result <b>SHALL</b> ensure encryption of data, in transit and at rest, to provide end-to-end security of personal data.

<b>DDCCTR.FXNREQ.015</b>	The DDCC Generation Service <b>MAY</b> be the agent responsible for issuing the HCID, provided that the HCID can be associated at the time of the test event in a timely manner. If the DDCC Generation Service is responsible for issuing HCIDs, it <b>SHALL</b> issue only unique HCIDs. The same HCID <b>SHOULD</b> never be reused for multiple Tested Persons.
<b>DDCCTR.FXNREQ.016</b>	If pre-generated HCIDs are used, the generation of the HCIDs, along with any supporting technology to ensure HCIDs will not be duplicated within or across certificate generation sites, <b>SHALL</b> be managed by PHA policy.
<b>DDCCTR.FXNREQ.017</b>	It <b>SHALL</b> be possible for the DDCC Generation Service to accept data transferred from an authorized, connected LIS where such a system exists.
<b>DDCCTR.FXNREQ.018</b>	It <b>SHALL</b> be possible for the DDCC Generation Service to represent test result data using the HL7 FHIR format.
<b>DDCCTR.FXNREQ.019</b>	It <b>SHALL</b> be possible for the DDCC Generation Service to digitally sign the HL7 FHIR document representation of the test result data.
<b>DDCCTR.FXNREQ.020</b>	It <b>MAY</b> be possible for the DDCC Generation Service to generate a machine-readable 2D barcode (e.g. a QR code) 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.
<b>DDCCTR.FXNREQ.021</b>	It <b>MAY</b> be possible for the DDCC Generation Service to generate a 2D QR code that includes the unencrypted minimum core data set content (in HL7 FHIR standard) of the test result, thus providing a machine-readable version of the test result certificate.
<b>DDCCTR.FXNREQ.022</b>	The DDCC Generation Service <b>SHALL</b> create an association between an HCID, the test result data associated with it in a DDCC:TR, any QR code generated from the data, and the private key used to sign the data.

1D: one-dimensional; 2D: two-dimensional; FHIR: Fast Healthcare Interoperability Resources; HCID: health certificate identifier; ID: identifier; HL7: Health Level Seven; LIS: laboratory information system; PHA: Public Health Authority.

<sup>a</sup> For definitions of "MAY", "SHALL" and "SHOULD", please see the glossary.

# Test result certificate verification and validation



*This section describes the use cases and actors involved in using a DDCC:TR for proof of a negative SARS-CoV-2 test result or proof of previous SARS-CoV-2 infection, and functional requirements for a digital solution.*

Certificate **verification** relies on the Verifier confirming the status of a test result certificate and ensuring that the certificate is a true and unaltered certificate that has been signed and issued under the authority of a Public Health Authority (PHA) of a Member State. Certificate verification depends on the PHA having access to a trusted means of digitally signing a Health Level Seven (HL7) Fast Healthcare Interoperability Resources (FHIR) document that represents the core data set content for the DDCC:TR.

Certificate **validation** relies on the Verifier validating and accepting the test result certificate based on the acceptance criteria and associated validity period determined by the policies of the Member States in which the certificate will be used. The acceptance criteria or business rules for acceptance of a test result certificate and for the validity period for each proof scenario are discussed in more detail in section 4.1.

## 4.1 Proof scenarios

In the context of certificate validation, the DDCC:TR can be leveraged in one of two ways, as: (a) proof of a negative SARS-CoV-2 test result, or (b) proof of previous SARS-CoV-2 infection. It will be at the discretion of the Member States to define the purposes for which proof scenarios are applied and adapted to their own contexts and levels of digital maturity, in compliance with their legal and policy frameworks. Member States will need to determine the related workflows and the criteria for acceptance of a test result certificate and the validity period for each proof scenario for domestic and/or international use cases. The validity period is determined by the policies of the country in which the certificate will be used.

Table 6 provides example acceptance criteria structures to support each type of proof. These criteria will need to be established and clearly communicated by Member States based on their local policies and on agreements made with other Member States. The Event Information Site for National IHR Focal Points, maintained by the WHO Secretariat, contains timely information related to testing regimes from different countries.

**Table 6**  
**Example of acceptance criteria or business rule decisions to support each type of proof scenario**

Proof scenario	Test type <sup>a</sup>	Test result	Validity period <sup>b</sup>
Proof of previous SARS-CoV-2 infection	Determined by the Member State	Detected	Sample date more than [number of days] ago and less than [number of days] ago
Proof of negative SARS-CoV-2 test result	Determined by the Member State	Not detected	Sample time less than [number of hours] ago

<sup>a</sup> The accepted types of SARS-CoV-2 diagnostic tests will need to be determined by the Member State in which the certificate will be used, for each proof scenario.

<sup>b</sup> The time periods, to be defined by the Member State in which the certificate will be used, are given in square brackets.

Acceptance criteria for proof of previous SARS-CoV-2 infection should reflect each Member State's risk-based approach (6,18). As the available science evolves, and as the application of risk-based approaches may evolve, it is expected that WHO guidance related to these acceptance criteria will also evolve.

## 4.2 Key settings, personas and digital services

As with Digital Documentation of COVID-19 Certificates: Vaccination Status (DDCC:VS), the DDCC:TR includes a verification site where people can present their SARS-CoV-2 diagnostic test result. There are a variety of possible verification sites (e.g. restaurants, airports, cinemas), but how, when, where and by whom the DDCC:TR can be verified and validated should be defined and regularly updated by the Member State in which the certificate is intended to be used. Relevant policies, including data protection policies, should be put in place by the Member State accordingly.

The key personas, or relevant stakeholders, involved in the verification and validation of a DDCC:TR are outlined in Table 7. These key personas are anticipated to interact with digital services (Table 8). Not all these digital services will have a user interface that the key personas directly interact with, but the services are still critical building blocks of a DDCC:TR system architecture.

**Table 7**  
**Key personas for test result certificate verification and validation**

Role	Description
DDCC:TR Holder	The person who wants to assert a claim related to a SARS-CoV-2 diagnostic test result. This person could be the Tested Person or, for example, a caregiver who holds the DDCC:TR for a child or other dependant.
Verifier	The person or entity that wants to verify and validate the claim of a diagnostic test result (i.e. verify the digital signature and validate the test result shown on a DDCC:TR for proof of a negative SARS-CoV-2 test result or proof of previous SARS-CoV-2 infection, using a predefined set of acceptance criteria or business rules).
National Public Health Authority (PHA)	The entity under whose auspices a SARS-CoV-2 diagnostic test is performed and a DDCC:TR is issued. The National PHA is also responsible for the DDCC Generation Service and the DDCC Registry Service.
International PHA	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 8**  
**Digital services for test result certificate verification and validation**

Digital service	Description
Health Certificate Identifier (HCID)	<p>A unique identifier for a physical and/or digital health folder that contains one or more DDCC:TR. The HCID may be provided by an existing national system or, alternatively, also be issued directly by the DDCC Generation Service, which will then encode the ID in the DDCC:TR. The HCID appears on paper test result certificates in both a human-readable format and as a 1D or 2D barcode. The HCID is included as a data element in the DDCC:TR core data set.</p> <p>An index that associates the HCID with metadata about the DDCC:TR is stored in the DDCC Registry Service.</p>
Verifier Application	A digital solution that can inspect, cryptographically verify, and validate the DDCC:TR using a predefined set of acceptance criteria or business rules. This can be an application on a mobile phone or otherwise, and it can operate online or offline.
DDCC Registry Service	<p>The service that persists a record of the DDCC:TR certificate metadata and (optionally) the location of the DDCC Repository Service end point, which can be leveraged for online verification.</p> <p>The DDCC Registry Service can be utilized to determine whether a DDCC:TR has been revoked, for example due to revocation of a key within the PKI or issues within the supply chain.</p>
DDCC Repository Service	The optional service that may be leveraged to look up a DDCC:TR and/or return one or more representations of the DDCC:TR based on the DDCC:TR HCID. The DDCC Repository Service may be implemented as a single centralized database or as a federation of databases.
Public Key Directory (PKD)	The service that maintains the public keys (and, potentially, the PKI certificate revocation lists) of all DSCs that have been used to digitally sign each DDCC:TR and 2D barcode representation of a DDCC:TR artefact. Verifier Applications that support offline verification will need to regularly refresh their local PKD cache from the PKD.

1D: one-dimensional; 2D: two-dimensional; DSC: document signer certificate; ID: identifier; PKI: public key infrastructure.

### 4.3 Test result certificate verification and validation workflows and use cases

The process for certificate verification is summarized in Fig. 7. It is assumed that for a test result certificate and/or its representations to be verified, the following activities have already taken place as per the norms and processes of the Member State.

1. A signed HL7 FHIR document, the DDCC:TR, has been generated by the DDCC Generation Service and registered within the DDCC Registry Service. Optionally, the DDCC:TR may be persisted to a DDCC Repository Service.
2. The Verifier Application has, as part of a regular update procedure, downloaded and cached the public keys of all verifiable DDCC:TR 2D barcodes from the Public Key Directory (PKD) service as well as, optionally, a set of public key infrastructure (PKI) certificate revocation lists that denote public keys that have been revoked.
3. The DDCC:TR Holder is presenting a digitally signed DDCC:TR or representation(s) of it signed by a document signer certificate (DSC) for which the Verifier Application has a cached copy of the relevant public key.
4. The DDCC:TR Holder's 2D barcode is encoded using a format that is understandable by the Verifier Application and can be used to link to the corresponding digital certificate in the National PHA's trusted online verification service.

The workflow's actors and settings, and its related high-level requirements, may be described as follows (Fig. 7).

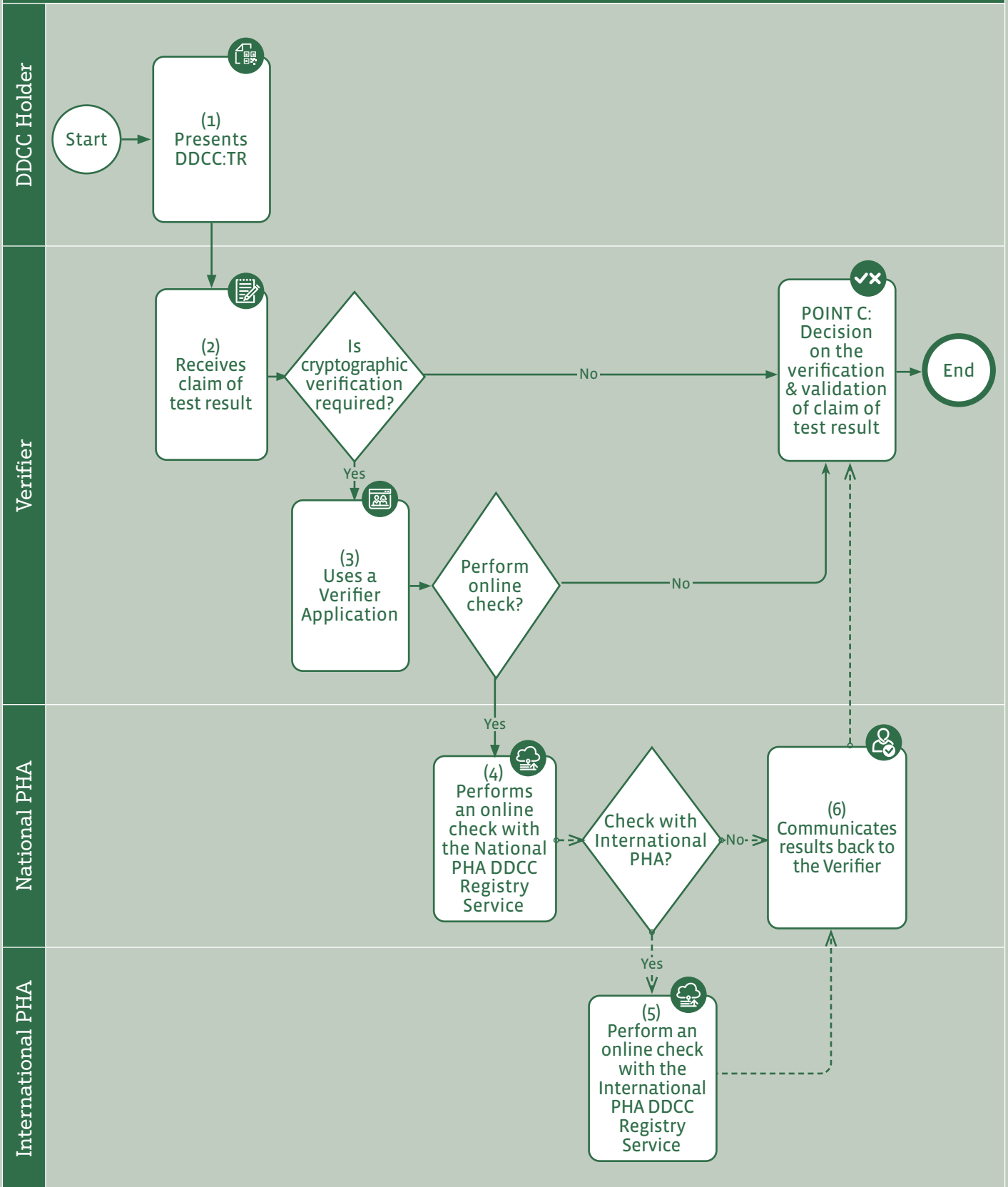
1. A DDCC:TR Holder presents a DDCC:TR to a Verifier in support of a claim of a SARS-CoV-2 diagnostic test result.
2. To verify and validate the claim by a verifiable DDCC:TR Holder of a SARS-CoV-2 diagnostic test result, there are four pathways that a Verifier could take to check the SARS-CoV-2 diagnostic test result claim at point C, elaborated in Table 9 and Figs. 8–11. A Verifier may:
  - a. visually verify and validate a DDCC:TR (manual verification);
  - b. verify and validate using a digitally signed, machine-readable representation of the core data set content (e.g. as a 2D barcode) (offline cryptographic verification); or
  - c. verify and validate by scanning a machine-readable version of the health certificate identifier (HCID) for the DDCC:TR and accessing a verification service (online status check [for a national or an international DDCC:TR]).

Note that, regardless of the use case, a DDCC Generation Service is required as a precondition to support registration of a DDCC:TR within the DDCC Registry Service, which is required as part of the certificate generation workflow (see [section 3.2](#)).

The DDCC Repository Service is optional, depending on which use case is being implemented. To support online verification, both the DDCC Registry Service and DDCC Repository Service are required.

Figure 7

Test result certificate verification and validation<sup>a</sup>



PHA: public health authority

<sup>a</sup> The business process symbols used in the workflows are explained in [Annex 1](#).

### 4.3.1 Test result certificate verification and validation use cases

The workflow diagram in Fig. 7 shows four possible verification and validation pathways. These use cases for test result certificate verification and validation are listed in Table 9 and shown separately in Figs. 8–11. The required digital services for each use case are also outlined in Table 9.

Table 9  
Test result certificate verification and validation use cases

Use case ID	TR001	TR002	TR003	TR004
Use case name	Manual verification and validation	Offline cryptographic verification and validation	Online status check (National DDCC:TR)	Online status check (International DDCC:TR)
Figure	Fig. 8	Fig. 9	Fig. 10	Fig. 11
Use case description	A Verifier verifies and validates a DDCC:TR based on its human-readable content using purely visual means and based on subjective judgement. This type of check is common, is currently well accepted, is quick and easy to do, and requires no digital technology.	A Verifier verifies and validates a DDCC:TR using digital cryptographic processes in an offline mode	This pathway is used when the DDCC:TR is being verified and validated in the same jurisdiction as it was issued. A Verifier verifies and validates a DDCC:TR using digital cryptographic processes in an online mode that includes a status check against the PHA's DDCC Registry Service and optionally the DDCC:TR Repository Service.	This pathway is used when the DDCC:TR is being verified in a foreign jurisdiction other than where it was issued. A Verifier verifies and validates an internationally issued DDCC:TR using digital cryptographic processes in an online mode that includes a status check against the National PHA's DDCC Registry Service, which in turn accesses an International PHA's DDCC:TR Registry and DDCC:TR Repository Services, if such services exist and such access is authorized by the issuing PHA. It is assumed in this workflow that a Verifier does not directly access an International PHA's DDCC:TR Registry or Repository Service.
Connectivity required?	Offline	Offline	Online	Online
Level of verification	Verification is visually performed by the Verifier. As judgement can be subjective, it relies on policies of the Member State to protect against discrimination and detect fraud.	<ul style="list-style-type: none"> <li>→ Can confirm that the HCID barcode on the printed test result is valid and has not been altered.</li> <li>→ Can confirm whether the DDCC:TR has been issued by an authorized PHA.</li> <li>→ Can confirm that the hash of any signed 2D barcode matches the health content represented therein.</li> </ul>	<ul style="list-style-type: none"> <li>→ Can confirm that the HCID barcode on the paper card is valid and has not been altered.</li> <li>→ Can confirm whether the DDCC:TR has been issued by an authorized PHA.</li> <li>→ If authorized to do so, can confirm that the content on a DDCC:TR paper card matches the DDCC:TR digital content.</li> <li>→ Can confirm that the hash of any signed 2D barcode matches the health content represented therein.</li> <li>→ Can check whether signed 2D barcodes containing DDCC:TR content have been revoked or updated.</li> </ul>	<ul style="list-style-type: none"> <li>→ Can confirm that the HCID barcode on the paper card is valid and has not been altered.</li> <li>→ Can confirm whether the DDCC:TR has been issued by an authorized PHA.</li> <li>→ If authorized to do so, can confirm that the content on a DDCC:TR paper card matches the DDCC:TR digital content.</li> <li>→ Can confirm that the hash of any signed 2D barcode matches the health content represented therein.</li> <li>→ Can check whether signed 2D barcodes containing DDCC:TR content have been revoked or updated.</li> </ul>



## SECTION 4

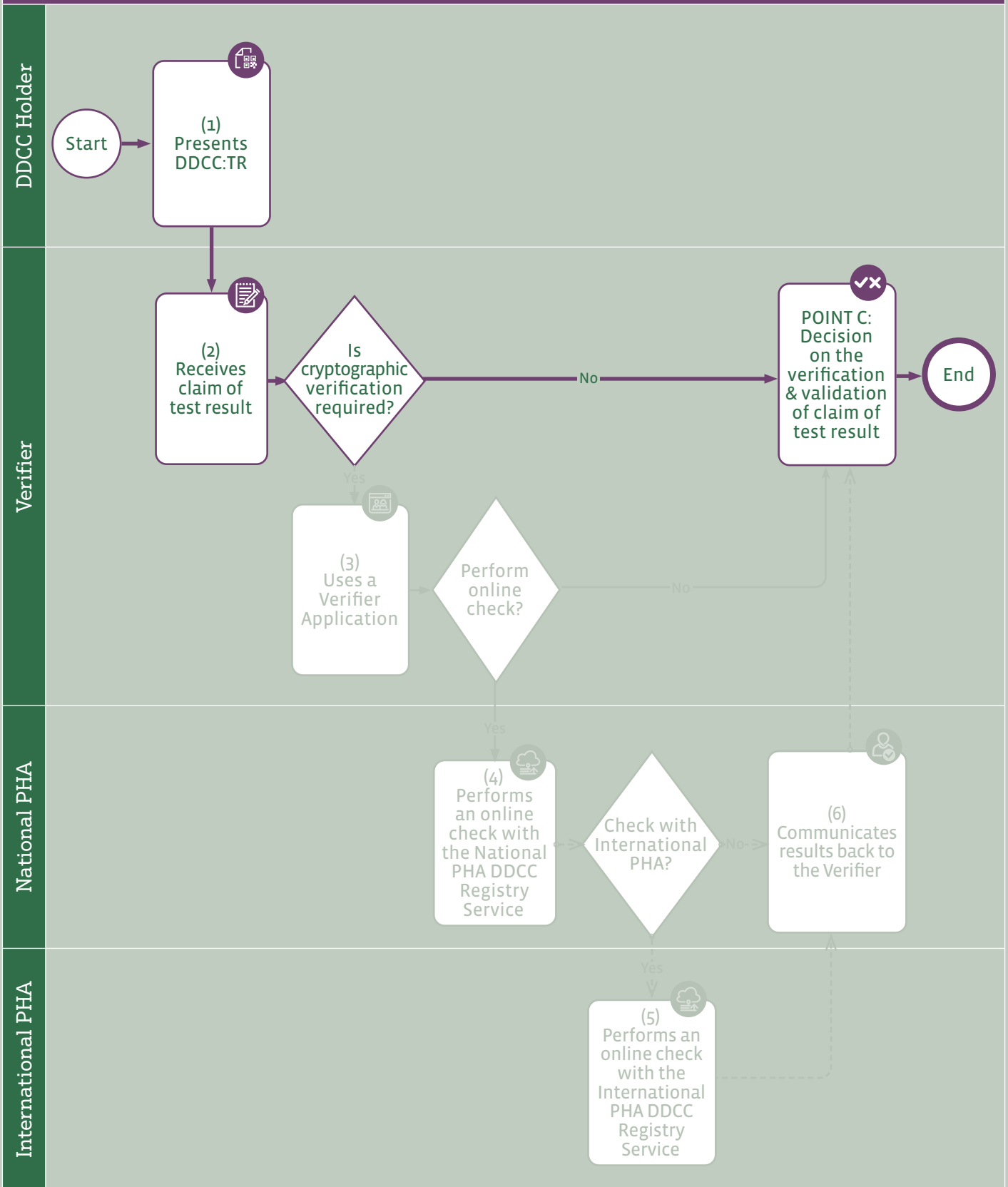
**Test result certificate verification and validation**

<b>Level of validation</b>	Validation is visually performed by the Verifier. The Verifier manually validates the certificate based on the acceptance criteria and validity period determined by the policies of the Member State.	Can confirm that the certificate is valid based on the automatic check conducted by the Verifier Application using a predefined set of acceptance criteria determined by the policies of the Member State.	Can confirm that the certificate is valid based on the automatic check conducted by the Verifier Application using a predefined set of acceptance criteria determined by the policies of the Member State.	Can confirm that the certificate is valid based on the automatic check conducted by the Verifier Application using a predefined set of acceptance criteria determined by the policies of the Member State.
<b>Verify whether the DDCC:TR has been revoked?</b>	Not possible	Possible if a cache of revoked certificates is maintained by the Verifier	Possible	Possible
<b>DDCC Registry Service</b>	Not required	Required	Required	Required
<b>DDCC Repository Service</b>	Not required	Optional	Required	Required

HCID: health certificate identifier; ID: identifier; PHA: Public Health Authority.

Figure 8

**Test result certificate verification and validation: manual verification and validation use case<sup>a</sup>**

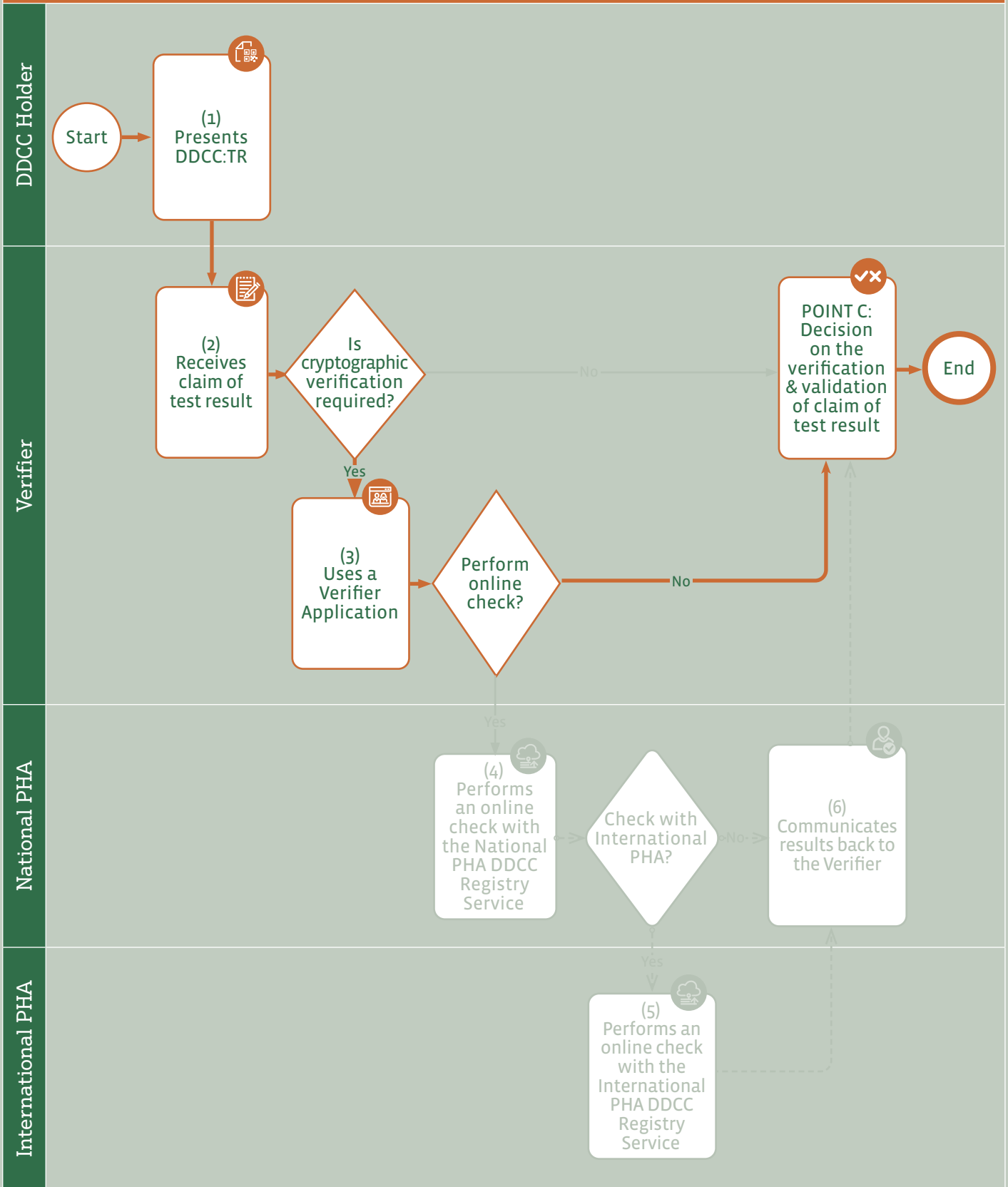


PHA: public health authority

<sup>a</sup> The business process symbols used in the workflows are explained in [Annex 1](#).

Figure 9

### Test result certificate verification and validation: offline cryptographic verification use case<sup>a</sup>

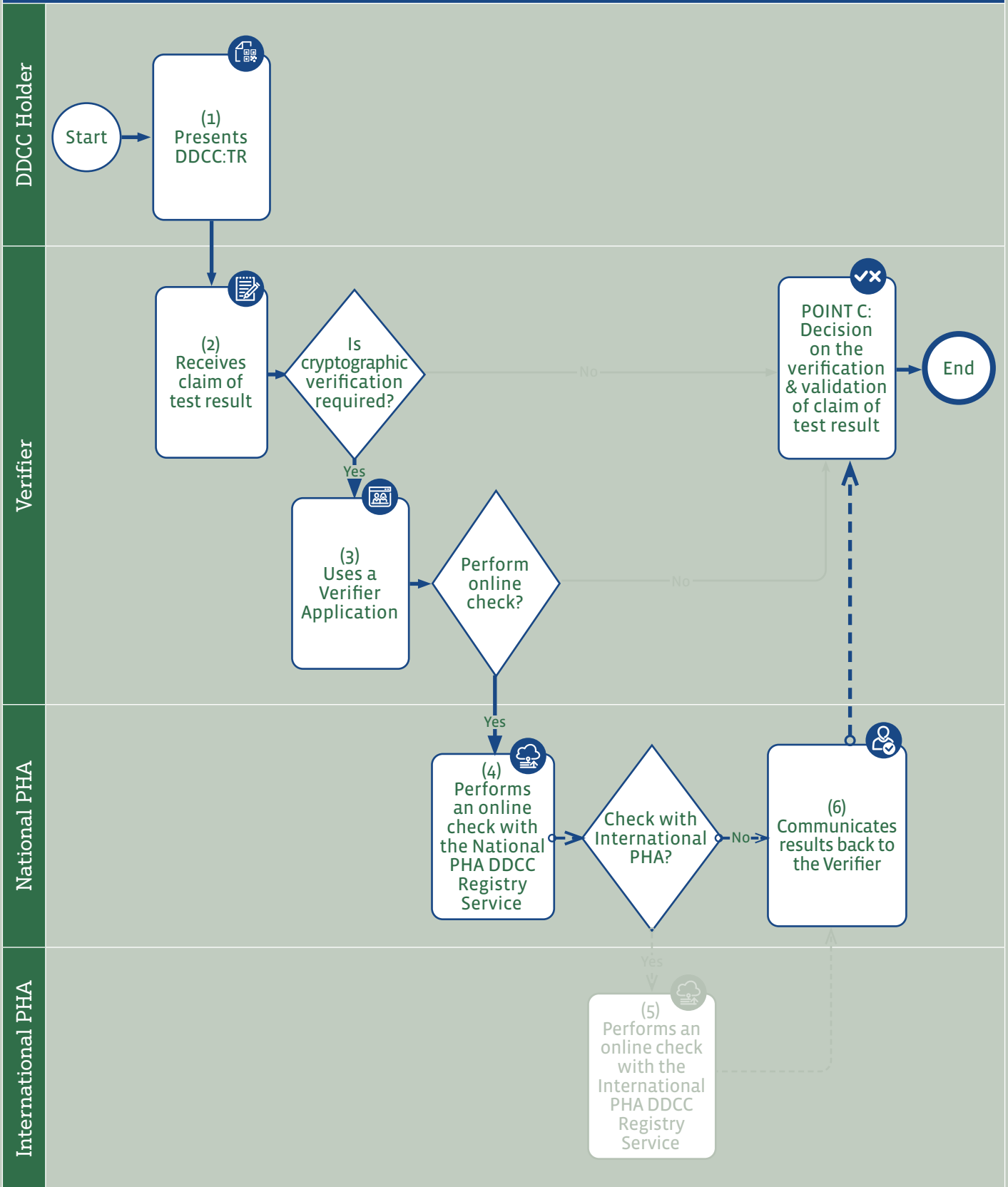


PHA: public health authority

<sup>a</sup> The business process symbols used in the workflows are explained in [Annex 1](#).

Figure 10

**Test result certificate verification and validation: online status check (national DDCC:TR) use case<sup>a</sup>**

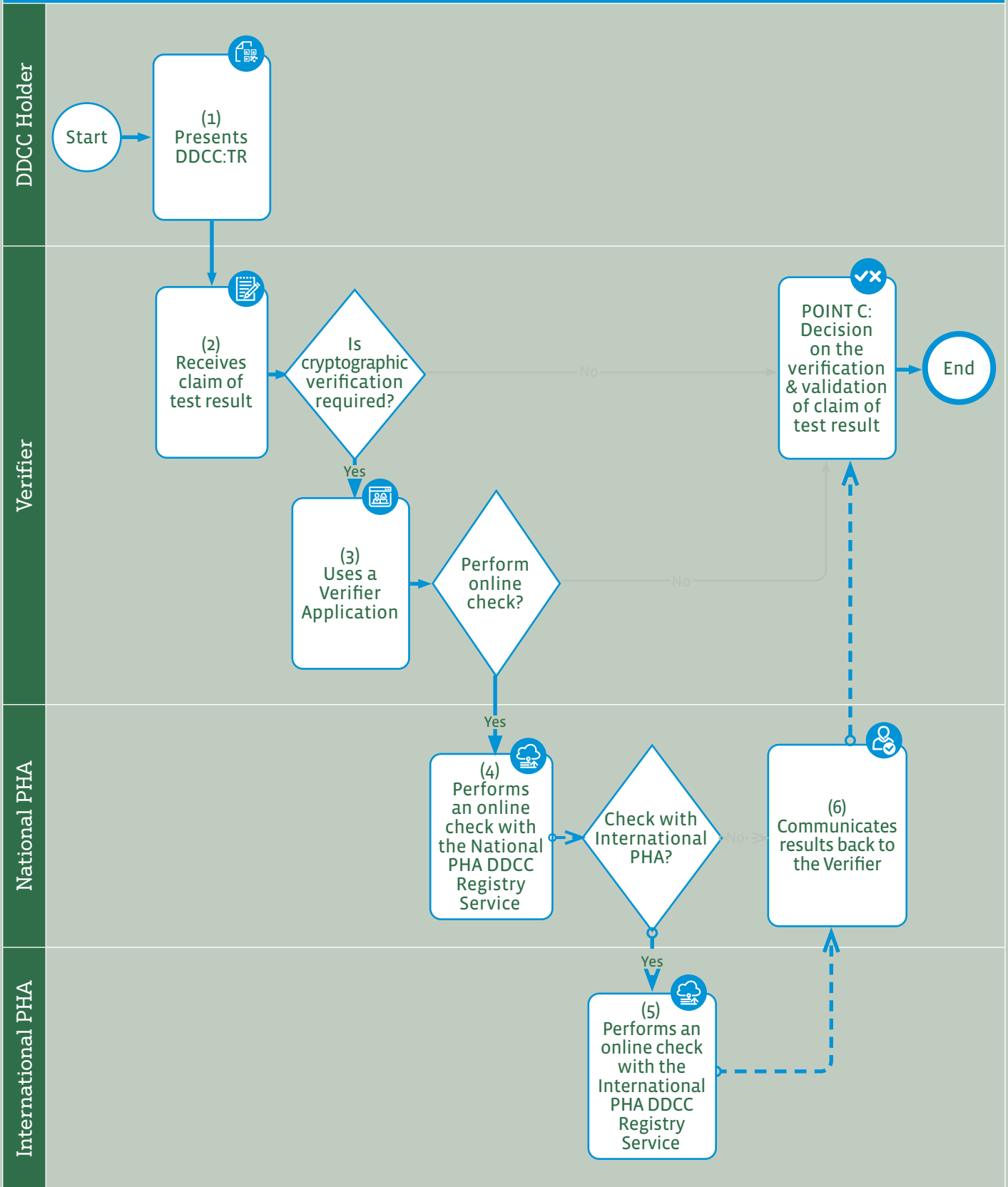


PHA: public health authority

<sup>a</sup> The business process symbols used in the workflows are explained in [Annex 1](#).

Figure 11

**Test result certificate verification and validation: online status check (international DDCC:TR) use case<sup>a</sup>**



PHA: public health authority

<sup>a</sup> The business process symbols used in the workflows are explained in [Annex 1](#).

### 4.3.2 Operationalizing the test result certificate verification and validation use cases

The WHO DDCC HL7 FHIR implementation guide (available at <https://worldhealthorganization.github.io/ddcc>) (17) includes implementable specifications for the test result certificate verification and validation use cases described in this document. The WHO DDCC HL7 FHIR implementation guide contains a standards-compliant specification that explicitly encodes interoperable logic, including data models, terminologies and logic expressions, in a computable language sufficient for the implementation of test result certificate verification and validation use cases.

## 4.4 Functional requirements for test result certificate verification and validation

High-level functional requirements for the activities described in *Fig. 7* are presented in Table 10 as suggested features that any digital solutions that would facilitate DDCC:TR verification and validation may have. These guidance requirements are to be only used as a starting point to be adapted by Member States or other interested parties that need to develop their own specifications for a digital solution for DDCC:TR.

Non-functional requirements are included in *Annex 4*.

Table 10

**Test result certificate verification and validation functional requirements<sup>a</sup>**

Requirement ID	Functional requirement	TR001 Manual	TR002 Offline	TR003 Online - National	TR004 Online- International
DDCCTR.FXNREQ.023	Paper test result certificates and the validation markings they bear <b>SHOULD</b> be designed to combat fraud and misuse. Any process that generates a paper test result certificate <b>SHOULD</b> include elements that support the Verifier in visually checking that the paper test result certificate is genuine (e.g. watermarks, holographic seals, etc.) without the use of digital technology.	✓	✓	✓	✓
DDCCTR.FXNREQ.024	If a paper test result document bearing a 1D or 2D barcode is presented to a Verifier, then it <b>SHALL</b> be possible for the Verifier to scan the code and, at a minimum, read the HCID encoded in the barcode, to visually compare it with the HCID written or printed on the paper test result certificate, if present.		✓	✓	
DDCCTR.FXNREQ.025	If a paper test result certificate or computable test report document bears a QR code and that barcode includes a digital signature, then it <b>MAY</b> be possible for the Verifier to check the signature, using information downloaded from a PKD, to ensure it is genuine.			✓	✓
DDCCTR.FXNREQ.026	It <b>MAY</b> be possible to log all offline verification operations so that, at a later stage when an online connection is available, verification and validation decisions can be reviewed and reconfirmed against data, such as the HCID and public key, provided by the online DDCC Registry Service. For example, this may be done to confirm that a certificate that was checked offline in the morning using public key and revocation data downloaded from the DDCC Registry Service the day before has not been added to a public key revocation list issued that same day. However, personal data, such as name and date of birth, accessed at the point of verification of the DDCC:TR should not be retained and stored in a repository, database or otherwise.		✓		

## SECTION 4

## Test result certificate verification and validation

Requirement ID	Functional requirement	TR001 Manual	TR002 Offline	TR003 Online – National	TR004 Online– International
DDCCTR.FXNREQ.027	It <b>SHALL</b> always be possible to perform some form of offline verification and validation of paper test result certificates; any solution should be designed so that a loss of connectivity to online components of the solution does not force the verification and validation work to stop.		✓	✓	✓
DDCCTR.FXNREQ.028	If, at the time of verification, a Verifier has connectivity to a DDCC Registry Service managed by a PHA, then it <b>SHALL</b> be possible to query whether the HCID in the barcode, and the public key, if also present, of the paper test result certificate is currently valid.			✓	✓
DDCCTR.FXNREQ.029	When making the verification check, any solution <b>SHALL</b> send only the minimum information required for the verification to complete. The minimum information comprises the metadata (see <a href="#">section 5.2</a> ) and the digital signature of the DDCC:TR.			✓	✓
DDCCTR.FXNREQ.030	When receiving a request for verification, a PHA <b>SHALL</b> consult its DDCC 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.			✓	✓
DDCCTR.FXNREQ.031	A PHA servicing a request for verification of a test result certificate via an HCID <b>MAY</b> respond with basic details of the Tested Person (i.e. name, date of birth), in accordance with PHA policies, so that the Verifier can confirm that the paper test result certificate corresponds with the DDCC:TR Holder who has presented for verification.			✓	✓
DDCCTR.FXNREQ.032	A PHA <b>SHALL</b> 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 <b>MAY</b> be linked to the DDCC Generation Service to associate public keys with HCIDs.		✓	✓	✓
DDCCTR.FXNREQ.033	A PHA <b>MAY</b> 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.			✓	✓
DDCCTR.FXNREQ.034	A PHA <b>SHALL</b> be able to return a verification status, as defined by the implementer, to a requestor, based on the information provided.			✓	✓
DDCCTR.FXNREQ.035	A PHA <b>MAY</b> be able to service individual verification requests (i.e. details relating to one test result certificate) or requests sent in bulk (details of multiple certificates sent in one request).			✓	✓
DDCCTR.FXNREQ.036	When receiving a request for verification, a PHA <b>MAY</b> respond with the most recent test result certificate or provide a history of test result certificates, in accordance with Member State policies regarding privacy and consent.			✓	✓
DDCCTR.FXNREQ.037	A PHA <b>SHOULD</b> be able to validate that the requestor making a verification request is an authorized agent, but <b>MAY</b> also allow anonymous verification requests.			✓	✓
DDCCTR.FXNREQ.038	The certificate authority (or authorities) in each country <b>SHALL</b> maintain records of the DSCs issued for the purpose of signing test result certificates and expose any service(s) that allow a public key to be looked up and checked against its records to check for validity.			✓	✓
DDCCTR.FXNREQ.039	Any communication between a Verifier and a DDCC Registry Service or other data service managed by a PHA <b>SHALL</b> be secured to prevent interference with the data in transit and at rest.			✓	✓
DDCCTR.FXNREQ.040	SMS-based verification of alphanumeric HCIDs <b>MAY</b> be provided by a PHA as a means of sending a verification request or receiving a response with a status code.			✓	

Requirement ID	Functional requirement	TR001 Manual	TR002 Offline	TR003 Online – National	TR004 Online– International
DDCCTR.FXNREQ.041	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 <b>SHOULD</b> have a means of transferring the request and querying the data held by that authority.				✓
DDCCTR.FXNREQ.042	A Member State <b>SHOULD</b> put in place bilateral or multilateral agreements with other countries or with a supranational entity or regional body for access to other countries' test result certificate metadata and digital signatures.		✓		
DDCCTR.FXNREQ.043	A Member State <b>SHOULD</b> put in place bilateral or multilateral agreements with other countries or with a supranational entity or regional body for access to other countries' test result certificate test event data and digital signatures.				✓
DDCCTR.FXNREQ.044	Communications between one country and another country's PHA or a supranational DDCC Registry Service <b>SHALL</b> be secure and prevent interference with the metadata or data in transit and at rest.		✓		✓
DDCCTR.FXNREQ.045	It <b>SHALL</b> be the ultimate responsibility of the country where verification and validation take place to decide whether a test result claim is accepted or not.		✓		✓
DDCCTR.FXNREQ.046	There <b>SHOULD</b> be a mechanism for the country that issued a DDCC to revoke a DDCC.		✓	✓	✓
DDCCTR.FXNREQ.047	There <b>SHOULD</b> be a mechanism for a verifying country to be able to determine whether a certificate issued by an issuing country has been revoked.		✓		✓
DDCCTR.FXNREQ.048	A Verifier Application <b>SHALL</b> be able to perform a check against the defined set of acceptance criteria, as defined by the Member State's policies, to check for validity of the certificate.		✓	✓	✓
DDCCTR.FXNREQ.049	There <b>SHOULD</b> be a mechanism for the Verifier Application to be regularly updated with the defined set of acceptance criteria, in accordance with the latest policies defined by the Member State.		✓	✓	✓

<sup>a</sup> For definitions of "MAY", "SHALL" and "SHOULD", please see the glossary.



## DDCC:TR core data set



*The DDCC:TR core data set includes data elements about the Tested Person and SARS-CoV-2 diagnostic test result and related information that is required to support proof of a negative SARS-CoV-2 test result or proof of previous SARS-CoV-2 infection. Member States may use the DDCC:TR core data set as defined or may continue to use their existing terminology, with a map to the DDCC:TR core data set, so long as it contains the required data elements in the DDCC:TR core data set. The recommended core data set is intended to include the critical data required for interoperability, specific to each proof scenario defined and driven by public health needs. 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, existing digital certificates and guidelines such as ICAO VDS-NC for travel-related public health proofs (28), the EU DCC (29), DIVOC (30) and SMART Health Cards (31) were considered.

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 SARS-CoV-2 diagnostic test result for the purposes of a DDCC:TR 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 DIGITALLY AND ON 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.

To underscore the importance of the ability to implement, the data content model for the DDCC:TR core data set has been developed as a Health Level Seven (HL7) Fast Healthcare Interoperability Resources (FHIR) implementation guide. The DDCC implementation guide is based on the widely adopted HL7 FHIR international patient summary (IPS) health data content model (36). Specific linkages to the IPS data model are provided in the WHO DDCC HL7 FHIR implementation guide (available at <https://worldhealthorganization.github.io/ddcc>) (17).

International Classification of Health Interventions (ICHI) and International Classification of Diseases (ICD) are the preferred terminology standards for DDCC:TR. To support broadly deployed legacy systems, the DDCC:TR normative core data set includes one-to-one equivalent mapping to Systematized Nomenclature of Medicine Clinical Terms Global Patient Set (SNOMED CT GPS) codes that may be leveraged, in some cases, as allowed alternatives (37).

ICHI is a common tool for reporting and analysing health interventions (38). ICHI covers interventions that are carried out by a broad range of providers across all sectors of the health system, such as diagnostic, medical, surgical, mental health, primary care, functioning support and public health. ICHI also allows for a high level of detail for all kinds of clinical documentation and data usage. Extension codes are provided to allow users to describe detail about the intervention in addition to the relevant ICHI code.

The 11th revision of the ICD (ICD-11), which came 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:TR data dictionary (33). ICD-11 is:

- a global public good that is completely free and available for all to use in its entirety; no payment is 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:TR;
- easy to integrate into software systems via a public application programming interface (API) for use in all settings, without additional tooling; this is due to the digital multilingual structure of ICD-11; and
- human-readable and machine-readable.

For the guiding principles of the WHO Family of International Classifications (WHO-FIC) and other classifications, and terminology mapping in the context of the WHO DDCC:TR, see [Annex 2](#).

## 5.2 Core data elements

The three key sections of the core data set are:

1. header section
2. SARS-CoV-2 test event section, which includes data elements for each test result
3. certificate metadata.

The **header section** data elements (Table 11) include the Tested Person's identifier (ID). The header section captures information about the Tested Person so that information in the test result certificate can be linked to a specific person.

**Table 11**  
**Header section of the DDCC:TR, with preferred code system**

Data element label	Description	Data type	Preferred code system	Requirement status for proof of negative SARS-CoV-2 test result	Requirement status for proof of previous SARS-CoV-2 infection
<b>Name</b>	The full name of the Tested Person	String	Not applicable	Required	Required
<b>Date of birth</b>	The Tested Person's date of birth, if known. If unknown, use assigned date of birth for administrative purposes.	Date <sup>a</sup>	Complete date (YYYY-MM-DD) compatible with HL7 FHIR date format	Required	Required
<b>Unique identifier</b>	Unique ID for the Tested Person, according to the policies applicable to each country. More than one unique identifier may be used to link records (e.g. national ID, health ID, medical record ID).	ID	Not applicable	Optional	Optional

ID: identifier

<sup>a</sup> HL7 FHIR date format is available at <https://www.hl7.org/fhir/datatypes.html#date>.

The **SARS-CoV-2 test event** section outlines the data elements to collect for each SARS-CoV-2 test (Table 12).

**Table 12**  
**Data elements for each SARS-CoV-2 test event, with preferred code system**

Data element label	Description	Data type	Preferred code system	Requirement status for proof of negative SARS-CoV-2 test result	Requirement status for proof of previous SARS-CoV-2 infection
<b>Pathogen targeted</b>	Name of the pathogen being tested for (i.e. SARS-CoV-2)	Coding <sup>a</sup>	ICD-11	Required	Required
<b>Type of test</b>	Name of the type of test that was conducted, e.g. NAAT or Ag-RDT	Coding	ICHI	Required	Required
<b>Test brand</b>	The brand or trade name used to refer to the test conducted	Coding	As defined by Member State	Optional	Optional
<b>Test manufacturer</b>	Name of the manufacturer of the test conducted	Coding	As defined by Member State	Optional	Optional
<b>Specimen sample origin</b>	Type of sample that was taken, e.g. nasopharyngeal swab or saliva specimen	Coding	ICHI	Optional	Optional
<b>Date and time of sample collection</b>	Date and time when sample was collected	dateTime <sup>b</sup>	Compatible with HL7 FHIR dateTime with time zone specified	Required	Required
<b>Test result</b>	Presence of SARS-CoV-2 infection: "Detected" or "Not detected"	Coding	ICD-11	Required	Required
<b>Test centre or facility name</b>	A codable name or identifier of the facility responsible for conducting the test	Coding	As defined by Member State	Optional	Optional
<b>Test centre country</b>	The country in which the individual was tested	Coding	ISO 3166-1 alpha-3 (or numeric)	Required	Required

Ag-RDT: antigen detection rapid diagnostic test; FHIR: Fast Healthcare Interoperability Resources; HL7: Health Level Seven; ICD-11: International Classification of Diseases 11th Revision; ICHI: International Classification of Health Interventions; ID: identifier; ISO: International Organization for Standardization; NAAT: nucleic acid amplification test.

<sup>a</sup> Coding data element types are multiple choice, and the input options, or values, are data elements taken from a set of predefined options (e.g. type of test, test brand).

<sup>b</sup> HL7 FHIR dateTime format is available at <https://www.hl7.org/fhir/datatypes.html#dateTime>.

The **test result certificate metadata** (Table 13) contain data elements that are not typically visible to the user, but that are required to be linked to the certificate itself. It is anticipated that additional metadata elements will be added by Member States at the time when certificates are generated, to support implementation of specific use cases.

**Table 13**  
**Test result certificate metadata**

Data element label	Description	Data type	Preferred code system	Requirement status for proof of negative SARS-CoV-2 test result	Requirement status for proof of previous SARS-CoV-2 infection
<b>Certificate issuer</b>	The authority or authorized organization that issued the test result certificate	String	Not applicable	Required	Required
<b>Health certificate identifier (HCID)</b>	Unique ID for a physical and/or digital health folder that contains one or more test events and associated certificates of a Tested Person	ID	Not applicable	Required	Required
<b>Certificate schema version</b>	Version of the core data set and HL7 FHIR implementation guide that the certificate is using	String	Not applicable	Required	Required
<b>Certificate valid from</b>	Date and time at which the test result certificate became valid; no health or clinical inferences should be made from this data	dateTime <sup>a</sup>	Compatible with HL7 FHIR dateTime with time zone specified	Optional	Optional

FHIR: Fast Healthcare Interoperability Resources; HL7: Health Level Seven; ID: identifier.

<sup>a</sup> HL7 FHIR dateTime format is available at <https://www.hl7.org/fhir/datatypes.html#dateTime>.

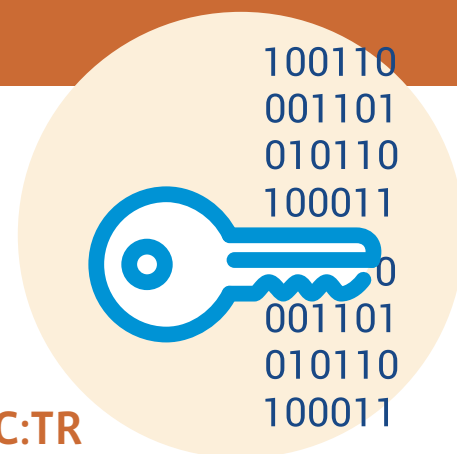
It should be noted that a Member State may choose to add its own data fields to this model. The Member State may additionally choose to have one core data set for both proof scenarios or have two separate data sets. The proposed specification is intended to provide a basis for generating interoperable certificates.

## SECTION

# 6

## Public key infrastructure

for signing and verifying a DDCC:TR

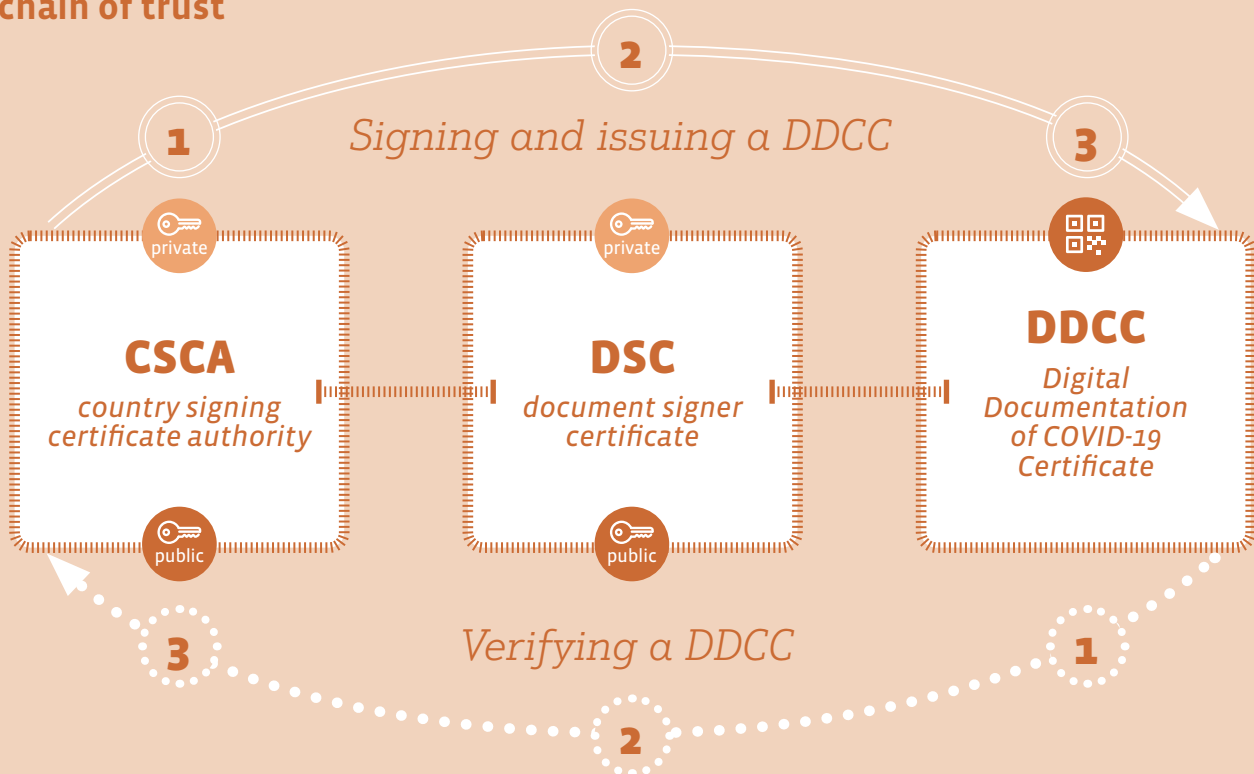


*The proof scenarios presented in earlier chapters, and the data associated with them, suggest the need for a digital ecosystem within a country to issue, update and verify DDCC:TRs. This ecosystem would comprise a suite of digital tools to manage DDCC:TR data and the processes and governance rules for using these digital tools. A digital ecosystem could be as simple as a server for storing and managing data or as extensive as an entire health information exchange infrastructure.*

In [Annex 5](#), 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:TR 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 to suit the specific needs of each Member State.

To sign a digital document, public key infrastructure (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; Fig. 12). There are many different mechanisms/technologies to implement this approach. PKI is described in further detail in [Annex 3](#).

Figure 12

**The chain of trust**

Member States will need to establish or utilize a PKI that can be leveraged to issue and verify a DDCC:TR. An existing PKI framework may be used, provided it meets the requirements outlined in this document.

The PKI can be maintained and managed by another government entity (e.g. ministry of information and communications technology, ministry of interior, ministry of foreign affairs) or by a contractor that the Public Health Authority (PHA) has selected. Regardless, the PHA will have 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:TR.
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 [Chapter 7](#).

There are many ways in which a PKI can be implemented. An example implementation of digital signing is provided in the WHO DDCC HL7 FHIR implementation guide (available at <https://worldhealthorganization.github.io/ddcc>)(17). The precise algorithms used for the implementation (e.g. algorithms used for hashing and for signature generation) are at the discretion of the Member State.

This document assumes that a PKI has already been deployed or is available within a country to support the DDCC:TR workflows described in [Chapter 3](#) and [Chapter 4](#).

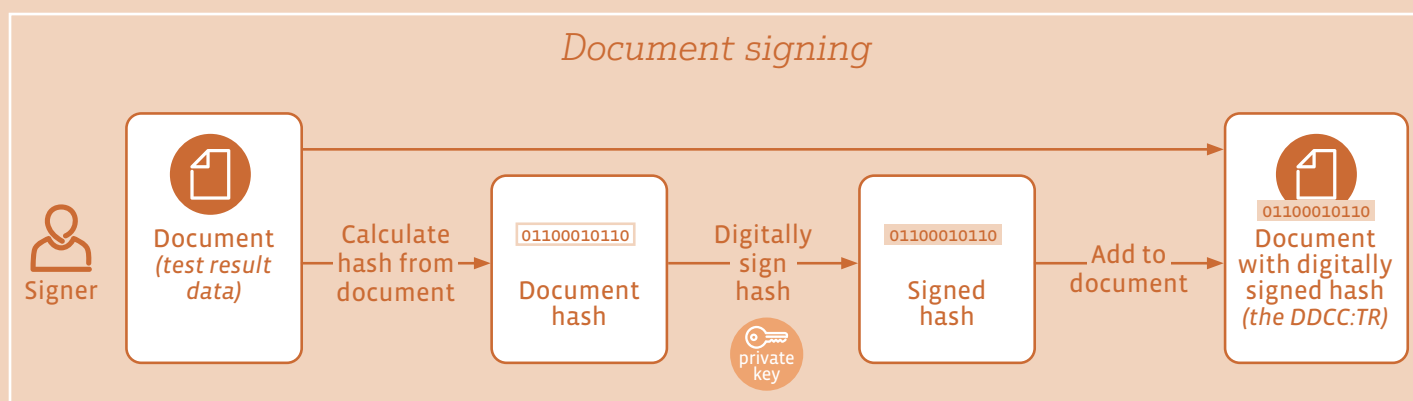
## 6.1 Signing a DDCC:TR

The process of signing a DDCC:TR is shown in the top row of Fig. 12 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 password-protected, etc.); the public key is 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:TR is digitally signed using the DSC’s private key. A two-dimensional (2D)-barcode representation (e.g. QR code) of the signed content can be generated, if required. The process of signing (Fig. 13) is as follows.
  - a. A human-readable plain text description of the test result 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:TR in a non-human-readable and cryptographically secure format.

Figure 13

### How digital signatures work





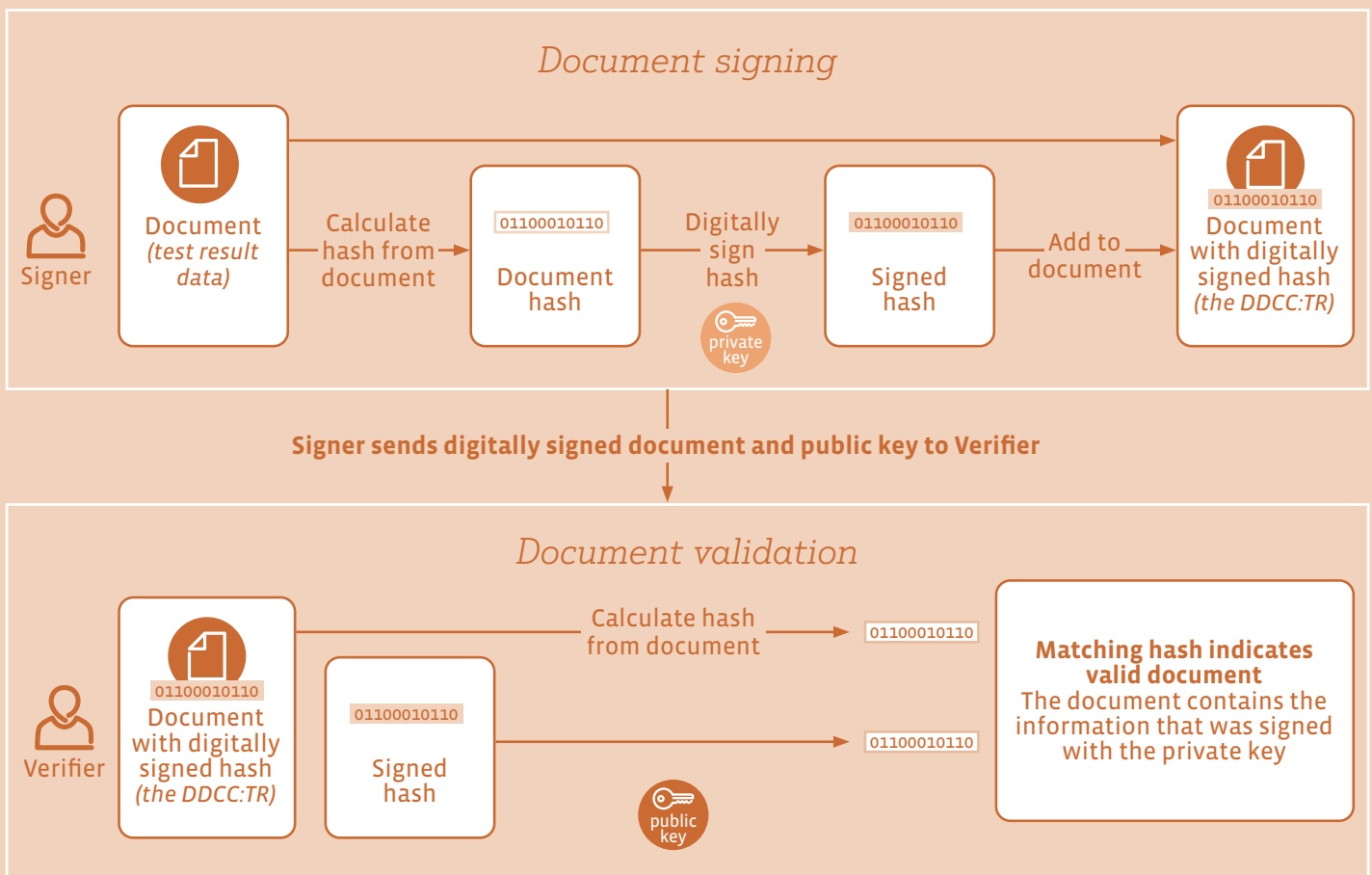
## 6.2 Verifying a DDCC:TR signature

The verification process, shown in the bottom row of Fig. 12 and in more detail in Fig. 14, reverses the signing process to verify content in the signed DDCC:TR:

1. A Verifier calculates its own hash (i.e. "calculated hash") from the information in the DDCC:TR, using the same hashing algorithm as was used by the document signer.
2. The DDCC:TR's signed hash is read by a digital solution as follows.
  - a. The document signer's public key is used to cryptographically transform the signed hash back into the document hash. The Verifier can compare the document hash with its calculated hash from step 1. If the document hash and calculated hash match, the Verifier can trust the digital signature and that the data that were signed are the same as the data read from the DDCC:TR.
3. 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 14

### How digital signature verification works



## 6.3 Trusting a DDCC:TR 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 difficult to reverse.

Operationally, private keys are kept highly secure and public keys are broadly shared. Private–public key pairs provide a high level of security provided the private key is not compromised and remains available only to the entity performing the signing. 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 decrypted with a public key can have been signed only by someone with access to the DSC’s private key, because the public key was able to decrypt the document hash; and
2. the holder of the private key cannot deny having 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.

# 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” (16). A national framework to govern the complex and dynamic health policy for implementing a DDCC:TR solution 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:TR solutions. However, it will be the responsibility of the Member State and/or relevant governing bodies to determine the most appropriate governance mechanisms for the context.*

Fundamentally, trust in the system should derive from the security-by-design of a public key infrastructure (PKI) and the governance rules put in place by the Member State to operate it. For verification of test result certificates, governance is required to be established at two levels: (a) the Public Health Authority (PHA), and (b) the Member State. At PHA level, at least one document signer certificate (DSC) needs to be utilized to sign the DDCC:TR. At Member State level, an authorized DSC-sharing mechanism needs to be established to indicate which DSCs are currently permitted to sign the DDCC:TR. The two recommended approaches are as follow.

1. **ROOT CERTIFICATE AUTHORITY:** The Member State establishes a root certificate authority, which holds a root certificate for the DDCC:TR. 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. However, it is used to denote that a root certificate authority may be trusted directly (39).

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 DDCC:TRs.

Member States can leverage an existing PKI or create a new one specifically for a DDCC:TR solution. 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 A DDCC:TR:** There should be clear and transparent processes in place for issuing a DDCC:TR, to establish trust in the system. Transparently acknowledging which entities are eligible to issue a DDCC:TR reduces the potential for fraudulent issuance of a DDCC:TR and provides accountable entities when possible fraud has occurred. Member States need to define the accreditation processes and provide parameters for identification of reliable tests and testing centres. It will be up to the PHA to determine which laboratories and testing centres are authorized to participate in generating and issuing a DDCC:TR (27,40).
- **VERIFYING A DDCC:TR:** Member States need to define the requirements for what constitutes a "verified" DDCC:TR. Furthermore, Member States will need to decide whether the DDCC:TR can be verified by anonymous Verifiers; alternatively, they may decide on a list of trusted Verifiers, in which case only trusted Verifiers would be able to verify and validate a DDCC:TR. The appropriate privacy mechanisms should be built into the implementation, based on this decision.
- **VALIDATING A DDCC:TR:** Member States need to define the requirements for what constitutes a "valid" DDCC:TR. Additionally, Member States need to establish and clearly communicate business rules driving the acceptance criteria of a DDCC:TR, based on their local policies and agreements made with other Member States.
- **REVOCAION OF DDCC:TR:** There should be clear and transparent processes for revocation of a DDCC:TR. Revocation may be required in case fraud has occurred, incorrect information needs to be rectified, issues have been discovered at a laboratory and test results need to be recalled, or for any other identified reason. There are two sequential steps for revocation:
  1. Revoke a PKI DSC, which can be checked against the certificate revocation list from a Public Key Directory (PKD).
  2. Revoke a DDCC:TR, which can be checked against the DDCC Registry Service.

Further details of the revocation processes are provided in the WHO DDCC HL7 FHIR implementation guide (available at <https://worldhealthorganization.github.io/ddcc>) (17).

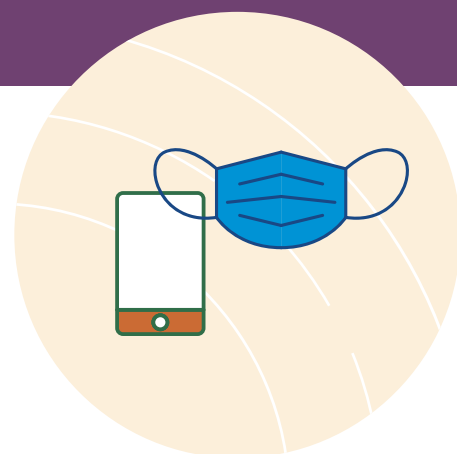
Revocation processes should also include standard operating procedures for the following.

- » **INFORMING INDIVIDUALS:** Individuals will need to be informed if their DDCC:TR 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 a DDCC:TR has been revoked in order to be able to continuously trust that every DDCC:TR issued by a specific entity is still valid. For example, if there are reports of counterfeit DDCC:TRs, Verifiers should be informed about the possibility of encountering a counterfeit DDCC:TR. This allows for continued trust in the system.

- » **REMEDY PROVISION:** If a DDCC:TR is revoked, Member States should apply measures to rectify the situation, for example by providing the option for a new diagnostic test to be conducted, if advisable. Alternatively, there might be processes to obtain a new, verifiable, DDCC:TR.
- **DATA MANAGEMENT AND PRIVACY PROTECTION:** Member States are responsible for data timeliness and completeness, and for the accuracy of every DDCC:TR issued under the authority of their PHAs. Personal data about individuals with a DDCC:TR from another country need to be processed according to a set of principles and processes agreed upon by Member States, to establish trust between Member States.

# Implementation considerations

for a DDCC:TR solution



*Since COVID-19 was declared a Public Health Emergency of International Concern under the International Health Regulations (2005) (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 was also immediate acknowledgement that digital health solutions can effectively and immediately be leveraged to support the public health response to the pandemic. Some key implementation considerations need to be taken into account before deploying a digital health solution.*

## 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 (41) and the guidance provided in the Digital implementation investment guide (DIIG) (42), the following considerations and key questions should be examined prior to deployment of a DDCC:TR solution.

### STRATEGY AND INVESTMENT

- What are the potential benefits, risks and costs of implementing a DDCC:TR solution? These should be assessed before introducing a DDCC:TR system and its associated infrastructure. An impact assessment should include ethical and privacy implications and potential risks that may arise with the implementation of a DDCC:TR solution.
- What is the potential impact on individuals, families, businesses, health workers and other relevant stakeholders?
- What is the potential impact on public health and on the economy?
- What is the value added beyond using existing unverifiable systems?

## 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 handwritten rapid test results are to be used, is there the ability for high-volume pre-printing of barcoded health certificate identifiers (HCIDs) on paper test result forms?
- Is high-volume printing capacity for paper certificates 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 major urban areas? Among those with mobile phones, is there broad adoption of smartphones?
- Is a public key infrastructure (PKI) in place that can be leveraged to support digital signing of DDCC:TRs?
- Where sample collection is done at a site different from the specimen-evaluation site, challenges relating to specimen transportation will need to be addressed.

## LEGISLATION, POLICY AND COMPLIANCE

- Are policies for appropriate use and data protection in place to address the ethical considerations and data protection principles of a DDCC:TR solution?
- How will it be assured that individuals are not treated differently or given different levels of trust because of the format of the DDCC:TR they are using (e.g. smartphone application or paper test result certificate)?
- 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, notification of data breach) 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 a DDCC:TR solution.
- Is there a clear governance mechanism and are standard operating procedures in place to support the use and maintenance of the DDCC:TR solution?
- What agency will be responsible for independent oversight for use of the DDCC:TR solution, and what level of authority will it be given? How will the impact of DDCC:TR 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 agreements need to be established bilaterally, multilaterally or at a regional level to establish trusted recognition between DDCC:TRs of different provenance? Are bilateral or regional agreements in place that can be leveraged?

## WORKFORCE

- Is the value added by the verifiable digital representation clearly communicated to personnel, who may face the additional burden of operating new digital solutions?
- Are change management processes and support in place when implementing a DDCC:TR solution?
- Is there a ready domestic supply of digitally competent health workers? If not, what level of effort and resources would be needed to conduct training and other capacity-building measures?
- Are there health informatics programmes at national level or in the private sector, provided through institutions such as universities and learning platforms that can support health workers who are taking up new digital health solutions?
- Given the frequently changing context of the COVID-19 pandemic, how will continuous training and updating of health workers, health facility managers, and public health officials take place to ensure continued relevance of the DDCC:TR solution?

## SERVICES AND APPLICATIONS

- Do point-of-service applications exist that are used for other workflows not related to test results, but which could be leveraged to collect the DDCC:TR core data set and associate these data with an HCID? Examples may include existing health management information system (HMIS) solutions that can be readily extended to support new workflows.
- Are there products in the marketplace that 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 in-house capacity, a responsive established user community, or a software services provider that will provide support and help add features?
- Which services and applications would be the most environmentally sustainable?

## STANDARDS AND INTEROPERABILITY

- Is there an existing interoperability framework to guide how a DDCC:TR solution 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:TR 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 Open Health Information Exchange [OpenHIE] framework is given in [Annex 5](#).)

## 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, new health content requirements may emerge and business rules and/or validity periods for the acceptance of a test result certificate may need to be revised. Implementation of the DDCC:TR solution should change in accordance with the changing health context and remain evidence based.



- If the sample-evaluation site (e.g. laboratory) is generating the DDCC:TR, core data set elements captured at the time of the sample collection will need to be conveyed to the sample-evaluation site along with the specimen, using either an electronic or paper-based means.

## 8.2 Key factors to consider with solution developers

If a Public Health Authority (PHA) that is responsible for the delivery of a digital solution does not have appropriate technology skills in house, it may want one or more partners to provide that service.

A digital partner will ideally be chosen through a competitive process: multiple 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. When deciding the approach to inviting tenders for the work, assessing tenders, awarding a contract and then working with a partner, the following high-level key factors should be considered.

- The terms of reference for the work to be performed should be clearly expressed and in 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 for on a pro-rata basis).
- The timeline set for work should be realistic. 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 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 to use a single supplier (with subcontractors) or a consortium of suppliers. 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 vendors.
- The metrics for success of the work should be defined early so that the goals and intended outcomes of the project are clear to all involved. Ideally, these metrics should be measurable key performance indicators (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.

- 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 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

Specific cost categories and related cost drivers will affect the budget of the DDCC:TR work. However, how they will be incurred will depend on the Member State's implementation strategy. Table 14 provides a non-exhaustive list of possible cost drivers for implementing a DDCC:TR solution.

**Table 14**  
**Illustrative costs for a DDCC:TR solution**

Cost category	Key cost drivers and considerations
 Ongoing/all phases	
<b>Governance</b>	<ul style="list-style-type: none"> <li>→ Coordination of personnel to develop and maintain relevant partnerships</li> <li>→ Conducting an impact assessment and developing new policies, processes and standard operating procedures for ongoing monitoring of use and impact</li> <li>→ Independent oversight and monitoring</li> </ul>
<b>Management and staffing</b>	<ul style="list-style-type: none"> <li>→ Personnel to oversee the overall programme until the planned end (if there is one), including project management and vendor management, if applicable</li> <li>→ System set-up and end-user support</li> <li>→ Monitoring feedback and taking corrective action</li> <li>→ Handling complaints and exercising data subject rights, including legal redress</li> </ul>
 Development and setup	
<b>Technology adaptation</b>	<ul style="list-style-type: none"> <li>→ Building completely new COVID-19 systems or leveraging existing software systems (e.g. adapting an LIS)</li> <li>→ Subscriptions, licensing fees and implementation costs associated with the software model</li> <li>→ Custom configurations or any enhancements, if needed, or any custom-developed software</li> <li>→ Translations and localizations, if needed</li> </ul>

Cost category	Key cost drivers and considerations
 <b>Deployment</b>	
<b>Equipment and hardware</b>	<ul style="list-style-type: none"> <li>→ Data storage (e.g. costs for storage in the cloud or on local servers or individual devices)</li> <li>→ Devices (e.g. printers and scanners) needed at the certificate issuance site</li> </ul>
<b>Testing</b>	<ul style="list-style-type: none"> <li>→ 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</li> </ul>
<b>Training</b>	<ul style="list-style-type: none"> <li>→ Training technicians, health facility managers and data entry personnel, which may involve travel or other logistical costs</li> <li>→ Training materials for verifiers of DDCC:TRs</li> </ul>
<b>Roll-out</b>	<ul style="list-style-type: none"> <li>→ Transport of any necessary hardware, software or materials (including printed paper test results) to the certificate generation or certificate issuance sites</li> <li>→ Increased technical support required during the roll-out phase</li> </ul>
<b>Outreach and raising awareness</b>	<ul style="list-style-type: none"> <li>→ Communications on when, where and how people can obtain a DDCC:TR</li> <li>→ Communication of what a DDCC:TR can and cannot be used for</li> <li>→ Battling DDCC:TR-related “infodemics” (too much information, misinformation and disinformation)</li> <li>→ Meeting accessibility requirements of individuals and reaching groups with disadvantages, such as individuals with digital skill barriers or disability barriers</li> </ul>
 <b>Integration and interoperability</b>	
<b>Establishing trust frameworks</b>	<ul style="list-style-type: none"> <li>→ Adapting content, depending on acceptance agreements between Member States</li> <li>→ Coordination for establishing agreements between Member States</li> </ul>
<b>Interoperability with other systems</b>	<ul style="list-style-type: none"> <li>→ Undertaking mapping exercises and adopting standards agreed upon through the establishment of trust frameworks</li> <li>→ Any licensing fees associated with the use of standards (note that the standards proposed by WHO in this guidance document have no licensing fees)</li> </ul>
 <b>Scaling up</b>	
<b>Printing</b>	<ul style="list-style-type: none"> <li>→ With the paper test result certificate: the cost of printing, which will increase as more people are tested and, subsequently, more people receive a paper test result certificate</li> </ul>
<b>Human resources</b>	<ul style="list-style-type: none"> <li>→ As more people are tested: additional personnel to support use of the systems, including training, management, etc.</li> </ul>
<b>IT licensing</b>	<ul style="list-style-type: none"> <li>→ 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 volume of data increases, or as additional IT infrastructure is needed</li> </ul>
<b>IT scalability</b>	<ul style="list-style-type: none"> <li>→ 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</li> </ul>
 <b>Sustained operations</b>	
<b>Refresher training</b>	<ul style="list-style-type: none"> <li>→ Consistent training of new staff when staff leave, and refresher training for existing staff – with content updates made as the context changes</li> </ul>
<b>Adaptive management</b>	<ul style="list-style-type: none"> <li>→ Monitoring and evaluation of DDCC:TR implementation practices and processes, with application of lessons learned</li> </ul>
<b>Communication</b>	<ul style="list-style-type: none"> <li>→ Continued messaging, with consideration of accessibility needs</li> <li>→ Continued helpdesk or customer service technology support for users of the DDCC:TR</li> </ul>
<b>Technology maintenance</b>	<ul style="list-style-type: none"> <li>→ Fixing bugs, adding features, maintaining customizations, releasing updates, and hardware maintenance and replacement</li> </ul>

LIS: laboratory information system

## 8.4 Additional resources to support implementation

Additional resources that can support a DDCC:TR implementation include examples of implementations already deployed, additional technical specifications for specific use cases, and general guidance on implementing digital health solutions. The following is a non-exhaustive list of examples.

### WHO INTEROPERABILITY STANDARD FOR DDCC:TR

- WHO Digital Documentation of COVID-19 Certificates (DDCC) HL7 FHIR implementation guide (<https://worldhealthorganization.github.io/ddcc>) (17);
- DDCC:TR Core Data Dictionary (<https://apps.who.int/iris/bitstream/handle/10665/352585/WHO-2019-nCoV-Digital-certificates-diagnostic-test-results-data-dictionary-2022.1-eng.xlsx>) (43).

### EXAMPLE SPECIFICATIONS TO GUIDE IMPLEMENTATION

- EU Digital COVID Certificate ([https://ec.europa.eu/info/live-work-travel-eu/coronavirus-response/safe-covid-19-vaccines-europeans/eu-digital-covid-certificate\\_en](https://ec.europa.eu/info/live-work-travel-eu/coronavirus-response/safe-covid-19-vaccines-europeans/eu-digital-covid-certificate_en)) (29);
- International Civil Aviation Organization (ICAO): guidelines on visible digital seals (“VDS-NC”) for travel-related public health proofs (<https://www.icao.int/Security/FAL/TRIP/PublishingImages/Pages/Publications/Guidelines%20-%20VDS%20for%20Travel-Related%20Public%20Health%20Proofs.pdf>) (28).

### GENERAL IMPLEMENTATION WHO GUIDANCE FOR DIGITAL HEALTH SOLUTIONS

- Digital implementation investment guide (DIIG): integrating digital interventions into health programmes (<https://www.who.int/publications/i/item/9789240010567>) (42) – 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:TR solution.

### HEALTH SYSTEM ASSESSMENT TOOLS DEVELOPED BY WHO REGIONAL OFFICES THAT CAN BE USED BY MEMBER STATES IMPLEMENTING DIGITAL HEALTH SOLUTIONS

- Pan American Health Organization (PAHO): Information Systems for Health (IS4H) Toolkit (<https://www3.paho.org/ish/index.php/en/toolkit>) (44) – describes the method, tool and questions for assessing organizational capacity related to governance, data management, digital transformation, innovation and knowledge management;
- Pathways to health system performance assessment ([https://www.euro.who.int/data/assets/pdf\\_file/0005/169412/e96512-Eng.pdf](https://www.euro.who.int/data/assets/pdf_file/0005/169412/e96512-Eng.pdf)) (45) – a manual to conducting health system performance assessment at national or subnational level.

## References

1. Makhafola G. Joburg healthcare worker nabbed for allegedly selling fake Covid-19 test certificates. News24. 22 August 2021 (<https://www.news24.com/news24/southafrica/news/joburg-healthcare-worker-nabbed-for-allegedly-selling-fake-covid-19-test-certificates-20210822>, accessed 11 February 2022).
2. Margit M. Thousands of Israelis join Telegram groups selling fake COVID papers. The Media Line. 15 August 2021 (<https://themedialine.org/by-region/thousands-of-israelis-join-telegram-groups-selling-fake-covid-papers>, accessed 11 February 2022).
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. The Guardian. 16 May 2021 (<https://www.theguardian.com/world/2021/may/16/fake-covid-vaccine-and-test-certificate-market-is-growing-researchers-say>, accessed 11 February 2022).
5. Digital documentation of COVID-19 certificates: vaccination status – technical specifications and implementation guidance. Geneva: World Health Organization; 2021 (<https://www.who.int/publications/i/item/WHO-2019-nCoV-Digital-certificates-vaccination-2021.1>, accessed 11 February 2022).
6. Technical considerations for implementing a risk-based approach to international travel in the context of COVID-19: interim guidance. Geneva: World Health Organization; 2021 (<https://apps.who.int/iris/handle/10665/342212>, accessed 11 February 2022).
7. Criteria for releasing COVID-19 patients from isolation. Geneva: World Health Organization; 2020 (<https://www.who.int/news-room/commentaries/detail/criteria-for-releasing-covid-19-patients-from-isolation>, accessed 11 February 2022).
8. Living guidance for clinical management of COVID-19. Geneva: World Health Organization; 2021 (<https://www.who.int/publications/i/item/WHO-2019-nCoV-clinical-2021-2>, accessed 11 February 2022).
9. Diagnostic testing for SARS-CoV-2. Geneva: World Health Organization; 2020 (<https://www.who.int/publications/i/item/diagnostic-testing-for-sars-cov-2>, accessed 11 February 2022).
10. COVID-19 diagnostic testing in the context of international travel: scientific brief. Geneva: World Health Organization; 2020 (<https://apps.who.int/iris/handle/10665/337832>, accessed 11 February 2022).
11. SARS-CoV-2 antigen-detecting rapid diagnostic tests: an implementation guide. Geneva: World Health Organization; 2020 (<https://www.who.int/publications/i/item/9789240017740>, accessed 11 February 2022).
12. Recommendations for national SARS-CoV-2 testing strategies and diagnostic capacities: interim guidance. Geneva: World Health Organization; 2021 (<https://www.who.int/publications/i/item/WHO-2019-nCoV-lab-testing-2021.1-eng>, accessed 11 February 2022).
13. Antigen-detection in the diagnosis of SARS-CoV-2 infection. Geneva: World Health Organization; 2021 (<https://www.who.int/publications/i/item/antigen-detection-in-the-diagnosis-of-sars-cov-2infection-using-rapid-immunoassays>, accessed 11 February 2022).
14. Laboratory biosafety guidance related to coronavirus disease (COVID-19): interim guidance. Geneva: World Health Organization; 2021 (<https://www.who.int/publications/i/item/WHO-WPE-GIH-2021.1>, accessed 11 February 2022).
15. Advice on the use of point-of-care immunodiagnostic tests for COVID-19: scientific brief. Geneva: World Health Organization; 2020 (<https://www.who.int/news-room/commentaries/detail/advice-on-the-use-of-point-of-care-immunodiagnostic-tests-for-covid-19>, accessed 11 February 2022).
16. 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>, accessed 11 February 2022).
17. WHO digital documentation of COVID-19 certificates (DDCC) implementation guide. Geneva: World Health Organization; no date (<https://worldhealthorganization.github.io/ddcc>, accessed 11 February 2022).
18. Policy considerations for implementing a risk-based approach to international travel in the context of COVID-19. Geneva: World Health Organization; 2021 (<https://apps.who.int/iris/handle/10665/342235>, accessed 11 February 2022).
19. Considerations for implementing and adjusting public health and social measures in the context of COVID-19: interim guidance. Geneva: World Health Organization; 2021 (<https://apps.who.int/iris/handle/10665/341811>, accessed 11 February 2022).

20. Statement on the tenth meeting of the International Health Regulations (2005) Emergency Committee regarding the coronavirus disease (COVID-19) pandemic. In: World Health Organization/News [website]. Geneva: World Health Organization; 19 January 2022 ([https://www.who.int/news/item/19-01-2022-statement-on-the-tenth-meeting-of-the-international-health-regulations-\(2005\)-emergency-committee-regarding-the-coronavirus-disease-\(covid-19\)-pandemic](https://www.who.int/news/item/19-01-2022-statement-on-the-tenth-meeting-of-the-international-health-regulations-(2005)-emergency-committee-regarding-the-coronavirus-disease-(covid-19)-pandemic), accessed 11 February 2022).
21. Statement on the ninth meeting of the International Health Regulations (2005) Emergency Committee regarding the coronavirus disease (COVID-19) pandemic. In: World Health Organization/News [website]. Geneva: World Health Organization; 26 October 2021 ([https://www.who.int/news/item/26-10-2021-statement-on-the-ninth-meeting-of-the-international-health-regulations-\(2005\)-emergency-committee-regarding-the-coronavirus-disease-\(covid-19\)-pandemic](https://www.who.int/news/item/26-10-2021-statement-on-the-ninth-meeting-of-the-international-health-regulations-(2005)-emergency-committee-regarding-the-coronavirus-disease-(covid-19)-pandemic), accessed 11 February 2022).
22. 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]. Geneva: World Health Organization; 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 11 February 2022).
23. 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 11 February 2022).
24. 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 11 February 2022).
25. Key planning recommendations for mass gatherings in the context of COVID-19: interim guidance. Geneva: World Health Organization; 2021 (<https://www.who.int/publications/i/item/10665-332235>, accessed 11 February 2022).
26. COVID-19 natural immunity: scientific brief. Geneva: World Health Organization; 2021 ([https://www.who.int/publications/i/item/WHO-2019-nCoV-Sci\\_Brief-Natural\\_immunity-2021.1](https://www.who.int/publications/i/item/WHO-2019-nCoV-Sci_Brief-Natural_immunity-2021.1), accessed 11 February 2022).
27. Assessment tool for laboratories implementing SARS-CoV-2 testing: interim guidance: User Guide. Geneva: World Health Organization; 2020 (<https://www.who.int/publications/i/item/assessment-tool-for-laboratories-implementing-covid-19-virus-testing>, accessed 11 February 2022).
28. 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 11 February 2022).
29. 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](https://ec.europa.eu/info/live-work-travel-eu/coronavirus-response/safe-covid-19-vaccines-europeans/eu-digital-covid-certificate_en), accessed 11 February 2022).
30. Introduction to DIVOC: Digital Infrastructure for Vaccination Open Credentialing. In: DIVOC [website]. India: eGov Foundation; no date (<https://divoc.egov.org.in>, accessed 11 February 2022).
31. SMART Health Cards. In: SMART [website]. Boston, MA: SMART Health IT and Boston Children’s Hospital; no date (<https://smarthealth.cards/en>, accessed 11 February 2022).
32. 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).
33. 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 11 February 2022).
34. COVID-19 status certificates: human rights considerations. Edinburgh: Scottish Human Rights Commission; 2021 ([https://www.scottishhumanrights.com/media/2176/21\\_04\\_28\\_covid-certificates-and-human-rights-vfinal.pdf](https://www.scottishhumanrights.com/media/2176/21_04_28_covid-certificates-and-human-rights-vfinal.pdf), accessed 11 February 2022).
35. WHO 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 11 February 2022).
36. International patient summary implementation guide [website]. Ann Arbor, MI: Health Level Seven International – Patient Care Work Group; no date (<https://build.fhir.org/ig/HL7/fhir-ips>, accessed 11 February 2022).
37. Global Patient Set. In: SNOMED International [website]. London: SNOMED International; 2021 (<https://www.snomed.org/snomed-international/learn-more/global-patient-set>, accessed 11 February 2022).

38. International Classification of Health Interventions (ICHI). In: World Health Organization/Classifications [website]. Geneva: World Health Organization; 2021 (<https://www.who.int/standards/classifications/international-classification-of-health-interventions>, accessed 11 February 2022).
39. 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 11 February 2022).
40. Laboratory assessment tool for laboratories implementing SARS-CoV-2 testing. Geneva: World Health Organization; 2020 (<https://www.who.int/publications/i/item/laboratory-assessment-tool-for-laboratories-implementing-covid-19-virus-testing>, accessed 11 February 2022).
41. National eHealth Strategy Toolkit: overview. Geneva: World Health Organization and International Telecommunication Union; 2012 (<https://www.who.int/ehealth/publications/overview.pdf>, accessed 11 February 2022).
42. Digital implementation investment guide (DIIG): integrating digital interventions into health programmes. Geneva: World Health Organization; 2020 (<https://www.who.int/publications/i/item/9789240010567>, accessed 11 February 2022).
43. Digital Documentation of COVID-19 Certificates: Test Result – Web annex: DDCC:TR core data dictionary (<https://apps.who.int/iris/bitstream/handle/10665/352585/WHO-2019-nCoV-Digital-certificates-diagnostic-test-results-data-dictionary-2022.1-eng.xlsx>).
44. Information Systems for Health (IS4H) Toolkit [website]. At: Pan American Health Organization (PAHO). Washington, DC: PAHO; no date (<https://www3.paho.org/ish/index.php/en/toolkit>, accessed 11 February 2022)
45. OpenHIE [website]. OpenHIE; no date (<https://ohie.org/about>, accessed 11 February 2022).

# Annexes




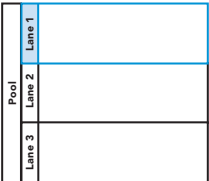








## Annex 1

# Business process symbols used in workflows

Table A1.1 provides an overview of the standardized notation for business process mapping that is used to depict the certificate generation and certificate verification and validation workflows.

**Table A1.1**  
**Business process symbols used in workflows**

Symbol	Symbol name	Description
	Pool	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	A designated area for noting the activities performed by or expected of each specific actor. Each persona is assigned to a swim lane.
	Start event, or trigger event	The beginning of the process.
	End event	The end of the process.
	Activity, process, step or task	One of the successive actions performed by the actor for that swim lane.
	Sequence flow	The flow direction from one process to the next.
	Message flow	The flow of information from one process to another.
	Gateway	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 2

# Guiding principles for mapping the WHO Family of International Classifications and other classifications

Mapping from classifications and terminologies used in existing systems to the International Classification of Diseases 11th revision (ICD-11), and other classifications in the WHO Family of International Classifications (WHO-FIC) should follow the principles listed below.<sup>2</sup>

1. Use case(s) should be established before 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. The purpose, scope and directionality of the map should be clearly defined.
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 maps.

Factors that may be involved in QA include QA 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.

<sup>2</sup> 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 <https://www.who.int/standards/classifications>.

Usage validation of maps is an independent process involving users of the maps (not developers of the maps) 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). Key principles for usage validation of maps include the following.

- 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. Dissemination: 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 and limitations of the maps, and the methodology used to create the maps.
9. Maintenance: establish an ongoing maintenance mechanism, and the 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 the foundation component first, then generate maps to mortality and morbidity statistics through linearization aggregation.

## Annex 3

# Additional details about public key infrastructure

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 public key infrastructure (PKI) – essentially all the components that need to be in place for a trusted solution to work.

PKI is a system needed to distribute public keys and to reassure recipients that each public key has come from an accredited source (i.e. the certificate authority). This is one purpose 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.

### WHY A PKI IS NEEDED IN A DDCC:TR SOLUTION

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

For paper-based records, verification was 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 for achieving verification 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.

### HOW PKI IS 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 my friend's 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 my same friend and give that friend confidence that it could only have come from me, I can encrypt the message 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:TR data. It can be guaranteed that data have 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 (Fig. A3.1). There are various software tools for generating public-private key pairs (Fig. A3.2).

Figure A3.1  
An example key

```
---- BEGIN SSH2 PUBLIC KEY ----
Comment: "rsa-key-20210528"
AAAAB3NzaC1yc2EAAAABJQAAAQEArK462nWt2/JsHvHgyciu2HzVo83IHYEKeLTL
g+7ewhCK26XRRe8f/WsG7qnIWShBvbcKDTARcM8jQS4qSG1KUCChogs6ZLRUT1mYF
JSB6BVBgGU/dDnsalKMMN4HRoutluzMTXnDypHrzDjXG3nqFrzfRoAtARf5aYNA1
ssZmh2jI3BF9M29jglv411WbMQzmmEBNrMYwmm3wCIZ826N/oLeeFuyp8q6TBMN
msRlOalpGsTeYl2GKU/oRtxzYcP2glYovLE/uGoySleYlI3ME6DSJbmUHtxqKsCm
13ggQvEwreysLX6oLouaUyYfHTTfF2kzCH8MWiB1iQP2z4izQw==
---- END SSH2 PUBLIC KEY ----
```

Figure A3.2  
An example of a key generation tool

The screenshot shows the PuTTY Key Generator application window. The title bar reads "PuTTY Key Generator". The menu bar includes "File", "Key", "Conversions", and "Help".

The "Key" section contains a text area for the public key, which is highlighted with a blue selection. The text in the area is: `ssh-rsa AAAAB3NzaC1yc2EAAAABJQAAAQEArK462nWt2/JsHvHgyciu2HzVo83IHYEKeLTLg+7ewhCK26XRRe8f/WsG7qnIWShBvbcKDTARcM8jQS4qSG1KUCChogs6ZLRUT1mYFJSB6BVBgGU/dDnsalKMMN4HRoutluzMTXnDypHrzDjXG3nqFrzfRoAtARf5aYNA1ssZmh2jI3BF9M29jglv411WbMQzmmEBNrMYwmm3wCIZ826N/oLeeFuyp8q6TBMNmsRlOalpGsTeYl2GKU/oRtxzYcP2glYovLE/uGoySleYlI3ME6DSJbmUHtxqKsCm13ggQvEwreysLX6oLouaUyYfHTTfF2kzCH8MWiB1iQP2z4izQw==`. Below this text area are input fields for "Key fingerprint" (displaying `ssh-rsa 2048 f6:39:2e:e6:2b:75:61:a6:10:07:4c:fa:cd:cd:af:19`), "Key comment" (displaying `rsa-key-20210701`), "Key passphrase", and "Confirm passphrase".

The "Actions" section contains three buttons: "Generate", "Load", and "Save public key" (with "Save private key" also visible).

The "Parameters" section includes radio buttons for "Type of key to generate":  RSA,  DSA,  ECDSA,  Ed25519, and  SSH-1 (RSA). Below this is a text field for "Number of bits in a generated key" with the value `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 A PKI WORKS FOR TEST RESULT CERTIFICATES

For the purposes of the DDCC:TR, 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. 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 does not sign test result documents and data. The signing of test result documents and data is handled by other agencies, such as public health actors and other stakeholders.
- C. 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. The different agencies then use the private key in their DSC to digitally sign documents. Signing involves encrypting the information using the private key so that it is rendered into a format that is not human-readable.

Any electronic information can be signed in this way: the health certificate identifier (HCID) could be signed; a representation of the whole test result record could be signed; or some other combination of information, as determined by the certificate authority, could be signed.

- E. An interested party (i.e. a Verifier) who wants to decrypt the encrypted information for the test result certificate must have both:
  - » 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.

A certificate authority usually sets up an online service for this purpose. The Verifier can interrogate the service:

- » The Verifier can 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 Registry Service.
  - » 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.
- F. 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 test result 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 by any other party after it was signed, otherwise the decryption would not work; and

- » the information can be trusted, because the Verifier both: trusts the certificate authority; and trusts the certificate authority to have issued the DSC, which must have been used to encrypt the information.

PKI is only as secure as the IT infrastructure within 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 4

# Non-functional requirements

This section contains a suggested set of generic non-functional requirements. Along with the functional requirements in [section 3.3](#) and [section 4.3](#), these non-functional requirements provide a set of requirements that can be adapted when specifying a digital solution for the proof 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 to that for 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.
- **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 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 up 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.

Non-functional requirements for the DDCC:TR are listed in Table A4.1.

**Table A4.1**  
**Non-functional requirements for the DDCC:TR<sup>a</sup>**

Requirement ID	Category	Non-functional requirement
DDCCTR.NFXNREQ.001	Accessibility	Any solution <b>SHALL</b> 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.
DDCCTR.NFXNREQ.002	Accessibility	Any solution <b>SHOULD</b> 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.
DDCCTR.NFXNREQ.003	Accessibility	Any solution <b>SHALL</b> provide a mechanism for the resynchronization/dispatch of data created offline when the solution is reconnected.
DDCCTR.NFXNREQ.004	Accessibility	Any solution <b>SHOULD</b> 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.)
DDCCTR.NFXNREQ.005	Accessibility	Any solution <b>SHOULD</b> 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).
DDCCTR.NFXNREQ.006	Accessibility	Any solution <b>SHOULD</b> 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.
DDCCTR.NFXNREQ.007	Availability	Any solution developed <b>SHOULD NOT</b> be able to accept more than 10 minutes of outage during normal usage and <b>SHOULD NOT</b> accept more than 1 minute of data loss of queries and responses.
DDCCTR.NFXNREQ.008	Availability	It <b>MAY</b> 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 <b>MAY</b> also notify of any planned downtime, retired functionality, release notes, etc.
DDCCTR.NFXNREQ.009	Capacity – current and forecast	The system <b>SHALL</b> 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.
DDCCTR.NFXNREQ.010	Capacity – current and forecast	During periods of peak usage, system traffic <b>MAY</b> surge the number of concurrent users performing read and write operations.
DDCCTR.NFXNREQ.011	Capacity – current and forecast	Forecast growth of the user base is anticipated to be high. As a safety contingency, the system <b>SHOULD</b> support, or have scaling up plans to support, growth of 25% per year.
DDCCTR.NFXNREQ.012	Disaster recovery, business continuity, resilience	All data and derived analysis <b>SHALL</b> be stored within an appropriate data architecture to ensure redundancy and rapid disaster recovery, to eliminate the risk of data loss.
DDCCTR.NFXNREQ.013	Disaster recovery, business continuity, resilience	The system <b>SHOULD</b> provide near-instantaneous switch-over if any one component of the system architecture fails critically (database server, web server, system monitoring job, service bus, etc.).

Requirement ID	Category	Non-functional requirement
DDCCTR.NFXNREQ.014	Disaster recovery, business continuity, resilience	The system <b>SHOULD</b> provide near-instantaneous switch-over if any one component of the physical architecture fails critically (data centre destroyed, server destroyed, etc.)
DDCCTR.NFXNREQ.015	Disaster recovery, business continuity, resilience	All components of the solution <b>SHOULD</b> be underpinned by robust monitoring tools that track usage across space and time, so that system load and source can be queried.
DDCCTR.NFXNREQ.016	Disaster recovery, business continuity, resilience	Data concerning system usage <b>SHOULD</b> 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 <b>SHOULD</b> be possible to export these data.
DDCCTR.NFXNREQ.017	Disaster recovery, business continuity, resilience	It <b>SHALL</b> be possible to automatically log any periods of outage of the system and to supplement and update this record manually.
DDCCTR.NFXNREQ.018	Disaster recovery, business continuity, resilience	It <b>SHALL</b> be possible to trigger system alerts based on uptime and performance.
DDCCTR.NFXNREQ.019	Disaster recovery, business continuity, resilience	It <b>SHOULD</b> 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.
DDCCTR.NFXNREQ.020	Performance/ response time	The solution <b>SHALL</b> 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.
DDCCTR.NFXNREQ.021	Performance/ response time	The solution <b>SHOULD</b> be designed so that degradation of performance due to increased load (surge of users) is minimized.
DDCCTR.NFXNREQ.022	Performance/ response time	Where appropriate, long-running processes such as complex queries <b>MAY</b> 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.
DDCCTR.NFXNREQ.023	Performance/ response time	The system <b>MAY</b> implement detection of a frozen (“hung”) interface to give the user the option to cancel a current request.
DDCCTR.NFXNREQ.024	Performance/ response time	The system <b>SHOULD</b> collect metrics on performance and response time to allow a system administrator to monitor system behaviour, identify bottlenecks or issues, and proactively address any risk of unacceptable degradation of speed.
DDCCTR.NFXNREQ.025	Performance/ response time	As with system availability, the solution <b>SHALL</b> provide dashboards of performance metrics, and allow querying of the performance log and export of performance data for reports.
DDCCTR.NFXNREQ.026	Performance/ response time	As with system availability, the solution <b>SHALL</b> 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 (e.g. bring an extra server into a load-balanced set).
DDCCTR.NFXNREQ.027	Security and privacy	Tools to request an account, log in, log out, set and change passwords, and receive password reminders <b>SHALL</b> be provided.
DDCCTR.NFXNREQ.028	Security and privacy	All interactions between a client and a server component of the solution <b>SHALL</b> be securely encrypted to prevent “man in the middle” interference with data in transit.
DDCCTR.NFXNREQ.029	Security and privacy	Any cloud components of the solution <b>SHALL</b> store their cloud data-at-rest in an encrypted format.
DDCCTR.NFXNREQ.030	Security and privacy	The solution <b>SHALL</b> have a security model that is robust and flexible and controls both access to data and the operations that can be executed against data.
DDCCTR.NFXNREQ.031	Security and privacy	Information about the governance and restricted use of data <b>SHOULD</b> be available within any solution alongside the data concerned, so that users have a clear and consistent reminder of the level of confidentiality, the sensitivity and the permitted use of the data they are currently viewing.

Requirement ID	Category	Non-functional requirement
DDCCTR.NFXNREQ.032	Security and privacy	Dashboards, reports, standard queries and exports of security information <b>SHOULD</b> be provided to assist system administrators in the management of access permissions. Queries to highlight conflicting permissions <b>SHOULD</b> be available.
DDCCTR.NFXNREQ.033	Security and privacy	The confidentiality of data must be managed with utmost care. In shared data environments, there <b>SHALL</b> be a clear separation of between the system's data and any other hosted clients' information. Dedicated hosting and data sources are preferred.
DDCCTR.NFXNREQ.034	Regulation and compliance	Any solution <b>SHOULD</b> be designed to be mindful of existing reference architecture guidelines and standards for distributed trust framework solutions and tools for exchanging diagnostic test result and/or vaccination data.
DDCCTR.NFXNREQ.035	Regulation and compliance	Any solution <b>SHALL</b> be compliant with any data policies and legal requirements identified by the country in whose jurisdiction the solution will operate.
DDCCTR.NFXNREQ.036	Regulation and compliance	It <b>MAY</b> 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.
DDCCTR.NFXNREQ.037	Regulation and compliance	Any solution <b>SHALL</b> 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.
DDCCTR.NFXNREQ.038	Reliability	Any solution <b>SHOULD</b> be designed to maximize the mean time between failures, with appropriate best practice to deliver a robust, well-tested and reliable platform.
DDCCTR.NFXNREQ.039	Reliability	Any solution <b>SHOULD</b> 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.
DDCCTR.NFXNREQ.040	Scalability	Any solution <b>SHOULD</b> be designed so that elements can be scaled out 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.)
DDCCTR.NFXNREQ.041	Scalability	Any solution <b>SHOULD</b> be designed so that elements can be scaled up vertically by (for example) adding extra capacity to solution elements (increased CPU, increased RAM, etc.)
DDCCTR.NFXNREQ.042	Scalability	It <b>MAY</b> be possible to configure rules for automatic horizontal scaling out 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.
DDCCTR.NFXNREQ.043	Scalability	Any solution <b>SHOULD</b> log sufficient information about performance and load so that technical staff can refine the system's scaling strategy based on actual usage.
DDCCTR.NFXNREQ.044	Supportability	Any solution <b>SHOULD</b> provide a feedback channel as described in functional requirements for collecting information and support requests.
DDCCTR.NFXNREQ.045	Supportability	Any solution <b>MAY</b> provide access to learning material to support a user's understanding of how to use the tool and achieve specific aims.
DDCCTR.NFXNREQ.046	Supportability	The solution <b>SHALL</b> 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.
DDCCTR.NFXNREQ.047	Supportability	It <b>MAY</b> 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.
DDCCTR.NFXNREQ.048	Supportability	It <b>SHOULD</b> be possible for technical support staff to filter and query system logs to quickly identify sections of interest.
DDCCTR.NFXNREQ.049	Supportability	It <b>MAY</b> 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.
DDCCTR.NFXNREQ.050	Supportability	Any solution <b>SHALL</b> have a published strategy for the release of patches, maintenance releases and version upgrades.

Requirement ID	Category	Non-functional requirement
DDCCTR.NFXNREQ.051	Usability	Any interface created <b>SHOULD</b> 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.
DDCCTR.NFXNREQ.052	Usability	It <b>SHOULD</b> 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.
DDCCTR.NFXNREQ.053	Usability	The user interface <b>MAY</b> be designed so that navigation via keyboard (e.g. tab movement between fields, use of shortcut keys) is possible if the user does not have access to a pointer device.
DDCCTR.NFXNREQ.054	Usability	When the solution adapts for display on a smartphone/tablet, the interface <b>SHALL</b> be designed mindful of touch-screen interaction.
DDCCTR.NFXNREQ.055	Usability	The solution <b>MAY</b> provide an efficient and easy way to manage taxonomy (for administrator users) – to record standard definitions, relationships between terms, etc.
DDCCTR.NFXNREQ.056	Data retention/ archiving	It <b>SHOULD</b> be possible to manually request an archive of a selected subset of information.
DDCCTR.NFXNREQ.057	Data retention/ archiving	It <b>MAY</b> 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.
DDCCTR.NFXNREQ.058	Data retention/ archiving	It <b>MAY</b> be possible to trigger a notification alert when an archive operation completes (including success and failure reports).
DDCCTR.NFXNREQ.059	Data retention/ archiving	Any archive function <b>SHALL</b> not affect the performance of the system.
DDCCTR.NFXNREQ.060	Data retention/ archiving	Any archive material <b>SHOULD</b> 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.
DDCCTR.NFXNREQ.061	Data retention/ archiving	It <b>SHOULD</b> be possible, with the necessary authority and permissions, to restore information from a chosen archive back into the operational set of information.
DDCCTR.NFXNREQ.062	Data retention/ archiving	All archival operations <b>SHALL</b> be logged.
DDCCTR.NFXNREQ.063	Data retention/ archiving	It <b>SHOULD</b> be possible, with the necessary authority and permissions, to perform a limited search of the contents of archives to identify information of interest.
DDCCTR.NFXNREQ.064	Data retention/ archiving	All information written to archives <b>SHALL</b> be in an encrypted format to prevent misuse if accessed by an unauthorized system or person.

CPU: central processing unit; ID: identifier; RAM: random-access memory.

<sup>a</sup> For definitions of “MAY”, “SHALL” and “SHOULD”, please see the glossary.

## Annex 5

# 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 test event, it is anticipated that complementary digital health infrastructure, such as the architectural elements described by the Open Health Information Exchange (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”.<sup>3</sup>

The OpenHIE high-level architecture is shown in Fig. A5.1. To show how a health-data-sharing infrastructure could support point-of-care digital health solutions to issue DDCC:TRs, 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.

The registries and repositories defined in the OpenHIE architecture may play a role in providing data that are part of the DDCC:TR core data set defined in *Chapter 5*. These registries and repositories include the following.

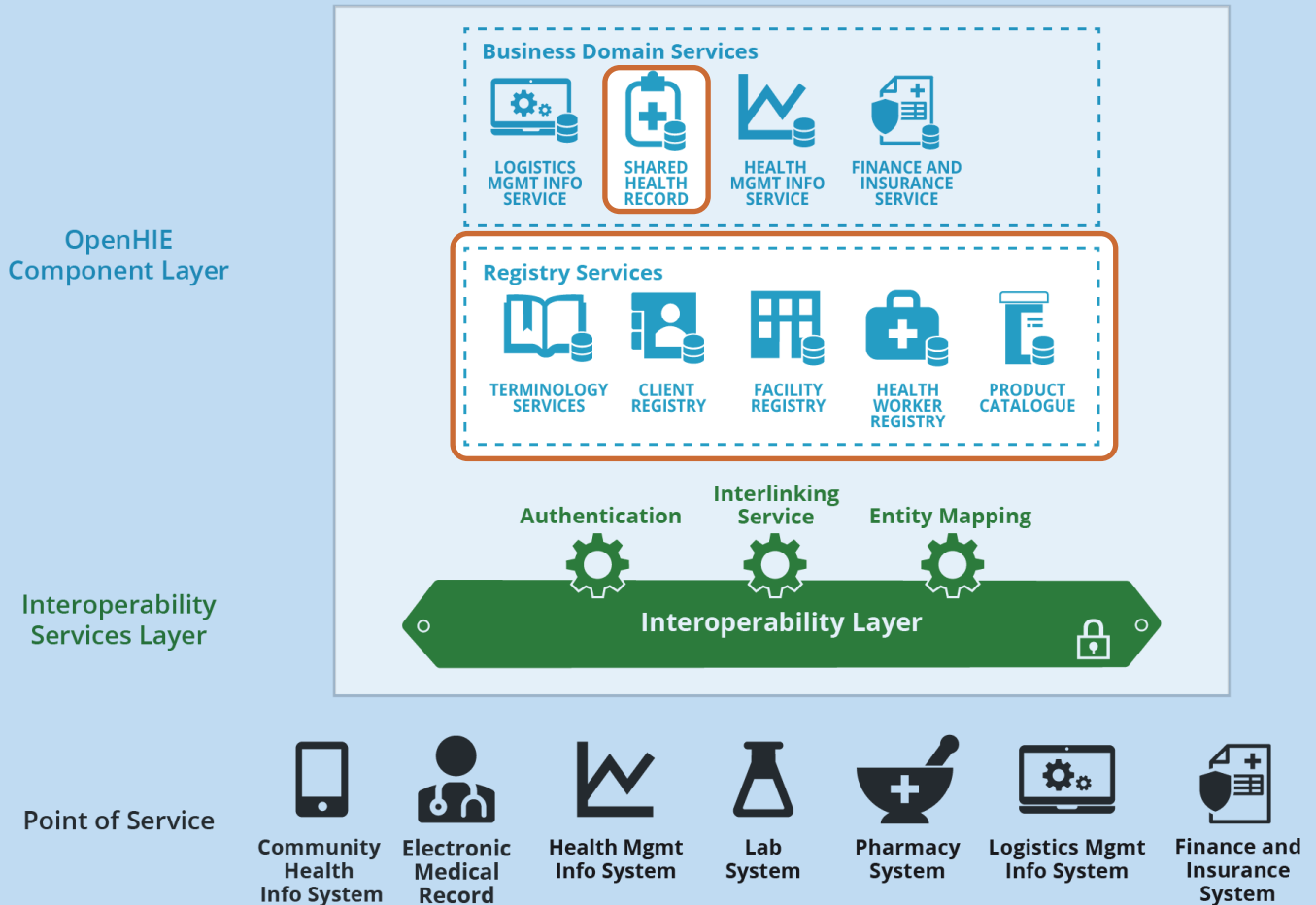
**TERMINOLOGY SERVICES:** Registry services used to manage clinical and health system terminologies, which health applications can use for mapping to other standard or non-standard code systems to support semantic interoperability. For example, a terminology service can be used to manage terminology 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 Tested Person. This database can include a Tested Person’s name, date of birth, sex, address, phone number and email address, plus 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 Tested Person can be found. The data elements in the DDCC:TR core data set that may be populated with data from the client registry include:

- name;
- date of birth; and
- unique IDs.

<sup>3</sup> OpenHIE [website]. OpenHIE; no date (<https://ohie.org/about>, accessed 11 February 2022).

Figure A5.1  
**OpenHIE architecture<sup>a</sup>**



OpenHIE 2021-09-29; CC BY 4.0

<sup>a</sup> Orange boxes indicate registries and repositories relevant to DDCC:TR.

Source: OpenHIE architecture specification, version 3.0. OpenHIE; 2020 (<https://ohie.org/wp-content/uploads/2020/12/OpenHIE-Specification-Release-3.0.pdf>, accessed 11 February 2022). Licensed under creative commons (<https://creativecommons.org/licenses/by/4.0>).

**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:TR 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 and
- country where test was conducted.

**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 organization or individual health facility.

**PRODUCT CATALOGUE:** A system used to manage the metadata and multiple IDs for medical commodities. The data elements in the DDCC:TR core data set that could be obtained from the product catalogue are:

- test type;
- test brand;
- test manufacturer; and
- pathogen targeted.

**SHARED HEALTH RECORD:** A repository that may be used to maintain longitudinal health information about a Tested Person and to support continuity of care over time, across different care delivery sites. Health data in the shared health record may include the Tested Person's diagnostic test results and other clinical information. 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.<sup>4</sup> Data generated during test events could be added to the shared health record, if in use, in order to support future provision of health services.

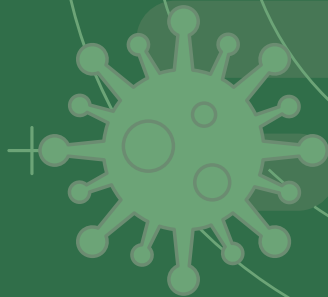
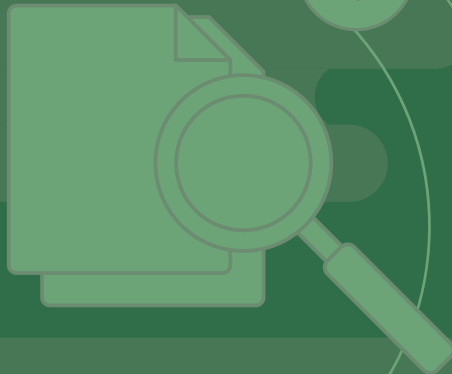
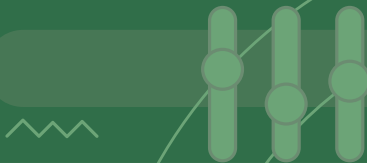
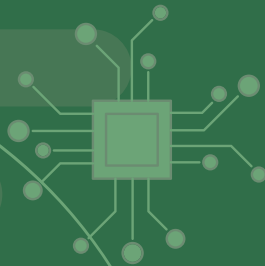
---

<sup>4</sup> International patient summary implementation guide [website]. Ann Arbor, MI: Health Level Seven International – Patient Care Work Group; no date (<https://build.fhir.org/ig/HL7/fhir-ips>, accessed 11 February 2022).





100110  
001101  
010110  
100011



World Health  
Organization