FRAMEWORK FOR THE ADMINISTRATION AND OPERATIONS OF THE WHO GLOBAL DIGITAL HEALTH CERTIFICATION NETWORK (GDHCN)

1 November 2023

I. INTRODUCTION

The WHO Secretariat has established the WHO Global Digital Health Certification Network (GDHCN) as an open, interoperable digital public infrastructure[1] to facilitate the verification and secure exchange of *Verifiable Digital Health Certificates* issued and utilized by *GDHCN Participants*. As a digital public infrastructure, the GDHCN has the potential to support a variety of *Trust Domains,* which are the sets of use cases operationalized by the GDHCN and utilized by *GDHCN Participants* subject to their respective rules, regulations and polices[2]. This document describes the overarching administrative and operational framework under which the GDHCN may be utilized for various *Trust Domains*, subject to WHO's rules, regulations, and procedures and governing bodies processes.

The GDHCN does not enable access by WHO to any content contained within individual *Verifiable Digital Health Certificates* issued by *GDHCN Participants*.

The GDHCN is responsive to the WHO Global strategy on digital health 2020-2025 (GSDH), which outlines the vision, goals, and strategic objectives for WHO and its Member States to harness the power of digital health to improve health outcomes and performance of health systems. In particular, the GDHCN contributes to the following proposed actions of the WHO Secretariat for implementing the GSDH[3]:

- "promote ethics, governance and security in handling and processing data for research or for other data-sharing requirements for the public good";
- "promote digital health collaborations and partnership models within and across organizations on the use of software global goods, open-standards, and common digital health architecture information systems;
- "develop a library of proven digital health solutions"; and

[1] Digital public infrastructure (DPI) is a concept of networked, open technology standards that enable governance and competitive markets for public programmes https://www.undp.org/digital/digital-public-infrastructure

[2] Annexes to this document describe the utilization of the GDHCN for a specific use case, whereby each use case is referred to as a *Trust Domain*. As of the date of this document, the scope of the GDHCN is limited to Digital Documentation of COVID-19 Certificates (DDCC) Trust Domain as described in Annex I, only. The WHO Secretariat may expand the scope beyond the DDCC Trust Domain, subject to the appropriate decision(s) or mechanisms implemented through WHO's Governing Bodies and will update this document accordingly.

[3] WHO Global strategy on digital health 2020-2025 https://apps.who.int/iris/handle/10665/344249

- "identify mechanisms to ensure the rapid deployment of surge capacity in response to an acute public health event."

In establishing the GDHCN, the WHO Secretariat recognizes the ethical, legal, and social implications of using digital health certificates, and the need to respect human rights, privacy, and data protection principles. The WHO Secretariat further acknowledges the challenges and opportunities that digital technologies present for achieving universal health coverage and advancing sustainable development goals.

II. DEFINITIONS

The following definitions apply herein:

***Business Owner Representative*:** The individual identified by a *GDHCN Participant* as having the primary business and programmatic responsibility for the *GDHCN Participant* for the implementation of the use cases covered by a *Trust Domain*.

***Encryption Key Certificate Governance*:** The process and technical specifications regarding the management and use of encryption keys for *Verifiable Digital Health Certificates*, *Public Key Infrastructure*, and for securing connections with *Trusted Services* and the *Trust Network Gateway*.

***Eligible GDHCN Participant*:** An *Eligible GDHCN Participant* is one of the following:

- a WHO Member State or Associate Member, or sub-national unit thereof;
- a State Party recognized by the International Health Regulations, or sub-national unit thereof;
- the United Nations (UN) and other intergovernmental organizations in effective relations with WHO;
- a fund, programme, specialized agency, or related organization within the UN system; or
- an organization officially delegated by one of the organizations mentioned above that can abide by the *GDHCN Terms of Participation* and fulfils one or more of the following health service functions:
    - *Public Health Agency;*
    - *Health Professions Education Accreditation Agency;*
    - *Health Services Licensing Agency;* or
    - *Public Health Security Agency.*

and, once accepted to the GDHCN, after the successful conclusion of the *Onboarding Process*, will be referred to as *GDHCN Participant* throughout this document. An *Eligible GDHCN*

Participant that has initiated the *Onboarding Process* will be referred to as an *Eligible GDHCN Applicant* throughout this document,

GDCHCN Secretariat: The WHO Secretariat serves as the operational and management leadership of the GDCHN, and in this role, the *GDHCN Secretariat*.

***GDHCN Trust Network*:** The *GHDCN Trust Network* is a *Trust Network* comprised of the GDHCN Secretariat and *GDHCN Participants*. The *GDHCN Trust Network* operationalizes *Trust Domains* through a *Trust Network Gateway* by enabling bilateral verification and utilization of *Verifiable Digital Health Certificates* and the utilization of *Trusted Services* by *GHDCN Participants*.

***Key Master Representative*:** The individual identified by a *GDHCN Participant* as having the primary responsibility for the management of the *Public Key Infrastructure*, including the generation of any needed public-private key pairs, and the configuration and management of the connections between the *GDHCN Participant*'s *Public Key Infrastructure* and the *GDHCN Trust Network Gateway*.

***Legal Representative*:** The individual designated by a *GDHCN Participant* as having the primary responsibility for reviewing the requirements related to a *Trust Domain* on behalf of this *GDHCN Participant*. This person should be someone that the *GDHCN Secretariat* can consult in relation to any legal or policy issues that may arise, such as changes to this document or changes to one of its Annexes that defines a *Trust Domain*.

***Letter of Application*:** A formal application sent via a verifiable and secure channel from an *Eligible GDHCN Participant* to the *GDHCN Secretariat* to join the *GDHCN Trust Network* and participate within a particular *Trust Domain*.

***Health Professions Education Accreditation Agency*:** An organization or organizational unit that is responsible for establishing and/or implementing procedures for accreditation of health professions education institutions[4].

***Health Services Licensing Agency*:** An organization or organizational unit that is responsible for establishing and/or implementing procedures for licensure, and the licensing of organizations or individuals to provide clinical, health system or public health services within their jurisdiction. Licensing comprises processes through which duly authorized governmental authorities, such as recognized professional organizations, grant permission to an individual or healthcare organization to operate or engage in a medical occupation or profession[5].

***Onboarding Process*:** The processes required for an *Eligible GDHCN Participant* to join the *GDHCN Trust Network*. At the successful conclusion of the *Onboarding Process*, the *Eligible*

[4] See: https://apps.who.int/iris/rest/bitstreams/1473223/retrieve and https://applications.emro.who.int/docs/em_rc50_r9_en.pdf?ua=1

[5] See: https://apps.who.int/iris/rest/bitstreams/1473223/retrieve and https://cdn.who.int/media/docs/default-source/documents/health-systems-strengthening-glossary.pdf

GDHCN Participant shall be considered a *GDHCN Participant*. Sometimes simply referred to as "*Onboarding*".

***Public Health Agency*:** An organization, or organizational unit, that is responsible for establishing procedures for and/or implementation of activities related to the protection, promotion, and improvement of public health within a specific jurisdiction or domain. May also be referred to as a Ministry of Health, Department of Health, or Public Health Authority.

***Public Health Security Agency*:** An organization, or organizational unit, that is responsible for establishing procedures for and/or implementing required activities, both proactive and reactive, for minimizing the danger and impact of acute public health events that endanger people's health across geographical regions and international boundaries[6].

***Public Key Infrastructure (PKI)*:** A system of hardware, software, policies, procedures, and roles that support the management of public keys and supports authentication, encryption, integrity, or non-repudiation services via a database of digital public keys.

Technical Representative: The individual designated by a *GDHCN Participant* as having the primary overall responsibility for the security, technical matters and systems infrastructure of this *GDHCN Participant* for the applicable *Trust Domain* including ensuring compliance with technical specifications.

***Trust Domain*:** Consists of:

- Defined **use cases** and business processes related to the utilization of *Verifiable Digital Health Certificates*;
- the open, interoperable **technical specifications** that identify or define the applicable *Trusted Services* and *Verifiable Digital Health Certificates;* and
- a set of **policy and regulatory standards** describing expected behavior of *GDHCN Participants* in relation to operation of the *Trusted Services* and utilization of *Verifiable Digital Health Certificates* (e.g. data minimization, privacy, scope of use).

***Trust Network*:** A *Trust Network* is a means to authenticate the encryption public keys used by participants within a network to perform encryption services, verify digital signatures, establish secure connections between systems, and otherwise make use of encryption public keys.

***Trust Network Gateway*:** The open-source software and its IT operational infrastructure, utilizing open standards, for a *Public Key Infrastructure* and metadata management services which is used to operationalize one or more *Trust Domains*.

***Trusted Service*:** A service (digital or otherwise) related to the issuance, management, verification, exchange, or other relevant processes, of *Verifiable Digital Health Certificates* which is defined using open, interoperable digital health standards.

[6] See: https://www.who.int/health-topics/health-security

***Verifiable Digital Health Certificate*:** A digital representation of a data set comprising a certificate or document, designed for a set of specific clinical or public health use cases which is defined using open, interoperable digital health standards; that contains within, or is associated to, a digital signature which can be verified by the public key of a public-private encryption key pair, and which is issued by a *GDHCN Participant*.

III. PURPOSE AND SCOPE OF THE GDHCN

The purpose of the GDHCN is to:

1) Enhance global health security and cooperation by facilitating the utilization and exchange of *Verifiable Digital Health Certificates* among *GDHCN Participants* and other stakeholders to:
    a. Empower individuals to access their own *Verifiable Digital Health Certificates* in a secure and convenient way;
    b. Enable health services of *GDHCN Participants* to verify *Verifiable Digital Health Certificates* easily for the use cases defined by the relevant *Trust Domain (e.g.,* continuity of care, travel) across different settings and jurisdictions; and
    c. Help link *Verifiable Digital Health Certificates* to *GDHCN Participants.*
2) Help *Eligible GDHCN Participants* and *GDHCN Participants* comply with technical specifications and policy and regulatory standards.
3) Identify and maintain open, interoperable specifications for the core infrastructure of a *Trust Network*, including a *Trust Network Gateway*, which enables the verification of *Verifiable Digital Health Certificates*.
4) Identify *Trust Domains* that can utilize the GDHCN core infrastructure and develop specifications and requirements for each identified *Trust Domain*.
~~5)~~ Promote innovation and learning in digital health by sharing best practices and experiences among *GDHCN Participants* and other stakeholders.

IV. PRINCIPLES

The following principles govern the operation of the GDHCN and the *GDHCN Secretariat*:

1) Equity: The GDHCN strives to support *GDHCN Participants'* efforts so that *Verifiable Digital Health Certificates* are accessible, affordable, and acceptable for all people, regardless of their location, income, gender, age, disability, or other factors that may affect their health status or opportunities.
2) Human rights: The GDHCN is established in a manner intended to respect human rights.

3) Privacy and data protection: The GDHCN is intended to be operated in compliance with generally recognized principles related to personal data protection. WHO is not to have access to underlying personal data, which will continue to be the exclusive domain of *GDHCN Participants*.

4) Trust and transparency: The GDHCN is intended to foster trust and transparency among *GDHCN Participants* and all other stakeholders by providing clear and accurate information about its objectives, operations, outcomes, and impacts.

5) Quality and safety: The GDHCN is intended to support the issuance, exchange, verification, updating, and revocation of *Verifiable Digital Health Certificates* in a reliable and consistent manner that meets the relevant technical specifications and quality standards.

6) Innovation and learning: The GDHCN is intended to promote innovation and learning in digital health by sharing best practices and experiences among participants and other stakeholders. The GDHCN also encourages research and development of new solutions that can improve the functionality and interoperability of *Verifiable Digital Health Certificates*.

V. GDHCN OPERATIONAL FRAMEWORK

The operations framework for the GDHCN is outlined, as follows:

1) The GDHCN is a voluntary *Trust Network* administered by the *GDHCN Secretariat*, operationalized through the *Trust Network Gateway* and is comprised of the *GDHCN Participants*.

2) As of the date of this document, the GDHCN is funded through existing contributions to WHO and does not require fees or payment by *GDHCN Participants*.

3) The GDHCN operationalizes *Trust Domains* approved by the *GDHCN Secretariat.* The Trust Domains operationalized by the GDHCN are defined in the Annexes. To maximize the utilization of GDHCN as digital public infrastructure at regional and global levels, *Trust Domains* may be proposed for consideration to the *GDHCN Secretariat* by one or more *Eligible GDHCN Participants* by providing a description for the proposed *Trust Domain,* which should include: use cases; technical specifications; and policy and regulatory standards.

4) The *Onboarding Process* is initiated by an *Eligible GDHCN Participant* through a *Letter of Application* for one or more *Trust Domains* and is overseen by the *GDHCN Secretariat*. During the *Onboarding Process*:

    a. the *GDHCN Secretariat* shall verify whether the *GDHCN Terms of Participation* of an *Eligible GDHCN Participant* have been satisfied;

b. the *GDHCN Secretariat* shall validate compliance with any technical specifications required for *Verifiable Digital Health Certificates* or *Trusted Services f*or applicable *Trust Domains*; and

c. *Eligible GDHCN Participants* shall configure and create necessary connections required for the *Public Key Infrastructure* and any applicable *Trusted Services* for applicable *Trust Domains*.

5) The GDHCN shall always be administered in accordance with WHO's rules, regulations, policies and procedures, and subject to the availability of resources for its operation.

VI. GDHCN SECRETARIAT

Contingent on available resources, the *GDHCN Secretariat* is responsible for establishing and maintaining the GDHCN including:

1) Maintaining the Framework for the Administration and Operations of the GDHCN (this document), including approving any amendments thereto;

2) Approving and maintaining technical specifications for a *Trust Domain* as an Annex to The Framework for the Administration and Operations of the GDHCN (this document);

3) Convening *GDHCN Advisory Committees* to support continued evolution of the *Trust Network Gateway* and *Trust Domains*;

4) Facilitating technical preparations for *Eligible GDHCN Participant*s;

5) Overseeing the *Onboarding Process* of *Eligible GDHCN Participants* for which additional technical details are provided here:

   https://worldhealthorganization.github.io/smart-trust/concepts_onboarding.html; and

6) Acting as a trust anchor[7] for the *Public Key Infrastructure* according to the technical specifications underpinning the *Trust Network Gateway*, which may be found here:

   https://worldhealthorganization.github.io/smart-trust

   and the *Encryption Key Certificate Governance*, which may be found here:

   https://worldhealthorganization.github.io/smart-trust/concepts_certificate_governance.html

VII. GDHCN PARTICIPANT

Each *GDHCN Participant* shall:

[7] See: https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=X.509

1) Determine which *Trust Domains* it intends to participate in;

2) Abide by all GDHCN Terms of Participation as defined in the Framework for the Administration and Operations of the GDHCN (this document) and relevant annexes for the relevant *Trust Domain*;

3) Adhere to the technical specifications that define the operation of the *Trust Network Gateway*;

4) Manage the encryption keys for securing connections to the *GDHCN Trust Network Gateway* according to the *Encryption Key Certificate Governance*;

6) Manage the encryption keys and publish through the *Trust Network* Gateway the public keys for verifying *Verifiable Digital Health Certificates* according to the *Encryption Key Certificate Governance*, as defined in the Annex for the relevant *Trust Domain*; and

7) Adopt the necessary legal instruments related to the utilization of *Trusted Services* with other *GDHCN Participants* according to their own applicable policies and legal frameworks for the relevant *Trust Domain*.

VIII. GDHCN TERMS OF PARTICIPATION

Participation in the GDHCN is subject to the *Onboarding Process* set forth by the *GDHCN Secretariat* in its sole and absolute discretion, and in accordance with WHO rules, regulations, policies and practices, as may be amended from time to time.

The requirements for the GDHCN Terms of Participation are comprised of the following components:

TOP0 Sharing of necessary credentials to establish an mTLS (mutual transport layer security) connection between a *GDHCN Participant's* backend system(s) and the *Trust Network Gateway*;

TOP1 Compliance, during initial *Onboarding Process* and during routine validation periods, with technical specifications required for a PKI;

TOP2 Compliance, during initial *Onboarding Process* and during routine validation periods, with technical specifications for *Verifiable Digital Health Certificates* and APIs of *Trusted Services* for each applicable *Trust Domain*;

TOP3 Compliance with policy and regulatory standards that *GDHCN Participants* pertaining to *Trusted Services* that a *GDHCN Trust Participants* operates or utilizes for each applicable *Trust Domain*; and

TOP4 Provision of supporting documentation (e.g. mandate, legal framework) demonstrating that it is an *Eligible GDHCN Participant*, as may be requested by WHO, at its sole discretion, from time to time.

The TOP4 requirement is waived for the following *Eligible GDHCN Participants*:

- a WHO Member State or Associate Member, or sub-national unit or equivalent thereof;
- a State Party recognized by the International Health Regulations, or sub-national unit or equivalent thereof;
- the United Nations and other intergovernmental organizations in effective relations with WHO; and
- a fund, programme, specialized agency, or related organization within the UN system.

IX. GDHCN LETTER OF APPLICATION

A *Letter of Application* must be officially signed for each *Trust Domain* and contains, in general, the following:

- An agreement to abide by the GDHCN Terms of Participation as defined in the Framework for the Administration and Operations of the GDHCN (this document) and in the Annex for the relevant *Trust Domain*;
- The contact information for the *Business Owner Representative*, *Key Master Representative*, *Legal Representative*, and *Technical Representative*; and
- Technical information needed to establish and verify the security of the connections between the *GDHCN Participant's Public Key Infrastructure* and the *Trust Network Gateway* according to the *Encryption Key Certificate Governance*, including:
    - a private GitHub repository containing appropriate public key material; and
    - a GNU Privacy Guard (GPG)[8] key or key otherwise compliant with the RFC4880 specification [9] associated to the *Key Master Representative*.

As a *Letter of Application* includes information to establish the trust between the *Trust Network Gateway* and the *Eligible GDHCN Applicant's* infrastructure, the *Letter of Application* must be conveyed through a secure channel to the *GDHCN Secretariat*. This secure channel may be one of the following:

- Face-to-face meeting between an authorized WHO staff member working in the *GDHCN Secretariat* or WHO Country Representative and the *Legal Representative* or *Business Owner Representative*, including confirmation of identity via passport. Subsequently, the *Letter of Application* will be submitted via diplomatic pouch from the WHO Country Office in the relevant country to WHO Headquarters; or from the relevant Permanent Mission to the UN in Geneva, Switzerland, to WHO Headquarters; or

[8] https://www.gnupg.org/
[9] https://www.ietf.org/rfc/rfc4880.txt

- Face-to-face meeting between an authorized WHO staff member working in the *GDHCN Secretariat* and an official delegate at the World Health Assembly, or any other meeting of WHO's governing bodies, including confirmation of identity via passport.

Any changes to the technical specifications needed to establish trust between the *GDHCN Applicant* or *GDHCN Participant*'s *Public Key Infrastructure* and *Trust Network Gateway* must be communicated via these same secure channels or through other secure channels that may be identified by the *GDHCN Secretariat*. *GDHCN Participants* should notify the *GDHCN Secretariat* of any changes to the appointed representatives to the *GDHCN Participant* in a timely manner.

The *Letter of Application* for each *Trust Domain* is provided in the relevant Annex[10].

Upon receipt of a *Letter of Application,* the *GDHCN Secretariat* will verify the accuracy and eligibility of the applicant. Once verified, the *Eligible GDHCN Applicant* must complete the necessary technical preparations, including user acceptance testing before being onboarded to the *Trust Network Gateway*. Details on the technical preparations may be found on the GDHCN website at:

https://worldhealthorganization.github.io/smart-trust/concepts_onboarding_checklist.html

X. GDHCN ADVISORY COMMITTEES

The *GDHCN Advisory Committees are* convened by the WHO Secretariat to provide technical and strategic advice to the *GDHCN Secretariat* relating to standards, technical specifications, and operations of the GDHCN. As appropriate and pertinent to *Trust Domains* and the GDHCN*,* the *GDHCN Secretariat* will convene *GDHCN Advisory Committees* under WHO processes and with respect to the terms of reference established per WHO standards for either:

- Advisory Groups[11];
- Expert advisory panels and committees[12]; or
- Other relevant mechanisms that have been established through WHO Governing Bodies.

XI. AMENDMENTS AND ANNEXES

The following applies to any amendments, inclusive of any Annex for a Trust Domain, for The Framework for The Administration and Operations Of The GDHCN (this document):

1) Amendments are established by the *GDHCN Secretariat;*
2) All amendments will be published on the GDHCN website and will be communicated to the *Legal Representative*, *Technical Representative* and *Business Representative*

[10] As of the date, only Annex I related to the Digital Documentation of COVID-19 Certificates (DDCC) Trust Domain is available.
[11] https://www.who.int/about/collaboration/open-calls-for-advisory-groups
[12] https://www.who.int/about/collaboration/expert-advisory-panels-and-committees

identified in the *Letters of Application* for the relevant *Trust Domain* and will come into effect from such date of notice.

XII. RESPONSIBILITY

1) WHO will bear no liability towards *Eligible GDHCN Participants*, *GDHCN Participants* or any third party, including users of the GDHCN, including with regard to any claims, damages, or financial losses of any kind.

2) Each *GDHCN Participant* will be responsible towards other *GDHCN Participants* and WHO for any damage caused, including through errors or omissions, in the issuance and uploading of its public keys and will be solely responsible for its own damage caused by it in the issuance and uploading of its public keys.

3) *GDHCN Participants* will not be responsible or liable for the errors or omissions of other *GDHCN Participants*, or of WHO, in relation to the GDHCN.

4) Under no circumstances shall WHO assume any liability for acts carried out by *GDHCN Participants* regardless of whether such acts were carried out in the name of the GDHCN.

5) *GDHCN Participants* are responsible for managing personal data contained in a *Verifiable Digital Health Certificate* or accessible through a *Trusted Service* of health system users within their respective jurisdictions and any related claims, bearing in mind that WHO will not have access to underlying personal data.

XIII. WHO NAME AND EMBLEM

No *GDHCN Participant*, shall, in any statement or material of an advertising or promotional nature, refer to its relationship with WHO or otherwise use the name (or any abbreviation thereof) and/or emblem of the World Health Organization.

XIV. TERMINATION OF PARTICIPATION

1) At least 30 days' notice, transmitted in writing to the *GDHCN Secretariat* via formal diplomatic channels, is required for termination of participation in the GDHCN for one or more *Trust Domains*. Termination takes effect 30 days after the *GDHCN Secretariat* receives the notice in writing.

2) Upon receipt of a notice of termination of participation in accordance with paragraph XIV.1, the *GDHCN Secretariat* will inform the other *GDHCN Participants* of the termination.

3) The *GDHCN Secretariat*, in its sole discretion, may terminate the participation in the GDHCN of any *GDHCN Participant*.

4) The *GDHCN Secretariat* may, at any time and for any reason, cease the operation of the GDHCN. In the event of such a decision by the *GDHCN Secretariat*, the *GDHCN Secretariat* will make reasonable efforts to provide due notice to *GDHCN Participants*, and, if appropriate, facilitate the transfer of the operations and modalities of the GDHCN

to another organization or entity approved by *GDHCN Participants* for that purpose, subject to provision of appropriate resources for that purpose.

XV. SURVIVING PROVISIONS

Those rights and obligations as set forth in the Framework for the Administration and Operation of the GDHCN (this document) that are, by their nature, intended to survive its expiration or earlier termination for whatever reason shall survive indefinitely. This includes, but is expressly not limited to, paragraphs XII, XIII, this paragraph XV, paragraph XVI, and the corresponding definitions contained in paragraph II.

XVI. SETTLEMENT OF DISPUTES

Any dispute relating to the interpretation or application of the Framework for the Administration and Operations of the GDHCN (this document) shall, unless amicably settled, be subject to conciliation. In the event of failure of the latter, the dispute shall be settled by arbitration. The arbitration shall be conducted in accordance with the modalities to be agreed upon by the parties or, in the absence of agreement, with the rules of arbitration of the International Chamber of Commerce. The arbitration proceedings shall be conducted in the English language, and the place of arbitration shall be Geneva, Switzerland. The parties shall accept the arbitral award as final.

XVII. PRIVILEGES AND IMMUNITIES

Nothing contained in or relating to the Framework for the Administration and Operations of the GDHCN (this document) shall be deemed to constitute a waiver of any of the privileges and immunities enjoyed by WHO under national or international law and/or as submitting WHO to any national court jurisdiction.

XVIII. NOTICES

Except in the case of notices or other communications that require a secure channel, as described under paragraph IX, all communication to the *GDHCN Secretariat* may be sent through email to tng-secretariat@who.int.

ANNEX I – GDHCN TRUST DOMAIN: DDCC

Participation in the GDHCN for the *DDCC Trust Domain* is completely voluntary and is open to *Eligible GDHCN Participants*.

USE CASES

The Digital Documentation of COVID-19 Certificates (DDCC) *Trust Domain* covers the utilization of COVID-19 Vaccine Certificates and Test Certificates for the use cases, data requirements, and data requirements outlined in the following documents:

1) DDCC: Vaccination Status (DDCC:VS) technical specifications and implementation guidance for vaccination certificates for the purposes of continuity of care and proof of vaccination.
2) DDCC: Test Result (DDCC:TR) technical specifications and implementation guidance for test result certificates that attest to: (a) the fact that an individual has been tested for SARS-CoV-2, and (b) the result of that SARS-CoV-2 diagnostic test.

TECHNICAL SPECIFICATIONS

Technical specifications are available in the above mentioned documents and at: https://worldhealthorganization.github.io/ddcc/

POLICY AND REGULATORY STANDARDS

GDHCN Participants shall confirm their readiness and intent to:

1) comply with Ethical principles and data protection considerations outlined in Section 2 of: https://www.who.int/publications/i/item/WHO-2019-nCoV-Digital_certificates-vaccination-2021.1 and in particular ensure that the personal data contained in the certificates issued shall be processed only for the purpose of accessing and verifying the information included in the certificate, shall be limited to what is strictly necessary for the intended use case, and shall not be retained longer than is strictly necessary;

2) comply with standards, cybersecurity requirements and technological systems and processes for the GDHCN as described in: https://worldhealthorganization.github.io/smart-trust; and

3) ensure that COVID-19 certificates issued can be verified for their authenticity, validity and integrity utilizing the WHO GDHCN.

The *Letter of Application* for the DDCC Trust Domain under the general Terms of Participation is available at:

https://worldhealthorganization.github.io/smart-trust/Letter_of_Application_DDCC.docx.

TRANSITIVE TRUST - EU DCC

Through 31 December 2023, *Eligible GDHCN Participants* that have participated in the European Union's Digital Covid Certificate (DCC) Trust Network shall have the option of joining the GDHCN for the Digital Documentation of COVID-19 Certificates (DDCC) *Trust*

Domain under the notion of *Transitive Trust* for which the following special considerations apply:

1) Terms of Participation:
    a. TOP0: signed certificates (TNP_{TLS}[13] and TNP_{UP}[14]) may be transferred using the EU directly to the WHO after a verification of EU's digital signature.
    b. TOP1: will be waived during initial *Onboarding Process*; and
    c. TOP2: will be waived during initial *Onboarding Process* for the DDCC *Trust Domain*.
2) Onboarding Process:
    a. *GDHCN Participants* do not need to provide a GitHub of public key material repository nor a GPG key if the same signed certificates (TNP_{TLS} and TNP_{UP}) will be used for connection to the *Trust Network Gateway*.
3) Letter of Application:
    a. The *Letter of Application* for the *Transitive Trust – EU DCC* is available at: https://worldhealthorganization.github.io/smart-trust/Letter_of_Application_Transititve_Trust.docx

[13] The TLS client authentication public key certificate of a *GDHCN Participant*'s back-end system.

[14] The public key certificate that a *GDHCN Participant* uses to sign data packages that are uploaded to the TNG.