IBM Digital Health Pass: A Privacy-Respectful Platform for Proving Health Status

Whitepaper

Elli Androulaki[1], Ilie Circiumaru[1], Jesus Diaz Vico[1], Miguel Prada[1], Alessandro Sorniotti[1], Marc Stoecklin[1], Marko Vukolić[1], and Marie Wallace[2]

[1]*IBM Research – Zurich*
[2]*IBM Watson Health*

Abstract

IBM Digital Health Pass (IDHP) is a technology developed by IBM offering the technical infrastructure to allow individuals to prove their COVID19-related health status (e.g., whether that individual was tested negative for COVID19, has been partially/fully vaccinated, or recovered from COVID19) to third parties in a *secure* and *privacy-respectful* way.

In a nutshell, IBM Digital Health Pass technology enables *issuers*, i.e., authorized healthcare providers onboarded to the system by health authorities of a given country or jurisdiction, to produce digital attestations about individuals' health status. These attestations, called *Health Certificates* are issued to individuals, called *subjects* or *holders*, and are stored on a piece of paper or within subjects' mobile phone wallets. Subjects can then demonstrate the authenticity of one or more of their Health Certificates to third parties of their choice called *verifiers*, when the necessity of demonstrating COVID19 related health status arises. Subjects can also demonstrate their association with each of their Health Certificates.

IBM Digital Health Pass is built around preserving individuals' privacy as a first-class requirement, based on established public key cryptography concepts in a way that can easily scale to millions of Health Certificates.

1 Introduction

IBM Digital Health Pass is a technology developed by IBM to help our world transition to a more sustainable COVID19-aware lifestyle.

More specifically, IBM Digital Health Pass offers the technical infrastructure to allow individuals (owning smart phones or not) to prove their COVID19-related health status to third parties in a *secure* and *privacy-respectful* way, while at the same time putting in place necessary foundations for *interoperability* with other systems with similar purpose. Examples of health status include, e.g., whether an individual was tested negative for COVID19, has been partially/fully vaccinated, or recovered from COVID19. IDHP approach also comes with no special hardware requirements on the individuals side, who are not required to have or even know how to operate a smart phone to make use of the technology.

To this end, IBM Digital Health Pass (IDHP) technology enables *properly authorised* healthcare providers, called *Issuers*, to produce digital attestations about the individuals' health status. We call these attestations *Health Certificates*, while referring to an individual the Health Certificate is issued to, as Health Certificate *Subject* or *Owner*. In IDHP, we also adopt the term *Holder* to denote the individual or device that holds/stores the Health Certificate on behalf of the Certificate's subject. As IDHP Subjects are very frequently identical to these subjects' certificates holders, the terms Subject, Owner, Holder will be used interchangeably henceforth. Health Certificates can be printed on a piece of paper or scanned and imported to the Holder's smart phone.

Subjects can choose whether to demonstrate ownership of one or more of their Health Certificates to third parties, called *Verifiers* in a way that assures that Health Certificates (i) have not been tampered

with, (ii) have been produced by a properly authorised Issuer(s), and (iii) they refer to the claimed Subject.

Methodology. At the heart of IBM Digital Health Pass technology sits traditional Public Key Infrastructure (and digital signatures) [AL03] and a publicly accessible registry of authorised issuers and their signature public keys. More specifically, Health Certificates have the form of digitally signed verifiable claims of individuals' health status. At the same time, authorised issuers are equipped with digital signature key-pairs, allowing them to produce Health Certificates. To assess the authenticity of a Health Certificate, Verifiers confirm that the key that was used to generate the Health Certificate belongs to an authorised Issuer by querying the public key registry of Issuers. In our solution the registry is being administered by one or more special authorities, the *healthcare administration authority(ies)* of a country, that decide on the authorised Issuers (e.g., vaccination centers, testing centers, etc.) and their exact issuing authorisation (e.g., what types of certificates they are entitled to issue).

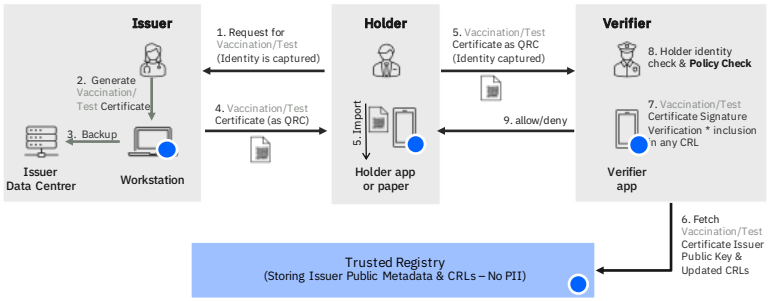

Figure 1: Issuing and Verification of IDHP Health Credentials. The blue sphere indicates components that IDHP offers functionality for.

Paper Outline. In the remainder of this paper, we first present the IBM Digital Health Pass architecture in Section 2, followed by the discussion of the privacy and security properties of the system, deployment alternatives and prospective interoperability with other similar systems in Sections 3, 4, and 5 respectively.

2 System Architecture

2.1 Actors

In IBM Digital Health Pass (IDHP) we identify four types of actors: Issuers, Subjects and Verifiers, as well as one or more Administration Authorities. The system also utilizes a Trusted Registry, which holds metadata pertaining to Issuers and Health Certificate revocation information. More specifically:

Administration Authorities are responsible for authorising Issuers and controlling the types of credentials that are made available through the system (e.g., structure of test certificates, vaccination certificates, or others). Administration Authorities may represent a country's Health Ministry, local or national governments, or other higher-level (healthcare) institutions. In certain solution scenarios, Verifiers are required to obtain a permission from an Administration Authority in order to use the system. IDHP Administration Authorities constitute the roots of trust for IDHP.

Issuers are the entities authorised by an Administration Authority to issue Health Credentials of a specific type. These types may include, e.g., vaccination certificates, test certificates, proofs of recovery from COVID19, etc. Issuers can be medical representatives (e.g., doctors) from hospitals, test and vaccination centres, pharmacies and similar healthcare providers. Issuers are entrusted to attest the

health status; from the trust model perspective, Issuers are trusted to only issue Health Certificates to individuals in accordance to their demographics and clinical data, i.e., do not introduce false information into the Health Certificates they issue. Furthermore, they are trusted not to share Subject's Personally Identifiable Information (PII) to unauthorised entities without Subject's consent. Issuers local health records are outside the scope of IDHP. Should Issuers be required (e.g., by law) to maintain their own system of healthcare records, this requires a system external to IDHP.

Subjects are individuals who need to obtain a statement attesting their health status (PCR test result, vaccination, or any other type of claim that is deemed necessary by the authorities) and demonstrate that statement's authenticity to Verifiers. From the trust model perspective, Subjects may attempt to tamper with a Health Certificate, or to mislead a victim Verifier into accepting a Health Credential of another user/subject as their own; for this reason they may collude with other subjects or with other Verifiers. Every Health Certificate is associated to a single Subject, which is called the Subject of the Health Certificate.

Verifiers are individuals or organisations that check the health status of individuals that want to access their premises or use their services. From trust a model perspective, IDHP Verifiers are motivated to learn the validity result of a given Health Certificate and to the extent to which this matches to the individual that is showing it to them. From a trust model perspective, verifiers are trusted to not share information of the Health Certificate that a Subject has shared with them. At the same time our system guarantees authenticity and confidentiality of health certificates even against verifiers that collude with other participants of the system, to gain access to health data that none of the colluding entities are authorised to access.

Trusted Registry is an entity controlled by (one or more) Administration Authorities. Its objective is to maintain and provide upon request public metadata of authorised Issuers, as well as Health Certificate revocation information that are crucial for the secure verification of Health Certificates. The Trusted Registry implements the following functionalities upon properly authorised requests:

- Issuer onboards, by creating an entry for an authorised Issuer;
- Updates an authorised Issuer public information;
- Provides the public information associated to an Issuer;
- Sets and updates an authorised Issuer's Certificate Revocation Lists (CRL);
- Provides the CRL of a specific Issuer;
- Sets and updates authorised Health Certificate types.

2.2 Security & Privacy Requirements of Health Passport Systems

Due to the sensitivity of the Health Passport use case, security and privacy are key requirements.

From a security perspective, we require that Health Certificates issued by Issuers satisfy the following properties:

- **Authenticity.** Health Certificates cannot be tampered with without the collaboration of the Issuer who produced the Health Certificate.
- **Non-transferability.** A Health Certificate must not be transferable to a Subject other than the one the Health Certificate refers to.
- **Non-repudiation.** Issuers cannot repudiate the issuance of a Health Certificates that they have previously issued.

From a privacy perspective we require that the access to a Health Certificate is restricted only to authorised parties. More specifically, IDHP satisfies the following property.

Privacy A given Health Certificate may be accessible *only* by:

- the Issuer who issued the Health Certificate,
- the Subject of a Health Certificate (i.e., the Subject that the Health Certificate refers to),
- any party authorised by the Subject (e.g., a Verifier).

Parties who have not explicitly been given access to the Health Certificate by its owner cannot access the Health Certificate even if they collude with other actors in the system.

2.3 Approach

In the following we detail how issuers acquire the necessary authorisation to join the system, receive required credentials and start issuing health certificates; we also discuss how health certificates are being verified by verifiers, and how health certificates are being revoked.

Issuer Registration Administration authorities authorise issuers to issue different types of health certificates. The overall process is depicted in Figure 2.

Administration authorities operate Standard X.509 PKI Certificate Authorities, granting issuers with X.509 certificates detailing their issuing authorisation as part of an issuer-specific registration/enrolment process.

The credentials issued in this phase qualify the issuers to onboard with the Trusted Registry. More specifically, during the *registration phase*, Administration authorities perform appropriate due diligence to the issuers requesting to register to the system, after which they engage with issuers to the *enrolment phase*.[1] In the enrolment phase, issuers locally generate a key-pair, and receive an *enrolment certificate* (an X.509 certificate). This certificate (and respective key-pair) gives the issuer ways of authenticating to the trusted registry.

Issuer Onboarding Issuer onboarding takes place with the issuer reaching out to the trusted registry where issuers authenticate themselves using *enrolment certificates*. To produce health certificates, issuers generate a new signing key-pair and submit the verification key to the trusted registry. The latter creates a record for the onboarded issuer accordingly, mapping the issuer to its verification key. The issuer locally stores their signing key to use it to sign health certificates.

Health Certificate Schema Definition The administration authorities or issuer also submits to the trusted registry one or more *schemas*. A schema describes the set of fields that constitute a health certificate, from the byte-level representation up to the certificate structure. The schema definition is accessible to all verifiers. Conversely, schema definitions can be modified by the corresponding issuer by creating a new version of an existing schema (e.g., remove one field or add another), or a whole new schema for a different use-case. This way, the system achieves consensus on how to interpret all health certificates, all the while permitting the system to evolve (e.g., to accommodate new FHIR concepts).

Certificate Issuing Figure 1, visualises the interactions associated to the issuing of health certificates.

At issuing time, subjects are expected to physically visit the premises of an issuer of their choice, authenticate themselves to that issuer using traditional means of identification (e.g., government issued identity cards, health-insurance cards etc), perform the appropriate test or the requested vaccination, and receive a valid health certificate in return in the form of QR code. In fact the returned QR code encodes the health certificate that is a digital signature generated by the issuer using their respective signing key.

There are multiple ways in which the health certificate can be delivered to the subject, but this is out of scope of this whitepaper. In the end, the subject can decide where to store its health certificate: get a physical printout of the QR code and store it in its physical premise, or import it on their smart phone by leveraging IDHP or other wallet apps[2].

[1] We emphasise that the honest behaviour of Administration authorities are assumed to be enforced by contract, e.g., through audits from regulatory entities that ensure compliance. In this sense, enforcing this behaviour is outside the technical scope of this paper.

[2] IDHP wallet application does not require synchronisation with any cloud provider/server; data in the wallet reside fully on the phone.

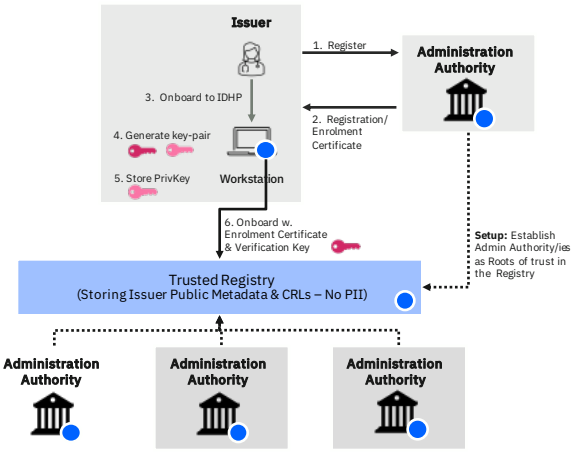

Figure 2: Issuer registration and onboarding. The blue sphere indicates components that IDHP offers functionality for.

At the end of the issuing process the issuer may decide to store the issued health certificate locally in their own system of record for audit purposes. The exact implementation of this system of record is out of the scope of the IDHP platform.

Certificate Verification Figure 1, visualises the interactions associated to the verification of health certificates.

At verification time, the subject shows their health certificate to a verifier of choice. This is done by exposing the health certificate as QR code on the subject's phone or on a piece of paper, from where the verifier can scan it using the IDHP Verifier App.

The verifier app subsequently decodes the QR code, and extracts the issuer identifier, the certificate identifier, subject identification information and the schema. It first queries the trusted registry for the metadata associated to the claimed issuer. In this way, the verifier app confirms the issuing authorisation of the issuer and retrieves the verification key of the issuer. Using the latter, the verifier checks the digital signature in the certificate and get assured that the health certificate was indeed generated by the claimed issuer. In cases where health certificates can be revoked, the verifier also checks whether the certificate's identifier[3] is included in the certificate revocation list published by the claimed issuer to the trusted registry. To enable offline verification of certificates, verifiers can cache the issuing public keys and revocation lists of authorised issuers in their app.

To ensure that the health certificate is bound to the subject that has initiated the verification process, the verifier has to compare the subject's identification information in the certificate with the one included in traditional forms of subject identification (e.g., driver's license, government issued identity card, etc). This is done with the consent of the subject.

After the signature has been verified, the verifier will parse the payload of the health certificate according to the schema that is also specified in the certificate, and whose definition the verifier can reliably retrieve from the trusted registry. The payload can then be interpreted unambiguously to reveal the certified medical data. Verifiers can check for expiration of certificates if this is prescribed in their policy. Expiration can also be enforced directly from the credential schema, in which case, no active revocation is needed for expired certificates.

Certificate Revocation When an issuer decides to revoke a health certificate that has already been issued to a user, they publish its unique identifier in the trusted registry. This way all verifiers will be able to reject this certificate. This happens when verifiers fetch from the trusted registry the list of revoked health certificates associated to the claimed issuer and check that the identifier of the health certificate they are to verify is not part of that list. Figure 3, visualises the described interactions.

Key rotation Over time, issuers will generate new signing key-pairs and submit the verification key to

[3]The certificate's identifier is a random number, picked by its issuer at the issuing of the certificate.

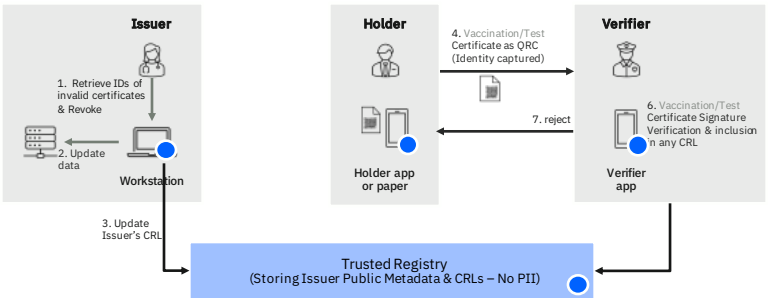

Figure 3: Revocation of IDHP Health Credentials. The blue sphere indicates components that IDHP offers functionality for.

the trusted registry. They will also revoke their old key-pairs. These operations can be performed by the issuer after authenticating itself to the trusted registry using its enrolment certificate.

3 Security & Privacy of IDHP

Security We argue that IDHP meets the properties established for Health Passport systems in Section 2.2.

- *Authenticity.* Health Certificates are digitally signed statements, produced by approved issuers. The public keys used by issuers to sign certificates are listed in the trusted registry, maintained by a (set of) trusted authority(ies) and easily auditable. This registry also lists the identifier of all revoked Health Certificates. Therefore: (i) digital signatures ensure that the certificates have not been tampered-with and cannot be forged; and the trusted registry ensures that (ii) only accepted issuers can produce credentials, which (iii) will be rejected in case of revocation. Thus, only legitimate and unrevoked credentials produced by approved issuers will be accepted by IDHP-enabled verifiers.
- *Non-transferability.* The Health Certificates produced by IDHP include information that binds them to the (legal) identity of its subject. Consequently, since credentials cannot be tampered with nor forged, only the subject in possession of the corresponding identifier can successfully prove having been issued that credential.
- *Non-repudiation.* Approved Issuers register in the trusted registry the public keys associated to the private keys they use to issue Health Certificates. The produced certificates thus directly inherit from digital signatures their non-repudiation property, and no Issuer can claim not having issued a certificate that validates against one of its public keys written in the trusted registry.

Privacy We argue that, as required in Section 2.2, in IDHP, the contents of a Health Certificate are accessible only by: (i) Issuers, when they digitally sign them; (ii) any Verifier to whom the Subject decides to show his Health Certificate; and (iii), of course, its legitimate Holder – who may decide to store it in paper or digital form. When issuing a Health Certificate, the Issuer has access to the certificate information. However, this information is not used by the Issuer afterwards, with the only exception of the certificate identifier, which may be used if revocation is needed. In order to verify a Health Certificate, the verifier only needs to fetch the public key of the alleged issuer, and the list of revoked credentials. Thus, no information whatsoever about the Health Certificate needs to leave the verifier's software, who is trusted to properly perform verification and delete any information afterwards. We assume the latter is the case, as the verifier has been selected by the subject as trustworthy to honour the confidentiality of the subject's Health Certificate's data. At the app level this trust is justified through contract and code audits that such apps are subjected to.

Issuers and verifiers having access to (part of) the credential data during issuance and verification is a hard requirement given the need to attest the Subject's legal identity and physical health. We emphasize, however, that in order to perform their duties, IDHP does not require issuers or verifiers to send any PII to any other component – and, specifically, no such information is ever sent to the trusted registry, which is used to enhance the transparency of PKI-related management tasks. Consequently, no party

that has not been explicitly authorised by the Subject will have access to any information related to his Health Certificates.

4 Realising a Trusted Registry

As indicated in the previous sections, the trusted registry is an important component of our system's security architecture.

More specifically, IDHP security relies on the assumption that the trusted registry will update issuer metadata and health certificate revocation lists according to authorised issuer and administration authorities requests. Moreover, IDHP security provisions rely on the fact that the trusted registry will respond to verifier queries correctly, i.e., in accordance to the content of the registry.

Clearly, one could implement the trusted registry as a robust, but centrally controlled service. This would still position the trusted registry as a single point of failure for IDHP: if the single entity that controls the registry is compromised, then the answers of the trusted registry to verifier queries can no longer be trusted, and the system would no longer be able to accurately assess health certificate validity. On the other hand, such centralisation is frequently inconvenient in settings where health administration is distributed across the various municipalities of a country (e.g., USA, Spain, Germany), or member states of a union of states (e.g., European Union). In these cases, having responsibility of the correct operation of the major security component of the system being shared across the system's stakeholders may be appropriate.

The IDHP Trusted Registry is implemented using permissioned Distributed Ledger Technology(DLT), as we wanted our registry to provide resistance to authority missbehavior/compromise by shifting the functional responsibility to the system's stakeholders, while at the same time ensuring that these stakeholders would enjoy full control over the system's governance (adding new members, upgrade functionality, etc.). Figure 4 demonstrates IDHP interactions with a decentralised Trusted Registry.

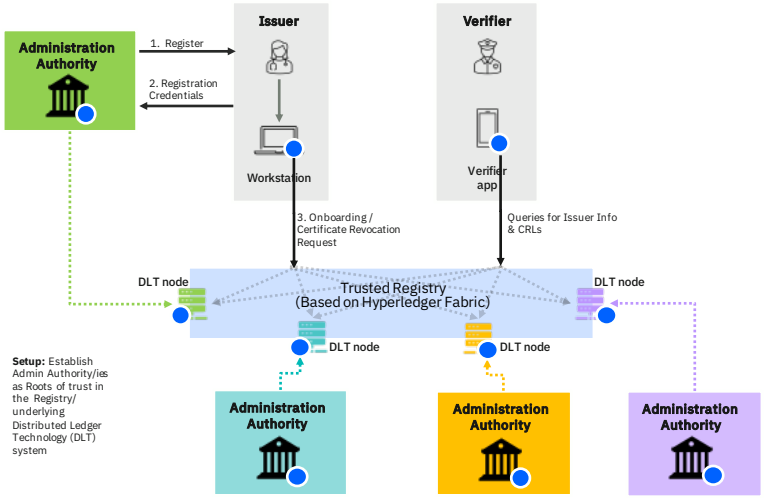

Figure 4: IDHP interactions using a Distributed Ledger Technology (DLT) based Trusted Registry. The registry is configured to acknowledge one or more Administration authorities as its roots of trust, and accept onboarding requests from issuers accordingly. Each Administration authority can optionally provide a node for the operation of the DLT. Issuer's onboarding or health certificate revocation requests are being sent to the DLT nodes of the different stakeholders, as do queries of the verifiers on the updated Certificate Revocation Lists (CRLs) and Issuer public keys/info. In this way it is guaranteed that the correct action is always taken by the Registry as a whole.

IDHP leverages Hyperledger Fabric [ABB+18], an open-source platform, whose architecture has been peer- reviewed by top-tier scientific conferences committees, and has been largely adopted by the enterprise DLT world. On the purely technical level, Hyperledger Fabric offers multiple advantages compared to other enterprises alternatives from scalability, performance, and governance perspective, and nicely integrates traditional Public Key Infrastructure hierarchies.

5 Other Architectural Considerations

In this section we elaborate on other important IDHP deployment alternatives concerning services that could facilitate administration and issuing operations of the system, as well as interoperability objectives and features of the system.

5.1 Facilitating Issuer Administration & Health Certificate Issuing

Issuer Registration/Enrolment and Onboarding, as well as Health Certificate Issuing is an operation that requires infrastructure on the issuer side beyond installing a mobile phone application. More specifically, all these operations would require extensions or the installation of completely new systems in the existing (inflexible) technical infrastructure of hospitals, doctors, other health care facilities.

As such a change is not always easy to be accommodated, and in order to meet the urgency of the times, IDHP is offering *Administration Authority*, and *Issuer* as a Service, which also avoids large investments to deploy extensive infrastructures. The use of these two services are depicted in Figures 5, and 6.

An Administration Authority can leverage the *IDHP Administration Authority Service* to facilitate the Registration and Enrolment of issuers of its choice, where the service would manage the generation and maintenance of related signing keys and issuer authorisation requests on behalf of the Administration Authority. In the same spirit an Issuer can leverage the IDHP Issuer Service to onboard itself to the system (using the Administration Authority issued registration credentials) and to request the issuing/revocation of Health Certificates. It is important to note that IDHP services do not include the storing of the Health Certificates on behalf of the issuers, and this is something that Issuers should tackle out of band. Health Certificate data is being deleted from the service, right after the issuing request is accommodating, positioning the IDHP Issuing Service as PII data processor and not controller.

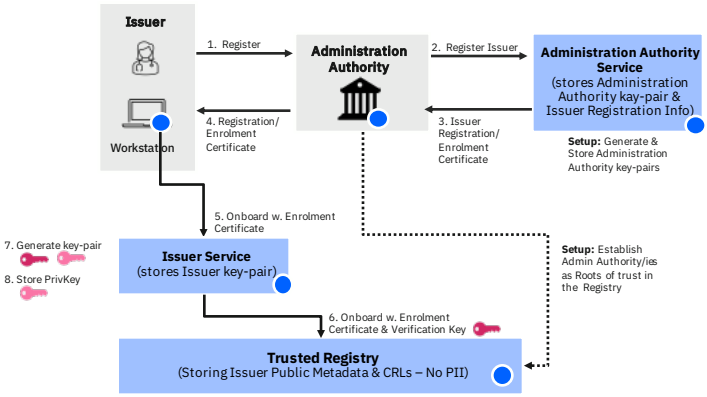

Figure 5: Use of Administration Authority Service to register and Issuer Service to onboard an Issuer. The Administration Authority Service can generate or be configured with the considered Administration Authority's key-pair. From that point onwards it accepts Administration Authority's requests to register an Issuer of choice with a specified authorisation type to the system. The Service responds to these requests with that issuer's registration credentials, as described in Section **??**. If applicable, these credentials are used henceforth by the Issuer to setup his Issuer Service, that facilitates the actual Issuer onboarding to the Trusted Registry.

Finally, IBM offers the possibility of hosting the DLT-based Trusted Registry on behalf of the involved Administration Authorities. This can be a temporary or permanent setup depending on the specific use-case requirements. Clearly, in such a centralised deployment of the Trusted Registry, IDHP/IBM would be entrusted the correct operation of the Trusted Registry (as the operator of that system). However, we emphasise that the Trusted Registry at no point handles PII, and as such its responsibility is restricted to ensuring the integrity of the Trusted Registry's content and authorised updates.

5.2 Interoperability Considerations

Interoperability comes as an important requirement in IDHP, as we expect that many instances of IDHP and/or related third-party (external) solutions will be deployed in different jurisdictions motivated by

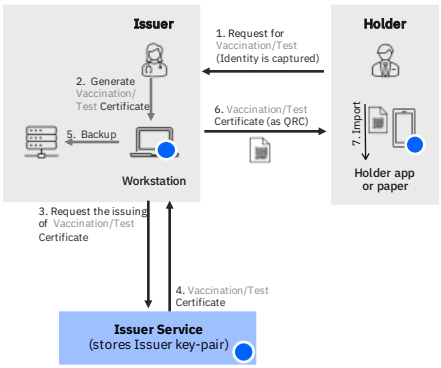

Figure 6: Use of Issuer Service to issue IDHP Health Certificates. The Issuer Service stores the issuer's key-pairs allowing the service to generate Health Certificates upon Issuer request. The Issuer Service stores and leverages Issuer's registration credentials with the trust registry to update the Issuer's issuing public key or CRLs when asked by the Issuer.

disconcerted efforts to enable economic activity and movement of people in the light of ongoing COVID19 pandemic. In the context of interoperability, we require that:

- Health Certificates issued in one IDHP system can be parsed/decoded and verified by other IDHP-based systems;
- IDHP Health Certificates can be parsed/decoded and ultimately verified in the context of external health certificate solutions;
- IDHP Verifier can parse/decode and ultimately verify Health Certificates having originated in external health certificate solutions.

With future interoperability in mind, we implemented IDHP compatible with W3C standards around Decentralized Identity [RSL+19] (used for Issuers) and Verifiable Credentials [SLC19] (used for Health Certificates). This means that IDHP Health Certificates can be parsed by any W3C standard compliant solution. In addition, IBM has open sourced the specifications of the decentralized identifier (DID) used in IDHP as well as a resolver component for that DID as required by the Decentralized Identity Foundation [4], making available all the necessary components for the verification operations of other systems to perform verification of IDHP Health Certificates.

IDHP is also compatible with EU regulation around vaccination and testing certificates [EN21b, EN21a, C21], and can be easily become interoperable with EU Member states systems once APIs of the interoperability bridge called the *trust framework* becomes available.

Finally, because of its integration in a smart-contract enabled distributed ledger system (Hyperledger Fabric), IDHP infrastructure instance can easily upgrade its health certificate structures, e.g., to ones that are more accurately reflecting EU or WHO requirements once specifications of these structures become available or more accurate. In addition, because IDHP is build on Hyperledger Fabric, potential unification of several IDHP instances into a smaller number of them or even a single one would be relatively straightforward, further streamlining interoperability.

References

[ABB+18] E. Androulaki, A. Barger, V. Bortnikov, C. Cachin, K. Christidis, A. D. Caro, D. Enyeart, C. Ferris, G. Laventman, Y. Manevich, S. Muralidharan, C. Murthy, B. Nguyen, M. Sethi, G. Singh, K. Smith, A. Sorniotti, C. Stathakopoulou, M. Vukolic, S. W. Cocco, and J. Yellick. Hyperledger fabric: a distributed operating system for permissioned blockchains. In *Proceedings of the Thirteenth EuroSys Conference, EuroSys 2018, Porto, Portugal, April 23-26, 2018*, 2018.

[AL03] C. Adams and S. Lloyd. *Understanding PKI: concepts, standards, and deployment considerations*. Addison-Wesley Professional, 2003.

[4] `https://identity.foundation`

[C21] E. Commission. Proposal for a regulation of the European Parliament and of the Council on a framework for the issuance, verification and acceptance of interoperable certificates on vaccination, testing and recovery to facilitate free movement during the COVID-19 pandemic (Digital Green Certificate). Technical report, 03 2021.

[D21] DW.com. Coronavirus: Entire class quarantined after Swiss students fake COVID test to cut school, 2021.

[E21] H. Ellyatt. Criminals are selling fake Covid test results as they look to profit from travel restrictions, 2021.

[EN21a] eHealth Network. Guidelines on verifiable vaccination certificates -basic interoperability elements v1.0. Technical report, 03 2021.

[EN21b] eHealth Network. Interoperability of health certificates Trust framework v1.0. Technical report, 03 2021.

[J21] W. S. Journal. In Covid-Era Travel Scam, Fraudsters Offer Fake Test Results, 2021.

[RSL+19] D. Reed, D. Sporny, M. Longley, C. Allen, R. Grant, and M. Sabadello. Decentralized Identifiers (DIDs) v1.0 Technical report. Technical report, W3C, 2019.

[SLC19] M. Sporny, D. Longley, and D. Chadwick. Verifiable Credentials Data Model 1.0 Technical report. Technical report, W3C, 2019.