DICE | Digital Health Centre of Excellence

Digital Documentation of COVID-19 Certificates (DDCC)

Communication materials for policy makers and program managers

unicef World Health Organization

unicef for every child World Health Organization

Acknowledgements

This work was made possible through the support of the WHO and was conducted by Vital Wave.

Special thanks are also extended to the organizations that offered their time and shared their expertise: the Bill and Melinda Gates Foundation, CDC, GAVI, UNICEF, and the World Bank.

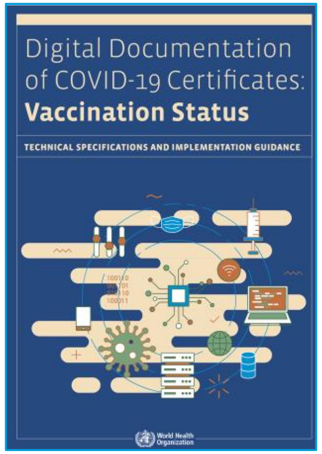
Country support for implementation of DDCC is being coordinated through Digital Health Centre of Excellence (DICE), a multi-agency mechanism co-led by WHO and UNICEF.

https://www.digitalhealthcoe.org/

How to use these and other DDCC materials

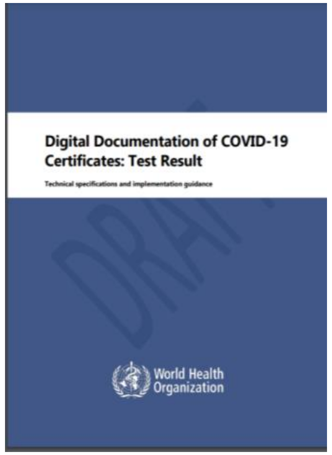
DDCC Guidance and Communication Materials

DDCC Guidance provides guidance to adapt and implement digital certificate programs for vaccination status and SARS-CoV-2 diagnostic test result use cases in country.


Digital Documentation of COVID-19 Certificates: Vaccination Status

TECHNICAL SPECIFICATIONS AND IMPLEMENTATION GUIDANCE

World Health Organization


Digital Documentation of COVID-19 Certificates: Test Result

Technical specifications and implementation guidance

World Health Organization

Vaccination Status (VS) Test Result (TR)

See also: *FAQ – 1. How can countries use Digital Documentation of COVID-19 Certificates (DDCC) materials?*

DICE Digital Health Centre of Excellence

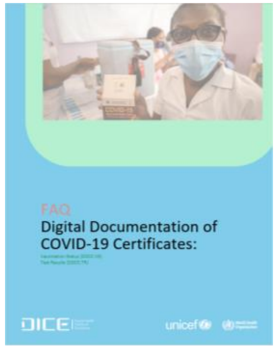
DDCC Overview

DDCC Overview summarizes the key concepts and value of digital certificates and supports policy makers and program managers to make the case for sustainable investment in national digital certificate programs.

DICE Digital Health Centre of Excellence

Operational Guidance

Operational Guidance elaborates on technical and operational concepts contained in the DDCC Overview with detail on how to estimate costs and operationalize a national digital certificate program.


FAQ

Digital Documentation of COVID-19 Certificates:

The **DDCC FAQ** is a companion document to the DDCC communication materials, providing detailed answers to frequently asked questions.

Target audiences for these materials

Policy Makers

- Policy makers, digital leads for ministries (e.g., health, ICT, border control)
- Need to make decisions to inform policy and advocate for funding

Key Contents

- Value
- Concepts
- Why invest

Program Managers

- Program managers, operational support staff (e.g., government, implementing partner)
- Need to evaluate many certificate options and quickly choose best solution, make operational decisions, and plan implementation

Key Contents

- Pre-requisites
- What's needed
- How to determine cost
- How to make a plan

See also: *FAQ – 2. Who is the audience for DDCC materials?*

DICE | Digital Health Centre of Excellence

DDCC Overview

Digital Documentation of COVID-19 Certificates (DDCC) is a standard and guidance for health certificate generation and status verification and validation across domestic and international use cases, at any stage of digital system maturity.

See also: *FAQ – 3. What is the DDCC?*

DDCC is:

a digitally signed HL7 FHIR document that represents the core data set content for the relevant COVID-19 certificate

DDCC guidance is:

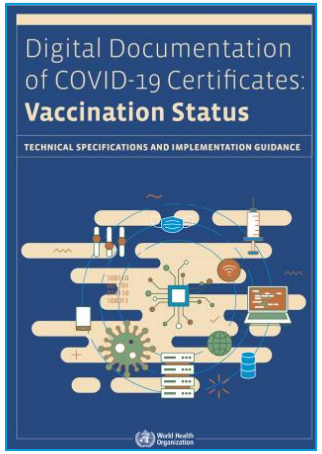
- Guidance for capturing the **minimum data set** to document an individual's vaccination status and SARS-CoV-2 diagnostic test results
- A mechanism for **linking different certificate products into a compatible certificate** for issue via paper, PDF, or smartphone
- A **flexible solution** that allows countries to customize for different use cases and data elements
- An approach that is **adaptable for future use cases and guidance**, beyond COVID-19

DDCC guidance is not:

- Guidance on national COVID-19 travel or vaccination policies
- An International Certificate of Vaccination or Prophylaxis (i.e., "yellow card")
- An identity card or passport

See also: *FAQ – 3. What is the DDCC?*

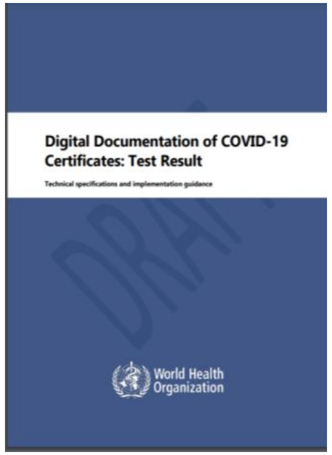
The DDCC contains implementation guidance for policymakers and requirements and specifications for technology implementers



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

TECHNICAL SPECIFICATIONS AND IMPLEMENTATION GUIDANCE

World Health Organization



Digital Documentation of COVID-19 Certificates: Test Result

Technical specifications and implementation guidance

DRAFT

World Health Organization

Vaccination Status (VS)   Test Result (TR)

Implementation guidance

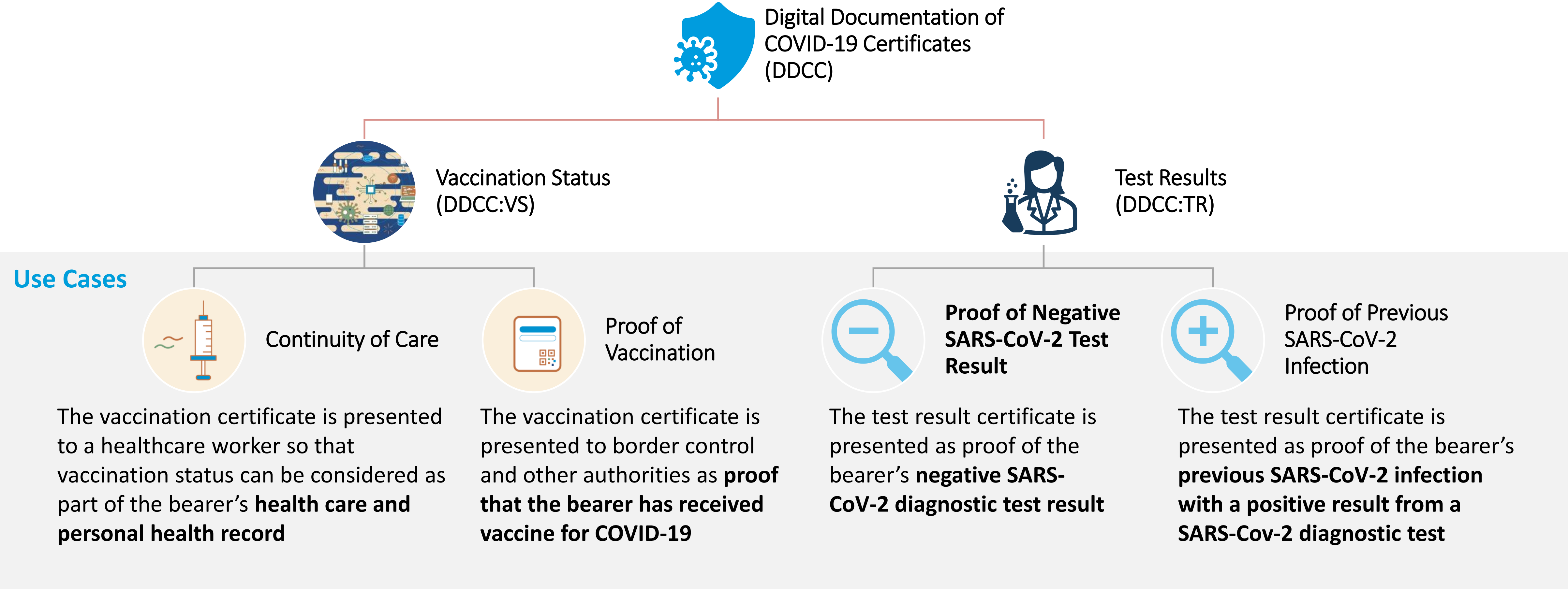
- Data protection principles
- Ethical considerations
- National governance considerations

Requirements and specifications for technology implementers

- Functional and non-functional requirements for different use cases
- Core data sets, defining data that is required for DDCC:VS and DDCC:TR certificates and optional data elements
- DDCC HL7 FHIR Implementation Guide detailing data standards for consistent representation and interoperability

See also: *FAQ – 4. What is included in DDCC Guidance?*

DDCC guidance supports the development of standardized health certificates for COVID-19 vaccination status and SARS-CoV-2 diagnostic test result use cases



Digital Documentation of COVID-19 Certificates (DDCC)

Vaccination Status (DDCC:VS)

Test Results (DDCC:TR)

Use Cases

Continuity of Care

The vaccination certificate is presented to a healthcare worker so that vaccination status can be considered as part of the bearer's **health care and personal health record**

Proof of Vaccination

The vaccination certificate is presented to border control and other authorities as **proof that the bearer has received vaccine for COVID-19**

Proof of Negative SARS-CoV-2 Test Result

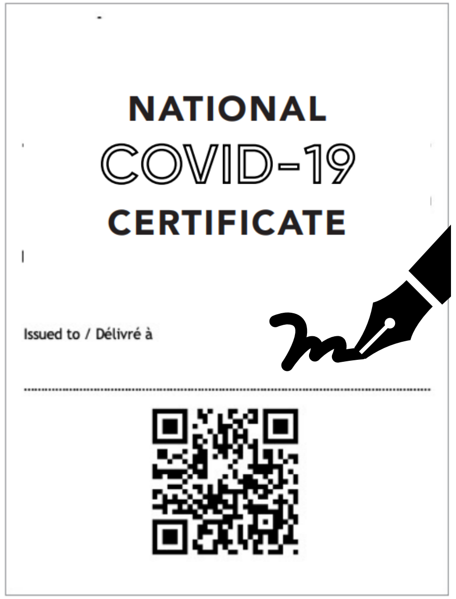
The test result certificate is presented as proof of the bearer's **negative SARS-CoV-2 diagnostic test result**

Proof of Previous SARS-CoV-2 Infection

The test result certificate is presented as proof of the bearer's **previous SARS-CoV-2 infection with a positive result from a SARS-Cov-2 diagnostic test**

See also: *FAQ – 5. What are the use cases for Vaccination Status and Test Result certificates?*

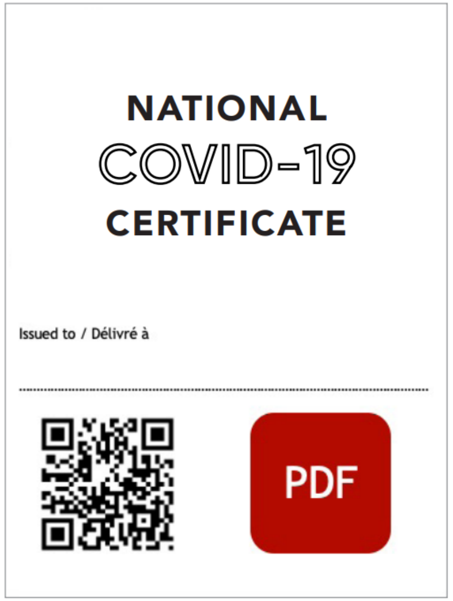
DDCC supports three different certificate issuing modalities



NATIONAL
COVID-19
CERTIFICATE

Issued to / Délivré à

Traditional paper record (e.g., paper certificate with a pre-printed QR code and a handwritten unique ID)



NATIONAL
COVID-19
CERTIFICATE

Issued to / Délivré à

PDF

Digital representation of traditional paper record (e.g., **PDF** file or certificate printout)

NATIONAL
COVID-19
CERTIFICATE

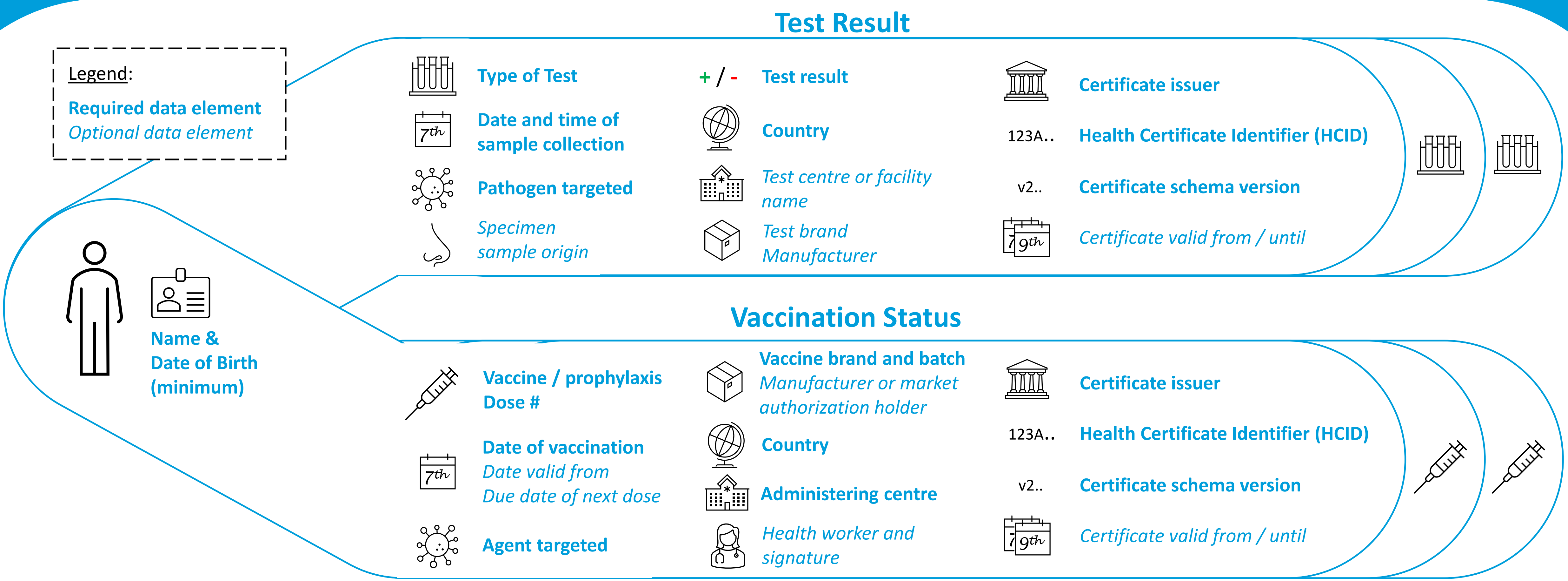
COVID-19 | 21 May 2021

COVID-19
18 June 2021

Purely digital (e.g., stored in a smartphone application or on a cloud-based server)

See also: *FAQ – 6. How are Vaccination Status and Test Result certificates issued?*

DDCC defines the standardized core data set* required to generate, verify, and validate certificates for test results and vaccination status



Legend:

Required data element

Optional data element

Name & Date of Birth (minimum)

Test Result

Type of Test

Date and time of sample collection

Pathogen targeted

Specimen sample origin

+ / - **Test result**

Country

Test centre or facility name

Test brand Manufacturer

Certificate issuer

123A.. **Health Certificate Identifier (HCID)**

v2.. **Certificate schema version**

Certificate valid from / until

Vaccination Status

Vaccine / prophylaxis Dose #

Date of vaccination

Date valid from

Due date of next dose

Agent targeted

Vaccine brand and batch

Manufacturer or market authorization holder

Country

Administering centre

Health worker and signature

Certificate issuer

123A.. **Health Certificate Identifier (HCID)**

v2.. **Certificate schema version**

Certificate valid from / until

*Countries may extend this core data set to store other data based on their requirements. Required and optional data elements may vary depending on certificate use case.

See also: *FAQ – 7. What standardized data does the digital certificate include?*

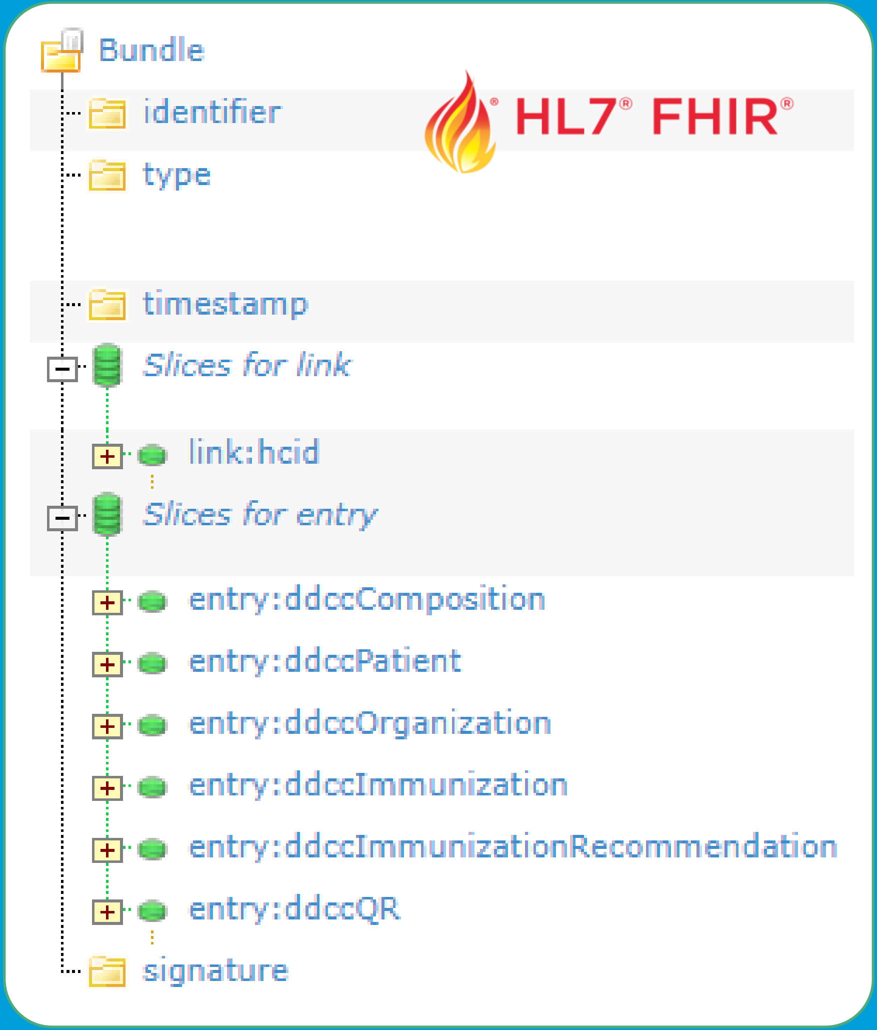
Digital Documentation of COVID-19 Certificates are human- and machine-readable packages of data in a standard HL7 FHIR “Bundle” containing all information necessary to verify and validate vaccination status or test results

Example FHIR Bundle* contents for a Vaccination Status certificate:

- Unique identifier for the certificate bundle
- Type of FHIR Bundle (e.g., document)
- Date and time FHIR Bundle was assembled
- Link to health certificate identifier (HCID)
- Health information including:
  - Patient details
  - Organization where immunization was administered
  - Immunization details (e.g., type of vaccine, lot number)
  - Recommended date of next immunization (if applicable)
  - QR code representation of health information
- Signature of issuing public health authority to verify the authenticity of the certificate

* In FHIR, a “Bundle” is simply a container for a collection of resources. DDCC uses a FHIR Bundle to bring together the required resources related to a certificate into a single document.

Source: https://worldhealthorganization.github.io/ddcc/StructureDefinition-DDCCDocument.html



```
Bundle
├ identifier
├ type
├ timestamp
├ Slices for link
│  └ link:hcid
├ Slices for entry
│  ├ entry:ddccComposition
│  ├ entry:ddccPatient
│  ├ entry:ddccOrganization
│  ├ entry:ddccImmunization
│  ├ entry:ddccImmunizationRecommendation
│  └ entry:ddccQR
└ signature
```

See also: *FAQ – 8. What digital health interoperability standard does DDCC certificates use?*

DICE Digital Health Centre of Excellence

DDCC is an umbrella specification that is compatible with other digital certificate formats

Countries are producing digital certificates COVID-19 vaccination status and SARS-CoV-2 diagnostic test result use cases and linking those certificates with national, regional, and global standards.

DDCC provides a common international and extensible format that is interoperable with other available digital certificate formats currently used in African, European, and South-East Asia regions and supports specific renderings of certificates that can be verified through these specifications.

Several COVID-19 certificates in the marketplace

- Digital Infrastructure for Vaccination Open Credentialing (DIVOC)
- EU Digital Covid Certificates (DCC)
- Smart Health Cards
- Custom Country Solutions

See also: *FAQ – 9. How are countries approaching digital certificates today?*

Source: https://dhis2.org/digital-certificates/

DDCC guidance recommends ethical considerations as integral to the design and deployment of any digital certificate solution

Ethical Considerations

- To protect and promote the welfare of individuals, communities and the population as a whole
- To ensure equal treatment for all individuals and prevent or mitigate, as far as possible, avoidable and unfair health inequalities (i.e., health inequities) within the boundaries of the state
- To create and maintain trust in public health activities as part of the health-care system

See also: *FAQ – 11. What ethical considerations and data protection principles need to be considered in a digital certificate solution?*

Recommendations

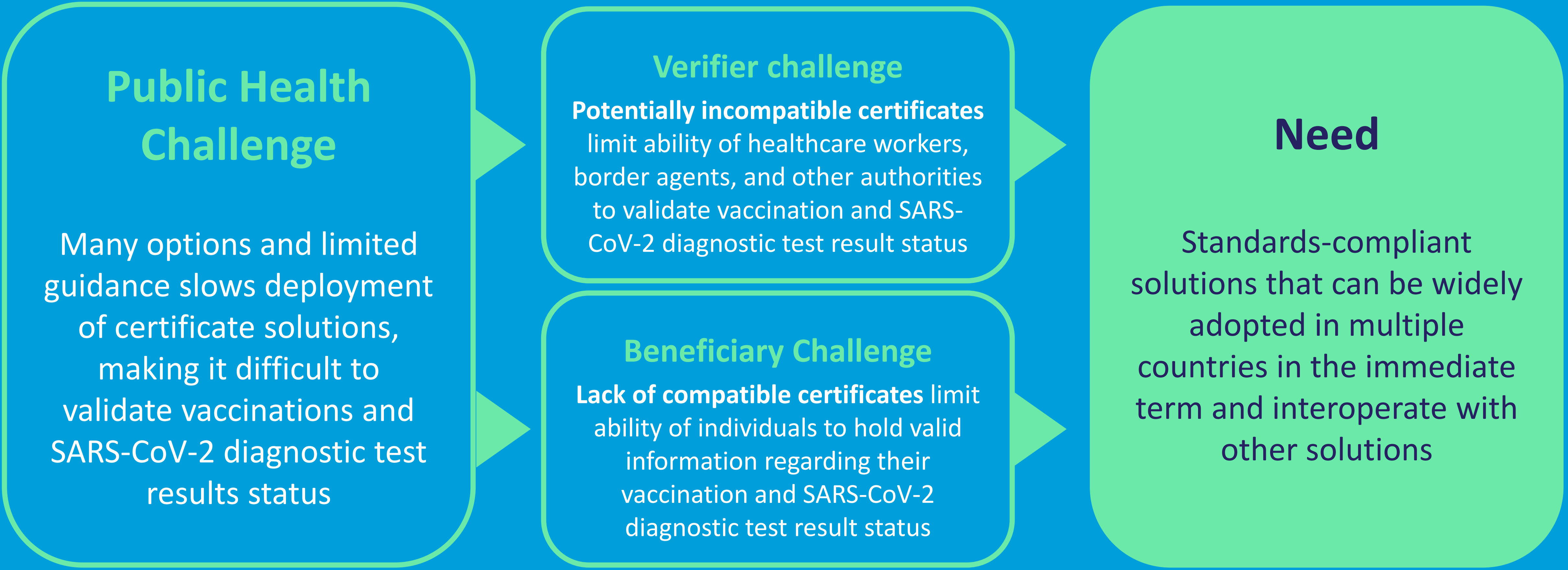
1. The scope of use of digital certificates should be clearly defined
2. Potential benefits, risks, and costs should be assessed before introduction of a digital certificate
3. Obtaining and using a digital certificate should be as inclusive and fair as possible
4. All necessary measures should be put in place to protect participants for continuity of care
5. All communication should be clear and transparent
6. The digital certificate program should be constantly monitored for impact and adjusted as necessary

DICE | Digital Health Centre of Excellence

Value of Digital Certificates

Global Situation

Complicated, evolving scientific landscape around COVID-19 and lack of global policy coordination on **vaccination status** and **test result** certificates creates challenges for Member States



Public Health Challenge

Many options and limited guidance slows deployment of certificate solutions, making it difficult to validate vaccinations and SARS-CoV-2 diagnostic test results status

Verifier challenge

Potentially incompatible certificates limit ability of healthcare workers, border agents, and other authorities to validate vaccination and SARS-CoV-2 diagnostic test result status

Beneficiary Challenge

Lack of compatible certificates limit ability of individuals to hold valid information regarding their vaccination and SARS-CoV-2 diagnostic test result status

Need

Standards-compliant solutions that can be widely adopted in multiple countries in the immediate term and interoperate with other solutions

See also: *FAQ – 12. What is the need for standardized and interoperable certificates?*

Standardized digital certificates have advantages over paper to prevent fraud and other issues

Paper certificates or photocopies are prone to fraud and a host of other issues (e.g., loss, damage, unauthorized use)

Incidence of fraudulent health certificates is expanding rapidly around the world. Health data can be sold for nearly 50 times payment card data on the black market[1].

Digital systems ensure authenticated certificates and precise data can be shared domestically and internationally

This provides a technical basis to support bilateral agreements (EU equivalency) to recognize legal requirements for vaccination status and SARS-CoV-2 diagnostic test results across borders

See also: *FAQ – 13. What advantages do digital certificates have over paper formats?*

[1] Trustwave Global Cybersecurity Report (2018)

Standardized digital certificates help rebuild economies and strengthen health systems to address COVID-19 and beyond

Policy Makers

Supports Reopening Economies

Enables verification and validation required to facilitate cross-border movement, commerce, and economic security and access certain socioeconomic activities

Increases Equitable Access to Health Information

Brings authenticated information into the context of care and personal health records via digital tools (e.g., digital immunization records)

Strengthens Digital Health Infrastructure

Standardizes health content and provides infrastructure that strengthens health information exchange capabilities

Program Managers

Improves Exchange of Health Information

Provides clear guidance for designing systems that easily interoperate with existing digital tools (e.g., vaccination campaign systems and immunization registers) and build a foundation for long-term health information exchange

Adapts to Country and Regional Ecosystems

Works for central or federated certificate issuers and generates QR codes that are compatible with other certificate programs (e.g., EU, DIVOC)

Supports Local Solution Development

Supports local developers and technology providers to develop solutions for COVID-19 and future digital health interventions by providing a flexible standard that can be adapted to local needs

See also: *FAQ – 14 & 15. What value do standardized digital certificates bring to country health systems / technical implementers?*

Standards-based certificates and guidance benefit decision makers and their technical partners

Guidance

✓ Policy Makers

Guidance enables usable and compatible digital certificates and supports rapid dissemination and application of new policy

✓ Program Managers

Guidance and clearly defined business requirements support easier implementation, reduce vendor lock-in

Digital Certificates

✓ Healthcare Workers

(Vaccination Status)

Clinical decision support ensures health worker knows vaccination status of patient and can provide a subsequent dose and better care based on guidelines

✓ Software Developer

Ecosystem of open-source FHIR tools reduces software development time

✓ Border Control and other Verifiers

Allows faster and more accurate interpretation of vaccination status or SARS-CoV-2 diagnostic test result in accordance with rapidly changing science, policies, and agreements

✓ Individuals

Provides standardized core data that applies across borders and use cases

See also: *FAQ – 16. What value does DDCC certificates and guidance bring to individual stakeholders?*

Next steps for policy makers

☑ Identify applicable policies that are in place and any gaps for use of digital certificates

☑ Make certificate decisions to inform policy development

- Short-term (COVID-19) vs. long-term approach to solution development
- Issuing modality: paper vs. digital representation
- Which QR specification to support
- How to identify individuals (e.g., passport, national ID, health ID)

☑ Consider intergovernmental recognition of certificates to inform negotiations and discussion with other countries and regional networks

Additional Support: Requests for technical assistance can be made through DICE. contact@digitalhealthcoe.org

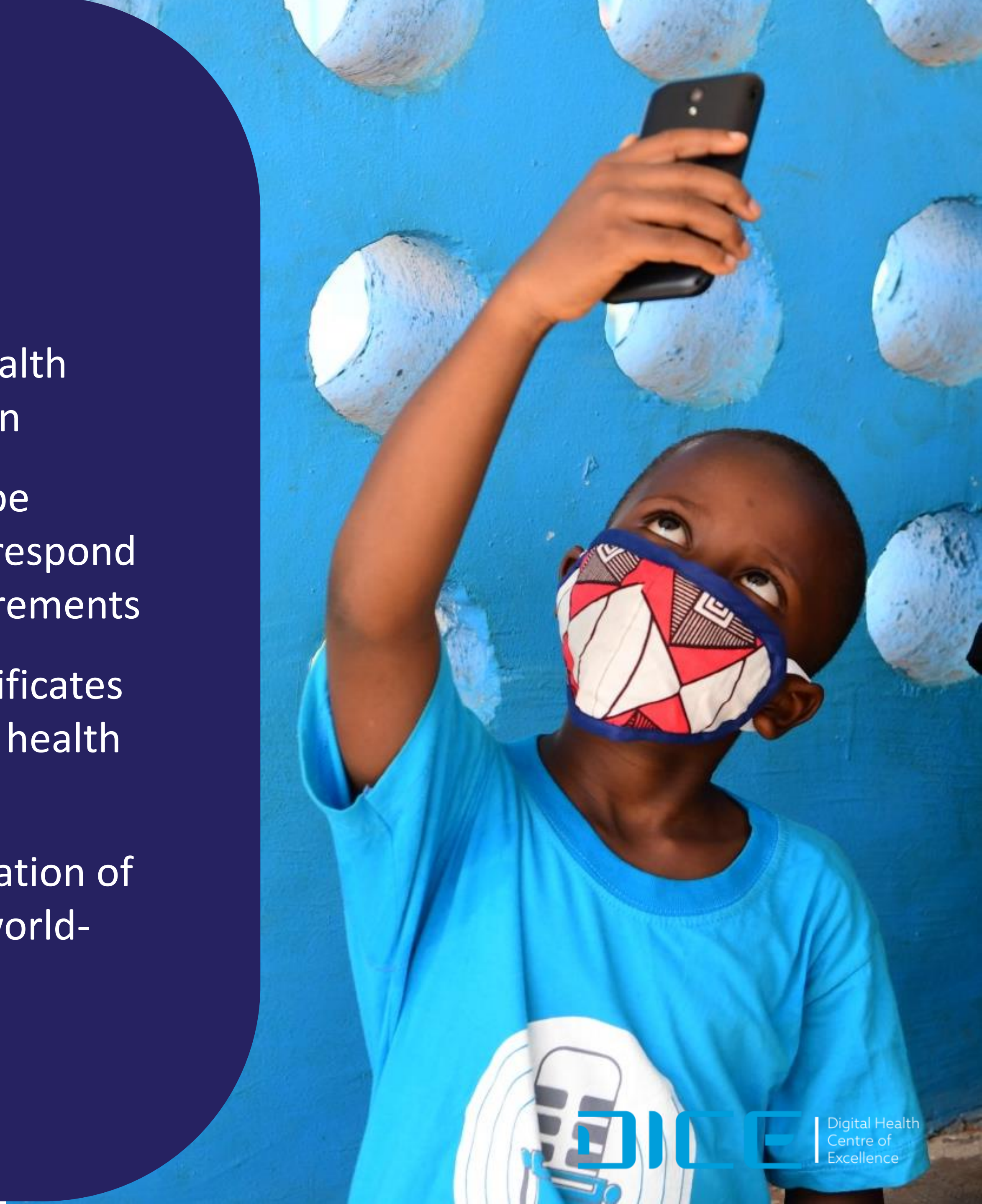
See also: *FAQ – 35. What are next steps for countries considering digital certificate implementation?*

DICE | Digital Health Centre of Excellence

Making the Case for Investment

Make the case for the upfront investment in digital certificates, infrastructure, and policy

- Upfront investment supports standards-based digital health interventions now and reduces their costs in the long run
- Digital certificate and services are extensible. They can be updated to include additional data or functionalities to respond to policy changes such as evolving traveler testing requirements
- Infrastructure can be used to service other types of certificates in health, such as digital immunization records, or other health domains
- Investments in policy and human capacity build a foundation of trust that extends beyond country borders to improve world-wide response to COVID-19 and future epidemics



See also: *FAQ – 17. Why invest in digital certificates over traditional paper certificates?*

Understand the digital health ecosystem to estimate costs and upfront investment required for a long-term digital certificate solution

Leadership and Governance

- Is there an existing department within the ministry of health that will be accountable for this work?
- Which regulatory agencies (e.g., pharmaceutical, health, ICT) need to be engaged?
- Will there need to be agreements established bilaterally?

Strategy and Investment

- What are the potential benefits, risks, and costs of implementing a DDCC solution?

Services and Applications

- Are point-of-care applications used to support immunization?
- Are there existing products in the marketplace that would fit your needs?

Standards and Interoperability

- Is there an existing interoperability framework?
- Are there existing systems that capture the minimum data for identification of an individual?

Infrastructure

- Is there adequate supply of equipment (e.g., mobile devices for health workers and verifiers, printers for certificates)?
- How can existing digital health investments be leveraged?
- Is a public key infrastructure (PKI) in place that can also be leveraged to support digitally signing DDCC?

Legislation, Policy, and Compliance

- Are policies for appropriate use and data protection in place?
- Are digital health data sharing and consent management policies in place?

Workforce

- How will training and technical support for health workers and officials be provided?
- Are change management processes and support in place?
- Is there a ready domestic supply of digital health workers?

See also: *FAQ – 18. What key considerations impact upfront investments for a long-term digital certificate solution?*

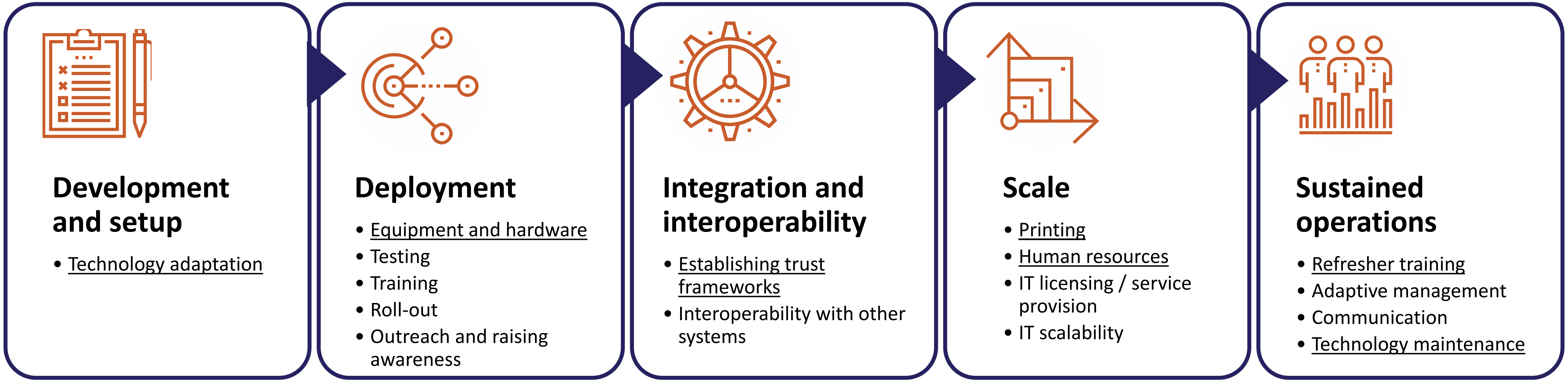
Graphic and information adapted from the WHO ITU eHealth National Strategy Toolkit.

Estimate costs for each implementation phase to align with country context and intended use cases

underline = significant cost driver

Ongoing / all phases

- Governance
- Management and staffing



Development and setup

- Technology adaptation

Deployment

- Equipment and hardware
- Testing
- Training
- Roll-out
- Outreach and raising awareness

Integration and interoperability

- Establishing trust frameworks
- Interoperability with other systems

Scale

- Printing
- Human resources
- IT licensing / service provision
- IT scalability

Sustained operations

- Refresher training
- Adaptive management
- Communication
- Technology maintenance

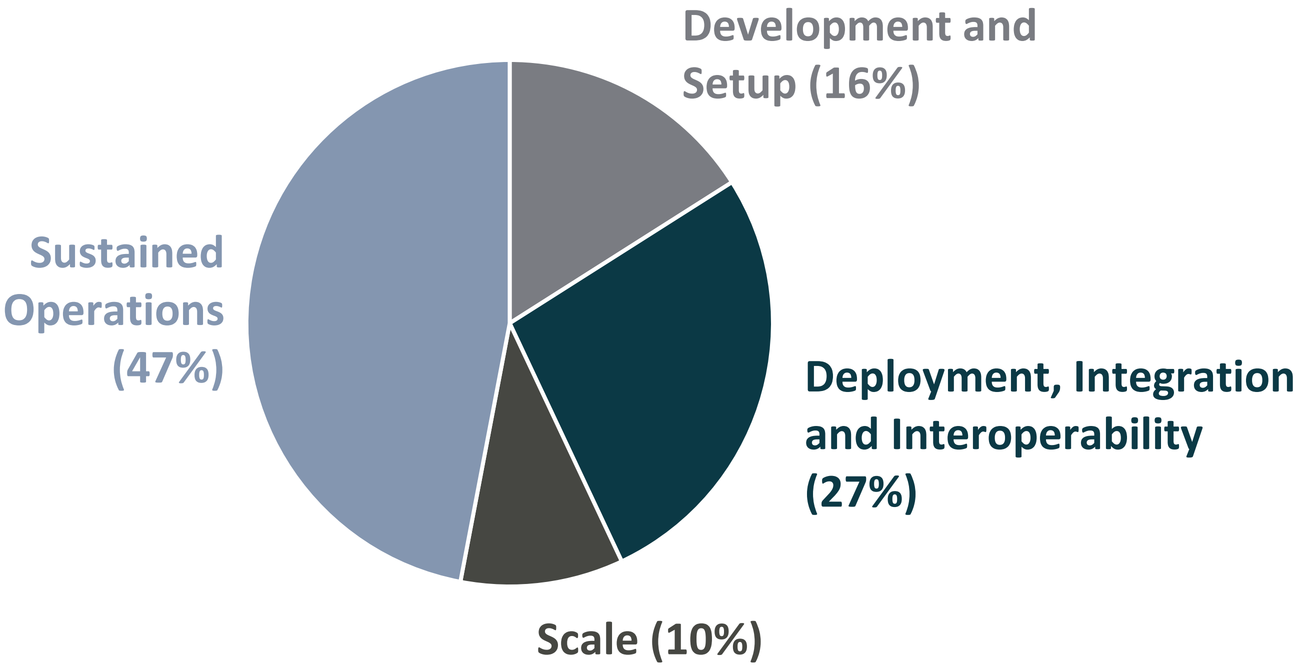
See also: *FAQ – 19. What types of costs need to be considered across digital certificate implementation phases?*

Typical costs by phase for digital health interventions*

While exact costs will vary depending on country context, sustained operations over five years average close to 50% of total cost.

Development and setup costs, commonly equated with the "cost of a solution," average less than 20% of total cost.

Illustrative Breakdown of Total Cost of Ownership* By Implementation Phase Over Five Years



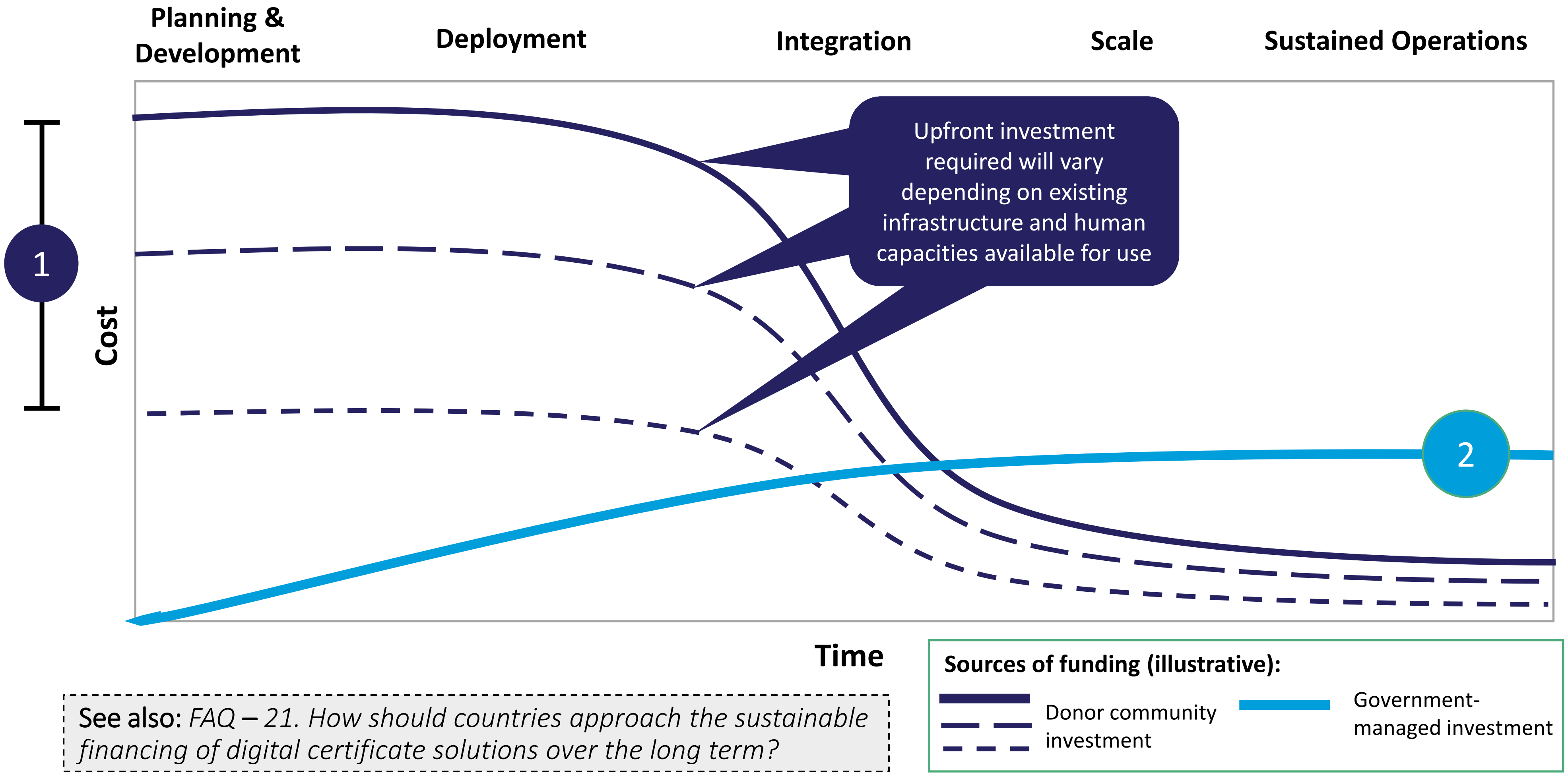
Source: Understanding Total Cost of Ownership for Digital Health. https://digitalsquare.org/market-analytics.

** Based on a comprehensive evaluation of costs for five, nationally scaled logistics management information systems (LMIS) used to manage stock and distribution of life-saving commodities. This is provided as a point of reference since there is no reliable cost data specific to COVID digital certification implementation projects.*

See also: *FAQ – 20. How might costs for a digital certificate program break down by implementation phase?*

DICE | Digital Health Centre of Excellence

Create a transparent understanding of costs per phase to advocate for upfront investment and long-term government budget commitments



Upfront investment required will vary depending on existing infrastructure and human capacities available for use

Sources of funding (illustrative):

▬ ▬ ▬ - - -	Donor community investment	▬	Government-managed investment

See also: *FAQ – 21. How should countries approach the sustainable financing of digital certificate solutions over the long term?*

Establishing a plan for sustainable financing

1. Determine level of up-front investment required for initial phases, depending on country context
2. Determine annual operating costs and obtain government commitment to schedule annual operating costs under government budget (or long-term health system strengthening funding)

Seek funding through the digital health ecosystem or related national programs

→ Make a request through the Digital Health Centre of Excellence (DICE) to connect with implementing partners and access technical assistance (contact@digitalhealthcoe.org)

→ Work with leaders of related national digital health investments (e.g., electronic immunization registries or vaccine distribution programs) to identify shared resources or infrastructure

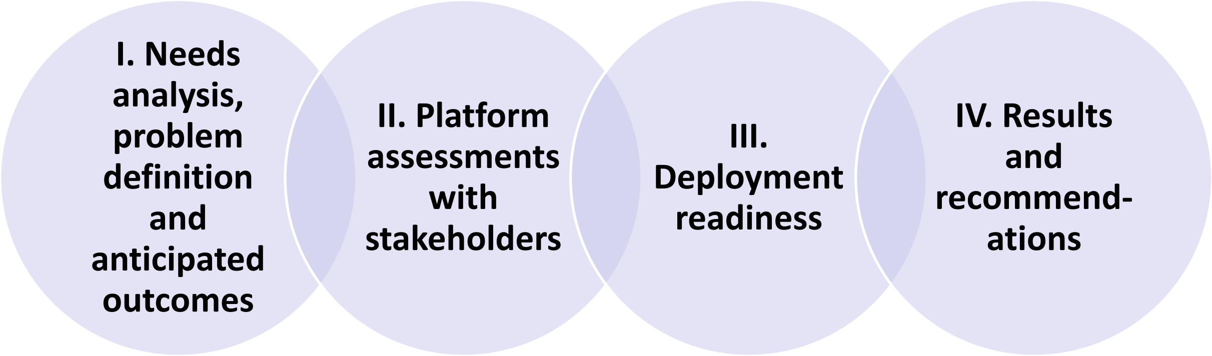
→ Engage with regional groups working on certificate standards (e.g., WHO, EU, DIVOC) to support bilateral agreements and knowledge sharing

See also: *FAQ – 22. What sources of financing may be available to support DDCC implementation?*

Request technical assistance through DICE

Depending on the type of request, DICE may be able to provide either direct technical assistance or recommend consultants, vendors, or in-country partner organizations who can provide direct support.

DICE Technical Assistance Approach



I. Needs analysis, problem definition and anticipated outcomes

II. Platform assessments with stakeholders

III. Deployment readiness

IV. Results and recommend-ations

Approximate timeframe: 3 weeks to 3 months

See also: *FAQ – 23. How can countries request technical assistance through DICE?*

Requests for technical assistance should come from a government institution or endorsed partner and include a brief description of:

- The specific health system processes or functions that need to be addressed through the digital health intervention.
- If COVID-19 vaccine related, how the need for the digital health intervention (technology/system/platform) is described in the National Vaccine Deployment Plan (NVDP).
- How the digital health intervention is supported by a National eHealth or Digital Health strategy.
- The main in-country stakeholders that should be included in the process.

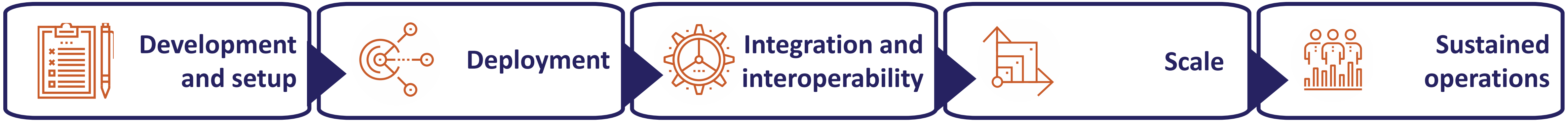
DICE | Digital Health Centre of Excellence

Operational Guidance

Steps to plan and implement a digital certificate solution

1. **Country Readiness:** Determine country readiness to fulfill prerequisites: (1) Unique identification and (2) Public Key Infrastructure
2. **Use Case Planning:** Determine the intended uses for a digital certificate system
3. **Benefit and Cost Assessment:** Assess the potential risks, benefits, and high-level costs of a digital certificate program
4. **Policy Framework:** Establish policies and a legal framework to support your intended uses of the digital certificate
5. **Landscape Assessment:** Determine whether to leverage existing digital systems that document certificate status or adopt a new system
6. **Requirements Gathering:** Gather health content requirements and system requirements for the intended use of your digital certificate
7. **Finalize Plans and Budget:** Finalize plans to develop, deploy, implement, and scale the solution

Development & Implementation



See also: *FAQ – 24. What are the overall steps to planning and implementing a digital certificate solution?*

Investigate whether key prerequisites are in place to ensure trust before beginning digital certificate planning

☑ **Countries must determine an acceptable and ethical way to link certificates to the identity of the individual holding the certificate**

- Name and date of birth are required by DDCC.
- Countries must decide if certificates should be linked to additional unique identifiers (e.g., health ID, national ID number, passport number, biometrics), if available.

☑ **Countries must determine if national Public Key Infrastructure (PKI) exists that can be used to issue, verify, and sign digital certificates**

- Suitable PKI may already be available for other domains (e.g., law enforcement, banking transactions). If not, the country must set one up.
- A PKI guarantees that the information contained in digital certificates has been validated by an accredited authority.
- Each country is responsible for managing its own PKI through its Public Health Authority (PHA) or another national delegated authority.

See also: *FAQ – 25. What pre-requisites need to be in place for country readiness prior to planning a digital certificate system (Step 1: Country Readiness)?*

See Annex A for additional detail on these key concepts

Select one or more use case for digital certificates that support country policies, and determine which organizations are likely verifiers

Continuity of Care

The vaccination certificate is presented to a healthcare worker so that vaccination status can be considered as part of the bearer's **health care and personal health record**

Proof of Vaccine

The vaccination certificate is presented to border control and other authorities as **proof that the bearer has received vaccine for COVID-19**

SARS-CoV-2 Negative Test Results

The test result certificate is presented as proof of the bearer's **SARSCoV-2 diagnostic test results**

Proof of Previous SARS-CoV-2 Infection

The test result certificate is presented as proof of the bearer's **previous positive result of SARS-CoV-2 infection**

Inputs

- National digital health or eHealth strategy (if one exists)
- Documents including COVID-19 response intervention objectives, progress, and any evaluations
- Organograms describing directorates or departments in the relevant government bodies, such as ministries of health, ICT, border control, and civil registrars

Outputs

- Problem statement detailing specific challenges that each digital certificate use case will address
- List of priorities for the digital certificate program that align with national digital health strategy
- Organogram for prospective digital certificate program
- List of stakeholders to engage

See also: *FAQ – 26. How do countries determine priority use cases for digital certificates (Step 2: Use Case Planning)?*

Conduct an assessment to understand risks, benefits, and high-level costs

Recommendations on ethical and privacy protections for design, development and implementation of digital certificates

1. The scope of use of digital certificates should be clearly defined
2. Potential benefits, risks, and costs should be assessed before introduction of a digital certificate
3. Obtaining and using a digital certificate should be as inclusive and fair as possible
4. All necessary measures should be put in place to protect participants for continuity of care
5. All communication should be clear and transparent
6. The digital certificate program should be constantly monitored for impact and adjusted as necessary

Inputs

- Documented objectives for digital certificate program
- Identified team and list of stakeholders to be engaged throughout the planning and implementation process
- Prospective personas for the digital certificate program
- Historical budgets and total cost of ownership (TCO) data for comparable digital health interventions
- Knowledge sharing of digital certificate implementations in other countries to inform feasibility and total cost estimate

Outputs

- Current-state (“status quo”) workflow diagrams illustrating the user journey for vaccination and testing
- Prioritized bottlenecks mapped to list of health system challenges to be addressed
- Enabling-environment assessment defining possible constraints
- High-level cost estimate to inform go / no-go decision to proceed with program development

See also: *FAQ – 27. How do countries conduct a benefit and cost assessment for digital certificate programs (Step 3: Benefit and Cost Assessment)?*

Establish policies and a legal framework to support appropriate use, data protection, and governance of the digital certificate

Additional governance considerations*

- Issuing digital certificates
- Appropriate use of digital certificates
- Verifying digital certificates
- Validating digital certificates
- Data management and privacy protection
- Revocation of digital certificates (informing individuals, informing verifiers, remedy provision)

**in addition to the authorized DSC- sharing mechanism*

Additional WHO guidance documents include:

- Technical considerations for implementing a risk-based approach to international travel in the context of COVID-19: Interim guidance
- Policy considerations for implementing a risk-based approach to international travel in the context of COVID-19
- Interim guidance on considerations for implementing and adjusting public health and social measures in the context of COVID-19

Inputs

- Enabling-environment assessment
- Ethical considerations
- Personas and future state user task flow diagrams
- High-level data requirements and national data privacy laws

Output

- Detailed implementation plan for digital certificate program, specifying:
  - Governance, workforce and training, links to strategy and investment plans

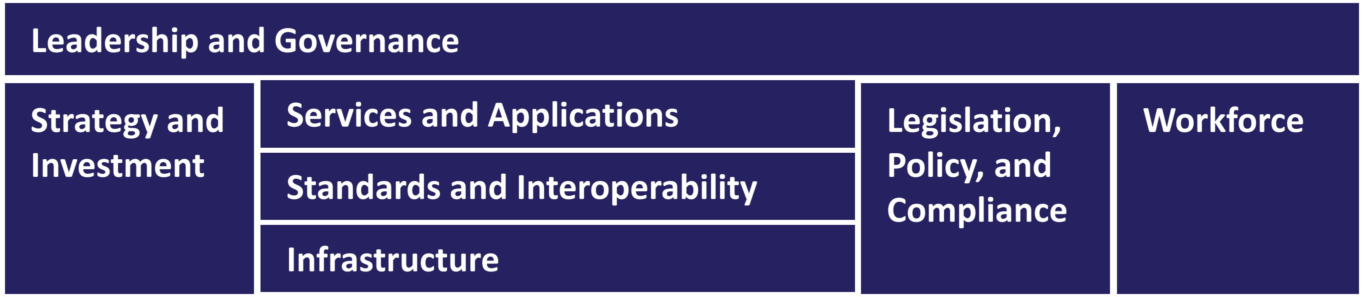
See also: *FAQ* – *28. What needs to be considered when establishing policies and a legal framework to support intended use of digital certificates (Step 4: Policy Framework)?*

See Annex A for additional detail on these key concepts

Determine whether to leverage existing digital systems that document certificate status or adopt a new system

Additional implementation consideration components

- Decisions related to digital health investments and selection of solutions should be guided by country strategy
- Refer to the next slide for a series of questions to guide this decision-making process



Leadership and Governance

Strategy and Investment

Services and Applications

Standards and Interoperability

Infrastructure

Legislation, Policy, and Compliance

Workforce

Inputs

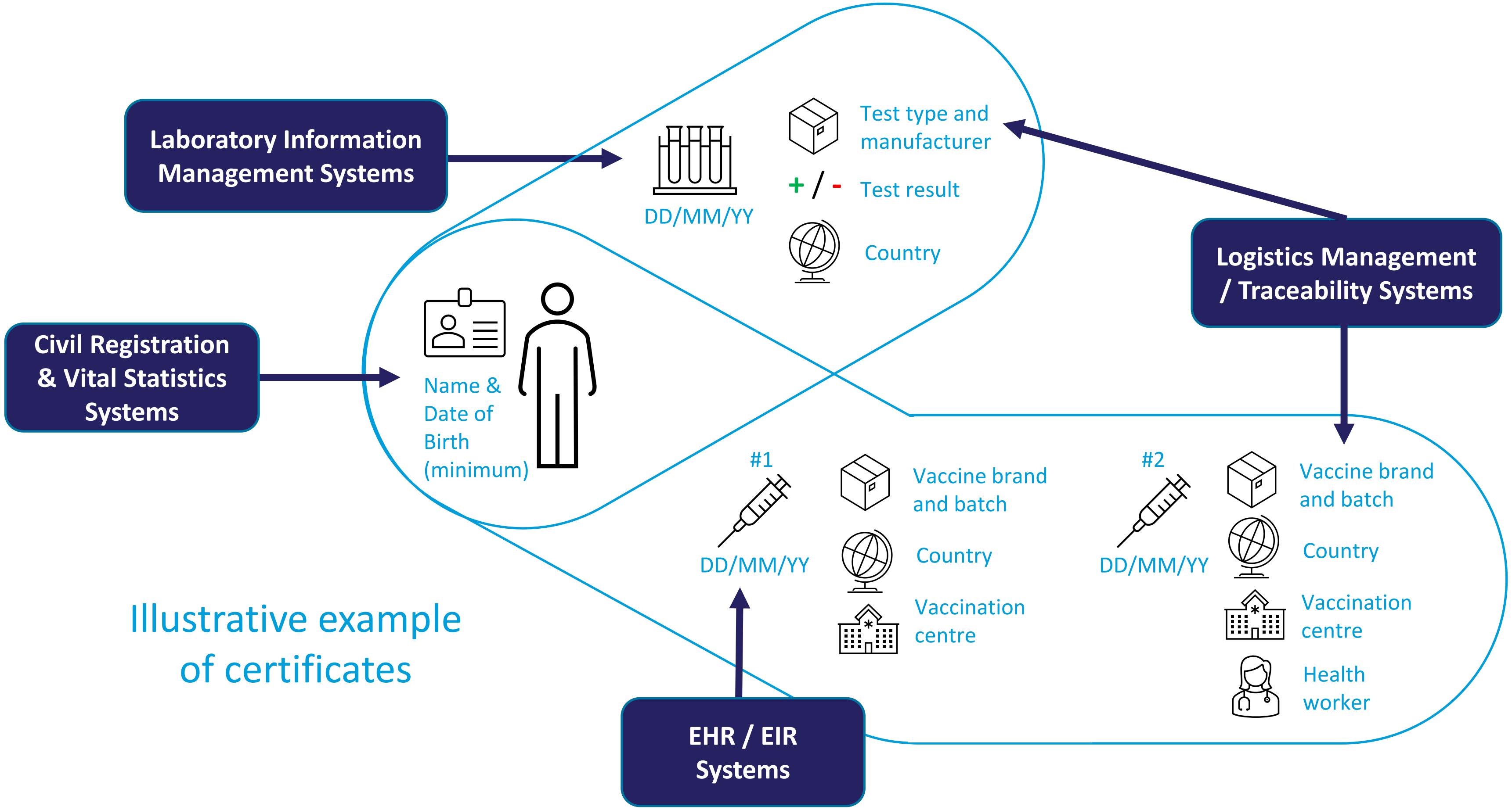
- Defined future-state workflow and functional requirements for digital certificate program
- National digital health enterprise architecture (if available in country)

Outputs

- Core functional requirements for the planned digital certificate investment within the enterprise architecture
- Identification of which applications and shared services already collect data for certificates and which will require further investment
- Linkages of digital certificate investment detailing the benefit to the broader set of digital health systems and enterprise architecture
- Identified digital health interventions that capture the data required for the digital certificate program

See also: *FAQ – 29. How do countries assess existing digital systems and architecture (Step 5: Landscape Assessment)?*

Identify data from existing data systems that can be pulled into the certificate generation service, if available


Laboratory Information Management Systems
DD/MM/YY
Test type and manufacturer
+ / - Test result
Country
Logistics Management / Traceability Systems
Civil Registration & Vital Statistics Systems
Name & Date of Birth (minimum)
#1
DD/MM/YY
Vaccine brand and batch
Country
Vaccination centre
#2
DD/MM/YY
Vaccine brand and batch
Country
Vaccination centre
Health worker
EHR / EIR Systems

Illustrative example of certificates

Associated activities

- Data mapping determine requirements for system integration
- Discussions with system owners and establishing data sharing agreements
- Building and testing system integrations
- Maintaining systems

See also: *FAQ – 30. How can data from existing digital health system be utilized for digital certificates (Step 5: Landscape Assessment)?*

Explore other ecosystem considerations that may impact how a new digital certificate system will be introduced and managed

Leadership and Governance

- Is there an existing department within the ministry of health that will be accountable for this work?
- Will there need to be agreements established bilaterally?

Strategy and Investment

- Is the DDCC solution intended to be a short-term solution or a long-term digital vaccination certificate or test result solution?
- What are the potential benefits, risks and costs of implementing a DDCC solution?
- What is the potential impact on public health and on the economy?
- What is the additional value added beyond using the paper system only?

Services and Applications

- Are point-of-care applications used presently to support immunization?
- Are there existing products in the marketplace that would fit your needs and adhere to international specifications and guidance?

Standards and Interoperability

- Is there an existing interoperability framework to guide how DDCC can interoperate with other existing solutions?
- Are there reusable components, such as terminology services, that could be incorporated?

Infrastructure

- How can existing digital health investments be leveraged?
- Consider the coverage of mobile phone adoption before pursuing a mobile-only solution. Is there broad mobile phone adoption and high coverage of mobile phone networks outside the major urban areas?
- Is a PKI in place that can also be leveraged to support digitally signing DDCC digital documents?

Legislation, Policy, and Compliance

- Are policies for appropriate use and data protection in place to address the ethical considerations and data protection principles of DDCC?
- For continuity of care, are digital health data sharing and consent management policies in place?
- What review processes are needed for newly developed policies?

Workforce

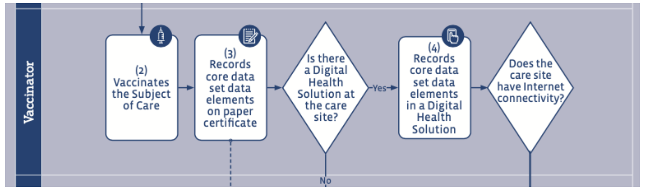
- Is the value added by the digital representation clearly communicated?
- Are change management processes and support in place when implementing DDCC?
- Is there a ready domestic supply of digital health workers? Does this workforce have the skillsets needed?

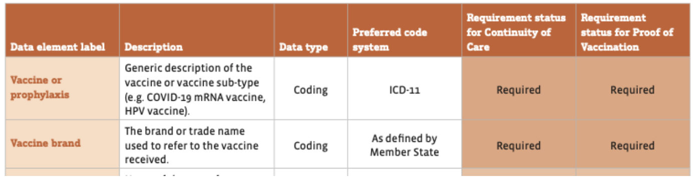
See also: *FAQ – 18. What key considerations impact upfront investments for a long-term digital certificate solution?*

Graphic and information adapted from the WHO ITU eHealth National Strategy Toolkit.

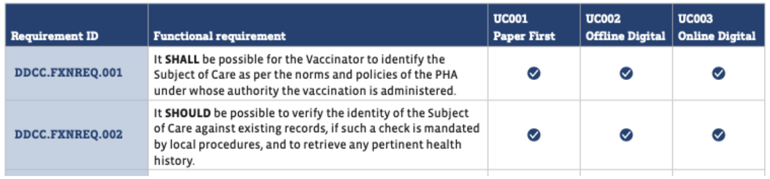
Gather health content requirements and system requirements, and adapt DDCC guidance for the intended use of digital certificates

Example workflows, data requirements, and functional requirements


Vaccinator
(2) Vaccinates the Subject of Care
(3) Records core data set data elements on paper certificate
Is there a Digital Health Solution at the care site?
Yes
No
(4) Records core data set data elements in a Digital Health Solution
Does the care site have Internet connectivity?



Data element label	Description	Data type	Preferred code system	Requirement status for Continuity of Care	Requirement status for Proof of Vaccination
Vaccine or prophylaxis	Generic description of the vaccine or vaccine sub-type (e.g. COVID-19 mRNA vaccine, HPV vaccine).	Coding	ICD-11	Required	Required
Vaccine brand	The brand or trade name used to refer to the vaccine received.	Coding	As defined by Member State	Required	Required



Requirement ID	Functional requirement	UC001 Paper First	UC002 Offline Digital	UC003 Online Digital
DDCC.FXNREQ.001	It **SHALL** be possible for the Vaccinator to identify the Subject of Care as per the norms and policies of the PHA under whose authority the vaccination is administered.	✓	✓	✓
DDCC.FXNREQ.002	It **SHOULD** be possible to verify the identity of the Subject of Care against existing records, if such a check is mandated by local procedures, and to retrieve any pertinent health history.	✓	✓	✓

Inputs

- Enabling-environment assessment
- Landscape analysis and data mapping results (Step 5)
- Personas and future state user task flow diagrams
- Functional and nonfunctional requirements for the digital certificate from the Technical Specifications and Implementation Guide
- Future state workflow with digital health interventions and requirements for digital certificate program
- National digital health architecture

Outputs

- Detailed implementation plan for digital certificate program, specifying:
  - Relevant health and data content, infrastructure, existing digital systems, standards and interoperability needs
- Functional and nonfunctional requirements for the digital certificate adapted to country needs

See also: *FAQ – 31. How do countries gather solution requirements for digital certificates (Step 6: Requirements Gathering)?*

See Annex A for additional detail on these key concepts

Finalize plans and budget for all phases of implementation

Additional resources to support implementation

- WHO interoperability standard
- Example implementations
- Software consistent with specifications' dataset and architecture
- Example specifications that can be used to guide implementation
- General implementation guidance for digital health solutions
- WHO international travel guidance
- WHO guidance on mass gatherings

Inputs

- Historical budgets and costs
- Implementation considerations for digital certificate program
- Historical and/or baseline data and analysis
- Historical M&E and adaptive management plans
- Guidance from other digital certificate implementations (e.g., EU, DIVOC)

Outputs

- Logic model for digital certificate implementation
- Implementation plan that is appropriate for the environmental limitations
- Clear mechanism for obtaining and responding to feedback from end users
- Detailed financial plan and costing (see next slides)
- M&E plan, including for adaptive management and data use

See also: *FAQ – 32. How do countries finalize plans to develop, deploy, implement, and scale digital certificates (Step 7: Plan for Development & Implementation)?*

Estimate detailed budget for each implementation phase to align with country context and intended use cases

underline = significant cost driver

Ongoing / all phases

- Governance
- Management and staffing

Development and setup

- Technology adaptation

Deployment

- Equipment and hardware
- Testing
- Training
- Roll-out
- Outreach and raising awareness

Integration and interoperability

- Establishing trust frameworks
- Interoperability with other systems

Scale

- Printing
- Human resources
- IT licensing / service provision
- IT scalability

Sustained operations

- Refresher training
- Adaptive management
- Communication
- Technology maintenance

See also: *FAQ – 32. How do countries finalize plans to develop, deploy, implement, and scale digital certificates (Step 7: Plan for Development & Implementation)?*

Investigate country context to understand unique and variable costs

Relevant cost variances*

- Equipment: whether required equipment (e.g., mobile phones, printers) is already available and can be shared across different interventions
- Training: how many people need to be trained and how training is delivered (e.g., classroom-based training, on-the-job training)
- Maintenance: how much and how frequently the solution needs to change over time (e.g., to match rapidly changing policies)

* See *Understanding Total Cost of Ownership for Digital Health* for more details on common cost variances and hidden costs for digital health interventions. https://digitalsquare.org/market-analytics.

Unique cost drivers

- Governance and outreach: how much time will be required to develop and socialize new policies with the public and prospective verifiers
- Establishing trust frameworks: how much effort will be required to establish agreements between countries and ensure certifications are accepted across borders
- Adaptive management: monitoring and evaluating use and uptake worldwide, and adapting to emerging best practices

See also: *FAQ – 33. What contextual factors need to be considered when estimating costs for a digital certificate program (Step 7: Finalize Plans and Budget)?*

Estimate ongoing costs associated to governance across all phases of implementation

Example activities* and five-year budget table

Description	One-time Costs + Year 1	Year 2	Year 3	Year 4	Year 5	Total Costs
Ongoing / all phases: Governance						
Developing new policies for ongoing monitoring of use and impact						
Allocate dedicated resources within the government or hire consultants to draft new policies for DDCC						
Conduct ongoing consultations with key partners (e.g., industry associations, PHA, regional groups) to build consensus						
Seek formal approval or ratification of new policies with relevant government bodies						
Socialize new policies with key stakeholders and the public						

* Example activities for illustrative purposes only. Each country will define actual activities, level of effort required by new or existing human resources to complete activities, and the associated cost of human resources based on country context.

See also: *FAQ – 34. What are example costs for a digital certificate program (Step 7: Finalize Plans and Budget)?*

Estimate upfront costs to adapt the DDCC standard to align with new or existing technologies to capture individual data

Example activities* and five-year budget table

Description	One-time Costs + Year 1	Year 2	Year 3	Year 4	Year 5	Total Costs
Development and setup: Technology adaptation						
Leveraging existing software systems (e.g., adapting EHR, EIR, and HMIS systems)**						
Map required data elements for certificate to existing systems						
Adapt existing system to capture additional information (e.g., vaccines), if needed						
Establish a link or integration with other electronic systems and digital health solutions (e.g., logistic management information systems (LMIS), lab management systems, Immunization eRegistry) to pull core data for DDCC						
Ensure compliance with relevant national guidelines						

* Example activities for illustrative purposes only. Each country will define actual activities, level of effort required by new or existing human resources to complete activities, and the associated cost of human resources based on country context.

** Existing systems that may already be used to capture relevant individual data required to generate digital certificates may include electronic health record (EHR) systems, electronic immunization registry (EIR) systems, and health management information systems (HMIS).

See also: *FAQ – 34. What are example costs for a digital certificate program (Step 7: Finalize Plans and Budget)?*

Estimate costs to raise awareness and establish trust in certificates both domestically and across borders

Example activities* and five-year budget table

Description	One-time Costs + Year 1	Year 2	Year 3	Year 4	Year 5	Total Costs
Deployment: Outreach and raising awareness						
Communications on when, where, and how people can obtain digital certificates						
Develop and draft communications materials for the public on obtaining a digital certificate						
Conduct workshops or meetings with key stakeholders to finalize package of communications assets						
Seek approval of communications materials with appropriate government body, if needed						
Draft a communications plan, including outreach mechanisms and timeline						
Distribute communications materials to the public across key platforms						
Integration and interoperability: Establishing trust frameworks						
Coordination for establishing bilateral agreements with other countries						
Allocate dedicated resources within the government to attend coordination meetings						
Conduct ongoing consultations with key stakeholders across ministries on potential agreement						
Seek formal approval of agreement with relevant government bodies						

See also: *FAQ – 34. What are example costs for a digital certificate program (Step 7: Finalize Plans and Budget)?*

* Example activities for illustrative purposes only. Each country will define actual activities, level of effort required by new or existing human resources to complete activities, and the associated cost of human resources based on country context.

Estimate costs to scale availability of digital certificates country-wide and sustain operations over years

Example activities* and five-year budget table

Description	One-time Costs + Year 1	Year 2	Year 3	Year 4	Year 5	Total Costs
Scale: Printing						
With the paper-first approach: need for printing increases as more people are vaccinated and subsequently receive a physical vaccination certificate						
Forecast domestic requirements for high-volume printing capacity for paper forms						
Procure devices (e.g., printers) and related materials (e.g., toner, paper) needed at the vaccination site, sample collection sites, or in the back office						
Provide continuous maintenance and replacement for devices and related materials, as needed						
Sustained operations: Adaptive management						
Monitoring and evaluation of digital certificate implementation practices and processes, with application of learnings						
Develop an M&E plan for digital certificates, including the adaptive management cycle						
Schedule regular meetings with key stakeholders to reflect on digital certificate implementation and progress						
Regularly update the M&E plan to align with ongoing digital certificate content updates in accordance with changes in national policy and context (e.g., available vaccines, available test types, variants), if needed						

See also: *FAQ – 34. What are example costs for a digital certificate program (Step 7: Finalize Plans and Budget)?*

* Example activities for illustrative purposes only. Each country will define actual activities, level of effort required by new or existing human resources to complete activities, and the associated cost of human resources based on country context.

Next steps for program managers

☑ **Ensure appropriate policy and legal frameworks are in place**

☑ **Evaluate readiness for deployment** using DDCC:VS **and** DDCC:TR guidance

☑ **Create implementation plan and budget using** Operational Guidance and DIIG

☑ **Coordinate across partners** using DDCC:VS and DDCC:TR guidance to:

- Identify partners with appropriate technical skills
- Ensure compliance for technology vendors
- Align digital certification with PHA business rules for vaccination and SARS-CoV-2 diagnostic test results

Additional Support: Requests for technical assistance can be made through DICE.
contact@digitalhealthcoe.org

See also: *FAQ – 35. What are next steps for countries considering digital certificate implementation?*

DICE | Digital Health Centre of Excellence

Annex A: Other Key Concepts

Key Concepts: Trust networks

Countries must establish trust in the issuance and verification of digital certificates

Countries must set up a national trust framework consisting of public key infrastructure (PKI) to align with established governance processes and policies to enable digital signing of digital certificates

See also: *FAQ – 36. Key Concepts: What is a Trust Network and Public Key Infrastructure (PKI)?*

Trust Network Value

- Maintains **trust in the certificate issuing and verification authorities and systems,** both domestically and across borders
- **Reduces potential for fraudulent issuance** and enables the revocation of certificates if there is evidence of fraud
- Ensures that data in the certificate was **not corrupted or modified** from its original form
- Provides a **secure method for both offline and online verification**

Key Concepts: Public Key Infrastructure (PKI)

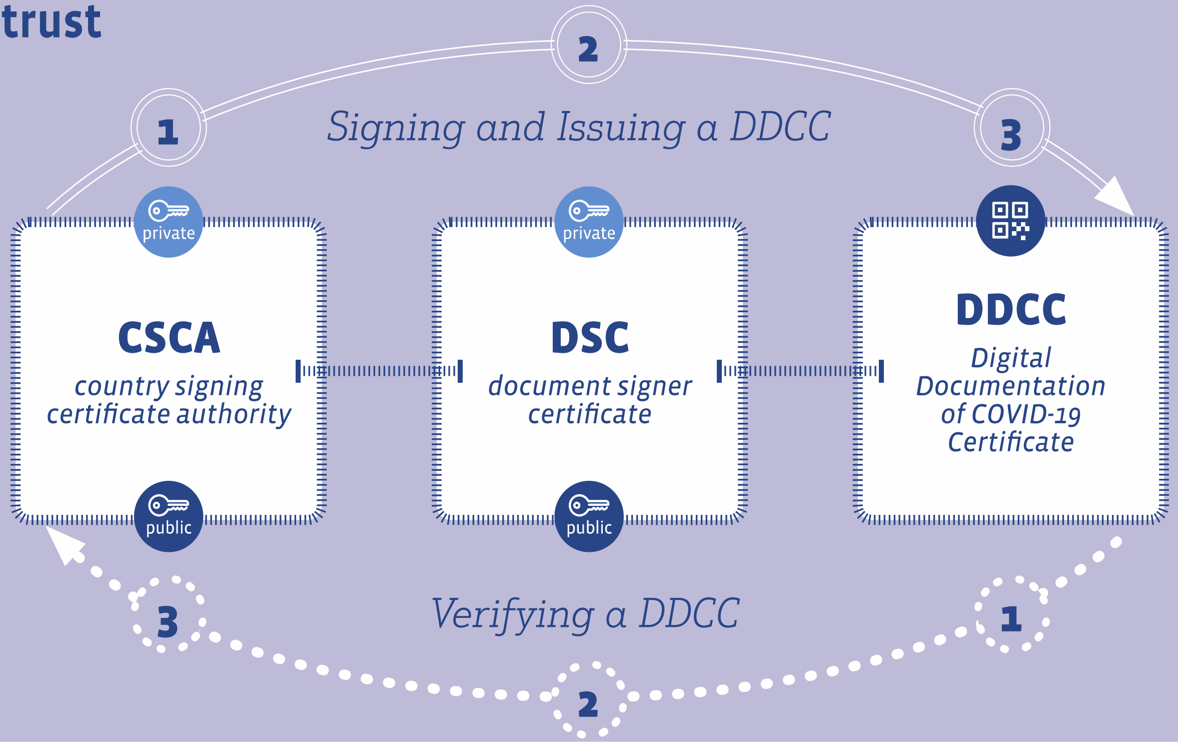
A domestic PKI is required for signing and verifying digital certificates

1 A designated government entity acts as a Country Signing Certificate Authority (CSCA)

2 A CSCA issues at least one Document Signer Certificate (DSC) with a public-private key pair that can be used to digitally sign and verify DDCC

3 A DDCC issuer must have a DSC to sign a digital certificate

The chain of trust



2
1
Signing and Issuing a DDCC
3
private
private
CSCA
country signing certificate authority
DSC
document signer certificate
DDCC
Digital Documentation of COVID-19 Certificate
public
public
3
Verifying a DDCC
1
2

$ **Activities with cost implications**

- Countries need to establish agreements with other countries that outline the governance process (e.g., policies, technical specifications, and interoperability criteria) for establishing trust
- The systems these countries have in place will impact what is needed to interoperate
- Countries must consider how to manage and ensure security of private keys

See also: *FAQ – 36. Key Concepts: What is a Trust Network and Public Key Infrastructure (PKI)?*

Key Concepts: Linking unique identification

Countries must determine the policies and procedures for linking a digital certificate to an individual's identity which is verifiable

- DDCC may encode just the Health Certificate ID (HCID) or it could encode a full representation of a certificate
- Countries may determine which unique identification (e.g., health ID, national ID number, passport number, etc.) to link with a certificate, if any
- Policies should align with agreements established with other countries

Vaccination status and SARS-CoV-2 diagnostic test result certificates are health documents, and therefore are not intended to be used as identity documents

See also: *FAQ – 37. Key Concepts: What is Identity Binding and Unique Identification?*

Key Concepts: Governing trust networks

Countries establish a PKI and determine the most appropriate governance mechanisms for its context to support the trust network

Governance needs to be established at two levels

Public Health Authority (PHA): need to generate at least one **document signer certificate (DSC)** – a private–public key pair that can be used by the trusted agents of the PHA to sign the digital certificate

Member State: need to establish a mechanism to assert that a DSC from a PHA has been authorized to sign health documents

Two approaches:

1. Root Certificate Authority
2. Master list

$

Activities with cost implications

- Determine whether to leverage an existing PKI or establish a new one
- Establish governance mechanisms for digital signing infrastructure at **PHA** and **Member State** levels with clear policies for:
  - Issuing certificates
  - Verifying certificates
  - Revocation of certificates
  - Data management and privacy protection

See also: *FAQ – 38. Key Concepts: What governance mechanisms need to be established to support the trust network?*

Key Concepts:

Cross-border policies

Bilateral and regional policy negotiations may be complicated and require significant effort by policy makers

To ensure that national governing bodies can establish mutual trust with other countries through bilateral or multilateral agreements, governance mechanisms should be in place for the digital signing infrastructure based on each country's governance context.

Considerations

- What agreements or formal collaborations will need to be established in a memorandum of understanding?
- Will there need to be agreements (e.g., data agreements) established bilaterally, multilaterally or at a regional level to establish trusted recognition between DDCC of different provenance?
- Are bilateral or regional (e.g., EU) agreements in place that can be leveraged?

Several digital certificates for COVID-19 use cases are available in the global marketplace

- EU Digital Covid Certificates (DCC) [link]
- DIVOC [link]
- Smart Health Cards/ VCI [link]

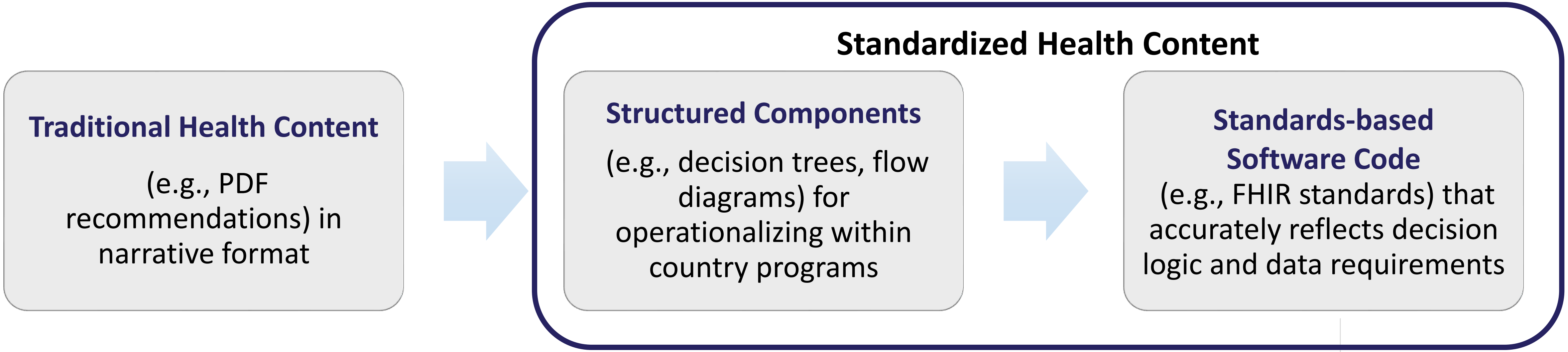
EU DCC **DIVOC** **VCI**

See also: *FAQ – 39. Key Concepts: What needs to be considered in bilateral and regional policy negotiations for digital certificates?*

Key Concepts: Standardized health content

DDCC guidance provides standardized, trusted health content aligned with international standards

DDCC standardized health content applies the WHO evidence base for any stage of digital health maturity



Traditional Health Content

(e.g., PDF recommendations) in narrative format

Standardized Health Content

Structured Components

(e.g., decision trees, flow diagrams) for operationalizing within country programs

Standards-based Software Code

(e.g., FHIR standards) that accurately reflects decision logic and data requirements

Standardized health content converts traditional health content into structured components for operationalizing DDCC guidance within country programs and software code that is aligned with international FHIR standards

Preferred digital health interoperability standards:

- **Semantic standard:** International Classifications of Diseases, 11th edition (ICD-11)
- **Syntactic standard:** Health Level Seven (HL7) Fast Healthcare Interoperability Resources (FHIR)®

See also: *FAQ – 40. Key Concepts: What is standardized health content?*

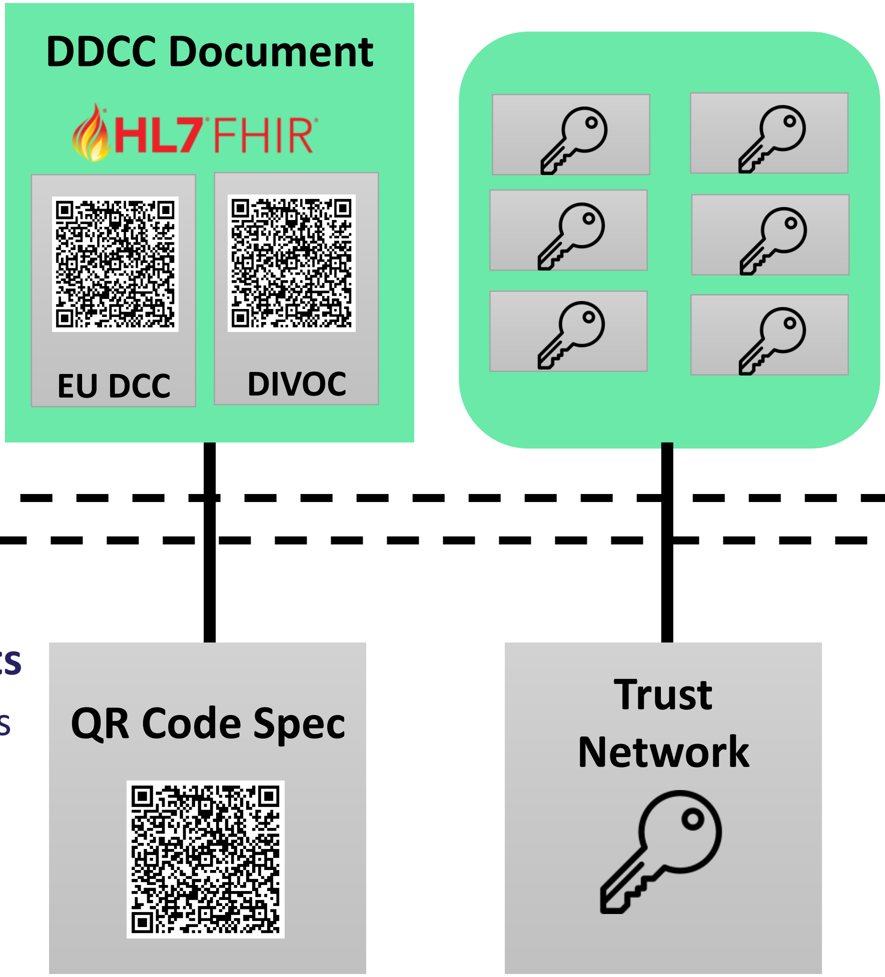
Key Concepts:

Digital certificate interoperability

DDCC is designed to enable interoperability between certificates issued in other formats and creates a compatible certificate issued via paper, PDF, or smartphones, reducing the long-term risk of changing certificates

DDCC provides an "umbrella" specification using international HL7 FHIR standard

- Provides common data model and support for multiple QR codes



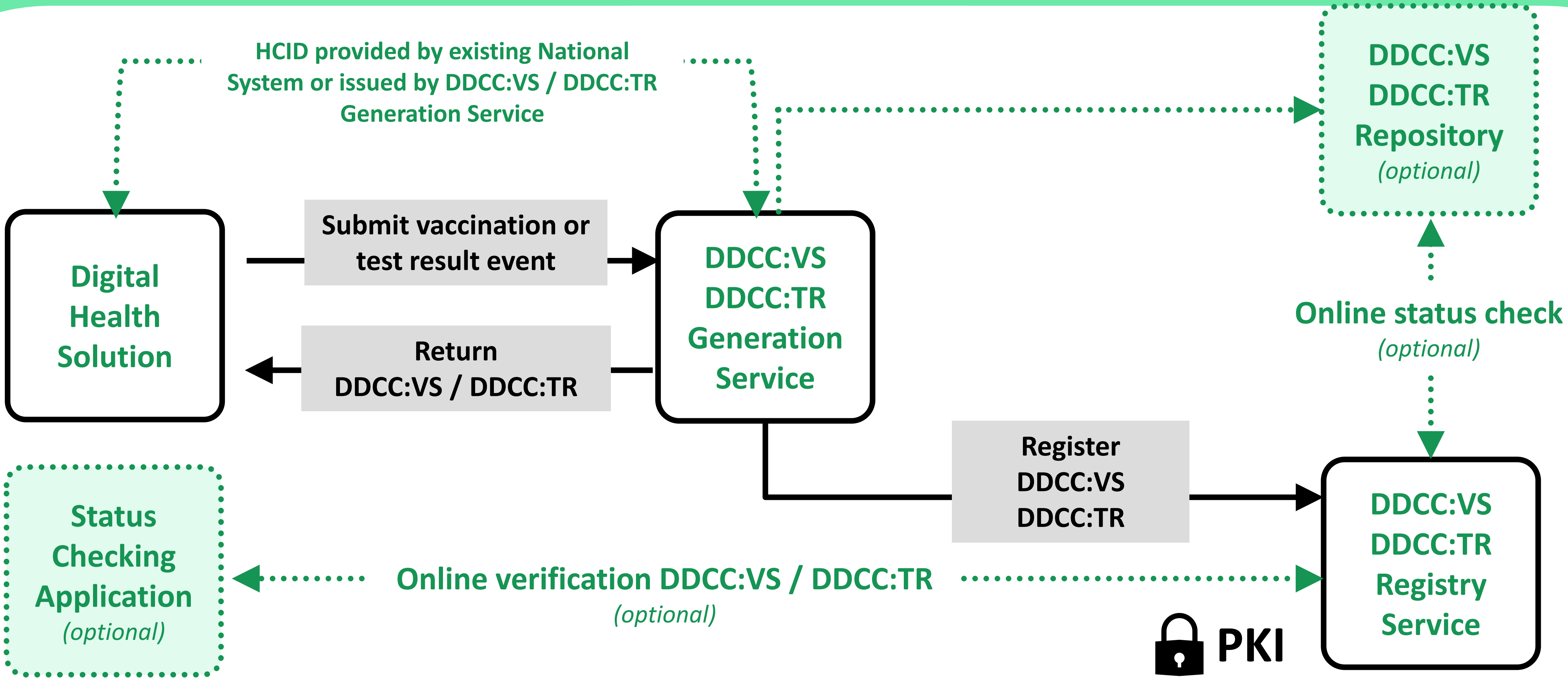
Compatible with other regional certificate formats

- EU Digital Covid Certificates (DCC) [link]
- DIVOC [link]
- Smart Health Cards / VCI [link]

See also: *FAQ – 41. Key Concepts: How does DDCC enable interoperability between certificates issued in other formats (e.g., DIVOC, EU DCC)?*

Key Concepts: Workflow for generation and verification

Required technologies include services to generate and register certificates, while additional services and applications can be built in iteratively as needed


HCID provided by existing National System or issued by DDCC:VS / DDCC:TR Generation Service
DDCC:VS DDCC:TR Repository (optional)
Digital Health Solution
Submit vaccination or test result event
DDCC:VS DDCC:TR Generation Service
Return DDCC:VS / DDCC:TR
Online status check (optional)
Register DDCC:VS DDCC:TR
Status Checking Application (optional)
Online verification DDCC:VS / DDCC:TR (optional)
DDCC:VS DDCC:TR Registry Service
PKI

See also: *FAQ – 42. Key Concepts: What are the required and optional components of DDCC?*