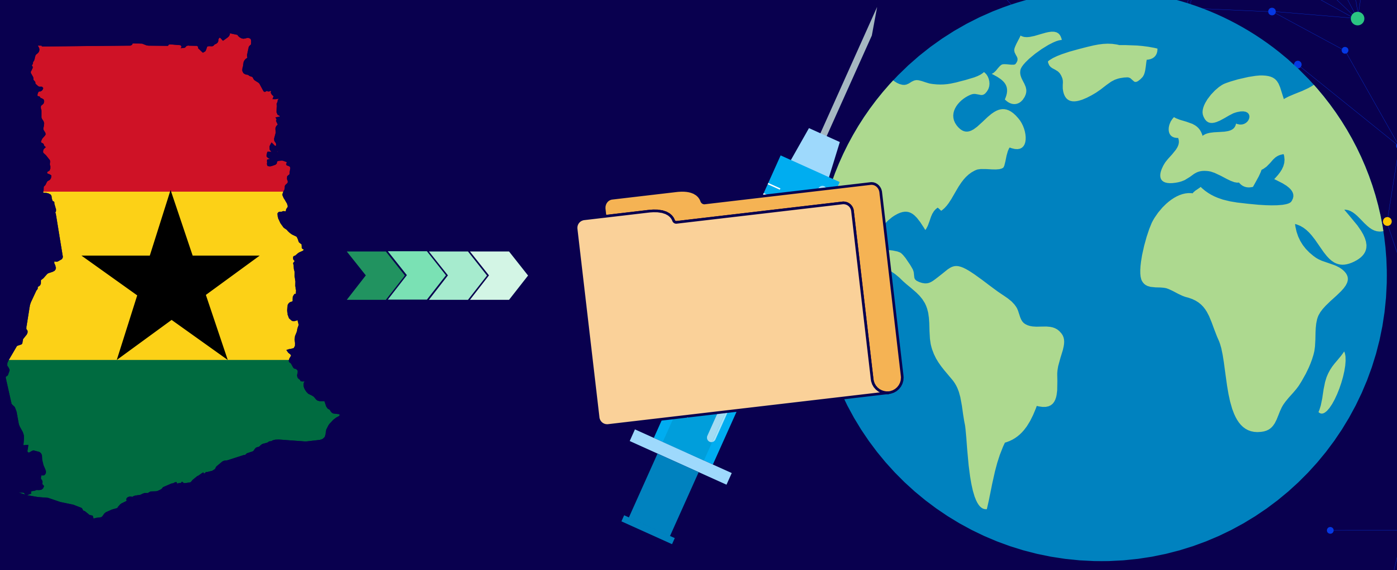
Data Economy

DIPC



Playbook:

Ghana’s integration into the WHO Global Digital Health Certification Network (GDHCN)

german cooperation
DEUTSCHE ZUSAMMENARBEIT

Implemented by
giz Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) GmbH

Co-funded by the European Union

PAHO Pan American Health Organization World Health Organization Americas Region

PATH

digital square

unicef

Regenstrief Institute

ROBERT KOCH INSTITUT

Published by:
Deutsche Gesellschaft für
Internationale Zusammenarbeit
(GIZ) GmbH

Registered offices:
Bonn and Eschborn
Friedrich-Ebert-Allee 32 + 36,
53113 Bonn, Germany
T +49 228 44 60-0
F +49 228 44 60-17 66

E: digital-health@giz.de
I: www.giz.de

Acknowledgement
Digital Square at PATH

DIPC - Digital Innovation in Pandemic Control:
dipc@giz.de / Tessa Lennemann

Design and layout:
Diego Narrea Sheen

URL links:
This publication contains links to external websites. Responsibility for the content of the listed external sites always lies with their respective publishers.

On behalf of:
German Federal Ministry for Economic Cooperation and Development (BMZ)

GIZ is responsible for the content of this publication.

Disclaimer:
The data in the publication has been collected, analysed and compiled with due care; and has been prepared in good faith based on information available at the date of publication without any independent verification. However, Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) GmbH does not guarantee the accuracy, reliability, completeness or currency of the information in this publication. GIZ shall not be held liable for any loss, damage, cost or expense incurred or arising by reason of any person using or relying on information in this publication.

Bonn and Eschborn, Germany
November 2025

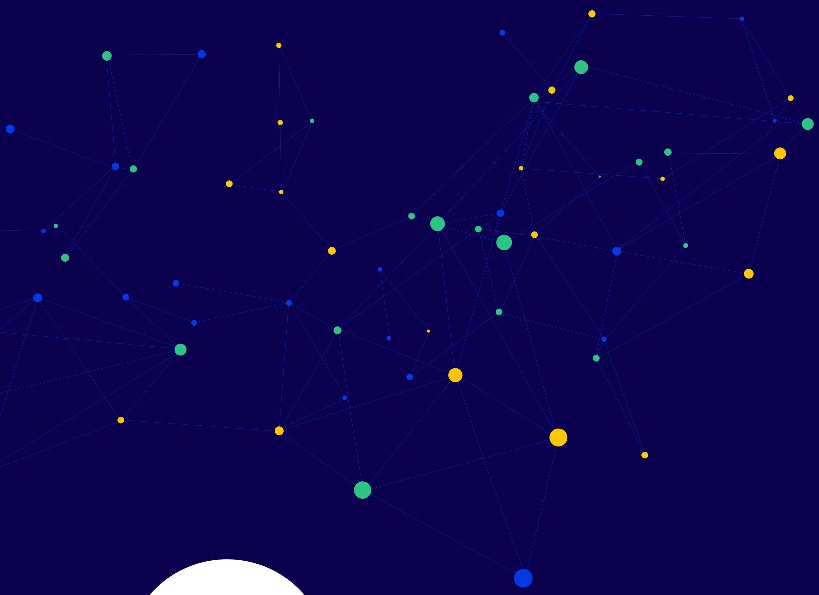


TABLE *of* CONTENTS

▶ **Chapter 1:** Overview of the Global Digital Heath Certification Network 04

▶ **Chapter 2:** A high-level glance at the playbook—the launchpad for Ghana's five key plays 13

P1 **Chapter 3:** Play 1—Governance and participation 21

P2 **Chapter 4:** Play 2—Operational procedures and management of certificates 27

P3 **Chapter 5:** Play 3—Technical infrastructure 44

P4 **Chapter 6:** Play 4—Integration with national systems and trust delegation 55

P5 **Chapter 7:** Play 5—Legal and regulatory considerations 66

▶ **Chapter 8:** Sealing the win—connecting Ghana to the Global Trust Network 72

← →

©alexander sinn/unsplash

CHAPTER

01 Overview of the Global Digital Heath Certification Network

Contents:

What is the GDHCN?
Why does the GDHCN matter?
What are core principles and uses of the GDHCN?
How does the GDHCN work?
GDHCN value proposition
Key terms

What is the GDHCN?

WHO-led digital trust architecture allowing for signing and verifying health certificates.

Facilitates authentication (i.e., provenance) of data and supports cross border data use.

Certificates (e.g., COVID-19, immunisation, health worker credentials) are digitally signed and trusted globally.

Why does *the* GDHCN matter?

In an increasingly interconnected world, **people, data, and diseases cross borders every day.** The GDHCN offers a way for countries to issue and sign digital health data (such as certificates or staff credentials) that are:

Globally trusted

Secure and tamper-proof

Privacy-preserving

Interoperable with other countries' systems

What are core principles *and* uses of the GDHCN?

Trust

Uses a Public Key Infrastructure (PKI) where each country or organisation is a trusted issuer. WHO serves as the trust anchor, maintaining a global registry and verifying participants' cryptographic keys. This allows Ghana's certificates to be recognised and trusted globally.

Privacy

Personal data stays within Ghana. Certificates are digitally signed but don't include personal identifiers unless required. WHO does not store or access any individual health data, supporting compliance with Ghana's Data Protection Act (2012) and ECOWAS privacy laws.

Interoperability

Built on global standards like W3C Verifiable Credentials, HL7® FHIR®, and ICAO travel specs, the system integrates easily with national tools—immigration systems, public health databases, and mobile apps.

Decentralisation

The network has no central controller. Each country manages its own keys, policies, and certificate issuance, while adhering to shared protocols to ensure interoperability and mutual trust.

GDHCN use cases

Authentication of personal health documents

Enables patients and providers to verify that digital health documents are authentic and issued by a trusted national system. For example, TB program patients in Ghana can present a QR code linking to a certified International Patient Summary (IPS) containing their treatment data.

International travel

Provides verifiable proof of vaccination, testing, or recovery to streamline border control, reduce fraud, and support safe mobility. A traveler with a digital certificate from GHS can have it instantly verified abroad—no need to access Ghana’s internal systems.

Routine immunisation and public health campaigns

Extends the GDHCN infrastructure to support certified childhood immunisation records, yellow fever certificates, and flu campaign documentation, ensuring accuracy and authenticity for care delivery.

Health worker credentials

Supports issuance of verifiable digital credentials for health professionals, improving hiring, license verification, and cross-border work. Aligns with ECOWAS and AU goals for professional mobility.

Digital continuity of care

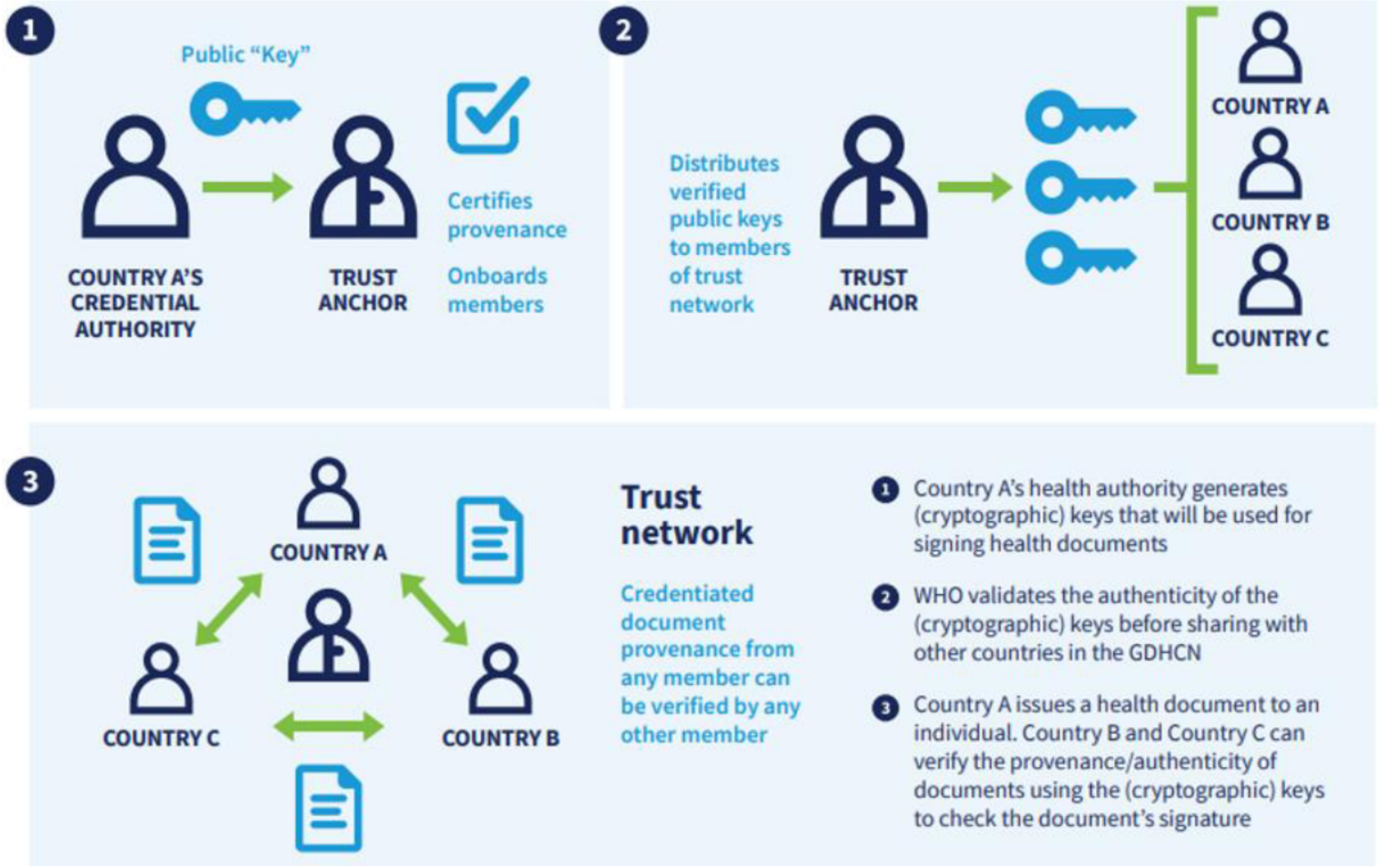
Allows Ghanaians to carry verifiable health credentials when traveling or seeking care abroad. Health providers across the network can validate documents without needing to contact Ghana directly.

Disaster preparedness and epidemic response

Facilitates rapid issuance and global verification of health documents during emergencies, enabling efficient and trusted public health responses.

Trust Framework:

Key Exchange and Verification Process


1
Public "Key"
COUNTRY A'S CREDENTIAL AUTHORITY
TRUST ANCHOR
Certifies provenance
Onboards members
2
Distributes verified public keys to members of trust network
TRUST ANCHOR
COUNTRY A
COUNTRY B
COUNTRY C
3
COUNTRY A
COUNTRY C
COUNTRY B
Trust network
Credentiated document provenance from any member can be verified by any other member

1. Country A's health authority generates (cryptographic) keys that will be used for signing health documents
2. WHO validates the authenticity of the (cryptographic) keys before sharing with other countries in the GDHCN
3. Country A issues a health document to an individual. Country B and Country C can verify the provenance/authenticity of documents using the (cryptographic) keys to check the document's signature

Image: https://smart.who.int/trust/

Why the GDHCN matters *for* Ghana

Strengthens Ghana's digital health ecosystem

By adopting open standards, trust mechanisms, and security protocols, Ghana builds a more modern and resilient digital health infrastructure.

Improves global trust and mobility

Citizens can travel with globally accepted health credentials. This improves access to work, study, and services abroad and positions Ghana as a forward-thinking digital health leader in the region.

Reduces fraud and improves public safety

Digitally signed certificates are tamper-proof and can be verified instantly, reducing risks of counterfeit documents and supporting national security.

Saves costs through open standards

GDHCN is built on open-source tools and standards, avoiding vendor lock-in. Ghana can leverage WHO-provided reference implementations to reduce time and development costs.

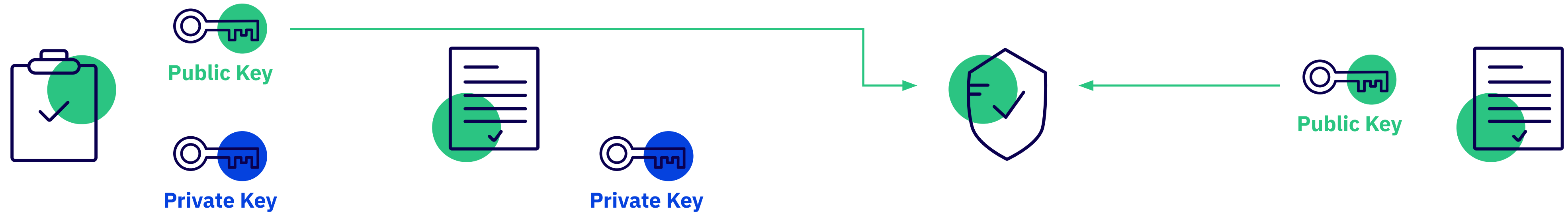
Scales with future use cases

The infrastructure supports long-term evolution, including integration with national ID, insurance, e-pharmacy, and digital health records systems.

Key terms

Term	Definition
GDHCN	**Global Digital Health Certification Network –** a WHO-led trust framework enabling cross-border verification of digital health certificates.
VDHC	**Verifiable Digital Health Certificate –** a digitally signed, tamper-proof certificate for vaccination, testing, recovery, or health worker credentials.
CSCA	**Country Signing Certificate Authority –** the national root certificate authority responsible for signing digital health certificates.
PKI	**Public Key Infrastructure –** a framework for managing digital keys and certificates for secure data exchange.
FHIR®	**Fast Healthcare Interoperability Resources –** a global standard for exchanging healthcare information electronically.
W3C VC	**World Wide Web Consortium Verifiable Credential –** a data model for issuing and verifying tamper-evident digital credentials.
UAT	**User Acceptance Testing –** a WHO-provided environment where countries test their GDHCN integration before going live.
TNG	**Trust Network Gateway –** WHO's central infrastructure for indexing and distributing metadata and public keys of participating entities.

Deep dive *on* Public Key Infrastructure



A Country A (e.g., a Ministry of Health) issues **digital certificates** to entities (e.g.: hospitals) in their country that confirms their identity. Country A generates public and private keys. Country A provides the public key to the GDHCN Public Key Directory (PKD).

Country A’s authorised entity issues a digital health document (e.g., proof of vaccination), using its **private key** to create a **digital signature** for that certificate.

The signature ensures that:

- The document **has not been tampered with** (integrity).
- The document **truly comes from** an authorised issuer (authenticity).

GDHCN’s PKD is a trusted registry that contains the public keys of all trusted member countries and the network.

The **WHO acts as the Trust Anchor,** ensuring that all members follow agreed verification and security standards.

In Country B:
When someone presents their digital health document for verification (e.g., at an airport, at a health facility), the verifier uses the issuer’s public key (retrieved from the GDHCN PKD) to cheque the signature.

If the signature is valid the verifier can trust the data.

Digital certificate: proves the issuer’s identity and provides the public key

Digital signature: proves the message was created by that issuer and hasn’t been altered

©Jonas Jacobsson /Unsplash

CHAPTER

02

A High-Level Glance at the Playbook—the Launchpad for Ghana's Five Key Plays

Contents:

What is the playbook's purpose?

What is the playbook's scope and who is the target audience?

How the playbook aligns with WHO's Global Digital Health Strategy 2025?

The five essential moves to build digital trust

DISCLAIMER!

This playbook is intended to be **adapted to local contexts,** and **final decisions should be made by each country.** It offers guidance and is intended as a helpful resource to translate complex technical concepts involving multiple stakeholders into actionable steps.

What is the playbook's purpose?

Provides a national roadmap for onboarding, implementing, and operating within WHO's GDHCN.

Outlines the technical, legal, and governance structures required to issue, verify, and manage verifiable digital health certificates (VDHCs).

Ensures alignment with WHO standards for compliance, privacy, and interoperability.

Builds a strong foundation for digital public goods and long-term digital health capacity.

Lays the foundation for future use cases such as verification of vaccine certificates, health workforce credentialing and ultimately, cross-border travel.

What is the playbook's scope and who is the target audience?

Policy & Regulatory Leaders:

NITA, Cyber Security Authority, Data Protection Commission (DPC)

Technical Teams:

Government IT units, developers, health informatics teams

Health Authorities:

MOH, Ghana Health Service (GHS), public and private providers

Legal and Compliance Experts:

Specialists ensuring alignment with Ghana's Data Protection Act and cybersecurity laws

Development Partners:

WHO country office, GIZ, UNICEF, UNDP, and other digital health supporters

The playbook covers policy, technology, operations, security, onboarding processes, and public communication strategies, enabling both high-level coordination and practical implementation at the service delivery level.

AUDIENCES

We encourage all audiences to read the full playbook. However, certain chapters offer particularly relevant guidance depending on your role. While **Chapters 1, 2, and 8** provide essential context for everyone, the sections below highlight where specific audiences may want to focus additional attention.

Policy & Regulatory Leaders:

This playbook offers step-by-step guidance for national digital health authorities on engaging with and joining the WHO Global Digital Health Certification Network (GDHCN). It clarifies policy requirements, governance structures, and coordination processes needed to support national participation in a globally trusted framework.

Key Chapters:

- **Chapter 3 – Play 1:** Governance and Participation
- **Chapter 4 – Play 2:** Operational Procedures and Management of Certificates
- **Chapter 7 – Play 5:** Legal and Regulatory Considerations

Technical Teams:

For system architects and technical implementers, the playbook provides practical, actionable guidance on meeting the technical specifications and interoperability standards required for GDHCN participation. It outlines integration pathways, testing procedures, and system readiness steps to support alignment with WHO's digital trust architecture.

Key Chapters:

- **Chapter 4 – Play 2:** Operational Procedures and Management of Certificates
- **Chapter 5 – Play 3:** Technical Infrastructure
- **Chapter 6 – Play 4:** Integration with National Systems and Trust Delegation

Health Authorities:

Health authorities will find support for planning and overseeing the national process of joining the GDHCN. The playbook explains roles, responsibilities, and implementation milestones across the health system to ensure digital certification efforts are well-governed, secure, and aligned with national priorities.

Key Chapters:

- **Chapter 3 – Play 1:** Governance and Participation
- **Chapter 4 – Play 2:** Operational Procedures and Management of Certificates

AUDIENCES

We encourage all audiences to read the full playbook. However, certain chapters offer particularly relevant guidance depending on your role. While **Chapters 1, 2, and 8** provide essential context for everyone, the sections below highlight where specific audiences may want to focus additional attention.

Legal and Compliance Experts:

Legal and compliance teams will find detailed guidance on regulatory requirements, data protection considerations, and trust framework obligations for GDHCN participation. The playbook supports assessment of legal readiness, identification of required policy updates, and harmonisation of national frameworks with WHO standards.

Key Chapters:

- **Chapter 6 – Play 4:** Integration with National Systems and Trust Delegation
- **Chapter 7 – Play 5:** Legal and Regulatory Considerations

Development Partners:

For development partners and funders, the playbook outlines where targeted support can accelerate national participation in the GDHCN. It highlights priority investment areas, alignment opportunities, and coordination mechanisms that strengthen interoperability and advance global digital trust.

Key Chapters:

- **Chapter 4 – Play 2:** Operational Procedures and Management of Certificates
- **Chapter 5 – Play 3:** Technical Infrastructure
- **Chapter 6 – Play 4:** Integration with National Systems and Trust Delegation

The playbook aligns with WHO's Global Digital Health Strategy 2025 by advancing its four strategic objectives in Ghana:

01

STRATEGIC OBJECTIVE 1: Promote global collaboration and advance the transfer of knowledge on digital health. Ghana's alignment with WHO standards and participation in GDHCN reinforces regional and international collaboration, ensuring compatibility with global systems for health security, travel, and care continuity.

02

STRATEGIC OBJECTIVE 2: Advance the implementation of national digital health strategies. By formalising roles, procedures, and technologies required for certificate issuance and verification, this playbook contributes to operationalizing Ghana's national eHealth policy and related frameworks.

03

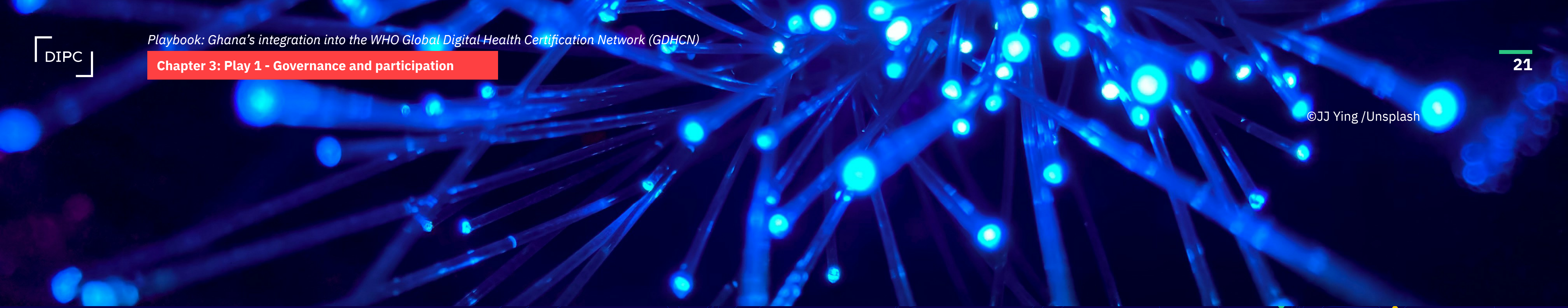
STRATEGIC OBJECTIVE 3: Strengthen governance for digital health at national and global levels. The playbook establishes a robust governance structure, assigning clear responsibilities for certificate management, public key infrastructure (PKI) operations, and oversight in compliance with international norms.

04

STRATEGIC OBJECTIVE 4: Advocate for people-Centered Health Systems Enabled by Digital Health. Through secure, privacy-preserving digital certificates, Ghana empowers citizens with greater control over their health data, while improving the transparency, security, and accessibility of health services.

The following chapters unpack **five strategic plays** essential for implementing trusted, interoperable, and inclusive digital health systems:

- **P1** **Play 1:** Governance and participation
- **P2** **Play 2:** Operational procedures and management of certificates
- **P3** **Play 3:** Technical infrastructure
- **P4** **Play 4:** Integration with national systems and trust delegation
- **P5** **Play 5:** Legal and regulatory considerations



©JJ Ying /Unsplash

CHAPTER

03

PLAY 1

Overview of the Global Digital Heath Certification Network

This chapter details how Ghana must set up a multi-agency governance model, formalise roles for MOH, GHS, NITA, DPC, and other stakeholders, and comply with WHO's participation requirements. It covers the process for joining GDHCN, including letters of application, technical readiness, and policy compliance. It also explains global participation, working groups, and the responsibilities for maintaining the playbook.

Contents:

WHO as trust anchor

Participation requirements for Ghana

National governance model overview

Global participation and detailed role descriptions of national actors involved in governance

WHO serves as the **neutral** and **authoritative** trust anchor of GDHCN.

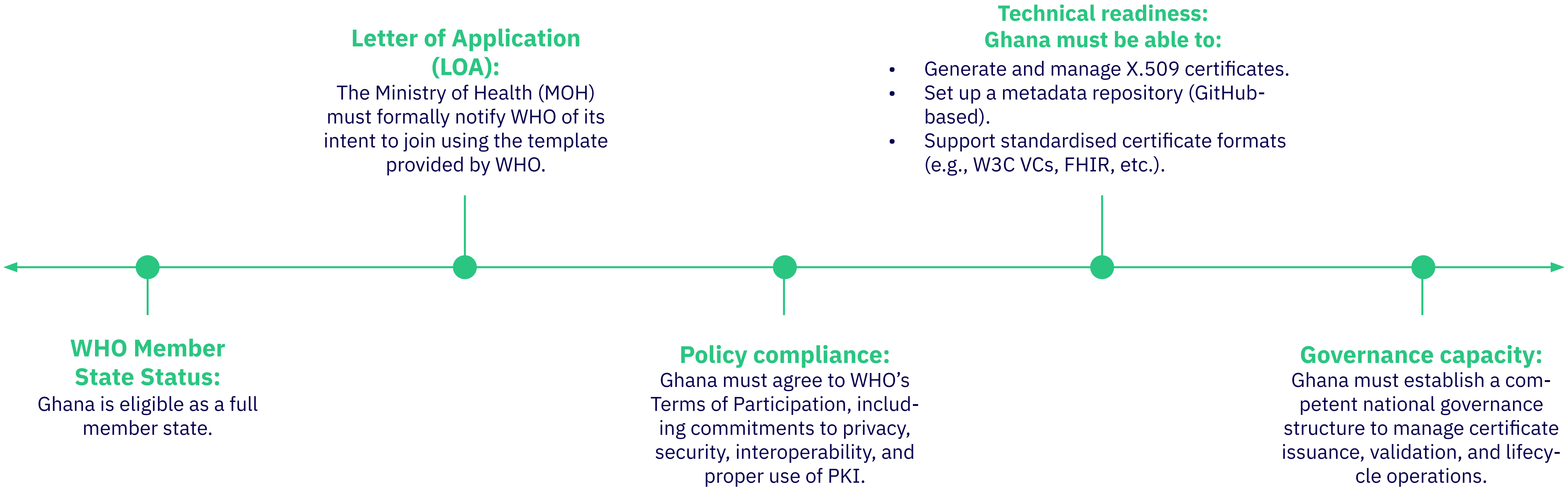
WHO's responsibilities

- Maintains Trust Network Gateway (TNG), a global registry of verified issuers. Structure ensures global interoperability and trust among participating entities, without compromising national data sovereignty.
- Verifies cryptographic keys and policies, enabling countries to be in full control of their data and operations.
- Provides technical assistance, onboarding guidance, and tools such as participant templates on GitHub for onboarding and UAT environments to validate integration before going live.

What WHO does not do

- Issue certificates.
- Store personal data.

By completing these nationally led steps, Ghana becomes eligible to in the WHO Global Digital Health Certification Network (GDHCN).



WHO Member State Status:
Ghana is eligible as a full member state.

Letter of Application (LOA):
The Ministry of Health (MOH) must formally notify WHO of its intent to join using the template provided by WHO.

Policy compliance:
Ghana must agree to WHO's Terms of Participation, including commitments to privacy, security, interoperability, and proper use of PKI.

**Technical readiness:
Ghana must be able to:**

- Generate and manage X.509 certificates.
- Set up a metadata repository (GitHub-based).
- Support standardised certificate formats (e.g., W3C VCs, FHIR, etc.).

Governance capacity:
Ghana must establish a competent national governance structure to manage certificate issuance, validation, and lifecycle operations.

National governance structure

To effectively manage its role in the GDHCN, Ghana will need to adopt a multi-agency governance model with defined responsibilities.

Multi - agency roles in GDHCN governance

MOH

Provides national policy leadership, signs participation agreements, and serves as the official liaison with WHO.

GHS

Leads operational implementation across health facilities, oversees certificate issuance, and trains healthcare providers.

NITA

Manages digital infrastructure, public key infrastructure (PKI), cybersecurity standards, and GitHub repository hosting.

DPC

Ensures adherence to Ghana's Data Protection Act (Act 843) and advises on international privacy and data-sharing standards.

Public and private health facilities

Act as points of certificate generation and verification; provide user education and front-line support.

Accredited laboratories and testing centers

Supply verified health data for diagnostic or test-based certificates, integrated with national systems.

Global participation

At the international level, Ghana will participate in GDHCN technical and governance working groups, share feedback to help shape future protocols and use cases, and collaborate with other countries and WHO on cross-border interoperability. All WHO member states are eligible to participate in the working groups and can contact the secretariat directly using gdhcn-secretariat@who.int.

WHO remains the global coordinator and validator, while all day-to-day operations remain within Ghana's national control.

MOH

- Acts as the designated authority representing Ghana to WHO.
- Carries the responsibility and authority to sign the Letter of Intent and Terms of Participation.
- Oversees national legal and policy frameworks for GDHCN integration.
- Mobilises resources and coordinates cross-sector stakeholders.

NITA

- Serves as the technical lead for system integration and digital infrastructure.
- Manages Ghana's certificate authority (CA) and key lifecycle.
- Hosts and updates the public GitHub repository containing certificates and metadata.
- Ensures cybersecurity controls are in place and updated regularly.

GHS

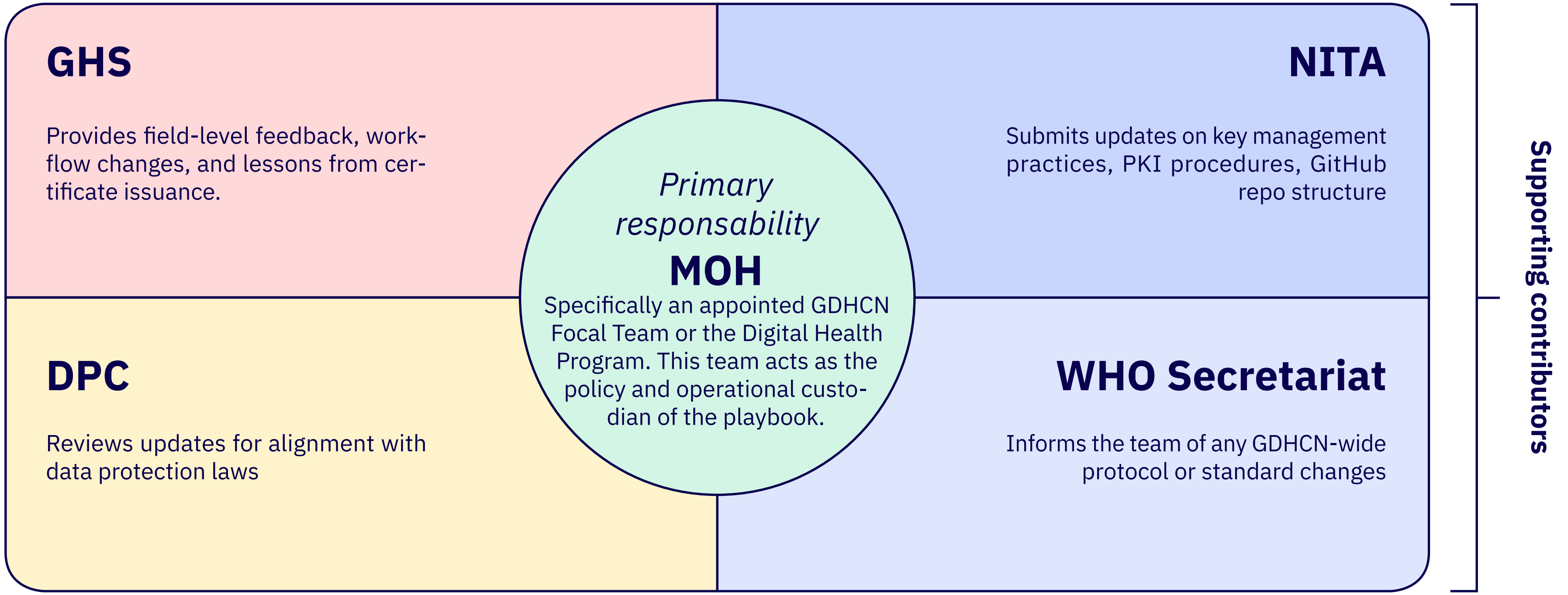
- Leads the on-ground implementation of GDHCN enabled tools across hospitals, testing
- centers, and immunisation campaigns.
- Trains clinical and administrative staff in the use of digital health certificates (in systems such as health wallets).
- Monitors certificate issuance practices and ensures data quality.

DPC

- Provides legal oversight to ensure that health data usage complies with Ghana's Data
- Protection Act.
- Advises on cross-border data sharing agreements and public communication about data rights.

Certifying bodies (e.g., labs, immunisation clinics)

- Collects and verifies data before digital certificate issuance.
- Ensures the accuracy, validity, and privacy of patient information.
- Reports certificate usage statistics and operational metrics to the MOH.



GHS

Provides field-level feedback, workflow changes, and lessons from certificate issuance.

NITA

Submits updates on key management practices, PKI procedures, GitHub repo structure

Primary responsability

MOH

Specifically an appointed GDHCN Focal Team or the Digital Health Program. This team acts as the policy and operational custodian of the playbook.

DPC

Reviews updates for alignment with data protection laws

WHO Secretariat

Informs the team of any GDHCN-wide protocol or standard changes

Supporting contributors

Whose responsibility is it to own and maintain the playbook?

©Árpád Czapp/Unsplash

CHAPTER

04

PLAY 2

Operational Procedures and Management of Certificates

This chapter covers the operational steps for onboarding, designating focal points, preparing documentation, and managing the certificate lifecycle. It outlines the roles of key stakeholders, the onboarding process, user acceptance testing (UAT), and post-go-live support. It also describes how Ghana will verify certificates from other countries and the responsibilities of border control, aviation, and health authorities.

Contents:

Governance and roles

Required documentation and focal point designation

Onboarding process

Go-live and post-go-live support

Ghana's participation in the GDHCN requires strong national leadership and a clear governance structure. This coordinated model ensures operational readiness, alignment with WHO standards, and long-term sustainability. The roles of each of the four lead issuance stakeholders must be formalised and coordination mechanisms established before onboarding begins.

01 National GDHCN Lead Authority – MOH

Role: National coordinator and WHO liaison

- Aligns GDHCN with national health policies and universal health care (UHC) goals.
- Coordinates cross-sector partners (public/private).
- Submits formal documentation (e.g., LOI, Terms of Participation).
- Leads national launch and communications.

02 Technical Implementation Lead – National Information Technology Agency (NITA)

Role: Implements GDHCN in health facilities.

- Builds and maintains systems for certificate issuance and verification.
- Manages Public Key Infrastructure (PKI) lifecycle.
- Hosts national trust repository (GitHub).
- Ensures cybersecurity compliance.
- Interfaces with WHO on specs and testing.

03 Clinical and Public Health Lead – Ghana Health Service (GHS)

Role: Implements GDHCN in health facilities.

- Deploys workflows in immunisation/ testing sites.
- Trains providers on certificate use and data security.
- Integrates data with DHIMS2 and EMRs.
- Monitors feedback and service KPIs.

04 Legal Oversight – Attorney General's Dept. / Data Protection Commission (DPC)

Role: Ensures legal and regulatory compliance

- Reviews policies for alignment with Data Protection Act (Act 843).
- Supports lawful cross-border data sharing.
- Validates digital signatures and legal trust chain.
- Provides guidance on redress and user protections.

In addition to key issuance stakeholders for health information certification, Ghana will also have to outline roles and governance for verification stakeholders since joining the GDHCN means that Ghana will be able to verify certificates issues in other countries that are part of the GDHCN.

01 Ministry of Foreign Affairs

Role: Oversees international verification processes (i.e., verification lead).

- Coordinates with foreign governments for mutual recognition of GDHCN certificates.
- Manages diplomatic communications regarding health certifications.
- Ensures compliance with international travel and health regulations.

02 Ghana Immigration Service (Border Control)

Role: Implements verification at entry points (i.e., verification support).

- Trains border officers on digital certificate verification procedures.
- Integrates GDHCN verification systems at land borders and seaports.
- Monitors compliance with health-related entry requirements.

03 Ghana Civil Aviation Authority (GCAA)

Role: Facilitates verification at airports (i.e., verification support).

- Coordinates with health and border agencies for on-site verification workflows.
- Supports integration of GDHCN systems at airport checkpoints.
- Identifies responsible units for verifying yellow fever and other health certificates.

1.
Letter of application

Signed by the Ministry of Health (MOH), the letter of application initiates the onboarding process and must:

- Affirm Ghana's intent to join the GDHCN.
- Identify designated national focal points (technical and policy).
- Outline Ghana's capacity to meet technical, legal, and operational requirements.
- Request onboarding support and user acceptance testing.

Letter of application led by MOH, template available here

2.
Terms of participation (TOP)

A WHO-issued agreement that outlines:

- Governance principles and mutual responsibilities.
- Use of global standards (e.g., W3C Verifiable Credentials, ICAO DCC, HL7 FHIR).
- Commitments to trust, transparency, and certificate integrity.
- Protocols for updates, revocation, and audit cooperation.

This serves as the binding contract between WHO and Ghana.

TOP coordinated between WHO Secretariat and MOH

3.
National digital health policy reference

Ghana must cite relevant national strategies and legal frameworks, including:

- The national eHealth strategy and digital health policy.
- Data Protection Act (2012), Cybersecurity Act, and Health Professions Regulatory Laws.
- Frameworks for interoperability, data governance, and digital health systems.

This provides WHO with context on Ghana's digital health maturity and regulatory alignment.

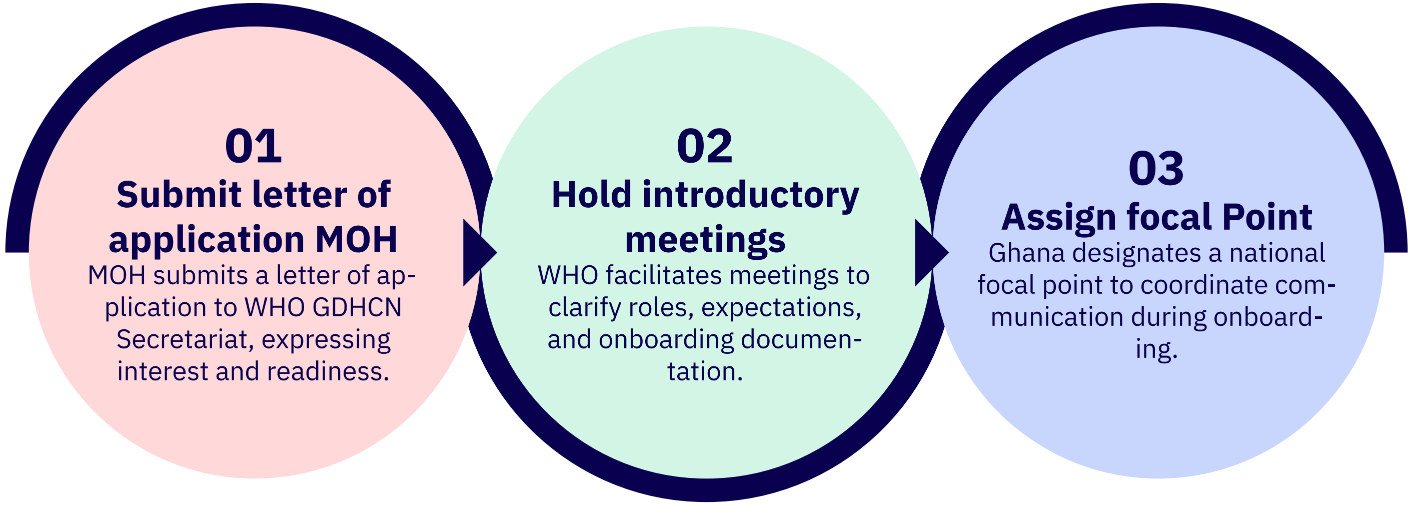
Policy reference led by MOH with support from GHS and DPC

4.
Certificate policy (CP) and certificate practice statement (CPS)

These technical documents define how Ghana's certificate authority (CA) will:

- Issue, manage, and revoke digital certificates.
- Secure private key storage and authentication processes.
- Ensure compliance with X.509 standards and WHO trust metadata requirements.
- Maintain and publish up-to-date versions via Ghana's GitHub metadata repository.

CP and CPS led by MOH with support from NITA



01
Submit letter of application MOH
MOH submits a letter of application to WHO GDHCN Secretariat, expressing interest and readiness.

02
Hold introductory meetings
WHO facilitates meetings to clarify roles, expectations, and onboarding documentation.

03
Assign focal Point
Ghana designates a national focal point to coordinate communication during onboarding.

Approaching WHO:

Pre-Onboarding Consultation

Before integration, Ghana should engage in a 3-step pre-onboarding consultation with the WHO GDHCN Secretariat.

Once the three steps are completed, WHO provides these resources to support onboarding:

- WHO onboarding guides.
- Standard certificate formats.
- GitHub repository templates.
- WHO-hosted test environments.

Ideal profile of national focal point	Key responsibilities
• Policy and governance knowledge. • Health system understanding. • Digital health/informatics fluency. • Diplomatic and interagency communication. • Technical literacy (PKI, FHIR, etc.).	• Coordinate onboarding with WHO (TOP, GitHub repo, metadata). • Ensure alignment across MOH, GHS, NITA, and DPC. • Support legal review of TOP and data policies. • Connect WHO with technical teams for implementation.

Option 1: Ministry of Foreign Affairs / Health Attaché'

- Best suited when International coordination and diplomatic recognition are central to GDHCN rollout.
- Leverages existing expertise in cross- border health documentation and travel protocols.
- Facilitates alignment with consular services and global health verification standards.
- Strengthens Ghana's representation in international health diplomacy and certificate recognition.

Option 2: MOH Senior Digital Health/eHealth Director

- Best suited if the MOH leads national digital health programs.
- Has political clout to coordinate GHS, NITA, DPC, etc.
- Already represents Ghana in global health tech platforms (e.g., WHO, AU, Smart Africa).

Option 3: GHS Director for Health Informatics/Public Health IT

- More hands-on, with deeper knowledge of data flows from immunisation, testing, and care delivery systems.
- Ideal if technical integration and coordination with labs/clinics is the bigger challenge.

Option 4: Hybrid: dual-point model

- A MOH policy lead (official national focal point) paired with a GHS or NITA technical focal point.
- This mirrors WHO's recommendation to designate a primary and a technical contact.

The step-by-step GDHCN onboarding process and timeline (approximation)

Step	Activity	Responsible	Est. duration	Dependencies
1. Prepare and coordinate internally	Appoint focal points, align MOH, GHS, NITA, legal, confirm intent.	MOH	2–4 weeks	Internal leadership and legal readiness.
2. Submit LOI to WHO	Formal submission and response.	MOH, led by assigned Ghana focal point(s)	1–2 weeks	None
3. Receive WHO onboarding pack	WHO sends TOP, GitHub templates, guides.	WHO	1 week	LOI submitted.
4. Complete key generation and policy draughting	Generate CSCA/TLS certs, draught CP/CPS.	MOH, with support from NITA, GHS, and DPC	2–3 weeks	NITA and legal teams.
5. Setup Metadata and GitHub repository	Configure JSON, publish certificates.	Led by NITA, approved by MOH	1–2 weeks	Keys must be ready.
6. Undergo WHO metadata review	WHO validates GitHub, provides feedback.	WHO	1–2 weeks	Metadata uploaded.
7. Conduct UAT with WHO	Connect to test environment, validate signing/verification.	Technical focal point from LOA	2–4 weeks	Systems/development teams in place.
8. Issue production keys	Generate and submit final certificates for go-live.	Technical focal point from LOA	1 week	UAT passed.
9. Go live ("switch on")	WHO publishes metadata to Trust Gateway.	WHO	1 week	Final certificates validated.

Internal Ghana (in-country steps) in support of setting up internal GDHCN compliance

These are key steps countries need to undertake to internally align to the GDCHN

1. Establish certificate authority (CA) and governance

1.1 Designate a national CA, usually under NITA, and generate root certificates for signing Verifiable Digital Health Certificates (VDHCs).

1.2 Define operational procedures for key management, renewal, and revocation.

1.3 Draught and approve CP and CPS

2. Prepare metadata repository

2.1 Create a public GitHub repository using WHO's Trust Network Gateway Participant Template.

2.2 Upload the following:
- X.509 certificates (CSCA and TLS).
- Metadata in JSON format, including country name, expiration, key ID, and other requested information.
- Country contact information and public trust details.

3. WHO metadata validation

3.1 WHO reviews the GitHub repository for compliance and technical accuracy.

3.2 Ghana may be asked to revise metadata to meet formatting or policy requirements.

4: Perform acceptance testing (UAT Phase)

4.1 Ghana connects to the WHO UAT environment via the TNG.

4.2 Execute the following:
- Endpoint reachability and secure connection test.
- Certificate validation test (sample VDHCs).
- Signature and cryptographic compliance checks.

4.3 WHO provides feedback and error logs. Ghana iterates as needed.

Governance and roles | Required documentation and focal point designation | **Onboarding process** | Go-live and post-go-live support

Who is involved in User Acceptance Testing (UAT)?

WHO GDHCN technical team

Acts as the technical verifier and gatekeeper for GDHCN compliance.

- Provides the UAT test environment, guidance, sample certificates, and trust gateway.
- Validates:
  - Ghana's certificate metadata and key usage.
  - Signature integrity.
  - Adherence to standards (e.g., FHIR, VC, JSON schemas).

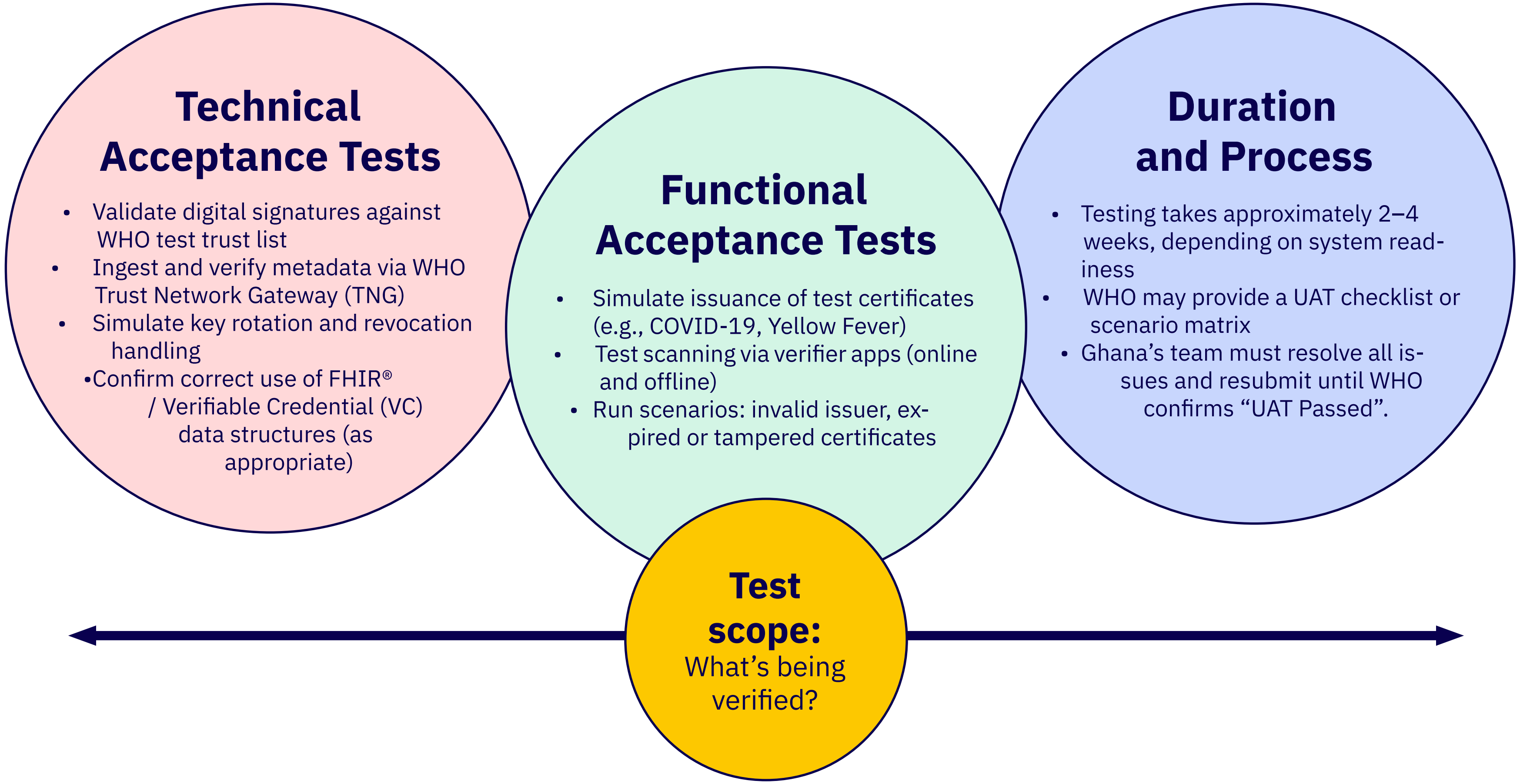
Ghana's National UAT team

- Cross-functional team with both technical and functional testers.
- Lead Coordinating Agency:
  - NITA (or MOH/National Digital Health Program Unit).
  - Leads UAT planning, coordination, and reporting.

Required roles

Role	Responsible entity*	Responsibilities
PKI/Metadata manager	NITA	Manages CSCA keys, GitHub repo, TLS setup
Issuance system owner	GHS / MOH	Runs test issuance platform (e.g., DIVOC or national system)
QA/Test engineer	MOH/NITA	Executes test cases, logs issues
Interoperability lead	GHS / MOH	Ensures FHIR/VC compliance, correct data mapping
WHO liaison/Focal point	MOH	Facilitates back-and-forth with WHO

***Note:** This information is provided as guidance only. This playbook is intended to be adapted to local contexts, and final decisions are made by each country.



Technical Acceptance Tests

- Validate digital signatures against WHO test trust list
- Ingest and verify metadata via WHO Trust Network Gateway (TNG)
- Simulate key rotation and revocation handling
- Confirm correct use of FHIR® / Verifiable Credential (VC) data structures (as appropriate)

Functional Acceptance Tests

- Simulate issuance of test certificates (e.g., COVID-19, Yellow Fever)
- Test scanning via verifier apps (online and offline)
- Run scenarios: invalid issuer, expired or tampered certificates

Duration and Process

- Testing takes approximately 2–4 weeks, depending on system readiness
- WHO may provide a UAT checklist or scenario matrix
- Ghana's team must resolve all issues and resubmit until WHO confirms "UAT Passed".

Test scope: What's being verified?

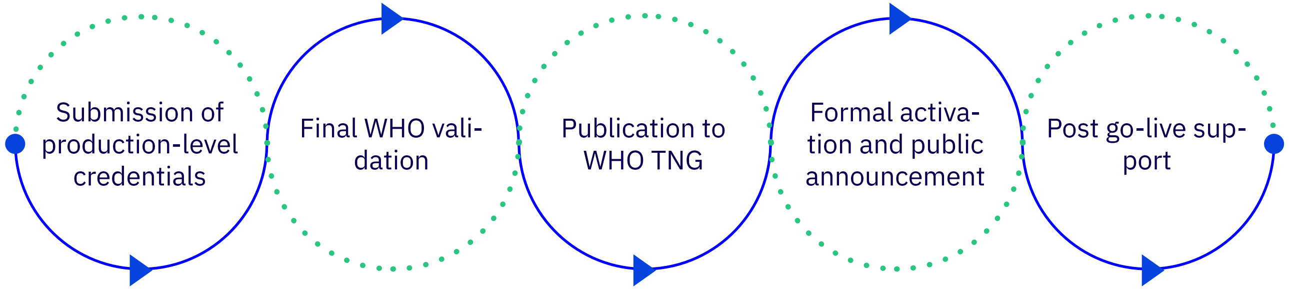
Production Go-Live: *The official "switch on"*

What it means

- Marks Ghana's official entry into GDHCN's production environment.
- Ghana's digitally signed health certificates become globally verifiable.
- Final step in the onboarding process, following UAT approval by WHO.

Significance

- A technical and symbolic milestone.
- Culmination of cross-sector collaboration, policy alignment, and digital infrastructure readiness.
- Signals Ghana's full operational integration into the international trust framework.


Submission of production-level credentials
Final WHO validation
Publication to WHO TNG
Formal activation and public announcement
Post go-live support

Key requirements for go-live

Final Go-Live typically takes 2-3 weeks after UAT is passed, depending on:

Timely submission of production-level cryptographic certificates

- Country Signing Certificate Authority (CSCA)
- Transport Layer Security (TLS) certificate

Accurate and complete metadata

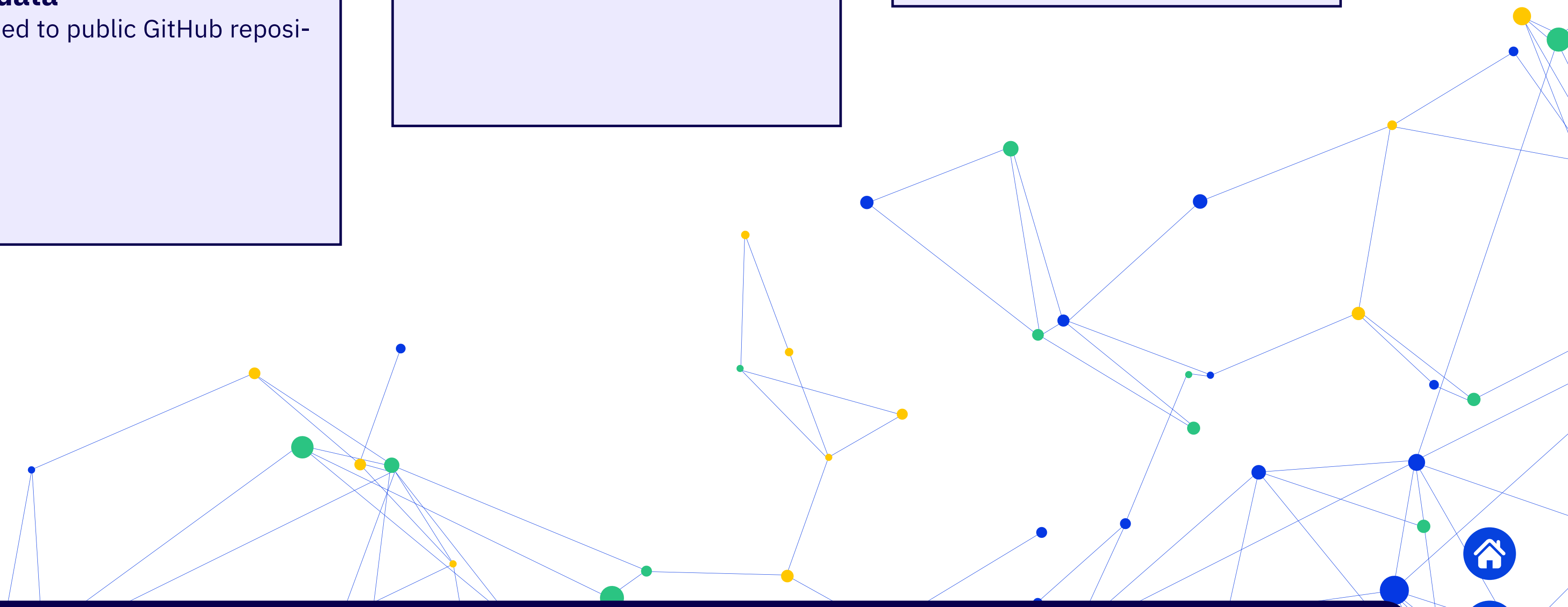
uploaded to public GitHub repository

Internal sign-off from:

- Ministry of Health (MOH)
- Ghana's Public Key Infrastructure (PKI) authority

Final coordination with WHO

- Validation of readiness
- Listing on WHO Trust Network Gateway (TNG)



Step 1:

Submission of production-level credentials

Upon successful UAT clearance, Ghana will prepare and submit the following to WHO:

- **Production CSCA public keys.** These keys are used to sign VDHCs and must be distinct from the UAT/test keys.
- **TLS certificate for secure API endpoint communication.** Ensures encrypted, authenticated exchanges between Ghana's systems and external verifiers.
- **Updated GitHub metadata repository.** Includes valid, timestamped production certificates, updated JSON metadata (WHO schema-compliant), country-level identifiers (e.g., ISO codes), technical contact information and endpoint URLs, and certificate policy documentation.

Entity	Primary Role	Key Skills / Capabilities
NITA (or National PKI Authority)	Lead agency for generating, securing, and submitting production-level cryptographic credentials.	• PKI expertise: CSCA/TLS key generation, signing, rotation, and secure storage • Cybersecurity: Secure key storage (e.g., HSM/KMS), endpoint security, key access logging • DevOps/GitHub CI: Managing public metadata repositories per WHO TNG
MOH	Authorizes submission; validates governance and compliance structures.	• Program coordination: Documentation, timing, and stakeholder readiness • Standards compliance: Oversight of FHIR, W3C VC, and schema requirements
GHS	Confirms issuance system is functionally ready and operational at pilot sites.	• Standards compliance: FHIR, W3C VC validation • Technical readiness assessment at implementation level
DPC (optional)	Advisory role on privacy and compliance readiness to support public trust.	• Privacy and compliance validation: Review of legal and data protection frameworks
Technical consultants	Support DevOps and implementation needs as needed.	• DevOps/GitHub CI: Assisting NITA in updating WHO-compliant public repositories

Step 2:
Final WHO validation

WHO conducts a thorough review across three key areas:

01

Certificate metadata reviews

- Validity periods, key usage, and country identifiers align with WHO schema.
- Metadata must be complete, correctly formatted, and standards-compliant.

02

Signature integrity verification

- Sample VDHCs (e.g., vaccination, testing) checked for valid digital signatures.
- Ensures issuance from registered CSCA and no cryptographic errors.

03

GitHub repository compliance

- Public metadata repository must be well-structured, HTTPS-accessible, and linked to WHO master trust registry.

Note: Any discrepancies must be addressed before go-live. WHO may host a live session with Ghana's technical team to expedite resolution.

Step 3:

Publication to WHO Trust Network Gateway

Once validated, WHO updates the TNG—the globally accessible trust registry—to include Ghana's production metadata. This update enables all GDHCN participants worldwide to:

- Discover Ghana's issuer identity.
- Retrieve and cache its public keys.
- Verify signatures on Ghana-issued certificates in real-time.

Ghana's inclusion on the TNG confirms its technical and policy eligibility as a trusted certificate issuer.

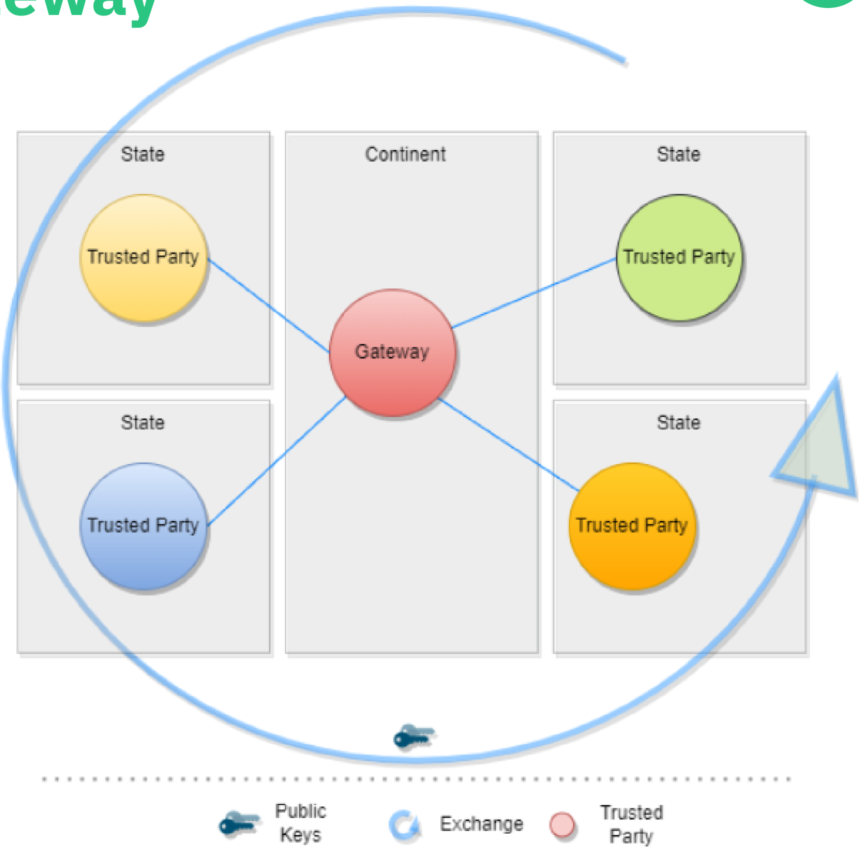


Image: This image is published on the WHO SMART Trust V1.1.2 depicting the TNG architecture.

Step 4:
Formal activation and public announcement

With the trust metadata live, WHO and Ghana proceed to the official "switch on," activating Ghana's global verification status.

WHO confirmation

WHO issues a formal acknowledgement to Ghana's MOH, confirming active participation in the GDHCN.

Public announcement

A joint announcement is made by WHO and the Ghanaian government (MOH, GHS, and NITA), notifying:

- The public and travelers that Ghana-issued digital health certificates are now internationally valid and verifiable.
- Global stakeholders (airlines, border agencies, health organizations) that Ghana is a trusted issuer on the WHO platform.

This announcement may be shared via press release, social media, GDHCN portal, and Ghana's official government communication channels.

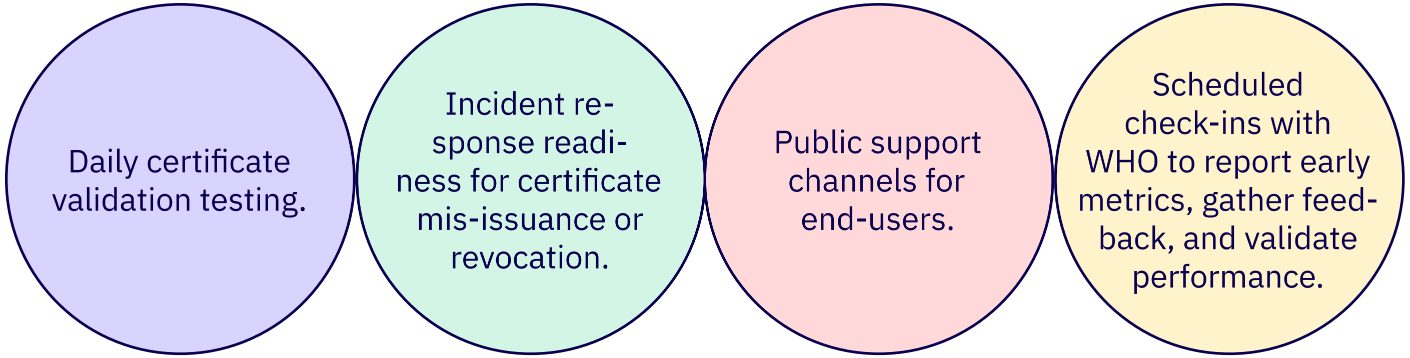
Operational activation

Health facilities, labs, and issuing authorities across Ghana begin producing production-ready VDHCs. These certificates will now pass verification by border authorities, airlines, and digital wallets across all GDHCN member jurisdictions.

Step 5:

Formal activation and public announcement

After activation, Ghana should implement a monitoring period to ensure stable operations:



- Daily certificate validation testing.
- Incident response readiness for certificate mis-issuance or revocation.
- Public support channels for end-users.
- Scheduled check-ins with WHO to report early metrics, gather feedback, and validate performance.

This transition from testing to trusted production marks Ghana's commitment to digital health leadership and its ability to participate securely in a global digital public good infrastructure.

©Clark Van Der Beken/Unsplash

CHAPTER

05

PLAY 3

Laying the Digital Rails for Health Trust: Technical Infrastructure

A robust, secure, and standards-compliant technical infrastructure is essential for Ghana's successful integration into the WHO GDHCN. This chapter explains the technical requirements for joining GDHCN, including PKI setup, certificate formats, metadata registries, and system components for issuance, verification, and validation. It describes Ghana's options for implementation tiers (starter, mid-level, enterprise), integration recommendations, and training needs for technical teams.

Contents:

Global Technical Architecture | Certificate Formats and Standards | Metadata Registry and Public Key Exchange | Core Systems Components | Ghana's Local Technical Architecture | Implementation Tier's: Ghana's Options | Technical Integration Recommendations

Global Technical Architecture

WHO Trust Framework and PKI Setup

At the heart of the GDHCN lies a Public Key Infrastructure (PKI) maintained by WHO. This framework ensures trust across borders by enabling verifiers in one country to confirm the authenticity of certificates issued in another, without requiring access to any sensitive or personal health data.

WHO acts as the Trust Anchor, validating participants' certificates and managing a global metadata registry via its Trust Network Gateway (TNG).

Participants (like Ghana) submit cryptographic keys (X.509 certificates), associated metadata, and governance documentation to WHO, which then publishes this information for all other members to access and trust.

Global Technical Architecture | Certificate Formats and Standards | Metadata Registry and Public Key Exchange | Core Systems Components | Ghana's Local Technical Architecture | Implementation Tier's: Ghana's Options | Technical Integration Recommendations

Certificate Formats *and* Standards

To ensure interoperability and consistency, GDHCN certificates must conform to international standards:

W3C Verifiable Credentials (VCs)	A globally recognised data model for expressing cryptographically verifiable health credentials.
HL7® FHIR® – Health Level Seven Fast Healthcare Interoperability Resources	Used to encode health data content (e.g., vaccination records).
X.509	Digital certificate standard used in PKI to sign and validate certificates.
EU Digital COVID Certificate (EU DCC) Compatibility	Optional configuration to allow Ghana’s digital certificates to be verified in systems that support EU DCC scanning and QR decoding (common in border control scenarios).

Metadata Registry *and* Public Key Exchange

Each GDHCN participant maintains a public metadata repository hosted on GitHub, based on WHO's TNG participant template. This repository includes:

01
CSCA (Country Signing Certificate Authority) public

02
TLS (Transport Layer Security) public keys for secure transmission

03
JSON-formatted metadata with country name, expiration dates, key usage, and contact info

WHO's TNG ingests these repositories and maintains a master trust registry that powers the global verification process.

Core System Components

01 Issuance

Generation of Verifiable Digital Health Certificates (VDHCs) by trusted authorities (labs, clinics, vaccination centers), cryptographically signed by Ghana's national CSCA.

02 Verification

Systems in foreign countries (or at local entry points) use WHO's trust registry to validate the signature of a Ghana-issued Certificate.

03 Validation

Software or services confirm certificate integrity, issuer authenticity, and expiration status without revealing personal data.

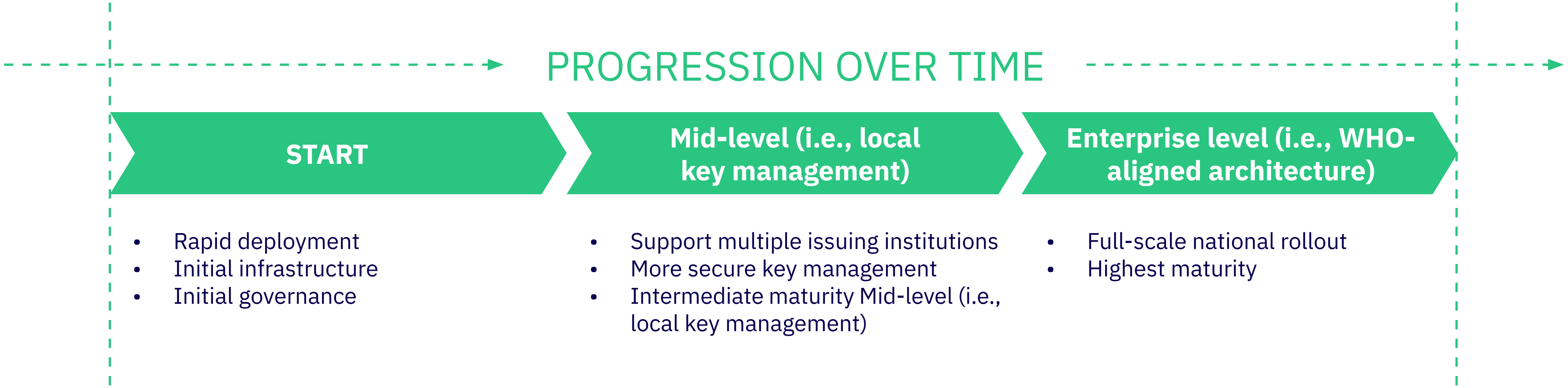
Ghana's Local Technical Architecture: Minimum infrastructure requirements

At a baseline level, Ghana must deploy systems capable of performing the following:

- Key generation and management (e.g., issuing and rotating CSCA and TLS certificates).
- Secure, cloud-accessible GitHub repository for public key and metadata publishing.
- Internet-facing web services for verification API (if desired).
- Issuance software that can create certificates from trusted data sources (vaccination databases, test results, etc.).

Implementation Tiers: Ghana’s Options

Ghana will progress through three levels of implementation on the road to full adoption.



PROGRESSION OVER TIME

START

- Rapid deployment
- Initial infrastructure
- Initial governance

Mid-level (i.e., local key management)

- Support multiple issuing institutions
- More secure key management
- Intermediate maturity Mid-level (i.e., local key management)

Enterprise level (i.e., WHO-aligned architecture)

- Full-scale national rollout
- Highest maturity

01

Starter level (Envelope key model)

Use case:

- Rapid deployment, especially in response to emergencies or pilot programs.

Approach:

- Generate and manage a single static key pair (CSCA) for signing certificates.
- Manual publishing of metadata to GitHub.
- Use WHO-provided issuance/verification tools or open-source solutions (e.g., DIVOC, GoVDHCN)

Strengths:

- Fast to deploy.
- Low overhead.

Limitations:

- Limited scalability.
- Key rotation is manual
- No advanced audit trails.

02

Mid-level (Local key management)

Use case:

- Intermediate maturity.
- Can support multiple issuing institutions (labs, clinics) and manage keys more securely.

Approach:

- Deploy key management service (KMS) or Hardware Security Module (HSM) for secure key handling.
  - Automate metadata updates via GitHub Actions or CI/CD.
- Create internal PKI governance policy for managing subordinate signing authorities.

Strengths:

- Increased security.
- Automated updates.
- Scalable for more facilities.

Limitations:

- Requires technical training integration work

03

Enterprise level (WHO-aligned architecture)

Use case:

- Full-scale national rollout.
- Aligned with WHO's own architecture and suitable for future use cases (e.g., cross-border worker credentials, health insurance).

Approach:

- Implement multi-tier PKI with root CA and multiple intermediate CAs.
- Build/operate issuance and verification systems compliant with W3C VC and HL7 FHIR.
- Establish national governance board, support system, compliance audit logs, and threat monitoring.

Strengths:

- Highly scalable.
- Fully autonomous.
- Can serve as regional trust anchor.

Limitations:

- Higher cost.
- More complex governance and ongoing technical support.

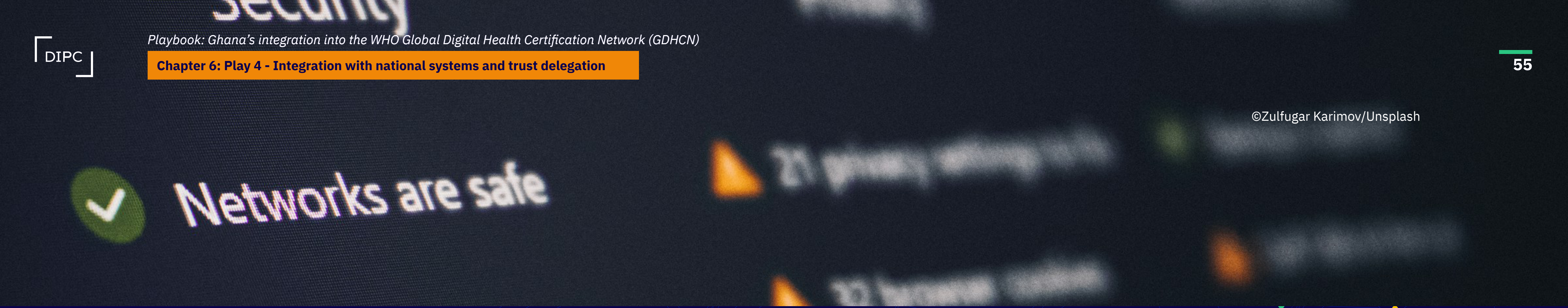
Technical Integration Recommendations for Ghana:

Aim for a mid-level architecture, leveraging NITA's existing CA infrastructure and integrating with GHS health data sources.

Use open-source tools provided by WHO or partners (e.g., GovStack, DIVOC) to reduce development time.

Establish internal monitoring tools to track certificate issuance volumes, system uptime, and security events.

Ensure digital literacy training for local tech teams responsible for key operations.



©Zulfugar Karimov/Unsplash

PLAY 4

CHAPTER 06

Connecting Systems, Enabling Continuity: Integration with National Systems and Trust Delegation

This chapter focuses on integrating GDHCN with Ghana's domestic digital platforms (EHRs, immunisation registries, national ID systems), managing signing authority, and ensuring only approved systems can issue certificates. It covers prerequisites for signing authority, clearinghouse models, audit trails, offline capabilities, and interoperability requirements.

Contents:

Overview of prerequisites for signing authority
Detailed steps outlining prerequisites for signing authority
National Clearinghouse Model
How do we know systems have accurate information?
Technical Considerations for Signing Documents
Interoperability Requirements for Data-Providing Systems
Summary: Integration Framework

As Ghana deepens its participation in the GDHCN, two priorities must be addressed:

System interoperability

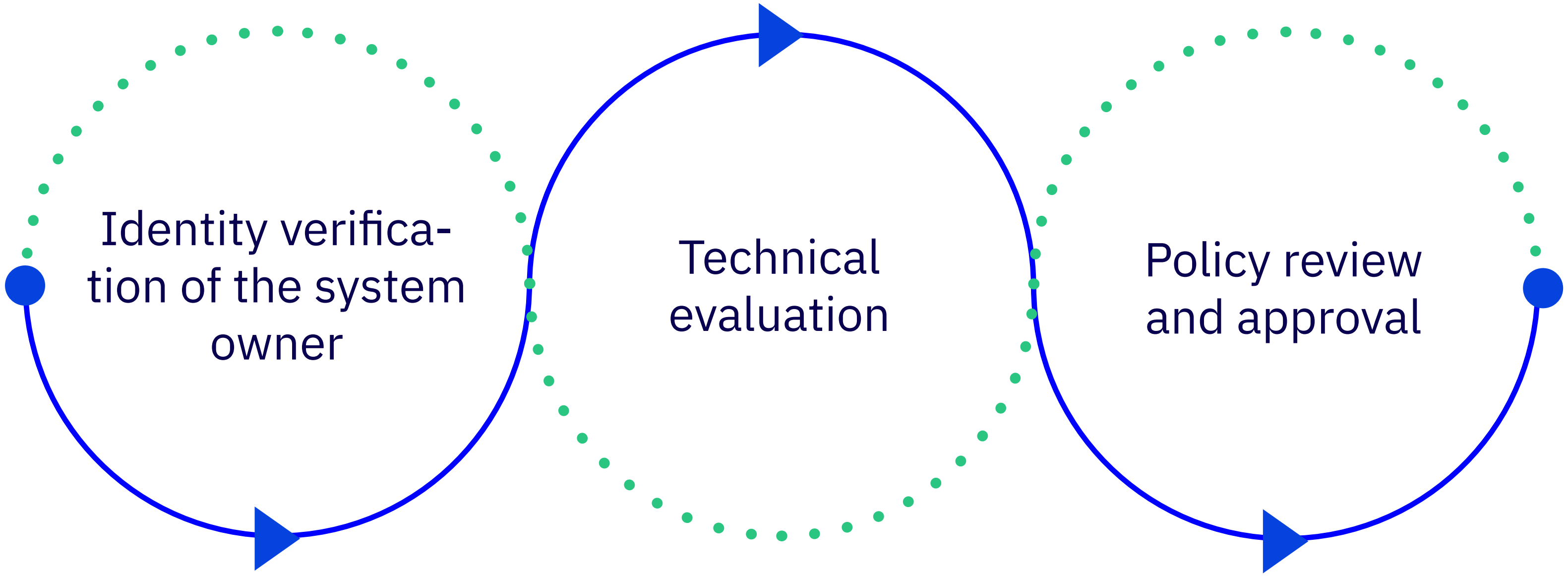
Domestic digital platforms—such as electronic health records (EHRs), immunisation registries, and national ID systems—must be able to securely and accurately transmit data into digital health certificates.

Governance of signing authority

Strong oversight of government signing keys is essential to maintain trust, prevent misuse, and ensure that only authorised systems can issue health certificates recognised globally.

Overview of prerequisites *for* signing authority

Local systems cannot automatically be granted the ability to sign documents with national Country Signing Certificate Authority (CSCA) keys. Local systems must demonstrate compliance and undergo a formal onboarding process to gain signing privileges. This includes:


Identity verification of the system owner
Technical evaluation
Policy review and approval

Detailed steps outlining prerequisites for signing authority (cont.)

01

Identity verification of the system owner

- Clear assignment of responsibility (e.g., government-owned system, accredited private provider).
- Organisational vetting by the Ministry of Health and technical review by NITA.

02

Technical evaluation

- Evidence that the system meets WHO and national requirements for:
  - Data integrity and accuracy.
  - Logging and audit capability.
  - Use of appropriate document formats (e.g., HL7® FHIR®, W3C VCs).
  - Cryptographic operations (correct use of private/public key pairs).

03

Policy review and approval

- Each system seeking signing rights must submit a policy and practice statement explaining:
  - What kind of data it will sign
  - Who will use the signed data
  - How the keys will be stored, used, rotated, and revoked
- Approved systems receive delegated authority (intermediate key or envelope key) under a clearinghouse or signing gateway model governed by NITA or GHS

National Clearinghouse Model

Why Select a Clearinghouse Model

To centralise trust delegation and reduce key exposure, Ghana may adopt a Signing Gateway or Clearinghouse Architecture.

How Clearinghouse Works

- Local systems (e.g., EHRs, immunisation registries, national ID platforms) send signing requests to a centralised service.
- The gateway:
  - Validates the payload (e.g., validates a vaccine dose from the immunisation registry)
  - Ensures schema and policy compliance
  - Applies the national digital signature

Benefits

- Signing keys remain secure and unshared
- Signing actions are traceable and centrally governed
- Unauthorised systems cannot inject false data into the global trust network

How do we know systems have accurate information?

Trusting a system to sign or submit certificate data depends on:

01 Data provenance

The system must demonstrate it receives data from trusted health facilities, clinicians, labs, or registries.

02 Audit trails

Must support timestamped logs for every issued or signed certificate.

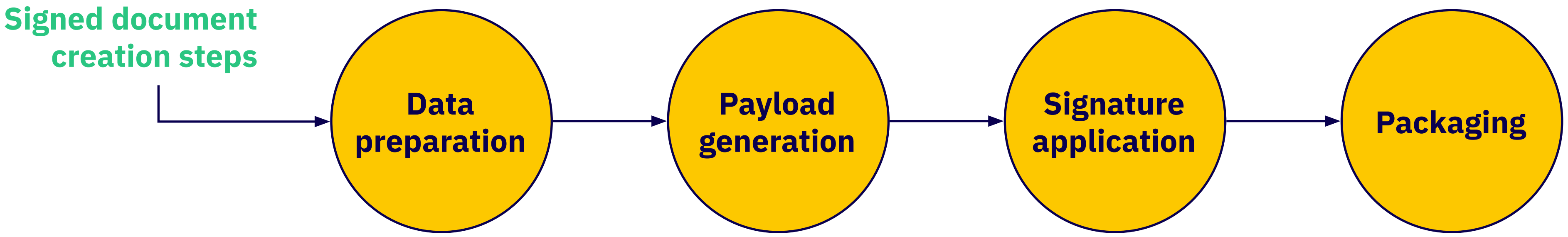
03 Validation mechanisms

Real-time schema validation (e.g., FHIR profiles, ICD-11 codes), cross-checks against national registries (e.g., NHIS, immunisation programs).

Periodic audits and simulated issuance checks should be part of the compliance program managed by GHS and NITA.

Technical Considerations for Signing Documents

When a local system is authorised to create signed health certificates, it must support the following workflow:



Data preparation: Export health data (e.g., vaccine record) in a compliant format (FHIR, IPS, etc.).

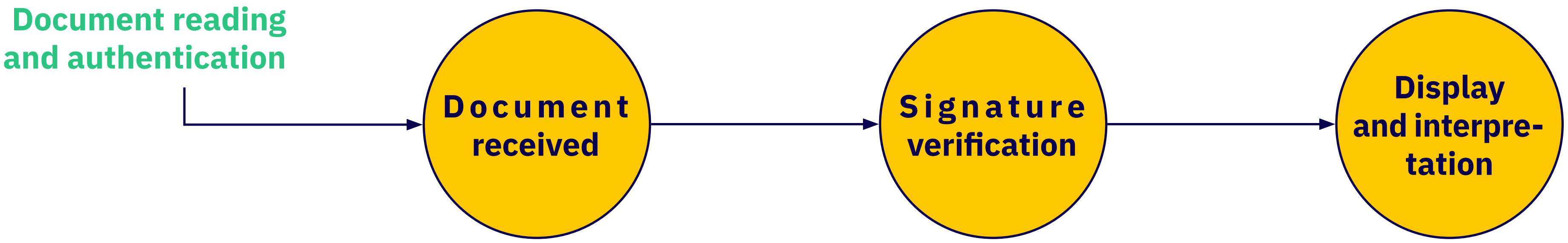
Payload generation: Generate a Verifiable Credential or HL7-FHIR Compliant payload.

Signature application:

- Apply a digital signature using an approved key (centralised or delegated).
- Include Cryptographic metadata, issuer ID, and timestamp.

Packaging: Embed in a QR code or JSON Web Token (JWT) for delivery.

When a local system is authorised to create signed health certificates, it must support the following workflow:



Document reading and authentication

Document received

Signature verification

Display and interpretation

A verifier (e.g., border agent, health worker) scans the QR code or receives the payload.

- Use public Metadata from WHO TNG to verify authenticity.
- Confirm the issuer is Ghana and the key is valid and unrevoked.

Render the health data and outcome (valid/invalid) for the verifier.

Offline capabilities and fallback mechanisms

In many rural or underserved areas in Ghana, continuous online access cannot be assumed. Local systems and verifiers must support **offline operations** to maintain continuity:

Local key caching

- Store the latest trusted public keys from WHO's metadata registry locally.
- Refresh them periodically when connectivity is available.
- See [WHO's Federated PKD Aggregation model]() for design guidance.

Offline document verification

- Use preloaded public keys and certificate metadata to verify digital signatures.
- QR code scanning apps should work without active internet, falling back to visual checks or expiration validation when needed.

Delayed syncing

- Systems issuing certificates while offline should cache signed documents.
- Automatically sync to national systems once connectivity is restored for backup, analytics, and revocation tracking.

Interoperability Requirements *for* Data-Providing Systems

Systems which are providing data to be signed by the certificates, such as EHRs, immunisation registries, and national ID systems, must:

01

Enable secure API-based data access to signing or issuance services.

02

Align with national and WHO schemas for Verifiable Digital Health Certificates (VDHCs) and provide localised mapping where needed (e.g., Ghana's vaccine codes mapped to WHO vaccine reference tables).

03

Support the national and globally agreed structured, standards-based data formats. These may include but are not limited to:

- HL7 FHIR as data structures and exchange formats
- ICD-9/10/11, LOINC, SNOMED, etc. codes as content classifications and data standards
- International Patient Summary (IPS) profiles as structured profiled FHIR resources.

Summary: Integration Framework

Requirement	Local system must...	Managed by*
Data accuracy	Use verified sources (labs, clinics, registries)	GHS
Signing authorisation	Be approved through a national trust-clearing process	MOH/NITA
Key management	Use envelope keys or submit payloads to centralised signer	NITA
Format compliance	Use HL7 FHIR, W3C VC, ICD-11, etc.	Local dev teams
Offline support	Cache trust list, sign and verify offline, sync later	System admins

***Note:** Entity designations are suggested for guidance only. This playbook aims to support countries in adapting technical concepts that involve many stakeholders, while ensuring final decisions remain with each country.

©Árpád Czapp/Unsplash

CHAPTER 07

PLAY 5

Safeguarding Rights, Enforcing Trust: Legal and Regulatory Considerations

This chapter outlines Ghana's legal and regulatory framework for digital health certificates, focusing on compliance with the Data Protection Act, electronic transactions, and international standards (GDPR, ICAO, IHR). It provides a checklist for legal actions, policy directives, ethical considerations, and responsibilities for various authorities to ensure secure, equitable, and compliant certificate issuance and verification.

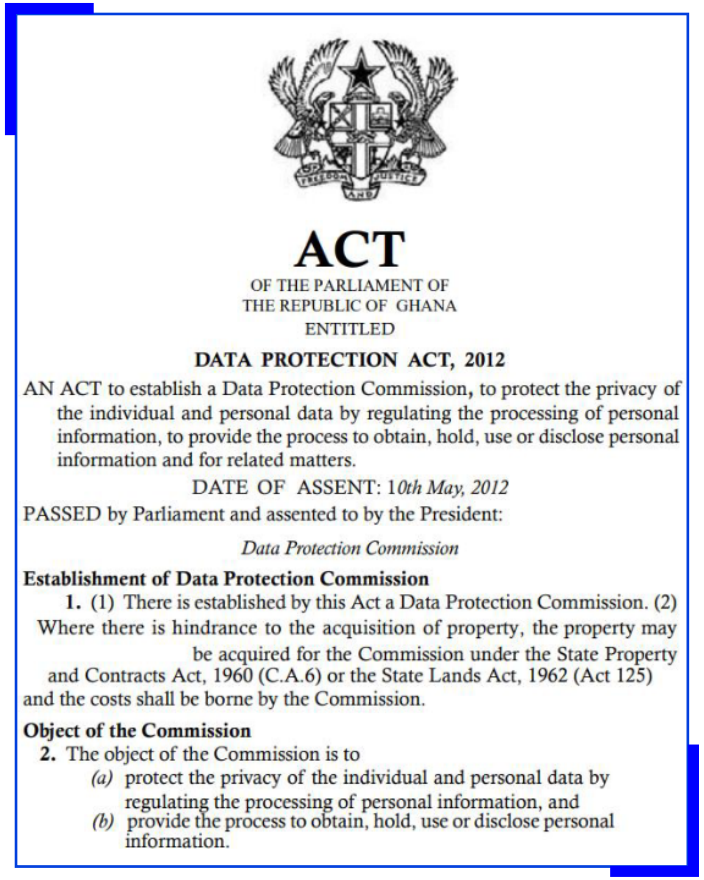
Contents:

National Data Protection Framework
Applicable Provisions of the Data Protection Act, 2012 (Act 843)
Legal and policy enablers for national rollout
Ethical and human rights considerations for digital health certificates
Legal and policy checklist for Ghana's digital health certificate rollout

National Data Protection Framework

For Ghana to effectively participate in the GDHCN, it must ensure that all certificate issuance, transmission, and verification processes are compliant with national laws and aligned with international standards, particularly in areas of **data protection, privacy, cybersecurity, and digital trust.**

Ghana's primary data protection legislation — **[the Data Protection Act, 2012 (Act 843)]** — serves as the baseline for managing personal health information, and thereby its national data protection framework.



ACT

OF THE PARLIAMENT OF
THE REPUBLIC OF GHANA
ENTITLED

DATA PROTECTION ACT, 2012

AN ACT to establish a Data Protection Commission, to protect the privacy of the individual and personal data by regulating the processing of personal information, to provide the process to obtain, hold, use or disclose personal information and for related matters.

DATE OF ASSENT: *10th May, 2012*

PASSED by Parliament and assented to by the President:

Data Protection Commission

Establishment of Data Protection Commission

1. (1) There is established by this Act a Data Protection Commission. (2) Where there is hindrance to the acquisition of property, the property may be acquired for the Commission under the State Property and Contracts Act, 1960 (C.A.6) or the State Lands Act, 1962 (Act 125) and the costs shall be borne by the Commission.

Object of the Commission

2. The object of the Commission is to

(a) protect the privacy of the individual and personal data by regulating the processing of personal information, and

(b) provide the process to obtain, hold, use or disclose personal information.

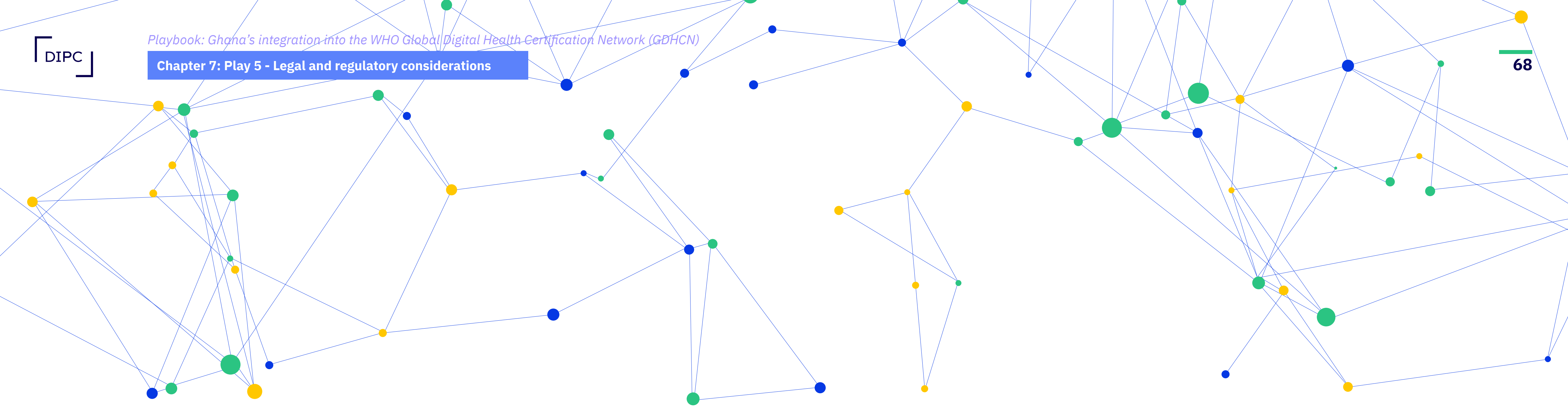
National Data Protection Framework

Applicable Provisions of the Data Protection Act, 2012 (Act 843)

Legal and policy enablers for national rollout

Ethical and human rights considerations for digital health certificates

Legal and policy checklist for Ghana's digital health certificate rollout



Applicable Provisions *of the* Data Protection Act, 2012 (Act 843)

Provision	Description
Data security	Strong encryption and secure data handling protocols must be used during certificate generation, storage, and verification.
Cross-border data sharing	Ghana must establish formal legal agreements or MoUs for any future bilateral interoperability involving personal data, **even though GDHCN itself does not transmit personal health data cross-border.**

Legal and policy enablers *for* national rollout

To enable the national implementation of verifiable digital health certificates (VDHCs), Ghana should take the following steps:

01

Ensure legal recognition of digital certificates

Establish that certificates issued under the GDHCN are valid for official purposes such as travel, employment, and access control.

02

Align digital signature practices with existing law

Confirm that digital signatures used for VDHCs comply with the Electronic Transactions Act, 2008 (Act 772) and are legally enforceable.

03

Define procedures for certificate revocation and disputes

Create clear legal pathways for addressing misuse, erroneous revocations, or challenges by recipients or verifiers.

04

Issue a national policy directive

The Ministry of Health (MOH) and Ghana Health Service (GHS) should publish a directive outlining how VDHCs will be used nationally.

05

Conduct a legal review of Ghana's PKI model

Assess the suitability of the public key infrastructure for health data, in collaboration with the Data Protection Commission.

06

Integrate certificate governance into national systems

Embed VDHC oversight into existing digital identity and e-governance frameworks to ensure consistency and accountability.

Ensuring international compliance and standards

To support global interoperability and trust, Ghana should align its implementation of GDHCN with key international frameworks:

01 **Adopt WHO GDHCN terms of participation**
Formally agree to WHO's policies, including technical, security, and privacy requirements for digital health certificate systems.

02 **Align with GDPR principles**
While the EU's General Data Protection Regulation (GDPR) is not legally binding in Ghana, adopting its principles enhances credibility and facilitates cross-border data exchange, especially with European certificate verifiers.

03 **Ensure compatibility with ICAO and IHR (2005)**
For certificates used in travel, Ghana must meet ICAO standards for health travel documents and comply with the International Health Regulations (2005).

Illustrative Legal and policy checklist for Ghana’s digital health certificate rollout

To help facilitate national implementation and promote international alignment, Ghana is encouraged to consider the following legal and policy actions:

□ **01. Confirm compliance with the Data Protection Act, 2012 (Act 843)**
Ensure that all digital health certificate processes meet national data protection standards.
Responsible: Data Protection Commission

□ **02. Draught a national policy recognising digital health certificates**
Establish legal recognition of certificates issued under GDHCN for official use (e.g., travel, employment).
Responsible: Ministry of Health (MOH), Legal Unit

□ **03. Verify legality of digital signatures under Act 772**
Confirm that digital signatures used for certificates are enforceable under the Electronic Transactions Act.
Responsible: NITA, Ministry of Justice

□ **04. Finalise a public trust governance policy**
Define how signing keys and certificate issuance will be governed to maintain public trust.
Responsible: NITA, Ghana Health Service (GHS)

□ **05. Sign WHO terms of participation for GDHCN**
Formally commit to WHO’s technical, security, and privacy standards.
Responsible: Ministry of Health (MOH)

□ **06. Conduct a legal impact assessment for GDHCN certificate usage**
Evaluate how certificate use affects existing laws and identify any gaps or risks.
Responsible: Legal Unit, Data Protection Commission

□ **07. Ensure digital health policies reference certificate standards and protections**
Update or draught policies to explicitly include standards for digital certificates and safeguards for users.
Responsible: MOH, Legal Unit

National Data Protection Framework | Applicable Provisions of the Data Protection Act, 2012 (Act 843) | Legal and policy enablers for national rollout | Ethical and human rights considerations for digital health certificates | **Legal and policy checklist for Ghana’s digital health certificate rollout**

©Towfiqu barbhuiya/Unsplash

CHAPTER

08 Safeguarding Rights, Enforcing Trust: Legal and Regulatory Considerations

This chapter outlines Ghana's legal and regulatory framework for digital health certificates, focusing on compliance with the Data Protection Act, electronic transactions, and international standards (GDPR, ICAO, IHR). It provides a checklist for legal actions, policy directives, ethical considerations, and responsibilities for various authorities to ensure secure, equitable, and compliant certificate issuance and verification.

Contents:

Conclusion

Annex A: Support Resources

Conclusion

With all five plays executed, Ghana will stand at the threshold of a transformative win—securely connected to the GDHCN. This onboarding to GDHCN celebrates the culmination of strategic governance, robust infrastructure, and legal alignment, all built on a foundation of trust. By enabling patients to own and share their health data, and equipping health workers with timely access to verified records—always with patient consent—Ghana will not just improve care but also fortify global health resilience. In a world where pandemics and health threats know no borders, this trusted connection through the GDHCN will empower faster responses, safer communities, and a healthier future for all.

Annex A: Support Resources

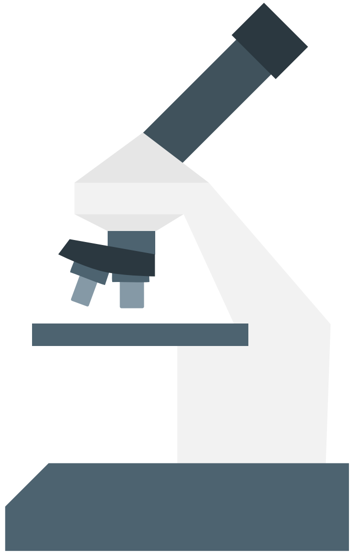
WHO GDHCN Secretariat (Global Support)

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

Onboarding Guidance:
https://smart.who.int/trust/concepts_onboarding.html

Technical Documentation:
https://smart.who.int/trust

GitHub Reference:
https://github.com/WorldHealthOrganization/tng-participant-template



References

- https://smart.who.int/trust/overview.html
- https://www.who.int/health-topics/digital-health
- https://www.who.int/initiatives/global-digital-health-certification-network/global-digital-health-certification-network-faqs
- https://smart.who.int/trust/concepts_onboarding_initialguideline_full.html
- https://www.who.int/initiatives/global-digital-health-certification-network/global-digital-health-certification-network-faqs
- https://smart.who.int/trust/concepts_onboarding_initialprocess_full.html?
- https://smart.who.int/trust/1.1.4/concepts_onboarding.html?
- https://smart.who.int/trust/business_requirements.html
- https://smart.who.int/trust/concepts_onboarding.html
- https://github.com/WorldHealthOrganization/tng-participant-template
- https://smart.who.int/trust/concepts_onboarding.html
- https://smart.who.int/trust/v1.1.5/concepts_onboarding_checklist.html

DIPC