Digital Documentation of COVID-19 Certificates: Test Result

Technical specifications and implementation guidance

World Health Organization

Digital Documentation of COVID-19 Certificates: Test Result: Interim Guidance

WHO reference number: *Will be available*

Suggested citation. *Will be available*

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

CONTENTS

ACKNOWLEDGEMENTS

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

ABBREVIATIONS

1D	one-dimensional
2D	two-dimensional
AEFI	adverse event(s) following immunization
Ag-RDT	Antigen detection rapid diagnostic test
API	application programming interface
COVID-19	Coronavirus disease 2019
DDCC	Digital Documentation of COVID-19 Certificates
DDCC:TR	Digital Documentation of COVID-19 Certificates: Test Result
DDCC:VS	Digital Documentation of COVID-19 Certificates: Vaccination Status
DSC	document signer certificate
EIS	Event Information Site
FHIR	Fast Healthcare Interoperability Resources
HCID	health certificate identifier
HL7	Health Level Seven
HPV	human papillomavirus
ICD	International Classification of Diseases
ICT	information and communications technology
ID	identifier
IHR	International Health Regulations (2005)
IPS	International Patient Summary
ISO	International Organization for Standardization
LIS	Laboratory Information System
NAAT	Nucleic Acid Amplification Test
OpenHIE	Open Health Information Exchange
PHA	public health authority
PHSMs	public health and social measures
PKI	public key infrastructure
QA	quality assurance
SHR	shared health record
SLA	service level agreement
SNOMED CT GPS	Systematized Nomenclature of Medicine Clinical Terms Global Patient Set
WHO-FIC	WHO Family of International Classifications

GLOSSARY

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 method of lateral flow immunoassay.

Certificate: A document attesting a fact. In the context of the lab 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 (CA): Also known as a "certification authority" in the context of a PKI, 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 the processing of personal data. A data controller has primary responsibility for the protection of personal data.

Data processing: 'processing' means any operation or set of operations performed on personal data or on sets of personal data, whether 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 the Tested Person, such as a minor child, or represents a person who is physically or legally incapable to give consent for the processing of its personal data.

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

Digital Documentation of COVID-19 Certificate(s) (DDCC): A digitally signed HL7 FHIR document that represents the core data set for the relevant COVID-19 certificate.

Digital Documentation of COVID-19 Certificate(s): 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 Health Level Seven (HL7) Fast Healthcare Interoperability Resources (FHIR) document containing the data elements included in the DDCC:TR core data set.

DDCC:TR 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.

DDCC:TR Registry Service: The service that can be used to request and receive metadata associated with a DDCC:TR.

DDCC:TR Repository Service: A, potentially federated, service that serves as a repository, or database, of the health content associated to DDCC:TR.

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 and/or digital health folder which contains one or more test events and associated certificates. Each test event corresponds to a DDCC:TR.

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

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

Identifier: A name that labels the identity of an object or individual. 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 identifiers 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, is a software system that supports the laboratory activities. Key functionality includes receiving and storing requests for tests and test results. 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, etc.).

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

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 (e.g. 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. For this document, it is assumed that the 1D barcode follows one of the international specifications.

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 it can be pre-printed 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 includes biographical data (biodata), such as name, sex, civil status, date and place of birth, country of origin, country of residence, individual registration number, occupation, religion, and ethnicity; biometric data, such as a photograph, fingerprint, facial or iris image; health data; as well as any expression of opinion about the individual, such as assessments of his or her health status and/or specific needs.

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

Public key infrastructure (PKI): The policies, roles, software and hardware components and their governance that facilitate digital signing of documents and issuance, distribution, and exchange of keys.

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

SHALL: SHALL is used to describe technical features and functions that are mandatory for this specification.[2]

SHOULD: SHOULD is used to describe technical features and functions that are recommended, but they 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 highly recommended to review the reasons for not following the recommendations before deviating from the technical specifications outlined.[3]

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 information needed for clinical use. Test reports differ from a "test certificate" 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 way to represent information using individual black dots within a square or rectangle. For example, a QR code is a type of 2D barcode. It is similar to a linear (1D) barcode, but it can represent more data per unit area. There are different types defined by open standards.

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

Verifier Application: A secure application used to verify the SARS-CoV-2 diagnostic test result presented on the DDCC:TR. A verifier can use the verifier app to scan the barcode and display the data held within the DDCC:TR. The verifier app does not store or transmit any personal data.

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

EXECUTIVE SUMMARY

In the context of the coronavirus disease (COVID-19) pandemic, the concept of **Digital Documentation of COVID-19 Certificates (DDCC)** is proposed as a mechanism by which a person's COVID-19-related health data can be digitally documented via an electronic certificate. A test report that documents a person's SARS-CoV-2 diagnostic test result can be used to generate a certificate that serves 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 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.

The document is the second part of a series of two guidance documents (see Figure 1) on digital documentation of COVID-19-related data of interest: vaccination status and test result (this document). Technical specifications and implementation guidance regarding certificates for "Proof of Negative SARS-CoV-2 Test Result" and "Proof of Previous SARS-CoV-2 Infection" have been combined into a single DDCC:TR document because both certificates will require some form of testing prior to issuance.

Figure 1 Guidance documents for DDCC

DDCC: Vaccination Status	DDCC: Test Result	
SARS-CoV-2 Vaccination Status	**Proof of Negative SARS-CoV-2 Test Result**	**Proof of Previous SARS-CoV-2 Infection**
Guidance on digitally documenting SARS-CoV-2 vaccination status	Guidance on digitally documenting SARS-CoV-2 diagnostic test results	Guidance on digitally documenting proof of previous SARS-CoV-2 infection

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

What is the DDCC:TR?

A test result certificate 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. It includes minimal details 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). When required by government authorities, based on technical and ethical considerations, a test result certificate can be used as proof of negative SARS-CoV-2 test result or proof of previous SARS-CoV-2 infection[1] (1) for individualized exemptions from public health and social measures and/or (2) for accessing certain socioeconomic activities.[11] A test result certificate is a health document, and it is not intended for use as an identity document. It is up to Member States to determine the policies and procedures for binding a test result certificate to an individual's identity.

A "test result certificate" differs from a "test report". "Test reports" contain all relevant medical information, clinical interpretation of that test, and detailed information for use by authorized health workers for ongoing clinical care, early detection and containment measures (e.g. contact tracing and case reporting). Table 1 provides a non-exhaustive list of different uses of a "test report" compared to a "test result certificate".[2] A "test report" does not have an expiration date, and it may not necessarily be verifiable by a third party. A "test result certificate", however, requires the information contained on a SARS-CoV-2 "test report" to generate a DDCC:TR. The "test result certificate" describes the SARS-CoV-2 diagnostic test result for a tested person, and it often has a time-bound period of validity. Furthermore, unlike a "test report", the "test result certificate" is digitally signed and can be verified in an online, or offline, manner. Table 2 provides additional details related to the distinction between a "test report" and "test result certificate".

Table 1 Different uses for a "test report" and a "test result certificate"

Test Report	Test Result Certificate
Test reports are widely known and accepted. There is no additional need to verify these reports as they are already commonly used for clinical care, early detection of cases, and infection containment measures: • Clinical care • Contact tracing • Case reporting • Screening	The use of test result certificates should be determined by Member States, based on their existing legal frameworks, and their risk-based approach to pandemic control and mitigation. They can be used domestically or internationally. Some example scenarios of use include: • International travel • Access to socioeconomic activities (e.g. restaurants, sporting events, etc.)

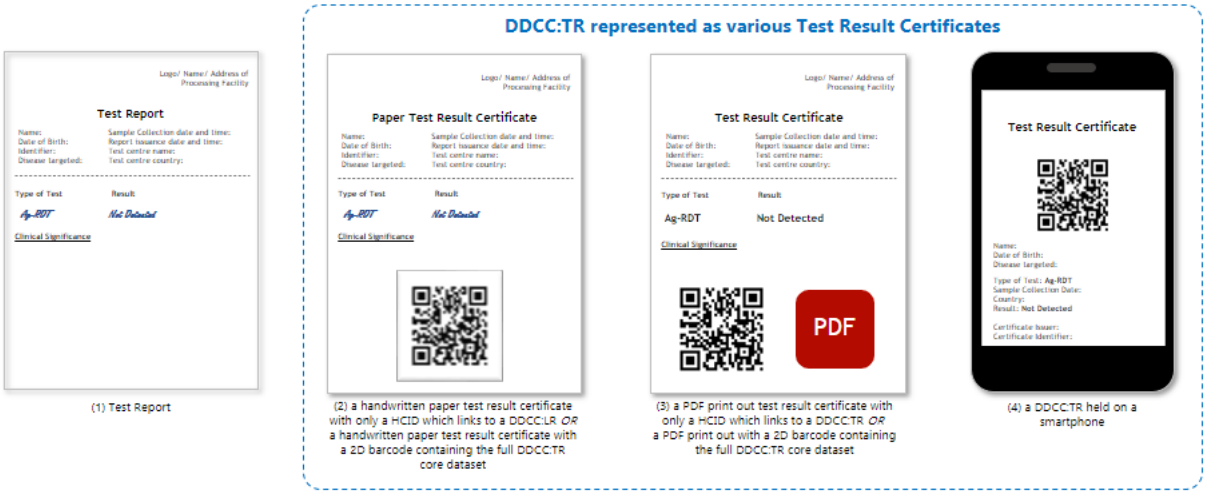
A DDCC:TR can be purely digital (e.g. stored in a smartphone application or on a cloud-based server) or it can be a computable representation of a test report rendered as a paper test result certificate

[1] Technical considerations for implementing a risk-based approach to international travel in the context of COVID-19: interim guidance (https://apps.who.int/iris/handle/10665/342212)
[2] Requirements and Scope of Digital Certificates (https://sciencetaskforce.ch/en/policy-brief/requirements-and-scope-of-digital-certificates/)

(see Figure 2). A digital certificate should never require individuals to have access to a smartphone or computer. The link between the paper test result certificate and the digital record can be established 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 a SARS-CoV-2 diagnostic test result 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 test result certificates can then be produced from a DDCC:TR.

Figure 2 Different representations of a test result



Proof Scenarios of the DDCC:TR

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

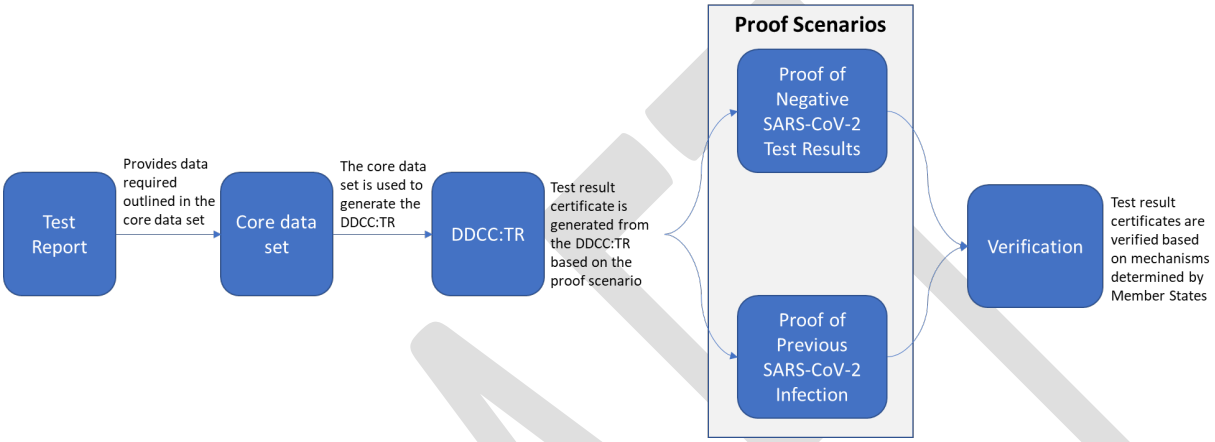
1. **Proof of Negative SARS-CoV-2 Test Result:** Test result certificates can be used as documented evidence of a negative test result when SARS-CoV-2 is not detected by a SARS-CoV-2 diagnostic test for viral detection (e.g. a nucleic acid amplification test (NAAT) or an antigen detection rapid diagnostic test (Ag-RDT)).[1]
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. nucleic acid amplification test (NAAT) or antigen detection rapid diagnostic test (Ag-RDT)).[1] 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 Proof of Previous SARS-CoV-2 Infection and proof that the individual is no longer infectious as per WHO's criteria for releasing COVID-19 patients from isolation.[1,8,9]

Member States can use WHO guidance to determine which type of tests are appropriate for each certificate. A risk assessment on the impact of the use of diagnostic testing for the DDCC is recommended. Key considerations for this risk assessment can include considerations related to

sensitivity and specificity of SARS-CoV-2 diagnostic tests, access to testing (e.g. does it lead to inequality in society) and the Member State's epidemiological situation.[1]

Figure 3 depicts the overall steps of how a test report is leveraged to create a verifiable test result certificate.

Figure 3 Overall DDCC:TR Process



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 specific SARS-CoV-2 diagnostic test used to generate the test report.[16,17,18,20,21,22,23,36] Furthermore, how these 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 business rules for test result certificates in cross-border use cases. The use cases within the two scenarios will further vary depending on the digital maturity and local context of the country in which a DDCC:TR solution is implemented.

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

DDCC:TR 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 (e.g. due to a digital divide) or access to diagnostic testing. The recommendations for the implementation of DDCC:TR 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 accordingly to allow the greatest possible flexibility for Member States and their implementer(s) to build a solution that is fit for purpose in the context of their overall health information systems.

The minimum requirements for a DDCC:TR implementation are as follows.

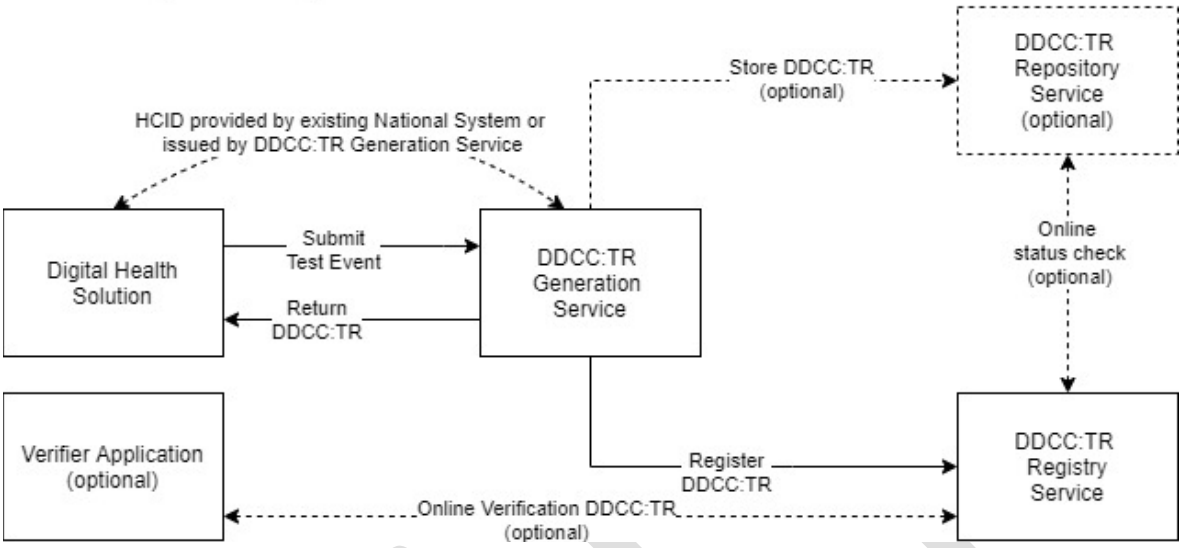
- The potential benefits, risks and costs of implementing a DDCC:TR solution should be assessed before introducing a DDCC:TR system and its associated infrastructure. This includes

an impact assessment of the ethical and privacy implications and potential risks that may arise with the implementation of a DDCC:TR.

- Member States must establish policies for the appropriate use, data protection and governance of the DDCC:TR 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 either in a paper 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:TR Generation Service to digitally sign an electronic version of the required data elements in the core data set (including metadata), to produce a DDCC:TR. The DDCC:TR Generation Service is responsible for taking test result data, representing it using the HL7 FHIR standard, digitally signing the HL7 FHIR document and updating the DDCC:TR Registry (see below).
- Where a paper test result certificate is used, it must be associated with a health certificate identifier (HCID). A DDCC:TR must be associated, as a digital representation, with the paper test result certificate via the HCID. Multiple digital representations of the DDCC:TR (e.g. a 2D barcode) may be associated with paper test result certificate via the HCID. One or more test result certificates may be associated to a single HCID, and each test result certificate may have its own identifier.
- 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:TR Registry Service must exist and is responsible for storing metadata about the DDCC:TR that is retrievable with the HCID. At a minimum, the DDCC:TR Registry Service stores the core metadata described in section 5.2.
- One or more DDCC:TR Repository Service(s) may exist, which can be used to retrieve a DDCC:TR, in which case the location of the DDCC:TR may also be included in the metadata within the DDCC:TR Registry Service.

Figure 4 shows the relationships between the digital services. The different services are discussed in more detail in Sections 3 and 4.

Figure 4 The relationships between the digital services



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

1 INTRODUCTION

Coronavirus disease (COVID-19), caused by the severe acute respiratory syndrome coronavirus 2 (SARS-CoV-2), was first identified in December 2019 and has spread to become a global pandemic. The pandemic has negatively impacted 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 will still need to be in place due to the continued transmission in all countries. As part of an overall package of interventions, some countries are requiring proof of SARS-CoV-2 diagnostic test results to facilitate the safe and free movement of citizens, including access to socioeconomic activities and public gatherings.

Digital technology can be leveraged to augment paper-based SARS-CoV-2 diagnostic test results, which are easily lost and prone to fraud.[3,4,5,6] There are a wide range of digital solutions that can be used to digitally document a SARS-CoV-2 diagnostic test results, and choices on design and implementation should be guided by balancing various values and contextual considerations. To ensure respect for human rights and protection of values such as equity and public trust, the technical specifications and implementation guidance outlined in this document have been built on the basis of the ethical considerations and data protection principles described in Chapter 2 of the document.

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 a core data set of key information to be recorded, 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 negative SARS-CoV-2 test result or proof of previous or history of SARS-CoV-2 infection. The document leverages existing free and open standards, and is driven by the ethics, use cases and requirements for Digital Documentation of COVID-19 Certificates: Test Result (DDCC:TR).

[3] Joburg healthcare worker nabbed for allegedly selling fake Covid-19 test certificates (https://www.news24.com/news24/southafrica/news/joburg-healthcare-worker-nabbed-for-allegedly-selling-fake-covid-19-test-certificates-20210822)

[4] Margit, M. Thousands of Israelis Join Telegram Groups Selling Fake COVID Papers - The Media Line (https://themedialine.org/by-region/thousands-of-israelis-join-telegram-groups-selling-fake-covid-papers/)

[5] 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.

[6] Fake Covid vaccine and test certificate market is growing, researchers say (https://www.theguardian.com/world/2021/may/16/fake-covid-vaccine-and-test-certificate-market-is-growing-researchers-say)

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 target audience of this document are national authorities tasked with creating or overseeing the development of digital certificates for COVID-19. The document may also be useful to government partners such as local businesses, international organizations, non-governmental organizations and trade associations, that may be required to support Member States in developing or deploying a DDCC: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, and privacy and data protection principles for the design, implementation and use of a DDCC:TR;
- → Proof scenarios and use cases arising from the operation of a DDCC:TR, including the sequence of steps involved in executing the scenarios;
- → A core data set with the data elements that must be included in a DDCC:TR documenting a SARS-CoV-2 diagnostic test result as required by the use cases;
- → A Health Level Seven (HL7) Fast Healthcare Interoperability Resource (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, 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 test result certificates
- → Any guidance regarding interpretation or decision-making of the information provided in a DDCC:TR for any purpose.
- → Digital documentation of COVID-19 vaccination status certificate (which is covered in a separate guidance document)[7];
- → Digital documentation of COVID-19 certificates for proof of recovery status to exempt individuals from testing or quarantine requirements for travelling internationally because of the uncertainty around any immunity status arising from recovery from previous infection

[7] Digital documentation of COVID-19 certificates: vaccination status: technical specifications and implementation guidance, 27 August 2021 (https://www.who.int/publications/i/item/WHO-2019-nCoV-Digital_certificates-vaccination-2021.1)

and the additional data required to provide proof that an individual has met WHO's criteria for releasing COVID-19 patients from isolation;[1,8,9]

- → Processes for specimen collection, data collection and sample analyzation. WHO guidance on diagnostic testing for SARS-CoV-2 can be found in the separate reference documents;[16,17,18,20,21,22,23,36]
- → Processes for generation and verification of test reports (which will be up to the Member States);
- → Issuance and validation of test result certificates for self-tests, at-home tests and antibody tests;
- → 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 Tested Person identification should be based on existing policies and mechanisms of Member States;
- → Any requirements in regard to quality assurance of laboratories, medical devices and diagnostic tests used to perform the test and provide a test report. These should be guided by existing national and international standards and regulations for diagnostic laboratories, medical devices and tests as defined by the mandated authorities of the Member States.
- → Considerations for monitoring and evaluation of DDCC:TR roll-out and use;
- → The choice of algorithm for generating any two-dimensional (2D) barcodes, which is at the discretion of the Member State. A Member State may augment the core data set with additional information to provide a stronger identity binding than is presumed in this document, for use cases that require it under existing Member State policies and regulations. Identity binding would enable utilization of existing 2D barcode algorithms such as those set out by the International Civil Aviation Organization (ICAO) and the European Union. The HL7 FHIR implementation guide (at https://WorldHealthOrganization.github.io/ddcc) provides an algorithm for generating (2D) barcodes that may be used in the absence of identifying information beyond that found within the core data set; and
- → Technical functionality to support selective disclosure of information contained in DDCC:TR.

1.4 Assumptions

The technological specification for a DDCC:TR 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

[8] Criteria for releasing COVID-19 patients from Isolation (https://www.who.int/news-room/commentaries/detail/criteria-for-releasing-covid-19-patients-from-isolation)

[9] COVID-19 Clinical management: living guidance (https://www.who.int/publications/i/item/WHO-2019-nCoV-clinical-2021-1)

solutions will be implemented to operationalize the requirements described in this document. This allows for support of local and sustainable development so that Member States have a broad choice of appropriate solutions without excluding compliant products from any source.

The following assumptions are made about Member States' responsibilities as foundational aspects of setting up and running a DDCC: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, in any event, any applicable obligations related to respecting human rights and data protection policies.
- Member States will adhere to ethical principles and act to prevent new inequities from being created by a DDCC:TR solution.
- The DDCC:TR is a health document associated with an individual who has proved they are who they claim they are, based on the policies established by the Member State; it is not, itself, an identity card or identification document.
- It will be up to the Member State to determine the business rules for acceptance of a test result certificate and the certificate validity period for each proof scenario for domestic and/or international use cases.
- It will be up to the Member State to determine the mechanism for identification of the Tested Person.
- It will be up to the Member State 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 in another format.
- If a Member State decides to implement the DDCC:TR in a paper format containing a machine-readable barcode (1D or 2D) (i.e. a paper test result certificate), any paper test result certificate issued will need to have a health certificate identifier (HCID) in both a human-readable and machine-readable format to link it to a digital record. The HCID will be used as an index key for the DDCC:TR.
- Respecting the data protection principles (see section 2.2), Members States will adhere to data protection and privacy laws and regulations established under national law or adopted through bilateral or multilateral agreements.
- The PHA of a Member State will need to have access to a national public key infrastructure (PKI) for digitally signing the DDCC:TR. This document does not describe the PKI in detail, but key assumptions are that the PHA will need 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 DDCC:TR;
    - generate and cryptographically sign document signer certificates (DSCs);
    - authorize document signer private keys to cryptographically sign digital DDCC:TR;
    - broadly disseminate public keys if there is a desire to allow others to cryptographically validate 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, including, as a minimum, a DDCC:TR identified through the HCID; a Member State may choose to also generate and distribute to the DDCC:TR Holder a signed 2D barcode as a digital

representation, containing, as a minimum, the core data set content (e.g. printed on or attached to the paper record, sent by email, loaded into a smartphone app, downloaded from website);
    - keep the signature-verification processes manageable; the number of private keys used by the PHA to sign DDCC:TR should be no more than a small proportion relative to the number of digital health solutions used to capture health events; and
    - ensure private keys used to sign DDCC:TR will not be associated with individual health workers.
- The PHA of a Member State will need to operate a DDCC:TR Generation Service to create DDCC:TR, and a DDCC:TR Registry Service to record their issuance. Optionally, the PHA may also decide to provide a DDCC:TR Repository Service to allow requestors to search for, and retrieve, a DDCC:TR using the HCID (for the purposes of verification).

1.5 Methods

Since the COVID-19 pandemic began, the number of digital solutions for test result certificate has increased. WHO intends to remain software agnostic, and have conducted consultations with multisectoral experts focused on supporting development of key standards for digital test result certificate, sharing joint learning and supporting development of a governance model with a national trust framework architecture. Furthermore, the WHO has developed this guidance in consultation with Member States and partner organizations to ensure it is implementable in all contexts.

1.6 Additional WHO guidance documents

Specific guidance on when, where and how DDCC:TR 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, 2 July 2021[10]Technical considerations for implementing a risk-based approach to international travel in the context of COVID-19: interim guidance, 2 July 2021[1]

→ Considerations for implementing and adjusting public health and social measures in the context of COVID-19: interim guidance, 14 June 2021[11]

→ Statement on the ninth meeting of the International Health Regulations (2005) Emergency Committee regarding the coronavirus disease (COVID-19) pandemic[12]

[10] Policy considerations for implementing a risk-based approach to international travel in the context of COVID-19. Geneva: World Health Organization; 2 July 2021 (https://apps.who.int/iris/handle/10665/342235, accessed 6 July 2021)

[11] Considerations for implementing and adjusting public health and social measures in the context of COVID-19. Geneva: World Health Organization; 14 June 2021 (https://apps.who.int/iris/handle/10665/341811, accessed 17 September 2021)

[12] Statement on the ninth meeting of the International Health Regulations (2005) Emergency Committee regarding the coronavirus disease (COVID-19) pandemic (who.int)

- → Statement on the eighth meeting of the International Health Regulations (2005) Emergency Committee regarding the coronavirus disease (COVID-19) pandemic[13]
- → Statement on the seventh meeting of the International Health Regulations (2005) Emergency Committee regarding the coronavirus disease (COVID-19) pandemic[14]
- → Statement on the sixth meeting of the International Health Regulations (2005) Emergency Committee regarding the coronavirus disease (COVID-19) pandemic[15]

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, 11 September 2020[16]
- → COVID-19 diagnostic testing in the context of international travel: scientific brief, 16 December 2020[17]
- → SARS-CoV-2 antigen-detecting rapid diagnostic tests: An implementation guide, 21 December 2020[18]
- → COVID-19 natural immunity, 10 May 2021[19]
- → Recommendations for national SARS-CoV-2 testing strategies and diagnostic capacities, 25 June 2021[20]

---

[13] 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)

[14]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, accessed 27 June 2021)

[15] 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, accessed 27 June 2021)

[16] Diagnostic testing for SARS-CoV-2, 11 September 2020 (https://www.who.int/publications/i/item/diagnostic-testing-for-sars-cov-2)

[17] COVID-19 diagnostic testing in the context of international travel: scientific brief, 16 December 2020 (https://apps.who.int/iris/handle/10665/337832)

[18] SARS-CoV-2 antigen-detecting rapid diagnostic tests: An implementation guide, 21 December 2020 (https://www.who.int/publications/i/item/9789240017740)

[19] COVID-19 natural immunity, 10 May 2021 (https://www.who.int/publications/i/item/WHO-2019-nCoV-Sci_Brief-Natural_immunity-2021.1)

[20] Recommendations for national SARS-CoV-2 testing strategies and diagnostic capacities: interim guidance. 25 June 2021 (https://www.who.int/publications/i/item/WHO-2019-nCoV-lab-testing-2021.1-eng, accessed 8 September 2021).

→ Antigen-detection in the diagnosis of SARS-CoV-2 infection, 6 October 2021[21]
→ Assessment tool for laboratories implementing SARS-CoV-2 testing: interim guidance 23 October 2020[36]
→ Laboratory biosafety guidance related to COVID-19: interim guidance, 28 January 2021[22]
→ Advice on the use of point-of-care immunodiagnostic tests for COVID-19 scientific brief 8 April 2020[23]

1.7 Other initiatives

The DDCC:TR core data set guidance laid out in this document may be leveraged to generate artefacts conformant with other initiatives such as the International Civil Aviation Organization (ICAO) guidelines on visible digital seals ("VDS-NC") for travel-related health proofs[24] and the European Union (EU) EU Digital COVID Certificate.[25] Additional technical details can be found on the DDCC:TR implementation guide available at: WorldHealthOrganization.github.io/ddcc.

[21] Antigen-detection in the diagnosis of SARS-CoV-2 infection, 6 October 2021 (https://www.who.int/publications/i/item/antigen-detection-in-the-diagnosis-of-sars-cov-2infection-using-rapid-immunoassays)
[22] Laboratory biosafety guidance related to coronavirus disease (COVID-19): Interim guidance, 28 January 2021 (https://www.who.int/publications/i/item/WHO-WPE-GIH-2021.1)
[23] Advice on the use of point-of-care immunodiagnostic tests for COVID-19 (https://www.who.int/news-room/commentaries/detail/advice-on-the-use-of-point-of-care-immunodiagnostic-tests-for-covid-19)
[24] Guidelines: visible digital seals ("VDS-NC") for travel-related health proofs. International Civil Aviation Organization (ICAO) Technical Advisory Group (TAG) on the Traveler Identification Group (TRIP); no date (https://www.icao.int/Security/FAL/TRIP/PublishingImages/Pages/Publications/Guidelines%20-%20VDS%20for%20Travel-Related%20Public%20Health%20Proofs.pdf, accessed 27 June 2021).
[25] 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, accessed 27 June 2021).

2 ETHICAL CONSIDERATIONS AND DATA PROTECTION PRINCIPLES

As with any digital solution, there are ethical considerations, such as potential impacts on equality and human rights, and data protection principles that need to inform the design of the DDCC:TR technical specifications, as well as provide guidance on how resulting solutions can be ethically implemented. [26] The following sections discuss key ethical considerations and data protection principles that Member States are encouraged to – and, where they have legal obligations, must – include in their respective deployments of DDCC:TR. These ethical considerations and data protection principles have also informed the design criteria for a DDCC:TR outlined in the following section.

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).[20] As proof of a negative SARS-CoV-2 test result, or proof of previous SARS-CoV-2 infection, a DDCC:TR may be issued to individuals based on test results initially recorded for these individual or public health reasons, or they could undergo testing to specifically obtain a DDCC:TR. The functions of a DDCC:TR are distinct from the aforementioned individual or public health purposes because it is a test certificate (as opposed to a test report) issued to individuals that may be used for individualized exemptions from public health and social measures (e.g. post-exposure quarantine), or to facilitate safe free movement or regulation of access to socio-economic 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 and provides some recommendations for their ethical implementation.

2.1.1 Key ethical considerations for current proposed uses of 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, including the ethical aims of public health action, and procedural values for governing the decision-making process.

[26] 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).

2.1.1.1 Ethical Aims

A good 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 WELFARE**: to protect and promote the welfare of individuals and communities.
2. **ENSURING EQUAL TREATMENT:** to ensure equal treatment for all individuals and prevent or mitigate, as far as possible, avoidable and unfair health differences (i.e. health inequities) within the boundaries of the state.
3. **ENGENDERING PUBLIC TRUST:** to create and maintain 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 result for individuals in a reliable and accurate manner, which can be used exempt holders from certain public health and social measures; or, to facilitate their safe free movement and access to socio-economic activities in lieu of or in addition to a 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 Equal Treatment

Equal treatment requires respecting and protecting all persons equally and acting to ensure, as far as possible, that there is no wrongful or unfair discrimination which 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 to prevent discrimination against those who have not been vaccinated and are not able to provide a DDCC:VS; and to promote equity through the mitigation of possible disadvantages in opportunities for participation in civil, social, and economic life. For example, DDCC:TR will be especially useful for those who lack access to, or who 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 availability; those who are vaccinated but cannot obtain or provide proof of a valid vaccination status (e.g. individuals who obtain COVID-19 vaccines from illicit sources, recipient country does not recognize or accept the vaccine brand); and, those who are waiting to receive a subsequent dose according to recommended vaccination schedules. Depending on epidemiological and other reasons, a DDCC:TR may also be required as an additional certificate for individuals with a DDCC:VS to ensure safe free movement and gatherings, especially in environments that pose higher risks.

Like the introduction of DDCC:VS, use of a DDCC:TR as a "health pass" for access to socio-economic activities (e.g. work, domestic and international travel, cultural, entertainment, leisure, conferences, industry trade shows and sporting events) may exacerbate inequalities highlighted by 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 below or at 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 DDCC:TR for safe movement may face more burdens than those who have a DDCC:VS. For example, individuals who rely on DDCC:TR as a requirement to perform their work, to travel, or access other socio-economic activities may need to undergo multiple or 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) which 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 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:TR will ensure that the burdens for individuals who use a DDCC:TR for safe free movement are not disproportionate, and that DDCC:TR and DDCC:VS holders are treated equivalently with respect to exemptions from public health restrictions, unless there are evidence-informed, risk-based reasons to impose differentiated measures. 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 the delivery of the aim of protecting and promoting welfare. To enhance trust, a DDCC:TR should only be used for its intended purpose, as illegitimate uses (e.g. unjustified exclusion from a socio-economic activity) may result in legitimate uses (e.g. facilitation of safe free movement) being undermined.

2.1.1.2 Procedural Values

The pursuit of the ethical aims above can raise additional ethical issues. One way to mitigate ethical issues associated with the pursuit of these ethical aims via deployment of a DDCC:TR is by ensuring that decision-making processes uphold important procedural values. These values, in turn, also contribute to the effective pursuit of the aims. Such values include:

→ **TRANSPARENCY:** providing clear, accurate and publicly accessible information about the basis for the policy and the process by which it is made, from the onset (i.e. notifying the public that such a process is underway). Such a process disciplines decision-making and ensures accountability by providing 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 face distinct or heightened risks with the implementation of DDCC:TR (e.g. individuals who have concerns with SARS-CoV-2 testing due to, for example, the burdens of isolation if one is tested 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 series of recommendations are for the two proof scenarios: Proof of negative SARS-Cov-2 test result and Proof of previous SARS-CoV-2 infection.

1. TESTING AND CERTIFICATION SHOULD BE AS ACCURATE AS POSSIBLE: Use of DDCC:TR to facilitate exemptions from public health and social measures, safe free movement, or access to socio-economic activities is based on the assessment that those with the certificate are at sufficiently low risk of transmitting SARS-CoV-2 to others (proof of negative SARS-CoV-2 test result), and/or at sufficiently low risk of severe disease and death if they contract COVID-19 (proof of previous SARS-CoV-2 infection). Therefore, testing and certification should be reliable and accurate to minimize false negatives to mitigate the risk of disease spread or the incidence of severe cases (which would help prevent healthcare resources and systems from being strained), as well as to minimize false positives to prevent the unnecessary imposition of public health and social restrictions on individuals. Member States should conduct the necessary risk assessment to determine what types of SARS-CoV-2 diagnostic tests for proof of negative SARS-CoV-2 test result are appropriate and sufficiently accurate and reliable for the different uses of DDCC:TR.[1,10,17,20,21] It is also for Member States to determine the requirements for proof of a previous SARS-CoV-2 infection to obtain a DDCC:TR, such as the type of

test needed and who should carry out the testing, based on relevant scientific information and risk assessment. [16,17,18,20,21,22,23,36]

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

3. DDCC:TR SHOULD NOT BE REQUIRED TO ACCESS ESSENTIAL SERVICES. COVID-19 certificates should not be a requirement to access goods and services that support the basic necessities of daily life (e.g. health and social services, buying groceries, public transport). Exclusion of those without a COVID-19 certificate from goods and services that meet basic needs would violate human rights. In addition, any public health benefits 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 use of such services could be mitigated by compliance with public health and social measures by everyone (e.g. wearing a mask, physical distancing) as well as broader measures such as contact tracing and isolation.

4. POTENTIAL BENEFITS, RISKS AND COSTS SHOULD BE ASSESSED BEFORE INTRODUCTION OF A DDCC:TR. The creation or development of a DDCC:TR should be based on an assessment of the benefits and costs of its uses, and the advantages and disadvantages of the proposed infrastructure, in comparison with other potential or existing ways to record, validate and verify test results and records. A benefits and costs 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 ensure safe 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 to individuals, families, businesses, and other relevant stakeholders should be assessed prior to implementation. Community engagement, particularly with representatives of groups who are likely to face increased disadvantages or risks, should also be conducted.

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, timely, and affordable and/or free of charge. For the specific activities, venues or services that require a DDCC:VS for access, DDCC:TR can be permitted as an alternative certificate to a DDCC:VS to regulate safe free

movement.[27] It is necessary to provide cost-effective DDCC:TR solutions, including paper-based certificates, 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. Any additional public health and social measures imposed on individuals with a DDCC:TR that are not required for those with a DDCC:VS should be based on clear scientific evidence that the additional measures are necessary and proportionate and do not constitute violation of human rights.

6. ALL COMMUNICATION SHOULD BE CLEAR AND TRANSPARENT. Relevant information pertaining to the implementation of a DDCC:TR should be communicated in a transparent and accessible manner (including in language that is comprehensible to affected parties), which would help contribute to the promotion of public trust and acceptance of DDCC:TR. This communication includes how DDCC:TR would work to benefit individuals, public health and society at large; the threshold or criteria for why 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 would also include specific requirements of the testing process (e.g. recognized tests and providers, number of tests), costs, the duration of validity of the certificate, the locations or activities for which a DDCC:TR is used, the restrictions that would be removed or remain for a DDCC:TR holder in a given context, and the implications of testing positive for active infection and required or recommended actions (e.g. the need to self-isolate and physically distance from others).

7. THE DDCC:TR SHOULD BE CONSTANTLY MONITORED FOR IMPACT AND ADJUSTED AS NECESSARY. Post implementation, it is important to monitor and evaluate the effects of DDCC:TR regularly in terms of positive and negative outcomes (e.g. impact on public health, equity, 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 legitimate and illegitimate use categories 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, and the information should be made publicly available to promote transparency and trust.

8. THERE SHOULD BE ETHICAL SAFEGUARDS WHEN DDCC:TR DATA IS USED FOR SCIENTIFIC PURPOSES. Use of DDCC:TR data for scientific purposes (e.g. research) is ethically justifiable when they 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 this regard, appropriate ethics oversight and governance of such data uses (including for

[27] Scottish Human Rights Commission. COVID-19 status certificates: human rights considerations. April 2021 (https://www.scottishhumanrights.com/media/2176/21_04_28_-covid-certificates-and-human-rights-vfinal.pdf, accessed 30 August 2021)

non-research activities such as surveillance[28]) should be implemented. Data subjects and other members of the public should also be informed of the nature and occurrences of these activities in advance, and any options they may 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 the data subjects. Where DDCC:TR data need to be retained in an identifiable form for these purposes, consideration should be given to whether consent is required or should be waived based on satisfaction of appropriate ethical criteria (e.g. minimal risk, impracticability of obtaining consent, no adverse effects on the rights and welfare of the data subjects and serving a public health good).

2.2 Data protection principles for a DDCC:TR

The previous section highlights the importance of data protection to the fostering of public trust in the implementation of DDCC:TR. This section presents specific and fundamental data protection principles for the deployment of a DDCC:TR 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 the DDCC:TR. The objectives are to encourage Member States to adopt or adapt their national laws and regulations, as necessary, respect personal data protection principles, and ensure respect for the human rights and fundamental freedoms of individuals, in particular the right to privacy, to build trust in the implementation of the DDCC:TR.

The data protection principles are as follows.

1. LAWFUL BASIS, LEGITIMATE USE AND FAIR PROCESSING

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

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

Any retention of personal data processed in the interest of the application of the DDCC:TR should have a legitimate and fair basis. Before any data are retained, the potential risks, harms and benefits

[28] 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 15 Sept 2021)

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 carried out to be transparent to the data subjects. Data subjects should be provided with easily accessible, concise, comprehensible and reader-friendly information in clear and unambiguous language regarding: the purpose of the data processing; the type of data processed; how data will be retained, stored and shared, or made otherwise accessible; who will be the recipients of the data and how long the data will be retained. Information should also be provided to data subjects on applicable data retention schedules, and on how to exercise their data subject rights. A list of entities authorized to process personal data in the interest of the application of the DDCC: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 this data for any other purpose, including the sale and use of personal data for commercial purposes, should be prohibited, except with the explicit, unambiguous and freely given prior consent of the data subject.

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

Personal data processed in the interest of the application of the DDCC: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 on 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 their purpose. The amount of data, including their granularity, should be limited to the minimum necessary. Selective disclosure mechanisms should be used to support proportionate data access.

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

5. CONFIDENTIALITY AND SECURITY

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

With regard to the nature and sensitivity of the personal data processed in the interest of the application of the DDCC: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, applications, servers or networks, or if they are sent through services involved in collection, transmission, processing, retention or storage.

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

In case of a security breach leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or access to personal data transmitted, stored or otherwise processed, DDCC: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, correction, deletion, objection and restriction of personal data, subject to conditions regulated by national law, decree, regulation or other official act or order. Data subjects have the right to seek redress by a complaint procedure if they suffer harm or loss as a result of misused DDCC: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 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 valid proof of previous SARS-CoV-2 infection, within the window period recognized by relevant competent authorities, has the right to obtain and hold a DDCC:TR where it is a prerequisite for access to socio-economic 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.
4. Individuals should not be treated differently or given different levels of trust 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 paper card).
5. Any 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 valid 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 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 solution should be designed to augment and work within the context of existing health information systems, as appropriate.
10. Any 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 safe movement and access to socioeconomic activities, and privacy-protecting features should be built into the system and be respected accordingly
11. Anti-fraud mechanisms should be built into any approach.
12. Digital technology should not be the only mechanism available for verification. There should always be possible ways to revert to a paper-only manual verification of test result certificates. For example, a paper representation may be printed from the DDCC:TR and combined with an identity verification as outlined within the policy set by the public health authority.

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

3 TEST RESULT CERTIFICATE GENERATION

This section broadly describes the use cases and actors involved in generating a test result certificate. In the context of COVID-19, a DDCC:TR can be employed to generate 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 serve as pre-conditions for test result certificate generation. 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	→ Contains all relevant medical information → Encodes detailed information for use by authorized health professionals → Has no expiration date → Test report(s) in combination with clinical symptoms can aid diagnosis or evaluation of disease status → May not be verified by a third party	→ Requires information contained on a test report to generate a DDCC:TR → Provides a claim about the SARS-CoV-2 diagnostic test result of a tested person → Contains the minimum information necessary for verifying the validity of the claim → Has a time-bound validity period → Is digitally signed and can be verified in an offline or online manner
Possible Uses	→ For individual health purposes and clinical care → For early detection and containment measures (e.g. contact tracing, case reporting, surveillance, screening) → Depending on Member State policies, used to inform vaccination requirements	→ For individualized exemptions from public health and social measures (e.g. post exposure quarantine) → To facilitate safe and free movement and access to socioeconomic activities (e.g. national and/or international travel, participation in public gatherings)

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 pre-conditions 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 could be a lab 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 in ways supportive of the workflow's successful execution.

Table 3 Key personas for Certificate Generation

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

Table 4 Digital services for Certificate Generation

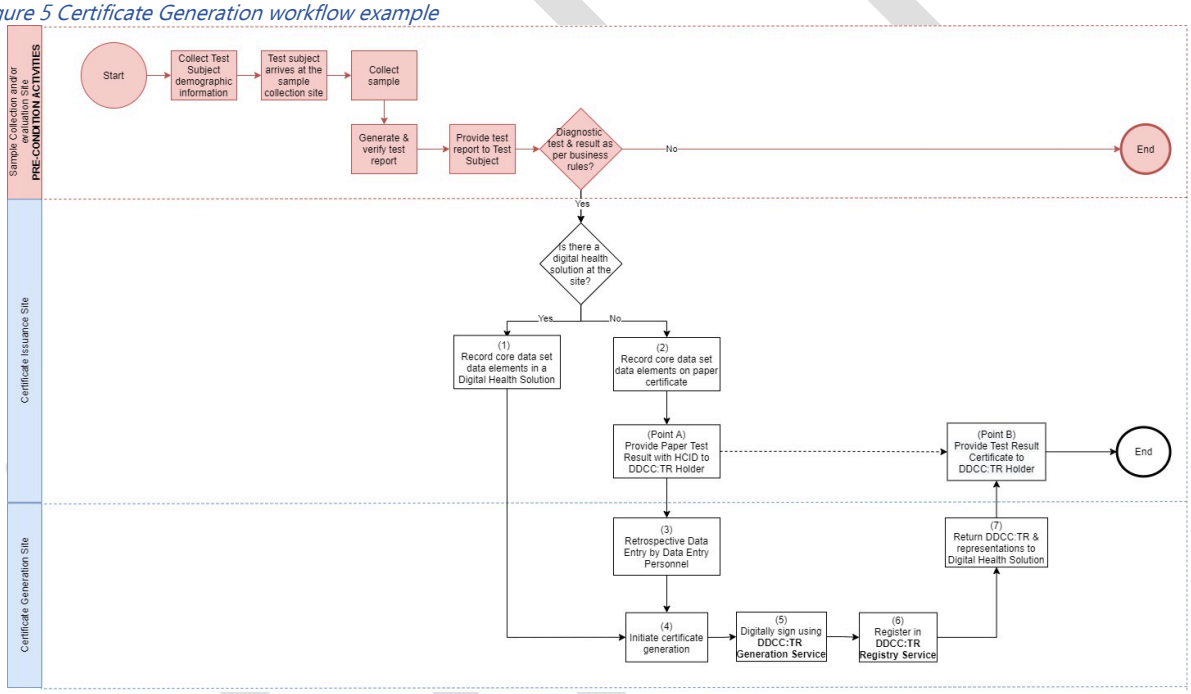
Digital service	Description
Digital Health Solution	A secure system that is used to record and/or manage a digital record of the DDCC:TR core data elements (e.g. Laboratory Information System, Laboratory Management Information System). The Digital Health Solution is responsible for distribution the DDCC:TR and any associated representations (such as a QR code) to the DDCC:TR Holder, based on the PHA policy.
DDCC:TR Generation Service	The service that is 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 this signed document in a location available to the DDCC:TR Registry Service and (optionally) persisting the signed HL7 FHIR document to the DDCC:TR Repository Service and potentially generates extra representations, such as QR code representations.
DDCC:TR Registry Service	The service that persists a record of the DDCC:TR certificate metadata and (optionally) the location of the DDCC:TR Repository Service endpoint, which can be leveraged for online verification.
DDCC:TR Repository Service	The DDCC:TR Repository Service is an optional digital service that has a repository, or database, of all the DDCC:TR. It 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.

3.2 Certificate Generation workflow

The process for Certificate Generation is summarized in Figure 5. It is assumed that for a certificate to be generated, the following activities have already taken place as per the norms and processes of the Member State:

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

Figure 5 Certificate Generation workflow example



The workflow's actors and settings may be described as follows:

1. The Certificate Issuance Site SHALL have a local Digital Health Solution. The Data Entry Personnel records 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, the test result certificate is intended to be captured initially in a paper format, data elements of the DDCC:TR core data set content SHALL be entered onto the paper test result certificate. The paper test result certificate SHALL have an HCID in a human readable format and a 1D or 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 certificate 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, retrospective data entry of DDCC:TR core data set content SHALL occur at the Certificate Generation Site.
4. The DDCC:TR core data set content is submitted to the DDCC:TR Generation Service and the certificate generation process is initiated.
5. The DDCC:TR Generation Service SHALL generate a digitally signed HL7 FHIR document using a private key.
6. The signed HL7 FHIR document SHALL be registered in the DDCC:TR 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:TR 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 existing Member State norms and practices, in a digital format at Point B.

If a Digital Health Solution does not exist at the Certificate Issuance Site, details of the test event SHALL be recorded and persisted in a paper test result record, according to the required DDCC:TR core data set. Details of the test event can then be electronically recorded into a Digital Health Solution available at Certificate Generation Site, by Data Entry Personnel and resulting test result certificate and/or its representations may be provided to the DDCC:TR Holder at Point B.

3.3 Functional requirements for Certificate Generation

To sign a digital document, PKI technology is required. Each Member State would be responsible for managing its own PKI through its PHA or another national delegated authority. PKI is described in further detail in Chapter 6 and Annex 4. 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. This PKI supports the sharing of public keys that correspond to the private keys that have been used to cryptographically sign DDCC:TR and may support the sharing of public keys from trusted international PHAs so that signed DDCC:TR representations issued by these parties may be cryptographically verified.

High-level functional requirements for the activities described in Fig. 5 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 are included in Annex 4.

1122 *Table 5 Functional requirements for the Certificate Generation*

Requirement ID	Functional requirement
DDCC.FXNREQ.001	It **SHALL** 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.
DDCC.FXNREQ.002	A PHA **SHALL** put in place a process to replace or reissue lost or damaged paper test result certificate with the necessary supporting technology.
DDCC.FXNREQ.003	It **SHALL** be possible to associate a globally unique HCID to a Tested Person under which test result certificates are registered.
DDCC.FXNREQ.004	It **SHALL** 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).
DDCC.FXNREQ.005	It **SHALL** be possible to manually record the core data set content on a paper test result certificate issued to the Tested Person (or the DDCC:TR card holder).
DDCC.FXNREQ.006	It **SHALL** 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.
DDCC.FXNREQ.007	It **SHALL** be possible to retrieve information about the lab test event of the Tested Person from the content in the DDCC:TR or one of its representations.
DDCC.FXNREQ.008	All data concerning the test result **SHALL** be handled in a secure manner to respect confidentiality of the Tested Person's health data.
DDCC.FXNREQ.009	Digital technology **SHALL NOT** be needed for any aspect of paper test result certificate issuance – the process **SHALL** function in an entirely offline and non-electronic manner.
DDCC.FXNREQ.010	Paper test result certificate and the validation markings they bear **SHALL** be designed to combat fraud and misuse.
DDCC.FXNREQ.011	If a Digital Health Solution to capture and manage SARS-CoV-2 diagnostic test result and related content is available, then it **MAY** be responsible for outputting the test data using the HL7 FHIR standard.
DDCC.FXNREQ.012	If a Digital Health Solution to capture and manage SARS-CoV-2 diagnostic test result and related content is 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 **SHALL** register the DDCC:TR through the DDCC:TR Registry Service.
DDCC.FXNREQ.013	If an online or connected public health DDCC:TR Generation Service is available at the time of recording SARS-CoV-2 test results, then it **SHALL** be possible to register the test report as soon as possible after the result is available.
DDCC.FXNREQ.014	The DDCC:TR Generation Service involved in the test result **SHALL** ensure encryption of data, in transit and at rest, to provide end-to-end security of personal data.
DDCC.FXNREQ.015	The DDCC:TR Generation Service **MAY** be the agent responsible for issuing the HCID, provided that the HCID can be associated at the time of test event in a timely manner. If the DDCC:TR Generation Service is responsible for issuing HCIDs, it **SHALL** only issue unique HCIDs. The same HCID should never be reused.
DDCC.FXNREQ.016	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, **SHALL** be managed by PHA policy.
DDCC.FXNREQ.017	It **SHALL** be possible for the DDCC:TR Generation Service to accept data transferred from an authorized, connected LIS where such a system exists.
DDCC.FXNREQ.018	It **SHALL** be possible for the DDCC:TR Generation Service to represent test result data using the HL7 FHIR format.
DDCC.FXNREQ.019	It **SHALL** be possible for the DDCC:TR Generation Service to digitally sign the HL7 FHIR document representation of the test result data
DDCC.FXNREQ.020	It **MAY** be possible for the DDCC:TR 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.

DDCC.FXNREQ.021	It **MAY** be possible for the DDCC:TR 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.
DDCC.FXNREQ.022	The DDCC:TR Generation Service **SHALL** 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.

1123

4 TEST RESULT CERTIFICATE VERIFICATION: PROOF OF NEGATIVE SARS-COV-2 TEST RESULT OR PROOF OF PREVIOUS SARS-COV-2 INFECTION

This section describes the use cases and actors involved in using a DDCC:TR for proof of negative SARS-CoV-2 test result or proof of previous SARS-CoV-2 infection, as well as functional requirements for a digital solution. Certificate verification relies on the PHA having access to a trusted means of digitally signing an HL7 FHIR document, which represents the core data set content for the DDCC:TR. It will be up to Member States to define the purposes for which this scenario is applied and adapted to their own contexts and levels of digital maturity, in compliance with their legal and policy frameworks.

4.1 Proof Scenarios

In the context of certificate verification, the DDCC:TR can be leveraged in one of two ways, as: (1) proof of a negative SARS-CoV-2 test result or (2) proof of previous SARS-CoV-2 infection. It will be up to the Member State to determine the business rules for acceptance of a test result certificate and the validity period for each proof scenario for domestic and/or international use cases.

Table 6 provides illustrative business rule structures to support each type of proof. These business rules will need to be established and clearly communicated by Member States based on their local policies and agreements made with other Member States. The Event Information Site (EIS) is maintained by the WHO Secretariat to be used by National IHR Focal Points. EIS contains timely information related to testing regime from different countries.

Table 6 Example of business rule decisions to support each type of proof scenario

Type of Proof	**Test Type***	**Test Result**	**Validity Period****
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

*The accepted types of SARS-CoV-2 diagnostic tests will need to be determined by the Member State for each proof scenario.

**The time periods to be defined by the Member State have been denoted in square brackets [*time period*].

Business rules for proof of previous SARS-CoV-2 infection will reflect each Member State's risk-based approach.[1,8] As the available science evolves, and as the application of risk-based approaches may evolve, it is expected that WHO's guidance related to these business rules would also evolve.

4.2 Key settings, personas and digital services

As with the DDCC:VS Proof of Vaccination, the DDCC:TR includes a verification site, where it is necessary for people to provide their SARS-CoV-2 diagnostic test result. This could include a variety of places (e.g. restaurants, airports, movie theatres); but how, when, where, and by whom the DDCC:TR can be verified should be defined and regularly updated by the Member State. The relevant policies, including data protection policies, should be put in place accordingly.

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

Table 7 Key personas for test result certificate verification

Role	Description
DDCC:TR Holder	DDCC:TR Holder is the person who wants to assert a claim related to a SARS-CoV-2 diagnostic test result. This person could be the same person as the Tested Person or, for example, could be a caregiver who may hold the DDCC:TR for a child or other dependant.
Verifier	The person or entity that wants to verify the diagnostic test result claim (i.e. verify 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 SARS-CoV-2 diagnostic test is performed and DDCC:TR is issued. The PHA is also responsible for the DDCC:TR Generation Service and the DDCC:TR Registry Service.

Table 8 Digital services for test result certificate verification

Digital service	Description
Health Certificate Identifier (HCID)	A unique identifier for DDCC:TR. The HCID may be provided by an existing national system or alternatively, it could also be issued directly by the DDCC:TR Generation Service which will then encode the ID in the DDCC:TR. It appears on paper test result certificate in both a human readable format and as a 1D or 2D barcode. It is part of the DDCC:TR core data set. An index that associates the HCID with metadata about the DDCC:TR is stored in the DDCC:TR Registry Service.
Verifier Application	A digital solution that can inspect and cryptographically verify the validity of the DDCC:TR. This can be an application on a mobile phone or otherwise, and it can operate online or offline.
DDCC:TR Registry Service	The service that persists a record of the DDCC:TR certificate metadata and (optionally) the location of the DDCC:TR Repository Service endpoint which can be leveraged for online verification.

	The DDCC:TR 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.
DDCC:TR Repository Service	The optional service that may be leveraged to look up DDCC:TR and/or return one or more representations of the DDCC:TR based on the DDCC:TR HCID. The DDCC:TR 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 certificate revocation lists) of all Document Signing Certificates (DSCs) that have been used to digitally sign DDCC:TR and 2D barcode representations of DDCC:TR artefacts. Verifier Applications that support offline verification will need to regularly refresh their local PKD cache from the PKD.

1170

1171

4.3 Test result certificate verification workflows and use cases

The process for Certificate Verification is summarized in Figure 6. 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, DDCC:TR, has been generated by the DDCC:TR Generation Service and registered within the DDCC:TR Registry Service. Optionally, DDCC:TR may be persisted to a DDCC:TR Repository Service.
2. The Verifier's application has, as part of a regular update procedure, downloaded and cached the public keys of all verifiable DDCC:TR 2D barcodes from a Public Key Directory (PKD) service as well as, optionally, a set of Certificate Revocation Lists (CRL) that denote public keys that have been revoked.
3. The DDCC:TR Holder is presenting a digitally signed DDCC:TR or its representation(s) that was signed by a DSC for which the Verifier's application has a cached copy of the relevant public key.
4. The Holder's 2D barcode is encoded using a method and format that is understandable by the Verifier's application and can navigate to the national PHA's trusted online verification service (for online verification).

The workflow's actors and settings, and its related high levels requirements, may be described as follows.

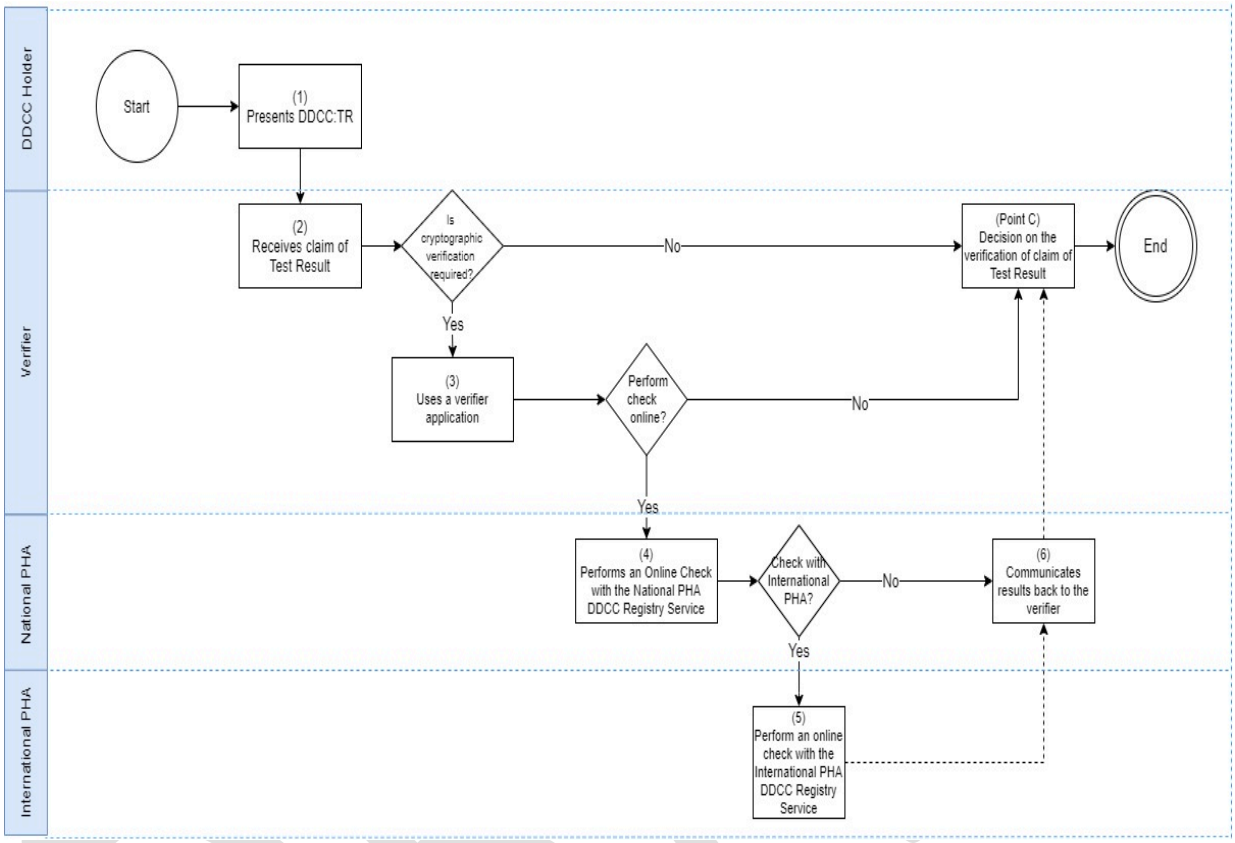
1. A DDCC:TR Holder presents a DDCC:TR to a Verifier in support of a claim of a SARS-CoV-2 diagnostic test result.

2. To verify the SARS-CoV-2 diagnostic test result claim of a verifiable DDCC:TR Holder, there are four separate pathways (Manual Verification, Offline Cryptographic Verification, Online Status Check [for national DDCC:TR], and Online Status Check [for international DDCC:TR]) that a Verifier could take to check the SARS-CoV-2 diagnostic test result claim at Point C, elaborated as test result certificate verification use cases in Table 9. A Verifier may visually verify a DDCC:TR, or scan a machine-readable version of the DDCC:TR's HCID and use that when accessing a verification service or verify using a digitally signed, machine readable representation of the core data set content (e.g. as a 2D barcode).

Note that, regardless of the use case, a DDCC:TR Generation Service is required as a precondition to support registration of DDCC:TR within the DDCC:TR Registry Service, which is required, as part of the Certificate Generation Workflow (see section 3.2).

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

Figure 6
Test Result Certificate Verification



DDCC:TR: Digital Documentation of COVID-19 Certificates: Test Result; PHA: public health authority.

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

4.3.1 Test result certificate verification use cases

Navigating through the workflow diagram shown in Figure 6, there are four possible verification pathways (illustrated separately in Fig. 7, Fig. 8, Fig. 9 and Fig. 10). These pathways are the use cases for test result certificate verification listed in Table 9. The required digital services for each use case are also outlined in Table 9.

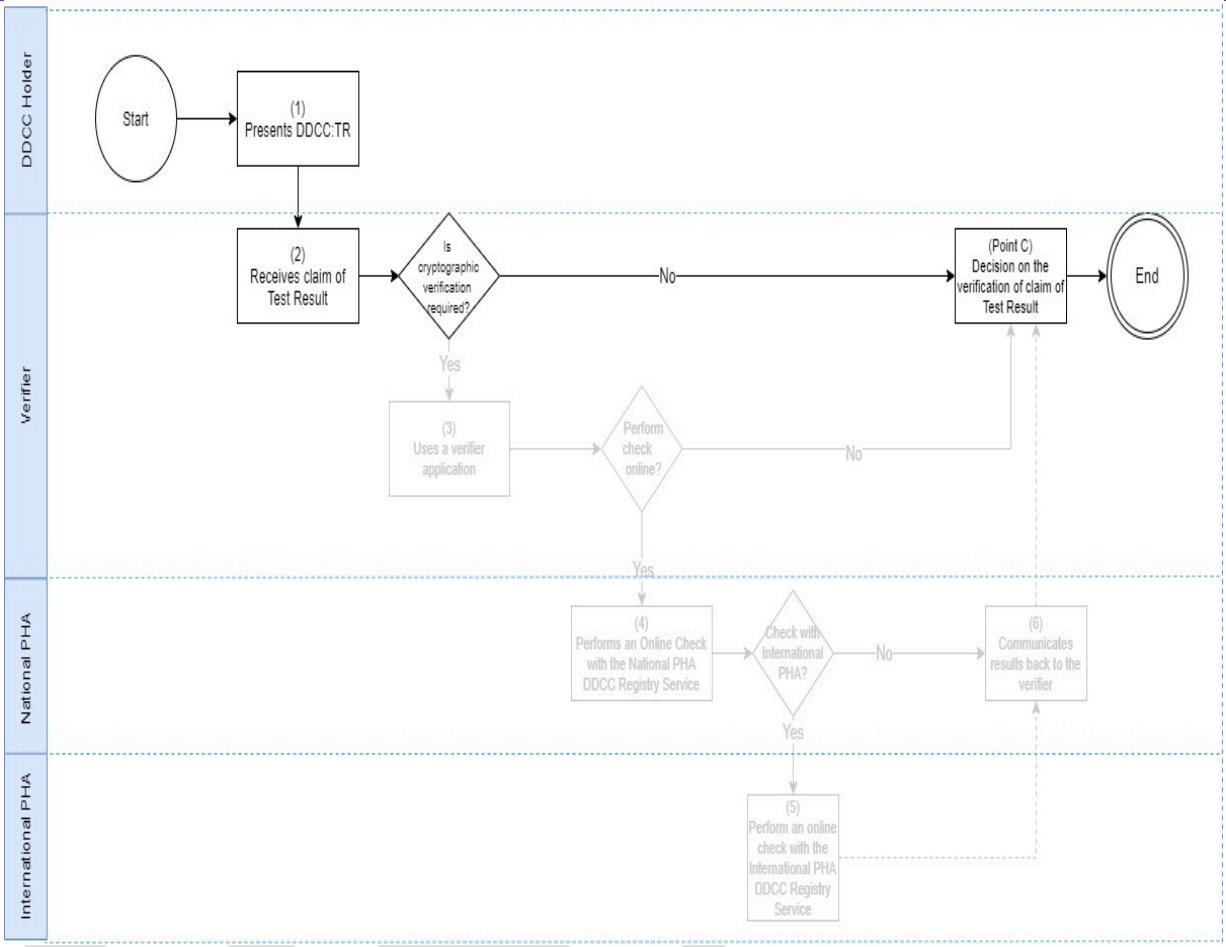
1220 *Table 9 Test result certificate verification use cases*

Use case ID	UC001	UC002	UC003	UC004
Use case name	**Manual Verification**	**Offline Cryptographic Verification**	**Online Status Check (National DDCC:TR)**	**Online Status Check (International DDCC:TR)**
Figure	Figure 7	Figure 8	Figure 9	Figure 10
Use case description	A Verifier verifies a DDCC:TR based on its human-readable content using purely visual means, based on their subjective judgement. This type of check is common, currently well accepted, is quick and easy to do, and requires no digital technology.	A Verifier verifies a DDCC:TR using digital cryptographic processes in an offline mode	This pathway is used when the DDCC:TR is being verified in the same jurisdiction as it was issued. A Verifier verifies a DDCC:TR using digital cryptographic processes in an online mode that includes a status check against the PHA's DDCC:TR Registry Service and optionally the DDCC:TR Repository.	This pathway is used when the DDCC:TR is being verified in a foreign jurisdiction to where it was issued. A Verifier verifies an internationally issued DDCC:TR using digital cryptographic processes in an online mode that includes a status check against the National PHA's DDCC:TR Registry Service, which in turn accesses an International PHA's DDCC:TR Registry and DDCC:TR Repository, 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 to protect against discrimination and detect fraud.	• Can confirm that the HCID barcode on the printed test result is valid and has not been altered. • Can confirm whether the DDCC:TR has been issued by an authorized PHA. • Can confirm that the hash of any signed 2D barcodes matches the health content represented therein.	• Can confirm that the HCID barcode on the paper card is valid and has not been altered. • Can confirm whether the DDCC:TR has been issued by an authorized PHA. • If authorized to do so, can confirm that the content on a DDCC:TR paper card matches the DDCC:TR digital content. • Can confirm that the hash of any signed 2D barcodes matches the health content represented therein. • Can check whether signed 2D barcodes containing DDCC:TR content have been revoked or updated.	• Can confirm that the HCID barcode on the paper card is valid and has not been altered. • Can confirm whether the DDCC:TR has been issued by an authorized PHA. • If authorized to do so, can confirm that the content on a DDCC:TR paper card matches the DDCC:TR digital content. • Can confirm that the hash of any signed 2D barcodes matches the health content represented therein. • Can check whether signed 2D barcodes containing DDCC:TR content have been revoked or updated.

Verify whether the DDCC:TR has been revoked?	Not possible	Possible if a cache of revoked certificates is maintained by the Verifier	Possible	Possible
DDCC:TR Registry Service	Not required	Required	Required	Required
DDCC:TR Repository Service	Not required	Optional	Required	Required

DDCC:TR, Digital Documentation of COVID-19 Certificates: Test Result; HCID, health certificate identifier; ID, identifier; PHA, public health authority.

Figure 7
Test Result Certificate Verification: Manual Verification Use Case

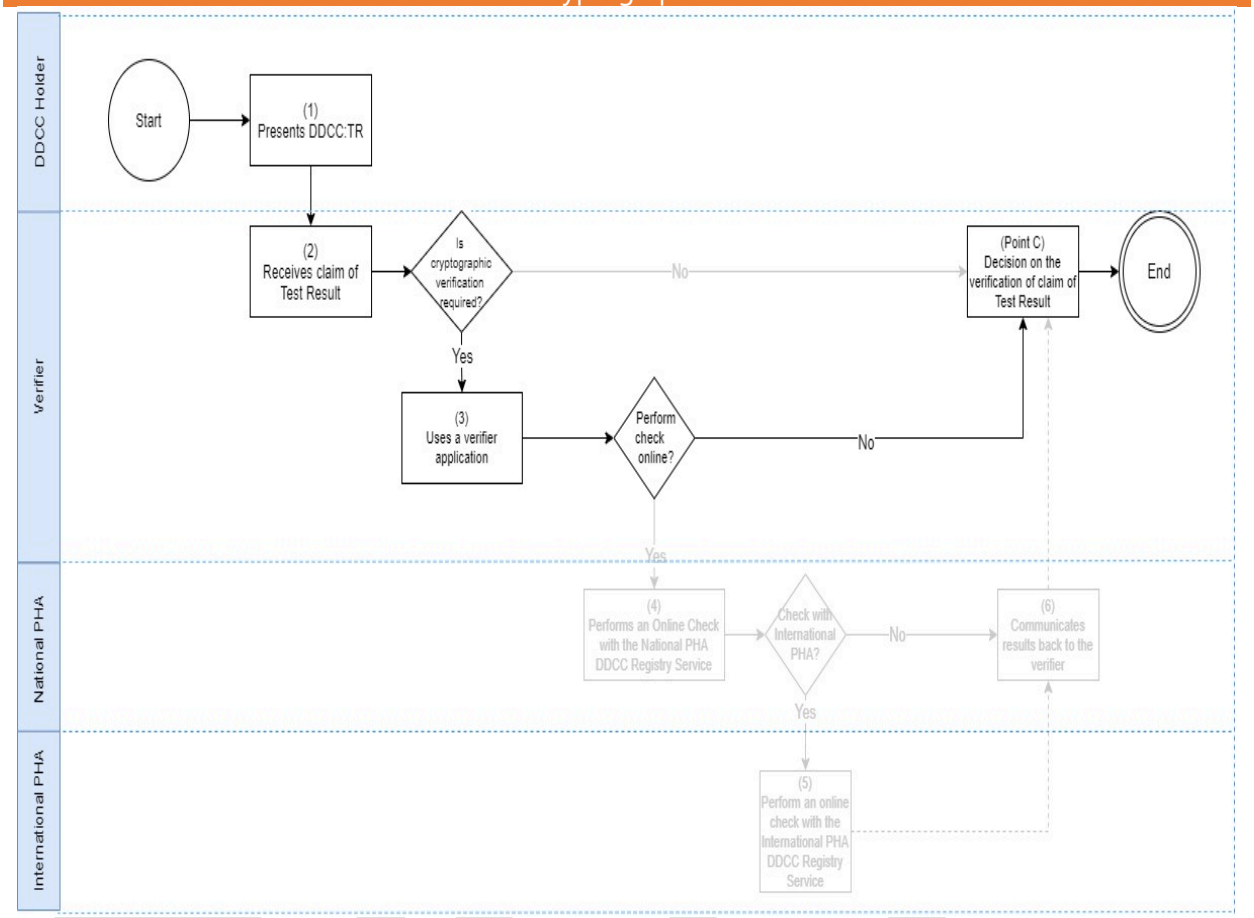


DDCC:TR: Digital Documentation of COVID-19 Certificates: Test Result; PHA: public health authority.

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

1225

Figure 8
Test Result Certificate Verification: Offline Cryptographic Verification Use Case

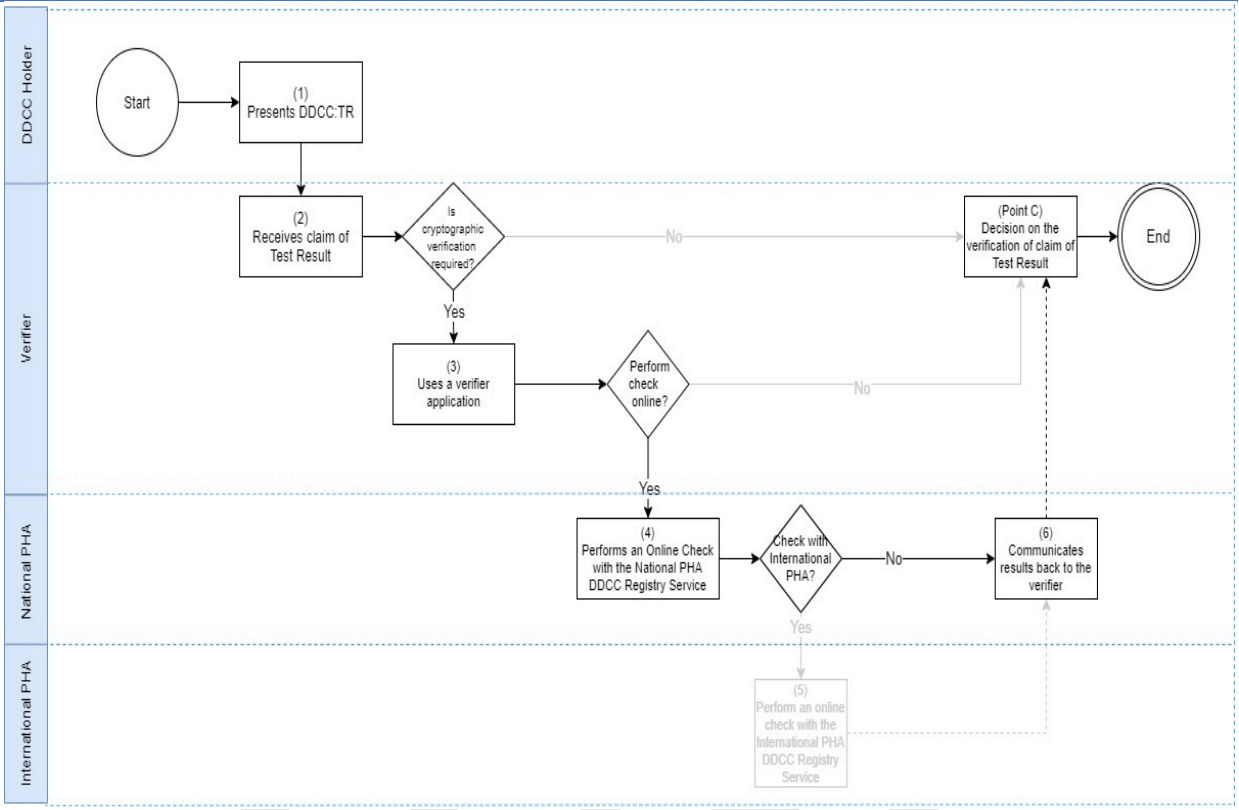


DDCC:TR: Digital Documentation of COVID-19 Certificates: Test Result; PHA: public health authority.

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

1226

Figure 9
Test Result Certificate Verification: Online Status Check (National DDCC:TR) Use Case

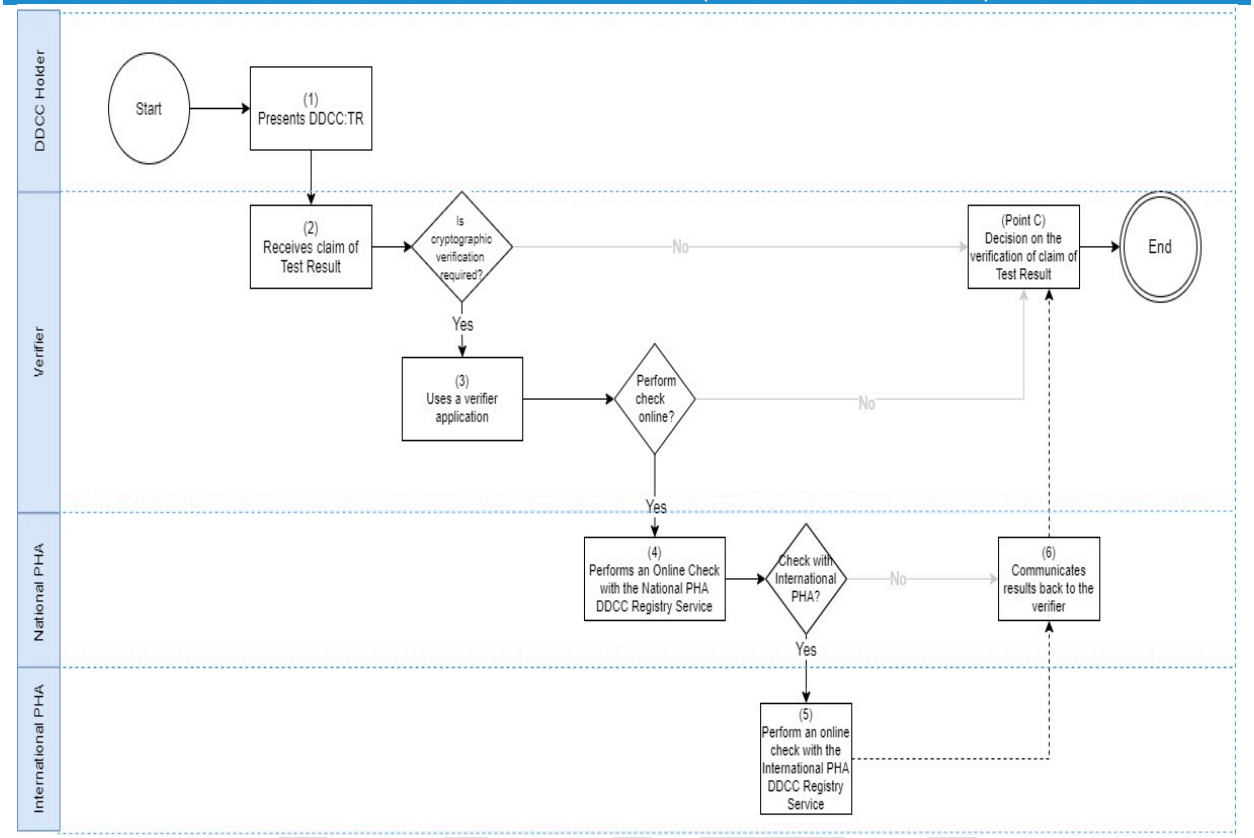


DDCC:TR: Digital Documentation of COVID-19 Certificates: Test Result; PHA: public health authority.

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

1227

Figure 10
Test Result Certificate Verification: Online Status Check (International DDCC:TR) Use Case



DDCC:TR: Digital Documentation of COVID-19 Certificates: Test Result; PHA: public health authority.

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

1228

4.3.2 Operationalizing the test result certificate verification use cases

The HL7 FHIR implementation guide includes implementable specifications for the test result certificate verification use cases described in this document, (available at WorldHealthOrganization.github.io/ddcc [Note: The HL7 FHIR implementation guide has yet to be updated to reflect additional DDCC:TR content.]). The HL7 FHIR implementation guide for DDCC:TR will contain a standards-compliant specification that explicitly encodes computer-interoperable logic, including data models, terminologies, and logic expressions, in a computable language sufficient for implementation of test result certificate verification use cases.

4.4 Functional requirements for test result certificate verification

High-level functional requirements for the activities described in Fig. 6 are presented in Table 10 as suggested features that any digital solutions that would facilitate DDCC:TR verification may have. These are written as guidance requirements only to be used as a starting point for Member States or other interested parties that need to develop their own specifications for a digital solution for DDCC:TR to take and adapt.

Non-functional requirements are included in Annex 4.

Table 10 Test Result Certificate Verification Functional Requirements

Requirement ID	Functional requirement	UC001 Manual	UC002 Offline	UC003 Online
DDCC.FXNREQ.023	Paper test result certificate and the validation markings they bear **SHOULD** be designed to combat fraud and misuse. Any process that generates paper test result certificate **SHOULD** include elements on the card that support the Verifier in visually checking that the card is genuine (e.g. water marks, holographic seals etc.) without the use of any digital technology.	x	x	x
DDCC.FXNREQ.024	If a paper test result document bearing a 1D or 2D barcode is presented to a Verifier, then it **SHALL** be possible for the Verifier to scan the code and, as a minimum, read the HCID encoded in the barcode, to visually compare it with the HCID written on the paper test result certificate, if present.		x	x
DDCC.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 **MAY** be possible for the Verifier to check the signature, using information downloaded from a PKD, to ensure it is genuine.			x
DDCC.FXNREQ.026	It **MAY** be possible to log all offline verification operations so that, at a later stage when an online connection is available, verification decisions can be reviewed and reconfirmed against data provided by the online DDCC:TR 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:TR Registry Service the day before has not been added to a public key revocation list issued that same day. However, personal data accessed at the point of verification of the DDCC:TR should not be retained and stored in a repository, database or otherwise.		x	
DDCC.FXNREQ.027	It **SHALL** always be possible to perform some form of offline verification of paper test result certificate; any solution should be designed so that a loss of connectivity to online components of the solution cannot force the verification work to stop.		x	x

DDCC.FXNREQ.028	If, at the time of verification, a Verifier has connectivity to a DDCC:TR Registry Service managed by a PHA, then it **SHALL** be possible to query whether the HCID present in the barcode (and the public key, if also present) of the paper test result certificate are currently valid.			x
DDCC.FXNREQ.029	When making the verification check, any solution **SHALL** send only the minimum information required for the verification to complete. The minimum information comprises the metadata (see section 5.2) and signature of the DDCC:TR.			x
DDCC.FXNREQ.030	When receiving a request for validation, a PHA **SHALL** consult its DDCC:TR 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.			x
DDCC.FXNREQ.031	A PHA servicing a validation request of a test result certificate via an HCID **MAY** respond with basic details of the test result certificate holder (name, date of birth, sex, etc.), in accordance with PHA policies, so that the Verifier can confirm that the paper test result certificate corresponds to the DDCC:TR Holder who has presented himself or herself for validation.			x
DDCC.FXNREQ.032	A PHA **SHALL** maintain a PKI to underpin the signing and verification process. Lists of valid public keys and revocation lists will be held in such a system and MAY be linked to the DDCC:TR Generation Service to associate public keys with HCIDs.			x
DDCC.FXNREQ.033	A PHA **MAY** log the requests it receives for verification (even if rendered anonymous), so that it has a searchable history for the purposes of audit and fighting fraud, provided that such logging respects data protection principles.			x
DDCC.FXNREQ.034	A PHA **SHALL** be able to return a verification status, as defined by the implementer, to a requestor, based on the information provided.			x
DDCC.FXNREQ.035	A PHA **MAY** 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).			x
DDCC.FXNREQ.036	When receiving a request for validation, a PHA **MAY** respond with the last test result certificate or provide history of test result certificates, in accordance with Member State policies.			x
DDCC.FXNREQ.037	A PHA **SHOULD** be able to validate that the requestor making a verification request is an authorized agent, but **MAY** also allow anonymous verification requests.			x
DDCC.FXNREQ.038	The certificate authority (or authorities) in each country **SHALL** 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.			x
DDCC.FXNREQ.039	Any communication between a Verifier and a DDCC:TR Registry Service or other data service managed by a PHA **SHALL** be secured to prevent interference with the data in transit and at rest.			x
DDCC.FXNREQ.040	SMS-based verification of alphanumeric HCIDs **MAY** be provided by a PHA as a means of sending a verification request or receiving a response with a status code.			x

1247

1248

5 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 are required to support proof of negative SARS-CoV-2 test result or proof of previous SARS-CoV-2 infection. Stakeholders and systems may use the DDCC:TR core data set as defined or they 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 the scenarios of use defined and driven by the public health need. A comprehensive data dictionary in spreadsheet format can be found in Web Annex A.

5.1 Core data set principles

To develop the core data set, existing digital certificates, and guidelines such as International Civil Aviation Organization (ICAO) guidelines on visible digital seals ("VDS-NC") for travel-related health proofs, the European Union (EU) EU Digital COVID Certificate International Civil Aviation Organization (ICAO), US-based Vaccine Certificate Initiative (VCI) specification, the ISO mdoc specification, and the ASEAN lab result are 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 elements must have a purpose in accordance with the predefined use cases. This is especially important for personal data.
- Open Standards: Aligned with the principle of open access, proprietary terminology code systems or proprietary standards cannot be recommended to Member States
- Implementable on Digital and Paper: Aligned with the principle of equity, data requirements should not increase inequities or put individuals at risk. Additionally, data input requirements should be feasible on paper but take advantage of the benefits of digital technology.
- To underscore the importance of the ability to implement, the data content model for the DDCC:TR core data set has been developed as an HL7 FHIR implementation guide. The DDCC test result implementation guide is based on the widely adopted HL7 FHIR International Patient Summary (IPS) health data content model.[29]

Logical Observation Identifiers Names and Codes (LOINC) and International Classification of Diseases (ICD) are the preferred data standards for DDCC:TR. To support broadly deployed legacy systems, the DDCC:TR normative core data set includes 1:1 equivalent mappings to SNOMED codes that may be leveraged, in some cases, as allowed alternatives.

[29] International Patient Summary Implementation Guide: 1.0.0 – Continuous Integration Build [website]. Health Level Seven International – Patient Care Work Group; 2021 (https://build.fhir.org/ig/HL7/fhir-ips, accessed 27 June 2021).

LOINC is identified as a universal code system for laboratory tests, health measurements and observations.[30] LOINC:

- is a rich catalogue of measurements, including laboratory tests, clinical measures and anthropometric measures;
- enables the exchange and aggregation of clinical results for care delivery, outcomes management and research by providing a set of universal codes and structured names;
- enables comparability and analysis of consolidated laboratory result data;
- accelerates secondary use of clinical results for other purposes such as public health reporting, quality measurements and other types of analyses.

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

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

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

[30] https://loinc.org/

[31] ICD-11: International Classification of Diseases 11th Revision. In: World Health Organization International Classification of Diseases [website]. Geneva: World Health Organization; 2021 (https://icd.who.int/en, accessed 27 June 2021).

[32] Global Patient Set. In: SNOMED International [website]. London: SNOMED International; 2021 (https://www.snomed.org/snomed-international/learn-more/global-patient-set, accessed 27 June 2021).

5.2 Core data elements

The three key sections of the core data set are:

1. The header
2. Data elements for the lab test result
3. Test result certificate metadata

The **header section** data elements include the Tested Person's ID information. The header section is intended to capture information about the tested individual to allow for information on the test result certificate 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 Test Result	Requirement status for Proof of Previous SARS-CoV-2 Infection
Name	The full name of the tested person	String	Not applicable	Required	Required
Date of Birth	The tested person's date of birth (DOB) if known. If unknown, use assigned DOB for administrative purposes.	Date	Complete date, following ISO 8601 (YYYYMMDD or YYYY-MM-DD)	Required	Required
Unique Identifier	Unique identifier for the tested person, according to the policies applicable to each country. There can be more than one unique identifier used to link records (e.g. national ID, health ID, medical record ID).	ID	Not applicable	Optional	Optional

ISO: International Organization for Standardization, ID: identifier

The **data elements for each SARS-CoV-2 test event** section outlines the data that need to have been collected for each SARS-CoV-2 test event.

1330 *Table 12 Data 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 Test Result	Requirement status for Proof of Previous SARS-CoV-2 Infection
Agent targeted	Name of the agent being tested for (such as SARS-CoV-2).	Coding[1]	ICD-11	Required	Required
Type of test	Name of the type of test that was conducted e.g. NAAT.	Coding	LOINC	Required	Required
Test brand	The brand or trade name used to refer to the test conducted.	Coding	As defined by Member State	Optional	Optional
Test manufacturer	Name of the manufacturer of the test conducted.	Coding	As defined by Member State	Optional	Optional
Specimen Sample Origin	The type of sample that was taken e.g. Nasopharyngeal swab or Saliva specimen.	Coding	ICD-11	Optional	Optional
Date and time of sample collection	Date and time when sample was collected.	DateTime	Time zone designator following ISO 8601 (YYYY-MM-DDThh:mm+/-HH:MM) e.g. 2021-11-01T12:30-2:00	Required	Required
Date and time of report issuance	Date and time when the test report was generated.	DateTime	Time zone designator following ISO 8601 (YYYY-MM-DDThh:mm+/-HH:MM) e.g. 2021-11-01T12:30-2:00	Optional	Optional
Test result	Detected or Not detected presence of SARS-CoV-2 infection	Coding	ICD-11	Required	Required
Test centre or facility name	A codable name or identifier of the facility responsible for conducting the test	Coding	As defined by Member State	Optional	Optional

Test centre country	The country in which the individual has been tested	Coding	ISO 3166-1 alpha-3 (or numeric)	Required	Required

ICD-11: International Classification of Diseases 11th Revision; ID: identifier; ISO: International Organization for Standardization, LOINC: Logical Observation Identifiers Names and Codes

1 Coding data elements 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)

The **test result certificate metadata** contains 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 of certificate generation to support specific use case implementations.

Table 13 Test Result certificate metadata

Data element label	Description	Data type	Preferred code system	Requirement status for Proof of Negative Test Result	Requirement status for Proof of Previous SARS-CoV-2 Infection
Certificate issuer	The authority or authorized organization that issued the test result certificate.	String	Not applicable	Required	Required
Health Certificate Identifier (HCID)	Unique identifier used to associate the test results represented in paper test result certificates to their digital representation(s).	ID	Not applicable	Required	Required
Certificate schema version	Version of the core data set and HL7 FHIR Implementation Guide that the certificate is using.	String	Not applicable	Required	Required
Certificate valid from	Date and time at which the test result certificate became valid. No health or clinical inferences should be made from this date	DateTime	Time zone designator following ISO 8601 (YYYY-MM-DDThh:mm+/-HH:MM) e.g. 2021-11-01T12:30-2:00	Optional	Optional

ID: identifier; UTC: Coordinated Universal Time, ISO: International Organization for Standardization

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 scenarios or have two separate data sets (as mentioned above). The proposed specification is intended to provide a basis for generating interoperable certificates that can serve the purposes of identifying persons who have a proof of previous SARS-CoV-2 infection or who have recently tested negative for SARS-CoV-2 infection.

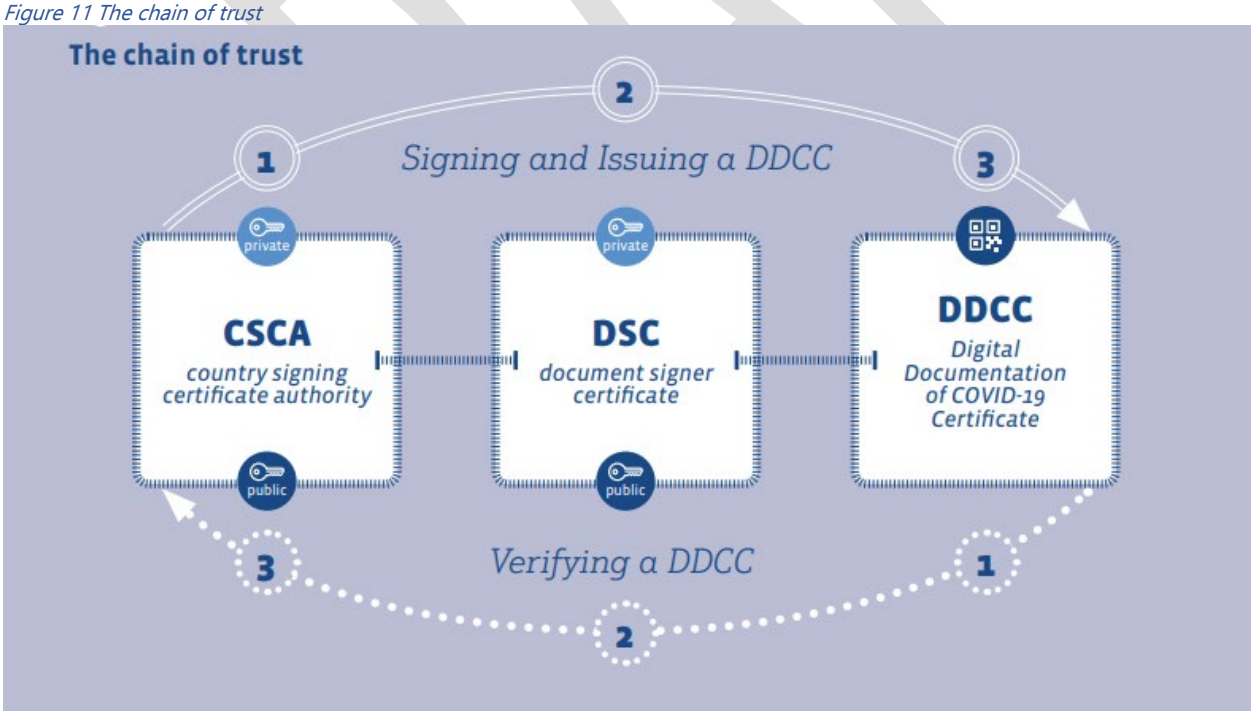
6 PKI FOR SIGNING AND VERIFYING A DDCC:TR

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

In Annex 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 and tailored to suit the specific real-world needs of each Member State.

To sign a digital document, PKI technology is required. PKI uses private and public key pairs to operationalize digital signing and cryptographic verification. Content that is signed by a private key can be verified by the corresponding public key of the key pair. This sign–verify mechanism is leveraged to establish the trust framework (chain of trust; see Fig. 11). There are many different mechanisms/technologies to implement this approach. PKI is described in further detail in Annex 3.

Figure 11 The chain of trust



CA, certificate authority; DDCC, Digital Documentation of COVID-19 Certificate; DSC, document signer certificate.

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

1. The PHA will need to generate at least one document signer certificate (DSC) – a private–public key pair that can be used by the trusted agents of the PHA to sign the DDCC: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.

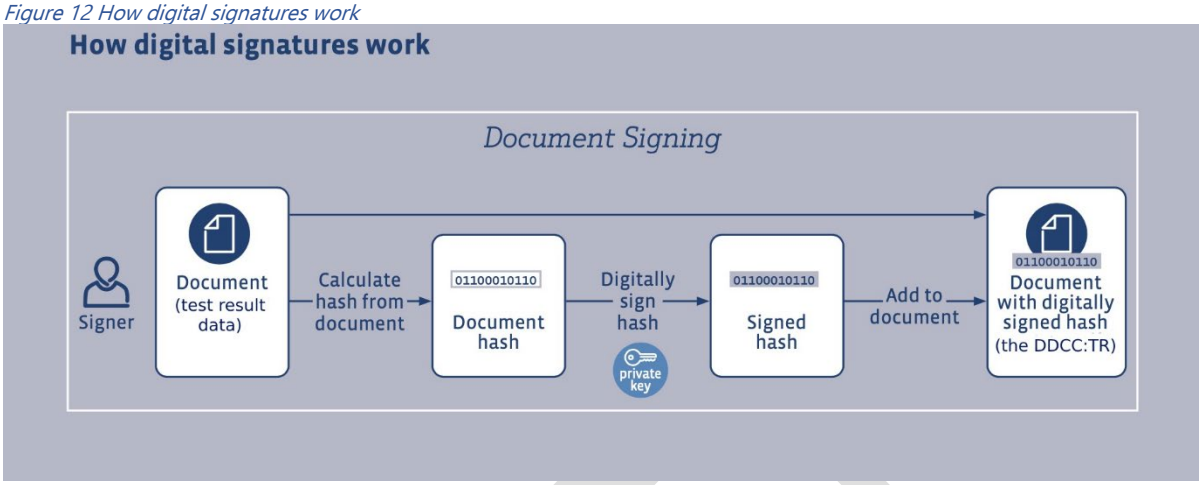
There are many ways in which a PKI can be implemented. An example implementation of digital signing is provided in the implementation guide available at https://github.com/WorldHealthOrganization/ddcc. The precise algorithms used for the implementation – for example for hashing and for signature generation – are at the discretion of the Member State.

6.1 Signing a DDCC:TR

The process of signing a DDCC:TR is shown in the top row of Figure 11 and involves three steps.

1. The PHA generates a private and public key pair that serve as the "root certificate". The private key is kept highly secure (never revealed to another party, maintained in a disconnected location, stored on media that is itself password-protected, etc.); the public key will be widely disseminated.
2. The PHA generates one or more DSC key pairs. DSC private keys are kept highly secure, and public keys are widely disseminated. The DSC key pair is digitally signed by the root certificate's private key.
3. A DDCC:TR is digitally signed using the DSC's private key. A 2D-barcode representation (e.g. QR code) of the signed content can be generated if required. The process of signing is illustrated in Figure 12 and works 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 12 How digital signatures work

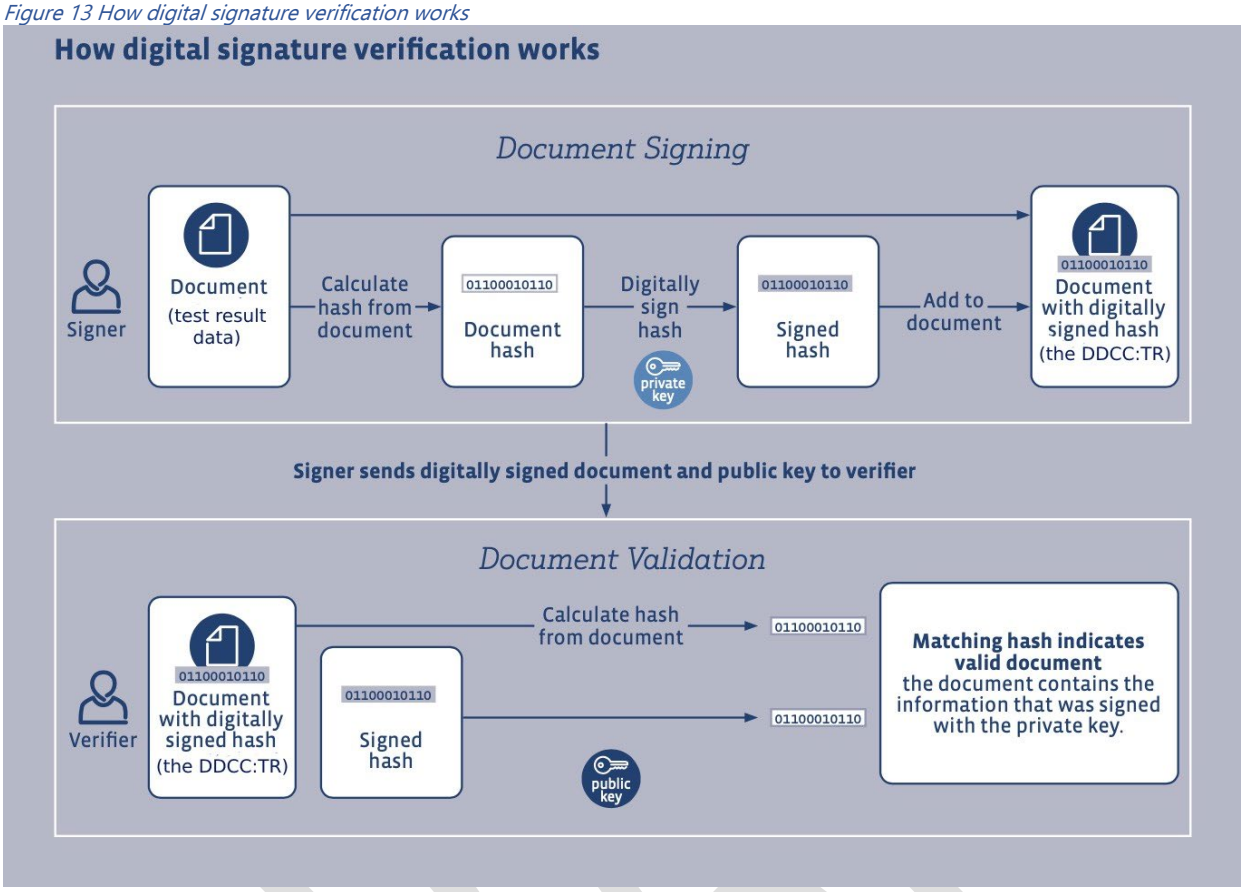


6.2 Verifying a DDCC:TR signature

The verification process, shown in in the bottom row of Fig. 11 and further detailed in Figure 13, 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.
3. The document signer's public key is used to cryptographically transform the signed hash back to the document hash. The Verifier can compare the document hash from step 2 to its own calculated hash from step 1. If they match, the Verifier is confident that:
    a. only someone with access to the DSC's private key could have signed the document, because the public key was able to decrypt the document hash; and
    b. the data that was signed is the same as the data read from the DDCC:TR, because the calculated hash matches the document hash.
4. The PHA's root certificate public key is used to cryptographically verify that the document signer's signature was issued under the responsibility of the PHA.

Figure 13 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 extremely hard to reverse. They provide a high level of security provided the private key is not compromised and remains available only to the entity performing the signing. Operationally, private keys are kept highly secure and public keys are broadly shared. Provided that a private key is not compromised and unintentionally revealed to another party, content that is "signed" by (i.e. encoded with) a private key may be readily verified by (i.e. decrypted by) anyone who has the corresponding public key. Anyone using the public key associated with the private key can be confident that:

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

PKI is the mechanism whereby the public key is circulated to all that 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.

7 NATIONAL GOVERNANCE CONSIDERATIONS

Governance in the health sector is "a wide range of steering and rule-making related functions carried out by governments/decisions makers as they seek to achieve national health policy objectives that are conducive to universal health coverage".[33] A national framework to govern the complex and dynamic health policy for implementing DDCC:TR 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 to determine the most appropriate governance mechanisms for its context.

Fundamentally, trust in the system should derive from the security-by-design of a PKI and the governance rules put in place by the Member State to operate it. The test result certificate verification requires governance to be established at two levels: (1) the PHA, and (2) the Member State. At PHA level, at least one DSC needs to be utilized to sign the DDCC: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. There two recommended approaches are:

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 which 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.[34]

2. **Master list**: The Member State establishes a mechanism to manage and distribute, as appropriate, a master list of DSCs that have been authorized for PHAs to use to sign DDCC:TR.

Member States can leverage an existing PKI or create a new one specifically for DDCC:TR. 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.

---

[33] Health system governance. In: World Health Organization/Health topics [website]. Geneva: World Health Organization; no date (https://www.who.int/health-topics/health-systems-governance#tab=tab_1, accessed 27 June 2021).

[34] Adams C, Farrell S, Kause T, Mononen T. Internet X.509 Public Key Infrastructure Certificate Management Protocol (CMP), section 3.1.1.2 Certification Authority. Reston (VA) and Geneva: The Internet Society Network Working Group; 2005 (https://datatracker.ietf.org/doc/html/rfc4210#section-3.1.1.2, accessed 27 June 2021).

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

- **Issuing DDCC:TR**: There should be clear and transparent processes in place for issuing 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 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 generation and issuance of DDCC:TR.[35,36]
- **Verifying DDCC:TR**: Member States need to define the requirements for what it means to have a "valid" DDCC:TR. Furthermore, Member States will need to decide whether the DDCC:TR can be verified by anyone with the means to verify a DDCC:TR; alternatively, they may decide on a list of trusted Verifiers, in which case only trusted Verifiers would be able to verify a DDCC:TR. The appropriate privacy mechanisms should be built into the implementation based on this decision.
- **Revocation of DDCC:TR**: There should be clear and transparent processes for revocation of a DDCC:TR in case fraud has occurred, incorrect information needs to be rectified, or issues have been discovered at a lab and test results need to be recalled. These revocation processes should also include standard operating procedures for:
    - **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 DDCC:TR have been revoked in order to be able to continuously trust that DDCC:TR issued by a specific entity are still valid. For example, if there are reports of counterfeit DDCC:TR, Verifiers should be informed about the possibility of encountering 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 of a new 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 DDCC:TR issued by their PHAs. Personal

[35] Laboratory assessment tool for laboratories implementing SARS-CoV-2 testing (https://www.who.int/publications/i/item/laboratory-assessment-tool-for-laboratories-implementing-covid-19-virus-testing)

[36] Assessment tool for laboratories implementing SARS-CoV-2 testing: Interim Guidance: User Guide. (https://www.who.int/publications/i/item/assessment-tool-for-laboratories-implementing-covid-19-virus-testing, accessed 22 October 2021).

data about individuals with DDCC:TR from other countries need to be processed according to a set of principles and processes agreed upon by Member States, to establish trust between Member States.

8 IMPLEMENTATION CONSIDERATIONS

Since COVID-19 was declared a Public Health Emergency of International Concern under the IHR in January 2020, there has been a clear and urgent need for all Member States to effectively address the COVID-19 pandemic. In the digital age, there has also been immediate acknowledgement that digital health solutions can effectively and immediately be leveraged to support the public health response to the pandemic. 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*[37] and the guidance provided in the *Digital implementation investment guide (DIIG)*[38], 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 DDCC:TR.
- 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 additional value added beyond using the paper system only?

Infrastructure

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

[37] National eHealth Strategy Toolkit: overview. Geneva: World Health Organization and International Telecommunication Union; 2012 (https://www.who.int/ehealth/publications/overview.pdf, accessed 28 June 2021).

[38] Digital implementation investment guide (DIIG): integrating digital interventions into health programmes. Geneva: World Health Organization; 15 September 2020 (https://www.who.int/publications/i/item/9789240010567, accessed 28 June 2021).

- Where sample collection is done at a site different from the lab, supply chain challenges will need to be addressed regarding the transport of specimens from the point of collection to the lab and regarding the issuing of paper documents to DDCC:TR holders.

Legislation, Policy and compliance

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

Leadership and governance

- Is there an existing department within the ministry of health that will be accountable for this work? There needs to be a clear accountable entity, whether it is a single department or a formalized cross-cutting group or committee, that is responsible for operationalizing DDCC:TR.
- Is there a clear governance mechanism and are standard operating procedures in place to support the use and maintenance of the DDCC:TR?
- What agency will be responsible for independent oversight for use of the DDCC:TR, 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 there need to be agreements established bilaterally, multilaterally or at a regional level to establish trusted recognition between DDCC:TR of different provenance? Are bilateral or regional agreements in place that can be leveraged?

Workforce

- Is the value added by the digital representation clearly communicated? Personnel may face the additional burden of operating a dual system of paper-based and digital solutions.
- Are change management processes and support in place when implementing a DDCC:TR?
- 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 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 update of health workers, health facility managers, and public health officials take place to ensure continued relevance of the DDCC:TR?

Services and applications

- Do point-of-service applications exist that are used for other workflows not related to test, but which could be leveraged to collect the DDCC:TR core data set and associate these data with an HCID? Examples may include existing LIS or HMIS solutions that can be readily extended to support new workflows.
- Are there existing products in the marketplace that would fit your needs and adhere to international specifications and guidance?
- Are there different types of software models, including: custom-developed software, commercial off-the-shelf (COTS) software, free packaged software, open-source software, and software as a service (SaaS)? The benefits and risks of these different software models should be considered.
- If deciding to use open-source products, is there a responsive established user community that will provide support and help add features at no cost?
- Which services and applications would be the most environmentally sustainable?

Standards and interoperability

- Is there an existing interoperability framework to guide how a DDCC:TR 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 OpenHIE framework is given in Annex 6.

Health content

- What is the process to account for the constantly changing context of COVID-19? As the evidence base increases and relevant clinical and/or public health guidelines are updated, there may be new health content requirements. Implementation of the DDCC:TR should change in accordance with the changing health context and remain evidence based.
- If the lab is to be generating the DDCC:TR, core data set elements captured at the time of the sample collection will need to be conveyed to the lab along with the specimen using either an electronic or paper-based means.

8.2 Key factors to consider with solution developers

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

- The terms of reference for the work that needs to be performed should be clearly expressed and at a level of detail that allows solution developers to respond with a high degree of confidence in their bids.
- An early decision is needed as to whether work will be performed under a fixed price or a time-and-materials arrangement (or a mixture of the two in which, for example, a core product is delivered but additional work paid on a pro-rata basis).
- The timeline for work should be realistically set. The realization of a digital solution is a technology project, and projects are subject to the triple constraints of scope, cost and time, with the quality of the work affected by all three. The engaging authority should have a realistic understanding of the likely effort of the project and the effects on scope and cost if the timeline is set to be too short. A phased approach to deliver a minimum viable product first and iterate further enhancements is often recommended.
- A decision is needed as to whether a single supplier (with sub-contractors) or a consortium of suppliers is permitted. Working with a consortium brings the advantage that multiple best-in-class vendors can collaborate, but also involves the complication of extra communication and coordination between these actors.
- The metrics for success of the work should be defined early so that the goals and outcomes of the project are clear to all involved. Ideally, these metrics should be measurable key performance indicators (speed of operation, compliance with regulations, etc.). Contracts (and payment schedules) can be tied to performance indicators to incentivize vendors and keep the focus clearly on the desired outcome.
- Suppliers should demonstrate solid expertise in the area of work for which they are being engaged; they should have a portfolio of previous experience and be able to provide references. A demonstration of relevant previous work can be requested to gain confidence in the vendor's expertise.
- Suppliers should also demonstrate a solid track record of project management for delivering digital solutions. This will include establishing a clear communication plan so that the regularity of and format for reporting on project progress is understood and the procedure for escalation of problems is agreed.
- The working hours, location and corporate culture (including working language) of any supplier should be considered to ensure that teams will work together well and that the risk of miscommunication is reduced.
- As noted at the start of the chapter, if the strategy is to build a digital solution as part of a longer-term investment in public health technology that will outlive the COVID-19 pandemic, then the choice of a supplier that can potentially become a long-term partner in that journey is advisable.
- It should be clear where the intellectual property for any work delivered by the digital supplier will reside, particularly if the supplier is creating new assets. The same applies to the purchase and use of any software licenses 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

Cost category	Key cost drivers and considerations
Ongoing/all phases	
Governance	• Coordination of personnel to develop and maintain relevant partnerships • Conducting an impact assessment and developing new policies, processes and standard operating procedures for ongoing monitoring of use and impact • Independent oversight and monitoring
Management and staffing	• Personnel to oversee the overall programme until planned end (if there is one), including project management – and vendor management, if applicable • System set-up and end-user support • Monitoring feedback and taking corrective action • Handling complaints and exercising data subject rights, including legal redress
Development and setup	
Technology adaptation	• Building completely new COVID-19 systems or leveraging existing software systems (e.g. adapting LIS) • Subscriptions, licensing fees and implementation costs associated with the software model • Custom configurations or any enhancements, if needed, or any custom-developed software • Translations and localizations, if needed
Deployment	
Equipment and hardware	• Data storage (e.g. costs for storage in the cloud, or on local servers or individual devices) • Devices (e.g. printers and scanners) needed at the certificate collection site
Testing	• Quality assurance, end-user testing and testing of conformity with standards and interoperability with other systems (if part of the design); ensure costs are allocated for collecting end-user feedback and updating the digital system according to feedback received
Training	• Training technicians, health facility managers and data entry personnel, which may involve travel or other logistical costs • Training materials for verifiers of DDCC:TR
Roll-out	• Transport of any necessary hardware, software or materials (including printed paper result) to the certificate generation or certificate-issuance sites

	• Increased technical support required during the roll-out phase
Outreach and raising awareness	• Communications on when, where and how people can obtain a DDCC:TR • Communication of what DDCC:TR can and cannot be used for • Battling "infodemics" (too much information, misinformation and disinformation) associated with DDCC:TR • Meeting accessibility requirements of individuals and reaching groups with disadvantages, such as individuals with digital skill barriers or disability barriers
Integration and interoperability	
Establishing trust frameworks	• Adapting content, depending on acceptance agreements between Member States • Coordination for establishing agreements between Member States
Interoperability with other systems	• Undertaking mapping exercises and adopting standards agreed upon through the establishment of trust frameworks • Any licensing fees associated with use of standards (note that the standards proposed by WHO in this guidance document have no licensing fees)
Scale	
Printing	• With the Paper Test Result: printing, which will increase as more people are tested and, subsequently, more people receive a paper test result certificate. If handwritten rapid test results need to be leveraged (e.g. at the entrance to sporting facilities or movie theatre), is there the ability to do high volume pre-printing of barcoded HCIDs on paper test result forms?
Human resources	• As people are tested: the additional personnel to support use of the systems, including training, management, etc.
IT licensing	• Depending on the licensing model associated with any digital solution, the additional licences that may need to be purchased as the number of operators or amount of data increases, or additional IT infrastructure is needed
IT scalability	• 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
Sustained operations	
Refresher training	• Consistent training of new staff when staff leave, and refresher training for existing staff – with content updates made as the context changes
Adaptive management	• Monitoring and evaluation of DDCC:TR implementation practices and processes, with application of learnings
Communication	• Continued messaging, with consideration of accessibility needs • Continued help desk or customer service technology support for users of the DDCC:TR
Technology maintenance	• Fixing bugs, adding features, maintaining customizations, releasing updates, and hardware maintenance and replacement

8.4 Additional resources to support implementation

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

WHO Interoperability Standard for DDCC:TR

- DDCC:TR HL7 Implementation Guide
- DDCC:TR Core Data Dictionary (Link to be added)

Example specification that can be used to guide implementation:

- EU Digital COVID Certificate[25]
- ICAO Guidelines: visible digital seals ("VDS-NC") for travel-related health proofs[24]

General implementation WHO guidance for digital health solutions:

- Digital implementation investment guide (DIIG): integrating digital interventions into health programmes[38] ***Error! Bookmark not defined.***– 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.

REFERENCES

1. Technical considerations for implementing a risk-based approach to international travel in the context of COVID-19: interim guidance : annex to: Policy considerations for implementing a risk-based approach to international travel in the context of COVID-19. Geneva: World Health Organization; 2 July 2021 (https://apps.who.int/iris/handle/10665/342212, accessed 6 July 2021).
2. Requirements and Scope of Digital Certificates (https://sciencetaskforce.ch/en/policy-brief/requirements-and-scope-of-digital-certificates/)
3. Joburg healthcare worker nabbed for allegedly selling fake Covid-19 test certificates (https://www.news24.com/news24/southafrica/news/joburg-healthcare-worker-nabbed-for-allegedly-selling-fake-covid-19-test-certificates-20210822)
4. Margit, M. Thousands of Israelis Join Telegram Groups Selling Fake COVID Papers - The Media Line (https://themedialine.org/by-region/thousands-of-israelis-join-telegram-groups-selling-fake-covid-papers/)
5. 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.
6. Fake Covid vaccine and test certificate market is growing, researchers say (https://www.theguardian.com/world/2021/may/16/fake-covid-vaccine-and-test-certificate-market-is-growing-researchers-say)
7. Digital documentation of COVID-19 certificates: vaccination status: technical specifications and implementation guidance, 27 August 2021 (https://www.who.int/publications/i/item/WHO-2019-nCoV-Digital_certificates-vaccination-2021.1)
8. Criteria for releasing COVID-19 patients from Isolation (https://www.who.int/news-room/commentaries/detail/criteria-for-releasing-covid-19-patients-from-isolation)
9. COVID-19 Clinical management: living guidance (https://www.who.int/publications/i/item/WHO-2019-nCoV-clinical-2021-1)
10. Policy considerations for implementing a risk-based approach to international travel in the context of COVID-19. Geneva: World Health Organization; 2 July 2021 (https://apps.who.int/iris/handle/10665/342235, accessed 6 July 2021)
11. Considerations for implementing and adjusting public health and social measures in the context of COVID-19. Geneva: World Health Organization; 14 June 2021 (https://apps.who.int/iris/handle/10665/341811, accessed 17 September 2021)
12. 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)
13. 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)

14. 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, accessed 27 June 2021).
15. 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, accessed 27 June 2021).
16. Diagnostic testing for SARS-CoV-2, 11 September 2020 (https://www.who.int/publications/i/item/diagnostic-testing-for-sars-cov-2)
17. COVID-19 diagnostic testing in the context of international travel: scientific brief, 16 December 2020 (https://apps.who.int/iris/handle/10665/337832)
18. SARS-CoV-2 antigen-detecting rapid diagnostic tests: An implementation guide, 21 December 2020 (https://www.who.int/publications/i/item/9789240017740)
19. COVID-19 natural immunity, 10 May 2021 (https://www.who.int/publications/i/item/WHO-2019-nCoV-Sci_Brief-Natural_immunity-2021.1)
20. Recommendations for national SARS-CoV-2 testing strategies and diagnostic capacities: interim guidance. 25 June 2021 (https://www.who.int/publications/i/item/WHO-2019-nCoV-lab-testing-2021.1-eng, accessed 8 September 2021).
21. Antigen-detection in the diagnosis of SARS-CoV-2 infection, 6 October 2021 (https://www.who.int/publications/i/item/antigen-detection-in-the-diagnosis-of-sars-cov-2infection-using-rapid-immunoassays)
22. Laboratory biosafety guidance related to coronavirus disease (COVID-19): Interim guidance, 28 January 2021 (https://www.who.int/publications/i/item/WHO-WPE-GIH-2021.1)
23. Advice on the use of point-of-care immunodiagnostic tests for COVID-19 (https://www.who.int/news-room/commentaries/detail/advice-on-the-use-of-point-of-care-immunodiagnostic-tests-for-covid-19)
24. Guidelines: visible digital seals ("VDS-NC") for travel-related health proofs. International Civil Aviation Organization (ICAO) Technical Advisory Group (TAG) on the Traveler Identification Group (TRIP); no date (https://www.icao.int/Security/FAL/TRIP/PublishingImages/Pages/Publications/Guidelines%20-%20VDS%20for%20Travel-Related%20Public%20Health%20Proofs.pdf, accessed 27 June 2021).
25. 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, accessed 27 June 2021).
26. 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).
27. Scottish Human Rights Commission. COVID-19 status certificates: human rights considerations. April 2021 (https://www.scottishhumanrights.com/media/2176/21_04_28_-covid-certificates-and-human-rights-vfinal.pdf, accessed 30 August 2021)

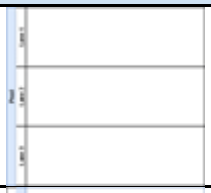
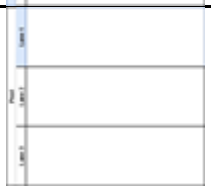
28. Guidelines on ethical issues in public health surveillance. Geneva: World Health Organization, 2017 (https://www.who.int/ publications/i/item/who-guidelines-on-ethical-issues-in-public-health-surveillance, accessed 15 Sept 2021)
29. International Patient Summary Implementation Guide: 1.0.0 – Continuous Integration Build [website]. Health Level Seven International – Patient Care Work Group; 2021 (https://build.fhir.org/ig/HL7/fhir-ips, accessed 27 June 2021).
30. https://loinc.org/
31. ICD-11: International Classification of Diseases 11th Revision. In: World Health Organization International Classification of Diseases [website]. Geneva: World Health Organization; 2021 (https://icd.who.int/en, accessed 27 June 2021).
32. Global Patient Set. In: SNOMED International [website]. London: SNOMED International; 2021 (https://www.snomed.org/snomed-international/learn-more/global-patient-set, accessed 27 June 2021).
33. Health system governance. In: World Health Organization/Health topics [website]. Geneva: World Health Organization; no date (https://www.who.int/health-topics/health-systems-governance#tab=tab_1, accessed 27 June 2021).
34. Adams C, Farrell S, Kause T, Mononen T. Internet X.509 Public Key Infrastructure Certificate Management Protocol (CMP), section 3.1.1.2 Certification Authority. Reston (VA) and Geneva: The Internet Society Network Working Group; 2005 (https://datatracker.ietf.org/doc/html/rfc4210#section-3.1.1.2, accessed 27 June 2021).
35. Laboratory assessment tool for laboratories implementing SARS-CoV-2 testing: Tool (https://www.who.int/publications/i/item/laboratory-assessment-tool-for-laboratories-implementing-covid-19-virus-testing)
36. Assessment tool for laboratories implementing SARS-CoV-2 testing: Interim Guidance: User Guide. (https://www.who.int/publications/i/item/assessment-tool-for-laboratories-implementing-covid-19-virus-testing, accessed 22 October 2021).
37. National eHealth Strategy Toolkit: overview. Geneva: World Health Organization and International Telecommunication Union; 2012 (https://www.who.int/ehealth/publications/overview.pdf, accessed 28 June 2021).
38. Digital implementation investment guide (DIIG): integrating digital interventions into health programmes. Geneva: World Health Organization; 15 September 2020 (https://www.who.int/publications/i/item/9789240010567, accessed 28 June 2021).

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 Continuity of Care use cases and Proof of Vaccination use cases.

Table A1.1 Business process symbols used in workflows

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

Annex 2: Guiding principles for mapping the WHO Family of International Classifications (WHO-FIC) and other classifications

Mapping from classifications and terminologies used in existing systems to the International Classification of Diseases, 11th revision (ICD-11), and other WHO-FIC classifications should follow the principles listed below.[39]

1. Establish use case(s) prior to developing the map – this involves identifying and formulating the purpose(s) for which the map will be used and describing the different types of users and how they will process data using the map.
2. Clearly define the purpose, scope and directionality of the map.
3. Maps should be unidirectional and single purpose. Separate unidirectional maps should be used in place of bidirectional maps (to support both a forward and a backward map table). Such unidirectional maps can support data continuity for epidemiological and longitudinal studies. Maps should not be reversed.
4. Develop clear and transparent documentation that is freely available to all and that describes the purpose, scope, limitations and methodology of the map.
5. Ideally, the producers of both terminologies in any map should participate in the mapping effort to ensure that the result accurately reflects the meaning and usage of their terminologies. As a minimum, both terminology producers should participate in defining the basic purpose and parameters of the mapping task, reviewing and verifying the map, developing the plan for testing and validation, and devising a cost-effective strategy for building, maintaining and enhancing the map over time.
6. Map developers should agree on the competencies, knowledge and skills required of team members at the onset of the project. Ideally, target users of the map should also participate in its design and testing to ensure that it is fit for its intended purpose.
7. Establish quality assurance (QA) and usage validation protocols at the beginning of the project and apply them throughout the mapping process. QA and usage validation involve ensuring the reproducibility, traceability, usability and comparability of the maps.

   Factors that may be involved in QA include quality-assurance rules, testing (test protocols, pilot testing) and quality metrics (such as computational metrics or precisely defined cardinality, equivalence and conditionality). Clear documentation of the QA process and validation procedures is an important component of this step in the mapping process. If it is feasible to conduct a pilot test, doing so will improve the QA and validation process. Mapping is an iterative process that will improve over time as it is used in real settings.

   Usage validation of maps is an independent process involving users of the maps (not developers of the maps) in order to determine whether the maps are fit for purpose (e.g. whether end users

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

reach the correct code in the target terminology when using manual and automated maps, etc.). Key principles for usage validation of maps include:

a. Use a "gold standard" (i.e. a statement in the original source data – e.g. a diagnosis as written in the medical record) as the reference point.

b. Compare the original source data with the end results of the following two processes.

    i. Coding of original source data with a source terminology – map code(s) of source terminology to code(s) of target terminology; and

    ii. 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, limitations and methodology used to create the maps.

9. Maintenance: Establish an ongoing maintenance mechanism, release cycle, types and drivers of changes, and versioning of maps. The maintenance phase should include an outline of the overall life-cycle plan for the map, conflict resolution mechanism, continuous improvement process, and decision process around when an update is required. Whenever maps are updated, the cycle of QA and validation must be repeated.

10. When map specialists are conducting mapping manually, it is recommended to provide the necessary tools and documentation to drive consistency. Such items include: the tooling environment (workflow details and resources related to both source and target schemes); source and target browsers, if available; technical specifications (use case, scope, definitions); editorial mapping principles or rules to ensure consistency of the maps, particularly where human judgement is required; and implementation guidance. Additionally, it is best practice to provide an environment that supports dual independent authoring of maps, as this is thought to reduce bias among human map specialists. Development of a consensus management process to aid in the resolution of discrepancies and complex issues is also beneficial.

11. In computational mapping, it is advisable to include resources to ensure consistency when building a map using a computational approach, including a description of the tooling environment, when human intervention would occur, documentation (e.g. the rules used in computerized algorithms), and implementation guidance. It is also advisable to always compute the accuracy and error rate of maps. It is important to manually verify and validate the computer-generated mapping lists. Such manual checking is necessary in the QA process, as maps that are generated automatically often contain errors. Such manually verified maps can also assist in the training of the machine-learning model when maps for different sections of terminologies are being generated sequentially.

12. The level of equivalence between source and target entities – such as equivalent, broader, narrower – should be specified.
13. If the mapping uses cardinality as a metric, then it must be clearly defined in terms of what is being linked between source and target, how the cardinalities are counted, and the direction of the map. The cardinality of a map (one-to-one, one-to-many, many-to-one, and many-to-many), without a clear definition, however, has a very weak semantic definition, being nothing more than the numbers of source entities and target entities that are linked in the map.
14. Maps should be machine-readable to optimize their utility.

When creating maps using ICD-11, map into the foundation component first, then generate maps to mortality and morbidity statistics through linearization aggregation.

Annex 3: What is public key infrastructure (PKI)?

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

Why is a PKI needed?

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

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

What is a PKI?

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

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

How is a PKI used?

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

Example 1: If I want to send a confidential message to a friend, then I can encrypt the message with 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.

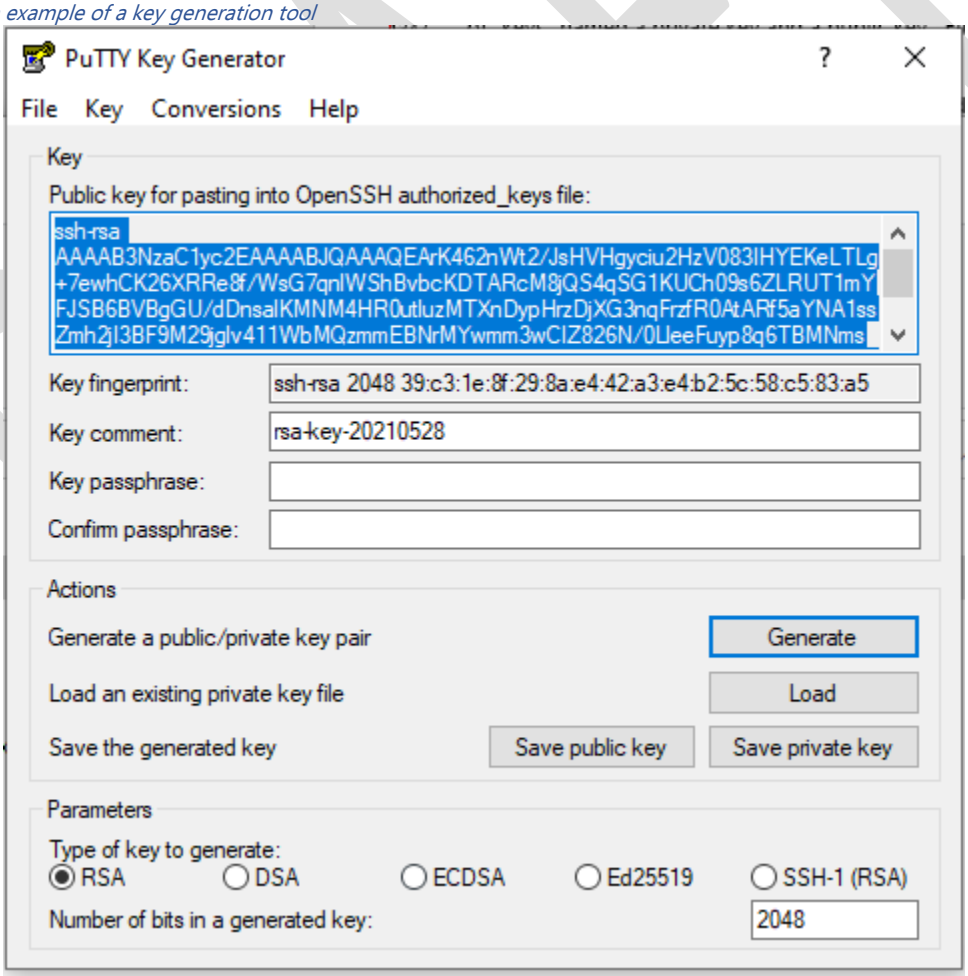
This second scenario is of interest for signing DDCC:TR data. It can be guaranteed that data has been approved and signed by a trusted authority if certificates are signed using private keys held by that authority and the person checking is in possession of the public key.

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

Figure A3.1 An example key

```
---- BEGIN SSH2 PUBLIC KEY ----
Comment: "rsa-key-20210528"
AAAAB3NzaC1yc2EAAAABJQAAAQEArK462nWt2/JsHVHgyciu2HzV083IHYEKeLTL
g+7ewhCK26XRRe8f/WsG7qnlWShBvbcKDTARcM8jQS4qSG1KUCh09s6ZLRUT1mYF
JSB6BVBgGU/dDnsalKMNM4HR0utluzMTXnDypHrzDjXG3nqFrzfR0AtARf5aYNA1
ssZmh2jI3BF9M29jglv411WbMQzmmEBNrMYwmm3wCIZ826N/0LleeFuyp8q6TBMN
msRlOaIpGsTeYI2GKU/oRtxzYcP2glY0vLE/uGoySIeYlI3ME6DSJbmUHtxqKsCm
13ggQvEwreysLX6oL0uaUyYfHTTfF2kzCH8MWiB1iQP2z4izQw==
---- END SSH2 PUBLIC KEY ----
```

Figure A3.2 An example of a key generation tool



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

How does a PKI work for vaccination certificates?

For the purposes of the DDCC: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, and that certificate authority becomes the "trust anchor" responsible for issuing certificates. Trust begins at this point, and this entity has to be a recognized and authorized actor.

B) The certificate authority doesn't sign vaccination documents and data. The signing of vaccination documents and data is handled by other agencies, such as public health actors and other stakeholders.

C) Therefore, the certificate authority issues private–public key pairs to these other actors in the form of document signer certificates (DSCs), providing them with the information needed to digitally sign documents.

D) These different agencies then use the private key in their DSC to perform this signing activity. Signing involves encrypting the information using the private key so that it is rendered into a format that is not human-readable.

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

F) An interested party (i.e. a Verifier) who wants to decrypt the encrypted information for the vaccination certificate must have two key things.
   - ❑ The public key corresponding to the private key in the DSC; and
   - ❑ Trust that the public key, from the DSC, came from a certificate authority that the interested party trusts.

G) To facilitate the two points in (F), a certificate authority usually sets up an online service for this purpose. The Verifier can interrogate the service and:
   1. 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:TR Registry Service in this paper.
   2. Once the Verifier has the public key, it can also check with the authority that the public key is valid and has not been revoked.

H) Finally, now that the Verifier knows that the public key came from a trusted source, the Verifier can decrypt whatever information has been provided for the vaccination certificate. If the decryption reveals the data, the Verifier can be confident that:
   - ❑ the information could only have been encrypted by someone with the private key, therefore it must have come from someone in possession of the DSC;

- ❑ the information has not been altered or tampered with after it was signed, otherwise the decryption would not work; and
- ❑ the information can be trusted, because the Verifier trusts the certificate authority, and trusts the certificate authority to have issued the DSC, which must have been used to encrypt the information.

I) If the public key decrypts the encrypted information so that it looks identical to the unencrypted version provided, the Verifier can be confident that only the entity in possession of the private key sent this data, and that it has not been altered since by any other party.
   - ❑ For the vaccination certificates, the HCID must resolve back to a digital record that is digitally signed in the manner described.
   - ❑ Optionally, the DDCC:TR core data set could also be encoded into a barcode to enable the Verifier to perform an offline check, but the Verifier would still need to be able to validate that the public key was a valid one.

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

Annex 4: Non-functional requirements

This section contains a suggested set of generic non-functional requirements (see Table A4.1). Along with the functional requirements in sections 3.3 and 4.3, these non-functional requirements provide a set of requirements can be adapted when specifying a digital solution for the scenarios in this paper. Non-functional requirements explain the conditions under which any digital solution must remain effective and are organized into the following categories.

- **Accessibility**: The provision of flexibility to accommodate each user's needs and preferences, along with appropriate measures to ensure access to persons with disabilities on an equal basis with others; for example, the solution should still be accessible to those with visual impairment.
- **Availability (service level agreements; SLAs)**: The definition of when the system will be available to the user community, how such metrics will be measured, and the functionality in the tool for managing planned downtime.
- **Capacity – current and forecast**: The number of concurrent users that can interact with the system without an unacceptable degradation in performance, speed or responsiveness. User populations are never static, and so the ability to handle current typical and peak volumes of usage and predicted future states, and the strategy for handling a traffic surge, must be considered.
- **Uptime SLAs – disaster recovery, business continuity, resilience**: The requirements for the system in terms of how it recovers from critical, unexpected failure and the support for business continuity. This includes time to recovery, how recovery is established, and at what levels resilience and redundancy are built into the system to minimize any data loss.
- **Performance/response time**: The speed with which the system is expected to respond under normal and exceptional loads, with a definition of what those terms mean.
- **Platform compatibility**: The different operating systems, machines and configuration on which the solution is expected to run.
- **Security and privacy**: The levels of security that the solution must provide in terms of user authentication and data protection.
- **Regulation and compliance**: Any regulatory/legal constraints with which the system must comply, such as data protection policies, WHO cloud policies, and information management and retention rules of the jurisdiction(s) in which the solution will run.
- **Reliability**: A measure of the reliability of the tool, for example the acceptable mean time between failures of the solution (both hardware and software components).
- **Scalability (horizontal, vertical)**: The ability to, and strategy for, handling an increasing load on the solution (in terms of increased number of users it can support, higher volumes of data it can handle, quicker performance and response, etc.). A solution can be scaled either horizontally (adding more elements to the solution, such as extra load-balanced servers) or vertically (adding extra capacity in existing elements, such as upgrading an existing server).

- **Supportability**: The requirements for engineers to detect, diagnose, resolve and monitor any issues and faults that arise while the solution is being used. This covers the features/functions that will be built into the system to facilitate technical support work.
- **Usability by target user community**: The extent to which a product can be used by specified users to achieve specified goals with effectiveness, efficiency and satisfaction in a specified context of use. This includes optimization of the interface for clarity and efficiency, and ensuring that the solution is appropriate to the needs and the experience level and expectations of the target users.
- **Data retention/archiving**: Requirements relating to how information will be archived from its normal location and then retained, including the frequency, the approval process, and any process for restoring information from the archive.

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

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

DDCC.NFXNREQ.012	**Disaster recovery, business continuity, resilience**	All data and derived analysis **SHALL** be stored within an appropriate data architecture to ensure redundancy and rapid disaster recovery, to eliminate the risk of data loss.
DDCC.NFXNREQ.013	**Disaster recovery, business continuity, resilience**	The system **SHOULD** 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.).
DDCC.NFXNREQ.014	**Disaster recovery, business continuity, resilience**	The system **SHOULD** provide near-instantaneous switch-over if any one component of the physical architecture fails critically (data centre destroyed, server destroyed, etc.)
DDCC.NFXNREQ.015	**Disaster recovery, business continuity, resilience**	All components of the solution **SHOULD** be underpinned by robust monitoring tools that track usage across space and time, so that system load and source can be queried.
DDCC.NFXNREQ.016	**Disaster recovery, business continuity, resilience**	Data concerning system usage **SHOULD** be available to system administrators via a dashboard to show current load, and recent load (last week, last month), and be able to perform custom queries by place and time. It **SHOULD** be possible to export this data.
DDCC.NFXNREQ.017	**Disaster recovery, business continuity, resilience**	It **SHALL** be possible to automatically log any periods of outage of the system and to supplement and update this record manually.
DDCC.NFXNREQ.018	**Disaster recovery, business continuity, resilience**	It **SHALL** be possible to trigger system alerts based on uptime and performance.
DDCC.NFXNREQ.019	**Disaster recovery, business continuity, resilience**	It **SHOULD** be possible to use system alerts to perform actions such as dispatch of a warning email/SMS to a system administrator or to execute a script that (for example) spins up a new virtual machine for load balancing.
DDCC.NFXNREQ.020	**Performance/ response time**	The solution **SHALL** follow best practices to deliver a responsive interface in which typical requests can be served (end-to-end interaction) in a maximum time specified in a number of seconds to be determined based on typical bandwidths. Degradation to a greater maximum time in number of seconds for limited-bandwidth scenarios is acceptable.
DDCC.NFXNREQ.021	**Performance/ response time**	The solution **SHOULD** be designed so that degradation of performance due to increased load (surge of users) is minimized.
DDCC.NFXNREQ.022	**Performance/ response time**	Where appropriate, long-running processes such as complex queries **MAY** be available for asynchronous execution, to allow a user to continue to interact with the system while the job executes and to receive a notification when the work is complete.
DDCC.NFXNREQ.023	**Performance/ response time**	The system **MAY** implement detection of a frozen ("hung") interface to give the user the option to cancel a current request.
DDCC.NFXNREQ.024	**Performance/ Response time**	The system **SHOULD** collect metrics on performance and response time to allow a system administrator to monitor system behaviour, identify bottlenecks or issues, and pro-actively address any risk of unacceptable degradation of speed.
DDCC.NFXNREQ.025	**Performance/ response time**	As with system availability, the solution **SHALL** provide dashboards of performance metrics, allow querying of the performance log and export of performance data for reports.
DDCC.NFXNREQ.026	**Performance/ response time**	As with system availability, the solution **SHALL** have the ability to set thresholds on performance and use the breach of those thresholds to raise alerts that can trigger email notifications or automated system actions (bring an extra server into a load-balanced set, for example).
DDCC.NFXNREQ.027	**Security and privacy**	Tools to request an account, log in, log out, set and change passwords, and receive password reminders **SHALL** be provided.
DDCC.NFXNREQ.028	**Security and privacy**	All interactions between a client and a server component of the solution **SHALL** be securely encrypted to prevent "man in the middle" interference with data in transit.
DDCC.NFXNREQ.029	**Security and privacy**	Any cloud components of the solution **SHALL** store their cloud data-at-rest in an encrypted format.

DDCC.NFXNREQ.030	**Security and privacy**	The solution **SHALL** have a security model that is robust and flexible and controls both access to data and the operations that can be executed against data.
DDCC.NFXNREQ.031	**Security and privacy**	Information about the governance and restricted use of data **SHOULD** be available within any solution alongside the data concerned, so that users have a clear and consistent reminder of the level of confidentiality, the sensitivity, and the permitted use of the data they are currently viewing.
DDCC.NFXNREQ.032	**Security and privacy**	Dashboards, reports, standard queries and exports of security information **SHOULD** be provided to assist system administrators in the management of access permissions. Queries to highlight conflicting permissions **SHOULD** be available.
DDCC.NFXNREQ.033	**Security and privacy**	The confidentiality of data must be managed with utmost care. In shared data environments, there **SHALL** be a clear separation of between the system's data and any other hosted clients' information. Dedicated hosting and data sources are preferred.
DDCC.NFXNREQ.034	**Regulation and compliance**	Any solution **SHOULD** be designed mindful of existing reference architecture guidelines and standards for distributed trust framework solutions and tools for exchanging vaccination data.
DDCC.NFXNREQ.035	**Regulation and compliance**	Any solution **SHALL** be compliant with any data policies and legal requirements identified by the country in whose jurisdiction the solution will operate.
DDCC.NFXNREQ.036	**Regulation and compliance**	It **MAY** be possible to tag data sets with any regulation and compliance information relevant to them so that this is readily available with the data set. Such information might include the data provider, intended purpose of the data, restrictions on the use of the data, and restrictions on where data can be stored.
DDCC.NFXNREQ.037	**Regulation and compliance**	Any solution **SHALL** be compliant with any data storage, retention and destruction laws mandated by the data policies and data laws of the countries in which data are located.
DDCC.NFXNREQ.038	**Reliability**	Any solution **SHOULD** be designed to maximize the mean time between failures, with appropriate best practice to deliver a robust, well-tested and reliable platform.
DDCC.NFXNREQ.039	**Reliability**	Any solution **SHOULD** provide a log in which failures in any part of the system are logged, so that mean time between failures can be calculated and tracked.
DDCC.NFXNREQ.040	**Scalability**	Any solution **SHOULD** be designed so that elements can be scaled horizontally by (for example) adding extra resources (more servers, extra virtual machines, etc.) and the mechanisms for coordinating their activity (load balancing, session management, etc.)
DDCC.NFXNREQ.041	**Scalability**	Any solution **SHOULD** be designed so that elements can be scaled vertically by (for example) adding extra capacity to solution elements (increased CPU, increased RAM, etc.)
DDCC.NFXNREQ.042	**Scalability**	It **MAY** be possible to configure rules for automatic horizontal scaling of the system to respond to increased load (e.g. spinning up a new virtual machine and adding it to a load-balanced pool of resources). Rules will be based on thresholds for system load and performance.
DDCC.NFXNREQ.043	**Scalability**	Any solution **SHOULD** log sufficient information about performance and load so that technical staff can refine the system's scaling strategy based on actual usage.
DDCC.NFXNREQ.044	**Supportability**	Any solution **SHOULD** provide a feedback channel as described in functional requirements for collecting information and support requests.
DDCC.NFXNREQ.045	**Supportability**	Any solution **MAY** provide access to learning material to support a user's understanding of how to use the tool and achieve specific aims.
DDCC.NFXNREQ.046	**Supportability**	The solution **SHALL** include a system log of activity in which events of interest, the time and date when they occur, their categorization, and the user (if appropriate) who triggered the event are recorded. The log must be of sufficient detail to assist technical staff with debugging issues.

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

268

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

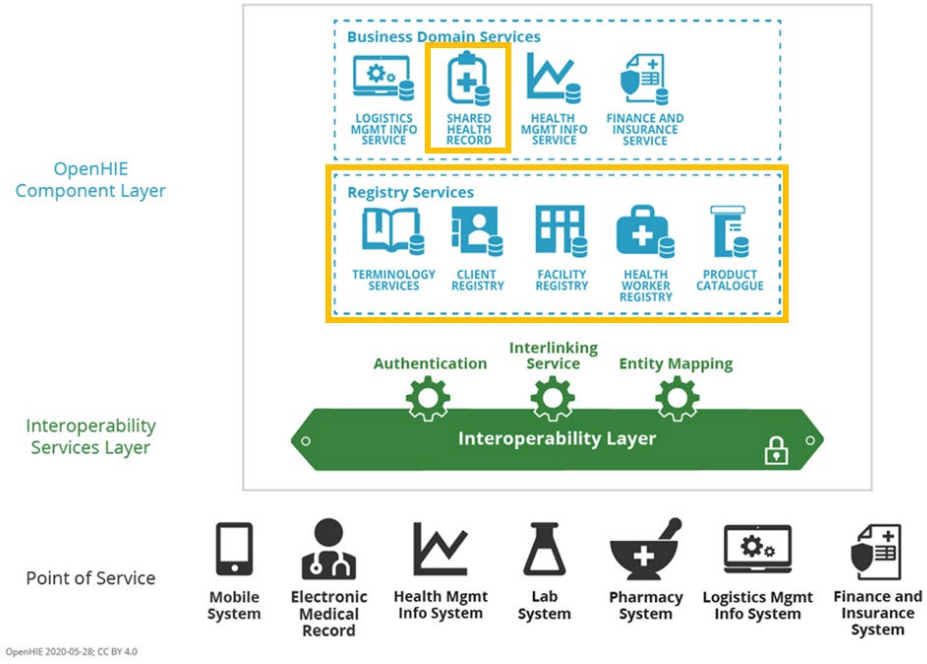
Annex 5: Open Health Information Exchange (OpenHIE)-based architectural blueprint

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 vaccine administration event, it is anticipated that complementary digital health infrastructure, such as the architectural elements described by the OpenHIE specification, could be leveraged.

OpenHIE describes a reusable architectural framework that leverages health information standards, enables flexible implementation by country partners, and supports exchange of individual components. OpenHIE also serves as a global community of practice to support countries towards "open and collaborative development and support of country-driven, large-scale health information sharing architectures".[40]

The OpenHIE high-level architecture[41] is shown in Figure A5.1. To show how a health-data-sharing infrastructure could support point-of-care digital health solutions to issue Digital Documentation of COVID-19 Certificates: Test Result (DDCC:TR), 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.

Figure A5.1 OpenHIE architecture[a]



[a]Yellow boxes indicate registries and repositories relevant to DDCC:TR.

[40] OpenHIE. In: OpenHIE [website]. OpenHIE; no date (https://ohie.org/about, accessed 29 June 2021).
[41] OpenHIE Architecture Specification. OpenHIE; September 2020 (https://ohie.org/wp-content/uploads/2020/12/OpenHIE-Specification-Release-3.0.pdf, accessed 29 June 2021).

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

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

Client registry: Also referred to as a patient registry, a demographic database that contains definitive information about each Tested Person. This database can include a Tested Person's name, date of birth, sex, address, phone number, email address, as well as other person-specific information such as parent–child relationships, caregiver relationships, family–clinician relationships and consent directives. It is also in the client registry that the list of unique identifiers (IDs; e.g. national ID, national health ID, health insurance ID) for a particular 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
- sex
- unique IDs.

Facility registry: A database of facility information, including data such as the facility name, a Public Health Authority (PHA)-issued unique ID, the organization under whose responsibility the facility operates, location (by address and/or Global Positioning System [GPS] coordinates), facility type, hours of operation, and the health services offered. The data elements in the DDCC: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
- 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 organizations or individual health facilities.

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

- test type
- test brand
- test manufacturer
- disease or agent targeted.

Shared health record (SHR): 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 SHR can include content such as the Tested Person's medication list, allergies, current problem list, immunization records, history of procedures, medical devices, diagnostic results, vital sign observation record, history of illness, history of pregnancies and current pregnancy status, care plan and advance directives. Such health data may be expressed using health data content standards such as the Health Level Seven (HL7) Fast Healthcare Interoperability Resources (FHIR) International Patient Summary (IPS) specification. Data in the SHR can be important for delivering guideline-based care during vaccine administration. Furthermore, data generated during test events could be added to the SHR, if in use, in order to support future provision of health services.