Session 3: Building trust frameworks for Verifiable Health Credentials including digital COVID-19 certificates

Joint ITU/WHO Workshop on "Future of Verifiable Health Credentials Beyond COVID-19"

Dr. Carl Leitner, Technical Officer - WHO
11 September 2023

World Health Organization

Global Digital Health Strategy: Actions for the WHO secretariat – Mandate for Trust Architecture

“A national interoperable digital health ecosystem should be set up in such a way that the information technology health infrastructures **are both interoperable among each other and**, allowing for differences in national legislation and policies, **capable of sharing health data with infrastructures of other countries**”

Collaboration and knowledge transfer

- To 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.**

Digital health governance

- **To Develop regulatory framework on international health data**, to agree on global appropriate use of health data, and to outline principles of equitable data-sharing principles for research, consistent metadata and definitions, artificial intelligence and data analytics; primary and secondary use of data
- Develop a guideline on **global interoperability standards for digital health**.

Digital strategy implementation

- To Identify and engage with relevant stakeholders, regulatory bodies and regional eHealth/digital health networks to **support the implementation of digital health transformation at national or regional level**.

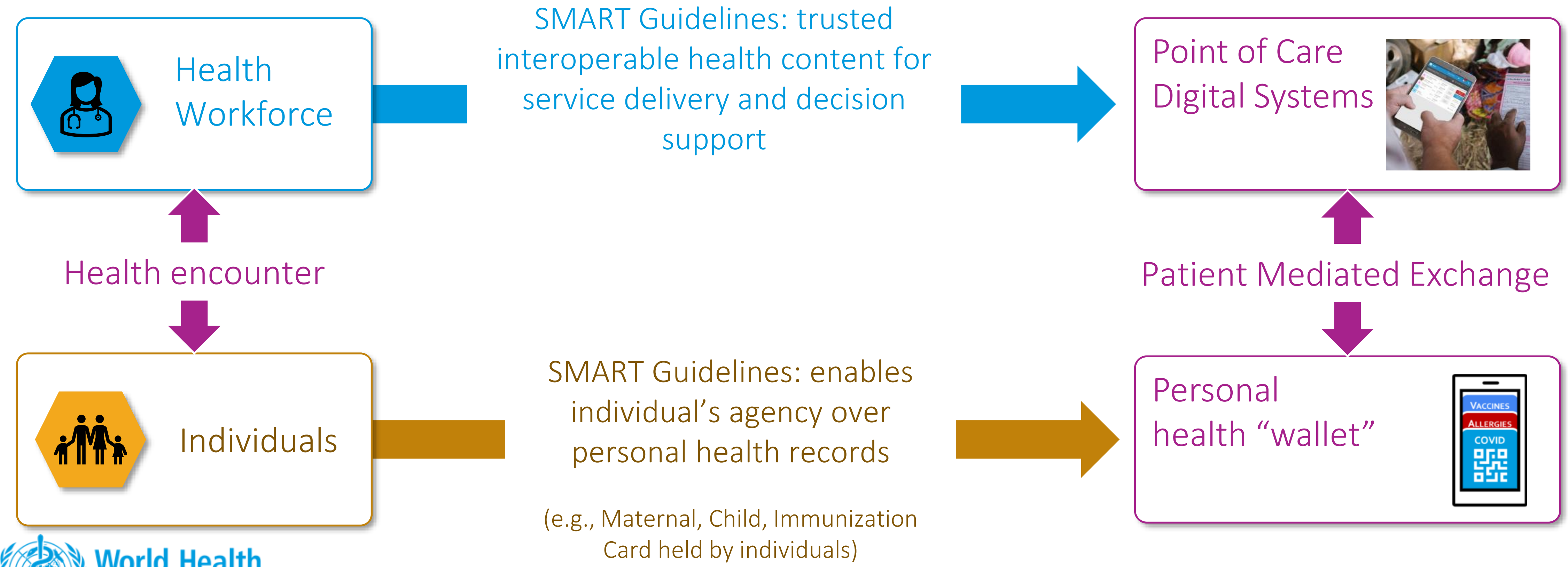
Human-centred health system

- **To Support Member States and stakeholders to use person-centric, digital health devices and systems** to enhance health workforce performance and facilitate evidence-based decision to improve public trust in using digital health technologies inside or outside the context of a public health emergency.
- **To Develop and promote the use of tools that support the digitalization of integrated health service with a focus on patient’s managed quality of service.**

World Health Organization

Digital personal health record: Leveraging the SMART Guidelines methodology to digitize and scale provider-side and client-side solutions

Leveraging technology to achieve person-centered care ***everywhere***



Health Workforce

SMART Guidelines: trusted interoperable health content for service delivery and decision support

Point of Care Digital Systems

Health encounter

Patient Mediated Exchange

Individuals

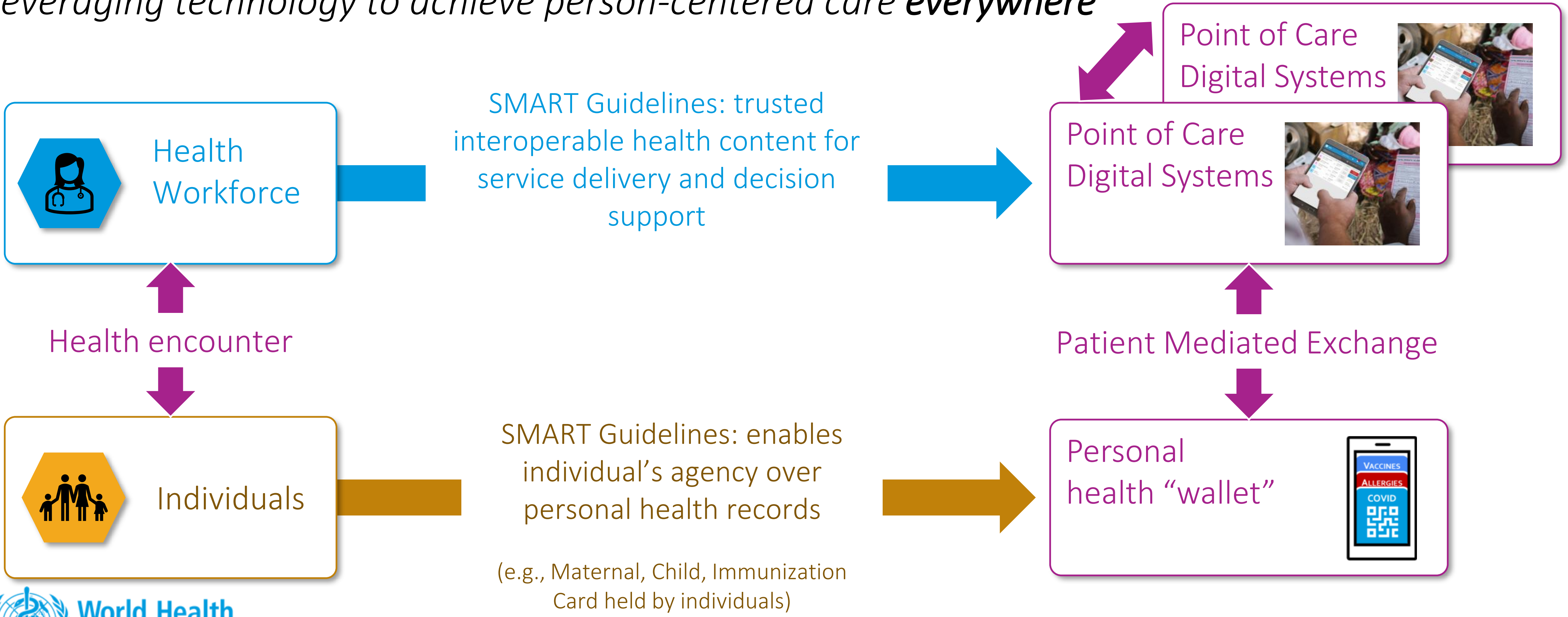
SMART Guidelines: enables individual's agency over personal health records

(e.g., Maternal, Child, Immunization Card held by individuals)

Personal health "wallet"

Digital personal health record: Leveraging the SMART Guidelines methodology to digitize and scale provider-side and client-side solutions

Leveraging technology to achieve person-centered care ***everywhere***



Health Workforce

SMART Guidelines: trusted interoperable health content for service delivery and decision support

Point of Care Digital Systems

Point of Care Digital Systems

Health encounter

Patient Mediated Exchange

Individuals

SMART Guidelines: enables individual's agency over personal health records

(e.g., Maternal, Child, Immunization Card held by individuals)

Personal health "wallet"

A global health trust network would help address current challenges at individual, national and global levels

	Individual level	National level	Global level
Existing system without global health trust network	• Limited control over own health records • Paper based records • Limited ability to exchange and/or verify health information globally	• Lack of clear policies, principles and regulations • Lack of interoperability • Inadequate government resources	• Inconsistent design, document type and data collected • Lack of global coordinating platform • Few mechanisms for exchange of records
Digitally augmented system with global digital health trust network	• Individuals have access to & control over their health information • Digital records – always available • Ability to verify online and/or offline	• Clearly documented policies, principles and regulatory framework based on consensus • Standards compliant, interoperable infrastructure	• Standardized format for enabling exchange of health information • Global platform with WHO as the mediator

World Health Organization

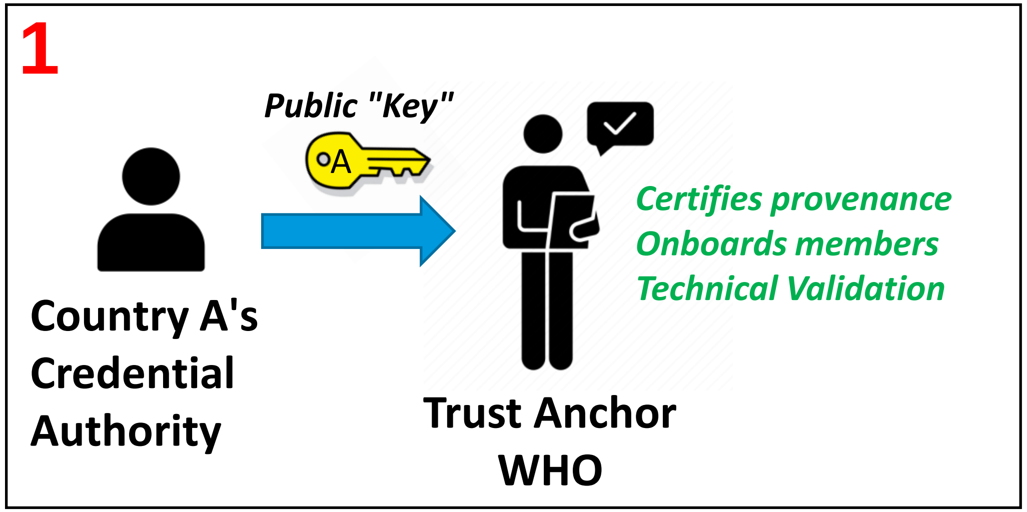
Global Digital Health Certification Network (GDHCN)

GDHCN takes up the EU DCC with shared values and principles: transparency and openness, inclusiveness, accountability, data protection and privacy (including data minimisation), security, scalability at a global level, and equity (implementable both digitally and on paper)

WHO Global Digital Health Certification Network
An open-source platform
Built on robust, transparent standards
Strengthening pandemic preparedness
World Health Organization
European Commission
Built on the EU Digital COVID Certificate (EU DCC)

- 100% Compatible with EU DCC Technical Specifications
- Utilizes “transitive trust” to enable rapid onboarding to GDHCN
- Builds on EU open-source DCC Gateway
- Separation of health content (verifiable digital health certificates) from trust network infrastructure (PKI)
- Future APIS & use cases aligned to WHO SMART Guidelines (HL7 FHIR)

WHO as a trust anchor - **Global Digital Health Certification Network (GDHCN)**



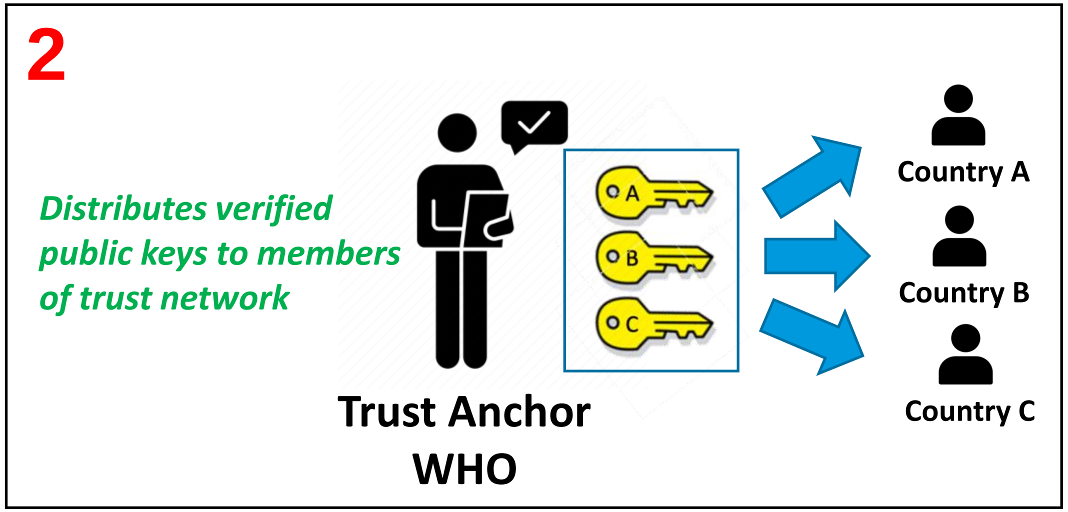
1

Public "Key"

Country A's Credential Authority

Trust Anchor WHO

Certifies provenance
Onboards members
Technical Validation

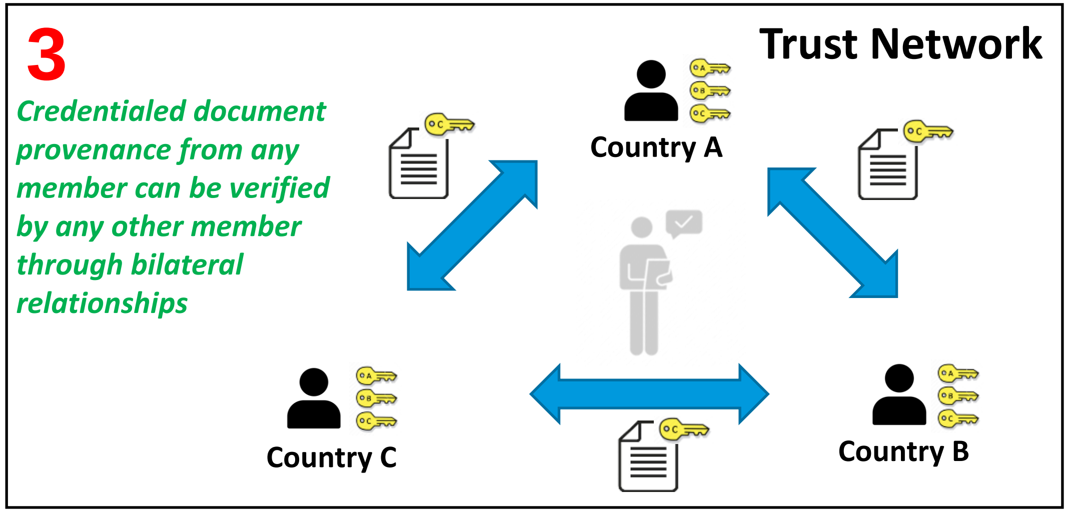


2

Distributes verified public keys to members of trust network

Trust Anchor WHO

Country A
Country B
Country C



3

Trust Network

Credentialed document provenance from any member can be verified by any other member through bilateral relationships

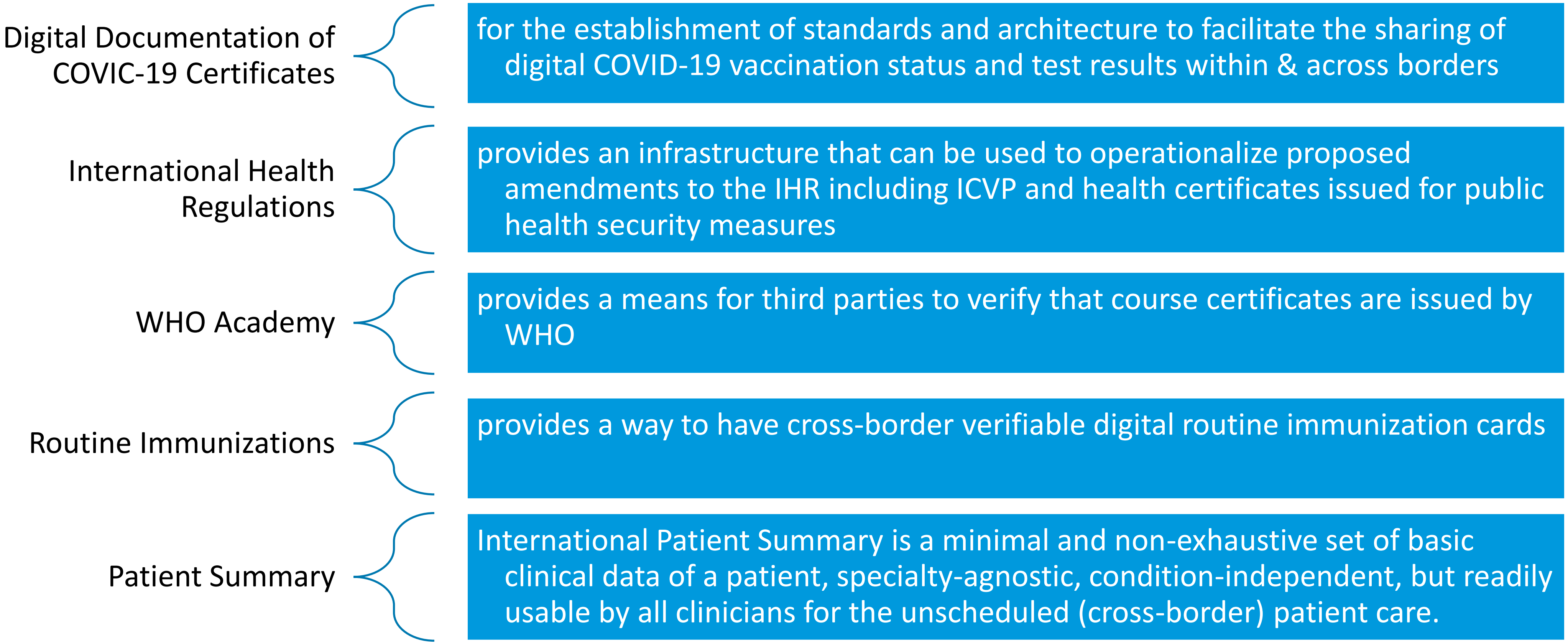
Country A
Country B
Country C

World Health Organization

Domains of trust

A **Domains of Trust** defined by a set of:

- Use cases and content specifications related to exchange of health documents
- Trusted services related to issuance, management, verification, revocation of health certificates
- Governance policies that apply across the set of use cases



Digital Documentation of COVIC-19 Certificates

for the establishment of standards and architecture to facilitate the sharing of digital COVID-19 vaccination status and test results within & across borders

International Health Regulations

provides an infrastructure that can be used to operationalize proposed amendments to the IHR including ICVP and health certificates issued for public health security measures

WHO Academy

provides a means for third parties to verify that course certificates are issued by WHO

Routine Immunizations

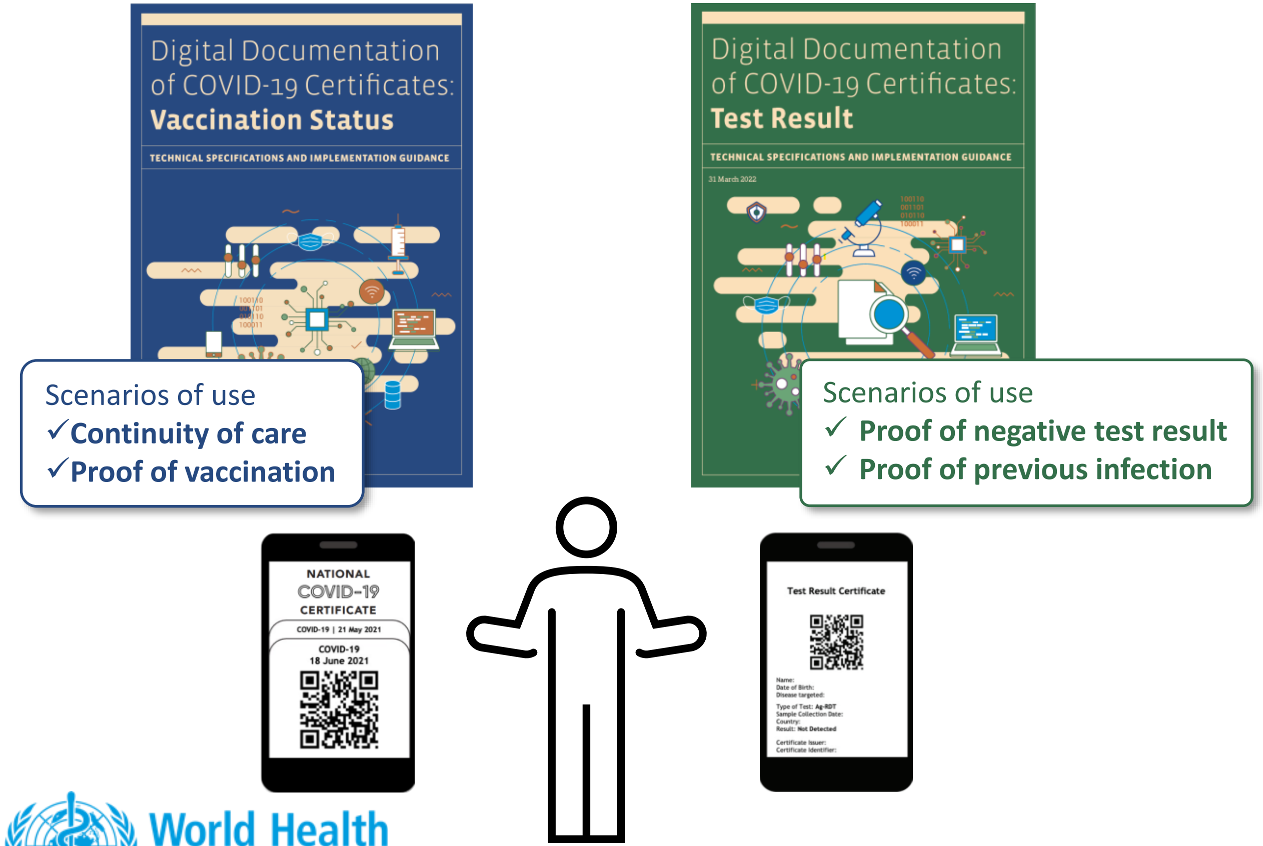
provides a way to have cross-border verifiable digital routine immunization cards

Patient Summary

International Patient Summary is a minimal and non-exhaustive set of basic clinical data of a patient, specialty-agnostic, condition-independent, but readily usable by all clinicians for the unscheduled (cross-border) patient care.

WHO and EU worked closely on technical guidance on COVID-19 Certificates

DDCC



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

TECHNICAL SPECIFICATIONS AND IMPLEMENTATION GUIDANCE

Scenarios of use
- ✓ **Continuity of care**
- ✓ **Proof of vaccination**

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

TECHNICAL SPECIFICATIONS AND IMPLEMENTATION GUIDANCE

31 March 2022

Scenarios of use
- ✓ **Proof of negative test result**
- ✓ **Proof of previous infection**

NATIONAL COVID-19 CERTIFICATE

COVID-19 | 21 May 2021

COVID-19
18 June 2021

Test Result Certificate

Name:
Date of Birth:
Disease targeted:

Type of Test: **Ag-RDT**
Sample Collection Date:
Country:
Result: **Not Detected**

Certificate Issuer:
Certificate Identifier:

DCC

eHealth Network

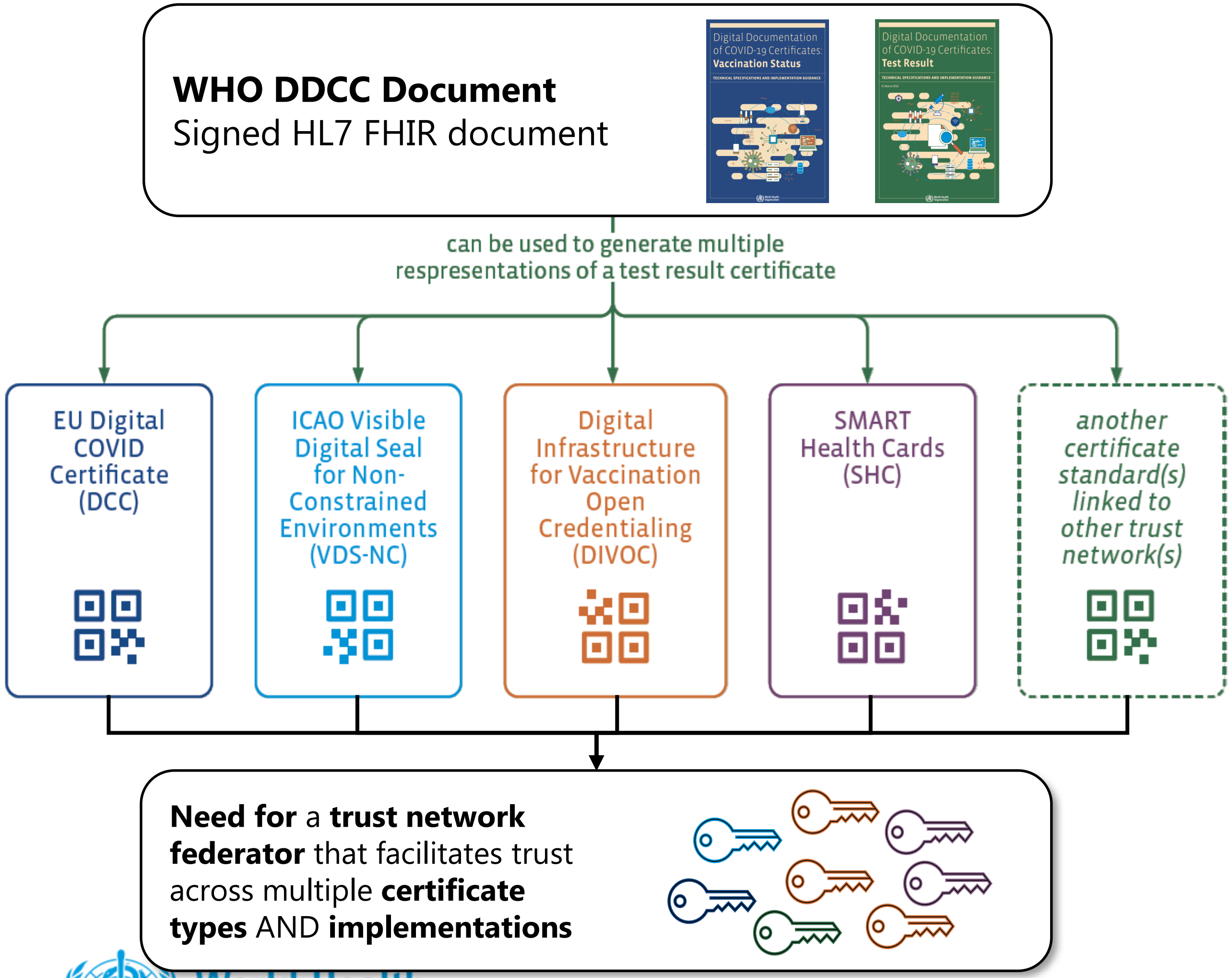
Guidelines on

Technical Specifications

for EU Digital COVID Certificates

World Health Organization

Global Digital Health Certification Network – COVID Certificates



WHO DDCC Document
Signed HL7 FHIR document

Digital Documentation of COVID-19 Certificates: Vaccination Status

Digital Documentation of COVID-19 Certificates: Test Result

can be used to generate multiple respresentations of a test result certificate

EU Digital COVID Certificate (DCC)

ICAO Visible Digital Seal for Non-Constrained Environments (VDS-NC)

Digital Infrastructure for Vaccination Open Credentialing (DIVOC)

SMART Health Cards (SHC)

another certificate standard(s) linked to other trust network(s)

Need for a **trust network federator** that facilitates trust across multiple **certificate types** AND **implementations**

Computable components described in HL7 FHIR Implementation Guide as part of WHO SMART Guidelines

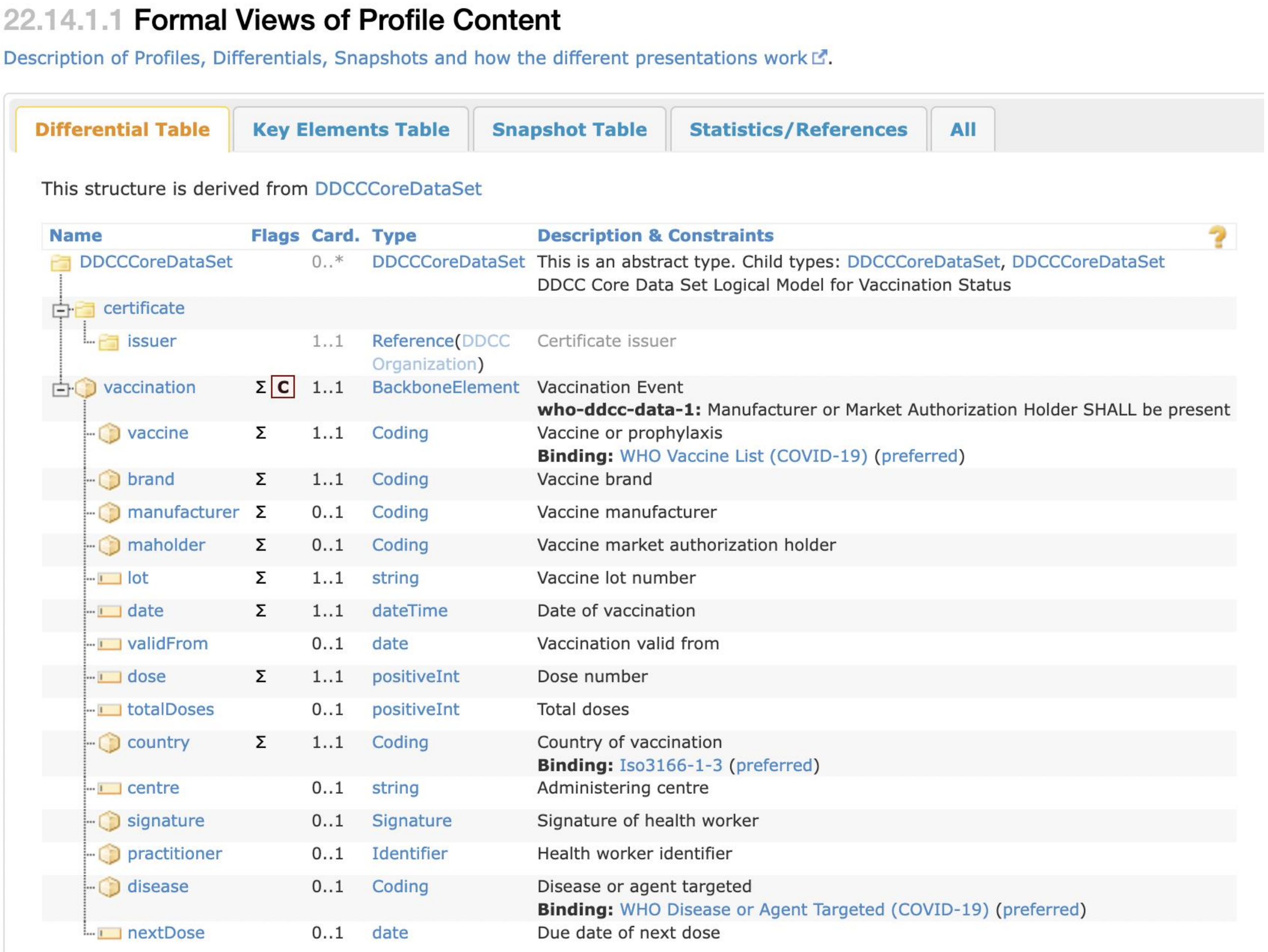
Structure and terminology mappings defined in DDCC Implementation guide using DDCC Logical Model as common data dictionary

PKI Infrastructure in GDHCN Gateway:

- EU DCC API & certificate governance will be preserved
- DID for public key distribution supported

COVID-19 Certificate – Technical Specifications

HL7 FHIR ® Logical Model for Core Data Set



22.14.1.1 Formal Views of Profile Content

Description of Profiles, Differentials, Snapshots and how the different presentations work.

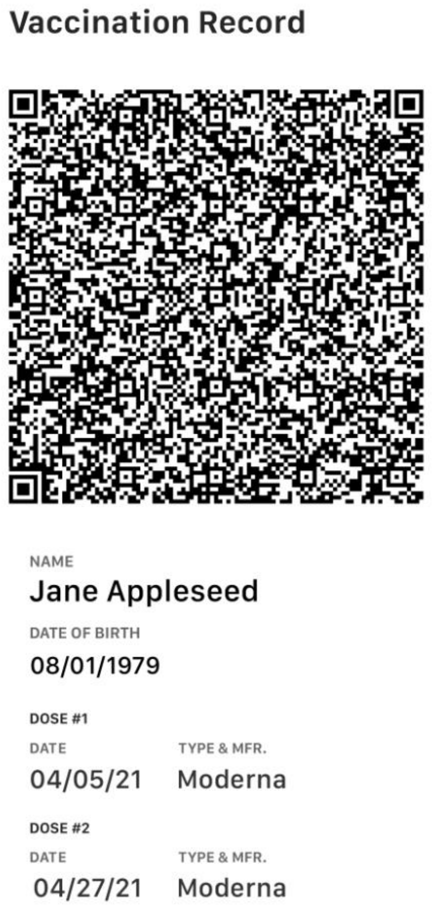
Differential Table | Key Elements Table | Snapshot Table | Statistics/References | All

This structure is derived from DDCCCoreDataSet

Name	Flags	Card.	Type	Description & Constraints
DDCCCoreDataSet		0..*	DDCCCoreDataSet	This is an abstract type. Child types: DDCCCoreDataSet, DDCCCoreDataSet DDCC Core Data Set Logical Model for Vaccination Status
certificate				
issuer		1..1	Reference(DDCC Organization)	Certificate issuer
vaccination	Σ C	1..1	BackboneElement	Vaccination Event **who-ddcc-data-1:** Manufacturer or Market Authorization Holder SHALL be present
vaccine	Σ	1..1	Coding	Vaccine or prophylaxis **Binding:** WHO Vaccine List (COVID-19) (preferred)
brand	Σ	1..1	Coding	Vaccine brand
manufacturer	Σ	0..1	Coding	Vaccine manufacturer
maholder	Σ	0..1	Coding	Vaccine market authorization holder
lot	Σ	1..1	string	Vaccine lot number
date	Σ	1..1	dateTime	Date of vaccination
validFrom		0..1	date	Vaccination valid from
dose	Σ	1..1	positiveInt	Dose number
totalDoses		0..1	positiveInt	Total doses
country	Σ	1..1	Coding	Country of vaccination **Binding:** Iso3166-1-3 (preferred)
centre		0..1	string	Administering centre
signature		0..1	Signature	Signature of health worker
practitioner		0..1	Identifier	Health worker identifier
disease		0..1	Coding	Disease or agent targeted **Binding:** WHO Disease or Agent Targeted (COVID-19) (preferred)
nextDose		0..1	date	Due date of next dose

bidirectional mappings

QR Code Renderings:
EU DCC, DIVOC, ICAO, Smart Health Cards



Vaccination Record

NAME
Jane Appleseed

DATE OF BIRTH
08/01/1979

DOSE #1

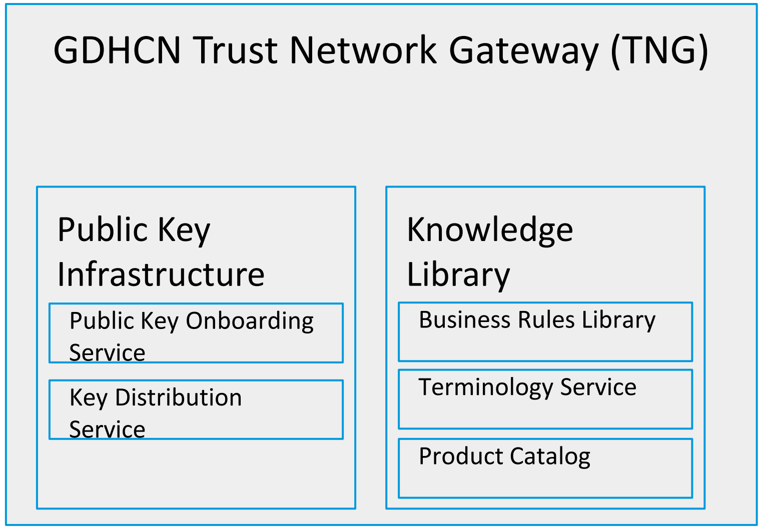
DATE	TYPE & MFR.
04/05/21	Moderna

DOSE #2

DATE	TYPE & MFR.
04/27/21	Moderna

GDHCN – Trust Network Gateway (TNG)

- Goal: Backwards compatible with EU DCC with only configuration changes (e.g. URLs)
- Future APIS & use cases aligned to WHO SMART Guidelines (HL7 FHIR®)
- Clear separation of health content (verifiable digital health certificates) from trust network infrastructure



GDHCN Trust Network Gateway (TNG)

Public Key Infrastructure

Public Key Onboarding Service

Key Distribution Service

Knowledge Library

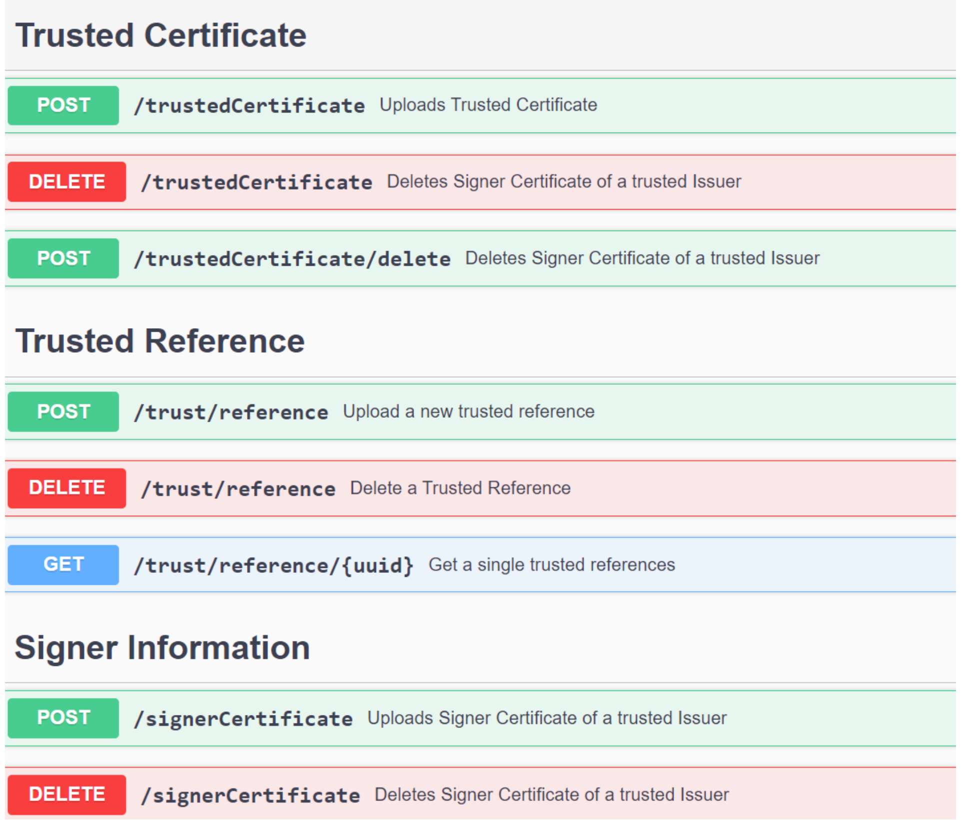
Business Rules Library

Terminology Service

Product Catalog

Go Live: WHO Gateway API (same as EU DCC Gateway)

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



Trusted Certificate

POST `/trustedCertificate` Uploads Trusted Certificate

DELETE `/trustedCertificate` Deletes Signer Certificate of a trusted Issuer

POST `/trustedCertificate/delete` Deletes Signer Certificate of a trusted Issuer

Trusted Reference

POST `/trust/reference` Upload a new trusted reference

DELETE `/trust/reference` Delete a Trusted Reference

GET `/trust/reference/{uuid}` Get a single trusted references

Signer Information

POST `/signerCertificate` Uploads Signer Certificate of a trusted Issuer

DELETE `/signerCertificate` Deletes Signer Certificate of a trusted Issuer

Notes:

- CRL will be operational but will be empty
- “Domains” defined by a set of:
  - Use cases related to exchange of health documents
  - Trusted services related to issuance, management, verification, etc of health documents
  - Governance policy that applies
- Default “Domain” is DDCC, in database backend
- Issue with response schema change related to schema has been addressed: https://github.com/WorldHealthOrganization/smart-trust-network-gateway/pull/56
- Support for Decentralized Identifiers (DID), did:web, is already available

Certificate Governance

Location of key material:

- Dev keys: https://github.com/WorldHealthOrganization/tng-participants-dev
- UAT keys: https://github.com/WorldHealthOrganization/tng-participants-uat
- Production Keys: https://github.com/WorldHealthOrganization/tng-participants-prod

Trust Network Gateway - Trust Anchor (TNG_{ROOT})

TNG_{ROOT} denotes she public key pair for the root certificate of the Trust Network. Use secp256r1 until its broken.

Trust Network Gateway - Signing (TNG_{SIGN})

Root of all keys used to sign key material coming from trust network participants. Subordinate certificate to TNG_{ROOT}

Trust Network Gateway - Trust Anchor (TNG_{TA})

TNG_{TA} denotes the Trust Anchor public key certificate of the TNG. The corresponding private key is used to sign the list of all DSCS and SCA certificates offline. Subordinate certificate to $TNG_{SIGN.}$

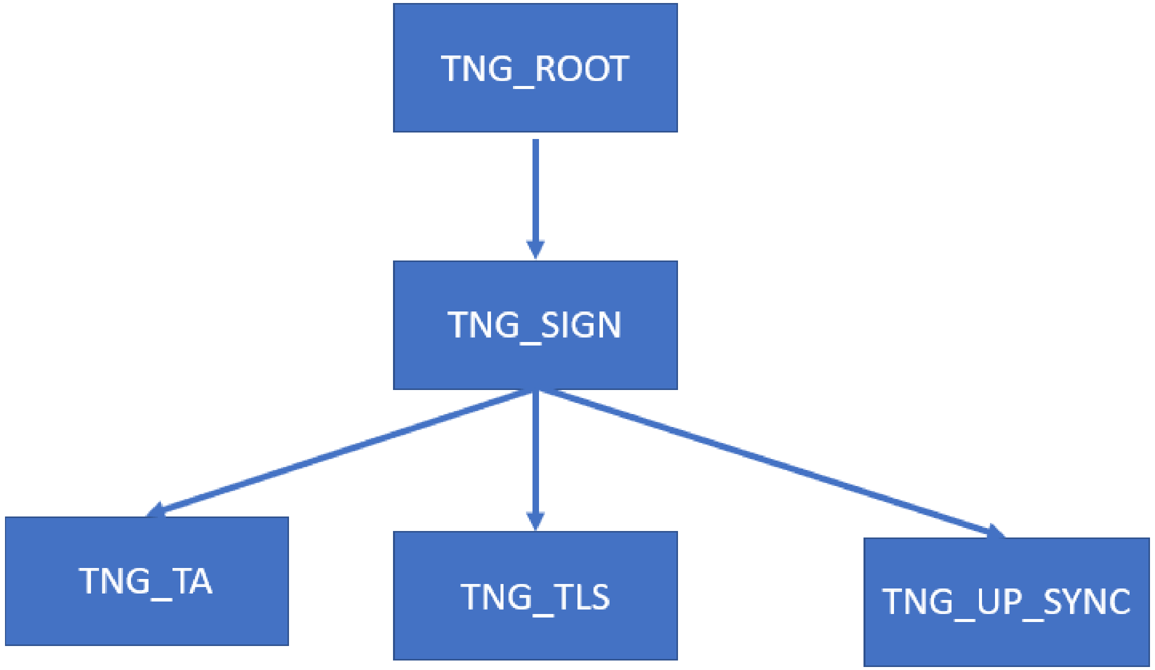
Trust Network Gateway – UP_SYNC (TNG_{UP_SYNC})

TNG_{SYNC_UP} denotes the Synchronization public key certificate of the TNG. The corresponding private key is used to sign the list of all DSCS and SCA certificates from synchronization import process during interim period. It will be thrown away after 2023. Subordinate certificate to $TNG_{SIGN.}$

Trust Network Gateway - Transport Layer Security (TNG_{TLS})

TNG_{TLS} denotes the TLS server public key certificate of the TNG. Use secp256r1 until its broken. Subordinate certificate to $TNG_{SIGN.}$

WHO Certificate Hierarchy



Timeline

- June 5:
  - Public Ceremony on EC support for WHO to uptake EU DCC trust network
  - Application open to EU DCC participants to join GDHCN under ”Transitive Trust” relationship
- June 25:
  - WHO GDHCN Trust Network Gateway Go-Live
  - Nightly sync EU DCC Gateway -> WHO TNG
  - EU DCC Gateway remain authority for public keys, replicate updates to WHO TNG
- September 30:
  - Expand eligibility to WHO Member States that did not join EU DCC participants
- December 31:
  - EU DCC network is shutdown
  - WHO-EU DCC transitive trust ends
- 2024
  - Expand to other Trust Domains

Thank you

For more information, please contact:

Dr. Carl Leitner

Technical Officer
Digital Health & Innovation (Science Division)

WHO HQ
leitnerc@who.int

World Health
Organization