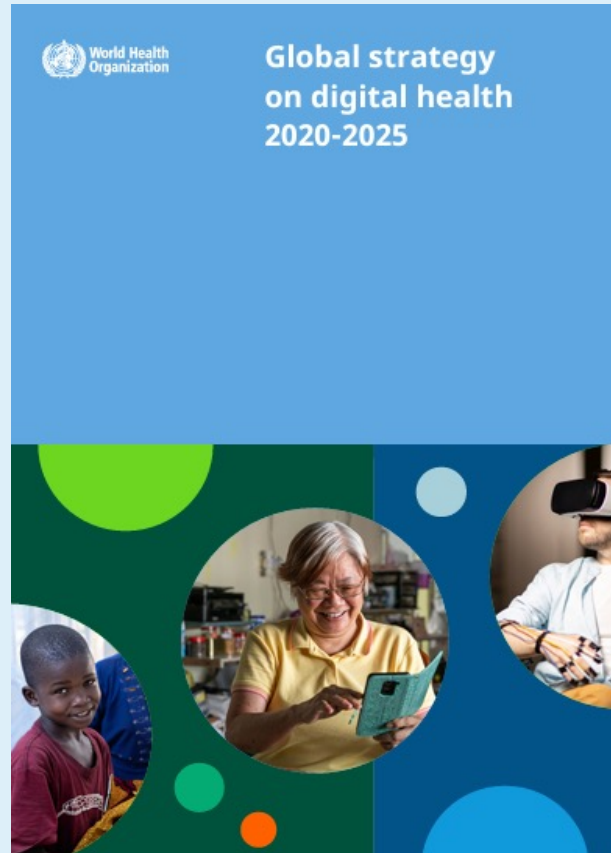

WHO's Global Digital Health Certification Network (GDHCN)

gdhcn-secretariat@who.int

9 May 2024



To improve health for everyone, everywhere by accelerating the development and adoption of appropriate digital health solutions to achieve the health-related SDGs



Global Digital Health Strategy Main Objectives



Promote global collaboration & advance the transfer of knowledge on digital health



Advance the implementation of national digital health strategies



Strengthen governance for digital health at global, regional and national levels



Advocate people-centered health systems that are enabled by digital health

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

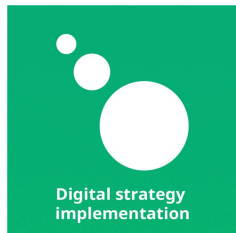
“A national interoperable digital health ecosystem should be set up in such a way that the information technology health infrastructures **are both interoperable among each other and**, allowing for differences in national legislation and policies, **capable of sharing health data with infrastructures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



- 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**.



- **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**.

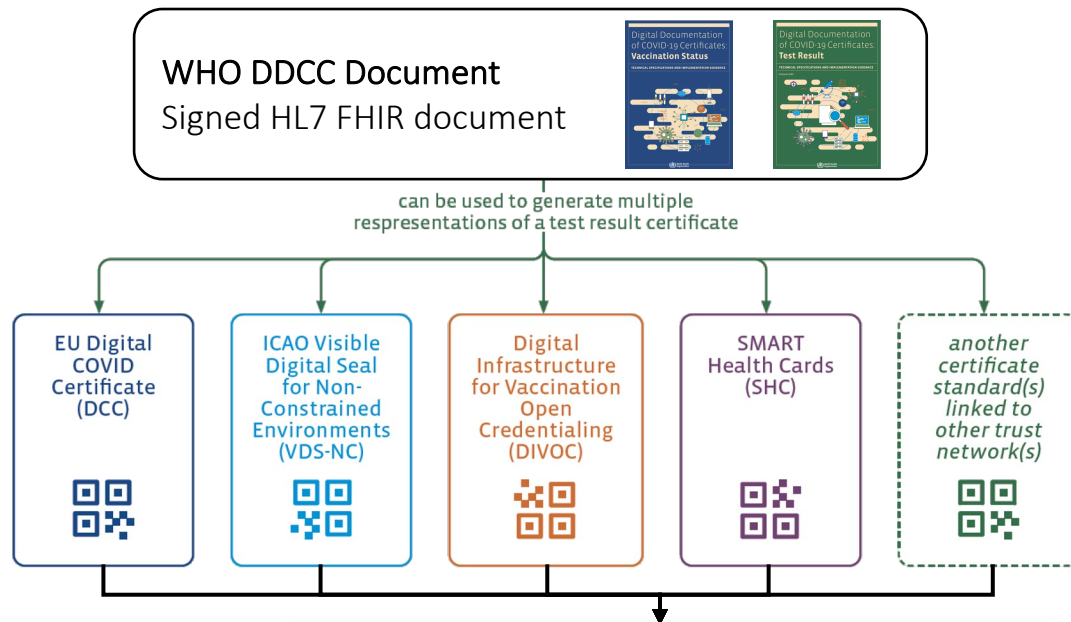


- To Identify and engage with relevant stakeholders, regulatory bodies and regional eHealth/digital health networks to **support the implementation of digital health transformation at national or regional level**.



- **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.**

Based on the experience from digital COVID-19 certificates, it is evident that consensus on global governance and policies are required so that health documents can be recognized and used globally



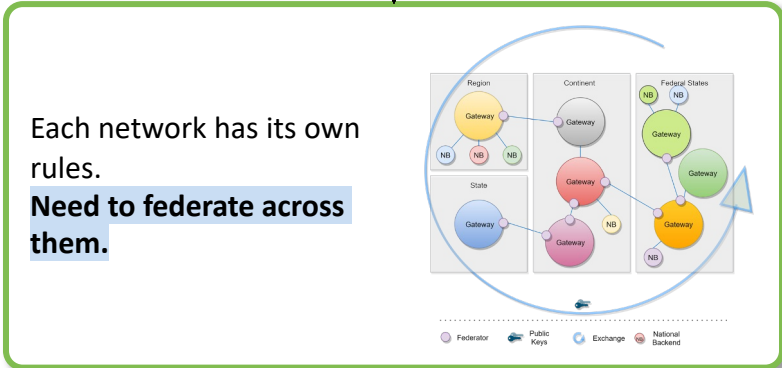
Varying public health **policies** across countries

Standards **implemented in a variety of ways** without governance

Many existing digital standards **don't interoperate**

Need to architect for **multiple use cases** beyond COVID-19

Need for a **directory to federate** across trust networks



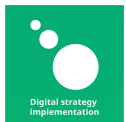
The GDHCN is digital public infrastructure to meet confluence of requests to the secretariat in the Global Strategy on Digital Health, requests for leadership during COVID-19, and understanding of need to build upon successes from COVID-19 for greater health systems resiliency



2020 *Actions for the WHO secretariat under the “Global Strategy for Digital Health”*



Promote common digital health architecture



Support **implementation** of digital health in countries & regions



Global **interoperability standards** for digital health

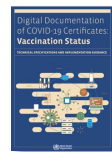


Promote use **person-centric**, digital health devices and systems



World Health Organization

2021 *Publication of “Digital Documentation of COVID-19 Certificates Technical Specifications & Implementation Guidance”*



- ✓ Specifications are **software-agnostic**
- ✓ For **mobile-based & paper-based certificates**

2022 *G20, WHO, OECD, Global Digital Health Partnerships Pilot for a “Federated Public Trust Repository”*

- ✓ **Successful federation** across existing networks: EU DCC, ICAO Health Master List, DIVOC, SMART Health Cards
- ✓ Leveraging **Public Key Infrastructure** technology



2023 *Uptake of EU DCC System & Launch of Global Digital Health Certification Network (GDHCN)*

- ✓ Creation of a “**phone book**” of public keys for countries
- ✓ **Expands upon the legacy** of the EU DCC network & lessons learned from G20 pilot
- ✓ Currently for **COVID-19**, but can be expanded
- ✓ **Circular sent by DG** for Member States for voluntary participation

List of participants currently onboarding or onboarded to GDHCN

Region of the Americas

1. Bahamas
2. Bolivia
3. Belize
4. Brazil
5. Canada
6. Chile
7. Ecuador
8. Honduras
9. Paraguay
10. Suriname
11. Uruguay
12. El Salvador
13. Panama
14. Guatemala
15. Argentina
16. Colombia
17. Costa Rica
18. Peru
19. British Virgin Islands

European Region

- | | |
|--------------------|---------------------|
| 1. Belgium | 24. Poland |
| 2. Croatia | 25. Kyrgyzstan |
| 3. Czech Republic | 26. Faroe Islands |
| 4. Cyprus | 27. Montenegro |
| 5. Estonia | 28. Ireland |
| 6. Finland | 29. Andorra |
| 7. France | 30. Monaco |
| 8. Greece | 31. Türkiye |
| 9. Israel | 32. North Macedonia |
| 10. Latvia | 33. Moldova |
| 11. Lithuania | 34. Armenia |
| 12. Malta | 35. Albania |
| 13. Netherlands | 36. Luxembourg |
| 14. San Marino | 37. Hungary |
| 15. Slovakia | |
| 16. Spain | |
| 17. Sweden | |
| 18. Ukraine | |
| 19. United Kingdom | |
| 20. Iceland | |
| 21. Slovenia | |
| 22. Portugal | |
| 23. Georgia | |

African Region

1. Benin
2. Zimbabwe
3. Madagascar
4. Burkina Faso
5. Tanzania
6. Burundi
7. Togo

Eastern Mediterranean Region

1. Morocco
2. Iraq
3. Qatar
4. Oman
5. Kingdom of Saudi Arabia

Western Pacific Region

1. New Zealand
2. Singapore
3. Japan
4. Australia
5. Mongolia
6. Malaysia

South East Asia Region

1. Indonesia
2. Thailand
3. Sri Lanka

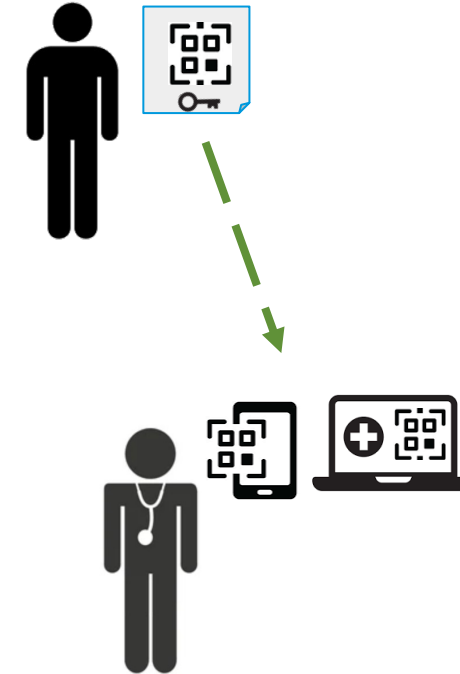
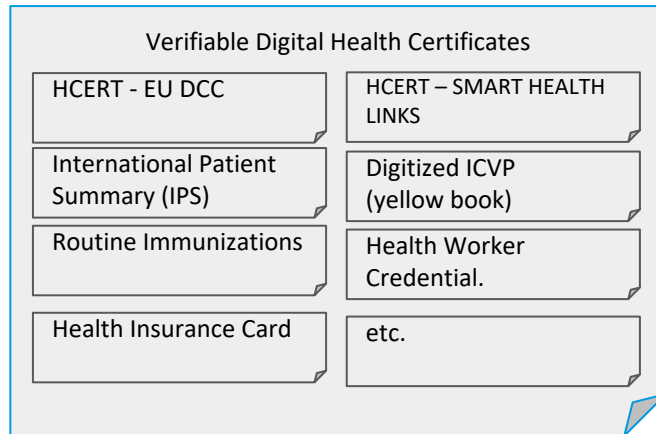
X = In progress. Currently going through technical preparation, testing and/or pending Letter of Application

X = Onboarding completed. Testing completed and Letter of Application received.

**77 participants
in total
as of
8 May 2024**

Global Digital Health Certification Network

– Individual-mediated exchange with consent

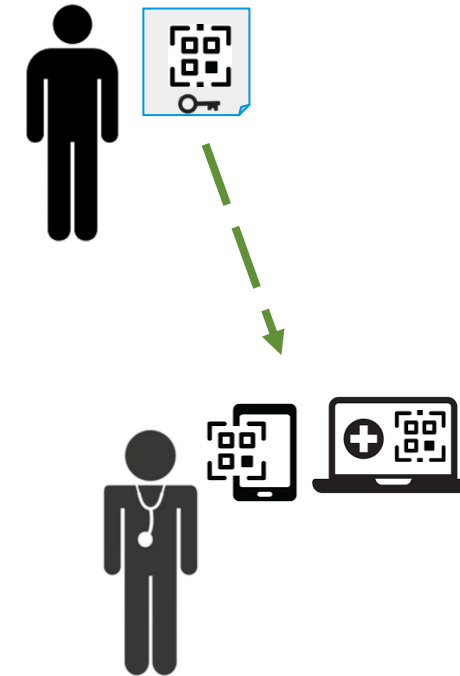


What digital public infrastructure do we need so that an individual present a digital health certificate, whose provenance can be verified, to a health worker?

Global Digital Health Certification Network

– Individual-mediated exchange with consent

Verifiable Digital Health Certificates	
HCERT - EU DCC	HCERT – SMART HEALTH LINKS
International Patient Summary (IPS)	Digitized ICVP (yellow book)
Routine Immunizations	Health Worker Credential.
Health Insurance Card	etc.



What digital public infrastructure do we need so that an individual present a digital health certificate, whose provenance can be verified, to a health worker?

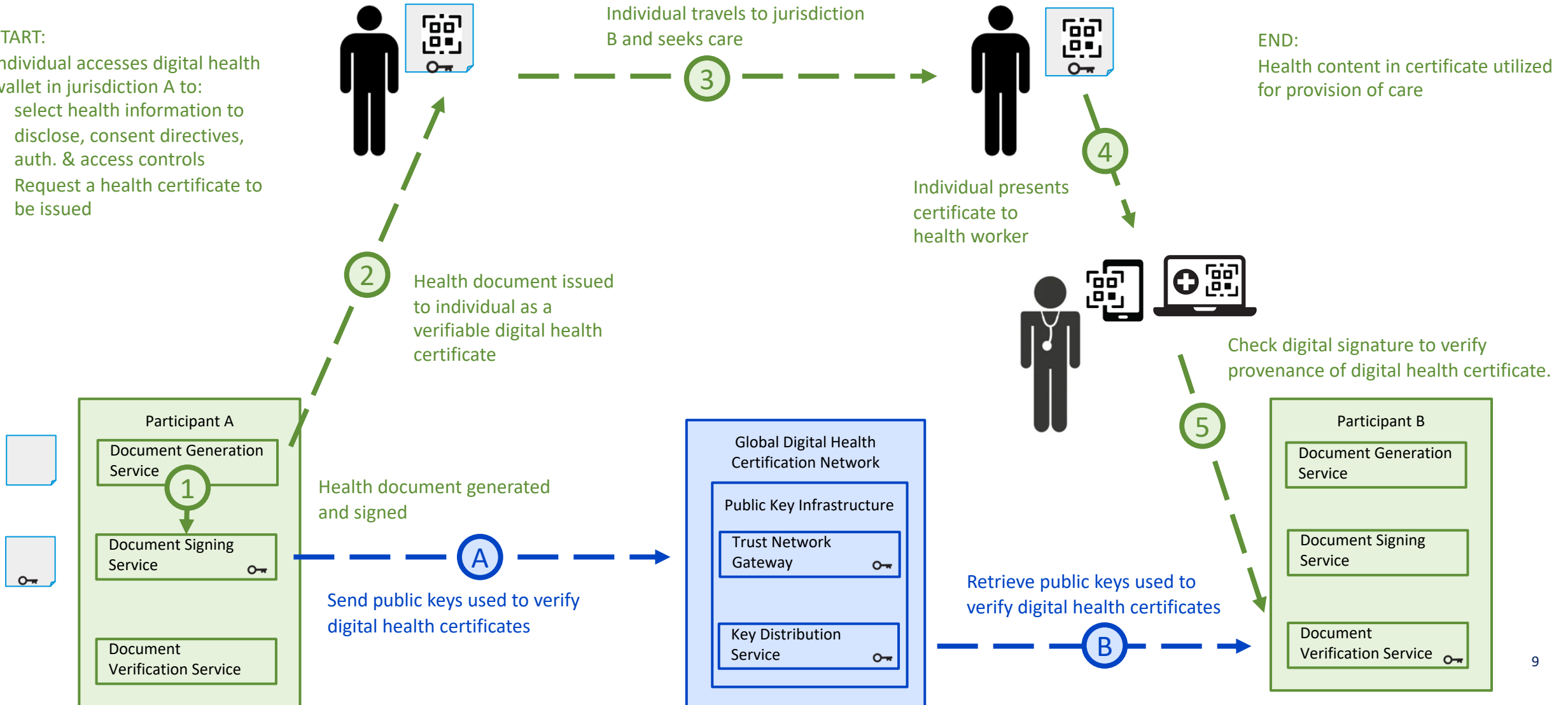
Global Digital Health Certification Network

– Individual-mediated exchange with consent

START:

Individual accesses digital health wallet in jurisdiction A to:

- select health information to disclose, consent directives, auth. & access controls
- Request a health certificate to be issued



END:
Health content in certificate utilized for provision of care



Pilgrim configures access to IPS via QR code on national health wallet

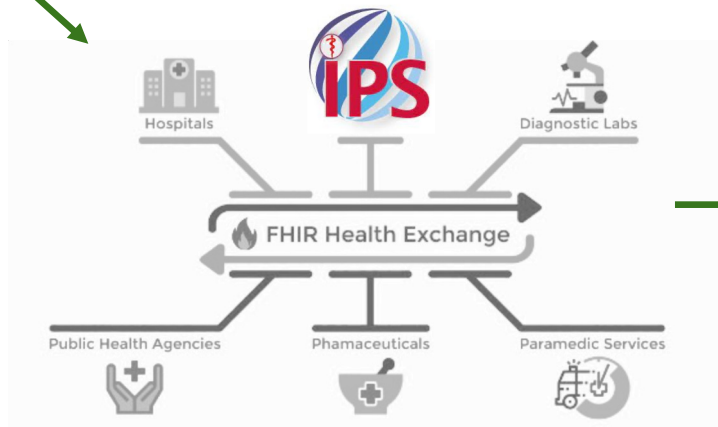


Pilgrim seeks care and shows IPS QR code to health worker



IPS generated from patient care history in origin country

Origin Country



EMR retrieves IPS from origin country HIE

Health worker scans IPS QR code in their EMR



KSA



IPS verification keys published to GDHCN



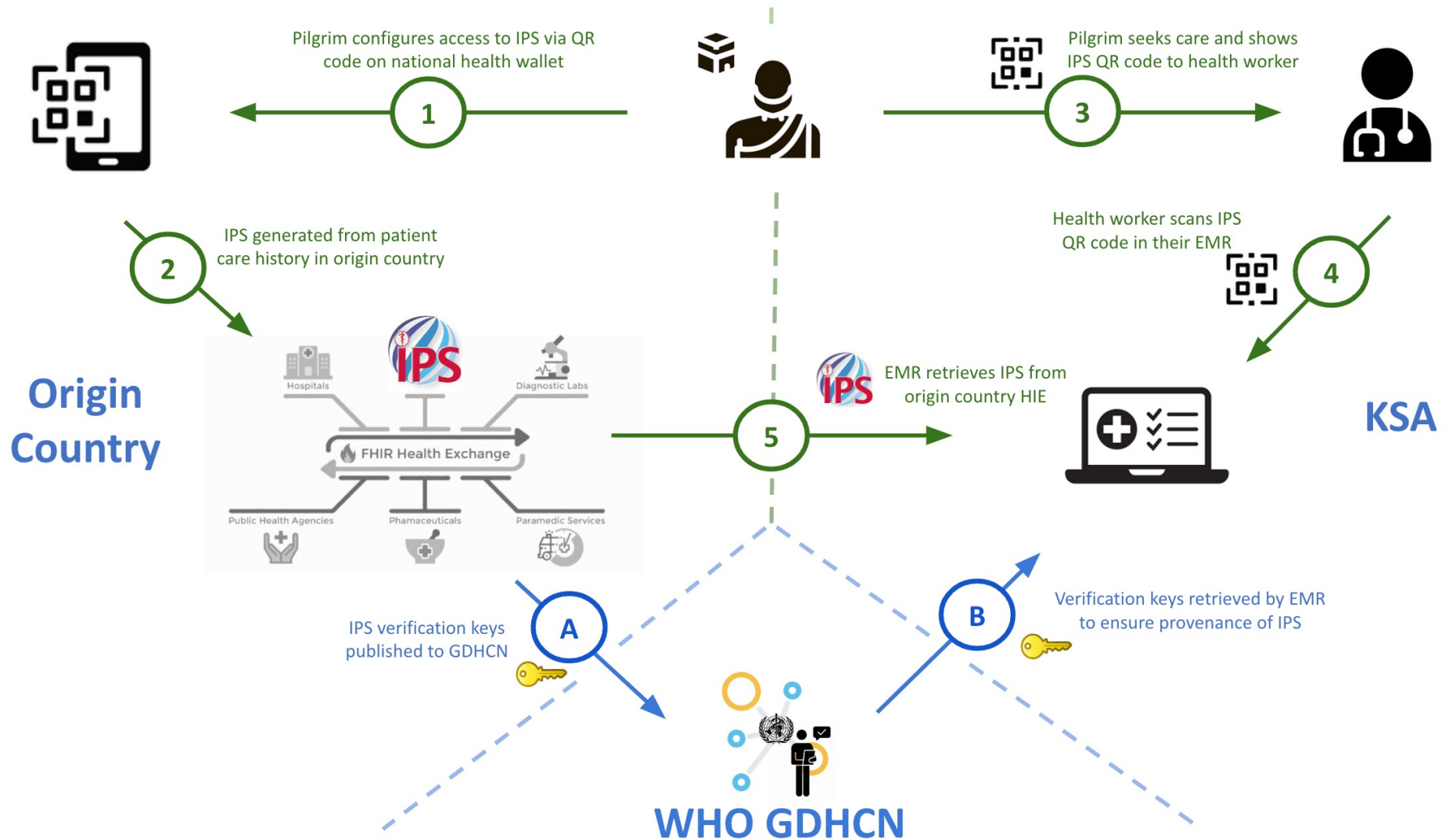
Verification keys retrieved by EMR to ensure provenance of IPS



WHO GDHCN



Pilgrims share health records using QR code on phone or ID badge



Global Digital Health Certification Network

– Hajj consent management

3.2.4 Health Assessment, Consent Counselling, and Issuance of Smart Health Link at Malaysia

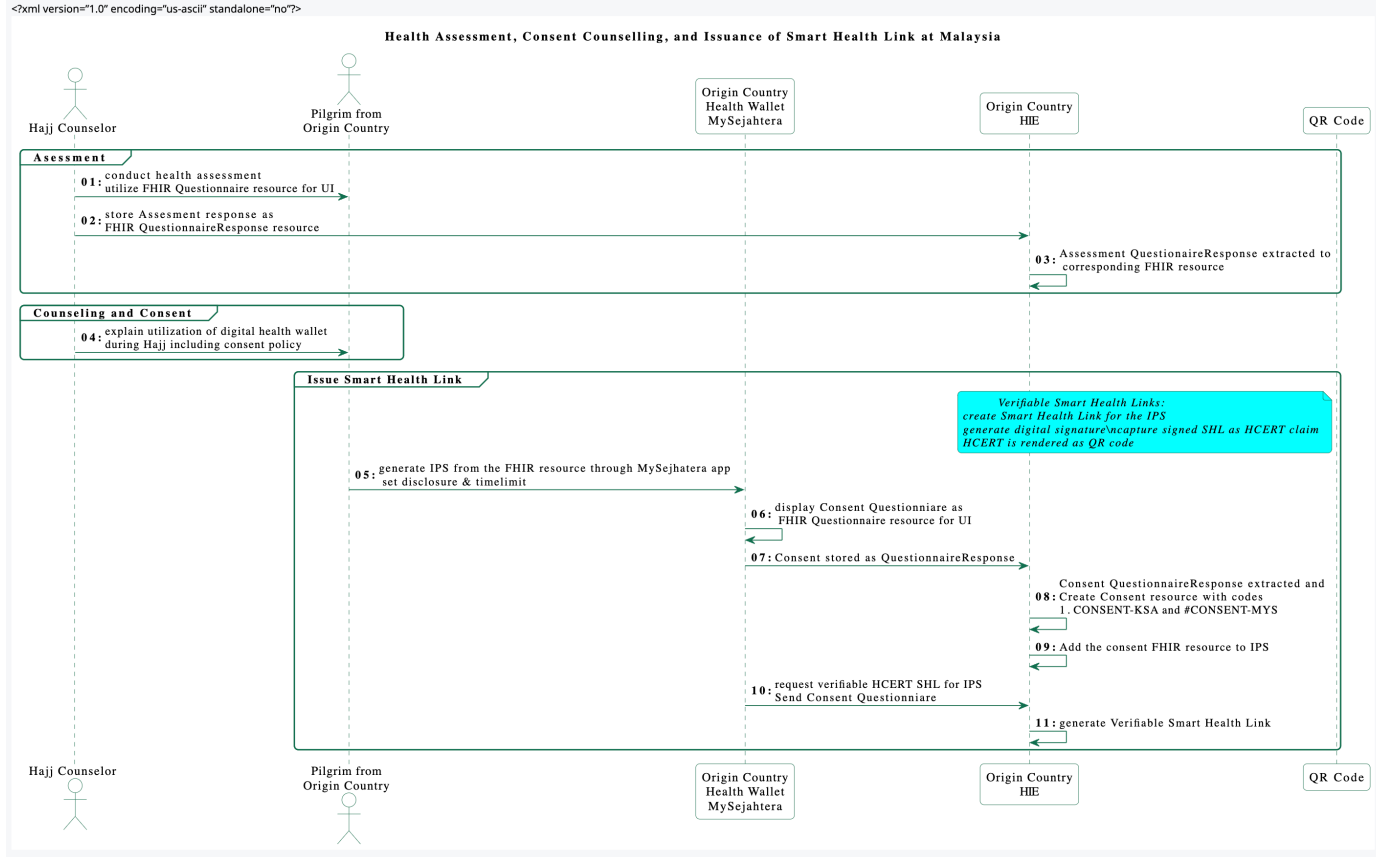


Table of Contents > Indices > Artifact Index > IPS.HAJJ.CONSENT CodeSystem

SMART Verifiable IPS for Pilgrimage, published by WHO. This guide is not an authorized publication; it is the continuous build for version 1.0.1 built by the FHIR (HL7® FHIR® Standard) CI Build. This version is based on the current content of <https://github.com/WorldHealthOrganization/smart-ips-pilgrimage> and changes regularly. See the [Directory of published versions](#)

Narrative Content XML JSON TTL

5.1.9.1 CodeSystem: IPS.HAJJ.CONSENT CodeSystem (Experimental)

Official URL: http://smart.who.int/ips-pilgrimage/CodeSystem/IPS.HAJJ.CONSENT	Version: 1.0.1
Active as of 2024-05-07	Computable Name: IPS_HAJJ_CONSENT

CodeSystem for IPS.HAJJ.CONSENT CodeSystem for utilization of IPS during Hajj

This Code system is referenced in the content logical definition of the following value sets:

- IPS_HAJJ_CONSENT

This case-insensitive code system <http://smart.who.int/ips-pilgrimage/CodeSystem/IPS.HAJJ.CONSENT> defines the following codes:

Code	Display	Definition
CONSENT-KSA	Consent for Kingdom of Saudi Arabia	The Pilgrim consents to share his/her International Patient Summary (IPS data) during the provision of clinical care at Ministry of Health-Saudi Arabia in Haj District area healthcare facilities through the Haj-1445 event as any follow up care that might be needed from any healthcare practitioners
CONSENT-IDN	Consent for Indonesia	<INSERT TEXT FROM INDONESIA: discuss pilgrims's consent to utilize Satushehat to enable access to KSA to their IPS if they are in need of care during Hajj>
CONSENT-MYS	Consent for Malaysia	The Malaysian Hajj pilgrim has provided consent for sharing the International Patient Summary (IPS) generated from the data recorded during the Hajj pilgrim health examination, as well as the vaccination records stored on MySejahtera to Kingdom of Saudi Arabia
CONSENT-OMN	Consent for Oman	<INSERT TEXT FROM OMAN: discuss pilgrims's consent to utilize Oman's e-Health Portal to enable access to KSA to their IPS if they are in need of care>



Global Digital Health Certification Network

A publish keys – EU API

B retrieve keys – EU API, DID



Table of Contents > Home > Concepts

This page is part of the Trust (v1.1.3: Release) based on FHIR (HL7® FHIR® Standard) R4. This is the current published version. For a full list of available versions, see the [Directory of published versions](#)

1.7 Concepts

1.7.0.1 Trust Lists

Universal verifier applications that support different credential standards are complicated by wide variability in format of the credential payloads, signatures, key formats, and key distribution methods. Public keys formats include x509 certificates, JSON Web Key Sets (JWKS), and DID documents. Signing key distribution methods include API gateways, hosted by issuer at a pre-defined URL, embedded in certificates, and by block-chain based resolution. Establishing root of trust by trust anchor or distributing trust list has been accomplished by API gateway, hosted URL, private dissemination and other bilateral sharing agreements.

While some variability is expected in an approach that preserves sovereignty, there are opportunities for alignment in key format and distribution for the sake of fostering interoperability. With that goal, we provide a unifying trust list format to assemble and share public key infrastructure for all credential specifications used by existing trust networks. Importantly, this format does not enforce a particular policy framework for participants of the trust network.

The GDHCN currently supports two means for key distribution of keys using trust lists

- EU DCC API required
- Decentralized Identifier (DID) optional

- [GDHCN Trust Network](#)
- [GDHCN Secretariat](#)
- [GDHCN Participant](#)
- [Eligible GDHCN Participant](#)
- [Terms of Participation \(TOP\)](#)
- [Business Owner Representative](#)
- [Key Master Representative](#)
- [Legal Representative](#)
- [Technical Representative](#)
- [Letter of Application](#)
- [Onboarding Process](#)
- [Health Professions Education Accreditation Agency](#)

Digital Documentation Covid Certificate Gateway

1.10.0 OAS3

openapi.json

The API defines how to exchange verification information for Digital Covid Certificates.

Apache 2.0

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

GDHCN

POST /trustedCertificate Uploads Trusted Certificate

POST /trust/reference Upload a new trusted reference

DELETE /trust/reference Delete a Trusted Reference

GET /trustList/references Returns the list of trusted issuers filtered by criteria.



IHE Digital Signatures



- IHE Digital Signature (DSG) profile currently supports XML digital signatures for document sharing
 - Leverage [XAdES](#), an European Telecommunications Standards Institute (ETSI) for XML digital signatures
 - Detached and Enveloping signatures, not Enveloped
- Gap in IHE DSG for JSON documents (preferred by many HL7 FHIR vendors)
 - Will leverage JAdES, the JSON equivalent of XAdES
- Current work underway to clarify how the International Patient Summary (IPS) and other HL7 FHIR documents should be signed.
- Draft for Public Comment ready being prepared for release next week
- Potential to test at IHE Europe, Trieste, Italy June 3-7

XAdES extends the IETF/W3CXML-Signature Syntax and Processing specification [\[XMLDSIG\]](#) into the domain of non-repudiation by defining XML formats for advanced electronic signatures that remain valid over long periods and are compliant with the European "Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures" [\[EU-DIR-ESIG\]](#) (also denoted as "the Directive" or the "European Directive" in the rest of the present document) and incorporate additional useful information in common use cases. This includes evidence as to its validity even if the signer or verifying party later attempts to deny (repudiates) the validity of the signature.

Key Links and Resources

Overview of the Global Digital Health Certification Network

<https://www.who.int/initiatives/global-digital-health-certification-network>

Onboarding process

https://smart.who.int/smart-trust/concepts_onboarding.html

Press release announcing the launch of the GDHCN and collaboration with the European Commission

<https://www.who.int/news/item/05-06-2023-the-european-commission-and-who-launch-landmark-digital-health-initiative-to-strengthen-global-health-security>

Secretariat email for onboarding

tng-secretariat@who.int

Secretariat email for technical support questions

tng-support@who.int

Technical specifications

<https://smart.who.int/smart-trust>

Thank you