Digital Documentation of COVID-19 Certificates (DDCC)

Frequently Asked Questions (FAQ)

DICE Digital Health Centre of Excellence

unicef

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/

Table of Contents

Introduction

1. How can countries use Digital Documentation of COVID-19 Certificates (DDCC) materials?

The Digital Documentation of COVID-19 Certificates (DDCC) provides implementation guidance for adapting digital certificate programs in country. This documentation is written as interim guidance for countries to respond to the ongoing global COVID-19 pandemic through immediate use cases of standardized digital certificates for Vaccination Status (VS) as well as a negative SARS-CoV-2 diagnostic Test Result (TR). The World Health Organization (WHO) has developed this guidance and accompanying technical specifications, in collaboration with a multidisciplinary group of partners and experts, to support WHO Member States in adopting interoperable standards for recording vaccination status and SARS-CoV-2 diagnostic test results in standardized certificates. The approach could eventually be extended to capture future use cases such as vaccination status to protect against other diseases.

Communication materials include the **DDCC Overview** presentation which summarizes the elements, key concepts, and value of the DDCC standard, and supports policy makers and program managers to make the case for sustainable investment in national digital certificate solutions. A separate **Operational Guidance** section elaborates on technical and operational concepts contained in the DDCC Overview presentation with detail on what costs to estimate and how to operationalize a digital certificate program in country.

This **FAQ** is intended to be used as a companion guide to the DDCC Overview and Operational Guidance materials. The FAQ contains further detail on the concepts presented in the DDCC Overview in narrative form, aligned with commonly asked questions, and links to further information.

2. Who is the audience for DDCC materials?

DDCC materials are written for two primary audiences:

- **Policy Makers** or other digital leads within different ministries. These are individuals who need to make decisions to inform policy and advocate for funding. The overview for this audience focuses on value, key concepts that may be unfamiliar, and making the case for investing in DDCC-based solutions.
- **Program Managers** and operational support staff, within government or external partner organizations. These are individuals who need to make operational decisions and plan implementations. This overview provides additional detail on how to set up a digital certificate program and how to plan deployments. Program managers and operational decision makers can use DDCC overview to help guide their technology partners on minimum requirements for vaccine status and test result certificates.

DDCC Overview

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 supports standardized health certificate generation and status **verification** and **validation** across domestic and international use cases, at any stage of digital system maturity.

- **Verification:** relies on the Verifier confirming the status of a test result certificate and ensuring that it is a true and unaltered certificate, which has been signed and issued under the authority of a Public Health Authority of a Member State (i.e., verification answers the question, "is this from a trusted source?").
- **Validation**: relies on the Verifier validating and accepting the test result certificate based on the acceptance criteria and associated validity period, as determined by the policies of the Member States that the certificate is going to be used in (i.e., validation answers the question, "with the data I am provided with, do I accept this certificate based on existing policies?").

DDCC Guidance is:

- Guidance for capturing the **core data set** to document an individual's vaccination status and SARS-CoV-2 diagnostic test results.
- A mechanism for **linking different certificate products** (e.g., EU DCC, DIVOC, Smart Health Card), **into a compatible certificate** for issue via paper, PDF, or smartphone.
- A **flexible solution** that allows Member States to customize for different use cases and data elements (e.g., which vaccines you use).
- An approach that is **adaptable for future use cases and guidance**, beyond COVID-19. It is also adherent to the international patient summary which can be a basis of a personal health record or shared health record.

While the DDCC is implementation guidance for adapting digital certificate programs in country, **it is not** intended to be an identity card or passport. Furthermore, DDCC does not provide guidance on national COVID-19 travel or vaccination policies or for the International Certificate of Vaccination or Prophylaxis (i.e., "yellow card")[1].

[1] The International Certificate of Vaccination or Prophylaxis and a national immunization home - based record are not considered DDCC:VS because they are not available in a digital format and do not meet the requirements outlined in this technical specifications and implementation guidance document.

Further information:

- Digital Documentation of COVID-19 Certificates: Technical Specifications and Implementation Guidance for Vaccination Status (VS) and Test Result (TR)
  - Refer to Executive Summary
- Policy guidance regarding the use of COVID-19 vaccination status and test result certificates is available from the WHO:
  - Technical considerations for implementing a risk-based approach to international travel in the context of COVID-19: Interim guidance, 2 July 2021
  - 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
- EU Equivalence decision procedure

4. What is included in DDCC Guidance?

DDCC contains implementation guidance for policy makers and requirements and specifications for technology implementers.

Implementation Guidance

- Data protection principles
- Ethical considerations
- National governance considerations

Requirements and specifications for technology implementers

- Functional and non-functional requirements
- Core data set, defining required and optional data elements, mapped to standard terminology code sets
- HL7 FHIR Implementation Guide detailing relevant standards for consistent representation and interoperability
- Business processes, workflows & use cases
- Overview of signing a digital certificate with Public Key Infrastructure (PKI)

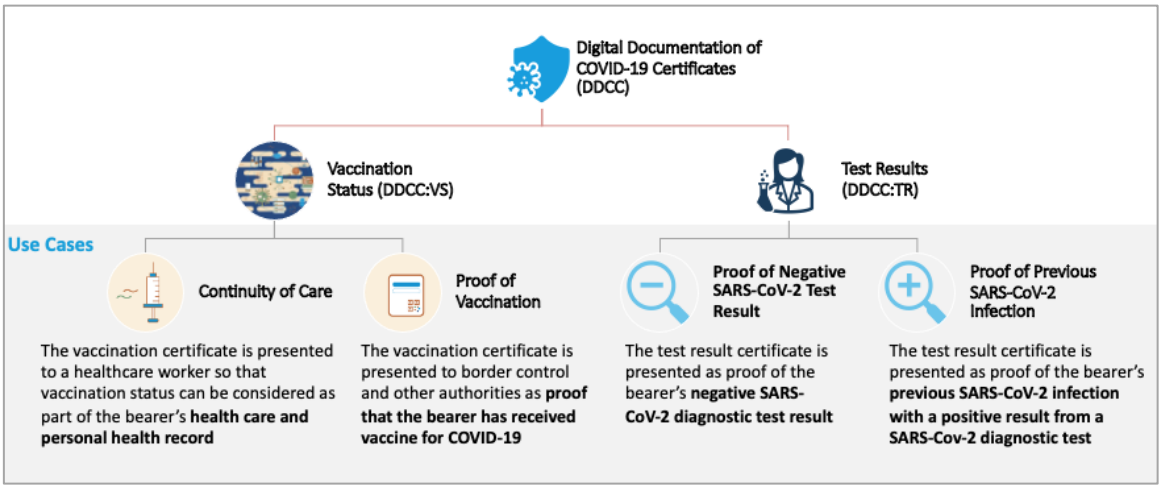
Further information:

- Digital Documentation of COVID-19 Certificates: Technical Specifications and Implementation Guidance for Vaccination Status (VS) and Test Result (TR)
- DDCC HL7 FHIR Implementation Guide

5. What are the use cases for Vaccination Status and Test Result certificates?

There are four use cases for Vaccination Status and Test Result certificates as represented in the figure below:

Figure A: Use Cases for Vaccination Status and Test Result Certificates



Further information:

- Digital Documentation of COVID-19 Certificates: Technical Specifications and Implementation Guidance for Vaccination Status (VS) and Test Result (TR)
  - Refer to Executive Summary (Table 1)

6. How are Vaccination Status and Test Result certificates issued?

DDCC supports **certificate issuance** in three modalities. Countries choose the modality that works best within the country context.

1. **Traditional paper record** (e.g., handwritten paper certificate with health certificate identifier or 2D barcode that gives unique ID).
2. **Digital** representation of traditional paper record (e.g., **PDF** print-out certificate).
3. **Purely digital** (e.g., stored in a smartphone application or on a cloud-based server).

The link between the paper record and the digital record can be established using a barcode, for example, printed on or affixed to the paper vaccination card.

Note: A digital certificate should never require individuals to have a smartphone or computer. Therefore, to ensure that citizens who do not have access to technology are able to benefit from a digital certificate, the provision of DDCC guidance and specifications follows an approach that supports paper augmented by printed digital QR codes.

Further information:

- Digital Documentation of COVID-19 Certificates: Technical Specifications and Implementation Guidance for Vaccination Status (VS) and Test Result (TR)
  - Refer to Executive Summary

7. What standardized data does the digital certificate include?

DDCC certificates include standardized human and machine-readable health data. DDCC defines the **core data set** required to generate and verify certificates for SARS-CoV-2 diagnostic test results and vaccination status. This includes key test result data such as personally identifiable information, test type, pathogen targeted, date and time of sample collection, test results, and the country where the testing took place. For vaccination status, this includes personally identifiable information, vaccine or prophylaxis, vaccine brand and batch, vaccination date, dose number, country of vaccination, and the centre where the vaccination took place. Countries may extend this core data set to store other data based on their requirements.

Further information:

- Digital Documentation of COVID-19 Certificates: Technical Specifications and Implementation Guidance for Vaccination Status (VS) and Test Result (TR)
  - Refer to Section 5.2: Core data elements

8. What digital health interoperability standard does DDCC certificates use?

DDCC uses the Health Level Seven (HL7) Fast Healthcare Interoperability Resources (FHIR)® standard. Each certificate is a human- and machine-readable package of data in a standard HL7 FHIR "Bundle" that contains all information necessary to verify a person's vaccination status or SARS-CoV-2 diagnostic test result. This "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.

Example FHIR Bundle contents for a Vaccination Status certificate includes a unique identifier for the certificate Bundle; the type of FHIR Bundle (e.g., document); the date and time the certificate Bundle was assembled; a link to health certificate identifier (HCID); and signature of issuing public health authority to verify the authenticity of the certificate. Health information contained in the certificate Bundle includes patient details, organization where the immunization was administered;

immunization details (e.g., type of vaccine, lot number); recommended date of next immunization (if applicable); and QR code representation of health information.

Further information:

- DDCC HL7 FHIR Implementation Guide
- External Links:
  - OpenSRP FHIR Core Smart Vaccination Certificates
  - Open SRP FHIR Core Smart Vaccination Certificates for Android
  - OpenHIE DDCC FHIR Implementation Guide

9. How are countries approaching digital certificates today?

There are many standardized certificates available in the marketplace. This includes major international certificate solutions such as the EU Digital Covid Certificates (DCC), DIVOC, and Smart Health Cards / VCI, each with its own standard that allows cross-border interoperability. Countries are also developing their own local solutions, which may or may not be interoperable for the certificate to be used across borders.

The DDCC standard is compatible with the major international certificate standards. DDCC provides a common international and extensible format that is interoperable with other available digital certificate formats used in African, European, and South-East Asia regions.

Countries are using data from their health systems to produce secure digital certificates for COVID-19 vaccination or SARS-CoV-2 diagnostic test results and linking those certificates with national, regional, and global standards, including WHO guidelines.

Further information:

- DIVOC (Digital Infrastructure for Vaccination Open Credentialing) in India
- EU Digital COVID Certificate Gateway
- CORESIA (COVID-19 Vaccination Policy Research and Decision Support Initiative in Asia)

10. How do DDCC certificates interoperate with other vaccination status and test result certificates?

The DDCC standard provides an “umbrella” specification to link these different certificates together using international standards (e.g., FHIR international patient summary). This allows a compatible certificate to be issued through paper, PDF, or smartphone that is linked to the DDCC. For instance, a country may have their own certificate and want a bilateral relationship with a country with a different certificate and QR code specification, and also want to interoperate with the EU DCC. The

DDCC provides a cohesive framework through which any certificate that is implemented by a country can be supported.

Further information:

- DDCC HL7 FHIR Implementation Guide
- External Links
  - DIVOC (Digital Infrastructure for Vaccination Open Credentialing) in India
  - EU Digital COVID Certificate Gateway
  - Open SRP FHIR Core Smart Vaccination Certificates for Android
  - OpenHIE DDCC Transactions Mediator

11. What ethical considerations and data protection principles need to be considered in a digital certificate solution?

Ethical considerations and data protection principles should be an integral part of the design and deployment of any digital certificate solution. This is to protect and promote the welfare of individuals, communities, and the population as a whole; 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. It also serves to create and maintain trust in public health activities as part of the health-care system. Using DDCC as a health pass risks introducing unfair disadvantages and injustices. For instance, requiring vaccination status certificates as a prerequisite for receiving healthcare or attending school could potentially exacerbate inequalities in the ability for all citizens to access fundamental public services.

The DDCC guidance provides recommendations for supporting the ethical use of digital certificates. These include clearly defining the scope of use of digital certificates and assessing the potential benefits, costs, and risks before introducing digital certificates. Countries should also ensure that all citizens have equitable access and the ability to use certificates and that all necessary measures are in place to protect sensitive health data. The use of digital certificates should be clearly and transparently communicated and constantly monitored for impact, making adjustments where necessary.

Further information:

- Digital Documentation of COVID-19 Certificates: Technical Specifications and Implementation Guidance for Vaccination Status (VS) and Test Result (TR)
  - Refer to Section 2: Ethical considerations and data protection principles

Value of Standardized and Interoperable Certificates

12. What is the need for standardized and interoperable certificates?

There is a complicated, evolving scientific landscape around COVID-19 and lack of global policy coordination on vaccination status and test result certificates. This creates challenges for countries that are moving forward with developing and deploying certificate solutions.

Countries are responsible for implementing their own policies and certificate solutions, but there is little understanding of the complexities of implementing certificates, the options available, or the best product to choose for the national context, which slows deployment of certificate solutions, making it difficult to validate vaccinations and SARS-CoV-2 diagnostic test results.

Potentially incompatible certificates limit ability of healthcare workers, border agents, and other authorities to validate vaccination and SARS-CoV-2 diagnostic test result status. Lack of compatible certificates also limits the ability of beneficiaries to hold their own information regarding vaccination status and SARS-CoV-2 diagnostic test results.

There is a need for a standards-based solution that will achieve compatible certificate systems and does not have to be re-done as the science and policies around COVID-19 change and can extend to future use cases as COVID-19 evolves.

13. What advantages do digital certificates have over paper formats?

There are issues today with paper-based COVID-19 vaccination status and test result certificates without QR codes. Paper certificates or photocopies are prone to fraud and other issues such as loss, damage, or unauthorized disclosure or breach of personal data. There is ample anecdotal evidence to suggest health certificate fraud is expanding rapidly around the world, including in low and middle-income countries where vaccination rates are lower. A recent study shows health-related data sells for nearly 50 times more on the black market than payment card data, due to the possible inclusion of personally identifiable information that can be used for identity theft or fraudulent billing[2].

Digital systems can ensure that **authenticated, digitally signed certificates** and **precise, standardized data** can be shared domestically and across borders. This supports bilateral or multilateral agreements to recognize **legal requirements for vaccination status and SARS-CoV-2 diagnostic test results** across borders, such as EU equivalency. These digital systems can also address fraud, loss, damage, or unauthorized use of paper certificates.

Digital systems can also address other issues with paper certificates such as **loss, damage**, or **unauthorized disclosure** or **breach of personal data**.

[2] https://www2.deloitte.com/content/dam/Deloitte/global/Documents/Risk/gx-feb-21-are-vaccine-credentials-the-next-vector-for-cyber-risks-v5.pdf

14. What value do standardized digital certificates bring to country health systems?

Implementing **standardized, authenticated digital certificates** can help nations as they adapt to the evolving COVID-19 landscape, and beyond. They support **reopening economies** by enabling the faster, more secure verification and validation of status required to facilitate cross-border movement, commerce, and economic security and access certain socioeconomic activities. They can **increase equitable access to health information** by bringing critical health information into the context of care and personal health records via digital tools (e.g., digital immunization records). Digital certificates also support the long-term need for countries to **strengthen digital health infrastructure** by standardizing health content and providing infrastructure that strengthens health information exchange capabilities.

15. What value do standardized digital certificates bring to technical implementers?

DDCC provides clear guidance for designing systems that easily interoperate with existing digital tools, such as vaccination campaign systems and immunization registers, and build a foundation for long-term health information exchange via **interoperable digital health systems.** DDCC is a flexible solution that can be **adapted to fit country and regional ecosystems**. It works for central or federated certificate issuers and generates QR codes that are compatible with other certificate programs (e.g., EU, DIVOC)**.** By adopting the DDCC standard, local technology partners can **develop local solutions** for COVID-19 and future digital health interventions that best fit local needs.

16. What value does DDCC certificates and guidance bring to individual stakeholders?

DDCC guidance and standardized digital certificates bring benefits to those making decisions and supporting the implementation.

For **Policy makers,** DDCC guidance enables the development of usable, compatible digital certificates and supports the rapid dissemination and application of new policy**.** For **Program managers**, DDCC guidance supports easier implementation by technical partners and reduces vendor lock-in.

For **Health workers**, clinical decision support enabled by standardized digital certificates ensures these workers know the vaccination status of a patient and can provide a subsequent dose and better care based on guidelines.

For **border control agents and other verifiers,** standardized digital certificates allow faster and more accurate interpretation of vaccination status or SARS-CoV-2 diagnostic test results through decision support in accordance with rapidly changing science and policy.

For **software developers** supporting the implementation, DDCC guidance provides an ecosystem of open-source FHIR tools that reduces software development time. For the support team, DDCC

guidance standardizes data and use cases for certificates, and resulting support needs regardless of health program.

For **individuals,** digital certificates provide the certificate holder with standardized core data that applies across borders and use cases and will remain valid even as policies evolve. This is particularly useful given the complexity, variation, and frequency of changes in policies and guidelines across different geographies.

Making the Case for Investment

17. Why invest in digital certificates over traditional paper certificates?

DDCC standards and implementation guidance is designed to advance country digital health systems. Upfront investment in DDCC certificate development, related infrastructure, and policy will not only support standards-based digital health interventions now but can also strengthen systems for future use cases and pandemics, reducing the overall costs for certificate generation in the long run.

For example, digital certificate and services are extensible and can be updated to include additional data or functionalities to respond to policy changes such as evolving traveler testing requirements. The infrastructure can be used to service other types of certificates in health, such as digital immunization records, or other health domains. In addition, 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.

18. What key considerations impact upfront investments for a long-term digital certificate solution?

There are several key considerations that may impact the required upfront investment. Countries should consider the governance and leadership structures that exist, the costs and benefits of digital certificates, services and applications that already exist or are readily available in country, the equipment and infrastructure available to support digitally signed certificates, the legal and policy environment for data protection and sharing, and the available workforce and mechanisms for change management and training. The major questions to be answered include the following:

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 (and planned) digital health investments be leveraged?
- Is a public key infrastructure (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?
- 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?

Further information:

- Digital Documentation of COVID-19 Certificates: Technical Specifications and Implementation Guidance for Vaccination Status (VS) and Test Result (TR)
  - Refer to Section 8.1 Considerations before deploying

19. What types of costs need to be considered across digital certificate implementation phases?

As with any digital health solution, costs for digital certificate implementation will need to factor in not only costs to develop and set up a digital certificate application, but also costs to deploy the certificates, integrate them into national systems, and scale and sustain their operation over a multi-year period.

There are six cost categories defined in the DDCC implementation guidance. They include ongoing costs related to the governance, management, and staffing of a digital certificate program as well as operations costs for five phases of solution implementation:

1. Development and setup - Technology adaptation
2. Deployment - Equipment and hardware, Testing, Training, Roll-out, Outreach and raising awareness
3. Integration and interoperability - Establishing trust frameworks, Interoperability with other systems
4. Scale – Printing, Human resources, IT licensing / service provision, IT scalability
5. Sustained operations - Refresher training, Adaptive management, Communication, Technology maintenance

The level of costs will depend on decisions and policies that a country is taking as well as what infrastructure and human capacities already exist to support a digital certificate program. For instance, whether a country is taking a short-term approach just for COVID-19 or a long-term view that contemplates future use cases, or the next pandemic - would have implication on the scope and cost. The operational guidance provides example activities within these different cost categories and an example budget template for implementers to cost each activity.

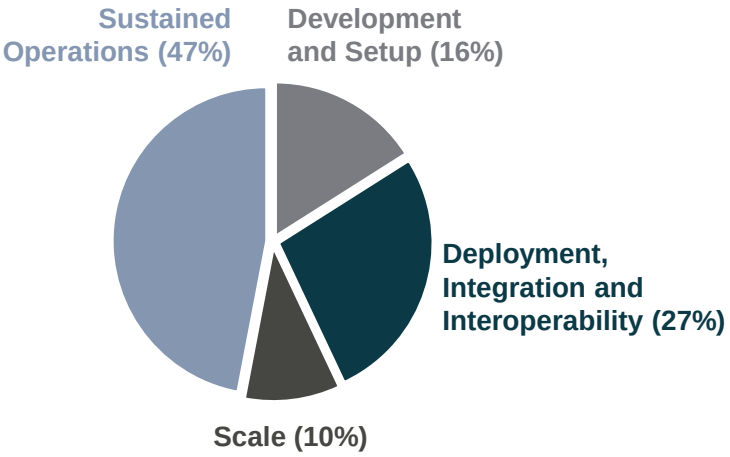
Further information:

- Digital Documentation of COVID-19 Certificates: Technical Specifications and Implementation Guidance for Vaccination Status (VS) and Test Result (TR)
  - Refer to Section 8.3: Cost category considerations
- Digital implementation investment guide (DIIG): integrating digital interventions into health programmes
  - Refer to Chapter 7: Develop a Budget
- Understanding Total Cost of Ownership for Digital Health (Digital Square): executive summary and full report

20. How might costs for a digital certificate program break down by implementation phase?

Countries considering long-term investments for digital certificates will want to consider the total cost of ownership (TCO) of the certificate solution over a multi-year period. The figure below provides an illustrative breakdown of a typical digital health solution over a five-year period. It is important to note that, 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.

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



Source: Understanding Total Cost of Ownership for Digital Health

** Total Cost of Ownership breakdown is 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.*

Further information:

- Understanding Total Cost of Ownership for Digital Health (Digital Square): executive summary and full report

21. How should countries approach the sustainable financing of digital certificate solutions over the long term?

Creating a transparent understanding of costs per phase of implementation allows countries to advocate for initial phase donor investment, bolstered by long-term government budget commitment, and supports aligning upfront with funder missions and priorities. It is envisioned that donor community investments would most likely support early stages of solution planning and development through deployment, and annual government-managed budget commitments would predominately support integration through to scale and sustained operations.

To achieve sustainable financing of digital certificate solutions, countries will need to determine the level of up-front investment required for initial phases, depending on country context. Countries

also need to determine annual operating costs and obtain government commitment to schedule annual operating costs under government budget (or long-term health system strengthening funding). With both sets of costs defined, countries can advocate for initial phase donor investment and demonstrate long-term government budget commitment to potential funders.

Further information:

- Digital implementation investment guide (DIIG): integrating digital interventions into health programmes
  - Refer to Chapter 7: Develop a Budget
- Understanding Total Cost of Ownership for Digital Health (Digital Square): executive summary and full report

22. What sources of financing may be available to support DDCC implementation?

Funding support for DDCC implementation may be available through the digital health ecosystem or related national programs. Countries can make a request through the Digital Health Center of Excellence (DICE) to connect with implementing partners and technical support. Countries can also work with leaders of related digital investments, such as electronic immunization registries or vaccine distribution programs, to determine where there may be shared resources and infrastructure. There is also opportunity to engage with regional groups working on certificate standards to support international agreements to see if there are resources or funding that could be available to support financing implementations.

Further information:

- How to engage with DICE or send an email to contact@digitalhealthcoe.org

23. How can countries request technical assistance through DICE?

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

The first step is to make a request to DICE for technical assistance. Requests should come from a government insitution or government-endorsed partner. The request should include a brief description of 1) the specific health system processes or functions that need to be addressed through the digital health intervention (e.g., technology, system, or platform); 2) the need addressed for the digital health intervention and how it advances national strategies and plans, such as the county's eHealth or Digital Health strategies and the National Vaccine Deployment Plan

(if COVID-19 vaccine related); and 3) the main in-country stakeholders that should be included in the process.

The general process for engaging with DICE can take a few weeks to a few months. The process typically begins with a needs analysis, problem definition, and anticipated outcomes. This is followed by an assessment of platforms and deployment readiness with stakeholders to make recommendations for technical assistance.

Further information:

- How to engage with DICE or send an email to contact@digitalhealthcoe.org

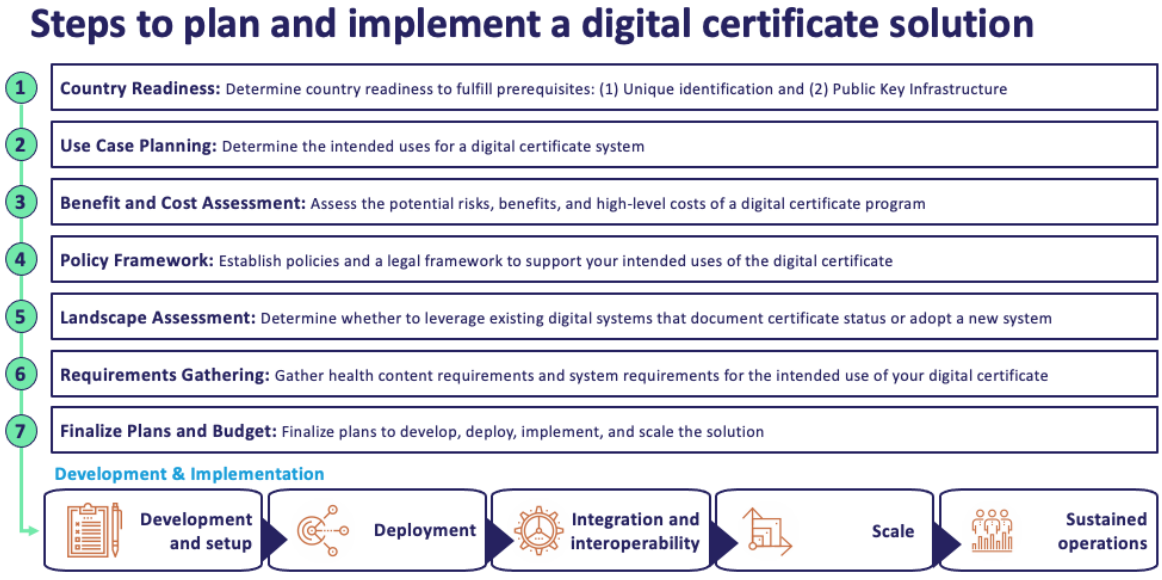
Operational Guidance

24. What are the overall steps to planning and implementing a digital certificate solution?

The first step to planning a digital certificate system is assessing country readiness to fulfill pre-requisites, namely evaluating the readiness of a Public Key Infrastructure (PKI) and determining how the unique identification of indivdiuals and entities will be linked to the certificate through the PKI (Step 1).

Once these pre-requisites have been established, implementation planning starts with determining intended uses for a digital certificate system (Step 2). This is followed by a benefit and cost assessment to understand the potental uses for a digital certificate system (Step 3). Countries will need to establish policies and a legal framework to support the intended use cases of the digital certificate (Step 4) and make decisions whether to utiize any existing digital systems that document certificate status or adopt a new system (Step 5). Once these key decisions are made, the next step is to gather health content and system requirements for supporting the intended use of the digital certificates (Step 6). Finalize plans and budget for development and implementation (Step 7), prior to starting implementation activities to develop, deploy, integrate, scale, and sustain the digital certificate solution. These seven steps are outlined in the graphic below and further elaborated in the Operational Guidance section of the DDCC Overview.

Figure C: Steps to planning and implementing digital certificate solution



Further information:

- Digital Documentation of COVID-19 Certificates: Technical Specifications and Implementation Guidance for Vaccination Status (VS) and Test Result (TR)
- Digital implementation investment guide (DIIG): integrating digital interventions into health programmes

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

Two important prerequesites need to be in place to ensure trust in a digital certificate system**.**

1. **Countries must determine an acceptable and ethical way to link certificates to the identity of the individual holding the certificate.** At a minimum, name and date of birth are required by DDCC. Countries also determine which additional unique identification (e.g., health ID, national ID number, passport number, biometrics) to link with a certificate, if available.

2. **Countries must determine existence of a national Public Key Infrastucture (PKI) that can be leveraged to issue and to verify digital certificates.** A PKI guarantees that the information contained in DDCC certificates has been validated by an accredited authority. The PKI may already be available for other domains such as law enforcement or the financial sector. If a PKI is not already available to support signed digital certificates, one must be set up. Each country would be responsible for managing its own PKI through its Public Health Authority (PHA) or another national delegated authority.

Further information:

- Digital Documentation of COVID-19 Certificates: Technical Specifications and Implementation Guidance
  - Vaccination Status (VS) - Refer to Section 6: National Trust Architecture and Annex 4: What is public key infrastructure (PKI)
  - Test Result (TR) - Refer to Section 6: PKI for Signing and Verifying a DDCC: TR
- Digital documentation of COVID-19 certificates: vaccination status: technical specifications and implementation guidance, web annex B: technical briefing, 27 August 2021
  - Refer to annex B

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

Countries select one or more use case for digital certificates for vaccine status or SARS-CoV-2 diagnostic test results that support country policies. This step should result in a problem statement detailing specific challenges that each digital certificate use case will address; a list of priorities for the digital certificate program that align with national digital health strategy; an organogram for prospective digital certificate program; and a list of stakeholders to engage.

Key inputs to this process include the national digital health or eHealth strategy (if one exists), documents outlining COVID-19 response interventions (e.g., objectives, progress, and any evaluations); and any organograms describing relevant directorates or departments such as ministries of health, ICT, border control, and civil registrars.

Further information:

- Digital Documentation of COVID-19 Certificates: Technical Specifications and Implementation Guidance for Vaccination Status (VS) and Test Result (TR)
  - Refer to Executive Summary: Table 1 (uses of certificates)
- Digital implementation investment guide (DIIG): integrating digital interventions into health programmes

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

An assessment of risks, benefits, and high-level costs can inform inform the design of digital certificate programs as well as key policy decisions that need to be made to support the program. This step should result in current-state ("status quo") workflow diagrams illustrating the user journey of selected digital certificate program processes; prioritized bottlenecks mapped to a list of health system challenges to be addressed; an enabling-environment assessment defining possible constraints; and high-level cost estimate to inform go / no-go decision to proceed with program development.

Key inputs to this process include an identified team and list of stakeholders to be engaged throughout the planning and implementation process; the shared vision of digital certificate program goals; definition of personas for the digital certificate program; documentation of digital certificate program objectives and progress; 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.

Further information:

- Digital Documentation of COVID-19 Certificates: Technical Specifications and Implementation Guidance for Vaccination Status (VS) and Test Result (TR)
  - Refer to Section 2: Ethical considerations and data protection principles
- Digital implementation investment guide (DIIG): integrating digital interventions into health programmes

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

Countries should have policies and a legal framework for appropriate use, data protection, and governance of the digital certificate. The output of this step is a detailed implementation plan that specifies governance, workforce and training activities, and links to strategy and investment plans.

Inputs to this process may include an enabling-environment assessment; ethical considerations; personas and future state user task flow diagrams; and high-level data requirements and national data privacy laws.

Additional governance considerations include ensuring policies are in place for issuing and verifying digital certificates, including policies for data management and privacy protection, and policies for the revocation of digital certificates, including informing individuals, informing verifiers, and remedy provision.

Further information:

- Digital Documentation of COVID-19 Certificates: Technical Specifications and Implementation Guidance for Vaccination Status (VS) and Test Result (TR)
  - Refer to Section 1.6: Additional WHO guidance documents and Section 7: National governance considerations
- Digital implementation investment guide (DIIG): integrating digital interventions into health programmes

29. How do countries assess existing digital systems and architecture (Step 5: Landscape Assessment)?

Countries determine whether to leverage existing digital systems that document certificate status or adopt a new system. This decision is based on the existing digital health enterprise architecture and the country's overall digital health strategy.

Outputs for this step include: core functional requirements for the planned digital certificate investment within the enterprise architecture; the 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; and identified digital health interventions that capture the data required for the digital certificate program.

Inputs to this process include defined future-state workflow and functional requirements for digital certificate program and the national digital health enterprise architecture (if available in country).

Further information:

- Digital Documentation of COVID-19 Certificates: Technical Specifications and Implementation Guidance for Vaccination Status (VS) and Test Result (TR)
  - Refer to Section 8: Implementation considerations
- Digital implementation investment guide (DIIG): integrating digital interventions into health programmes

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

Data from existing data systems can be pulled into the certificate generation service. Countries implementing DDCC will need to do a mapping to determine the requirements for system integrations, hold discussions with system owners and establish data sharing agreements, and build out and maintain systems.

For the landscape assessment, countries will need to identify which digital health systems available in country could be accessed for the required information. This may include lab systems, Civil Registration and Vital Statistics (CRVS) systems, and Electronic Health Records (EHR) systems. The assessment should consider whether the information is directly accessible through a system integration, how many system integrations will be required, and their complexity.

Further information:

- Digital Documentation of COVID-19 Certificates: Technical Specifications and Implementation Guidance for Vaccination Status (VS) and Test Result (TR)
  - Refer to Section 4.4: Determine if existing digital health applications, platforms and enterprises can achieve the requirements
- Digital implementation investment guide (DIIG): integrating digital interventions into health programmes

31. How do countries gather solution requirements for digital certificates (Step 6: Requirements Gathering)?

Step 6 involves gathering health content requirements and system requirements and adapting DDCC guidance for the intended use of your digital certificate. These adapted system requirements should be informed by the supporting policy and legal framework (including ethical and privacy considerations) and country needs. Outputs of this step include a detailed implementation plan for digital certificate program, specifying: relevant health and data content, infrastructure, existing digital systems, standards and interoperability needs; and functional and non-functional requirements for the digital certificate adapted to country needs.

Inputs to this process include an enabling-environment assessment; results of a landscape analysis and data mapping results (see FAQ question 30, above); personas and future state user task flow diagrams; functional and non-functional 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; and national digital health architecture.

Further information:

- Digital Documentation of COVID-19 Certificates: Technical Specifications and Implementation Guidance for Vaccination Status (VS) and Test Result (TR). Refer to:
  - Sections 3 and 4: use cases
  - Section 5: core data set for workflows, data requirements and functional requirements
- Digital implementation investment guide (DIIG): integrating digital interventions

32. How do countries finalize plans and budget to develop, deploy, implement, and scale your digital certificate (Step 7: Finalize Plans and Budget)?

Once countries complete steps one through six, they are ready to finalize plans and budget for all phases of implementation. Outputs of this step include: 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 FAQ questions 33 and 34, below); and an M&E plan, including for adaptive management and data use.

Inputs to this step include historical budgets and costs; implementation considerations for digital certificate program; historical and/or baseline data and analysis; historical M&E and adaptive management plans; and guidance from other digital certificate implementations (e.g., EU, DIVOC).

A clear mechanism for obtaining and responding to feedback from end users will need to be established, including a mechanism to consistently push updates.

Additional resources to support implementation

- WHO interoperability standard for DDCC
  - DDCC HL7 FHIR Implementation Guide
  - DDCC:VS Core Data Dictionary
  - DDCC:TR Core Data Dictionary (available soon)
- 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

Further information:

- Digital Documentation of COVID-19 Certificates: Technical Specifications and Implementation Guidance for Vaccination Status (VS) and Test Result (TR).
  - Section 8: Implementation considerations
  - Section 8.4: Additional resources to support implementation
- Digital implementation investment guide (DIIG): integrating digital interventions into health programmes

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

As described in FAQ question 19, above, there are six cost categories defined in the DDCC implementation guidance. They include ongoing costs related to the governance, management, and staffing a digital certificate program as well as operations costs for five phases of solution implementation:

- 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

Country context is key to estimate cost for any digital health intervention. For instance, the existence of mobile phones and printers that can be used or shared across different interventions would impact equipment costs. The number of people that need to be trained and how that training is delivered (e.g., classroom-based training, on-the-job training) would impact training costs. Maintenance requirements informing how much and how frequently the solution needs to change over time (e.g., to match rapidly changing policies).

Digital certificate programs also involve some unique cost drivers. For instance, governance and outreach costs would need to factor in the required time to develop and socialize new policies with the public and prospective verifiers. Costs for establishing trust frameworks would need to consider the level of effort required to establish agreements between countries and ensure certifications are accepted across borders. Adaptive management costs for monitoring and evaluating use and uptake worldwide, and adapting to emerging best practices.

* See *Understanding Total Cost of Ownership for Digital Health* for more details on common cost variances and hidden costs for digital health interventions.

Further information:

- Digital Documentation of COVID-19 Certificates: Technical Specifications and Implementation Guidance for Vaccination Status (VS) and Test Result (TR)
  - Refer to Section 8.3: Cost category considerations
- Digital implementation investment guide (DIIG): integrating digital interventions into health programmes
  - Refer to Chapter 7: Develop a Budget
- Understanding Total Cost of Ownership for Digital Health (Digital Square): executive summary and full report

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

Countries will need to budget one-time and recurring cost activities across all phases for digital certificate implementation. Each country will define the key activities and cost details based on strategies, what currently exists, and what is needed to fulfill the scope of the implementation.

The following are illustrative examples of the types of activities to consider in digital certificate program budgets.

Example ongoing costs associated to governance across all phases of implementation
Under **governance,** countries may need to develop new policies for the ongoing monitoring of use and impact of digital certificates. This may include costs to 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, and socialize new policies with key stakeholders and the public.

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

Development and setup (technology adaptation) costs may include activities to map and utilize data from existing software systems such as electronic health records (EHR), electronic immunization registries (EIR), health management information dystems (HMIS), logistic management information systems (LMIS), and laboratory information management systems (LIMS). This activity may include costs to 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 to pull core data for DDCC; and ensure compliance with relevant national guidelines.

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

Deployment costs may include communication activities to raise awareness on when, where, and how people can obtain digital certificates. This may involve costs to 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; and distribute communications materials to the public across key platforms.

Under **Integration and interoperability,** countries may need to coordinate and establish bilateral agreements with other countries in order to support the trust framework. This activiy may include costs to allocate dedicated resources within the government to attend coordination meetings; conduct ongoing consultations with key stakeholders across ministries on potential agreement; and seek formal approval of agreement with relevant government bodies.

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

Activities to **Scale** a digital certificate may involve printing certificates. For instance, for countries starting with paper certificates (i.e., Paper First approach), printing costs will increase as more people are vaccinated and subsequently receive a physical vaccination certificate. To cost printing, countries may need to 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 or in the back office; and provide continuous maintenance and replacement for devices and related materials, as needed.

For **Sustained operations** of the digital certificate program, countries may need to implement digital certificate system monitoring to continually make informed decisions about the program as new data is gathered (i.e., adaptive management). This would include costs to: monitor and evaluate 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 discuss digital certificate implementation and progress; and 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.

Further information:

- Digital Documentation of COVID-19 Certificates: Technical Specifications and Implementation Guidance for Vaccination Status (VS) and Test Result (TR)
  - Refer to Section 8.3: Cost category considerations
- Digital implementation investment guide (DIIG): integrating digital interventions into health programmes
  - Refer to Chapter 7: Develop a Budget
- Understanding Total Cost of Ownership for Digital Health (Digital Square): executive summary and full report

35. What are next steps for countries considering digital certificate implementation?

Once a country completes all the steps to plan for a digital certificate solution, implementation activities can commence to develop, deploy, integrate, scale, and sustain the digital certificate solution.

Immediate next steps for the non-technical audience include identifying applicable policies currently in place, making certificate decisions to inform policy and considering bilateral recognition of certificates to inform negotiations and discussion with other countries and regional networks. Certificate decisions include approach to solution development (e.g., short-term or long-term), issuing modality (e.g., paper, smartphone, both), QR Specification, method for identifying individuals (e.g., passport, national ID, health ID).

Immediate next steps for the technical audience include ensuring appropriate policy and legal frameworks are in place, evaluating readiness for deployment using implementation guidance, creating an implementation plan and budget using Operational Guidance and DIIG, and coordinating across partners to identify partners with appropriate technical skills, ensure compliance for technology vendors, and align digital certification with PHA business rules for vaccination (e.g., which vaccines, spacing) and SARS-CoV-2 diagnostic test results.

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

Other Key Concepts

36. What is a Trust Network and Public Key Infrastructure (PKI)?

Countries must establish trust in the issuance and verification of digital certificates. For vaccination status, verifiers must trust that a verified and validated certificate signifies that a trusted vaccine was administered by a trusted provider to an individual with a trusted means of identification. For SARS-CoV-2 diagnostic test results, verifiers must trust that certificates signify a trusted test was administered by a trusted health professional to an individual with a trusted means of identification. This trust framework is the basis of a trust network, which can be enabled by technology.

What is a Trust Network?
A trust network operationalizes a trust framework. The trust network maintains trust in the certificate issuing and verification authorities and systems, both domestically and across borders. It provides transparency in who are the trusted issuing authorities, creating confidence that a vaccination status or SARS-CoV-2 diagnostic test result certificate was issued by a trusted authority. The trust network also reduces the potential for fraudulent issuance and enables the revocation of certificates if there is evidence of fraud, and provides a secure method for both offline and online verification, ensuring that data in the certificate was not corrupted or modified from its original form

A trust network is set up through a national trust framework consisting of public key infrastructure (PKI) and transparent governance processes to enable digital signing of certificates. Countries must establish agreements with other countries that outline the governance process for establishing trust; set up a Public Key Infrastructure (PKI) to digitally sign and securely transmit messages that are linked to identity; and determine how to set up a certificate authority that registers and issues certificates.

What is a PKI?
A domestic public key infrastructure (PKI) is required for signing and verifying digital certificates. PKI is a cryptography method that enables the digital signing and verification of documents by a trusted network. A PKI uses public-private key pairs for digital signing and verification such that a document signed by a private key can be verified by the corresponding public key.

Key elements of a PKI:

- A designated government entity (e.g., a public health authority, ministry of ICT) acts as a Country Signing Certificate Authority (CSCA).
- 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 digital certificates.
- A DDCC issuer must have a DSC to sign a digital certificate.

There are many methods to implement a PKI. Countries determine the approach that best meets their needs and aligns with agreements established with other countries. Specifically, countries need to establish agreements with other nations 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.

Further information:

- Digital Documentation of COVID-19 Certificates: Test Result: Technical specifications and implementation guidance
  - Refer to Section 6: PKI for Signing and Verifying a DDCC: TR and Annex 3: What is public key infrastructure (PKI)?
- Digital Documentation of COVID-19 Certificates: Vaccination Status: Technical Specifications and Implementation Guidance
  - Refer to Section 6: National Trust Architecture for the DDCC:VS and Annex 4: What is public key infrastructure (PKI)?

37. What is Identity Binding and Unique Identification?

Member States must determine the policies and procedures for linking a digital certificate to an individual's identity. The DDCC standard 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 for unique identification should align with agreements established with other countries.

Further information:

- Digital Documentation of COVID-19 Certificates: Technical Specifications and Implementation Guidance for Vaccination Status (VS) and Test Result (TR).
  - Refer to Section 1.4: Assumptions

38. What governance mechanisms need to be established to support the trust network?

Countries establish a PKI and determine the most appropriate governance mechanisms for its context to support the trust network. Countries determine whether to leverage an existing PKI or establish a new one and establish governance mechanisms for digital signing infrastructure at PHA and Member State levels with clear policies for issuing certificates, verifying certificates, revocation of certificates, and data management and privacy protection.

The Proof of Vaccination scenario of use requires governance to be established at two levels: 1. the PHA; and 2. the Member State. At PHA level, at least one DSC needs to be utilized to sign the digital certificate. At Member State level, an authorized DSC-sharing mechanism needs to be established to indicate which DSCs are currently permitted to sign the digital certificate. There are two recommended approaches.

- **ROOT CERTIFICATE AUTHORITY**: The country establishes a root certificate authority, which holds a root certificate for the digital certificate. The private key of the Root Certificate managed by the Member State may be used by the Member State to sign a PHA's DSC that has been authorized for use. The public key of the root certificate can be used to validate that the DSC is authorized. Note that the term "root" does not imply hierarchy or that the root certificate authority is at the top of that hierarchy. Rather, it is used to denote that a root certificate authority may be trusted directly.
- **MASTER LIST**: The Member State establishes a mechanism to manage and distribute, as appropriate, a master list of DSCs that have been authorized for PHAs to use to sign the digital certificate.

Further information:
- Digital Documentation of COVID-19 Certificates: Technical Specifications and Implementation Guidance for Vaccination Status (VS) and Test Result (TR).
  - Refer to Section 6: PKI for Signing and Verifying a DDCC: TR and Section 7: National Governance Considerations

39. What needs to be considered in bilateral and regional policy negotiations for digital certificates?

A national trust framework consisting of public key infrastructure (PKI) and transparent governance processes enables digital signing of certificates, underpinning trusted sharing. Bilateral and regional policy negotiations in support of digital certificates may be complicated and require significant effort from country policymakers.

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. Key considerations for these negotiations include:

- 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?

Further information:
- Digital Documentation of COVID-19 Certificates: Technical Specifications and Implementation Guidance for Vaccination Status (VS) and Test Result (TR).
  - Refer to Section 7: National Governance Considerations

40. What is standardized health content?

DDCC guidance provides standardized, trusted health content aligned with international standards. This content **incorporates the WHO evidence base** and is provided in different formats that can be adapted by countries at any stage of digital maturity.

Standardized health content converts traditional health content (e.g., traditional narrative guidelines in PDF format) into structured components for operationalizing DDCC guidance within country programs and software code that is aligned with international FHIR standards. Adapting this standardized health content into digital certificate programs can help **accelerate adoption of public health interventions though digital technologies.** Structured components and software code aligned with international FHIR standards ensures countries **consistently and accurately interpret** this content as they develop digital certificate solutions, and it helps **strengthen data analytics and reporting.**

Further information:

- DDCC HL7 FHIR Implementation Guide

41. How does DDCC enable interoperability between certificates issued in other formats (e.g., DIVOC, EU DCC)?

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.** The core data set allows the generation of a certificate that is compatible with the EU DCC certificates or other major international standards (e.g., DIVOC, Smart Health Cards/VCI). By mapping certificates to DDCC standards, issuers can easily convert between formats without losing information ("loss-less conversion").

Further information:

- DDCC HL7 FHIR Implementation Guide
- External Links
  - DIVOC (Digital Infrastructure for Vaccination Open Credentialing) in India
  - EU Digital COVID Certificate Gateway
  - Open SRP FHIR Core Smart Vaccination Certificates for Android
  - OpenHIE DDCC Transactions Mediator

42. What are the required and optional components of DDCC?

Digital Health Solutions record vaccination or test result data and send them to into **Certificate Generation Service** which generates cryptographically signed certificates whose signatures are enrolled in a **Registry** and content is optionally stored in a **Repository**. Validity of a certificate can be checked in the optional **Verifier Application** according to Member State defined business rules.

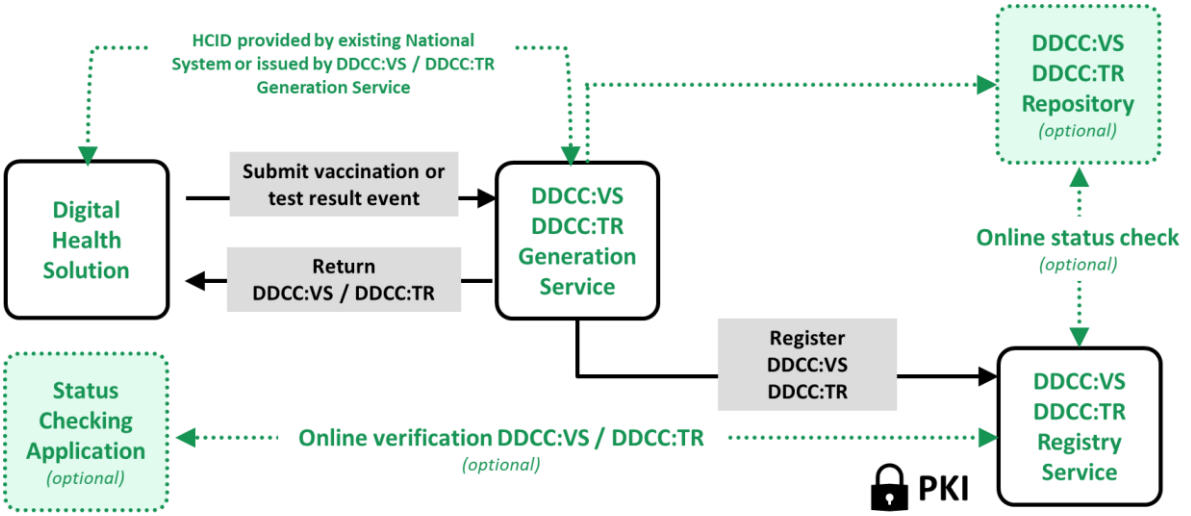
Required components:

- **Digital Health Solution:** Secure system that is used to capture and/or manage a digital record of vaccination status or test result core data.
- **Certificate Generation Service:** Generates cryptographically signed certificates of vaccination status or test results. This service is responsible for taking data about a vaccination event, converting that data to use the FHIR standard, signing that HL7 FHIR document, and returning it to the Digital Health Solution. The Digital Health Solution is in turn responsible for distributing the certificates and any associated representation of the data, such as a QR code, to the certificate holder based on PHA policy.
- **Registry Service:** Service that can be used to request and receive metadata associated with the certificate, such as its signature. The Registry Service can be utilized to determine whether a certificate has been revoked, for example, due to revocation of a key within the PKI, a compromised batch of vaccinations, or issues within the supply chain. The Registry Service is not the same as an electronic immunization registry.

Optional components:

- **Verifier Application**: A digital solution that can inspect and cryptographically verify the validity of certificates. This can be an application on a mobile phone or another device.
- **Repository Service:** The optional service that has a repository, or database, of all the certificates and which is able to return a copy of the certificate (the signed FHIR document) and potentially the one dimensional or two-dimensional barcode representation (such as a QR code) of the signed FHIR document. This can be architected in a centralized or decentralized manner. Regardless, it is a mechanism that stores and persists the certificate information. The Repository Service is optional depending on which use case is being implemented, but it is required for the online verification use cases.

Figure D: Workflow for Generating Digital Certificates



Further information:

- Digital Documentation of COVID-19 Certificates: Technical Specifications and Implementation Guidance
  - Vaccination Status (VS) – Refer to Section 4: Proof of Vaccination scenario
  - Test Result (TR) – Refer to Executive Summary: What are the minimum requirements to implement a DDCC:TR?

The DICE consortium

The views described herein are the views of DICE, and do not represent the views or opinions of the individual consortium partners, nor is there any approval or authorization of this material, express or implied, by the individual consortium partners.

Digital Health Centre of Excellence
unicef
World Health Organization