



Digital Documentations of COVID-19 Certificates (DDCC) legal framework assessment and decision-making framework

Final deliverable –11.02.2022



Table of content

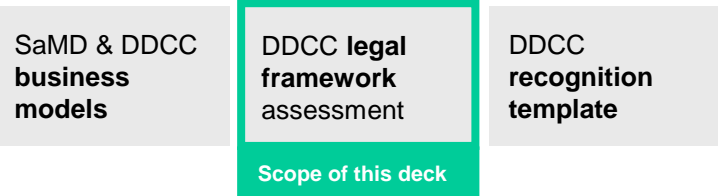
Item	Description
1. Project overview	Project objectives, scope, approach and accomplishments
2. Executive summary	Summary of findings gathered through interviews and desktop research
3. Framework assessment	Framework assessment and framework case studies
4. Decision-making framework	Decision-making framework with recommendations on legislative actions including a roadmap for policy makers to implement a DDCC in an ethically sound manner
5. Next steps	Next steps
Appendix I	Most relevant DDCC use cases
Appendix II	Detailed policy categories

1. Project overview

This deck covers insights on relevant frameworks for implementing a digital documentation of COVID certificates and a decision-making framework

Project structure and objectives

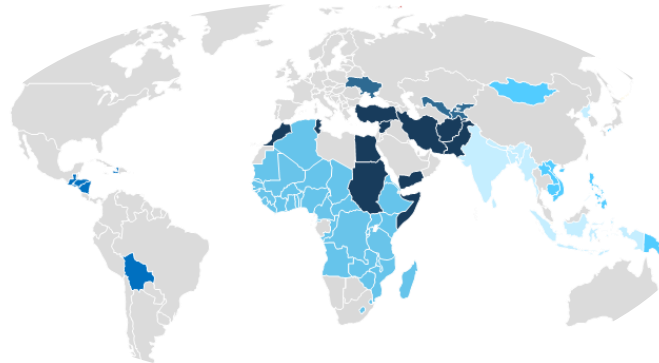
This project is separated into 3 workstreams:



- I. eHealth solutions, SaMD (i.e. software as a medical device) and DDCC business model use case development
- II. DDCC Framework leading practices identification and policy requirements for the implementation of digital COVID-19 certificates in LMICs
- III. DDCC mutual recognition template development to provide guidance to LMICs on the deployment and implementation of DDCC and SaMD through sustainable financing models involving public-private partnerships

Project scope

- The scope should cover:
 - Sustainable business models with a focus on their applicability to DDCC and SaMD
 - Policy requirements for implementing digital COVID-19 certificates
- The geographical scope is low- and middle-income countries (LMICs)



Expected output

- The output of this project will be used by the DH&I team to provide guidance on how to ensure the sustainability and coordination of investments into these approaches with the focus on:
 - Financing mechanism, deployment and maintenance models and potential synergies between DDCC and SaMD and key considerations to guide future efforts
 - Decision-making framework to support with the implementation of digital certificates for COVID-19
 - MOU templates for mutual recognition of COVID-19 certificates

The project will be carried out with the ultimate focus on gathering insights that WHO can use to support local ecosystems with relevant frameworks and guidance on sustainable business models for the deployment, maintenance and mutual recognition of digital health solutions in low- and middle-income countries (LMICs)

Acronyms

DDCC: Digital Documentation for COVID19 Certificates
 LMICs: Low- and Middle-Income Countries
 SaMD: Software as a Medical Device
 MOUs: Memorandum Of Understanding

What we are doing and why

What?

Identify existing relevant frameworks for DDCC for low- to middle-income countries (LMICs) and develop a decision-making framework

Why?

Establishing guidance for countries to be able to develop policies required to support the implementation of digital COVID-19 certificates in the absence of clearer and more specified policies under the IHR

Acronyms

IHR: International Health Regulations

We consolidated our findings through the framework assessment and conducted interviews and used those findings to develop a decision making framework for LMICs

Objectives

Workstream 2: Policy changes and updates to account for public-private partnerships and multi-lateral engagement needed for implementing digital COVID-19 certificates

Milestones	Conduct an assessment of relevant frameworks as case studies for countries to understand governance and policies required for implementing a digital solution for mutually recognizable COVID-19 certificates. → 1	Develop a recommended decision-making framework draft that could guide member states on paths forward for establishing governance mechanisms, including establishing national and multi-national trust frameworks. → 2
	<ul style="list-style-type: none"> • Conduct desktop research and interviews to gather existing challenges for implementing DDCC frameworks • Assess existing DDCC frameworks with a focus on applicability to LMICs 	<ul style="list-style-type: none"> • Identify the gaps in the existing legal frameworks in LMICs • Extract applicable frameworks for LMICs • Develop a decision-making framework draft
	<ul style="list-style-type: none"> ✓ Screened and analyzed 50 policies, trust frameworks, DDCC initiatives and digital solutions, through desktop research ✓ Prepared and conducted 11 interviews with external stakeholders (i.e. MOH Uganda, Patrick J. McGovern Foundation, WHO Sri Lanka, EU Commission) and five interviews with PwC experts 	<ul style="list-style-type: none"> ✓ Identified framework gaps and challenges for LMIC ✓ Developed a decision-making framework







2. Executive summary

Key insights and challenges of the framework assessment show gaps in data privacy and exchange policies as well as a highly fragmented DDCC trust framework ecosystem

	DDCC legal and trust framework assessments	<ul style="list-style-type: none"> • No international guidelines in place for DDCC legal frameworks • EU Regulation (EU) 2021/953 is the largest used (60 countries), most exhaustive DDCC legal Framework and applicable for LMIC • The existing frameworks and COVID solutions deployed are inconsistent at the global, regional and national level leading to siloed policy framework initiatives and solutions • There is a gap of DDCC policies (defining usage, validity, issuance and verification) in LMIC
	Data privacy and exchange frameworks	<ul style="list-style-type: none"> • No international guidelines in place for data privacy (except the Universal Declaration of Humans Rights stating the right to privacy) • There are domestic data privacy protection laws that have a general international applicability and should be considered for global data exchange such as the EU GDPR, South Africa's Protection of Personal Information POPI, Brazil's Lei Geral de Protecao de dados LGPD and California Consumer Privacy Act CCPA • EU GDPR is the largest used and most exhaustive legal framework on data privacy, including data exchange regulations enabling national and multinational collaboration • LMICs are mostly using EU GDPR as a guideline for data exchange and privacy measures as domestic data privacy laws are either missing or not comprehensive
	Technical frameworks and digital solutions	<ul style="list-style-type: none"> • DHIS2 is the largest used (73 LMICs) open source software platform that can be connected to DDCC and customized to comply with WHO technical guidelines and the EU DCC framework. DIVOC is built upon this platform and largely used as DDCC technology in LMIC. • There are many "wallet apps" like SMART Health Cards and IATA to enable international travel, providing an international trust framework with public-private partnerships • Most of the DDCC technologies are compliant with general technical frameworks such as HL7 FHIR and W3C. • There are two main technologies used for digital COVID certificates, either decentralized Verifiable Credentials (VC) (mostly wallet apps) or centralized Public Key Infrastructure (PKI) (mostly regional solutions as EU DCC and DIVOC) • Based on the main technologies different governance mechanisms has to be implemented
	Key considerations	<ul style="list-style-type: none"> • Lack and inconsistency of DDCC policies across the globe show that an international approach should be perused • Data privacy and exchange policies are fragmented and represent an impediment to national and multinational collaboration, therefore it is imperative to implement these policies in agreements for mutual recognition of DDCC • The development of a decision-making framework should take into account that the legislative situation, governance mechanisms, and the digital health maturity are very heterogeneous among LMICs







Source: PwC analysis of key insights through desk research and interviews

LMICs face major challenges in the developments of DDCC policy frameworks mostly due to a lack of guidance and resources

 <p>Holistic and national strategic planning:</p> <ul style="list-style-type: none"> Plan outlining and providing necessary resources, coordination, cooperation and leadership 	 <p>Data standardization, interoperability and exchange:</p> <ul style="list-style-type: none"> Laws and regulations to access and restrict the use of their medical data Interoperability challenge 	 <p>ICT infrastructure:</p> <ul style="list-style-type: none"> Lack of wide spread internet connection or poor internet connection Infrastructure varies, which makes it difficult to adapt a DDCC technology 	 <p>HCP digital skills:</p> <ul style="list-style-type: none"> Basic digital skills shortages across both professionals and patients 	 <p>Financial resources:</p> <ul style="list-style-type: none"> Few monetary resources to finance both the ICT infrastructure with large up-front costs And upskilling/retention of healthcare workforce 	 <p>Local population adoption and readiness:</p> <ul style="list-style-type: none"> Significant cultural challenges about vaccines and health digital solutions due to a lack of information and misconception
<p>“</p> <p>CEO of digital health solution deployed in LMIC</p> <p>There are only a few of public private partnerships established in LMICs which is crucial for implementing DDCC</p>	<p>“</p> <p>CEO of digital health solution deployed in LMICs</p> <p>Implementation of policies taking a lot of time and are not suitable for a fast response to a pandemic like COVID-19 what should countries do with no digital health or data security policies? Guidance on that is missing.</p>	<p>“</p> <p>LMIC government stakeholder</p> <p>WHO trying to provide THE solution and not considering the different challenges at national levels (different digital health maturity).</p>	<p>“</p> <p>LMIC government stakeholder</p> <p>In many LMICs the responsibility for eHealth initiatives lies within the ministry of health. Countries with a lower digital maturity have a lack of IT knowledge and skills in the MOH in common. Most LMICs have HCP working in the MOH without an IT background and there is a lack of courses and degrees in bioinformatics and medical informatics in universities in LMICs. This leads to few initiatives in advancing digital health in a country.</p>	<p>“</p> <p>LMIC government stakeholder</p> <p>There is lack of national and or multinational coordination on investments regarding implementation of DDCC or eHealth initiatives in general.</p>	<p>“</p> <p>PwC digital health expert in sub-Saharan Africa</p> <p>A lot of communication about the vaccines has been happening through social networking. Religious networking groups, WhatsApp community groups, misinformation has been rough. MOH has reached out to the religious groups and used the channel to spread correct information. Like I said not much social media but more around chatting of groups and communities – social networking.</p>
<p>PwC digital health expert in sub-Saharan Africa</p> <p>Because of the low vaccination rate the interest of the government in implementing a DDCC is very low</p>	<p>PwC digital health expert involved in DDCC LU</p> <p>It was the responsibility of each national certification body to deploy the right architecture to ensure interoperability. LMICs might need guidance on this.</p>	<p>PwC digital health expert involved in CoWIN India</p> <p>We were involved to see if CoWIN can be replicated in other countries. We struggle on technical challenges. Entire app was based on the infrastructure and organizational hierarchy in India. Not every adoption on local ICT and org. infrastructure is possible through frontend adjustments it requires sometimes changes on code level.</p>		<p>PwC digital health expert in sub-Saharan Africa</p> <p>Donors were shying away from investing in digital health solutions because it was not sustainable. It started to be interesting when there was the need for COVID passports.</p>	
<p>LMIC government stakeholder</p> <p>There should be a closer engagement between WHO and ITU to have a closer engagement between MOH and ministries of IT.</p>					

Source: PwC analysis of interviews
Glossary: Healthcare Professional (HCP)

Key success factors of best practice examples from the framework assessment

 <p>Holistic and national strategic planning:</p> <ul style="list-style-type: none"> Plan outlining and providing necessary resources, coordination, cooperation and leadership 	 <p>Data standardization, interoperability and exchange:</p> <ul style="list-style-type: none"> Laws and regulations to access and restrict the use of their medical data Interoperability challenge 	 <p>ICT infrastructure:</p> <ul style="list-style-type: none"> Most people living in LMICs do not have internet connection or poor internet connection Infrastructure varies, which makes it difficult to adapt a DDCC technology 	 <p>HCP digital skills:</p> <ul style="list-style-type: none"> Basic digital skills shortages across both professionals and patients 	 <p>Financial resources:</p> <ul style="list-style-type: none"> Few monetary resources to finance both the ICT infrastructure with large up-front costs And upskilling/retention of healthcare workforce 	 <p>Local population adoption and readiness:</p> <ul style="list-style-type: none"> There are significant cultural challenges about vaccines and health digital solutions due to a lack of information and misconception
<ul style="list-style-type: none"> Governments need to implement a digital healthcare strategy Have cross-functional and cross-border expert groups on digital health in place Support capacity building within the digital health area Use best practice regulations/technologies as guidance Apply for best practice trust registries and provide guidance for third countries how to enter the local one 	<ul style="list-style-type: none"> Set interoperability as a primary design principle Use technology that is adaptable and designed for low-resource environments Enact a data governance framework that balances data privacy and protection with innovation Adhere to international standards from the start 	<ul style="list-style-type: none"> Leverage already existent platforms, ICT infrastructure and technologies Include the connectivity and broadband infrastructure expansion in the digital health strategy Invest in wide access to digital devices and connectivity Establish public-private partnerships with local infrastructure providers 	<ul style="list-style-type: none"> Invest in digital literacy and capable workforce Include digital literacy in the healthcare workforce trainings Promote advantages of digital healthcare within the health workforce Leverage digital tools for trainings at scale Create an HR strategy within the ministry to sustain newly build capacities 	<ul style="list-style-type: none"> Sustainable financing, see outputs of WSI Establish public-private partnerships with local solution providers Develop local capacities to take over leadership in digital health and digital health policies DDCC should be free of charge 	<ul style="list-style-type: none"> Built trust in society by using transparent policies and open data standards Include digital skills in the education plan Use different channels like social media and social networking to inform the population social science perspectives should provide additional insight during policy development

Source: PwC analysis of CISCO Digital Readiness Index 2019; WHO recommendations on digital interventions for health system strengthening 2019; WHO/International Telecommunication Union National eHealth strategy tool kit, desktop research and interviews

Policy recommendations for building a strong regulatory environment for each stage of the DDCC maturity levels – (1/2)

DDCC maturity	Policy types along the maturity roadmap	Policy description and requirements	Policy ¹ / standard ² / initiative ³ / example ⁴
National DDCC	 <p>1. DDCC Policy / Trust framework</p>	<ul style="list-style-type: none"> To use a digital covid certificate in an ethically sound manner authorities should provide clear policies and regulations to determine the usage, validity (vaccines, tests and recovery), issuance, verification, and acceptance, ensuring authenticity and integrity of issued certificates including a trust framework addressing technical specifications structure and processes Either by creating a new policy, adjusting existing eHealth policies or by participating to existing international trust frameworks 	 <ul style="list-style-type: none"> EU Regulation 2021/953¹
	 <p>2. Data protection, privacy and security</p>	<ul style="list-style-type: none"> Authorities and technology providers should ensure that the data privacy and security of the users is well-protected By adhering to local or regional data privacy policies and/or; By ensuring privacy through technology (technology and privacy are intervened) therefore, strive for privacy preserving technologies using appropriate safeguarding techniques such as encryption, decentralization or de-identification, firewalls and zero-knowledge proof verification processes Adheres to the following principles: data minimization, access limitation, use limitation, purpose limitation, collection limitation, openness and transparency, individual participation and control, accountability Should cover the following topics: data ownership, data inventory, data subject rights (informed, access, rectification, erasure, restrict processing etc.), data subject consent, data processing records, personal data breaches, compliance monitoring, data protection impact assessment 	 <ul style="list-style-type: none"> GDPR¹ Convention 108^{3,1} Health Insurance Portability and Accountability Act (HIPAA)¹ AOKPass as example for privacy by design, the verifier does not process personal data⁴
	 <p>3. Data exchange and interoperability</p>	<ul style="list-style-type: none"> Digital vaccination certificates should use open standards and adhere to international technical standards like the WHO DDCC guidelines or the ICAO VDS-NC guidelines. There are three dimensions of interoperability: <ul style="list-style-type: none"> Technical interoperability (adhering to open and international technical standards) Trust interoperability (shared trust and governance mechanism) Legislative interoperability (policies covering topics like electronic exchange of health data within the country and on a cross-border context) 	<ul style="list-style-type: none"> ICAO guidelines² Decision No 1082/2013/EU on serious cross-border threats to health¹ Directive 2011/24/EU (cross-border healthcare)¹ HL7 FHIR², WHO guideline²

Policy recommendations for building a strong regulatory environment for each stage of the DDCC maturity levels – (2/2)

DDCC maturity	Policy types along the maturity roadmap	Policy description and requirements	Policy ¹ / standard ² / initiative ³ / example ⁴
Internationally recognized DDCC	 4. Mutual recognition	<ul style="list-style-type: none"> It is imperative to make individual, transparent agreements based on law, to ensure mutual recognition of the DDCC and enable international travel Agreements should include at least: purpose of equivalence decision (use case), shared trust framework and connection, acceptance definition, acceptance decision of each others certificates, data protection, connection to PKI if applicable, alignment on data sets and standards, enter into force, accepted vaccinations, tests, recovery and validity 	<ul style="list-style-type: none"> EU's equivalence decisions⁴ Agreement between Singapore and Taiwan following EU equivalence decisions⁴ Trusted travel – my COVID pass Africa initiative³
International best practice DDCC	 5. IT security	<ul style="list-style-type: none"> There should be national laws encouraging solution providers to introduce IT security policies and measures in order to safeguard the systems from potential malicious threats Policies should include topics like acceptable use, awareness training, incident response, disaster recovery plan, access, vendor management, password management, network security, access authorization, modification and identity access management, data retention, mobile device management and procedures, encryption and decryption, system maintenance (monitoring and auditing), and vulnerability management 	<ul style="list-style-type: none"> ISO/IEC 27001 and 27002² Cyber Essentials, UK information assurance scheme¹
	 6. Digital identity	<ul style="list-style-type: none"> Authorities should determine the mechanism for unique identification Consider binding the vaccination certificate to eIDs Policies should include regulations on electronic identification, electronic transactions, electronic identification schemes, electronic trust services, cooperation and interoperability, data protection 	<ul style="list-style-type: none"> eIDAS¹ Estonian eID policy¹ Adhaar used for CoWIN in India⁴
Post COVID-19 health super-app	 7. Streamlined digital eHealth policy	<ul style="list-style-type: none"> Using private-public partnerships and introducing transparent agreements based on a solid legal basis as described above to enable vertical use cases The agreements should be privacy preserving, publicly available and adhere to other domestic and international laws on data privacy, protection, security and exchange There should be a strong focus on user consent and trust by using a streamlined eHealth policy as the app would be handling highly sensitive data Under no circumstance should health data be sold or transferred to third parties who are not working in the public interest 	<ul style="list-style-type: none"> China's Wechat app offering Covid-19 services such as testing and vaccination appointment bookings⁴  EU Agenda on Better Regulation in 2015 addressing self-regulation, the legal basis of most super-apps³

3. Frameworks assessment

We identified 50 relevant frameworks and we developed 7 framework case studies for this deliverable

22 non-policy/legal frameworks have been screened and analyzed

15 policy/ legal frameworks government agencies driven to provide legal boundaries

Here are some relevant frameworks used and deployed in LMICs:

Here are some relevant frameworks used and deployed in LMICs:



The Good Health Pass Collaborative (GHPC) / interoperability blueprint / Global



The SMART Health Cards framework / DDCC trust framework / Global



International Civil Aviation Organization (ICAO) guidelines including a trust framework / Global



TrustNet Covid-19 Initiative / DDCC trust framework / Pakistan



Covid credentials initiative / technical framework / Global



The General Data Protection Regulation (GDPR) / data privacy and exchange legal framework / general applicability as soon as processing data of EU citizen



The EU regulation 2021/953 / DDCC policy / EU



OECD privacy principles / Guidelines on protection of privacy and transborder flow of personal data / Global



APEC framework / protect privacy and enable regional transfers of personal information / Asia-Pacific economies



African Union Convention on cyber security and personal data protection / establishment of a legal framework on data privacy and exchange / African Union

The assessment showed, that the following types of frameworks are relevant for countries to understand governance and policies required for implementing a digital solution for mutually recognizable COVID-19 certificates



1 DDCC policy framework has reached international scale

- Legally binding frameworks on authenticity, validity and integrity of the certificates
- Only **one** DDCC legal framework was found to have reached international scale: EU DCC regulation 2021/953
- LMICs can use this policy as guidance where local laws are missing and use the EU system to reach mutual recognition



21 International DDCC trust frameworks are used to develop DDCC

- Framework initiatives to establish international DDCC standards of trust ensuring the authenticity, validity and integrity of DDCC
- 14 among those frameworks belong to DDCC technologies (i.e. AOKpass, Smart Health Cards) providing their one DDCC trust framework
- When there are no resources to implement local DDCC policy, LMICs should make sure to comply at least with international DDCC trust frameworks and be compatible to their respective DDCC technologies to enable mutual recognition



15 Data privacy, protection and exchange policy frameworks have a multinational applicability of which four have general applicability

- Data privacy and exchange policies protect the right to privacy of the user while enabling secure data exchange
- DDCC should adhere to regional applicable data privacy policies and make sure to comply with the general applicable data privacy policies (i.e. EU GDPR, South Africa's Protection of personal information POPI, Brazil's Lei Geral de Protecao de dados LGPD and California Consumer Privacy Act CCPA)



12 Technical / operational / blueprint frameworks considered for DDCC applications

- Technical frameworks such as the [WHO DDCC technical guidance](#) set the technical standards on which a digital COVID certificate is based
- Locally developed DDCC technologies should comply to the international acknowledged W3C, HL7 standards and the WHO DDCC technical guidance



2 Data / system interoperability frameworks focuses on digital health and DDCC



































- Ensures interoperability of digital health solutions to enable free movement and mutual recognition
- Standards like the [Interoperability of health certificates Trust framework](#) and [initiatives like Integrating the Healthcare Enterprise](#) promote interoperability standards in healthcare and should be considered when implementing DDCC

We have assessed 50 frameworks and selected the 7 most relevant and applicable DDCC frameworks and technologies for LMICs based on some key criteria

We considered the following factors to rate the applicability of frameworks for LMICs

- Framework used by many low- and middle- income countries and regions
- Frameworks approved and/or recognized by governments
- Adherence of technical and trust frameworks (e.g.; SMART Healthcards, AOKPass) to international technical standards (WHO, W3C, HL7) and best practices
- Use of open source platforms for implementing COVID solutions
- Low local ICT infrastructure requirements for the implementation of the framework and or digital solution
- Easy applicable and or useable by stakeholders (government, labs, health care providers, patients, payers, and policy makers)



Most relevant framework for LMICs	National / international DDCC policy framework	DDCC trust framework	Data privacy, protection and exchange policy framework	Technical / operational / blueprint framework	Data / system interoperability framework
Good Health Pass Collaborative (GHPC) 					
DIVOC 					
DHIS2 					
EU Gateway and Regulation 2021/953 					
International Civil Aviation Organization VDS-NC Guidelines 					
AOKPass 					
SMART Healthcards framework 					



Source: PwC analysis of relevant frameworks.

Glossary: World Wide Web Consortium (W3C), Digital Infrastructure for Vaccination Open Credentialing (DIVOC), District Health Information Software (DHIS2), Visible Digital Seals (VDS), Non-constrained (NC), , Health Level Seven (HL7), Fast Healthcare Interoperability Resources (FHIR)

[Link to the exhaustive list of frameworks screened and analysed](#)




We analyzed the following 5 countries/regions and the DDCC policies that have been implemented to introduce a digital COVID-19 certificate and extracted their success factors (1/2)

- EU as the most used DDCC standard
- Togo as one of the first African countries to introduce a DDCC
- Morocco because it has been deploying digital health extensively
- India as it has been named as good DDCC example in many interviews
- El Salvador being an LMIC that is digitally advanced in many industries incl. the banking industry

Country/Region	Policies that have been implemented specifically for a DDCC	Success factors for the fast development and deployment of a DDCC
European Union 	<ul style="list-style-type: none"> • Regulation (EU) 2021/953 common framework for issuance, verification and acceptance of vaccination, test and recovery certificates • Regulation (EU) 2021/954 with regard to third-country nationals • Commission implementing decisions (i.e. laying down technical specifications) • Commission delegated regulations (i.e. acceptance period of vaccination certificates) • Released a number of guidelines and processes to enable “equivalence decisions” of other DDCC 	<ul style="list-style-type: none"> • The use of extraordinary power measures to enable quick policy changes in the context of pandemic • The use of the existing eHealth network to enable a quick development of policies and technologies • Leveraged human resources from the eHealth network already in place and semantic subgroups for i.e. data sets, technical sub groups (were reinforced because of contact tracing apps) • Accelerated international acknowledgement and acceptance by releasing well documented, well structured and free of charge “equivalence decision” process • Avoids centralisation where possible in line with the principle of flexibility
India 	<ul style="list-style-type: none"> • Leveraged the Information Technology Act, 2000 with the Information Technology Rules 2011 and two draft legislation: Personal Data Protection Bill, 2019 (pending in Parliament) and Digital Information Security in Health Care Act • Used UK and EU data privacy policies as guidelines • Works with CoWIN policies: <ul style="list-style-type: none"> – Asks for consent of patients when registering – Terms of Service addressing trust framework, data privacy, security and exchange, the ID verification, IT security, ownership of content, – Guidelines for Integration of CoWIN with Third-Party Applications Developed by Ecosystem Partners 	<ul style="list-style-type: none"> • Enabled quick measures under the Disaster Management Act 2005 • Leveraged the eVIN and DHIS2 platforms and their networks (i.e. HISP) that have been in place and built CoWIN on top • Used digital systems to train the health workforce • Increased user adoption by offering additional functionalities like appointment registry, alert systems and a platform for grievances • Cloud based platform doesn’t need local servers • Works on providing CoWIN for other LIMCs in the APEC region – increasing the range

Source: PwC analysis of key insights through desk research and interviews, [India's Policy Response to COVID-19](#), [Co-WIN platform](#)

We analyzed the following 5 countries/regions and the DDCC policies that have been implemented to introduce a digital COVID-19 certificate and extracted their success factors (2/2)

Country/Region	Policies that have been implemented specifically for a DDCC	Success factors for the fast development and deployment of a DDCC
Morocco 	<ul style="list-style-type: none"> DDCC based on law No. 09-08 on the Protection of Individuals with Regard to the Processing of Personal Data No policies specifically published for the DDCC except for the usage (entry requirements in businesses and for travel between regions) Entered the EU DCC trust registry 	<ul style="list-style-type: none"> "Moroccan Ministry of Health Strategy 2025" most far-reaching Moroccan healthcare-IT approach as groundwork National Digital Development Agency (ADD) has been created for accelerating digital health testifying government's determination, commitment, and support to the achievement of a digital transformation in the country Strong digital infrastructure and information structure Electrification extends across almost the entire country, including the most remote and rural areas
Togo 	<ul style="list-style-type: none"> DDCC PassCovid19TG complies with law No. 2019-014 relating to the protection of personal data Have implemented several measures and laws with extraordinary power and an emergency response project but not specifically on the DDCC except for the usage Personal data will only be managed locally on patient's smartphones Entered the EU DCC trust registry 	<ul style="list-style-type: none"> Government's roadmap aims at the digitalisation of all the country's economic sectors Togo has also fully digitised all elements of its vaccination plan Followed the example of Asian countries and the European Union Established public-private partnerships (i.e. PanaBIOS Consortium) to reach compatibility with the Trusted Travel and Trusted Vaccines standards in record time
El Salvador 	<ul style="list-style-type: none"> Bill on data protection is being developed, but there are other laws on computer crimes and related crimes, consumer protection law, and privacy aspects in the constitution Personal data included in the DDCC (Comprobante electrónico de vacunación) will be processed only to verify and confirm the holder's vaccination, test result or recovery status and will not be retained afterwards Released measures and regulations to tackle the pandemic but nothing specifically for the DDCC except for the usage Entered the EU DCC trust registry 	<ul style="list-style-type: none"> Country's Digital Agenda 2020-2030 allowing El Salvador to chart the way for a digital revolution President Nayib Bukele created an Innovation Department within his administration, and it became the unit in charge of promoting innovation and digital transformation in El Salvador The government is also working on connectivity and broadband infrastructure Started El Salvador COVID-19 Emergency Response Project Established a partnership with EU for national development plans including digital transformation

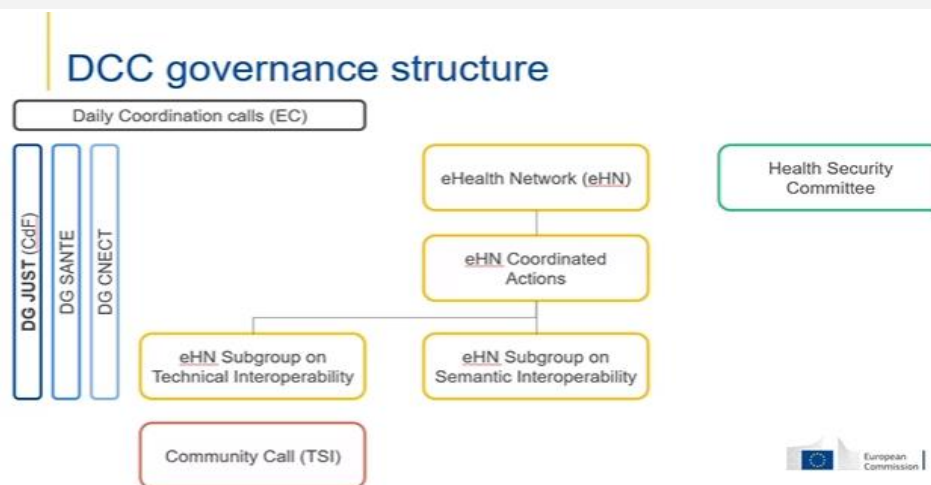
Source: PwC analysis of key insights through desk research and interviews , [Togo DDCC](#), [Data Guidance](#), [Moroccan Digital Health Response to the COVID-19 Crisis](#), [Centro virtual de documentacion regulatoria](#), [Ministry of health El Salvador](#), [Health Policy + Capacity for the COVID-19 Response](#)

The EU DCC is the best practice example regarding the legislative aspects

Initial situation

The existing eHealth network of the EU built the basis of the fast technological and legal response of the EU to implement the EU DCC

- Cross border healthcare patients' rights directive (Directive 2011/24/EU) established the [eHealth network](#)
- eHealth network already existent (10 y), governance framework in place and network of trusted experts (mutual trust and understanding) that was developed over time



Success factors

- The use of extraordinary power measures to enable quick policy changes in the context of a pandemic
- **The use of the existing eHealth networks to enable a quick development of policies** and technologies (networks involved see DCC governance structure)
- Leveraged human resources from the existing eHealth network (were reinforced because of contact tracing apps)

Policies implemented / adopted and used for the DDCC







The EU has implemented a digital COVID-19 certificate (DCC) policy, these were the three main steps:

- Decision to use the right to free movement as use case and legal basis
- Determining a goal for the usage of a DDCC (allow for coordinative way to lift restrictions)
- Developing a governance structure, enabling a fast legal response (see left side on the slide)

Below are all implemented policies/regulations and guidelines by the EU for their DCC

1. Introduced the DCC **regulation (EU) 2021/953** as common framework for issuance, verification and acceptance of vaccination, test and recovery certificates, considered relevant **GDPR data protection regulation**   
2. **Regulation (EU) 2021/954** with regard to third-country nationals 
3. **Commission implementing decision (EU) 2021/1073**
4. **Commission implementing decision (EU) 2021/2014**
5. **Commission implementing decision (EU) 2021/230** 
 - laying down technical specifications and rules for the implementation of the trust framework for the EU Digital COVID Certificate established by Regulation (EU) 2021/953 of the European Parliament and of the Council
6. **Commission delegated regulation (EU) 2021/2288** 
 - amending the Annex to Regulation (EU) 2021/953 of the European Parliament and of the Council as regards the acceptance period of vaccination certificates issued in the EU Digital COVID Certificate format indicating the completion of the primary vaccination series
7. **Released a number of guidelines and processes to enable “equivalence decisions” of other DDCC.** Set up parallel unilateral agreements for mutual recognitions of digital COVID certificates with third countries allowing the EU DCC becoming an international standard 

Summary key success factors

 <p>Holistic and national strategic planning:</p> <ul style="list-style-type: none"> Plan outlining and providing necessary resources, coordination, cooperation and leadership 	 <p>Data standardization, interoperability and exchange:</p> <ul style="list-style-type: none"> Laws and regulations to access and restrict the use of their medical data Interoperability challenge 	 <p>ICT infrastructure:</p> <ul style="list-style-type: none"> Most people living in LMICs do not have internet connection or poor internet connection Infrastructure varies, which makes it difficult to adapt a DDCC technology 	 <p>HCP digital skills:</p> <ul style="list-style-type: none"> Basic digital skills shortages across both professionals and patients 	 <p>Financial resources:</p> <ul style="list-style-type: none"> Few monetary resources to finance both the ICT infrastructure with large up-front costs And upskilling/retention of healthcare workforce 	 <p>Local population adoption and readiness:</p> <ul style="list-style-type: none"> There are significant cultural challenges about vaccines and health digital solutions due to a lack of information and misconception
<ul style="list-style-type: none"> Governments need to implement a digital healthcare strategy Have cross-functional and cross-border expert groups on digital health in place Support capacity building within the digital health area Use best practice regulations/technologies as guidance Apply for best practice trust registries and provide guidance for third countries how to enter the local one 	<ul style="list-style-type: none"> Set interoperability as a primary design principle Use technology that is adaptable and designed for low-resource environments Enact a data governance framework that balances data privacy and protection with innovation Adhere to international standards from the start 	<ul style="list-style-type: none"> Leverage already existent platforms, ICT infrastructure and technologies Include the connectivity and broadband infrastructure expansion in the digital health strategy Invest in wide access to digital devices and connectivity Establish public-private partnerships with local infrastructure providers 	<ul style="list-style-type: none"> Invest in digital literacy and capable workforce Include digital literacy in the healthcare workforce trainings Promote advantages of digital healthcare within the health workforce Leverage digital tools for trainings at scale Create an HR strategy within the ministry to sustain newly build capacities 	<ul style="list-style-type: none"> Sustainable financing, see outputs of WSI Establish public-private partnerships with local solution providers Develop local capacities to take over leadership in digital health and digital health policies DDCC should be free of charge 	<ul style="list-style-type: none"> Built trust in society by using transparent policies and open data standards Include digital skills in the education plan Use different channels like social media and social networking to inform the population social science perspectives should provide additional insight during policy development

Source: PwC analysis of CISCO Digital Readiness Index 2019; WHO recommendations on digital interventions for health system strengthening 2019; WHO/International Telecommunication Union National eHealth strategy tool kit, desktop research and interviews

A glance at other international standards of digital systems in general have shown the following key success factors for becoming an adoptable global standard

Relevant standards from the financial industry

Description and major milestones

Success factors for adopting the standards in LMIC

Society for Worldwide Interbank Financial Telecommunication (SWIFT)



International best practice DDCC analogue

- Provider of secure financial messaging services and money transfers
- Used to identify banks and financial institutions globally
- Used in payment system in over 70 countries
- 1973 – 239 banks from 15 countries formed SWIFT to solve a common problem
- 1980 – Connection of first central banks and forming the SWIFT community
- 1990 – Interbank File Transfer went live, strengthened focus on security
- 2000 – continued launching innovative products, increased security and further reduced prices through economies of scale
- 2020 – Established successful international joint ventures

- Provides assistance, training and technical support for its implementation
- Has a document center
- Launches adoption programs for structured implementations
- Have well documented joining procedures and guidance
- For smaller banks with no capacity to connect directly to SWIFT as a member, partnerships with financial service providers are offered to access the banking network at a fraction of the costs
- International governance and oversight
- Uses partnerships and joint ventures to enter new markets and support on a local basis
- Offers user engagement platforms like forums etc. to continually develop its services
- Ongoing cost reductions to enable access for LMIC

OECD Common Reporting Standard 

Foreign Account Tax Compliance Act (FATCA)/Global Account Tax Compliance Act (GATCA)

Internationally recognized DDCC analogue

- FATCA is an IRS international tax law to avoid tax fraud and GATCA is the global version based on it and is technically referred to as CRS
- CRS is a standard for automatic exchange of financial account information in tax matters developed by OECD, based on bilateral agreements
- Exchange of data of assets of income on a global level
- LMIC are among the CRS signatories
- 2014 – Declaration 47 tentatively agreed on the standard
- 2015 – 53 jurisdictions signed
- 2016 – 109 signatories

- A global need was existent based on a G20 request
- OECD aimed at presenting one single global standard from the start
- Asked the Global Forum for a mechanism to monitor and review the implementation
- Included the needs of developing countries in the development
- OECD has published an [implementation handbook](#) for CRS including legislative, technical and operational issues and other guidelines
- Using standardized formats
- OECD's Global Forum and other international organizations provide technical assistance and capacity building for implementation in LMIC

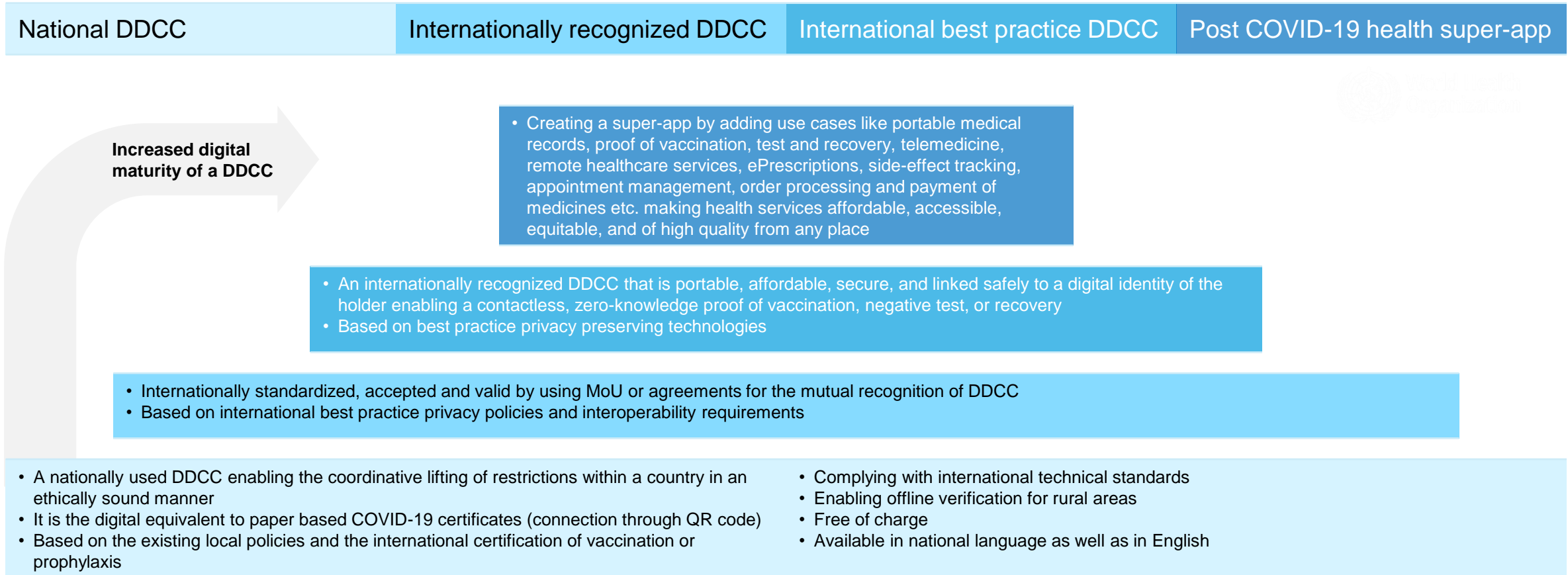
“

PwC financial sector expert

For a standard to be adopted globally there must be a global need, a standard brought forward by a big nation or region and being easy to implement. It simply must be a good standard. Eventually it will be adopted and by the time a critical mass is achieved, it becomes a global standard and every nation will feel the need to adopt it.

4. Decision-making framework

We categorized the different DDCC solutions/platforms into 4 maturity levels and created a policy roadmap accordingly



Source: PwC analysis of key insights through desk research and interviews




Policy recommendations for building a strong regulatory environment for each stage of the DDCC maturity levels – (1/2)

DDCC maturity	Policy types along the maturity roadmap	Policy description and requirements	Policy ¹ / standard ² / initiative ³ / example ⁴
National DDCC	 <p>1. DDCC Policy / Trust framework</p>	<ul style="list-style-type: none"> To use a digital covid certificate in an ethically sound manner authorities should provide clear policies and regulations to determine the usage, validity (vaccines, tests and recovery), issuance, verification, and acceptance, ensuring authenticity and integrity of issued certificates including a trust framework addressing technical specifications structure and processes Either by creating a new policy, adjusting existing eHealth policies or by participating to existing international trust frameworks 	 <ul style="list-style-type: none"> EU Regulation 2021/953¹
	 <p>2. Data protection, privacy and security</p>	<ul style="list-style-type: none"> Authorities and technology providers should ensure that the data privacy and security of the users is well-protected By adhering to local or regional data privacy policies and/or; By ensuring privacy through technology (technology and privacy are intervened) therefore, strive for privacy preserving technologies using appropriate safeguarding techniques such as encryption, decentralization or de-identification, firewalls and zero-knowledge proof verification processes Adheres to the following principles: data minimization, access limitation, use limitation, purpose limitation, collection limitation, openness and transparency, individual participation and control, accountability Should cover the following topics: data ownership, data inventory, data subject rights (informed, access, rectification, erasure, restrict processing etc.), data subject consent, data processing records, personal data breaches, compliance monitoring, data protection impact assessment 	 <ul style="list-style-type: none"> GDPR¹ Convention 108+^{3,1} Health Insurance Portability and Accountability Act (HIPAA)¹ AOKPass as example for privacy by design, the verifier does not process personal data⁴
	 <p>3. Data exchange and interoperability</p>	<ul style="list-style-type: none"> Digital vaccination certificates should use open standards and adhere to international technical standards like the WHO DDCC guidelines or the ICAO VDS-NC guidelines. There are three dimensions of interoperability: <ul style="list-style-type: none"> Technical interoperability (adhering to open and international technical standards) Trust interoperability (shared trust and governance mechanism) Legislative interoperability (policies covering topics like electronic exchange of health data within the country and on a cross-border context) 	<ul style="list-style-type: none"> ICAO guidelines² Decision No 1082/2013/EU on serious cross-border threats to health¹ Directive 2011/24/EU (cross-border healthcare)¹ HL7 FHIR², WHO guideline²

Policy recommendations for building a strong regulatory environment for each stage of the DDCC maturity levels – (2/2)

DDCC maturity	Policy types along the maturity roadmap	Policy description and requirements	Policy ¹ / standard ² / initiative ³ / example ⁴
Internationally recognized DDCC	 4. Mutual recognition	<ul style="list-style-type: none"> It is imperative to make individual, transparent agreements based on law, to ensure mutual recognition of the DDCC and enable international travel Agreements should include at least: purpose of equivalence decision (use case), shared trust framework and connection, acceptance definition, acceptance decision of each others certificates, data protection, connection to PKI if applicable, alignment on data sets and standards, enter into force, accepted vaccinations, tests, recovery and validity 	<ul style="list-style-type: none"> EU's equivalence decisions⁴ Agreement between Singapore and Taiwan following EU equivalence decisions⁴ Trusted travel – my COVID pass Africa initiative³
International best practice DDCC	 5. IT security	<ul style="list-style-type: none"> There should be national laws encouraging solution providers to introduce IT security policies and measures in order to safeguard the systems from potential malicious threats Policies should include topics like acceptable use, awareness training, incident response, disaster recovery plan, access, vendor management, password management, network security, access authorization, modification and identity access management, data retention, mobile device management and procedures, encryption and decryption, system maintenance (monitoring and auditing), and vulnerability management 	<ul style="list-style-type: none"> ISO/IEC 27001 and 27002² Cyber Essentials, UK information assurance scheme¹
	 6. Digital identity	<ul style="list-style-type: none"> Authorities should determine the mechanism for unique identification Consider binding the vaccination certificate to eIDs Policies should include regulations on electronic identification, electronic transactions, electronic identification schemes, electronic trust services, cooperation and interoperability, data protection 	<ul style="list-style-type: none"> eIDAS¹ Estonian eID policy¹ Adhaar used for CoWIN in India⁴
Post COVID-19 health super-app	 7. Streamlined digital eHealth policy	<ul style="list-style-type: none"> Using private-public partnerships and introducing transparent agreements based on a solid legal basis as described above to enable vertical use cases The agreements should be privacy preserving, publicly available and adhere to other domestic and international laws on data privacy, protection, security and exchange There should be a strong focus on user consent and trust by using a streamlined eHealth policy as the app would be handling highly sensitive data Under no circumstance should health data be sold or transferred to third parties who are not working in the public interest 	<ul style="list-style-type: none"> China's Wechat app offering Covid-19 services such as testing and vaccination appointment bookings⁴  EU Agenda on Better Regulation in 2015 addressing self-regulation, the legal basis of most super-apps³

We identified the following challenges faced by LMICs for each policy category and developed recommendations to overcome them (1/2)

	Remaining LMIC specific challenges	Recommendations to overcome challenges in LMIC
 General DDCC legislative	<ul style="list-style-type: none"> Lower digital health maturity countries (level 1-3)¹ completely lack digital policies or have planned policies that are not yet implemented Guidance for countries with no digital health or data security policies is missing Implementation of policies is time consuming and not suitable for a fast response to a pandemic like Covid-19. Digital health initiatives end up in the digital graveyard as soon as there is no funding available 	<ul style="list-style-type: none"> Use extraordinary power measures to enable a quick legal response without having to conduct the existing policy implementation process but ensure an ethically safe procedure thanks to regular human rights impact assessments Create a national digital health strategy focusing on, ICT infrastructure, digital skills, and data governance to build effective domestic digital health frameworks that fit within global regulations and standards and align the DDCC towards that strategy providing necessary resources, coordination, cooperation and leadership Partnering with international institutions (WHO/ITU) is of high value as they have great expertise Leverage already existing capacity, knowledge and experience from domestic or regional eHealth initiatives along IT, policy and health for DDCC strategy and policy development Coordinate investments and funding according to the national health strategy Capacity and funding should also be built around policymakers Policymakers need to build interoperability into their frameworks from the start Adhere to international standards and policies until the domestic legislative area is developed and implemented Allow adequate time for local companies and solution providers to adopt new policies and ensure support through funding, advice, trainings and a structured change management (incl. cultural change)
 1. DDCC Policy / Trust framework	<ul style="list-style-type: none"> The global DDCC policy landscape is fragmented LMICs have implemented DDCC without proper policies in place and relied on the trust framework, terms of condition and privacy policies of the solution providers 	<ul style="list-style-type: none"> Adopt and/or align with best practice DDCC policy (i.e. EU Regulation 2021/953) and trust frameworks and adhere to international standards to reduce global fragmentation Choose best practice regulations from which your citizen would benefit most (i.e. largest used/accepted framework etc.)
 2. Data protection, privacy and security	<ul style="list-style-type: none"> Highly fragmented data privacy landscape LMICs mostly lack a data privacy policy or have only limited to moderate regulations in place Clarifying Lawful Overseas Use of Data Act (CLOUD Act, allows federal law enforcement to compel U.S.-based technology companies to provide requested data stored on servers i.e. Amazon) posing a challenge to data privacy 	<ul style="list-style-type: none"> The Universal Declaration of Humans Rights states that everyone has the right to privacy. This is also valid in the absence of domestic law Adopt and/or align with existing best practice data protection, privacy and security policy (i.e. GDPR) and use it as guideline until domestic policies are effective Privacy by design during development of a DDCC and usage of privacy preserving technologies

¹ According to global digital health index

Source: PwC analysis of [Recommendations on privacy and data protection in the fight against COVID-19](#), [Learning from the past and present: social science implications for COVID-19 immunity-based documentation](#), [UNDP Suggestions for the Emergency](#), Interviews

We identified the following challenges faced by LMICs for each policy category and developed recommendations to overcome them (2/2)

	Remaining LMIC specific challenges	Recommendations to overcome challenges in LMIC
 3. Data exchange and inter-operability	<ul style="list-style-type: none"> Domestic data protection and privacy laws might contain regulations that stipulate that (health)data must not leave the borders of the country LMICs lack the capacity, finances or agreements to facilitate access to public and privately held data. Open data hindered by state-centric cultures Structures for sharing data are not standardized 	<ul style="list-style-type: none"> Change stipulating policies like the lock-in of data within the country or within certain facilities and databases to enable safe data exchange Adopt and/or align with international data exchange standards like the HL7 FHIR and WHO DDCC standards Create clear policies around data exchange with structured and transparent processes Facilitate the public's access to information around their data and data exchange to build trust in society Conduct regular data protection impact assessments
 4. Mutual recognition	<ul style="list-style-type: none"> Low capacity in LMICs to adjust local DDCC to comply international standards needed for mutual recognitions 	<ul style="list-style-type: none"> Establish public-private partnerships to build capacity and share knowledge to adjust DDCC platforms to international standards Conduct mandatory human rights impact assessments and due diligence processes for every public-private partnership
 5. IT security	<ul style="list-style-type: none"> There is a lack of IT security policies on national level in LMIC encouraging solution providers to ensure IT security. According to UNCAT 22 % of the least developed countries have no legislations on cybercrime in place Even advanced DDCC platforms in HIC show vulnerabilities 	<ul style="list-style-type: none"> Implement national IT security policies encouraging domestic solution providers to set up IT security policies and introduce corresponding security measures Continuous IT security life-cycle management is key to secure the DDCC platform Encouraging responsible cybersecurity culture within society
 6. Digital identity	<ul style="list-style-type: none"> Lack of trust / understanding / awareness in current setup in society General mistrust of population towards private companies The legal framework regulating eID is in motion 	<ul style="list-style-type: none"> eID initiatives should be governmental-led as the population is used to the government in charge of physical ID documents – leverage the existent trust Built on highest data security and privacy standards where the identity owner will be in full control. Personal data should only be transferred to third parties (RPs) upon patient consent Should not be pursued before proper domestic data protection, security and privacy laws are in place
 7. Streamlined digital eHealth policy	<ul style="list-style-type: none"> Specific super-app regulations are missing leading to markets taking initiatives to regulate themselves and decentralizing the law-making process There is no obligation to consult terms and conditions with the government and policy makers of a country The WeChat example shows how dangerous super-apps can be without proper data protection, security and exchange policies in place 	<ul style="list-style-type: none"> Policy framework of a super-app should adhere to national or international policies in data privacy, protection and security, data exchange, IT security, digital identity, consumer protection etc. and be consulted with the appropriate governments / policy makers There should be super-app specific policies safeguarding the risk of misuse of the collection of data in vertical use cases; Or policies to deal with the self-regulation of online platforms

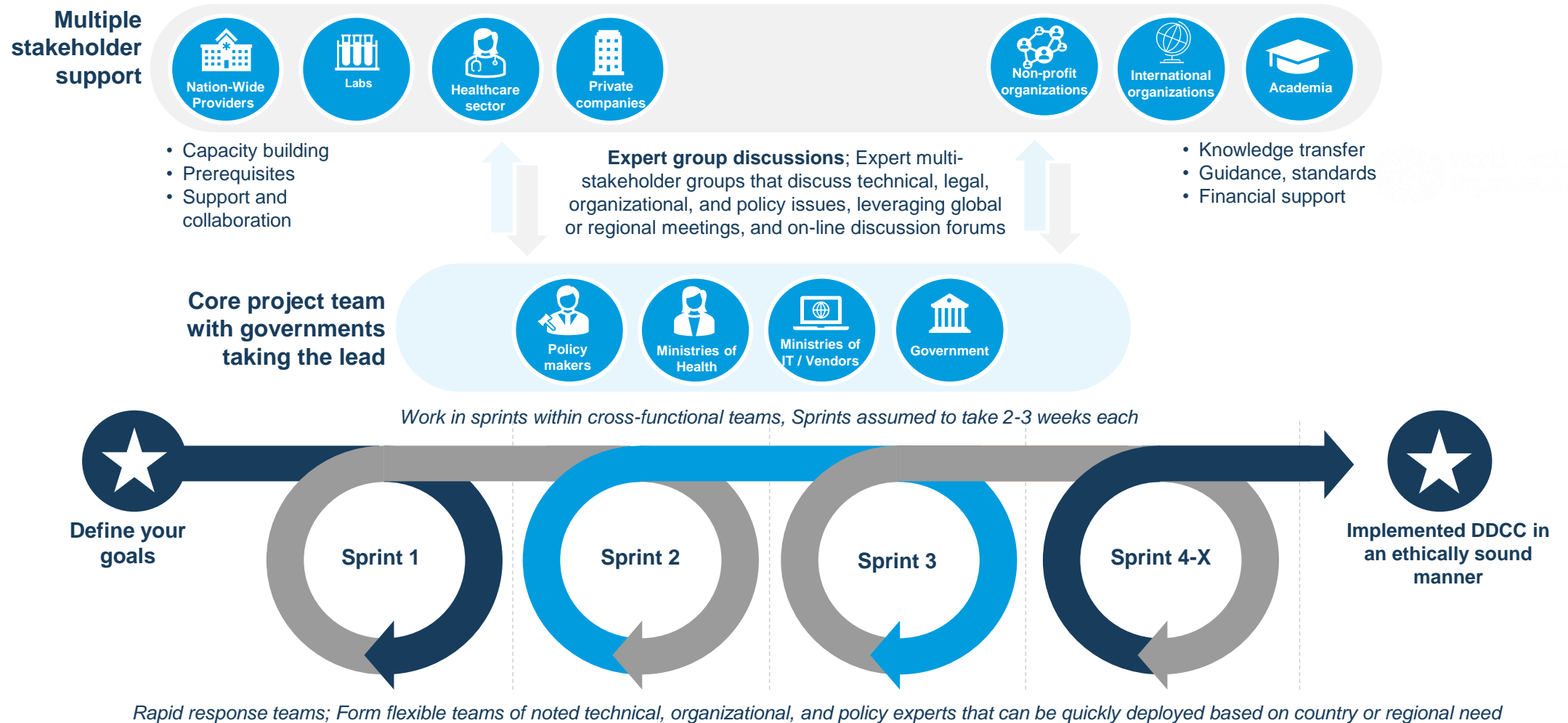
Source: PwC analysis of [Recommendations on privacy and data protection in the fight against COVID-19](#), [Learning from the past and present: social science implications for COVID-19 immunity-based documentation](#), Interviews

Extraordinary protections need to be in place when using extraordinary power measures for a fast legal response

- When in a crisis **states are allowed to use extraordinary power and measures** (Article 4 of the International Covenant on Civil and Political Rights, Article 15 of the European Convention on Human Rights and Article 27 of the American Convention on Human Rights incl. the procedural requirements that states should follow)
- This allows states to have a **fast response** to the pandemic as well as **legal policy changes or implementations** to adjust the law to the current needs due to the pandemic
- Special legal orders and measures should be **transparent, necessary and appropriate**, written and broadcast, and disseminated broadly in appropriate languages and forums
- They have to be coordinated, **risk and evidence based, limited in their severity, duration and geographic scope, Fundamental human rights continue to apply** in special legal orders or periods of emergency
- When they exist in LMIC, data protection and privacy laws should have **clear exceptions that apply to public health crises** to allow for greater use of data than usual
- UN released an [emergency measures and COVID-19 guidance](#) that LMICs could use
- Mandatory human rights impact assessments should:
 - Be conducted regularly, prior to decision-making, during development, at regular milestones, and throughout the policy roadmap
 - Include an evaluation of the possible transformations that they may bring upon existing social, institutional, or governance structures, and
 - Be made available to the public in an easily accessible and machine-readable format



We suggest to operationalize the policy roadmap by using a multi stakeholder approach, agile sprints and extraordinary measures for a quick legal response



Source: PwC analysis of interviews, Scaled Agile Framework (SAFe framework)

5. Next steps

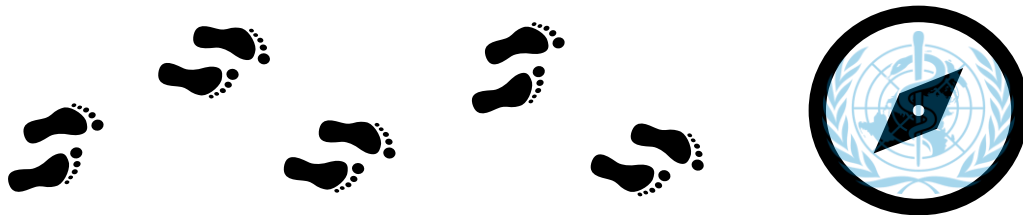
Next steps for WHO include providing guidance for member states to enable a globally coordinated implementation of policies

Next steps for member states using this policy roadmap:

- Evaluate and determine funding mechanism
- Assessing the current health policy environment and conduct a gap assessment
- Deciding which policies are missing and should be included based on the use case and the recommended minimum requirements
- Drafting a high-level DDCC policy roadmap
- Translating high-level DDCC policy into language for national legislations
- Updating an already established eHealth/data privacy policy or;
- Facilitating cross-border DDCC policy collaboration with other countries

What is needed from WHO:

- ✓ Policy guides; A summary of existing notable national- and international-level DDCC (and other categories) policy (see Appendix 1), an analysis of gaps that should be addressed and a guide for countries drafting or updating policies (roadmap incl. recommendations)
- ✓ Expert group discussions; expert multi-stakeholder groups that discuss technical, legal, organizational, and policy issues, leveraging global or regional meetings, and on-line discussion forums
- DDCC legislative templates; develop ready-to-use legislative templates that will guide countries in drafting and introducing policies
- Resource centre; create a systematically updated centre containing policy resources and an online collaborating space to aid users
- International policy resolution; promote an official and actionable policy resolution
- Rapid response teams; form flexible teams of noted technical, organizational, and policy experts that can be quickly deployed based on country or regional needs



“

PwC digital health expert involved in DDCC LU

It was the responsibility of each national certification body to deploy the right architecture to ensure interoperability. LMICs might need guidance on this

“

LMIC government stakeholder

There is lack of national and or multinational coordination on investments regarding implementation of DDCC or eHealth initiatives in general

Appendix I - Most relevant DDCC use cases for LMIC

The Good Health Pass Collaborative (GHPC) blueprint is used as a standard technical framework for deploying interoperable COVID solutions

Framework Overview

- Led by ID2020 with the purpose of reopening global travel
- [The Good Health Pass Interoperability Blueprint](#) is an interoperability and technical framework developed by the GHPC working group
- The blueprint provides a Good Health Pass Ecosystem including the following roles:
 1. Issuers of credentials and passes (i.e. labs, public health systems, rules engines)
 2. Holders of credentials and passes (i.e. travellers)
 3. Verifiers of credentials and passes (i.e. airlines, border authorities)
 4. Governing Authorities who publish rules and policies in a governance framework (aka trust framework)
- Addresses nine technical and interoperability challenges around which global consensus must be reached and provides recommendations on:
 - Interoperability
 - User experience
 - Security, privacy and data protection
 - Identity binding
 - Standard data models and elements
 - Credential formats, signatures and protocols
 - Offline paper credentials
 - Rules engines, trust registries
 - Governance and trust frameworks



Digital health expert from an international foundation working with LMICs

The work of the good health pass was focused on a solution that works globally and on international travel. The output were standards and technical guidance around interoperable platforms and verifiable credentials.

LMICs applicability and usage

- Formed partnerships with Trust over IP Foundation (ToIP) and Covid-19 Credentials Initiative (CCI)
- GHPC engages for interoperability purposes with the following credentialing ecosystems and emergent specifications:
 - EU Digital COVID Certificates
 - Digital Documentation of COVID-19 Certificates (DDCC) – World Health Organization (WHO)
 - Vaccination Credential Initiative (VCI) – United States
 - Digital Infrastructure for Vaccination Open Credentialing (DIVOC) – India
 - Collaborative Arrangement for the Prevention and Management of Public Health Events in Civil Aviation (CAPSCA) - International
 - International Civil Aviation Organization (ICAO)
 - Airports Council International (ACI)
 - CARIN Alliance - US
 - ToIP released a «[Paper Credentials Cookbook](#)» based on the GHPC for creating paper credentials and passes and [GHP Holder Wallet Requirements](#) and UX considerations
- GHPC has [members](#) across the airline and IT industry, international foundations, digital COVID certificate providers etc. (i.e. APEX, IBM, Hyperledger, COVID-19 credentials initiative, ICC, Linux Foundation Public Health, Trust over IP Foundation, Affindi, AOKpass, The Commons Project), therefore these principles are already deployed through DDCC of mentioned solution providers implemented in LMICs



The four layers of governance in the ToIP stack for decentralized digital trust infrastructure.

DIVOC is a DPGA listed public good that enables countries to digitally orchestrate large scale vaccination and public health programs using open source digital infrastructure

Framework Overview

DIVOC by eGovernments foundation India, with its six features (orchestration, facility app, issue vaccination certificates, citizen portal, feedback, analytics) is a standards-driven public good, enabling LMICs to implement the needed infrastructure and features for a large scale vaccination certificate.

- LMICs like India (CoWIN, EU/ICAO standards), Sri Lanka (WHO/DDCC based, with DHIS2), Philippines (with VIMS), Indonesia (with Pandulindugl app) and Jamaica (with Commcare) have implemented DIVOC and deployed a DDCC based on it.
- DIVOC benefits over a fifth of the world's population. Recognised format by 96+ countries globally
- Enables international recognition through compatibility with WHO DDCC:VS and EU:DCC standards
- [Data privacy](#) complies with GDPR, HIPAA for personalised medicines and 21 CFR part 11 (needs to be adopted by implementer if needed)
- Details about the [architecture](#) online available, enables interoperability
- DIVOC is built on top of the generalized electronic registry and credentialing framework available under Sunbird Registry and Credentialing
- [Technical documentation online available, open access to all codes, based on W3C verifiable credentials JSON-JWT](#) available free of charge (funded using philanthropic capital)
- Designed to plug and play with various certificate distribution schemes (printed with QR code, digital using smartphones, sms/email attachments, digital lockers, blockchain based apps, etc)
- Integrates with health wallet apps such as IATA, CommonPass, Digilocker, TravelPass, Folio, Affinidi, Pathcheck and CDC travel pass

Source: PwC analysis of [DIVOC](#), [Digital Public Goods Alliance](#), [DHIS2](#)

Glossary: Digital Infrastructure for Vaccination Open Credentialing (DIVOC) International Civil Aviation Organization (ICAO), District Health Information Software (DHIS2)

General Data Protection Regulation (by EU) (GDPR), Health Insurance Portability and Accountability Act (HIPAA), Code of Federal Regulations USA (CFR)

LMICs applicability and usage

A modular structure and flexible implementation enables LMICs to use and quickly scale up the DIVOC solution

- DIVOC can be connected to the open source platform DHIS2 used by 73 LMICs
- The DIVOC platform is built on the concepts of “Plug & Play” and “Single source of truth” Components can work in various combinations, based on countries’ digital ecosystem and end user needs. Eg : Various valid ID and payment systems of the country
- Can be integrated to the vaccination system of the country
- It covers a lot of digital solutions that has to be in place before being able to use a DDCC (provides all necessary back office components i.e. certificate repository, patient registries etc.)
- Has a modular structure enabling a customized implementation
- Certificates are natively digital, machine-readable, digitally signed, verifiable, and also printable with a QR code making it easy for LMICs to provide it electronically or physically
- Any digitally authenticable ID such as mobile, email, SMS, etc can be used to allow users securely access their certificate from the repository
- [Country adoption guide](#) available for implementation
- Enables LMICs to deploy a customizable, modular, scalable whole-in-one solution incl. DDCC providing the needed technical and legal frameworks and data preserving aspects for mutual recognition and the needed back office components for a fast response to the pandemic



“

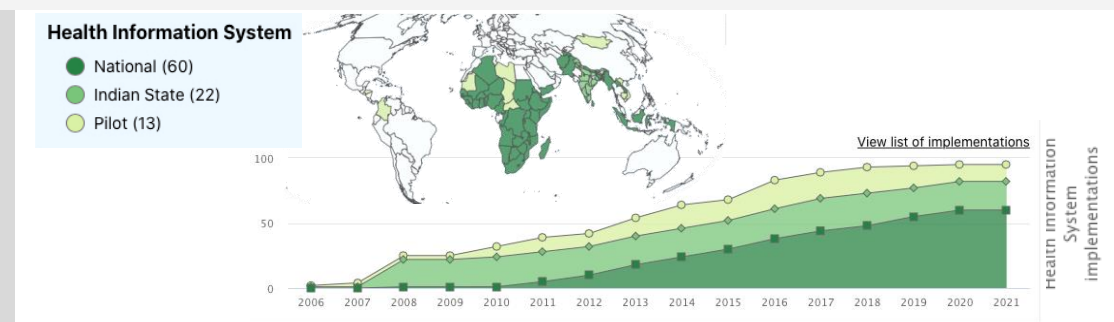
LMIC government stakeholder

“The technology challenges are not really there for us also at the moment we have implemented DIVOC without technology issues.”

The platform to which DIVOC can be integrated, District Health Information Software (DHIS2) is among the largest used digital health platforms in LMICs and is being leveraged for local DDCC platforms

Framework Overview

- DHIS2 is a global public good transforming health information management around the world, developed by the HISP Centre at University of Oslo. Does not have a specific framework, has to be customized by each country to meet local needs and regulations.
- Several countries use DHIS2 data to produce secure DDCC for vaccination or negative test results, through integration with external software applications like DIVOC
- Currently being used to respond to COVID-19 in countries around the world, and has been evaluated as a leading digital solution for COVID-19 response by [Johns Hopkins University](#), the [CDC](#), and [Digital Square](#)
- DDCC generated by DHIS2 are integrable in EU Digital COVID Certificate and DIVOC depending on their customization.
- Already in collaboration with WHO on data toolkits strengthening data use on national and international level, supports interoperability through the use of [OpenHIE](#)
- Can be customized to comply with Digital documentation of COVID-19 certificates, DDCC:VS core data dictionary of WHO, EU DCC Guidelines and WHO's Guidance on National Deployment and Vaccination Planning (NDVP) for COVID-19 vaccines
- Has an open and documented API
- Enables mobile data entry connecting rural areas in LMICs



Source: PwC analysis of [DHIS2](#)

Glossary: Health Information System Program (HISP), Electronic Immunization Registry (EIR)

LMICs applicability and usage

- The flexibility of the DHIS2 platform allows LMICs to deploy a customized DDCC with its needed architecture and software ready to be adjusted to domestic policy frameworks and government mechanisms while complying with international DDCC trust frameworks
- Several Success stories show how DHIS2 based applications enable LMICs to develop, deploy and scale up DDCC
- DHIS2 implemented in [73 LMICs](#)
- Allows the integration of domestic DDCC applications and other software needed for a fast pandemic response (i.e. platforms like RapidPro, Commcare, or applications like DIVOC and Go.Data, see [Digital Square Global Goods Guidebook](#))
- **Togo** is the first country using DHIS2 for COVID Vaccine Delivery to be accepted into the EU Digital COVID Certificate system. Their solution uses the DHIS2 API and an integration developed by Togo's Ministry of Digital Economy and Digital Transformation
- **Sri Lanka** has integrated DHIS2 data with DIVOC, a global public good for vaccine credentialing, to produce secure and verifiable vaccine certificates for national use
- HISP groups in several countries, including **Tanzania, Ethiopia, Rwanda, Laos, Uganda and Vietnam** have worked with national health authorities to develop custom solutions for DDCC that meet local needs
- Has [Covid-19 surveillance](#), [vaccine delivery](#) (incl. EIR), and [education management](#) packages needed for a fast pandemic response
- There are [implementation guidances](#) for DHIS2 and for [DDCC](#) with the example of Vietnam

“

LMIC government stakeholder

“Both of the systems we put in place for covid were built on DHIS2.”

The EU DCC legal framework 2021/953 is the largest used and most comprehensive DDCC framework globally

Framework Overview

The EU DCC framework and its digital pass is with 60 countries across five continents¹ the largest used framework and with its guidance's the most comprehensive one. 15¹ LMICs are already connected to the EU DCC ecosystem.

- Adheres to the comprehensive [EU General Data Protection Regulation \(GDPR\)](#) and ensures data protection and privacy
- Adheres to other wide used DDCC frameworks like the [WHO DDCC technical guidelines](#) and the [ICAO framework](#), IATA backs EU DCC as global standard
- The [EU digital COVID certificate](#) (originally called Digital Green Certificate) solution was released based on this framework designed and developed by T-Systems and SAP
- ICT Infrastructure requirements are suitable for LMICs: PKI-based certificate system (connected countries register their public key to the EU Gateway), offline verification is possible, paper based certificates are available
- The [technical specifications](#) are publicly available and interoperability is ensured with the released [trust framework](#) for interoperability of health certificates and [test certificates](#)
- The following LMICs are already connected to the EU DCC ecosystem and have mutual agreements with the EU in place²
- Examples: **El Salvador** «certificate system "Comprobante electrónico de vacunación"», **Morocco** „SGC'Cov“-system, **Panama** „Certificado de Vacunación Digital Nacional“, **Republic Togo** „PasseCOVID togolais“, **Thailand** "MOHPROMT«

LMICs applicability and usage

Various guidance's and frameworks help operationalize the EU DCC framework and connect a domestic solution to the EU DCC ecosystem.

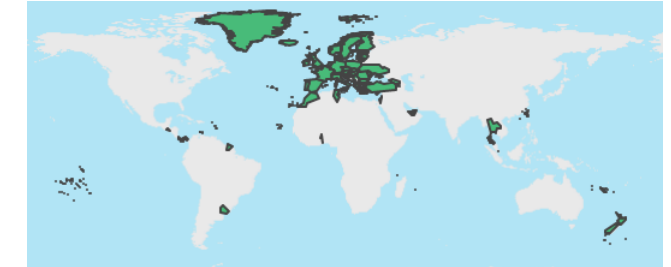
“

Mostly LMICs use the EU DCC regulation and EU GDPR rules as guidance, where domestic policies are missing. Member of an international organization in Sri Lanka: “For COVID certificate we pretty much used European regulations. Our data security laws have still not been passed by the govt. Hence, we try to comply with EU regulations like the GDPR and UK data privacy regulations.”

This is backed by IATA Travel pass that suggests the EU DCC to be used as blueprint and global standard. Even HIC such as Taiwan created their "Taiwan Digital COVID-19 Certificate System" using the EU DCC as blueprint according to their MoH Chen Shih-Chung

- EU has published the code of the solution, it is [Open source](#) and accessible for LMICs
- In case LMICs are seeking for acceptance of domestic digital solution in the EU region, EU has published the [Third Country EU Digital COVID certificate Equivalence Decision procedure](#) incl. a [checklist](#) for third countries to assess if they are able to connect to the EU Digital system, [technical procedure document](#) and an [application form](#)
- In most cases LMICs like Panama have developed a domestic DDCC and design or adjust it to fit the WHO and EU standards to join the EU DCC ecosystem

In green: effectively connected countries¹



“

PwC internal expert on the EU DCC

“The success of **EU DCC** was because each member state has different government mechanisms and manages these things differently. The EU Council put in place a guideline that was applicable for all member states. Thanks to this framework all countries were able to deploy the EU DCC within 2 months.”

¹ as of 21.12.2021 ²List is continuously growing see current [list](#).

Source: PwC analysis of [EU Regulation](#), [EU DCC briefing](#), [EU digital COVID certificate](#), [IATA Travel Pass](#)

Glossary: International Civil Aviation Organization (ICAO), International Air Transport Association (IATA), Information and communication technology (ICT), Public Key Infrastructure (PKI)

International Civil Aviation Organization has published VDS-NC Guidelines including a trust framework and collaborated with a digital Covid certificate ready to connect with local DDCC in LMICs

Framework Overview

The ICAO framework and the IATA Travel Pass provide an international digital covid certificate interoperable with domestic digital and paper based solutions in LMICs

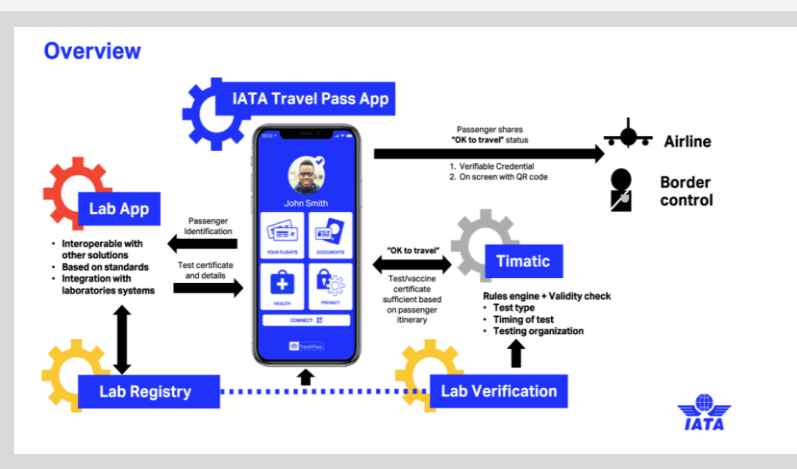
- Adherence to data privacy rights, passengers have the sole right to share their data Users can delete their data anytime on their app.
 - Based on Standards like ICAO DTC, W3C Digital Comms , One ID Initiative, WHO DDCC
 - Specifications for VDS are publicly-available in ICAO s Doc 9303, and are open for any vendor or State to leverage
 - Based on the field-proven VDS technology and trust framework from ePassports
 - See ICAO the public key certificate [member list](#) and [governance framework](#)
 - ICAO has closely collaborated with a digital solution called IATA Travel Pass
 - Use case: to support cross-border mobility of people
 - Using open sources and standards – particularly the ICAO VDS(visible digital seal)-NC – is advised, as this builds on the existing global trust model for travel document verification and offers potential for interoperability and universal access:
1. The 2-level PKI model consisting of a root of trust (CSCA = Country-signing public key certificate authority), a document (barcode) signer and a Public Key Directory. The CSCA does not have to be the same as for e-passports
 2. The certificate profiles as defined by ICAO. The certificate profile guarantees interoperability and security across the travel document and health proof use case
 3. The barcode signer certificate is stored in the barcode itself in order to avoid an additional repository
 4. A standardized barcode encoding. This could be finalized at the end of the discussion process. Easy readability is key

LMICs applicability and usage

The ICAO Framework and the IATA Travel Pass are easy to use and have low requirements on domestic digital or paper based certificates from LMICs

HIC use the DDCC for international travel **and** domestic regulations to manage free movement during the Covid-19 pandemic whereas LMICs are depended on DDCC mostly for international travel. Therefore, so called “Wallet apps” like IATA Travel Pass are sufficient as fast response solution to the Covid-19 pandemic to further ensure free movement and equal rights.

- Only requirements on other certificates to add them to the IATA Travel Pass:
 - Governments issue vaccinations certificates (paper format or digital) based on WHO Smart Vaccine Certificate data standards including QR codes
 - Test certificates are issued in accordance with the data elements set out by ICAO
- Issuance/verification infrastructures already exists among ePassport-issuing countries and can easily be adjusted to COVID passports.
- LMICs are already among member states see [member list](#)
- Some LMICs have already officially accepted the IATA Travel Pass such as [Panama](#)
- [India, Sri Lanka and Indonesia](#) are among those countries to launch IATA Travel Pass and test it
- IATA Travel Pass is a good addition to local digital solutions to enable international travel and accepts vaccine certificates from 52 countries



“

PwC internal expert on DDCC in ZA and sub-Saharan countries

“At the moment there are few options on DDCC for international level. IATA travel pass being one of them.”

Source: PwC analysis of : [ICAO Guidelines](#), [IATA Travel Pass](#)

Glossary: International Civil Aviation Organization (ICAO), International Air Transport Association (IATA), Visible Digital Seals (VDS), Digital Travel Credentials (DTC), World Wide Web Consortium (W3C), Public Key Infrastructure (PKI)

The International Chamber of Commerce enables international travel with their COVID technology AOKpass and its trust framework

Framework Overview

- Launched by the International Chamber of Commerce (ICC), AOKPass is a COVID-19 compliance status pass developed by AOKpass Pte Ltd (Singapore-based technology development firm) in partnership with, International SOS and SGS Group
- Working with the International Standards Organization (ISO) and other multilateral organizations to establish and document an accepted common standard for the provision of digital health certificates (ISO/TC 215 and WHO technical panel for vaccination eCerts)
- Compliant to the W3C standard
- Embed 'Privacy by design' in all data processing carried out by them, see [data privacy policy](#), the **verifier does not have to process personal data at all**.
- Hardcopy certificates issued by medical professionals are digitised, authenticated and then made available for efficient verification
- AOKpass uses pioneering distributed ledger technology based on the Ethereum permissionless blockchain
- Based on VCs technology, no EMR or specific PKI is needed
- Dynamically takes into account industry best-practices and standards as they evolve
- Ensures interoperability by certificate based framework allowing the system to integrate any verification and authentication standard
- Follows the following process:
 - Government issues health and safety requirements for border entry (i.e. COVID-19 negative test result)
 - User completes a COVID-19 screening test at an accredited clinic
 - Clinic issues a digital pass for the user using the ICC AOKpass application
 - User presents the ICC AOK digital pass to border authorities using a scannable QR-code
 - Border agents scan the QR-code to validate the user's pass and allow entry based upon government's health and safety requirements

LMICs applicability and usage

- AOKpass is working with the European Commission IATA, ICAO, G20/B20, OECD, WHO, WEF, WTTC & UNWTO
- Requirement: Healthcare providers have to be accredited by AOKpass first
- As issuer of an AOKPass a computer is the only hardware requirement (an application has to be installed), no server needed.
- International network of over 80,000 accredited clinics and health providers due to partnership with International SoS
- Implemented in the following LMICs governments: **Malaysia, Indonesia, Philippines, Thailand, Argentina, Turkey, Colombia, Timor Leste**
- Implemented in the following LMICs Airports: **Chile, Georgia, Guinea, India, New Delhi, North Macedonia**
- LMICs use the AOK pass like other “wallet apps” in addition to domestic DDCC solutions to enable international travel



CEO of a foundation working with digital health solutions deployed in LMICs

“There is a company that is quite well established international SOS (AOKpass) they work with countries in Africa and manage hospitals in LMICs.”



Source: PwC analysis of [AOKpass](#), [AOKpass Network](#),

Glossary: International Civil Aviation Organization (ICAO), International Air Transport Association (IATA), World Economic Forum (WEF), World Travel and Tourism Council (WTTC), World Tourism Organization (UNWTO), Electronic Medical Record (EMR), Public Key Infrastructure (PKI), International Chamber of Commerce (ICC), Organization for Economic Co-operation and Development (OECD)

SMART Health Cards framework supported by the Commons Project and Vaccination Credentials Initiative (VCI) provides a basis for several certificate apps in use and enable international travel

Framework Overview

The interoperability with other wallet apps and various public-private partnerships with 477+ data sources pose a high applicability of this framework and its digital solution SMART Health Cards for LMICs

- Initiative by HL7, supported by the Commons Project and the Vaccination Credential Initiative (Microsoft and Oracle etc.) to make medical records portable
- Based on WC3 and HL7 FHIR standards and on the VCI™ Principles
- FHIR API access which enable many LMICs working with FHIR to connect to Smart Health Cards.
- Open source technology, [technical specifications](#) are available
- Discloses a minimum amount of information see [privacy policies](#) and code of conduct included in the framework and compliant to GDPR
- Implements government policies regarding COVID of the destination country when travelling
- Framework is applicable for digital solutions as well as paper based certificates
- The DDCC exists of several building blocks making it easy for LMICs to start small and add functionalities as needed
- SMART Health Cards comply with many other solutions such as Commonhealth's CommonPass, EU DCC, providers supported by Epic and providers supported by Cerner making it largely applicable
- The Framework and the SMART Health Cards was established through public private partnerships with many pharmacies, testing labs and vaccination facilities
- DDCC can be issued by listed private entities which is very important for LMICs where governments have only limited resources



LMICs applicability and usage

LMICs use the framework and it's digital solutions for international travel and add domestic digital certificates to the SMART Health Card app

- The SMART Health Cards operate independent of any trust framework, allowing domestic trust frameworks to be layered on top
- For LMICs interested there is a [SMART Health Cards: Vaccination & Testing Implementation Guide](#)
- Supported by the **CommonPass** (IBM) and the Common Trust Network with 45+ national governments
- LMICs like [North Macedonia](#), [South Africa](#), [Rwanda](#) [Senegal](#) and [other African countries](#) are adopting the solution either as stand alone certificate or as addition to other local digital certificates for international travel
- Requirement: Each role (issuer, holder, app) has to be implemented by any organization following open standards, provided they sign on to the relevant trust framework
- SMART Health Cards provide an international trust framework including privacy preserving features and a DDCC ready to use for end-users even applicable to lower income countries without governmental support, as trusted issuers include private entities



Source: PwC analysis of: [SMART Health Cards Framework](#), [SMART Health Cards](#), [The VCI™ Charter](#), [The Commons Project](#)

Glossary: World Wide Web Consortium (W3C), Health Level Seven (HL7), Fast Healthcare Interoperability Resources (FHIR), General Data Protection Regulation (by EU) (GDPR), Verifiable Clinical Information (VCI), Application Programming Interface (API)

Appendix II - Detailed policy categories

1. A DDCC specific policy or trust framework should be in place to ensure a legal basis for digital COVID-19 certificates and their use

Policy requirements and considerations

To quickly enable the right to free movement (Article 13 of the Universal Declaration of Human Rights) and allow for a coordinative way to lift restrictions in an evidence based, and ethically sound manner, a legal basis for the usage of a DDCC shall be created through a DDCC policy. The following topics should be covered.

1. Use case definition

- Use cases should always have a legal basis
- Proof of vaccination and/or continuity of care
- Proof of vaccination should not be a requirement for travel.
- Considering vulnerable populations and religious freedom the use of DDCC should enable proof of negative tests and proof of recovery as well as proof of vaccination

2. Validity of vaccines, tests and recovery

- Specification for verifying certificates
- Acceptance and authorization of the various COVID-19 vaccines
- Combinations of dosages from different vaccine brands, which impacts vaccination/ immunity recognition
- Define whether recovery from COVID-19 infection is seen as equivalent (or superior) to vaccination and whether such infection histories should be combined with a single vaccine dose
- How long immunities/tests are considered valid

3. Issuance and verification, authenticity and integrity

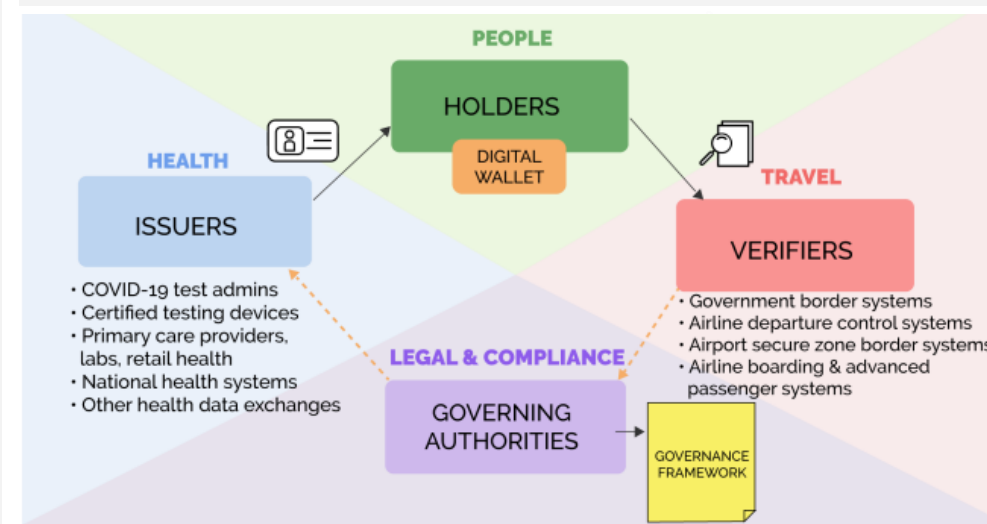
- Specifications for the issuance and verification of the certificate
- To ensure inclusiveness the medium of certificate should be in digital and physical (i.e. paper) due to the digital divide
- Offline verification should be ensured
- Identity authentication should be determined
- Shall allow revocation of certificates

4. Trust framework

- Shall allow for the reliable and secure issuance and verification of the authenticity, validity and integrity of the certificates, based on a PKI or decentralized technology.
- Shall allow for detection of fraud
- References to technical standards (ensure interoperability), used information systems and data protection and privacy policies
- Shall address mutual recognition / agreements and their procedures
- Data fields of users to be recorded, data stored in the digital code (i.e. QR code), and what is displayed to officials or verifiers, should be managed in accordance with local or regional policy needs
- Payment of costs should be defined (shall be free of charge for citizens)
- Human rights impact assessments shall be performed and nation-wide vaccination & test access should be ensured before implementing such policies

Best practice examples

- EU: Regulation (EU) 2021/953
- CH: 818.102.2 Ordinance on Certificates to Prove COVID-19 Vaccination, COVID-19 Recovery or a COVID-19 Test Result
- TrustNet COVID-19 initiative Pakistan



The ecosystem of the trust framework from the Good Health Pass Collaborative blueprint

Remaining challenges and gaps

- There is no international DDCC policy in place
- The global DDCC policy landscape is highly fragmented
- Some governments like the US that do not encourage the use of a DDCC on national level accelerate the development of siloed frameworks
- LMIC have implemented DDCC without proper policies in place and relied on the trust framework, terms of condition and privacy policies of the solution providers

2. Data protection, privacy and security – using data responsibly, protecting data from malicious threats and safeguarding important information

Policy requirements and considerations

According to [UNCAT](#) 45 % of the least developed countries have legislations on data protection and privacy in place, 11 % have draft legislation and 38 % have no legislation at all.

Increased privacy concerns are mentioned towards DDCC. Further, due to the sensitive nature of health data, users face the security risk of being tracked and data snooping by a third party. Thus, it becomes very important to have the right policy set in place covering the following aspects.

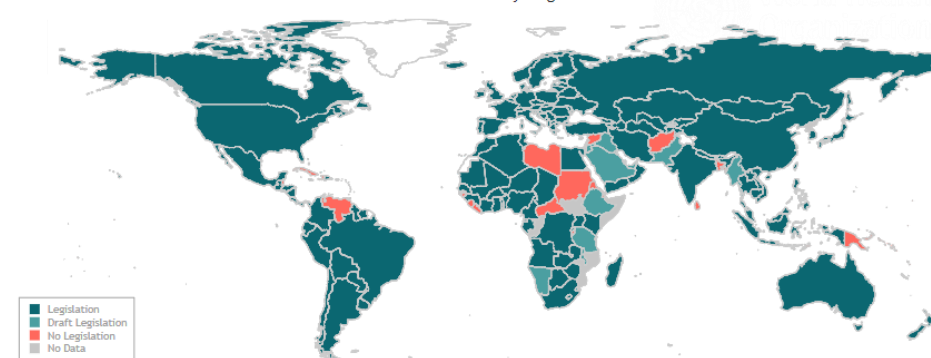
- **Data privacy** - guarding the data against unauthorized access
- **Data protection** - safeguarding important information from corruption, compromise or loss, backup and recovery in the event that it's deleted - overwritten or corrupted
- **Data security** - defence of digital information against internal and external, malicious and accidental threats (related to IT security) by using firewalls, user authentication, network limitations, and internal

The following topics should be covered in data protection, privacy and security policies:

- Data ownership, data inventory
- Data subject rights (informed, access, rectification, erasure, restrict processing etc.), data subject consent
- Data processing records
- Personal data breaches
- Compliance monitoring
- Data protection impact assessment
- Should follow the following principles: Data minimization, access limitation, use limitation, purpose limitation, collection limitation, openness and transparency, individual participation and control, accountability
- Technology and policy are intervened, therefore technically strive for privacy preserving technologies using appropriate safeguarding techniques such as encryption, decentralization or de-identification, firewalls and zero-knowledge proof verification processes

- The development of a DDCC should follow privacy by design and by default principles using i.e. security practices, defence-in-depth strategy, tokenization and encryption
- Data protection and privacy frameworks should balance the need to protect privacy and enable secure innovation

Data Protection and Privacy Legislation Worldwide



Best practice examples

- **GDPR - extraterritorial effect** applicable to any entity that collects/controls data of EU citizens
- Convention 108+, first legally binding international instrument in the data protection field
- Health Insurance Portability and Accountability Act (HIPAA)

- OECD privacy principles
- California Consumer Privacy Act (CCPA)
- AOKPass as example for privacy by design, the verifier does not process personal data

Remaining challenges and gaps

- Highly fragmented data privacy landscape at global level
- LMIC mostly lack a data privacy policy or have only limited to moderate regulations in place
- It is debatable whether working with user consent is applicable for DDCC when it is mandatory for existential activities (enter grocery stores, schools, workplace etc.)

- Clarifying Lawful Overseas Use of Data Act (CLOUD Act) allows federal law enforcement to compel U.S.-based technology companies to provide requested data stored on servers regardless of whether the data are stored in the U.S. or on foreign soil -> some solution provider might use Amazon servers (i.e. Nyaruka Ltd (TestIT/RapidPro)) where the CLOUD Act would apply and cause privacy concerns

Source: PwC analysis of UNCAT, [Data Protection Laws of the World](#), [Digital Landscape of COVID-19 Testing: Challenges and Opportunities](#), [Data protection vs. data security at chino.io](#), [Comparing data protection vs. data security vs. data privacy](#)

Interviews
Glossary: United Nations Conference on Trade and Development (UNCAT), General Data Protection Regulation (GDPR)

22/04/2022 DDCC legal framework assessment and decision-making framework development

3. Data exchange and interoperability are key to enable international travel with digital COVID-19 certificates

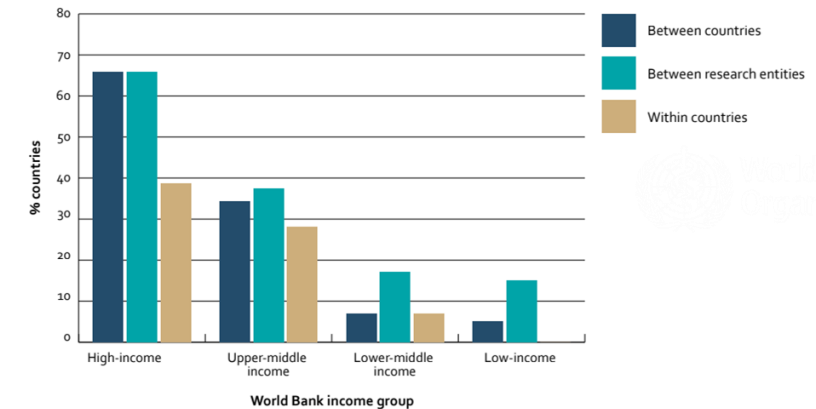
Policy requirements and considerations

There are legal considerations while implementing DDCC in a cross-border setting, due to issues such as data protection and privacy and data interoperability between countries to ensure safe transmission and use of these sensitive information.

- Interoperability shall be one of the primary design principles of the DDCC and it has implications in all components of the trust framework
- The trust framework should enable interoperability with global standards, such as the standards from WHO and ICAO
- Interoperability should enable seamless, on-demand information exchange but should also ensure sharing of data is minimized, strictly limited and whenever possible anonymized
- There are three dimensions of interoperability:
 1. For the **technical interoperability** the following recommendations should be followed
 - Adhering to open standards
 - Adhering to international technical standards like the technical standard WHO DDCC and other international standards like FHIR (standard data models and elements, formats, signatures, and exchange protocols)

2. A **shared trust and governance mechanism** has to be developed and agreed on
3. **Legal basis** for interoperability, policies have to be in place covering the following topics
 - Electronic exchange of health data between databases and facilities
 - Electronic cross-border exchange of health data, the law should allow cross-border transfers on the basis of contractual arrangements that stipulate appropriate data privacy and security controls to be implemented by the organizations, thus establishing sufficient levels of protection for data leaving the jurisdiction
 - Cooperation (establishing MoU) and shared policies (i.e. data privacy, security, protection and exchange, data ownership, user consent etc.)

Fig. 6.4b. Country legislation governing sharing of health-related data, by World Bank income group



Best practice examples

- HL7 & FHIR
- Covid credential initiative
- Good health pass collaborative interoperability blueprint
- WHO Digital documentation of COVID-19 certificates: vaccination status: technical specifications and implementation guidance
- ICAO guidelines Visible Digital Seals ("VDS-NC") for TravelRelated Public Health Proofs
- [IATA blueprint](#) for simplifying air travel
- GDPR, Convention 108+ and other data privacy policies address data exchange as well

Remaining challenges and gaps

- Domestic data protection and privacy laws might contain regulations stipulating that (health)data must not leave the borders of the country posing a challenge for data exchange
- Open data policies are still relatively new and underutilized in LMICs. They lack the capacity, finances, or agreements to facilitate access to public and privately held data
- **Open data in many LMICs is also hindered by state-centric cultures** within which it is considered sufficient to have public institutions alone responsible for controlling and monitoring data collection
- Thus far, the structures for sharing such proprietary data are **not standardized, so private data in most existing public-private partnerships is only made available on an ad hoc basis**

Source: PwC analysis of [Blockchain applications in health care for COVID-19 and beyond: a systematic review](#), [Essential Legislative Approaches for Enabling Cross-Border Data Transfers in a Global Economy](#), Interviews

Glossary: International Civil Aviation Organization (ICAO), International Air Transport Association (IATA), Health Level Seven or HL7, Fast Healthcare Interoperability Resources

4. Mutual Recognition of local DDCC lowers the complexity for users during travelling

Policy requirements and considerations

Users should be able to rely on a single DDCC app wherever they are. Therefore, mutual recognitions of local DDCC among different countries have to be set up. There are two main topics to be agreed on for mutual recognition of DDCC:

1. The governance and trust framework on issuance, verification and acceptance of the certificates;
2. The data included in a DDCC, privacy and ethical issues

Questions¹ to be asked before setting up mutual recognitions

- Which countries are most of our visitors from?
- How is the COVID-19 situation in those countries? How do their case incidence rates compare to ours?
- Do we have adequate capacity to detect and cope with expected additional COVID-19 cases while maintaining essential health services?
- Which COVID-19 vaccines should we recognize for a visitor's proof of inoculation?
- Are visitors' countries issuing national COVID-19 certificates, and in what formats?
- How can those certificates be verified?
- Do we have the infrastructure and personnel to conduct verifications, or the resources to build up such capacity?


Topics to be covered within a mutual recognition:

- Purpose of equivalence decision (use case)
- Shared Trust framework and connection
- Governance
- Acceptance definition
- Acceptance of each others certificates
- Data protection (which data is processed, for which reason, retention of data, data ownership etc.)
- Information exchange processes
- Applications and IT infrastructure (i.e. connection to PKI and alignment on data set etc.)
- Enter into force
- Accepted vaccinations, tests, recovery and validity

Best practice examples

- EU's **parallel unilateral agreements** for mutual recognitions of digital COVID-19 certificates with third countries. The EU sets up two agreements per country, one for the acceptance of DDCC issued by a third country in the EU and vice versa with a second agreement. The agreements are called "**Commission Implementing Decision (EU) on the equivalence of COVID-19 certificates issued by [country name]**" and can be found [here](#)
- EU's successful "equivalence decisions" even enable third countries that have been accepted into the EU system, to set up agreements with each other following the EU decision like the example of Singapore – Taiwan below.
- There are other ongoing initiatives to have regional aligned and interoperable COVID-19 certificates like the [Trusted travel my covid pass Africa](#) reducing the number of agreements that have to be set up at global level



Singapore Trade Office in Taipei 
about 2 weeks ago

Following the decisions by the European Commission to recognise Singapore's and Taiwan's digital COVID-19 vaccination and test certificates on 24 November 2021 and 21 December 2021 respectively, the authorities in Singapore and Taiwan now recognise and accept each other's digital COVID-19 vaccination and test certificates. This is a positive step towards the further easing of border measures for travel between Singapore and Taiwan.

繼歐盟委員會分別於 2021 年 11 月 24 日和 2021 年 12 月 21 日承認新加坡和台灣的數位新冠病毒健康證明後，新加坡與台灣的相關單位已承認和接受雙方的數位新冠病毒健康證明。這是新加坡與台灣為雙邊旅行進一步放寬邊境措施所邁出的積極一步。 — 😊 feeling happy.

Remaining challenges and gaps

- Challenges such as the reliability of the certificates and trustworthiness of certifying bodies or authorities, the data protection guarantees, and the interoperability prospects
- Capacity in LMIC to conduct adjustments to local DDCC to comply international standards
- "One of the major global problems we face is that common standards and governance for security, authentication, privacy and health data exchange have yet to be agreed on," says Bernardo Mariano, Chief Information Technology Officer at the United Nations

¹Adopted from [The territorial impact of COVID-19: Managing the crisis and recovery across levels of government](#)

Source: PwC analysis of: [Quick Guide on Digital COVID-19 Certificates: Re-enabling Cross-Border Travel](#), [Emerging Issues From a Global Overview of Digital Covid-19 Certificate Initiatives](#), [Taiwan, Singapore recognize each other's COVID vaccination certificates](#), DDCC equivalence decisions by EU
Glossary: Public Key Infrastructure (PKI)

5. National and international laws on IT security should be developed to enable trust in a digital COVID-19 certificate

Policy requirements and considerations

Cybersecurity and privacy is an investment in what is potentially the most precious asset in DDCC: **Trust**. A **digital** COVID-19 certificate is aspired to avoid fraud. To be able to rely on the truthfulness of a DDCC and avoid malicious threats, IT security is imperative. There has to be IT security policy in place not only by the solution providers (no. 1 concern in [PwC CEO Survey 2022](#)) but by the government in general. A policy-driven development should be pursued.

The following topics shall be covered in a IT security policy that might be used for a DDCC

- Acceptable Use policy
- Security awareness and training policy
- Incident response policy
- Disaster recovery plan
- Access and Remote access policy
- Vendor management policy
- Password creation and management policy
- Network security policy
- Access Authorization, Modification, and Identity Access Management
- Data Retention Policy

- Mobile Device Management (MDM) Policy and Procedures (especially important for DDCC)
- Encryption and Decryption Policy
- System Maintenance Policy (monitoring and Auditing)
- Vulnerability Management Policy
- Criminal consequences for cybercriminals

Cybersecurity comprise five dimensions that shall be perused

1. Developing cybersecurity policy and strategy;
2. Encouraging responsible cybersecurity culture within society;
3. Building cybersecurity knowledge and capabilities;
4. Creating effective legal and regulatory frameworks; and
5. Controlling risks through standards and technologies

Best practice examples

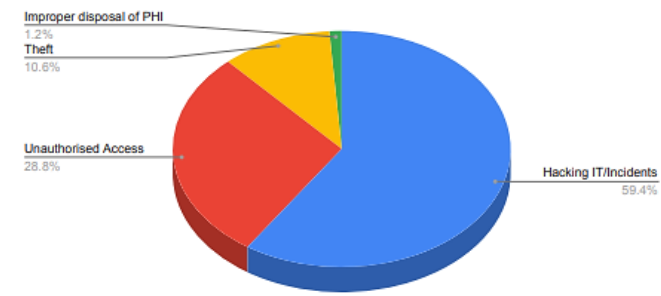
• International IT security standards, applicable for DDCC

- ISO/IEC 27001 and 27002, information security management system
- ISO 15408, secure integration and testing of software and hardware
- ISO/IEC 29115 Entity authentication assurance framework
- ETSI EN 303 645, for Internet of things (i.e. MedTech for OptiBP)

• National

- NIST, cybersecurity framework to help private entities that provide critical infrastructure with guidance
- Cyber Essentials, UK information assurance scheme encouraging organizations to adopt good practice information security
- GDPR and HIPAA also address IT and data security topics

Types of Healthcare breaches in 2019



Remaining challenges and gaps

- Security and cyber risks can result in direct costs, decrease trust in the DDCC system and lower user adoption
- There is a lack of IT security policies on national level in LMIC encouraging solution providers to ensure IT security. According to [UNCAT](#) 22 % of the least developed countries have no legislations on cybercrime in place
- A lot of security breaches are happening despite IT security measures in healthcare (i.e. Security vulnerability in the app used by New Jersey and Utah briefly made it possible to request the QR codes of other users, containing encoded name, date of birth, and vaccination history information)
- Therefore, a continuous IT security life-cycle management shall be pursued

Source: PwC analysis of [BITSIGHT the standard in security ratings](#), [PwC cybersecurity and privacy](#), [University of Oxford, Global Cyber Security Capacity Centre](#), [Opening up with COVID-19 passes](#), [Digital Landscape of COVID-19 Testing: Challenges and Opportunities](#)

Glossary: United Nations Conference on Trade and Development (UNCAT), International Organization for Standardization (ISO), International Electrotechnical Commission (IEC) General Data Protection Regulation (by EU) (GDPR), Health Insurance Portability and Accountability Act (HIPAA)

22/04/2022 DDCC legal framework assessment and decision-making framework development

6. Digital identity policies may be used to enable a contactless verification process in times of a pandemic

Policy requirements and considerations

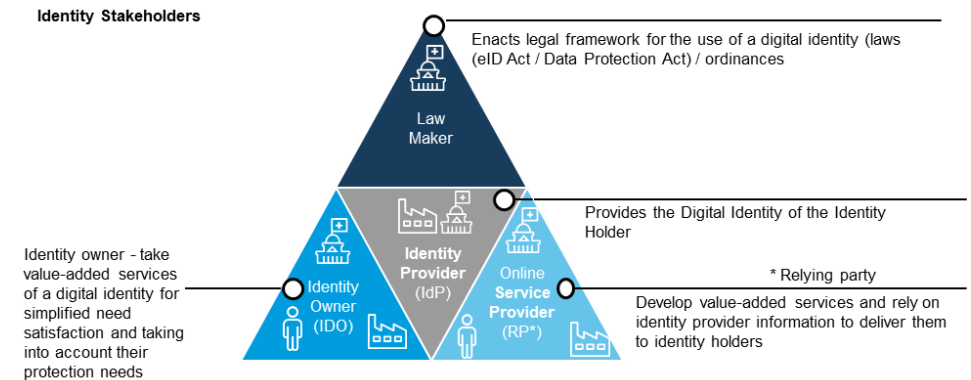
In the absence of a standardized way to identify people or entities, every website started to create its own digital identity solution with its own local accounts & passwords. As a result people **lost control of** where **personal data** has been provided

- People want to make use of digital identities and claim need for simplified and secure end-to-end interaction (COVID as accelerator)
- The protection of the **Identity Owners (IdO) data privacy is key**, eID-law needs to be built around data protection and should follow data minimization
- Identity owners must always have full transparency and control on the usage, distribution and storage of their information
- Enable trust through a **government managed solution** with one implementation provider
- An eID regulation should address the following topics: **Regulations on electronic identification, electronic transactions, electronic identification schemes, electronic trust services (CH: eID Draft legislation (under revision) / EU: eIDAS), cooperation and interoperability, data protection**
- Compliance with core identity regulations like **electronic trust services laws** (i.e. CH: eID / EU: eIDAS), eSignature (ZertES)
- **Electronic authentication mechanisms** like electronic signature, qualified digital certificates, electronic seals or timestamps shall be covered in the policy (i.e. eSignature law CH: CeS (German: ZertES) / EU: eIDAS), and health/eHealth policy (i.e. CH: Federal Act on the Electronic Patient Dossier (EPD – identity related)
- Determine how to handle undocumented individuals

- The risks arising from entering relationships with third parties need to be identified, assessed and controlled over the entire lifecycle of the business relationship
- Identity owners (residential) shall not have to pay fees, private corporations and public entities may be charged
- eID solution(s) will be successful in case the population clearly perceives its VALUE, therefore governments should focus on providing eID on the highest trust level to enable vertical use cases (e.g. Government / Health / Insurance / Banking / Commerce / Travel...)
- Compliance with vertical domestic regulations (i.e. CH and EU: banking (AML/KYC (AMLA) / FINMA AML ordinance / CDB20 (VSB), insurance: insurance contract act, specific regulations on eCommerce, eHealth, eGovernment et al.)

Best practice examples

- High success / widespread usage of eID solutions: Estonia / India / Singapore
- **Estonian eID**, data protection EU GDPR, simple to use, eSignature feature exists, fulfils other vertical use cases as well, capabilities to fulfil health requirements
- **EID SingPass**, data protection gov-led, simple to use, eSignature feature exists, fulfils other vertical use cases as well, capabilities to fulfil health requirements
- **eID India (Aadhaar)**, data protection gov-led, time consuming onboarding, signature feature does not exist, fulfils banking use case as well, in progress for other use cases, capabilities to fulfil health requirements (used for CoWIN identification)
- **eIDAS** as best practice example of a digital identity policy
- [One ID project](#) by IATA



Remaining challenges and gaps

- The risk of exposure, loss or harm of information through data breaches or cyber attacks
- Lack of trust / understanding / awareness in current setup in society
- General mistrust of population towards private companies with regards to governmental eIDs
- The legal framework regulating eID is in motion and therefore all potentially upcoming changes need to be closely monitored

Source: PwC analysis of Main - EPFL - Digital Identity Week / various, eIDAS, eID CH, Aadhaar, eID Estonia, SingPass

Glossary: Anti Money Laundering (AML), Know Your Customer (KYC), Anti Money Laundering Act (AMLA), Revised agreement on the Swiss banks' code of conduct with regard to the exercise of due diligence (CDB20 (VSB)), electronic Identification, Authentication and trust Services (eIDAS), General Data Protection Regulation (by EU) (GDPR), International Air Transport Association (IATA)



Health super-apps would allow the concentration and streamlining of fundings and capacity in the digital health area

Policy requirements and considerations

- Super apps serve as **single portal to several virtual products and services**
- Most popular in the Asian region, LMIC start to adopt in Asia and Africa
- Possibility to **add digital health use cases and services** like proof of vaccination, portable medical record, ePrescription, telemedicine, monitoring (i.e. OptiBP), side effect reporting etc.
- Super apps **fit in the ICT infrastructure of LMIC**, enable downloading from cheap smartphones with less capacity/storage needed (one app for everything)
- **Enables streamlining of funding's, capacity and policy frameworks**
- Avoids siloed health data
- Would serve as the main point of data exchange
- Key success factors include **partnerships, ecosystems, open data and API's**
- Policy framework of a super-app **should adhere to national or international policies** in data privacy, protection and security, data exchange, IT security, digital identity, consumer protection, specific regulations on eCommerce, eHealth, eGovernment and eBanking

Remaining challenges and gaps

- Specific super-app regulations are missing; innovation is faster than state regulations, leads to markets taking initiatives to regulate themselves and **decentralizing the law-making process** (shielded by principle of freedom of contract)
- There is **no obligation to consult terms and conditions with the government and policy makers** of a country
- The WeChat example shows how dangerous super-apps can be without proper data protection, security and exchange policies in place
- Risk of monopoly formation

Examples

Dominating on-demand services are taxi services, food delivery, grocery delivery, logistics, **doctor on-demand, pharmacy delivery**

WeChat, China



- [Terms of Service](#)
 - Regulating the use of WeChat, special terms for USA, Australia, UK, EU and Singapore considering i.e. their domestic consumer protection acts
- [Privacy Policy](#)
 - Servers located in Singapore and Hong Kong Special Administrative Region
 - Relies on the European Commission's model contracts for the transfer of personal data to third countries
 - Includes country/region specific terms
 - No end-to-end encryption
- [Acceptable Use Policy](#)
- [Copyright Policy](#)
- Concerns:
 - Banning of LGBTQ friendly and feminist accounts
 - Alleged foreign surveillance and censorship
 - May hand over any data to governments when necessary
 - Uses data of other vertical use cases to i.e. risk-assess loan applicants etc.

Other examples:

- Go-Jek, Indonesia (example with digital health services)
- Grab, Singapore and Indonesia
- Temtem ONE, Algeria
- M-Pesa, Kenya

[EU Agenda on Better Regulation in 2015](#) addressing “well-designed non-regulatory means” for better regulation in the EU

Glossary & references

Glossary (1/2)

Terminology	Description
APEC	Asia-Pacific Economic Cooperation
API	Application Programming Interface
CAPSA	Collaborative Arrangement for the Prevention and Management of Public Health Events in Civil Aviation
CFR	Code of Federal Regulations (USA)
DHIS2	The District Health Information Software is used in more than 60 countries around the world. DHIS is an open source software platform for reporting, analysis and dissemination of data for all health programs, developed by the Health Information Systems Program.
DTC	Digital Travel Credentials
EIR	Electronic Immunization Registry
EU	European Union
FHIR	Fast Healthcare Interoperability Resources is a standard describing data formats and elements and an application programming interface for exchanging electronic health records. The standard was created by the Health Level Seven International health-care standards organization.
Global goods	<ul style="list-style-type: none"> • Global Goods are digital health tools that are adaptable to different countries and contexts. There are three types of global goods: • Software A software tool that is free and open source (FOSS), and used to manage, analyze, or transmit health-related data, with proven utility in several settings. • Services A software tool that is used to manage, transmit, or analyze health-related data that can be freely accessed as a software service and adheres to open data principles. • Content A resource, toolkit, or data standard that is available under an open license and that is used to improve or analyze health data management processes.
GDPR	General Data Protection Regulation released by the European Union

Terminology	Description
GDPR	General Data Protection Regulation released by the European Union
HICs	High-income countries based on gross national income (GNI) per capita (for 2022 fiscal \$12,696 or more) as published by the World Bank.
HIPAA	Health Insurance Portability and Accountability Act (USA)
HISP	Health Information System Program (HISP)
HL7	Health Level Seven or HL7 refers to a set of international standards for transfer of clinical and administrative data between software applications used by various healthcare providers. These standards focus on the application layer, which is "layer 7" in the OSI model.
IATA	International Air Transport Association
ICC	International Chamber of Commerce
ICRC	International Committee of the Red Cross
ICT infrastructure	<p>Information and communication technology infrastructure are the components required to operate and manage enterprise IT environments. IT infrastructure can be deployed within a cloud computing system, or within an organization's own facilities.</p> <p>These components include hardware, software, networking components, an operating system (OS), and data storage, all of which are used to deliver IT services and solutions.</p>
ICAO	International Civil Aviation Organization
ID2020	ID2020 is a nongovernmental organization which advocates for digital ID for the billion undocumented people worldwide and under-served groups like refugees.
LMICs	Low to middle income countries based on gross national income (GNI) per capita (for 2022 fiscal year between \$1,045 or less and \$4,095) as published by the World Bank.
MOH	Ministry of Health

Glossary (2/2)

Terminology	Description
OECD	Organisation for Economic Co-operation and Development (OECD)
PaaS	Platform as a service
Policy/legal frameworks	A set of rules that govern the rights and responsibilities of governments, companies and citizens, Legal frameworks comprise a set of documents that include the constitution, policies and legislations, specific regulations as well as corresponding contracts.
PKI	Public Key Infrastructure
SaaS	Software as a service
SaMD	Software as a medical device
SMEs	Subject Matter Experts in global stakeholder donors, technical agencies, implementation agencies
Trust frameworks	A set of rules and policies that govern how federation members will operate and interact (e.g., with regard to identity certification, data security etc.). Trust frameworks serve as the basis for multilateral agreements that enable trust and governance amongst all its federation members.
VCI	Verifiable Clinical Information
VDS	Visible Digital Seals
W3C	The World Wide Web Consortium is the main international standards organization for the world wide web

References

Key references

- Building a Global Framework for Digital Health Services in the Era of COVID-19 ([Information Technology & Innovation Foundation](#))
- Connected Health: Empowering health through interoperability ([Global digital health Partnership](#))
- Essential Legislative Approaches for Enabling Cross-Border Data Transfers in a Global Economy ([Centre for information policy leadership](#))
- Cross-Border Data Transfer Mechanisms ([Centre for information policy leadership](#))
- The global footprint of data protection regulations ([PwC](#))
- eHealth Policy in LMICS: National Frontiers, Global Challenges ([Disruptive Cooperation in Digital Health](#))



Thank you



WHO

20, Avenue Appia
1211 Geneva

Switzerland