Achieving Global Interoperability of Health Certificates

OECD

ACHIEVING GLOBAL INTEROPERABILITY OF HEALTH CERTIFICATES

Introduction and background

In response to COVID-19, governments and organisations across the world have developed and adopted standards and technologies to create, present, and verify digital vaccination and testing credentials. To simplify public health measures at points of entry into a country, governments are looking at ways to ensure safe mobility for their people where mutual acceptance of commonly shared systems is vital. Such proof of credentials can also be used within countries, when access to bars, restaurants, cinemas, and similar, is made conditional on being vaccinated or having a recent negative test result.

In May 2021, in the OECD published a blueprint that included a basic set of principles and guidance on the development of digital certificates for proof of vaccination, diagnostic test results or recovery from COVID-19 (OECD, 2021[1]). In July 2021, the WHO has published extensive guidance around the concept of Digital Documentation of COVID-19 Certificates (DDCC), which are mechanisms by which the data of COVID-19 vaccination status or results of diagnostic tests for COVID-19 can be digitally documented via an electronic certificate (WHO, 2021[2]).

Since then, supranational political and economic unions, notably the European Union, international organisations, national governments, private sector organisations, and non-profit organisations have been developed standards for electronic certificates for COVID-19 vaccination, diagnostic test certificates, or evidence of recovery form COVID-19. Over time, many of these initiatives have been implemented, some of these initiatives have been abandoned and others have been implemented and consolidated with broader worldwide coverage.

While the contents below focus mainly on vaccine certificates, the main points relevant for interoperability are also applicable for other COVID-19 health certificates, such as results of diagnostic tests or proof of prior infection from COVID-19.

1. Main initiatives of digital COVID-19 vaccination certificates

As of early July 2022, the most widely adopted standards of COVID-19 vaccination credentials are:

- **European Union Digital COVID-19 Certificates (EU DCC)** – The European Commission has developed the EU DCC standard. It is used by 27 EU member countries to issue certificates for vaccines, diagnostic test results, and recovery from COVID-19. Another 45 countries issue equivalent certificates, which are recognised in the EU under the same terms as those issued by EU member countries.

- **Vaccination Credentials Initiative (VCI) Smart Health Cards** – The Smart Health Cards standard was developed by the VCI, a coalition of public and private organisations mostly based in the United States. Digital certificates using the VCI Smart Health Card standard are issued by 24 states and territories of the United States, eight other worldwide issuers, as well as health care providers, pharmacies and laboratories in the United States. The United States does not have a centralised national standard for vaccine certificates.
- **International Civil Aviation Organization (ICAO) Visible Digital Seal (VDS)** – The VDS standard was developed by ICAO, and currently two countries issue certificates using this standard.
- **Digital Infrastructure for Verifiable Open Credentialing (DIVOC)** – The DIVOC standard was developed the eGov foundation of India, and it is issued by 5 countries.

2. A global interoperability framework of vaccination credentials

A globally agreed upon framework to enable convenient use of these credentials – while also allowing domestic autonomy over their use – does not exist and is critically needed. A global interoperability framework would ideally enable digital vaccination credentials issued by one nation/jurisdiction, to be trusted, verified, converted, and reissued for domestic use within another nation/jurisdiction. This approach would:

a. **Seek to preserve a jurisdiction's autonomy regarding its domestic processes for the type(s) of vaccination credentials it will accept.** Achieving consensus on converting digital vaccination credential formats allows governments and organisations to make use of credentials in their desired format. Although support for each credential format could be provided, and some governments support multiple credentials today, having defined approaches for converting and reissuing credentials into a domestic format has greater potential to allow for a safer, more consistent experience within that jurisdiction.

b. **Establish technical, process, and policy agreement on the steps necessary to convert and reissue digital vaccination credentials from one framework/standard to another.** A global interoperability framework would include the most prominent global standards and technologies deployed to date, such as the EU DCC, Smart Health Cards, ICAO VDS, and DIVOC, and potentially others. Participation by all parties would be supported through the development of free and open-source standards and software implementations.

c. **Ensure a framework remains for federated, mutual recognition of credentials among participants, and help to consolidate demands around establishing a Global Trust Network, a regulatory framework, and technical interoperability.** Regardless of format, it is critical that shared data is trusted so that it can be acted upon with confidence. Guidance and a consensus on an approach for globally sharing trust information, whether through a federated or a centralised approach, will allow all national, regional, state/provincial, and local governments to quickly engage in this multilateral effort.

d. **Ensure jurisdictions with less resources will have the technical guidance and support to reduce the burden of implementing the technical infrastructure to participate in this effort.** Core to the mission of the organizing bodies sponsoring this effort is ensuring that resources will be applied to develop guidance, technical tools, and open-source code for all member jurisdictions to be able to leverage the multiple vaccination credential technologies and standards adopted across the world today. Sharing defined, open-source approaches for converting and reissuing credentials into a local format via co-ordinated gateways allows for a consistent experience within a certain locale.

3. The nuts of bolts of digital certificates

The operation of each of digital health certificates such as those used for COVID-19-related purposes requires an infrastructure and a set of rules to ensure that: (a) only authorised issuers can generate certificates; (b) the authenticity of certificates can be properly verified; (c) the information contained in them can be read, understood and trusted by intended users; (d) the privacy of certificate holders is protected; (e) each country can apply their own set of health policies to verify compliance; and (f) fraudulent or otherwise invalid certificates can be revoked. The main components of this infrastructure are described below.

Contents of certificates and terminology

Digital certificates contain a set of data points that varies according to their use. In the case of digital COVID-19 vaccination certificates, these typically include the name of the person that has received the vaccination, the date of birth of the person that received the vaccine, the name and manufacturer of the vaccine, the date of the injection and its order in a vaccination course (e.g. the second vaccine of two prescribed shots). Other data fields may be included, such as the number of the identification document of the person receiving the vaccination, the name and registration number of the professional who administered the injection, or the place where the vaccination took place.

Regardless of the contents, the format of the data in the digital certificates must either be uniform across all issuers in the system or there must be ways to convert the terminology used by different issuers. In other words, there must be an agreement about **terminology** for all certificates. For example, the way dates are stored must use a common format and the description of brand of vaccines used must follow a common standard.

Public key infrastructure

Digital certificates contain an electronic signature that can be used to attest the authenticity of their contents. This relies on mathematical formulas that convert the contents of the certificate into a “signed document”, which encodes the contents of the certificate. The conversion process combines the contents of the certificate using of sets of characters called “**private keys**” that are kept confidential and can only be known and used by authorised issuers. These certificates can then be decoded and read with the use a set of characters called “**public keys**”, which should be broadly disseminated from a trusted source. The use of public keys allow for a confirmation that the party that issued the certificate had access to the private keys, and therefore there can be certainty that the information displayed in the digital certificate presented at the point of use (e.g. a control by a border agent) is exactly same as the information that was included in the certificate when it was issued. The technology that stores, lists, and disseminates the public keys is called the **public key infrastructure** or **PKI**. A PKI is therefore, a set of processes, systems, software and rules around the management of digital certificates.

For this to work, a mechanism is needed to generate public and private keys, which are created in pairs because they have a unique mathematical relationship that allows for encoding and decoding of certificates. The private keys must be stored securely, and only authorised parties can access them to sign certificates. Moreover, a mechanism is also needed to distribute the public keys, which is called **public key directory** or **PKD**. The PKD can be centralised or distributed among participants (in that case, it is called federated), but in all cases it must include provisions to reassure the recipients that the public key has come from a trusted source, which in technical terms is known as the certificate authority (typically a ministry or a public agency). Preparations should also be made for certain certificated to be cancelled, or revoked, when there has been a breach of trust in any point of the production of certificates.

Trust frameworks

This system relies on agreed upon principles of trust, set of rules, and technical requirements which are typically called **trust frameworks**. Participants in the trust network must be able to trust that the parties within the digital signature system only allow authorized entities to use private keys for signing and issuing the certificates, and they must be able to obtain the public keys from a trusted source to verify the authenticity of the documents that were encoded using the private keys. For example, the participants in the EU DCC described before have agreed to participate in a trust framework, while the participants in the VCI Smart Health Cards participate in another trust framework, and so on.

QR-codes

In the majority of COVID-19 vaccination certificates, these are represented visually with the use of a **QR-code**, which is a visual representation of digital information which can be stored in a device such as a smartphone, but that can also be printed on paper and carried by the user. QR-codes contain the desired information which has been encoded by software used by the service that administered the vaccine, and which are then given to the vaccinated person. The underlying information contained in the vaccine certificate is not stored anywhere else, other than the code itself that is carried by the vaccinated person. The public key infrastructure purpose is therefore to verify that whatever contents are included in the QR code (e.g. name of the person, date of birth, date of injection and so on) is the same as it was included by the professional who had access to the private keys that are expected to be trusted.

Business rules (i.e., public health policies)

As indicated above, there must be uniformity in the way certificates are generated and there must be agreement about the rules for issuing certificates and how to verify them. However, the participation in a trust framework for COVID-19 vaccination certificates does not mean that all vaccines are going to be accepted in the same way for all participants. These will depend on the health policies that are adopted by each country, or in the language of digital certificates, on the **business rules** of each jurisdiction.

For example, if country A and country B participate in the same trust framework for COVID-19 vaccination certificates, they can be sure that the certificates are going to be issued using a same format, and that their authenticity may be verified at any point. However, country B may not recognise all of the types of vaccines used in country A. Therefore, a digital COVID-19 certificate carried by a person from country A can be read in country B and considered to be authentic (that is, not fraudulent), but not necessarily valid for travel or access to a public venue such as a restaurant or a concert for example, because country B may not approved the use of that vaccine.

Digital verification

The process of **digital verification** of a COVID-19 vaccination certificate must include two separate steps: first confirmation that the certificate is authentic, and second confirmation that the contents of the certificate attest that the person carrying it complies with the business rules (or health policies) established by the jurisdiction reading it. While the digital verification of a certificate means that its contents can be validated using the electronic signature, there are mechanisms that can be used for this verification to be done online (on a device connected to the internet) or even offline (depending on the design of the system and the software used for verification). The software that performs verification is commonly known as verifier.

4. Achieving interoperability and the G20 pilot

The Indonesian G20 Presidency has listed the harmonisation of global health protocol standards as one of its priorities, and it has worked to achieve this objective in close co-operation with a technical group led by the World Health Organization (WHO), and co-chaired by the Organisation for Economic Co-Operation and Development (OECD), and the Global Digital Health Partnership (GDHP).

Achieving global interoperability of COVID-19-related health certificates does not necessarily require that all jurisdictions used the same standard. Interoperability can also be achieved when there are mechanisms in place so that certificates issued by one jurisdiction are accepted in another. For this to happen, interoperability requires that there are pre-agreed mechanisms that will allow, among other things, to:

- **define common terminology –** interpret the information contained in the certificates of the different trust frameworks, and participants know the format used by each certificate and the codes that are used to represent the names of vaccines, dates included in the certificates, sequence and number of dose of vaccine received, and so on;
- **integrate or federate the distribution of public keys –** store and share the means for verification of authenticity of certificates including sharing of public keys used by the trust frameworks;
- **check for revocation –** verify whether certain groups of certificates have been revoked or not;
- **recognise or reissue –** prepare jurisdictions to either automatically accept certificates issued by other jurisdiction, or read certificates from other jurisdiction and reissue them using a local format;
- **verify compliance –** access a description of health policies related to travel in each countries to verify compliance of the certificate with the requirements in place.

References

eGov Foundation (2022), *DIVOC Home*, https://divoc.egov.org.in/. [5]

European Commission (2022), *EU Digital COVID Certificate*, https://ec.europa.eu/info/live-work-travel-eu/coronavirus-response/safe-covid-19-vaccines-europeans/eu-digital-covid-certificate_en. [3]

ICAO (2021), *Guidelines. Visible Digital Seals ("VDS-NC") for Travel-Related Public Health Proofs.*, ICAO. [6]

OECD (2021), "OECD initiative for safe international mobility during the COVID-19 pandemic (including blueprint)", *OECD Policy Responses to Coronavirus (COVID-19)*, OECD Publishing, Paris, https://doi.org/10.1787/d0594162-en. [1]

VCI (2022), *Issuers of SMART Health Cards*, https://vci.org/issuers. [4]

WHO (2021), *Digital documentation of COVID-19 certificates: vaccination status: technical specifications and implementation guidance*, World Health Organization, Geneva, https://www.who.int/publications/i/item/WHO-2019-nCoV-Digital_certificates-vaccination-2021.1. [2]

Points for discussion

- Is there agreement that there should be digital certification of proof of vaccination, or test results?
- How should the countries verify the authenticity and validity of certificates?
- Should digital vaccination certificates converge into a single standard, or is it sufficient to achieve interoperability among main blocks?
- Who should host the infrastructure for interoperability of digital health certificates in the long run?