Interoperability Blueprint Outline (DRAFT)

Collaborative Review Draft 02

March 2021

Table of Contents

Introduction

Public health precautions have helped curb the spread of COVID-19 and saved millions of lives. Yet they have also restricted the ability of individuals to work, study, travel, congregate, and participate meaningfully in the economy. The social and economic impacts are hard to overestimate.

We are all looking for solutions and approaches that would allow us to return to some version of our pre-pandemic lives. **Digital health passes – if properly designed and implemented – could help offer a path to safely restore domestic and international travel, resume public life, and restart the global economy.**

The Good Health Pass Collaborative (GHPC) was launched in February 2021 as an open, inclusive initiative, bringing together the technology, health and travel sectors to collaboratively create a blueprint for interoperable “digital health pass" systems. As vaccines and better testing become available – and we begin planning for an incremental return to “public life” – many governments, airlines, educational institutions, event venues, workplaces and others are considering whether they might require proof of COVID-19 vaccination – or proof of a recent negative test – as a supplement to continued social distancing and masking requirements.

This has sparked multiple efforts – many of which are already underway – to develop digital and paper-based solutions that would enable individuals to provide verifiable proof of their COVID-19 status (and, potentially, that of other future infectious diseases). As these solutions are brought to market, there is a critical need to standardize the mechanisms by which individuals can safely, privately, and appropriately share this information.

When we talk about digital health passes that are “good,” we mean that they align with the principles outlined in the Good Health Collaborative’s first white paper, entitled, ***Good Health Pass: a Safe Path to Global Reopening***. Published in February 2021, the paper outlines the principles that we believe must underpin the development of all digital health pass systems – whether for proof of vaccination or COVID-19 test results. It highlights critical considerations, such as privacy, user-control, choice and consent, trust, inclusivity, interoperability, and social responsibility, among others.

In addition to comporting with the Good Health Pass Collaborative principles, it is vitally important that solutions are designed and implemented in collaboration with healthcare experts, providers, and public health authorities around the world, and that they are reflective of current evidence-based public health guidance.

There are also essential ethical considerations – including where and for what purpose digital health passes are used – which must be addressed to ensure these solutions do not discriminate against disadvantaged groups and can offer an equitable return to public life.

We believe that such fundamental decisions on implementation, adoption, and governance of digital health passes should not be driven by the technology community alone. Rather, it should be the domain of our democratically elected policymakers to establish the circumstances under

which individuals may – and, as importantly, may NOT – be requested or required to provide proof of a recent test or vaccination. As these guidelines are developed, we urge governments and other implementers to work transparently with the broadest range of stakeholders to ensure that equity and inclusion, privacy, fundamental human rights, and civil liberties are protected.

Within this context, and to ensure that digital health passes work for as many people as possible, interoperability is absolutely critical. Yet this goal presents one of the most challenging principles to achieve.

For health passes from different vendors and service providers to meet the needs of the individuals and organizations relying on them, they must be able to work across institutional, jurisdictional and geographic borders, as well as for different modes of transportation. Interoperability will also ensure that institutions – such as airlines and airports (large and small) – can process customers safely and efficiently, while allowing individuals to choose the technology solution that best meets their needs.

This document is the first step towards that interoperability blueprint. It offers a map of the key questions and challenges which must be addressed to produce digital health pass implementations that are both strong and flexible enough to respond to dynamic public health guidance.

Clarifications on Scope

This paper does NOT represent the final set of recommendations from the Collaborative.

These challenges will be addressed through the GHPC drafting groups whose findings will be published in two forthcoming publications; the ***Good Health Pass Interoperability Blueprint,*** and the ***Good Health Pass Governance Framework Recommendations***.

This document does NOT make any public policy recommendations on the adoption of health passes—nor does it make recommendations about the use of COVID-19 vaccinations or testing for international or domestic travel.

That is not the purpose of the Collaborative. Rather, this document highlights the various areas of functionality where – *if* these systems are to be implemented – agreement must be reached to achieve a level of seamless interoperability on a par with other digital document solutions, such as ePassports or mobile boarding passes.

This document will focus on both paper and digital credentials.

Consistent with the Good Health Pass principles, we recognize that there *must* be paper-based (or other non-smartphone) versions of digital health passes to ensure equity, inclusion, accessibility, and enable offline usage and individual choice.

While many of the same interoperability considerations apply to both form factors, paper credentials have their own unique requirements and challenges, and thus we have assigned them their own dedicated workstream (see Challenge #1).

This document will focus primarily on credentials for COVID-19 tests, but will also be applicable to vaccines.

The Good Health Pass Collaborative recognizes the leadership of the World Health Organization (WHO) Smart Vaccination Certificate Working Group and the role that they are playing to develop standards for vaccination certificates, and is working to incorporate their recommendations.

Clarifications on Terminology

In the context of identity document, many use the terms “pass”, “passport” ,“credential”, and “certificate” interchangeably. However, these terms mean different things to different audiences.

For clarity – and to ensure continuity across all of our documentation – we will use the following definitions within the Good Health Pass Collaborative:

Term	Definition (*within the context of the Good Health Pass Collaborative)*
CERTIFICATE	Certificates are a Public Key Infrastructure (PKI) construct– typically issued to organizations– that are digitally signed by a signing authority (or may be self-signed). They follow a strict hierarchical model where each certificate (except the root) is signed by the parent certificate it was derived from, creating a certificate chain. Certificate chains can be verified for cryptographic trust by “walking the chain” back to the root of trust.
CREDENTIAL	Credentials contain attestations – usually made by a third party – about the identity attributes of a particular subject (such as a person). The term “credential” by itself may mean either a: a) paper credential, or b) digital credential. Either form may be verifiable according to various standards. The specific term “verifiable credential” (often abbreviated “VC”) refers to credentials conforming to the W3C Verifiable Credentials Data Model 1.0 standard. This defines the syntax and semantics of a credential so it can be digitally signed by the **issuer** and this proof of authenticity can be cryptographically verified by a **verifier** to ensure the data has not been tampered with. (Note that cryptographic verification alone may not be sufficient – in many cases a verifier may also need to verify that the issuer is trusted under one or more governance frameworks, aka trust frameworks.) Within the Good Health Pass Collaborative, a credential is documentation that a test event or vaccination event occurred. The credential carries with it the attributes, data, or results associated with the event.
PASS	A pass is a specific type of **secondary credential** that carries only the data a verifier requires in a specific context (such as boarding an airplane). A pass may carry attributes from one or more credential(s), from different issuers, as well as data from other sources.
PASSPORT	A passport is an international standard travel document as defined by ICAO. It is usually issued by a country's government to its citizens to certify the identity and nationality of the holder. Passports may contain information such as the holder's name, place and date of birth, photograph, signature, and other relevant identifying information.

IMPORTANT NOTE: The focus of GHPC and the interoperability blueprint is specifically on "credentials" and "passes" as defined above. We do not use the term "vaccine passports" for very specific reasons:

1) **Passports are not available to everyone.** A health credential or pass—in some form—should be available to anyone who wants or needs one.
2) **Passports require very strong identity proofing.** This cannot be a requirement for all COVID-19 testing or vaccinations that are delivered as part of essential public health services, where receiving care is deemed more important than identity verification.
3) **Passport issuers are strictly limited to governments.** A much broader range of issuers need to be able to issue digital health credentials and passes.

In addition to being tightly regulated by governments, the current ePassport system – operated by ICAO – restricts electronic verification of the digital signature on an ePassport to government-authorized border authorities. Others are only permitted to perform manual verification of the paper document. Given the broader scope and usage of health credentials and passes, such a restriction on verifiers does not appear feasible in the context of the Good Health Pass ecosystem.

The Good Health Pass Ecosystem

The stakeholders in globally interoperable health credentials or passes constitute a global **digital trust ecosystem** consisting primarily of four parties:

1. **Issuers** of credentials and passes
2. **Holders** of credentials and passes (in **digital wallets**)
3. **Verifiers** of credentials and passes
4. **Governance authorities** who publish rules and policies in a **governance framework** (aka **trust framework**)

Figure 1 shows the relationships between these four parties in a configuration sometimes referred to as the “trust diamond”.

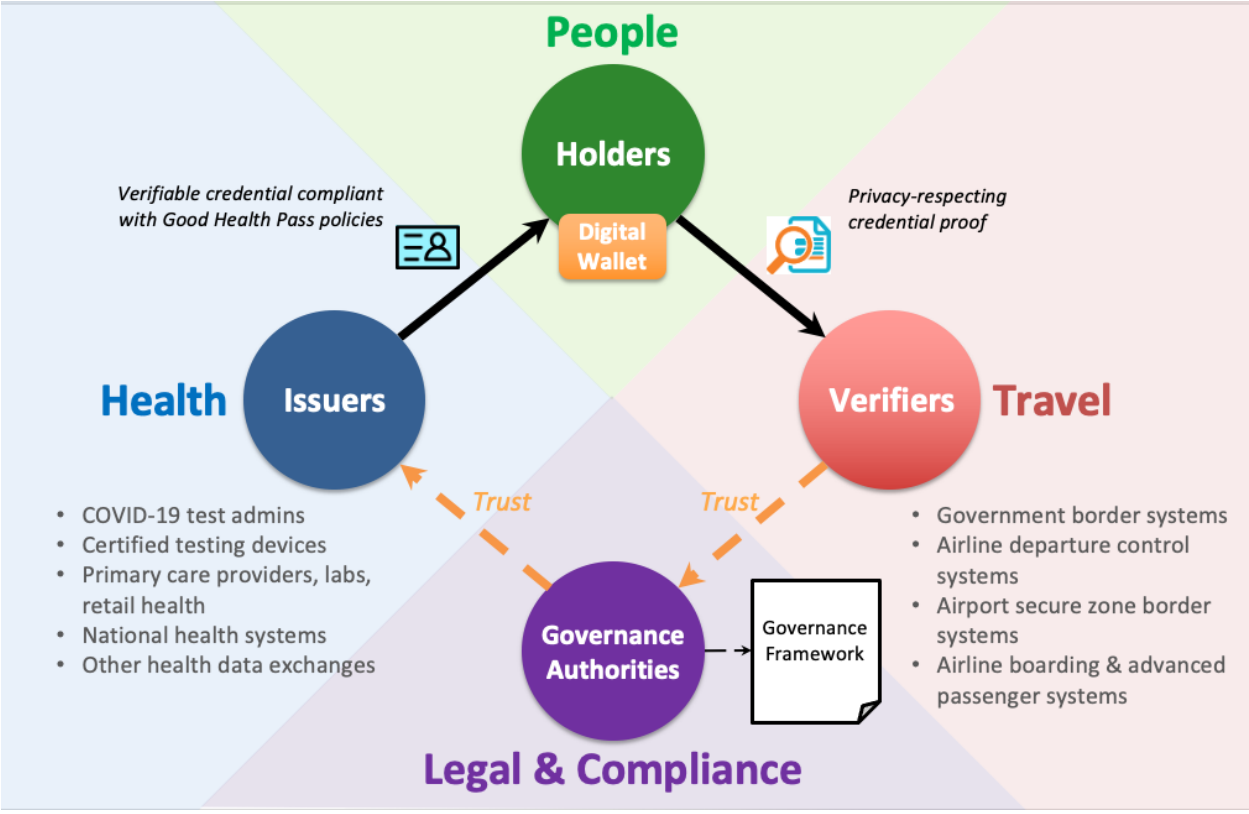


Figure 1: The Good Health Pass Digital Trust Ecosystem

Note that the term “digital trust ecosystem” does not mean that all credentials are in a digital format. As we have already noted, digital health pass systems must support both digital and paper-based credentials.

Given its breadth and scale, the Good Health Pass digital trust ecosystem must also support **any number of solution providers** who compete to offer solutions that meet the needs of participants while adhering to the interoperability requirements the Collaborative is developing.

The Three Zones

From the very start of the Good Health Pass Collaborative, there has a particular focus on one of the most vexing digital identity challenges: **identity binding**.

In the context of health credentials, this is the problem of how a credential describing a specific health event (such as a COVID-19 test or vaccination) can be linked – as strongly as possible – to the identity of the patient who received that care. Ideally, from a security standpoint, this binding is so strong that *only that patient* (or their authorized delegate) can subsequently prove the credential belongs to her/him.

In grappling with this identity binding challenge, the Good Health Pass steering committee found it helpful to break the challenge into the three distinct zones shown in Figure 2:

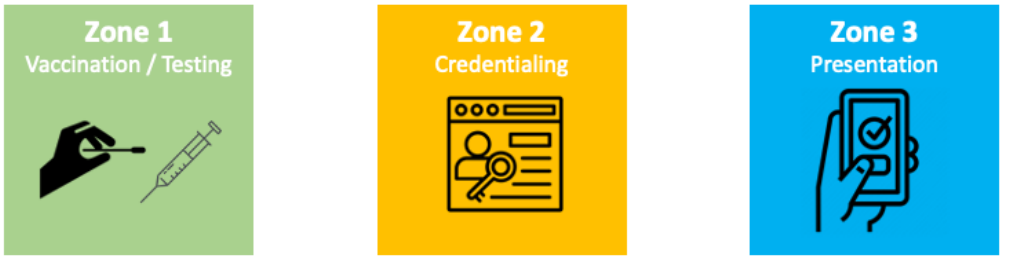


Figure 2: The three zones into which identity binding challenges can be separated

Once you separate the problem space into these three zones, certain conclusions emerge:

1. **Zone 1:** The Good Health Pass interoperability blueprint can make no assumptions at all about what identity binding data is collected at the point of care (if any). This is entirely up to the healthcare provider or other administrator of the test or vaccination.
2. **Zone 2:** The strength of the identity binding that can be achieved at credential issuance may depend completely on what identity binding data was (or was not) collected in Zone 1. However, in some cases, it may be possible to add other assurance in Zone 2.
3. **Zone 3:** No matter how advanced the technology used, the level of identity binding assurance achieved in Zone 3 cannot exceed the level achieved in Zone 2.
4. The further you move identity binding to the **left** (meaning the earlier in the process), the higher the assurance and the lower the risk of fraud. At the same time, it is necessary to consider the tradeoff between increased security and increased friction (or exclusion), and weigh that against the context of the public health risk.

For each of the interoperability challenges outlined in this document, we note the zones to which they are most relevant.

The Eight Key Challenges to Interoperability

1	**Paper Based Credentials**
	Good Health Pass compliant implementations must offer a paper based alternative, based on standard QR code formats and interoperable with their digital counterparts
2	**Consistent User Experience**
	Good Health Pass compliant implementations must use the same conceptual models, core terminology, interaction triggers (e.g., QR codes, deep links), consent models, and certification marks
3	**Standard Data Models and Elements**
	Good Health Pass compliant implementations must collect, process, and transmit a standard set of data elements
4	**Credential Formats, Signatures, and Exchange Protocols**
	Good Health Pass compliant implementations must use a standard set of credential formats, digital signature algorithms, and exchange protocols
5	**Security, Privacy, and Data Protection**
	Good Health Pass compliant implementations must meet baseline security and privacy requirements that enable holders to maintain full control of their personal data
6	**Trust Registries**
	Good Health Pass compliant implementations must be able to quickly and safely verify authorized issuers and verifiers
7	**Rules Engines**
	Good Health Pass compliant implementations should have the option to securely and privately interact with any number of rules engines from any number of governance authorities to accommodate variations in policy and regulations
8	**Identity Binding (Authenticity of the Holder)**
	Good Health Pass compliant implementations must implement standard methods for verifying the authenticity of the holder at specified levels of assurance

Challenge #1: Paper Based Credentials

An all-digital solution to health passes is simply not an option when it comes to combating a public health crisis. Simple, easy-to-use paper credentials **must** be an option so those in low-resource settings or those who do not own – or wish to use – a mobile phone are not excluded.

However paper credentials have numerous challenges when it comes to identity binding, including the potential for fraud and counterfeiting. Like digital credentials, they need to be verifiable as authentic, unaltered, and issued by an authorized issuer. And they need to include at least enough identity binding data so they can be manually verified against an individual's other identity documents (if available).

One solution is a printed QR code that can transmit a digitally signed credential payload. However such a solution comes with its own set of challenges, including:

- QR codes have different types and size limits (most are between 300 - 500 bytes); many QR readers start having problems (e.g., scanner crash) above 500 bytes.
- Different QR codes require different scanner capabilities.
- The specification – and order of operations – for data compression matters.

Many of the challenges described in this paper apply equally to both paper and digital credentials. Thus, the primary goal of this Good Health Pass Collaborative workstream is to enable implementations to produce paper credentials that are interoperable with – and contain as many benefits of – their digital counterparts as possible.

Zones Involved with Paper Based Credentials

Key Interoperability Questions That Must Be Answered

1. Which paper credential **format** or **formats** will digital health pass systems support?
2. Will paper credentials be compliant with the W3C Verifiable Credentials Data Model 1.0 specification?
3. Will paper credentials require a digital signature to be included? Which signature formats will Good Health Pass systems support?
4. Should the same privacy policies be applied to paper credentials, such as data minimization and disclosure limited to what is strictly required?
5. How will these digital QR codes relate to the QR codes for paper credentials?
6. Is there a need to turn a paper credential into a digital credential, and vice versa?
7. What considerations need to be made for smart cards?
8. How will interoperability between these choices be **tested/verified/certified**?

Challenge #2: Consistent User Experience

The Good Health Pass Collaborative was established, in part, to avoid a scenario in which people are faced with a mess of confusing, conflicting, overlapping requirements for how they can prove their COVID-19 status. Such fragmentation would not only introduce tremendous friction to the travel experience, but would also impede adoption, erode confidence, and hinder equitable economic and societal rebuilding.

The need to create a consistent user experience – based on a model of universal acceptance – is the most fundamental interoperability challenge we must meet. In short, a Good Health Pass-compliant digital health pass must be easy to obtain, use, and update, without any special user knowledge.

A consistent UX includes four key dimensions:

- **A consistent mental model** that reflects a natural, intuitive process for using either paper or digital credentials. As with the introduction of mobile boarding passes over the last decade, the use of verifiable credentials should be immediately adaptable to everyday processes and workflows, such as booking a flight, boarding a plane, crossing a border, etc.
- **Consistent terminology** (semantic interoperability) such that required data elements are collected accurately and user interface artifacts are presented consistently with meanings that are understood universally across all systems – the same way a red stop sign is universally recognized, regardless of language.
- **Consistent user ceremonies** – just as driving a car requires unlocking it, fastening the seat belt, starting it, putting it in gear, and using the accelerator and brakes, we need to agree on generally consistent “ceremonies” for travellers, whether they are using a general-purpose digital wallet or a special-purpose application. This includes setup, security and privacy warnings, consent and user rights management, backup and recovery, and compatibility with paper credentials.
- **Consistent governance** that is responsive to global, national, and regional regulations or operational parameters (e.g, for when a test has expired, etc.) and is adaptable to change.

User Experience Journey Map in Brief

A good user experience with intuitive user ceremonies is built on a “journey map” that describes the sequence of events in a typical usage scenario, such as purchasing a product on a website or taking a trip. The following is a brief overview of user experience, with details to be articulated in the final recommendation document:

1. The user plans to receive a service which, for reasons of public and personal health, requires COVID-19 risk mitigation – via testing and/or vaccination – and determines the related requirements. *For the purposes of the Good Health Pass Collaborative, we will focus on the travel use case.*
2. The user obtains a physical and/or digital identity document (or agreed equivalent in that

jurisdiction)

3. The user obtains a COVID-19 test – or vaccination – from an accredited health service provider.
4. The user obtains the necessary COVID-19 status credential from the provider after the user's identity is authenticated (note that this may be at same time as receiving service or at some time subsequent). *Note: this must allow for mitigation if the credential is issued in error or if the user disagrees with their health status determination.*
5. At an authorized verification point(s), the user is requested to provide proof of one or more COVID-19 status credentials in a compatible format and they consent to provide such a proof.
6. The authorized verifier is able to verify that the COVID-19 status credential(s) are: (1) authentic and unaltered, (2) bound to the identity of the presenter, and (3) satisfy the verifier's policy requirements.

Determining Health Pass Requirements

There will be a variety of state, regional, provincial, and national rules and policies that will govern when, where, and under what circumstances an individual might need to provide a proof of COVID-19 status. These policies may also specify what data needs to be verified and what levels of assurance are necessary for a given purpose (travel, return to work, return to school, etc.).

To help users – and, in some cases, verifiers – deal with the wide range of applicable policies, some health pass applications may need to invoke a rules engine to determine:

1. What Identity documentation is required (if any)?
2. What test and/or vaccination (and what metadata) is required?
3. What labs (or on-site medical devices) or health service providers are approved, based on the service(s) sought?
4. What are the requirements to register for – and obtain – services from approved labs or health service providers?
5. How long will the credential remain valid?
6. How can credentials be challenged or revoked?
7. How can credentials be renewed or re-issued (in case of loss or data corruption)?

Regardless of the use case, each of these questions must take into account equity (i.e., ensuring requirements do not exclude certain populations).

Additionally, these requirements will depend on emerging and evolving scientific understanding of the COVID-19 virus, as well as policies that may govern the use of credentials in general (e.g., timebound use of credentials only while COVID-19 is still designated a pandemic by the World Health Organization).

Provisioning of Strong Identity Documents

For some scenarios in which a health pass may be used, we expect individuals will need to have – or obtain – identity documents commensurate with identity assurance standards, such as NIST Special Publication 800-63A Identity Assurance Level or ISO/IEC TS 29003:2018 International Standard for identity proofing, as required by the countr(ies) and/or service provider(s) involved.[1]

As an example, for international travel, we expect that ICAO-compliant Machine Readable Travel Documents (MRTDs) such as passports, will be required. MRTD issuance follows ICAO guidelines for Evidence of Identity to gain confidence that:

a. The claimed identity is genuine (i.e. valid, not fictitious, and still living);
b. The presenter links to the identity (i.e. the identity is unique within the authority's system and the presenter is the sole claimant); and
c. The presenter uses the claimed identity in the community.[2]

Electronic MRTDs, such as ePassports, include cryptographic capabilities that enable electronic document authentication[3] in addition to optical / visual and source document authentication (e.g., checking a driver's license against the motor vehicle registry).

Obtaining a COVID-19 Test or Vaccination (Zone 1)

Ensuring that individuals can obtain COVID-19 tests or vaccinations in the safest, most efficient, and most equitable way possible must be a priority for the Good Health Pass ecosystem. This is why there have been many approaches to defining and binding an individual's identity to a test or vaccination. In fact, some systems have forgone formal identity verification, relying on self-attestation to ensure inclusivity and increase operational efficiency.

This underscores the need to create a user journey that is consistent enough for a credentialing process, but dynamic enough to minimize operational disruptions or barriers to health services. See Challenge #8 (Identity Binding) for more details.

---

[1] Outside of the travel use case, requiring identity documents in order to obtain health passes will be challenging - if not impossible - for many individuals. For use cases beyond travel - particularly those where identity verification is not already part of a given process - countries and organizations will need to weigh the impact on excluded persons—those without documents, with disabilities, or with outdated or shared devices. They must also consider gender equity.

[2] https://www.icao.int/Security/FAL/TRIP/Documents/ICAO Guidance on Evidence of Identity.pdf

[3] Electronic document authentication of an ePassport is performed via ICAO's Public Key Directory (PKD) which at present is only available to border control authorities.

Obtaining the COVID-19 Status Credential (Zone 2)

The Good Health Pass ecosystem should enable an individual who has received a test and/or vaccination to receive a credential (either digital or paper) using a range of mechanisms, including paper printouts, electronic health records (EHR), or via a QR code or secure Web link, or another appropriate form factor.

Depending on the timing and method of issuance of the credential, this step may require the individual to re-authenticate to the issuer in order to assure that the credential is bound to the individual's identity. For details, see Challenge #8 (Identity Binding).

Presenting the COVID-19 Status Credential (Zone 3)

So far the journey map has resulted in the issuance of a COVID-19 status credential bound to an individual's identity.

The final step in the user journey is the **presentation** of that credential to a **verifier** who needs to make a trust decision**.** The verifier must first **verify** the digital signature on the credential and secondly **validate** that the credential meets their legal and/or business requirements. Verification and validation rules are subject to temporal, legal, and business considerations.

There are two primary options for credential verification and validation:

1. **First-party rules enforcement**: This applies when a credential is presented, verified, and validated according to the rules of a governance authority using a published governance framework of some kind (including governmental legislation). For example, a US-based hospital or clinic may provide a COVID-19 test and then issue a credential based on requirements established by the Centers for Disease Control and Prevention (CDC). The US Transportation Security Administration (TSA) may then verify and validate this CDC-governed credential at the point of departure.
2. **Third-party rules enforcement**: This applies when a credential is presented, verified and validated by a rules engine operated by a third party. Such a service may aggregate rules from multiple governance frameworks. For example, a travel app might accept a travel itinerary as input, consult the rules engine, and return the COVID-19 test and/or vaccination requirements for that trip. Once a passenger has obtained the COVID-19 status credential(s) necessary to meet these requirements, the rules engine may then issue a secondary credential – a travel pass – that the traveller can use for that journey.

To meaningfully benefit global travel, credential presentation must be as lightweight, frictionless, and intuitive as possible. Typical presentation options include:

1. **QR codes** can be produced on paper or by a mobile device and then read by a QR code reader for verification exactly like a mobile boarding pass.
2. **Near Field Communications (NFC)** can be used by a mobile wallet to transmit the credential to the verifier.
3. **In-app** verification can be performed when a credential or pass is ingested and verified by an app designed to provide that function (e.g. an airline trip management app).

Zones Involved with Consistent User Experience

Key Interoperability Questions That Must Be Answered

1. How are credentials translated into QR codes – and with what required functionality – to meet the Good Health Pass functional requirements?
2. What needs to be encoded in these QR codes?
3. What is the standard set of user-facing terminology and iconography that all good health pass apps should use to ensure consistent user experience?
4. What is the standard set of options for presentation of a digital health pass that compliant apps and verifiers will support?
5. What is the standard user ceremony for providing consent for sharing of a digital health pass?
6. Should “self-attestation” credentials issued by a user to themselves – based on a home test result or inadvertent lack of formal records – be allowed?

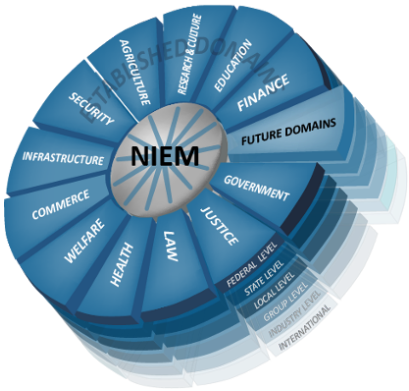
Challenge #3: Standard Data Models and Elements

As with passports and payment cards, fully interoperable digital health pass systems need a **common data model,** specifying standard data elements and supported by specific **data schemas** in specific implementations. Work in this area is currently ongoing across several cross-industry efforts.

One such effort is the Linux Foundation Public Health (LFPH) COVID-19 Credentials Initiative (CCI), which has established a task force to develop **schema specifications, Codes of Practice, technical guidelines, JavaScript Object Notation (JSON) code**, and related components. This includes the eHealth Network's Vaccination Proof Interoperability Guidelines.

The CCI task force is also seeking to collaborate with others in this space, including the CDC, the W3C Credentials Community Group, the EU vaccination group, C4 Credentials, IATA, ICAO, public health authorities, private health vendors and consortiums, electronic health record (EHR) providers, the UK National Health Service, pharma companies, major pharmacy chains (US), the FHIR Focus Group at the ToIP Foundation, and the Vaccination Credentials Initiative (VCI).

One example of a data model that enables efficient information exchange across diverse public and private organizations is the U.S. National Information Exchange Model (NIEM). NIEM provides rules and methodologies around the use of the model as well as a standardized Information Exchange Development Lifecycle that can be reused by everyone. NIEM also offers governance, training, tools, technical assistance, and an engaged community to support users and organizations in adopting NIEM.



To emphasize, this is just one example of the kind of approach that the Good Health Pass Collaborative could take to accommodate data requirements of different countries and jurisdictions around the world.

Zones Involved with Standard Data Models and Elements

Key Interoperability Questions That Must Be Answered

1. What are the minimal ***required*** elements for Good Health Pass schemas?
2. What are the ***optional***, country-specific elements for Good Health Pass schemas?
3. Is there a data model that will enable both interoperability and adaptability of data elements to different implementations, jurisdictions, and governance authorities?
4. How does the data model support identity binding (e.g., describing levels of assurance)? (See Challenge #8)

Challenge #4: Credential Formats, Signatures, and Exchange Protocols

The primary challenge in designing interoperabile digital credentials of *any* kind is how to standardize the **container** for the data — together with the **digital signature** on the container from the issuer — so that the data inside the container can be trusted by verifiers (and also so it can interoperate across multiple digital wallet implementations).

This standardization challenge was first recognized by the W3C Credentials Community Group in 2015, which incubated the early work that culminated in the establishment of the W3C Verifiable Claims Working Group in 2017. The final approval of the W3C Verifiable Credentials Data Model 1.0 specification followed in September 2019.

There is now strong market momentum toward production usage of verifiable credentials compliant with this W3C standard. This, together with the security, privacy, and data control benefits of decentralized identity architecture, have made W3C verifiable credentials the default choice of the Good Health Pass Collaborative.[4]

It is, however, important to note that: a) the W3C verifiable credential standard supports several different data container formats as well as multiple digital signature options, and b) the W3C standard does **not** standardize credential presentation and exchange protocols (which were explicitly out of scope for the W3C Working Group charter but were, rather, left for industry to innovate).

Therefore, to achieve global interoperability of Good Health Pass credential implementations, it is necessary to agree on:

1. **The credential data format(s)** (ideally just one).
2. **The credential digital signature suite(s)** (ideally just one).
3. **The credential presentation and exchange protocol(s)** (ideally just one).
4. The **credential revocation mechanism(s)** (ideally just one) for credentials that must be revocable.

Why in each case do we say, “ideally just one”? Because, in the words of Brian Behlendorf, GM of Blockchain, Healthcare, and Identity at the Linux Foundation, “Optionality is never free—it comes at the cost of combinatorial complexity for all implementers.” This cost is redoubled when security and privacy considerations are paramount.

[4] For more background, see this CCI report: https://www.lfph.io/wp-content/uploads/2021/03/CCI-Paper-Based-VC-Summit-Summary-Report.pdf

There are many other considerations that go into making these choices, including:

- Performance requirements at airports, airlines, and other travel industry verifiers where reducing travel friction is of critical importance,
- Offline verification requirements in some locales (e.g., no Internet, loss of power, etc.),
- Meeting regulatory requirements for security and privacy,
- Ease of integration with existing systems and solutions, especially legacy travel reservation, security, and check-in systems and procedures,
- Cost and availability

In short, this is one of the most difficult sets of choices that Good Health Pass collaborators must make. Thankfully, excellent work is already being done in this area.

In February 2021, the COVID-19 Credential Initiative (CCI) hosted by Linux Foundation Public Health published a paper by CCI Ecosystem Director Kaliya Young titled Verifiable Credentials Flavors Explained. It explains the differences between the major credential data formats and digital signature algorithm choices (JWT, JSON-LD with LD Signatures, ZKP-CL, JSON-LD with ZKP BBS+). CCI is also currently working on a paper, analyzing the differences between the major credential presentation and exchange protocols, including DIDComm, the Aries Protocol suite, DIF Presentation Exchange, OpenID Self-Issued OpenID Provider (SIOP), and Web/REST using the Credential Handler API (CHAPI).

Zones Involved with Credential Formats, Signatures, and Protocols

Key Interoperability Questions That Must Be Answered

1. Which verifiable credential **format** – or **formats** – compliant with the W3C Verifiable Credentials Data Model 1.0 specification will Good Health Pass systems support?
2. Which verifiable credential **signature suite** – or **suites** – compliant with the W3C Verifiable Credentials Data Model 1.0 specification will Good Health Pass systems support?
3. What verifiable credential **presentation and exchange protocol** or **protocols** will Good Health Pass systems support?
4. What are the requirements for credential **revocation**, and how will it be handled so that it is interoperable?
5. How will interoperability with these choices be **tested/verified/certified**?
6. How will decisions be made if/when additional formats, signature suites, and/or presentation and exchange protocols are developed?
7. How will credentials that don't comply with the W3C model be addressed?

Challenge #5: Security, Privacy, and Data Protection

All stakeholders in the Good Health Pass Collaborative digital trust ecosystem need to be confident in the security and privacy protections that the ecosystem enforces. In some jurisdictions, these protections are already required by existing data protection regulations; in other cases, governance authorities may seek to pass new legislation to enshrine them in law.

To be consistent with the Good Health Pass principles, it is anticipated that Good Health Pass solutions will need to be built on a decentralized identity architecture that places an emphasis on privacy and personal data control. Such systems seek to put the user in control of their personal identity data – including health attributes – which they can selectively disclose for a specified purpose and duration. Such systems stand in contrast to centralized models, which amass and store large amounts of personal data that is under the primary control of the aggregator.

For Good Health Pass systems, the issuance, holding, presentation, and verification of digital health credentials must – at a minimum – comply with applicable regulations requiring:

- **Privacy by Design and Default**
  - Non-linkable transactions: to prevent unintentional correlation of the holder
  - Data minimization: to enable selective disclosure of only the data strictly required by a verifier
  - Zero-knowledge proofs: privacy-preserving cryptography that supports selective disclosure
  - Privacy-preserving protocols: to help ensure that a user is not tracked when presenting their credentials
  - Transparency: to provide sufficient information to the holder about the processing of their personal data
  - Purpose limitation: to collect personal data for specified, explicit and legitimate purposes and not process it in a manner incompatible with those purposes
  - Auditable and informed consent (or delegation of consent)
- **Security by Design and Default**
  - Secure transmission of verifiable credentials
  - Secure storage of verifiable credentials (e.g, cloud- or edge-based wallet)
  - Secure issuance of verifiable credentials
  - Secure verification of verifiable credentials

Of particular importance with digital health credentials are *privacy-preserving identifiers*. This topic is discussed at length in the W3C Decentralized Identifiers (DIDs) Core 1.0 Specification. Specific DID methods support privacy-preserving identifiers that can provide the benefits of cryptographic verifiability without correlatability.

Zones Involved with Security, Privacy, and Data Protection

Key Interoperability Questions That Must Be Answered

1. Which local, regional, national, and international security standards apply?
    - ISO/IEC JTC1/SC 27 Information security, cybersecurity and privacy protection
    - ISO/IEC JTC1/SC 17 Cards and security devices for personal identification
    - ITU-T Study Group 13 - Future networks, with focus on IMT-2020, cloud computing and trusted network infrastructure
    - Others such as SOC 2 Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality or Privacy

2. Which privacy laws and regulations apply?
    - GDPR?
    - CCPA?
    - HIPAA?
    - Other?

3. Where should Good Health Pass compliant apps and systems mandate the use of privacy-preserving identifiers?

4. How do you prove that a specific Good Health Pass solution meets the security & privacy requirements?
    - Testing standards?
    - Self-test/self-attestation?
    - Third-party accreditations or certifications?
    - Open challenges to find vulnerabilities?
    - Data Protection Impact Assessments?
    - Privacy compliance assurance programs?

Challenge #6: Trust Registries

The sheer scale of the Good Health Pass digital trust ecosystem makes one challenge inherently obvious: how are verifiers supposed to determine – within seconds – that a Good Health Pass compliant credential or pass was issued by an authorized issuer?

The technical aspect of this problem – verification of a digital signature – is relatively easy (it is in scope for Challenge #4). The hard part is how to establish actual **transitive trust**, i.e., how a verifier can determine that a specific issuer is following the policies of a governance framework (aka trust framework) that the verifier trusts.

The term "trust registry" is not intended to suggest a specific solution to this problem. Rather, we use the term to suggest that – at the scale of the Good Health Pass digital trust ecosystem – some mechanism(s) will be required for verifiers to make this trust decision. Such a mechanism could be centralized, federated, or decentralized – or any combination that solves the problem.

The primary challenge of a centralized trust registry, operated by a single governance authority, is that it requires the trust of all verifiers. While this may be possible with a subset of verifiers in the Good Health Pass ecosystem, it is unlikely to work for all verifiers. However, a reasonably constrained set of centralized trust registries that collectively serve all verifiers might work.

Federated trust registries are another solution commonly used for PKI certificate chains. A root certificate authority (CA) self-signs its own digital certificate together with the certificates of its delegates. They, in turn sign the certificates of their delegates, and so on. Verifiers "walk the chain" back of digital certificates back to a root CA they trust. The World Health Organization has already indicated it intends to implement a federated public key directory (PKD) for its Smart Vaccination Certificates (SVCs).

Decentralized trust registries are a well-known solution in decentralized digital trust architectures. They are a particular focus of the Governance Stack Working Group (GSWG) at the Trust Over IP (ToIP) Foundation. The draft ToIP Governance Architecture specification recommends the use of trust registries that leverage decentralized identifiers (DIDs) based on the W3C DID Core 1.0 Specification. DIDs are cryptographically verifiable, globally unique identifiers that can be generated directly by an individual or organization for their own use and do not require the use of a centralized registry provider.

If authorized Good Health Pass credential issuers and verifiers have their own public DIDs, registered on an authorized verifiable data registry, DID-based trust registries can be implemented in several different configurations:

1. **Simple DID trust registries** are lists of the DIDs the issuers and verifiers authorized by a particular governance authority. They may be hosted on any suitable verifiable data registry designed by that governance authority.
2. **Federated DID trust registries** work the same way as conventional federated PKI registries, except that they use DIDs instead of digital certificates. Verifiers can walk the

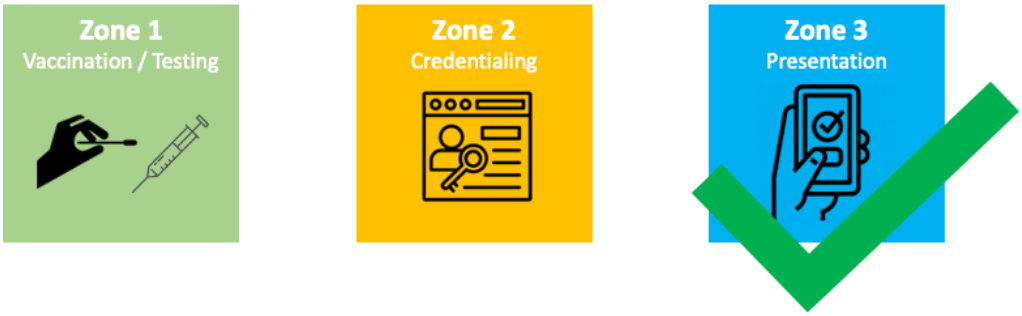
path of DIDs to the root DID of a governance authority they trust.

3. **DID web-of-trust registries** are a combination of simple DID trust registries and/or federated DID trust registries that have mutually-verifiable trust relationships ("cross-registrations"). Thus, they do not need to be organized into a specific hierarchy.

Any of these configurations can be optimized for different kinds of access and performance, including policies for replication and caching.

In addition, DID trust registries can be made searchable by implementing them as *credential registries*. In this case, governance authorities issue verifiable credentials describing the DID of each authorized issuer and verifier directly to the credential registry as the holder. The credential registry software then automatically creates a searchable directory consisting entirely of cryptographically verifiable data. For an example of a full production credential registry, see the OrgBook service from the Province of British Columbia which offers a searchable index of all legally-registered businesses in the Province.

Zones Involved with Trust Registries



Key Interoperability Questions That Must Be Answered

1. Is there a way to establish transitive trust between different subsets of the Good Health Pass digital trust ecosystem that can still result in global interoperability?
2. If so, what is the recommended technical architecture to support this solution or solutions?
3. How should this be reflected in the Good Health Pass Ecosystem Governance Framework and in any delegated governance frameworks?

Challenge #7: Rules Engines

As we explained in Challenge #2, the Good Health Pass ecosystem needs to provide a seamless and frictionless user experience. However, the Collaborative recognizes that in addition to variations in testing and vaccination procedures and data collection in different localities around the world, there will also be many variations in the rules and policies governing what tests and/or vaccinations are required where and for what purposes.

Making these rules and policies accessible to issuers, holders, and verifiers of Good Health Pass credentials may require the services of any number of *rules engines*. A rules engine is a network-accessible service that can be sent a machine-readable query (such as a flight itinerary) for evaluation. The rules engine determines the rules applicable to the query and then evaluates those rules to return a response (such as what COVID-19 tests and/or vaccinations required to complete that particular itinerary). A Good Health Pass implementation can then use that response to instruct the traveller.

Examples of rules engines include TravelDoc (ICTS) and the Timatic service, the latter of which is operated by the International Air Transport Association (IATA). The IATA Travel Pass app, for example, enables a user to input their itinerary and receive back an analysis of the visas, COVID-19 status credentials, and other travel restrictions or travel advisories that are necessary – or advised – for that itinerary.

In some cases, under some trust/governance frameworks, a rules engine could first serve as a verifier of Good Health Pass **credentials** from authorized issuers and then as an issuer of a **pass** as a secondary credential to the traveller. This pass would be the only credential the traveller actually needs to present in a specific context (such as to board a plane). Conceptually, this is very similar to an airline agent checking all of your travel documents before issuing you a boarding pass, which is then the only credential needed to board the plane.

As noted in Challenge #2, however, such a secondary credential is typically accepted only by a particular verifier, for a particular purpose, and for a particular time period.

As with trust registries, rules engines can be deployed in a centralized model (a single, global database to provide all rules and reconciliations of conditions), a federated model (where one general rules engine delegates to other more specialized rules engines serving specific geographies or governance authorities), or a distributed model (a decentralized network of rules engine “nodes” that determine “consensus” based on multiple inputs).

To preserve privacy, rules engines in the Good Health Pass ecosystem should operate without the traveller needing to provide personal data whenever possible. In most cases, a rules engine does not need that information to provide prescriptive information (e.g., a border is closed, or a test is no longer accepted) or conditional evaluations, based on non-personally identifiable data elements in a query (for example “test=negative AND less than 72 hours PLUS vaccine=true”).

Zones Involved with Rules Engines

Key Interoperability Questions That Must Be Answered

1. How many governance authorities will need to define their own rule sets?
2. Will rules engines be specific to geographies? Industries? Platforms?
3. How will government authorities indicate their entities, places, or devices are authorized to issue test or vaccination certificates?
4. How will rules be expressed such that they are semantically understandable to a rules engine?
5. Will rules expression be standardized across GHP-compliant rules engines?
6. How will developers and their applications be authorized to access rule sets and rules engines?
7. Will a downloadable rules engine or SDK be made available?

Challenge #8: Identity Binding

The final interoperability challenge is the one we described earlier in the paper about how a Good Health Pass compliant credential can be “bound” to the individual it describes (i.e., to the person who has received a COVID-19 test or vaccination) – and how, then, can that person subsequently prove that they are, indeed, the individual bound to that credential (**authentication**). The three zones involved with this challenge are repeated here for convenience:

Identity binding data may or may not be collected at the point of care depending on the circumstances

Identity authentication is performed by the issuer to bind the holder’s identity to the verifiable credential

Identity authentication is performed by the verifier to confirm that the credential holder is the bound identity

This challenge may seem trivial for the credentials we typically carry in our wallet or purse to identify ourselves (e.g., driving licenses or passports). That is because we go through an elaborate in-person **identity proofing** process to obtain those credentials. As a result, those credentials end up carrying a great deal of personal data (name, address, birthdate, hair color, eye color) including biometric data (picture, fingerprint, facial scan) that has been verified face-to-face.

This rich set of identity data on a printed credential makes authentication relatively easy when done in person (such as passing through an airport security checkpoint). However:

1. It can be difficult or impossible to use that same information to authenticate an individual remotely, over a digital connection (such as using a website or a smartphone application).
2. Aggregating all of this identifying information in a digital credential creates an unnecessary privacy risk vector if that information is not actually needed to perform adequate authentication.
3. Many individuals in the world – over 1 billion—do not have access to these forms of strong identity documents – or even any form of legally-recognized identity at all.

Furthermore, in the Good Health Pass ecosystem, identity binding is inherently more challenging because many health authorities cannot mandate an in-person identity authentication process – let alone a rigorously secure one – prior to administering a COVID-19 test or vaccination. In fact, some health authorities have rejected, on ethical grounds, any requirement for proof of identity as a prerequisite for receiving a test or vaccination.

Thus, specific identity binding challenges must be solved in each of the three zones:

1. **In Zone 1**, the Good Health Pass ecosystem must be able to accommodate the complete spectrum of identity binding strength – from no identity binding at all (e.g., giving a free COVID-19 test to a refugee) to a patient with full biometrics and an extensive EHR at a modern hospital. The strength of this initial binding can be described by assigning the **level of assurance** (LOA). Levels of assurance are described in various national and international standards documents including: 1) ISO/IEC 29115, 2) Pan-Canadian Trust Framework, 3) eIDAS, and 4) the NIST 800-63 series. The latter establishes some of the most widely referenced standards for LOA for identity proofing, including the Identity Assurance Level (IAL) as described in NIST-800-63A and the Authenticator Assurance Level (AAL) described in NIST-800-63B.
2. **In Zone 2**, Good Health Pass credential issuers must perform identity authentication of the holder to a sufficient LOA prior to issuance of the credential. The LOA achieved should also be described in the issued credential itself.
3. **In Zone 3**, Good Health Pass credential verifiers determine the LOA to which they require identity authentication of the holder at the time the credential is presented. The verifier can use this LOA, together with the issuance LOA, to apply its own policies (or the policies of the trust or governance framework under which it is operating) to determine the trust to place in the credential.

While many specialized technologies (such as biometric authentication) and business processes (such as identity proofing training) exist to provide higher levels of assurance, they are not always needed or used in healthcare delivery, which means some of these tools may be difficult, if not impossible, to implement. Thus, the Good Health Pass ecosystem must support:

- Low-tech or no-tech identity binding solutions alongside high-tech means.
- Remote or self-administered testing to provide the greatest impact and reach.
- Healthcare data systems that are not designed for the purpose of supporting a health credential service.

In short, Good Health Pass compliant credentials must be able to describe any level of identity proofing at the time of testing – from none to fully verified biometrics.

Zones Involved with Identity Binding

Key Interoperability Questions That Must Be Answered

1. What types of identity bindings should be standardized in the Good Health Pass ecosystem?
2. What IAL is required for the individual's identity document(s) presented to the health service provider?
3. What AAL is required to bind the individual's identity to the identity document(s) presented to the health provider for issuance of a Good Health Pass credential?
4. What IAL is required for the identity document(s) the individual presents to the verifier of a Good Health Pass credential (e.g., airline, border, school, employer)?
5. What AAL is required to bind the individual's identity to the identity document(s) presented to the verifier?
6. How should identity binding for paper credentials relate to identity binding for digital credentials?

The Good Health Pass Ecosystem Governance Framework

Interoperable digital trust infrastructure requires more than just technology. It requires that the members of a digital trust ecosystem agree on the business, legal, and social rules, and policies they will follow to achieve their trust objectives. This collection of rules and policies is called either a *trust framework* or a *governance framework* (the former term is used most often in federated identity systems and the latter in decentralized identity infrastructure).

As the Collaborative completes its recommendations for each of the interoperability challenges covered in this paper, those recommendations will be formulated into policies incorporated into the **Good Health Pass Ecosystem Governance Framework**. This will be a ToIP Layer 4 ecosystem governance framework developed according to the ToIP governance metamodel defined by the Governance Stack Working Group at the Trust over IP Foundation. Development of this ecosystem governance framework will follow best practices curated by the Ecosystem Foundry Working Group.

Specific Good Health Pass-compliant implementations may then publish their own ecosystem governance frameworks, localizing the policies of the Good Health Pass Ecosystem Governance Framework to reflect the requirements of their specific jurisdiction, market segment, or trust community. This is a key method by which together we can build a globally interoperable Good Health Pass *ecosystem of ecosystems*.

Appendix A: UK Royal Society's 12 Challenges for Vaccine Passports

On 19 February 2021, the SET-C (Science in Emergencies Tasking: COVID-19) group at the UK Royal Society published a report outlining the 12 criteria that should be satisfied to deliver an effective "vaccine passport". This table maps those 12 tests to the challenges in this paper.

Royal Society Challenge	Good Health Pass (GHP) Interoperability Challenge
Meet benchmarks for COVID-19 immunity	• #3: Standard Data Models and Elements • GHP Ecosystem Governance Framework
Accommodate differences between vaccines in their efficacy, and changes in vaccine efficacy against emerging variants	• #3: Standard Data Models and Elements • #7: Rules Engines • GHP Ecosystem Governance Framework
Be internationally standardised	• #3: Standard Data Models and Elements • #4: Credential Formats, Signatures, Protocols
Have verifiable credentials	• #4: Credential Formats, Signatures, Protocols
Have defined uses	• #2: Consistent User Experience
Be based on a platform of interoperable technologies	• #4: Credential Formats, Signatures, Protocols
Be secure for personal data	• #5: Security, Privacy, and Data Protection • #8: Identity Binding
Be portable	• #1: Paper Based Credentials • #4: Credential Formats, Signatures, Protocols • #8: Identity Binding
Be affordable to individuals and governments	• #1: Paper Based Credentials • GHP Ecosystem Governance Framework
Meet legal standards	• #5: Security, Privacy, and Data Protection • #6: Trust Registries • #7: Rules Engines • GHP Ecosystem Governance Framework
Meet ethical standards	• #5: Security, Privacy, and Data Protection • #7: Rules Engines • GHP Ecosystem Governance Framework
Have conditions of use that are understood and accepted by the passport [pass] holders	• #1: Paper Based Credentials • #2: Consistent User Experience • #5: Security, Privacy, and Data Protection • GHP Ecosystem Governance Framework