The Good Health Pass Interoperability Blueprint

Table of Contents

Notices

The Trust over IP Foundation's Interoperability Working Group for Good Health Pass (the "Project") would like to receive input, contributions, suggestions and other feedback ("Contributions") on the specifications, documents, source code, data, and other artifacts being developed within its working groups (the "Materials"). By signing below, you (on behalf of yourself if you are an individual and your company if you are providing Contributions on behalf of the company) grant the Project under all applicable intellectual property rights owned or Controlled by you or your company a non-exclusive, non-transferable, worldwide, perpetual, irrevocable, royalty-free license to use, disclose, copy, publish, license, modify, sublicense or otherwise distribute and exploit Contributions you provide for the purpose of developing and promoting the Materials and in connection with any product that implements and complies with the Materials. You warrant to the best of your knowledge that you have rights to provide these Contributions, and if you are providing Contributions on behalf of a company, you warrant that you have the rights to provide Contributions on behalf of your company. You also acknowledge that the Project is not required to incorporate your Contributions into any version of the Materials. You further agree that you and your company will not disclose it or distribute drafts of the non-public Project Materials to third parties. Unless the parties agree otherwise or the Project Materials are made publicly available by the Project, this obligation of non-disclosure will expire five (5) years from the date the material was disclosed to you.

Source Code
Any source code you provide to the Project is subject to the Developer Certificate of Origin version 1.1, available at http://developercertificate.org/ and the license indicated in the Project's source repository for the Materials.

Copyright Notice

THESE MATERIALS ARE PROVIDED "AS IS." The parties expressly disclaim any warranties (express, implied, or otherwise), including implied warranties of merchantability, non-infringement, fitness for a particular purpose, or title, related to the materials. The entire risk as to implementing or otherwise using the materials is assumed by the implementer and user. IN NO EVENT WILL THE PARTIES BE LIABLE TO ANY OTHER PARTY FOR LOST PROFITS OR ANY FORM OF INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES OF ANY CHARACTER FROM ANY CAUSES OF ACTION OF ANY KIND WITH RESPECT TO THIS DELIVERABLE OR ITS GOVERNING AGREEMENT, WHETHER BASED ON BREACH OF CONTRACT, TORT (INCLUDING NEGLIGENCE), OR OTHERWISE, AND WHETHER OR NOT THE OTHER MEMBER HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

License
The Project is made available by the Joint Development Foundation. The current Working Group charter, which includes the IP policy governing all working group deliverables (including specifications, source code, and datasets) may be found on page 20 of this link.

Currently, the licenses governing the Interoperability Working Group for Good Health Pass deliverables are:

Copyright mode: Creative Commons Attribution 4.0.
Patent mode: W3C Mode (based on the W3C Patent Policy).
Source code: Apache 2.0.

The WG is not expected to produce source code.

Table of Figures

1 The Problem We Are Solving: Reopening Global Travel

For more than a year, countries around the world have adopted various restrictions on mobility and public gatherings to prevent the spread of COVID-19 and prevent further strain on overburdened medical systems. While necessary and appropriate to protect public health, the economic consequences of these "lockdowns" have been staggering.

The COVID-19 pandemic has impacted every segment of the economy. Especially hard hit has been the travel and tourism sector. Representing 10 percent of global GDP, the sector is experiencing its single greatest shock since the terrorist attacks against the United States on September 11, 2001.

- Between January and October (2020), international tourist arrivals were down 72 percent;
- In 2020, the airline industry was expected to lose upwards of $118.5 billion USD, with additional losses expected in 2021; and
- In 2020, travel and tourism sector contributions to global GDP decreased by 49.1 percent – $4.5 trillion USD – nearly 18 times the impact felt during the 2009 global financial crisis.
- Employment in the travel and tourism sector decreased by 18.5 percent, a loss of 61.6 million jobs worldwide.

Faced with competing demands to restore mobility and economic activity, and protect public health, there is a growing consensus that the best route forward is one in which the global economy – and international travel – is restarted incrementally in a manner that keeps transmission in check. To that end, governments, employers, educational institutions, airlines, sports and event venues, and others are considering whether they might require proof of COVID-19 status (vaccination, negative test, or recovery) as a supplement to continued social distancing and masking requirements.

Such proposals, where individuals may be requested to share health-related data, raise genuine concerns about individual data privacy rights. While centralized registries of individuals' vaccine status or test results often underpin public health surveillance, they also carry significant risk of data theft, could facilitate problematic surveillance tactics, or inappropriately expose personal data, thus requiring a delicate approach to balancing public health and data security. Additionally, if not carefully implemented, limiting entry based on health status could prove inequitable and poses the risk that individual liberties, such as freedom of movement, freedom of association, and free choice of occupation, will be arbitrarily or discriminatorily restricted.

In addition, this exchange of health data raises technical and regulatory challenges:

- Existing paper-based credentials – such as the WHO "yellow card," the U.S. Centers for Disease Control and Prevention COVID-19 vaccination certificates, NHS COVID-19 vaccination cards and lab test results – are easy to lose, prone to counterfeiting, and unnecessarily expose sensitive personal information
- Health data may move outside of the highly regulated and controlled healthcare sector (i.e. health providers, public health authorities, private medical providers, lab testing companies) to a wide variety of organizations in the travel and tourism sectors (i.e. airlines, border agencies, hotels, cruise lines) that may be unaccustomed or ill-equipped to manage sensitive health data, or who may have financial incentives to sell personal health information.
- Healthcare data exchange standards were designed for healthcare use cases and for exchange between regulated entities, and not for the wide variety of use cases, business processes, and

organizations required to reopen economies and restart global travel. The lack of familiarity of healthcare standards outside of the sector in question, and the complexity that will arise from applying them to non-healthcare use cases, will further increase implementation challenges.

- Data exchange across sectors will need to work within existing (and complex) business processes, integrate with existing (and often, incompatibile) digital infrastructure, and address differing priorities.

At present, there is growing momentum: programs are in use, or being implemented, in many countries around the world, including countries in the European Union, Israel, and Singapore. Additionally, many companies across the travel and tourism industry, as well as concert venues and sports stadiums, have publicly announced plans to use proof of vaccination or testing as a condition for entry.

The sense of urgency is palpable; everyone is looking for solutions that can help equitably and safely reopen our global economies. But the urgency to adopt and implement digital health pass systems risks creating a patchwork of systems that are not interoperable with one another, and that vary greatly in terms of privacy, security, and user control over personal data. Further, the absence of coherent standards makes it difficult for implementers, policymakers, and the public alike to understand the utility — and accompanying risks — of such systems.

The Good Health Pass Collaborative (GHPC) was born out of this urgency — to weave together existing efforts and present a path toward "good" digital health passes built on key fundamental principles (as outlined in the first white paper, entitled, Good Health Pass: a Safe Path to Global Reopening).

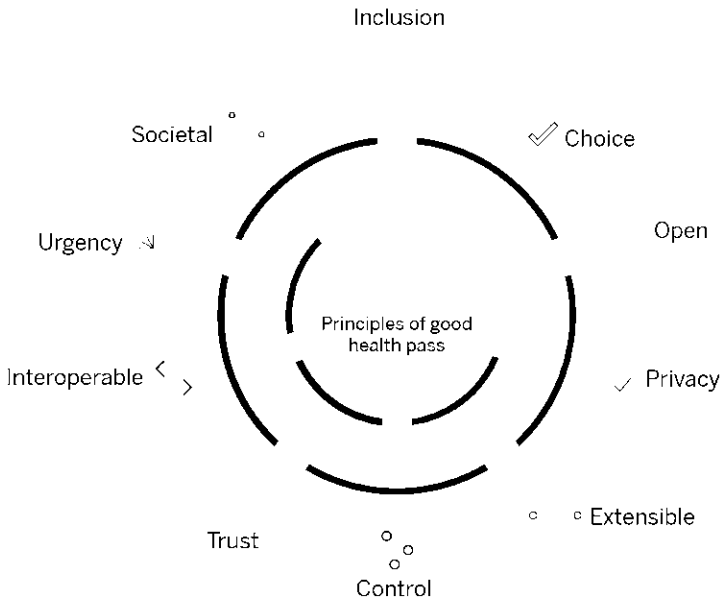

Figure 1: Good Health Pass Principles

The GHPC brought together organizations with a shared sense of responsibility to ensure that, if the exchange of health status information is required, health passes respect the rights of the individual first and foremost, appropriately balancing the data requirements of community health with the privacy rights of the individual. The GHPC has come together to help:

- **Restore Confidence:** Restoring international travel requires restoring confidence: the confidence of travelers that they can move about without significant risk, the confidence of businesses that they can resume normal operations without exposing their staff or customers, and the confidence of governments that they can adequately protect the health of their citizens. Digital health passes offer a route to reopening that can instill such confidence.
- **Promote Equity:** It is expected to take years to vaccinate the world's 7.9 billion people. Widespread testing is an essential public health tool – and one that must continue to be supported alongside vaccination to ensure an equitable return to public life.
- **Foster Collaboration**: Numerous efforts are currently underway to develop data sharing and exchange solutions– both vaccination and test certificates – for international travel and a variety of other applications. Given this, it is unlikely that a single solution will be implemented universally – or even across the entire travel industry. Thus, it is critical that solutions are designed to be interoperable, both with one another and across institutional and geographic borders.

1.1 The Challenge Of Health Data Exchange Across Ecosystems

By definition, proposals to use proof of health status as a condition of entry straddle multiple ecosystems and will require that data exchange works within existing business processes, digital infrastructure and regulatory frameworks.

1.1.1 The Current Health Data Landscape

Healthcare systems vary radically across the world. In many countries, COVID-19 vaccination is being coordinated almost entirely through public health authorities or national health systems, leading to a relatively small list of organizations (or singular entity) able to attest to an individual's vaccination status. In some countries, testing is similarly centralized. However, there are countries –including the United States – with a far more decentralized healthcare system, in which a multitude of organizations are providing and administering COVID-19 tests and vaccinations, and where each, hypothetically, could issue proof of an individual's health status.

Additionally, there is wide variation in the existing digital infrastructure within healthcare systems, with variability both between and within countries. In some jurisdictions, health care records are maintained largely in paper formats, with little individual-level data captured electronically. Healthcare systems in some areas can rely on constant, high-speed internet access, while others must contend with intermittent connectivity at the point of care.

Finally, despite recent advances in health systems' interoperability, different countries – and health providers – are at different points in adopting standards-based approaches for exchanging data electronically. The Health Level Seven International (HL7) Fast Healthcare Interoperability Resources (FHIR) standard, designed to enable health data to be quickly and efficiently exchanged within the healthcare ecosystem, is growing in use, but adoption remains patchy. Moreover, FHIR is only for the exchange of data between regulated providers of healthcare services and was never designed for broad and diverse exchange for non-healthcare use cases.

Interoperability becomes significantly more complex when considering health data exchange outside of the healthcare ecosystem. International travel presents one of the most complex of all possible use cases for exchange of health data, requiring extensive collaboration across multiple sectors and countless jurisdictions.

1.1.2 Complexity of International Travel and Health Data

International air travel is an inherently complicated process. It is highly regulated and, by definition, involves at least two governments who each require detailed information on who is intending to cross their borders. In addition, there are many stakeholders in the process, operating under more rules and regulations. Indeed, according to unpublished research from SITA, a multinational IT company that provides services to the air transport industry, as many as 23 different companies can be involved in the process of getting a passenger on board an aircraft and allowing it to take off.

The international travel industry has spent years ensuring underlying systems and processes are both interoperable and globally standardized. In addition, technology providers have worked to give the travellers a seamless journey experience, minimizing the interventions required.

However, these systems have largely broken down under the strain of new and shifting requirements for COVID-19 testing and vaccination. Historically, airlines and other providers of international travel have had to implement rules relating to immigration, which change, at most, a few times per year. In the midst of the pandemic, rules of entry are changing at short notice – sometimes on a daily basis – creating uncertainty for travellers, airlines and scheme providers alike.

Moreover, while the industry has existing digital infrastructure used to automate these processes, the lack of integration of health status information with existing passenger processing systems has necessitated manual checks of travelers' paperwork, causing delays and straining businesses. Many airports currently require 100% of their pre-pandemic staffing levels to process just 10-15% of traveller numbers, while immigration processes are commonly causing 5 to 6 hour delays.

And the travel industry is anticipating the situation becoming more complicated still, as multiple incompatible systems are rolled out relating to COVID-19 health status. The pent-up demand for travel could create an environment in which check-in agents, ground handlers, airport staff, immigration and border control officers are faced with thousands of travellers from all corners of the globe with no standard health pass formats, shifting rules of entry, little means to prove the authenticity of health credentials, and (in some cases) no access to the internet to carry out verification checks. At best, the result could be unhappy passengers; at worst, a bending of the rules with the potential for disastrous health consequences.

While outside of the scope of the GHPC, when considering use cases beyond proof of COVID-19 status for the purposes of international travel, the world of potential issuers and verifiers becomes nearly infinite. It is for this reason that open and interoperable standards are not only key to the current effort, but also to set the standard for future consumer protections.

2 The Good Health Pass Interoperability Blueprint

2.1 Our Approach To A Good Health Pass

If the exchange of health status is to become a requirement for reopening our economies and borders, then members of the GHPC believe **it is our responsibility to ensure that the technical ecosystem works for everyone: individuals, organizations, and governments.**

This means ensuring that:

- the exchange of data is a private exchange between the individual presenting the data (holder) and the organization receiving it (verifier), and cannot be tracked by a third party (which includes the original issuer or verifier);
- it minimizes the amount of data that the holder needs to exchange for the specific business process; and
- there is complete transparency between holder and verifier in terms of how the data will be used.

Technical interoperability also requires the creation of interoperable trust architecture.

We believe a health pass, as described below, offers a number of benefits over alternative models being discussed for COVID-19 recovery:

1. Is difficult to falsify because it is digitally signed by a trusted entity.
2. Is less prone to loss, and easier to recover.
3. Minimizes the personal or health-related data that needs to be exchanged for a business transaction.
4. Gives individuals control over their own data, including the ability to choose what information to share and with whom.
5. Can be automatically verified when presented, without the issuer (or anyone else) knowing where it has been used.

Here, terminology matters. Almost a dozen different terms have been used publicly to describe the container of data a traveller needs to prove their COVID-19 health status. Of these terms, we settled on four to use precisely and consistently in the Good Health Pass architecture, across either paper or digital versions.

- **Attestation:** A set of claims about a subject for which the attester can be held accountable. This includes a self-attestation.
- **Certificate:** A set of claims about a subject by an issuer that can be verified in some manner, either manually or automatically.
- **Credential:** a certificate issued in a form designed to be easily transported by the holder and easily verified by a verifier, especially using machine-readable data and/or cryptographic signatures.
- **Pass:** a credential to which data minimization and anti-correlation have been applied and any relevant travel data has been added, so it includes only what a verifier needs to make a trust decision in a specific context (such as boarding a plane).

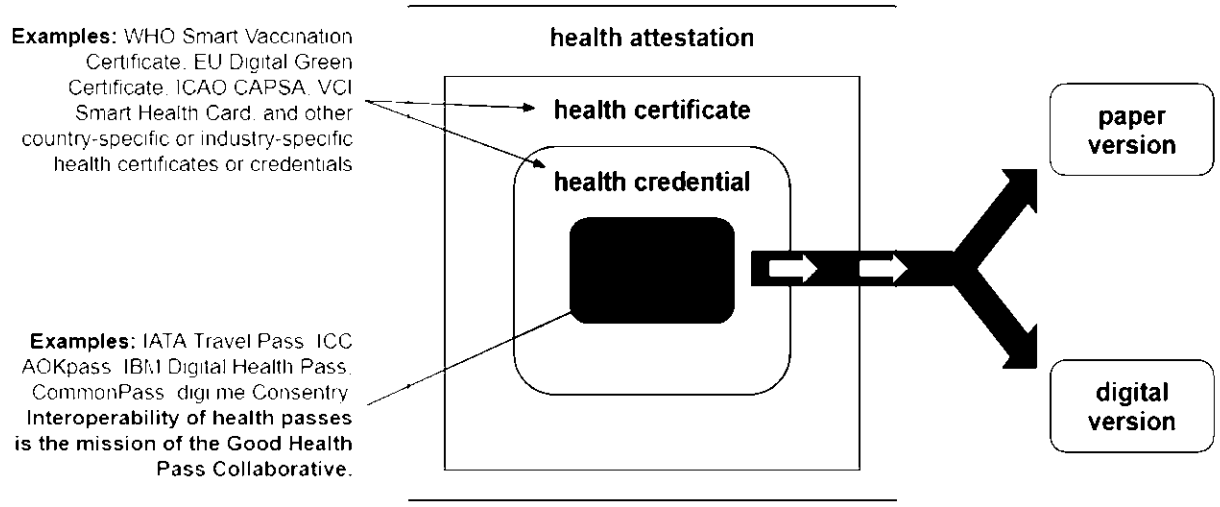

Figure 2: Good Health Pass Terminology

The key point of differentiation between a credential and a pass is that a pass encapsulates a business decision and only contains the data required to make that decision, such as "good to fly" or "good to return to work", filtering out all other unnecessary and sensitive personal health information.

For a health pass to be "good," it must obey the principles of lawfulness and purpose limitation, and apply data minimization and anti-correlation wherever possible, transmitting only the data the verifier absolutely needs to know. In many cases, the only information that should be provided to the verifier (such as an event venue) is that the individual is deemed "safe", based on the established requirements (e.g., vaccination, test status, etc.). This level of data minimization and privacy preservation is consistent with the European Union's General Data Protection Regulation (GDPR). It is critical for a global ecosystem with multiple providers of health status (vaccination status, testing status, immunity status) within and across jurisdictions (province, state, country, region), and with multiple organizations and governments implementing for the disparate, and changing, policy requirements.

2.2 Key Design Choices

The foundational principles of the Good Health Pass Collaborative lead to a number of key design considerations and technical choices. With these in mind, our analysis and recommendations are based on five key pillars, as set out below.

2.2.1 The individual must be at the center of the data exchange

- Individuals **SHOULD** control their own data: what they share, with whom, when, and for what purpose.
- Exchange of data **SHOULD** be private, between issuer/holder and holder/verifier, without third parties able to track it.
- There **MUST** be transparency over how the data is processed, used or shared, with collection and management of consent as required. Verifiers will be able to process data only, not to share it onwards, unless they get explicit consent to share the data with a specific entity.

- We have chosen to adopt a **decentralized identity architecture**, incorporating the **World Wide Web Consortium (W3C) Verifiable Credentials Standard**, to help enforce implementation of these principles, where:
    - Verifiable Credentials (VCs) can be used to create a digital version of any paper credential, such as a passport, driving license, health insurance card, employee ID, etc.
    - Once an issuing organization releases data, as a VC, to an individual, then they have full control to share with whomever they choose, and the receiving organization can trust the data without needing to go back to the original issuer.
    - The VCs are digitally signed by the issuer. This means that the verifier (i.e., the party who needs to see proof of the credential) can verify the cryptographic signature to ensure that it could only have come from the issuer and that it has not been tampered with. In other words, they know it is genuine.
    - When they present their data to a verifying organization, this is a private transaction in which the verifier doesn't need to interact with the issuer in order to check the validity of the data. This peer-to-peer transaction model, combined with data minimization and other privacy-preserving techniques, makes data exchange highly privacy preserving and reduces the opportunity for an individual's data activity to be tracked.
- Given the requirement that a Good Health Pass **MUST** transmit only the data the verifier absolutely needs to know, use of credential formats, signatures and exchange protocols that support **selective disclosure** is vital. This will allow individuals to generate dynamic passes, on demand and in response to the specific requirements of the verifier's business process, such as passing through border security.
    - We believe there is an important consumer education effort required to help individuals assert their agency about what information to share – or not share – with potential verifiers.
    - Without clear guidance on selective disclosure scenarios – the amount of information a verifier of a particular type (i.e. a hotel) can request of an individual – reliance on multiple, static passes creates friction for individuals and requires them to remember which pass to use in each setting. This could lead to regular use of the full "signed clinical health" data as a health pass, which shares a lot more information than is required for the particular use case.

2.2.2 Equity and inclusion are essential

- Until COVID-19 vaccines are universally available, health passes **MUST allow someone to show proof of COVID-19 health status (e.g. proof of a recent negative test result)** as a condition of entry, when required.
- Any system that restricts access to rights, privileges, activities, or venues exclusively to those able – and willing – to present proof of vaccination poses significant equity concerns. Fully addressing equity and inclusion concerns requires specifying and restricting the appropriate uses for a system. The GDPR defines purpose limitation as a requirement that personal data be collected for specified, explicit, and legitimate purposes, and not be processed further in a manner incompatible with those purposes (Article 5(1)(b), GDPR). We call upon policymakers and regulators to specify appropriate uses for a GHP system and agree, as a Collaborative, to abide by the purpose limitations set by all relevant jurisdictions.
- Using the term "vaccine passports" in a generic sense is both technically imprecise and politically inflammatory; instead, we suggest use of the term "digital health pass".

- Any digital health pass solution **MUST** work across the world **without the requirement to possess a smartphone**. Good Health Pass solutions **MUST** offer a hard copy alternative for those who do not own – or wish to use – a smartphone.
- In recognition that a Good Health Pass solution will take time to implement end-to-end, the blueprint needs to be pragmatic and allow for incremental adoption and coexistence with existing systems.

2.2.3 A decentralized approach is necessary for global security and scalability

In our post-pandemic world, the widespread requirement of COVID-19 health credentials and passes for international travel means that the exchange of health data will no longer be constrained to a small number of regulated healthcare service providers. And as the world becomes ever more data-driven, the number of data issuers, holders, and verifiers across different jurisdictions and business processes will continue to grow. The traditional centralised or federated approaches are no longer fit-for-purpose. New approaches are needed that allow the exchange of data in a way that is trusted, privacy-preserving, secure, scalable and controlled by the individual. The blueprint provides guidance on how to set up decentralized yet interconnected governance frameworks and trust registries for governments and industry coalitions that can support the issuance of trusted health credentials and passes.

A decentralized approach:

- Empowers individuals to manage their own data, so they have it when they need it and can exchange it through a secure, private, and verifiable channel.
- Allows any organization that can be proven to be trusted, through a global ecosystem of decentralized trust registries, to issue data to an individual and have that data trusted when presented to a verifier. We have elected to use the W3C Decentralized Identifier Standard as a decentralized approach to public key infrastructure.
- Moves data exchange to the person, where data is exchanged directly from person (device or paper) to verifier, giving significant security and performance benefits; firstly, this moves away from over-reliance on centralized repositories, reducing the risk of data breaches, and secondly it significantly reduces traffic between healthcare information systems and (a potentially huge number of) verifiers, each which could be a source of data breach.
- Reduces the ability for issuing organizations to track an individual's data activity. As the data exchange is peer-to-peer in nature, there is no requirement for the verifier to notify the issuer that a transaction occurs (which happens when they need to ping the issuer to verify).

2.2.4 Open standards are key to interoperability and participation

- For global interoperability, we have chosen to focus on adoption of open standards, such as the **W3C Verifiable Credentials**. Several GHPC members are also contributing to open source projects so that good practice, techniques and capabilities can be shared across the community, helping to drive interoperability and extensibility across use cases and geographies, and to increase participation.

2.2.5 We must be pragmatic and realistic

- The roll-out and adoption of a Good Health Pass is going to be a huge challenge that intersects with government policy, business process, legal regulation, technical systems, and societal norms.
- Accepting that technical implementation always takes time, any proposal **MUST** be **pragmatic** and be capable of being **phased**. The work of the GHPC will take a very practical approach, recognizing that we need to move fast, but NOT break things. We will need to work within existing constraints, making incremental improvements over the coming months and years to get us closer to our vision of a privacy-protecting, user-controlled, globally interoperable, and universally accepted digital health pass system.
- The approach adopted therefore enables downstream entities in the process (such as health passes) to act as verifiers of upstream data, where that health data cannot be fully verified at source, in order that the benefits of the decentralised system can be achieved rapidly within 30-90 days.

3 Where Does the Blueprint Fit Within the Industry?

3.1 Good Health Pass Ecosystem

In this race to meet the needs of the market it is unlikely that a single solution will be implemented universally – or even across the entire travel industry. Instead, we expect – and fervently hope – that a variety of solutions will offer choices, both for the public as well as for implementers (e.g., governments, airlines, employers, educational institutions, venues, etc.). Choice benefits users, who can select a solution that feels intuitive to them, and promotes inclusivity, as no single solution will ever be universally appropriate. However, with choice comes interoperability challenges, as well as the potential for confusion and lowered standards. For this reason, global collaboration and standardization is essential.

Enter the **Good Health Pass Ecosystem.**

The Good Health Pass Ecosystem aims to bring together standards bodies, technology providers, government, policy makers, consumer advocates, and other stakeholders in the implementation of good health credentials and passes within a global **digital trust ecosystem**, consisting of four core parties:

1. **Issuers** of credentials and passes (i.e. labs, public health systems, rules engines)
2. **Holders** of credentials and passes (i.e. travelers)
3. **Verifiers** of credentials and passes (i.e. airlines, border authorities)
4. **Governing Authorities** who publish rules and policies in a **governance framework** (aka **trust framework**)

The figure below shows the relationships between these four parties in a configuration sometimes referred to as the "trust diamond".

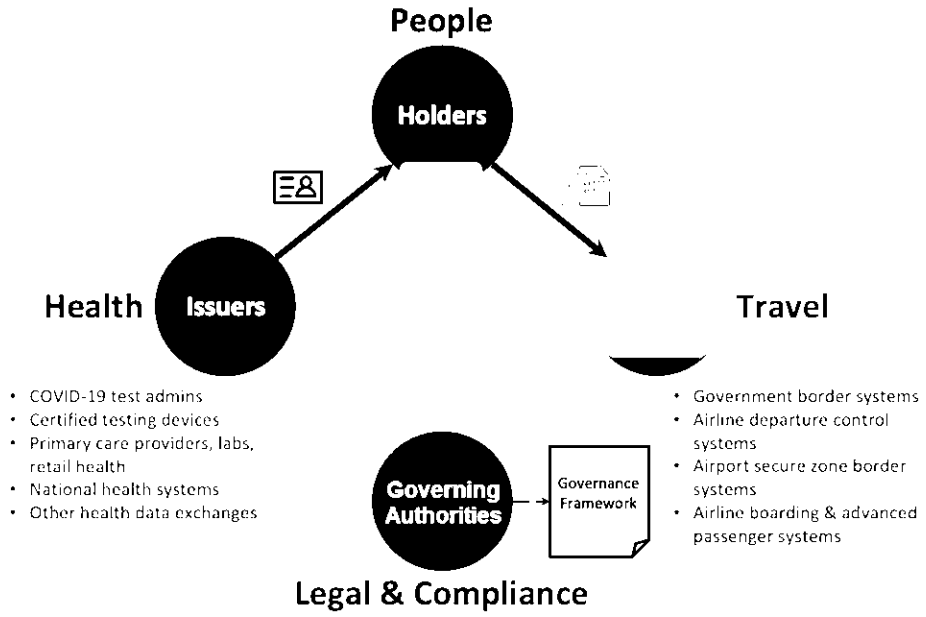

Figure 3: The Good Health Pass Ecosystem

The term "digital trust ecosystem" means that all credentials are in a digital format; however, it does not

mean that they are always stored or exchanged digitally, and in some cases paper **MAY** be used as the medium for storage and exchange. This is suboptimal from a privacy or security standpoint, but is a requirement for those who do not have access to a digital device, or do not want to use one.

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 GHPC is developing.

3.2 Integration With Open Standards

While an open market has a number of benefits, it does create a need for these solutions to be designed for interoperability – both with one another and across institutional and geographic borders. Technical and organizational interoperability can only be achieved through the creation of a common set of open standards to which all digital health pass systems must adhere, including standards for national lab and vaccinator accreditation, and identity binding and authentication. There are multiple standards efforts underway across the globe, many of which will be adopted by different jurisdictions, companies, and technology providers.

The Good Health Pass Collaborative was created with the express purpose of bringing together disparate geographic and vertical market efforts for health pass standards. From its inception, GHPC established affiliations with a number of groups across the industry for both dialogue and support. More than 120 organizations have endorsed GHPC – these organizations are listed on the GHPC website.

In addition, GHPC formed partnerships with the COVID-19 Credentials Initiative and the Trust over IP Foundation – both Linux Foundation projects – to address specification details.

- Trust over IP Foundation (ToIP): ToIP is defining a complete architecture for Internet-scale digital trust that combines cryptographic trust at the machine layer and human trust at the business, legal and social layers. The trust framework constructed for the Good Health Pass Blueprint has been developed in partnership with the ToIP Foundation.
- **COVID-19 Credentials Initiative (CCI):** CCI has been working with initiatives around the world to leverage verifiable credentials for COVID-19 use-cases and, since it joined Linux Foundation Public Health in December 2020, has been working with public health departments globally to understand their needs. CCI published a key paper about the flavors of verifiable credentials in February 2021 and has been an active contributor to GHPC, specifically driving the verifiable credential standardization and interoperability.

GHPC also invites collaboration with other emergent standards and specifications. Health credentials created to the following specifications are referred to and supported within the Good Health Pass Blueprint:

- **Digital COVID Certificates - European Union:** This is a pan-EU initiative for member states to align on an approach for the issuance of cryptographically-signed credentials in a Quick Response (QR) code format, and is based on a custom data model. Whilst the current specifications are limited to physical paper-based credential exchange, digital exchange is being investigated for the second release of the specification.
- **World Health Organization**: Work on definition of vaccine credentials for multiple use cases is currently in flight. Interim Guidance for Developing a Smart Vaccination Certificate, RC1, was published 19 March 2021. Health credentials created to this specification will be referred to and supported within the Good Health Pass Blueprint when the final WHO specification is published.

- **Vaccination Credential Initiative (VCI) – United States:** This consortia is developing a technical specification, the SMART Health Card Framework, for the issuance of cryptographically-signed credentials in QR code form. It is derived from the W3C Verifiable Credentials JWT data model; however it does not support selective disclosure, a key privacy-enhancing feature of the format chosen for the Good Health Pass principles.
- **Digital Infrastructure for Vaccination Open Credentialing (DIVOC) – India:** This is open-source software and associated specifications developed within the India community, intended to address an approach to digitally orchestrate data exchange for vaccination data. This is specifically addressing the issuance of cryptographically-signed credentials in QR code form and is based on the JSON-LD W3C Verifiable Credentials data model. See here for APIs, specifications, and backgrounders.

Without immediate collaboration to ensure that clear standards are applied across vaccination, health test, and immunity certificates, there is a significant risk of fragmentation. A failure to address interoperability – both from a technical and a trust perspective – will undermine acceptance, adoption and, ultimately, the expected public health and economic benefits of digital health pass systems.

Finally, there is other work across the community in motion; the following programs will be harmonized within the completed Good Health Pass Blueprint:

- **Collaborative Arrangement for the Prevention and Management of Public Health Events in Civil Aviation (CAPSCA):** This is a cross-sectoral program managed by the International Civil Aviation Organization (ICAO) and supported by WHO. It is a multi-stakeholder effort to develop a global framework for COVID-19 test credentials, including standardization of documentation, interoperability of systems and exchange of data.
- **Airports Council International (ACI)**: Airport Health Testing and Travel Information Standard, API V1.0, 23 February 2021. See more details here.
- **International Civil Aviation Organization (ICAO):** Technical Report VDS-NC Visible Digital Seal for non-constrained environments. Version 1.0, 23 April 2021. ISO/IEC JTC1 SC17 WG3/TF5 for ICAO. See more details here.
- **CARIN Alliance:** Digital Identity and Federation in Health Care, December 2020. See White Paper Reference here.

3.3 Building A Community Consensus

Bringing the vision of the Good Health Pass Interoperability Blueprint to life will require building a community committed to adopting these recommendations and creating GHP-compliant solutions. It will also require forming an official governing authority for an overarching governance framework, whose job is to:

1. Complete and approve the official first version of the governance framework.
2. Publish and maintain a dedicated website hosting the official governance framework documents.
3. Gather feedback and develop future versions based on the "in-the-field" experience of implementing V1, as well as changes in other external factors such as regulations and health authority guidelines.

In keeping with the principles of good governance, we recommend that the GHP governing authority be formed and governed by the primary stakeholders in the GHP digital trust ecosystem.

4 Solving for Interoperability: An Overview of the Blueprint

To realize the vision of a globally interoperable ecosystem issuing, holding, and verifying Good Health Passes, interoperability must be addressed at a number of levels.

Solutions must interoperate with one another technically; they must use common data models and elements, as well as standard credential formats, signatures and exchange protocols. This requires gaining agreement on the VC formats, signature types, and exchange protocols, mechanisms for binding the identity of the holder, and agreement on the QR codes to be used to present a digital health pass.

But, as important as technical interoperability, health pass solutions must offer a consistent user experience. They must also be governed under a holistic governance framework. Trust registries are necessary for accrediting the COVID-19 testing labs and vaccinators who will "issue" the credentials, as well as those verifying them (relying parties).

The GHPC has enumerated nine categories of interoperability challenges that must be addressed in order for functional interoperability, across borders and institutions. Over the last three months, members of the GHPC have been working to define the challenges that face us and to develop a cohesive set of recommendations, standards and specifications that will allow a Good Health Pass Ecosystem to flourish.

The table below summarizes the key recommendations from each.

Overall Recommendations **Consistent User Experience**	

The need to create a consistent user experience, based on a model of universal acceptance, is the most fundamental interoperability challenge, where a Good Health Pass **MUST** be easy to obtain, use, and update, without any special user knowledge.	• The Good Health Pass model encompasses three "zones" of a passenger's journey and which create the foundation for a good user experience.
	• These three zones are preceded by a person discovering the COVID-19 requirements of a given travel itinerary.
	• The zones (1 - 3) define the process by which a person:
	  ○ Zone 1: Obtains a COVID-19 Test or Vaccination that meets the requirements.
	  ○ Zone 2: Obtains the COVID-19 Credential.
	  ○ Zone 3: Presents their COVID-19 Credential.

Security, Privacy, and Data Protection	
Good Health Passes **MUST** meet baseline security and privacy requirements that enable holders to maintain full control of their personal data.	• A Good Health Pass solution **MUST** comply with globally-recognized privacy and data protection principles, namely lawfulness, consent, data minimization, retention requirements for data and technology, assurance of data quality, information security, purpose specification and use limitation, transparency, personal control and privacy rights, and auditability and accountability.

	• The drafting group makes detailed recommendations for what is required to meet each of the above principles.
Identity Binding	
Good Health Pass compliant implementations **MUST** apply standard methods for verifying the identity of the holder at specified levels of assurance	• Describes the role of identity binding in Zones 1 - 3. • Solutions **SHOULD** record the levels of identity assurance, working with existing systems to satisfy identity binding and authentication recommendations. • Identity binding **MUST** support low or no technology solutions, providing verifiers with information on the identity binding that has taken place so that the verifier can supplement, as required. • **MUST** follow globally accepted guidance for the levels of identity assurance driven by ISO/IEC 29115, chosen as the most internationally inclusive standard.
Credential Recommendations **Standard Data Models and Elements**	
Good Health Pass compliant implementations **MUST** comprise a standard set of data elements	• There **SHOULD** be vaccination, test, and recovery passes, in line with European Digital COVID Certificate minimal data elements. • Interoperability will require semantic alignment and harmonization with the recommendation to adopt the Overlays Capture Architecture (OCA). • FHIR is the recommended data exchange format, specifically when integrating with healthcare systems.
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	• The recommended credential format is the W3C VC standard, specifically the JSON-LD formatted VC with BBS+ LD-Signatures, and WACI PEx Protocol defined by the DIF Claims and Credentials WG. • Issuers and verifiers **MUST** demonstrate adherence to all jurisdictional security and privacy requirements, such as ISO 2700X, ISO 29100, ENISA, GDPR, HIPAA, NIST CSF, or Canadian ITSG-33. • Performance requirements **MUST** be specified, included against a variety of user devices to equity and cost concerns. • Support paper-based solutions. • Support offline credential exchange without Internet access. • Accept non-W3C compliant credentials.

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.	• Digital Credentials **SHOULD** be exchangeable as a QR code. • All data **SHOULD** be encapsulated within the QR code for offline exchange, • The card **SHOULD** include both human readable text and machine readable QR codes. • It **SHOULD** provide data minimization through a card design that can include multiple QR codes. • The card **SHOULD** include clear instructions for the holder of the credential. • The size, format, and encoding of the QR code needs to meet specific requirements so that it can be scanned and verified by a variety of devices. • It **SHOULD** be able to participate in digital transactions.
Operational Infrastructure Recommendations **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	• Describes in detail the optimal rules engine subsystem design to address Good Health Pass requirements and interoperability. • Proposes separate subsystems for health and travel. • Addresses passenger privacy, health status, and user experience.
Trust Registries	
Good Health Pass compliant implementations **MUST** be able to quickly and safely verify authorized issuers and verifiers	• A trust registry **SHOULD** be as basic as possible and not push design constraints on implementers beyond the most basic requirements. • It **MUST** be able to answer queries as to what issuers are authorized to issue what credentials or passes, and also what verifiers are authorized to request what credentials or passes. • Trust registries **MUST** support offline/no-network environments with caching. • Registry operators and data source providers **MUST** be aggressively committed to sustaining trusted registry sources, encourage accountability and be committed to

	rectifying problems that arise on an ongoing basis.
Governance and Trust Frameworks	
An interoperable digital trust infrastructure requires that members agree on the business, legal, and social policies they will follow to achieve their trust objectives, with the collection of policies, rules, and specifications called a governance framework or trust framework.	• The governance framework **MUST** take into account existing regulations, directives, and specifications for health credentials and health passes designed for proof of COVID-19 health status from governments and other global authorities and industry consortia, including the EU COVID-19 Certificate, the WHO Smart Vaccination Certificate, the VCI SMART Health Card. • It **MUST** follow all mandates specified in the ToIP governance metamodel unless otherwise noted. • It **MUST** incorporate all requirements specified in the Good Health Pass Interoperability Blueprint V1.

5 Overall Recommendations

5.1 Recommendation #1: Consistent User Experience

5.1.1 Introduction

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 make COVID health passes difficult to use, 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 (GHP) **MUST** be easy to obtain, use, and update, without any special user knowledge.

A consistent user experience 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 experience** – just as driving a car requires unlocking the car, fastening the seat belt, starting it, putting it in gear, and using the accelerator and brakes; we need to agree on generally consistent experience for travelers, 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.

5.1.2 Background

While the COVID-19 pandemic has impacted every segment of the global economy, no sector has been hit as hard as travel and tourism.

The travel industry has many stakeholders that work together to provide the services travelers expect. In aviation, travelers of all budgets typically have access to a range of dining, entertainment and shopping options. They have also grown used to the convenience of online services and mobile applications: receiving digital visas in advance, and navigating airports predictably with the help of online check-ins and self-service options.

At the onset of the COVID-19 pandemic, all of this came to a halt. Many airports and terminals closed, with flights cancelled or switched to cargo-only. For travelers still flying, requirements remain unclear and prone to change, resulting in a lack of certainty on whether they are in compliance and long queues for additional checks before departure and on arrival. Access to terminals is now restricted to "passengers only", and many of the self-service options have been disabled due to their inability to perform the ever-evolving requirement checks. All of these frictions further discourage travel.

Despite low passenger volumes, many travel stakeholders still have to maintain services and staff just below peak levels – a costly and inefficient situation that makes recovery a difficult prospect for the industry at large.

5.1.3 Objective of this Drafting Group

It is unlikely that one single health pass solution provider will be applicable or appropriate for every use case, even within the travel ecosystem. To that end, this group focused on articulating the myriad of user journeys related to obtaining and using a health pass in the context of international travel.

Given the multiple solutions that are coming to market, it is essential to outline functional interoperability that can help airlines, airports, and consumers alike choose the best privacy-preserving products and reduce barriers to use. This includes ensuring that:

1. Owners of **health certificates/credentials** are able to present them as **digital health passes** and prove they were issued by accredited labs or health authorities and have not been tampered with.
2. **Digital health passes** can be interpreted and verified by a verifier regardless of what kind of **health certificate** they are based on or what kind of software was used to issue, store, or present them.
3. To offer consistent user experience, different **digital wallet apps SHOULD** follow a standard way of receiving, verifying, presenting, and integrating **digital health passes**.
4. Sharing of **digital health passes SHOULD** be consent based. Exchange of personal identifiable information **SHOULD** be minimized or avoided.
5. The cost and system integration efforts required of stakeholders to implement the standard way of receiving, verifying and presenting **digital health passes MUST** be low.
6. Health pass solutions **SHOULD** also be able to process **paper health passes** for users who do not use mobile devices.

5.1.4 Understanding the User Journey

A good, intuitive user experience 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. The following is an overview of the user journey for a health pass, as it relates to the example of international air travel. For the sake of discussion, "credentials" and "certificates" are used interchangeably. For this scope of this discussion, we will use the term "certificate" to refer to any form of digitally-signed health credential, and the term "pass" to refer to such a credential when it contains only the minimum data required by a verifier.

5.1.4.1 Discovering COVID-19 Travel Requirements

Much like pre-pandemic planning, when a person decides to travel internationally, they create an itinerary, decide where and when they wish to travel, and initiate travel arrangements.

Part of the planning is determining immigration rules for the country, or countries, to be visited to verify what documentation is needed (e.g., visa, electronic declarations, and health information). Third party aggregators, such as Timatic, ICTS ACI, and Sherpa, **MAY** aggregate and apply these rules – often behind the scenes – so that travelers are prompted by carriers during the reservation process to ensure that they will be in compliance during their travels. The rules **MAY** include:

- "What are the entry requirements of my destination country(ies)?"
- "Where proof of a COVID-19 test or vaccination is required, what type of tests and vaccines are accepted and from whom"
- "How long is this test or vaccination valid?"
- "Will I need to get another test while I'm travelling?"
- "What types of health passes are recognized by my destination country(ies) or air carrier(s)?"
- "How will my health information be used, shared, and protected?"
- "Do I need to bring my passport for vaccination/testing?"

Now the traveler knows what is required of them and can seek out the appropriate tests, vaccinations, and/or pass(es) as and when needed.

GHP envisions three "zones" to delineate the foundation of the user experience and applicable workflows, as shown in Figure 4.

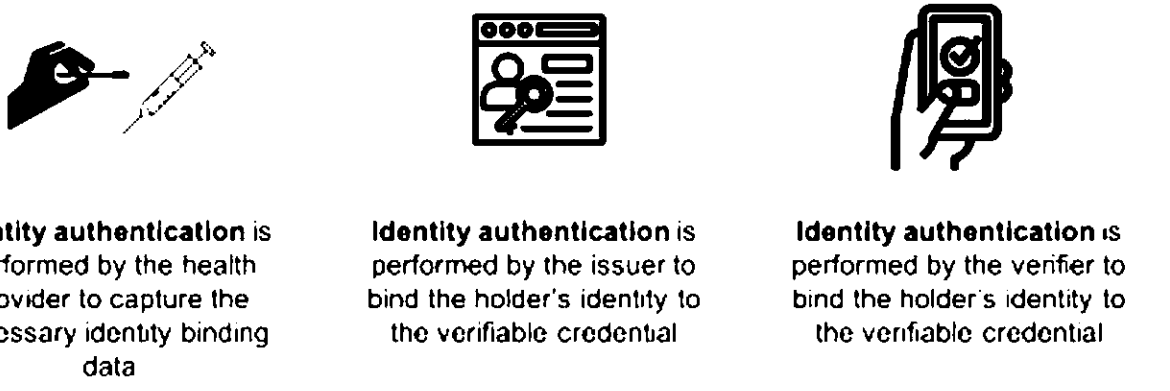

Figure 4: Identity binding and authentication zones in the Good Health Pass ecosystem

5.1.4.2 Zone 1: Obtaining a COVID-19 Test or Vaccination

A person completes a test from an authorized lab or provider (in person or at home), receives a vaccination (in person), or provides documentation of COVID-19 recovery (e.g., antibody test or release documentation, may also be at home or in person). They may ask:

- "Can I get my test results in the time-bound window to fulfill travel requirements?"
- "What proof of testing or vaccination does the lab or health facility provide? Is there a digital option, and can it be used internationally?"
- "How far in advance do I need to receive a vaccine in order to ensure acceptable levels of immunity? Is the vaccine I received recognized by or approved in my destination?"

In preparation for the COVID-19 test or vaccination appointment, and subsequently receiving a health pass or credential, the person may need to install a relevant application (e.g., from an airline, government, or other third party) and create an account following local regulation and guidelines provided by the lab or health facility.

5.1.4.3 Zone 2: Obtaining a COVID-19 Health Pass

A person obtains the necessary COVID-19 health pass(es) or credential(s) from the provider/issuer. This **MAY** occur at the same time as receiving the service or at some subsequent time. This **MUST** also allow for mitigation if the credential is issued in error or if the user disagrees with their health status determination. They may ask:

- "What certificates and in what format will be issued to me?"
- "Why do I need a digital health pass when I have a health certificate?"
- "Which health pass should I use for my travel purpose?"
- "How do I submit my certificates to my health pass?"
- "How/who should be allowed to delete or amend the test and vaccination result (when an error happened)?"
- "What else do I need to do?" (i.e., health pass solutions are unlikely to cover all aspects of international travel entry check, such as self-declaration, proof of hotel booking, proof of having sufficient funds).

Prior to receiving the health pass or credential, the person **MUST** be prompted in advance to consent (or not) to the collection and processing of required personal identity and medical data for the purpose of a health pass or credential in compliance with legal and privacy requirements.

The person's identity will then be authenticated based on the existing identity binding protocols. This could include creating a digital identity from physical ID (or record) or creating a digital identity by tying it to existing digital credentials.

5.1.4.4 Zone 3: Presenting the COVID-19 Health Pass

At an authorized verification point(s), the user is requested to provide proof of one or more COVID-19 health credentials or passes in a compatible format and they consent to provide such a proof.

The authorized verifier is able to verify that the COVID-19 health pass(es) are: (1) from an accredited lab or vaccinator, authentic and unaltered, (2) sufficiently bound to the identity of the presenter, and (3) satisfy the verifier's policy requirements.

The user should be able to perform the identification and verification digitally and remotely before arriving at the airport in order to reduce the anxiety from not knowing whether they have complied with requirements, to remove the manual checks that will inevitably cause queuing at check-in counter and immigration, and to minimize infection through a touchless user journey.

Key questions:

- "Can digital health passes enable users to submit and verify credentials and certificates before the event (e.g., travel) so that only (digital) identity check is required on the day of the event?"
- "Can users prepare and submit their entry declaration and contact tracing forms through digital health passes?"

5.1.5 Discovering COVID-19 Travel Requirements

5.1.5.1 Problem Description

As the COVID-19 pandemic progresses, the complex and fast-moving array of health requirements continue to vary by country and smaller jurisdictions. Without a standard set of requirements, these can be open to misinterpretation or even fraud.

In an ideal world, these requirements would be available in one place and accessible to all at every part of the journey. In reality, there are likely to be many sources (e.g. Timatic, ICTS ACI, Sherpa etc.) and travelers often have to seek advice from other sources such as labs, airlines, and embassies – all of which may present conflicting or slightly different requirements.

5.1.5.2 Good Health Pass Design Requirements & Considerations

In addition to providing the necessary information required for travel, a Good Health Pass could strive to address user pain points, such as determining entry requirements based on destination input or supporting search for a list of accredited, accepted, and supporting labs for test and vaccination, based on destination input or test/vaccine type. This type of user interface will make it easier for travelers and people to interact and feel comfortable with health passes.

5.1.5.3 Recommendations

5.1.5.3.1 Overall Recommendations

One key step will be advocating for simple, clear international standards. The speed of changing requirements will remain a challenge, but indications of which direction we are heading in will assist decision-making. In light of these changing requirements, the Good Health Pass Collaborative makes the following overall recommendation:

1. Travelers **SHOULD** follow the guidance from the International Civil Aviation Organization (ICAO) in **ICAO Doc 10152 5.2.2 Passenger journey through a PHC [Public Health Corridor]** to take the following actions pre-departure to ensure that their travel is as smooth as possible:
    2. Confirm governments' requirements (departure, transfer, and arrival) at time of booking and close to departure.
    3. Consult the airport / airline website and get acquainted to COVID-19 specific airport / airline recommendations and instructions.
    4. Obtain a COVID-19 health insurance policy (if necessary or recommended).
    5. Book an appointment in a testing facility in time to comply with states' requirements.
    6. Present an identification document during the test and collect testing results.
    7. Obtain authorised test result and upload to smartphone app and/or provide relevant information via government portal (if applicable).
    8. Ensure all traveling and entry requirements are fulfilled prior to departure to the airport.
    9. Make sure to have a copy of the printed test result or the digital certificates or credentials available to present at the airport.
    10. Prepare travel kit (sufficient number of face masks for travel, hydro alcoholic gel less than 100ml, etc.).
    11. Do not travel if you are feeling unwell, have symptoms suggestive of COVID-19 or if you have been in contact with someone with COVID-19, and inform the air carrier in advance.

The following phased recommendations apply to countries, public health authorities, health pass implementers, and international travelers who choose to follow Good Health Pass guidelines.

5.1.5.3.2 Phase One (30 Day Horizon)

1. Countries **SHOULD** publish their health-related entry requirements in a fashion similar to how they publish immigration entry requirements.
2. These health-related entry requirements **SHOULD** include what documentation (if any) is required to be presented at the point of testing (or vaccination), how it is to be authenticated by the health care provider, and what elements are to be recorded in the corresponding health record which will ultimately be required for entry into the destination country (or countries).

5.1.5.3.3 Phase Two (90 Day Horizon)

Countries **SHOULD** publish their health-related entry requirements as described above in a standardized way through digital channels (e.g., website).

5.1.5.3.4 Phase Three (180 Day Horizon)

1. Countries **MUST** make their health-related entry requirements publicly available through digital channels, including a list of accredited labs or health providers, what data is required, data format requirements, and any other relevant requirements so that international travelers are able to use automated, digital means to determine what is required to visit a country (or countries).
2. Travel authorities:
    - 2.1. **SHOULD**, in a similar fashion, enable international travelers to determine what is required to board aircraft based on their route.
    - 2.2. **SHOULD** not be required to process **protected health information** (PHI), especially as they are likely not staffed to interpret test results
    - 2.3. **SHOULD**, when possible, issue a GHP-compliant pass communicating a binary result (e.g., "Fly"/"No Fly") that is bound to the traveler's identity (see Obtaining a COVID-19 Health Pass).
3. Health pass implementers **SHOULD** consider providing features based on the list of accredited and/or accepted labs and clinics to facilitate easier booking and referencing for the users.

5.1.6 Zone 1: Obtaining a COVID-19 Test or Vaccination

5.1.6.1 Problem Description

Having discovered the requirements that must be satisfied, a traveler will then need to seek out the appropriate health service, including taking a COVID-19 test with an approved provider within a given timeframe.

Whether for travel or not, ensuring that individuals can continue to obtain COVID-19 tests or vaccinations in the safest, most efficient, and most equitable way possible **MUST** remain a priority for the Good Health Pass ecosystem. However, this must also be with the understanding that the more processes of identity proofing are relaxed, the more the risk of identity fraud grows. In general, this is why there have been many approaches to defining and binding an individual's identity – and/or resulting credential – to a test or vaccination. Many healthcare providers, for example, have no formal identity verification and others may rely on self-attestation to ensure inclusivity and increase operational efficiency.

Another issue is meeting common international legal and privacy requirements, namely the collection of compliant user consent at the appropriate points. These **MUST** be prior to data collection, and requested each time prior to the data being processed or transferred. Whereas the practice of providing medical information directly to an individual via printed or electronic copy does not require consent, it is standard practice for health care providers to require consent before export of any health information to a third party. Thus, if a health pass provider processes or receives medical information, it is recommended a health care institution obtain standard consent with appropriate archiving within the issuing institution.

This underscores the need to create user journeys for the creation of health passes that are consistent enough for an issuance process, but dynamic enough to minimize operational disruptions or barriers to health services. These journeys also differ substantially based on whether a person is seeking a test or vaccination.

5.1.6.2 Good Health Pass Design Requirements & Considerations

When taking steps to meet travel requirements, travelers **MAY** obtain tests, vaccines, or other evidence of health status in a variety of contexts – each of which **MAY** have their own informed consent process. Any consent for the creation of a digital health credential or pass **MUST** be completed in addition to this process.

5.1.6.3 Overall Recommendations

The steps to obtaining a traveler's consent for sharing of health pass data **MUST** follow the consent recommendations in the *GHP Security, Privacy, and Data Protection Recommendations.* As this is additional to consent for a test or vaccine procedure itself, consent may best be considered in scope of the issuance system the user interacts with.

5.1.7 Zone 2: Obtaining a COVID-19 Health Pass

5.1.7.1 Problem Description

Once a person has been vaccinated or tested, they will need to obtain a COVID-19 health credential or pass that will fulfill the requirements of the country(ies) to be visited. Carriers may also need a version of the COVID-19 credential or pass (e.g., one without PHI, e.g., a "Fly" / "No Fly" indicator).

In either case, the healthcare provider will issue the credential(s) commensurate with applicable regulations which, for international travel, will likely include a means for the COVID-19 health pass to be bound to the identity of the individual that received the test or vaccination.

Because health credentials for the use of international travel will often be displayed to verifiers in varied and often unfamiliar settings, the risk for inappropriate retention of medical information, even if it is limited in scope, presents a significant risk. For this reason, and regardless of the underlying architecture, health pass systems need to provide an overview of potential risks and guidelines for use of the health pass system. Acknowledgement of this information, along with the risks and benefits of system use, will constitute consent for participation in a Good Health Pass framework. This description should be in common language and targeted at a non-technical audience for both individual education and to aid the societal understanding of appropriate health pass expectations and usage.

There are two fundamental elements relevant to the validity of a COVID-19 health pass, (1) the provenance of the health information and (2) the identity to which it is bound. Multiple user flows for obtaining a COVID-19 health pass currently exist in reference to both identity binding and health record authentication which have consequences for downstream interoperability of health credentials:

Identity verification protocols have many applications and an established framework describing the level of assurance (LoA). The **ISO/IEC 29115** Entity Authentication Assurance Framework includes **identity proofing**(e.g., identity proofing, identity verification by passport agency), **credential management** (e.g., credential binding and issuance by passport agency), and **authentication** (e.g., authentication at point vaccination/test, at point of presenting health credential). The three zones depicted in the diagram at the beginning of this document are authentication zones where the authentication LoA is applicable.

The identity credential presented in each zone has an identity proofing LoA associated with it based on the issuance process of the identity provider (e.g., passport agency). Four levels of LoA are:

1. Low: Little or no confidence in the asserted identity
2. Medium: Some confidence in the asserted identity
3. High: High confidence in the asserted identity
4. Very high: Very high confidence in the asserted identity

Please refer to "Recommendation #3 – Identity Binding" for more detail on this topic.

5.1.7.2 Good Health Pass Design Requirements & Considerations

Given both the recommended waiting period after COVID-19 vaccination and lower cadence (i.e., a traveler **MAY** need to get tested before each trip, but only vaccinated once), it is more likely that health pass issuance processes for vaccination, compared to testing, will take place after the point of care. As such, there may be varying levels of identity assurance, which – to ensure equitable access to vaccinations in general – cannot be influenced by health pass providers.

5.1.7.3 Recommendations

5.1.7.3.1 Overall Recommendations

1. The Good Health Pass ecosystem **MUST** be capable of ingesting already-issued vaccine and test certificates into the digital credential ecosystem. Good Health Pass issuance processes **MUST** also fit existing health service and data exchange workflows for tests results and vaccinations. For example:
    1.1. A copy of the test outcome (e.g., paper-based certificate) is uploaded into a travel wallet for remote manual or automatic verification
    1.2. A travel wallet app is downloaded in advance of a test. The results from the lab are automatically populated into the application
    1.3. Proof of vaccine status is made available to a person when it is required for travel
    1.4. Detailed examples of user flows for obtaining health passes can be found in Appendix A: Example User Flows for Obtaining a Health Pass.
2. The Good Health Pass ecosystem **SHOULD** enable an individual who has received a test and/or vaccination to receive a credential (either digital, paper, or both) 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.
    2.1. 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.

2.2. In general, health passes **SHOULD** be able to be generated from multiple IDs, given that domestic travel and international air travel use cases have different identity assurance requirements.

3. Issuers (be they **health authorities** or **travel authorities**) **SHOULD** ensure the subject's identity is verified to the highest **level of assurance** supported by the issuer's current accepted process.
4. Travelers **SHOULD** be able to run the entry rule check against their trip(s) before travel so that they have opportunities to mitigate if something went wrong.
5. Travelers **SHOULD** be reminded to bring a copy of the test and/or vaccination certificate even if digital verification is accepted.
6. Travelers **SHOULD** be warned that different digital identity mechanisms and authentication requirements **MAY** be enforced at different points in their journey.

5.1.7.3.2 Phase One (30 Day Horizon)

The user experience will be impacted initially by the relevant government's policy, especially for vaccination certificates as this is normally written into country/state laws. The first dependency is the legal ability to support a digital and/or paper issuance procedure; most are paper currently and some jurisdictions may require new legislation to enable digital equivalents or replacements. The following recommendations address both practical and human rights issues.

1. Governing authorities, health authorities, and travel authorities **SHOULD** support issuance of health credentials and passes in both paper and digital formats and the corresponding user journeys.
2. The starting point **SHOULD** NOT disrupt existing processes.
3. Issuers **SHOULD** include a non-invasive method involving a minimum number of additional steps.
4. Issuers **SHOULD** where possible automate issuance using back-end electronic processes, for example synchronising records from a hospital system, to a central immunisation database, which automatically issues a credential provided specified conditions have been met. This effectively adds only the initialisation of the traveler's credential app, identity binding, and consent forms as user experience requirements.
5. Where automation like this is not possible, issuers **MAY** assign dedicated issuance resources to process a large volume of records from health authorities in order to avoid placing more burden on the health authorities themselves.
6. In countries with low-tech health facilities and infrastructure (i.e. no or basic IT systems) where automated approaches are not possible, health authorities **MAY** make simple software capabilities available in smaller health centres in order to record health data and issue digital credentials at the point of testing or immunization. Note that this does provide a solution for retrospective issuance – that requires an alternative approach.
7. With the large number of vaccinations and testing being done the number of paper records being generated is difficult to handle and control.
8. In cases where there are only paper records and no central immunisation database – especially when this involves large volumes of paper records – health authorities **SHOULD** employ a method to digitise these records, such as scanning or photographing them with an app, in order to bring them into the digital credential ecosystem.

8.1. Such a system **SHOULD** employ automated verification to authenticate and validate the vaccination or test (including dates and type), as well as the identity binding of the subject.

5.1.7.3.3 Phase Three Recommendations (180 Day Horizon)

Over time, the user flow MAY evolve into the following steps:

1. Traveler:
    1.1. Downloads app
    1.2. Registers appropriate information (including flight details, if not connected via API from airline booking system)
    1.3. Receives specific test requirements for trip (via API connection to TravelDocs or Timatic, etc.)
    1.4. Links to booking platform for test centre / lab to schedule test
    1.5. Goes to test centre
2. Health authority:
    2.1. Uses verifier app and verifies identity document (in person, not remote)
    2.2. Performs test and pushes health credential or health pass to individual's digital wallet app
3. Digital wallet app pushes health pass to (or is pulled by) departure control systems for clearance to fly
4. Individual
    4.1. Stores their results on app
    4.2. Has the ability to print a digitally signed health credential or health pass.

5.1.8 Zone 3: Presenting and Verifying a COVID-19 Health Pass

5.1.8.1 Problem Description

Travelers, especially internationally, will need to present different identity and health information to different entities, both public and private, during their travel journey. This **MAY** require selective disclosure from one or more health credentials or passes to ensure compliance and to minimize the sharing of health data.

Each verifier **MUST** first **validate** the credential's **authenticity**, **integrity**, and **revocation status**. After validating the credential or pass, the verifier needs to determine if it meets their legal and/or business requirements. Compliance rules are subject to temporal, legal, and business considerations.

5.1.8.2 Good Health Pass Design Requirements & Considerations

Interoperability of health credentials and health passes in zone 3 includes the following considerations.

1. Travelers **SHOULD** be able to present multiple credentials (e.g. vaccine + test; test 1 + test 2; recovery + test).
2. All credentials **SHOULD** include adequate identity binding to support cross-border acceptance and improve the overall user experience.
3. Travelers **SHOULD** be able to perform verification digitally and/or remotely before their journey to reduce uncertainty and anxiety. Verification **SHOULD** include both non-stop and transiting flights. Verification outcomes **SHOULD** be bound to an authenticated identity so that subsequent verifications can be simplified to identity verification only (unless otherwise prescribed by higher assurance level verifiers, such as immigration / border authorities). Note that in this case, face-to-face verification of health credential or passes can be removed from day of travel, and the user journey is streamlined to reduce frictions and risk of infection.
4. Travelers **SHOULD** be able to minimize or completely avoid storing their personal data (e.g.,

identity, medical, itinerary, booking, membership, etc.), to third-party systems other than the source system and their decentralized digital wallet. When sharing is needed, it **SHOULD** be kept at a need-to-know level and user consent **SHOULD** be obtained.

In the previous two zones, the focus was on ensuring healthcare institutions and travelers have easy access to methods of creating and storing COVID-19 verifiable credentials. In this zone, the focus is on creating a seamless experience for the traveler while at the same time enabling the verifier to verify that the traveler meets the applicable entry requirements.

In the use case of international travel, what does the journey on the date of travel look like?

5.1.8.2.1 Travel through the airport on departure

Most checks on health requirements – paper or increasingly digital – are carried out primarily by the airline agent. Often, they will use the same sources used by travelers when planning their journeys. However it can still take considerable time to navigate through these checks, especially for travelers with connections where two or more rule sets must be checked.

Some health pass providers are providing apps for airline agents to speed this up. In addition, they may use a rules engine to generate a "green tick" on a mobile boarding pass or other boarding document to negate the need for the airline agent to perform this check. Passports are often used as the identity check, with different levels of identity binding with health certificates depending on the source.

Ideally these checks are done prior to arrival at the airport as part of "at home check-in". This also has the benefits of:

- Assuring travelers they have met the requirements prior to travelling to the airport;
- Enabling travelers to use self-service machines, returning airport processing times back to pre-pandemic levels.

5.1.8.2.2 Arrival at destination border-entry

Upon arrival of the traveler, border control authorities in the arrival country **MUST**:

- Verify immigration eligibility
- Check health status and ensure that the COVID-19 credentials meet their entry requirements.

This usually duplicates the departure checks by airlines, but unfortunately there is no information flow between airlines and border control authorities. As with the airport departure systems, many of the automated machines for processing arrivals have not been put into place yet. However self-service is increasingly being integrated into airline and airport processes, and in some cases this includes privacy-preserving biometric verification.

5.1.8.3 Recommendations

For COVID-19 credential sharing and verification to contribute to the safe re-opening of international travel, healthcare providers, technology intermediaries, airlines, airports, and border authorities need to collaborate in an open, interoperable way to effectively protect public health and safety, while preserving data privacy. If such an alliance comes to fruition, there is a meaningful opportunity to show the potential of international, cross-industry cooperation to tackle this challenging global issue.

5.1.8.3.1 Overall Recommendations

1. Members of the Good Health Pass digital trust ecosystem **SHOULD** whenever possible focus on the issuance and verification of a health credential or pass prior to arrival at an airport by enabling back-end system integration.
    1.1. Whenever possible, this back-end system integration **SHOULD** verify the same health credential or pass as a native or independent verifier.
2. To meaningfully benefit global travel, credential presentation **MUST** be as lightweight, frictionless, and intuitive as possible.
3. Given the possible unreliability of airport wi-fi (or wi-fi anywhere while traveling), the amount of data needed by the traveler to download their digital pass as well as the amount of data needed by the verifier to validate that pass **SHOULD** be kept to a minimum.
4. Verifiers **MAY** employ rules engines and/or decision support systems. There are two primary options for credential verification and validation against a set of rules:
    4.1. **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).
        4.1.1. 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).
        4.1.2. The US Transportation Security Administration (TSA) **MAY** then verify and validate this CDC-governed credential at the point of departure.
    4.2. **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.
        4.2.1. For example, a travel app **MAY** accept a travel itinerary as input, consult the rules engine, and return the COVID-19 test and/or vaccination requirements for that trip.
        4.2.2. Once a passenger has obtained the COVID-19 health pass(es) necessary to meet these requirements, the rules engine **MAY** then issue a secondary credential – a travel pass – that the traveler can use for that journey.
5. Verification **MAY** occur natively (e.g., a digital health pass has an associated verifier that can authenticate its own credential), or independently (e.g., a third-party verifier can authenticate multiple different passes without issuing or holding a pass itself).
6. The recommend methods for requesting and presenting health passes are summarized in the following table:

	Sharing Credential Method	*Verification Methods*
Share QR code	QR codes **MAY** be produced on paper or by a mobile device and presented to verifying institution; QR codes **MAY** be uploaded in advance for either digital or manual verification; QR Codes **MAY** be scanned and ingested by an independent	*Read / scanned and verified by independent verifier, native verifier or human sight*

	verifier to get accepted or to be combined with info (e.g. identity, declaration) for entry check.	
NFC	**MAY** be used by a mobile wallet to transmit the credential to the verifier.	*Verifying institution needs a corresponding app to receive the credential for verification*
In-app	Apps **MAY** ingest a credential or pass designed from a digital or physical health record source (e.g., an airline trip management app). With user consent, ingested credentials or passes **MAY** be passed to 3rd parties (e.g. verifier, rule engine, notary, government) for relevant processing.	Verification is performed by checking the ingested credential / pass against a rules engine embedded in-app
Manual verification	QR codes **MAY** be produced on paper or by a mobile device and presented to verifying institution;	Verified by sight from trusted digital health passes
Integrated system	**MAY** perform pre-boarding verification of health credentials or passes for travel status verification prior to ticketing or boarding pass issuance	

5.1.8.3.2 Phase One (30 Day Horizon)

1. Governing authorities, travel authorities, and health pass implementers **MUST** make a joint, concerted effort toward educating health authorities about the use of digital credentials and passes, especially in the context of international travel during the COVID-19 pandemic.
2. In turn, governing authorities, travel authorities, and health pass implementers **MUST** work closely with healthcare providers to ensure that proposed solutions are designed with public health objectives in mind and do not exacerbate underlying inequities in healthcare delivery. This will pave the way for greater adoption of digital credentials needed to optimize the efficiency and effectiveness of digital credentials for international travel – both for travelers and verifying institutions (airlines, border authorities).

5.1.8.3.3 Phase Two (90 Day Horizon)

1. Members of the Good Health Pass digital trust ecosystem **MUST** undertake a collaborative effort

to obtain feedback from health authorities, travel authorities, and verifiers about operational feasibility and problem-solving.

2. Additionally, during this period, GHP-compliant ecosystems **MUST** improve the interoperability of health pass solutions by continuing the development of standards and systems to build momentum towards adoption.

5.1.8.3.4 Phase Three (180 Day Horizon)

1. Health pass implementers **MUST** consider solutions that will enable travelers and verifiers to return as closely as possible to pre-COVID user experiences, including restoring online check-in, and shorter counter check-in times.
2. Health pass implementers **SHOULD** explore how Good Health Passes could be used for proof of vaccination status in other travel-related use cases.

5.1.9 Additional Recommendations

The following are recommended requirements or features for future versions.

1. Aggregating family or traveler companion passes
2. Management of journey-specific health passes required by different jurisdictions (e.g., managing a pass for the EU and a pass for Singapore as part of one journey)
3. Single vs. multiple health passes within a user wallet
4. Priority travel experience for holders of digitally verifiable credentials via airline, immigration, or verifying institution express lanes

5.2 Recommendation #2: Security, Privacy, and Data Protection

5.2.1 Introduction to this Interoperability Challenge

All stakeholders in the Good Health Pass Collaborative (GHPC) digital trust ecosystem need to be confident in the security and privacy of the ecosystem.

The GHPC seeks to put individuals in control of their personal data – including health attributes – which they can selectively disclose for a specified purpose and duration. In order to achieve this aim, we have chosen to adopt a decentralized identity architecture which prioritizes privacy and personal data control.

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.

In some jurisdictions, these protections are already required by existing data protection regulations; in other cases, policy makers and regulators may seek to pass new legal and regulatory requirements to enshrine them in law.

5.2.2 Objective of this Drafting Group

The objective of this Drafting Group is to provide Privacy by Design and Secure by Design recommendations for Good Health Pass (GHP) solutions for international travel, and that are potentially extensible to other use contexts.

Privacy by Design places the individual at the center of the data exchange and takes into account privacy and data protection across the ecosystem and throughout user journeys, from point of issuance to point of verification. It includes all ethical, legal, operational, and technical considerations relevant to GHP design choices and default settings (i.e. Privacy by Default).

Secure by Design comes hand in hand with Privacy by Design and is a key requirement for GHP solutions. By "Security by Design" we mean an approach to information security which, like Privacy by Design, is at once holistic, creative, anticipatory, interdisciplinary, robust, accountable and embedded into systems. It stands in direct contrast to "security through obscurity," which approaches security from the standpoints of secrecy, complexity or overall unintelligibility.

This Drafting Group also provides practical advice and direction to help bring these principles into the processes and architectures used in the creation of GHP-compliant credentials and passes. These will need to be applied within the specific regulatory jurisdictions and contexts wherein those credentials and passes will be used.

5.2.3 Problem #1: What legal frameworks apply?

5.2.3.1 Problem Description

There has been a proliferation of privacy, data protection and information security laws globally over the last few years. Most notably, in the European Union (EU) the General Data Protection Regulation (GDPR) 2016/679, which has been in force since May 2018, triggered a trend for a number of countries and jurisdictions globally to reconsider their privacy and data protection legal frameworks. As a result of that, a

number of new privacy laws of general applicability have emerged, such as the California Consumer Privacy Act (CCPA) and the Lei Geral de Proteção de Dados Pessoais (LGPD) in Brazil. As of the end of 2020, there were hundreds of bills that address privacy, cybersecurity and data breaches that were pending across the 50 states, territories and the District of Columbia in the US.

Besides data protection laws of general applicability, we also observe sectoral legislation aimed at protecting individuals' privacy, such as the Health Insurance Portability and Accountability Act (HIPAA), along with other general legal frameworks with possible application to the collection and use of vaccination-related data.

Interoperable GHP solutions may be challenged by the proliferation and complexity of existing and evolving privacy and data protection law.

5.2.3.2 Recommendations

GHP-compliant solutions for international travel **MUST** comply with the principle of lawfulness. Lawfulness means that a legal basis exists for the processing of personal data in connection with the issuance of health credentials and passes, and for the purposes of collection and further processing of data related to vaccination, testing, credentialing and identity binding.

GHP-compliant solutions may be subject to one or more legal instrument which may be sector specific (e.g., a government law on health passes) or horizontal (e.g. the GDPR, the CCPA), depending on how the data processing activities fall into their legal territorial (or extra-territorial) scope. GHP-compliant solutions **MUST** comply with applicable law(s).

In some cases there may not exist specific laws regulating the use of health credential and pass solutions. In such cases, GHP solutions **MUST** comply with generally applicable law.

While privacy and data protection laws vary and take into account unique legal, geographical, sectoral and cultural specificities, such laws generally embody certain common principles.

If there is no privacy and data protection law in a jurisdiction in which a GHP-compliant solution is deployed, then that solution **SHOULD** take into account globally-recognised privacy and data protection principles, in order to ensure a minimum baseline for protecting individuals' data privacy and data protection.

GHP solutions **SHOULD** comply with the following globally-recognized privacy and data protection principles:

- Lawfulness
- Consent
- Data minimization
- Retention requirements for data and technology
- Assurance of data quality
- Information security
- Purpose specification and use limitation
- Transparency
- Personal control and privacy rights
- Auditability and Accountability

5.2.4 Problem #2: Consent

5.2.4.1 Problem Description

There is significant public, policy and regulatory debate on whether health credentials and passes should be mandated for public health purposes.

Mandates for health credentials and passes may not only interfere with fundamental human rights, such as equality and privacy, but may be inconsistent with data protection law.

Regardless of whether the issuance of health credentials and passes will be mandatory or not, there is a risk that processing of personal data in the context of health passes may take place without individuals' control. Therefore, user consent is needed for the creation of health credentials and passes.

5.2.4.2 Good Health Pass Design Requirements & Considerations

Primary considerations for this section include how consent manifests in the different zones, and the attributes of consent that would constitute "good" informed consent.

5.2.4.3 Recommendations

The processing of personal data in the context of GHP international travel solutions **MUST** have a legal basis.

For instance, under the GDPR, GHP-compliant solutions that process information relating to vaccination or test status **MUST** satisfy the requirements of consent (Article 6 GDPR) and special category data (Article 9 GDPR).

Valid consent means that the consent **MUST** be informed, specific, explicit and free.

Consent	**Zone 1**	**Zone 2**	**Zone 3**
Informed	Process **MUST** be put in place to allow individuals to consent to the issuance of a credential with COVID-19 health status information.	Process **MUST** be put in place to ensure that individuals consent to how their data is processed, used, retained and shared in the context of issuing a credential and binding it to an identity or for use in a health pass unless applicable law provides alternative legal grounds of processing personal data (e.g., the GDPR).	
Specific	Individuals **MUST** consent to issuing a credential with COVID-19 health status information specifically AND to the use of their data by a specific entity or entities for that specific purpose.	Consent **MUST NOT** be obtained in a vague manner for a number of undefined purposes. To the extent that Zones 2 and 3 involve biometric data for authentication purposes, for instance for credentialing or binding purposes, consent **MUST** be obtained specifically, unless otherwise permitted by applicable law	
Explicit	Individuals **MUST** take an affirmative action to proceed to vaccination or testing in connection	Consent to the processing of health data **MUST** involve an affirmative action.	

	with the issuance of a health credential.	Consent to the processing of biometric data **MUST** involve an affirmative action, unless otherwise permitted by applicable law.
Free	Free consent means that individuals **MUST** be provided with a number of valid alternatives. These **MAY** be: vaccination, testing or proof of recovery from Covid-19. In Zone 1, free consent **MUST** include a possibility to withdraw, (e.g., an individual decided to withdraw from a vaccination list).	Individuals **MUST** be able to withdraw consent at any point after consenting to the processing of their personal data. Digital GHP solutions **MUST** provide an easily accessible "withdraw consent" functionality in the user experience.

5.2.4.4 Recommendations

- The issuance of GHP solutions **MUST** rely on individuals' consent.
- The processing of personal data in the context of GHP health credential and pass solutions **MUST** rely on consent unless otherwise permitted by law.

5.2.5 Problem #3: Data minimization

5.2.5.1 Problem Description

Issuance and maintenance of health credentials and passes is an intrinsically data-driven activity that involves the processing of sensitive personal health data.

It may involve the processing of biometric data (like matching a photograph) which is also considered sensitive in several jurisdictions.

The development and deployment of health credential and pass solutions faces the risk of collecting or storing more data than is strictly necessary.

Importantly, it is essential to apply the principle of selective disclosure of information and avoid identifying individuals directly when identification is not required to verify health status.

5.2.5.2 Good Health Pass Design Requirements & Considerations

Data minimization plays an important role in terms of privacy, and there are several different techniques that can be used, often in conjunction with one another, to accomplish the goals of data minimization. This section considers those different approaches.

GHP solutions **MUST** comply with the principle of data minimization. Data minimization means that personal data processed, used, stored, and shared in health credential and pass solutions **MUST** be limited to what is absolutely necessary for a specific purpose (e.g., vaccination or testing, credentialing, identity binding and authentication).

5.2.5.3 Recommendations

GHP solutions **MUST** comply with the principle of data minimization.

GHP data minimization design practices **MUST** be considered as part of the GHP solutions design as follows:

1. GHP solutions **MAY** collect personal data and **MUST** store and/or retain the minimum amount of personal data possible.
2. GHP solutions **MUST** rely on the storage of anonymized/de-identified data to the extent feasible.
3. GHP solutions **MUST** consider whether anonymized/de-identified data stored in their systems still qualify as personal data and are subject to the requirements of applicable privacy and data protection law.
    3.1. This will be the case when information which has been de-identified or anonymized can still be linked back to an individual.
    3.2. In some jurisdictions (e.g., GDPR) the mere possibility to re-identify an individual when adding or combining information between different entities, even if an entity has no such ability on its own, renders the data personal.
4. GHP solutions **MUST** put appropriate measures in place to prevent re-identification when re-identification is not absolutely essential.

5.2.5.4 Identity binding and data minimization

While health credentials for international travel **MAY** contain more personal data (including personally identifiable information and protected health information) than GHP-compliant health passes, to implement the appropriate level of data minimization the assurance level required by the context of a specific use case **MUST** be considered. The following table explains the approach for GHP-compliant health passes used in international travel:

Use case	**Assurance Level**	**Data minimization**
Boarding a plane or a train	Need to bind an identity with a traveller	GHP-compliant health passes **MUST** bind the traveller to the pass. The pass **SHOULD** be a "Yes/No" or "Traffic Light" factor indicating eligibility to board a plane or a train. Passes **SHOULD NOT** collect or disseminate information about the date and time of a COVID-19 test OR the date, time and type of vaccine.
Crossing the borders	Need to be able to perform legally required border control checks	GHP-compliant health passes **MUST** bind the traveller to the credential. The pass **MUST** contain the minimum required information to perform legally required border control checks. In accordance with applicable law, it **MAY** involve more information compared to the case of boarding a plane or a train, for example, date and time of taking a COVID-19 test.

In use cases other than international travel, however, the principle of data minimization could be applied to entirely avoid the binding of individual identity to health passes. For example, a health pass solution used in public entertainment venues could employ a "Yes/No" or "Traffic Light" system to validate an individual's eligibility to enter a particular venue, and by doing so preserve anonymity by avoiding the need to bind individual identity to the pass.

5.2.6 Problem #4: Purpose specification and data use limitation ("Purpose Limitation")

5.2.6.1 Problem Description

Data protection laws generally require that entities collect and use an individual's personal data for the specific purposes for which that information will be used. Function creep, which can occur when the principle of purpose specification and data use limitation is not respected, can give rise to significant risks (for example, unjustified surveillance).

GHP solutions that collect personal data in connection with international travel **MUST** clearly explain the expected use purposes to the individual at the time the personal data is first collected and/or consented to, and also document the fact of the entity's disclosure of these purposes. Moreover, health credential and pass solutions **MUST** obtain consent if they decide to use the individual's personal data for a new purpose not originally disclosed, unless the purpose is otherwise duplicative or allowed by applicable law.

Without a basis for using the data for a new purpose, the entity **MUST** use the data solely for the purposes originally disclosed. Adherence by GHP solutions providers to the purpose specification and data use limitation principle prevents "function creep".

The requirements of purpose specification and data use limitation pose particular challenges for GHP-compliant solution providers: the operation of health passes necessarily implies not only the storage of individual health status information by credential issuers, but also downstream access by health pass verifiers to some portion of that health status information (depending on the requirements of the context in which the pass is presented).

Accordingly, responsibility for appropriate communication of data use **SHOULD** be shared across the "chain" of entities enabling the functionality of health passes; GHP health credential solutions **MUST** ascertain that they have defined and clearly communicated the purposes of data collection intended to support downstream use by health pass verifiers.

5.2.6.2 Good Health Pass Design Requirements & Considerations

GHP solutions for international travel **MAY** collect and process personal data for specific purposes, which include the validation of verifiable credentials and passes, as well as necessary system-level audit processes. However, GHP solutions **MUST NOT** collect, share or sell such personal data for marketing or advertising purposes.

In addition, GHP solutions **MUST NOT** use collected personal data for new and previously undisclosed purposes without appropriate safeguards. Prior to enabling new internal or external personal data uses, GHP solutions **MUST** perform a secondary purpose compatibility assessment, i.e. an assessment of whether a new data use is compatible with the original purpose for which the data was collected.

Subject to applicable data protection law, safeguards to ensure purpose specification and data use limitation **MAY** be the individual's explicit and informed consent, the description of each purpose of data usage in the privacy notice, and performing a secondary purposes compatibility assessment. Purposes of use of personal data **MUST** be clearly communicated to the individual.

In **Zone 1**, to the extent that a health organization is gathering data in connection with vaccination or health status that is intended to be used for the creation of GHP health credentials, such an organization **MUST** comply with the purpose specification and data use limitation principle, either at the time of delivery of vaccination or health evaluation, or at such time as access to the health-related data for an individual is first enabled for use in connection with a GHP solution.

In **Zones 2 and 3**, issuer and verifier solutions **MUST** comply with the principles of purpose specification and data use limitation for the use of individual health data in a GHP solution, unless such use has been previously disclosed or is compatible with prior disclosures.

5.2.6.3 Recommendations

1. To assist GHP solutions providers in ensuring that the principle of purpose specification is adequately addressed, model disclosures (or checklists of data purposes disclosures) **MAY** be developed for GHP credential and pass solutions providers in **Zone 1**, **Zone 2**, and **Zone 3**.
2. GHP solutions providers in **Zone 3 SHOULD** also conduct reasonable diligence to ascertain that where feasible, providers earlier in the "chain" of services necessary to support the issuance and verification of health passes for international travel have disclosed the expected purpose of uses of individual health status data for presentation to **Zone 3** GHP solutions providers.
3. GHP solutions **MUST** perform a secondary purposes compatibility assessment before new internal or external data uses are allowed.
4. GHP solutions providers **SHOULD** limit disclosure of health-pass related data to public authorities to the circumstances in which such disclosure is compelled by law or other appropriate legal process.

5.2.7 Problem #5: Retention requirements for data and technology

5.2.7.1 Problem Description

In addition to data minimization requirements, data protection laws generally prescribe that personal data shall be retained only as long as necessary to fulfill the purposes for which it is collected.

This principle of limited retention applies to the storage of personal data collected in connection with GHP solutions, and should be considered by any entity involved in the collection and use of such data in the credentialing and presentation process.

In addition, certain jurisdictions in which health passes are used may implement specific retention requirements tied to the type of health data stored within digital health pass technology. Just as a government may exercise the power to declare the onset – and conclusion – of a public health emergency relating to a particular disease, a government may also choose to define the appropriate retention of personal health data relating to that disease.

A government's declaration that a public emergency has "ended" may affect not only the retention of individual data stored within health pass technologies, but may also affect the conditions on which the technology underlying the health pass may continue to be lawfully maintained in that particular marketplace.

At the same time, to the extent that individuals have a legitimate interest in maintaining information relating to their prior health condition or vaccination as an element of their individual medical histories,

due consideration **MUST** be given to that individual interest in technologies used to support health credentials, to the extent consistent with applicable law.

5.2.7.2 Good Health Pass Design Requirements & Considerations

Personal data, including pseudonymous data, collected or used by GHPC entities in connection with GHP solutions for international travel **MUST NOT** be retained longer than the maximum duration permitted by governing data protection law in the relevant jurisdiction (including laws applicable to the retention of public health data), and **MUST** be deleted in the event of any superseding determination by a competent authority foreclosing the retention of specific categories of GHP-related data within certain technologies (such as a requirement for deletion of COVID-19-related health data following declaration of the end of the pandemic).

5.2.7.3 Recommendations

1. Providers of GHP solutions **MUST** comply with all relevant retention limitations for health status–related data. Providers of GHP technologies **SHOULD** apply the general principle that retention of individual data collected or used in connection with health passes will be limited to the strict minimum necessary. Personal data **MUST NOT** be retained without a specifically defined purpose.
2. Providers of GHP technologies **MAY** consider the de-identification or anonymization of health pass-related data in their data retention strategy. It **MAY** be justifiable to retain de-identified data longer than a full data set, whereas fully anonymous data in line with applicable law will not be subject to the data retention principle (recognizing that the threshold for full anonymization of data is very high in some jurisdictions and may only be met if it is impossible to link information back to an individual with any reasonable means).
3. As part of their application of the principle of Privacy by Design, providers of GHP solutions **SHOULD** design their technologies to anticipate the possibility that governments may impose particular retention requirements for certain categories of disease or health condition data (to the extent that a decentralized data architecture does not independently address this requirement).
4. For providers in both **Zones 2 and 3**, retention of personal data related to the locations in which that individual presents a health pass **MUST NOT** be retained in the absence of a specific legal requirement for such retention that is appropriately related to the use case in which it arises (for example, retention requirements for international travel).
5. Providers of GHP solutions **MUST** publicly disclose their data retention policies.

5.2.8 Problem #6: Data quality

5.2.8.1 Problem Description

A common principle across global data protection laws is data quality.

It is the notion that personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, it should be accurate, complete and kept up-to-date.

Data quality clearly links to the right to rectification, which gives individuals the right to have inaccurate personal data corrected.

Data quality is especially relevant for data-driven solutions such as health passes, as their value and efficiency derives from the quality and accuracy of the information they contain.

Another challenge that the principle of data quality intends to address is that personal data may be amended over time (for example, an individual may change their legal name after marriage).

Additionally, data may be lost, stolen, tampered or outdated.

5.2.8.2 Good Health Pass Design Requirements & Considerations

1. GHP solutions **MUST** take steps to keep personal data accurate and up-to-date and ensure that personal data is not incorrect or misleading.
2. In **Zone 1**, the quality of data used in health credentials is a responsibility of the health organization performing the vaccination or testing per their usual privacy and data protection practices. Robust identity binding is key to ensure the accuracy of the personal data in **Zones 2 and 3** for use in international travel.
3. GHP solutions **MUST** allow individuals to obtain, renew or update their credentials and passes free of charge. The credential/pass, as well as its history of modifications, **MUST** be issued upon request of the individual.

5.2.8.3 Recommendations

GHP solutions **MUST** comply with the principle of data quality and make sure that personal data is accurate, complete and kept up-to-date.

Participants in the GHP ecosystem **MUST** take all reasonable steps to achieve this by allowing individuals to update or issue new certificates in case their data is not accurate or up to date anymore or the certificate is no longer available to them (for example in case of loss, damage or theft).

5.2.9 Problem #7: Transparency

5.2.9.1 Problem Description

Health pass ecosystems are often characterized by complexity.

The number of actors, the sophistication of technology solutions as well as the type of governance involved are not immediately obvious or intuitively understood by the majority of the non-expert population using health passes.

This creates a major transparency challenge about personal data collection and usage in all three GHP zones, notably, at the stages of issuing, maintaining, binding identity, and authentication.

5.2.9.2 Good Health Pass Design Requirements & Considerations

GHP solutions **MUST** take steps to explain how they process personal data in a clear and simple manner.

In connection with international travel, GHP solutions **MUST** clearly outline their processes and provide individuals with information on the type of processing that is taking place and who is carrying it out.

At a minimum, this information **MUST** include:

1. Who is the entity processing the personal data
2. Who is the entity the user is agreeing to give access to their data
3. Why is the personal data processed including all relevant data usage purposes

4. If applicable, what legal basis an entity relies on to perform the data processing
5. Whether or not the personal data will be disclosed to other entities
6. How long the personal data will be stored
7. The existence of the individual's rights, including in particular, the right to access, correction, erasure, restriction, objection and portability to the extent applicable
8. The business model of the processing entity **MUST** be declared when joining the GHP Ecosystem Governance Framework

5.2.9.3 Recommendations

In light of the requirements in the previous section, GHP solutions **MUST** take reasonable steps to provide transparency in the clearest manner possible.

1. In **Zone 1**, the health organization performing the vaccination or testing in connection with health credentials **MUST** inform individuals in a clear and plain language of how their information will be processed by them.
2. In **Zones 2 and 3**, the issuer of the GHP solution as well as the verifier **MUST** also provide plain and clear information on how they process personal data.

Information about GHP solutions **MUST** be provided in layers or using visuals, in order to be understandable to different types of audiences and comply with applicable guidelines for accommodating disabilities. In addition, information contained in GHP solution certificates **MUST** be shown in human-readable form.

5.2.10 Problem #8: Information Security

5.2.10.1 Problem Description

Because GHP solutions for international travel will be dealing with personal data, including sensitive health data, information security is extremely important not just in each of the zones, but also in the boundary crossings between zones.

Data needs to be protected both in transit and at rest.

While specific standards and regulations vary across the globe, to achieve Security by Design, it is expected that actors in each zone are following local laws and regulations, and that information security best practices are being applied.

5.2.10.2 Good Health Pass Design Requirements & Considerations

The requirements and considerations will look at data and the different actors involved. In addition to the issuer–holder–verifier trifecta, we'll also look at organizations that either manually or automatically convert certificates to passes external to the holder ("intermediaries" herein).

Paper-based credentials and passes have their own special considerations. The same security requirements are in effect for issuers and verifiers regardless of the form of the issued credentials or passes. For the holder-specific parts of these requirements, we will focus on the non-paper formats.

1. Data at rest
   - 1.1. All credential and pass data, whether or not it is considered personal data, **MUST** be encrypted at rest.
   - 1.2. The security scheme protecting encrypted data **MUST** be separate from the security scheme protecting its encryption keys.
   - 1.3. Data at rest **MUST** be encrypted using strong encryption techniques as defined by jurisdiction-specific standard bodies.
2. Data in transit
   - 2.1. Data transiting between zones, whether or not it is considered personal data, **MUST** utilize end-to-end encryption.
   - 2.2. Transiting data **MAY** have multiple encryption "wrappers" applied while in transit.
   - 2.3. End-to-end encryption keys **MUST** be unique to the actors participating in the transmission.
   - 2.4. Nonces **SHOULD** be included in the data transmission approach to avoid replay attacks.
3. Issuer-specific requirements and considerations
   - 3.1. Medical issuers **MUST** have regulatory or other legitimate reasons for data retention.
   - 3.2. Issuers **SHOULD** be aligned with relevant, well-accepted information security standards such as ISO/IEC 2700x and 2910x.
   - 3.3. Issuers **MUST** publicly disclose the information security and privacy standards and guidelines that they are following.
   - 3.4. Issuers **SHOULD** publicly disclose their information security policies.
   - 3.5. Issuers **MUST** publicly disclose their credential issuance policies.
   - 3.6. GHP solution providers **SHOULD** ensure logging of events such that no personal data is captured or retained.
   - 3.7. All system-level or debugging logs **MUST** be sanitized of any and all personal data to the extent feasible. If logs qualify as personal data under applicable law (e.g., under the GDPR), GHP solutions **MUST** take steps to remove any personal data directly identifying individuals. (e.g., sanitization).
   - 3.8. Issuers **MUST** create and maintain an information security threat matrix, which **SHOULD** be reviewed quarterly.
   - 3.9. Issuers **MUST** perform a Risk Assessment including an information security threat matrix annually.
   - 3.10. Issuers **MUST** perform internal and external security audits of their information infrastructure.
4. Digital wallet app–specific requirements and considerations
   - 4.1. Digital certificates and passes **MUST** be stored securely.
   - 4.2. Digital certificates and passes **MUST** be accessible via multiple modalities (digitally, online, offline or paper based).
   - 4.3. Digital wallets **MUST** segregate users (e.g., parent and child) so that digital certificates and passes cannot be intermingled.
   - 4.4. Digital wallet apps **SHOULD** take advantage of "secure enclaves" when available on the device to store cryptographic key material.
   - 4.5. Solutions **MUST** provide a mechanism for the user to audit what data they have shared with whom.
   - 4.6. All system-level or debugging logs **MUST** be sanitized of any and all personal data to the extent feasible. If logs qualify as personal data under applicable law (e.g., under the GDPR), GHP solutions **MUST** take steps to remove any personal data directly identifying individuals.
   - 4.7. Digital wallet app vendors **SHOULD** publicly disclose their information security policy.

4.8. Digital wallet app vendors **MUST** create and maintain an information security threat matrix, which **SHOULD** be reviewed quarterly.
4.9. Digital wallet app vendors **MUST** perform internal and external security audits of their information infrastructure.

5. Verifier-specific requirements and considerations
5.1. Verifiers **MUST NOT** possess the provided personal data for more than the minimum time required to provide the granted benefit, unless otherwise required by law or regulation.[1]
5.2. Display of personal and sensitive health data during the verification process **SHOULD** minimize the possibility of visual eavesdropping.
5.3. Verifiers **SHOULD** be certified under a relevant GHP-compliant scheme such as well-accepted information security standards like ISO/IEC 2700x and 2910x.
5.4. Verifiers **MUST** publicly disclose the information security standards and guidelines that they are following.
5.5. Verifiers **SHOULD** publicly disclose their information security policies.
5.6. All system-level and debugging logs **MUST** be sanitized of any and all personal data to the extent feasible. If logs qualify as personal data under applicable law (e.g., under the GDPR), GHP solutions **MUST** take steps to remove any personal data directly identifying individuals.
5.7. Verifiers **MUST** allow holders to exercise the right to be forgotten.[2]
5.8. Verifiers **MUST NOT** share personal data, including sensitive health data gathered from holders without the holders explicit, informed consent,. (See also consent section).
5.9. Verifiers **MUST** create and maintain an information security threat matrix, which **SHOULD** be reviewed quarterly.
5.10. Verifiers **SHOULD** perform internal and external security audits of their information infrastructure.

5.2.11 Problem #9: Personal Control and Privacy Rights

5.2.11.1 Problem Description

Privacy is not about secrecy; it's not about having something to hide. Privacy is all about control – personal control over the use and disclosure of one's personal data. Only the individual knows the context associated with the data involved – its sensitivity or lack thereof. Therefore the individual **MUST** be the one to determine the fate of his or her personal data; the individual **MUST** be able to exercise control over its use and disclosure.

Individual rights of control over one's personal data encompass both control over the integrity of that data and control over the manner in which such data is accessed by others. With respect to the integrity of individual data embedded in health passes, GHP solutions providers **MUST** ensure data quality, and **MUST** also address individual rights to access, correct and delete information.

In circumstances in which a GHP solutions provider cannot provide rights of access and correction directly (for example, where a **Zone 2** or **Zone 3** solution provider receives information downstream from the original creator of a health data record in **Zone 1**), the solutions provider **SHOULD** provide access to an appropriate mechanism to request such correction from the original creator.

---

[1] See also the earlier section on retention requirements for data and technology.
[2] See also the next section on personal control and privacy rights.

With respect to control over the sharing of individual data embedded in health passes, GHP solutions providers' adherence to the principle of Privacy By Design ensures that individuals benefit from a variety of protections, ranging from de-centralized storage of their data to the ability to selectively disclose what is shared with health pass verifiers. Rights of deletion, however, remain fundamental: each GHP credential and pass solutions provider **MUST** allow for the deletion of personal health pass information held by that provider, unless such deletion is prevented by applicable law.

Finally, control of individual data also encompasses portability rights. GHP health credentials and passes are designed to be "portable", with users able to present them to different verifiers. Nonetheless, each GHP solutions provider should evaluate on a continuing basis the technical feasibility of individual rights of portability with respect to the particular personal data stored by that provider.

5.2.11.2 Recommendations

1. Individuals **MUST** retain control of their personal data in GHP-compliant health credential and pass solutions for international travel.
2. Individuals **MUST** be able to exercise their rights to access and correction of personal data contained within GHP solutions, or be provided appropriate mechanisms to request such access and correction.
3. Individuals **MUST** be able to delete their personal data within GHP solutions, unless such deletion is prevented by applicable law.
4. GHP solutions providers **SHOULD** address individual rights of portability by evaluating the technical feasibility of portability mechanisms or evaluating how portability addresses such rights.

5.2.12 Problem #10: Accountability for security & privacy requirements

5.2.12.1 Problem Description

Accountability of GHP solutions providers means that all entities in the health pass ecosystem take responsibility for Privacy by Design and Security by Design and the recommendations provided in this document.

Accountability cannot be demonstrated without producing some form of pertinent and persuasive evidence that such requirements have been met.

The Privacy by Design and Security by Design requirements and recommendations cover a large number of areas with clear levels of compliance, including **MUST**, **SHOULD, MAY,** and their associated "negatives". There is no accountability from these recommendations without evidence.

In order to give evidence a number of activities need to take place which are described next.

It should be noted that accountability is an iterative process of developing and continuously assessing and improving evidence that GHP solutions comply with Privacy by Design and Security by Design recommendations.

5.2.12.2 Good Health Pass Design Requirements & Considerations

Good Health Pass solutions for international travel – in order to meet Privacy by Design and Security by Design requirements – create, execute, audit, and report on the following:

1. Risk Assessment Report, including legally required Privacy Impact Assessments or Data Protection Impact Assessments for solutions that collect personal data.
2. Code of Conduct Compliance
3. Consent Receipt Management Plan

Organizations **MUST** do self-assessments against the stated recommendations, and **MAY** publicly disclose the results of those assessments, as well as remediation plans, if any.

A thorough information technology risk assessment is a systematic analysis by an organization to ensure it considers the negative outcomes and threats under its purview. GHP solution providers **MUST** perform a risk assessment which **MUST** consider security and privacy risks. The privacy assessment **MAY** be in the form of a Data Protection Impact Assessment (DPIA) or if following ISO 29134 Privacy Impact Assessment (PIA). For information security assessment the ISO 27005 **MAY** be followed.

GHP solutions that collect personal data **MUST** conduct a Privacy Impact Assessment or a Data Protection Impact Assessment, when it is required by applicable law (e.g., GDPR).

GHP solutions **SHOULD** maintain proof that an individual has read a GHP privacy notice OR that they have provided consent for the processing of their personal data. An example demonstration to an individual of their privacy rights **MAY** be addressed in a consent receipt (see for instance the Kantara Consent Receipt Specification v1.1.0) which is equivalent to a privacy policy and captures the proof of consent to the individual, as well as helps demonstrate to authority that consent has been given.

Consent receipts are beneficial for a number of other reasons, including increasing transparency. They can serve as an evidence, notably In cases of invocation of rights (e.g., right to be forgotten).

If personal data is collected by the verifier, an additional consent **MUST** be presented to the individual.

5.2.12.3 Recommendations

1. GHP solutions providers **MUST** disclose the information security and privacy standards and guidelines that they are following.
2. A Code of Conduct self-assessment against the GHP requirements **MUST** be conducted and evidenced. An external assessor **SHOULD** be used to perform the assessment to provide an impartial review of the compliance.
3. **All Zones MUST** conduct a Data Protection Impact Assessment or Privacy Impact Assessment to ensure privacy risks are identified and mitigated.
4. **All Zones SHOULD** conduct a self-assessment to make sure data minimization requirements are met. **Zones 2 and 3** passes **MUST** be data minimized.
5. If **Zones 2 and 3** processes trigger applicable legal requirements (e.g., due to biometric data usage) a Data Protection Impact Assessment **MUST** be conducted to identify and mitigate privacy risks.
6. A privacy notice indicating the process to exercise privacy rights and how privacy information is processed, shared and protected **MUST** be given by the Issuer and Verifier.
7. For **Zone 1** an evidence of consent or privacy notice, such as a consent receipt, **SHOULD** be maintained and provided to the individual upon request. Similar evidence of consent or notice **MAY** be provided by **Zone 2 and 3** organizations.
8. Holders **MUST** have the ability to remove consent, where allowed by regulation, and this **MAY** take whatever form is allowed within the jurisdiction for consent revocation (e.g., via email, letter, or other means).

5.2.13 Additional Recommendations

The aforementioned requirements, considerations and recommendations provide a number of principles and practical steps to achieve Privacy by Design and Security by Design. Both are key prerequisites for GHP providers to accomplish their ultimate objective: to provide interoperable, effective, safe and secure GHP technology solutions that are privacy-protecting and place the individual at the center of the design. Ultimately, ensuring that equity and inclusion, privacy, fundamental human rights, and other civil liberties are protected is key to ensure the successful uptake of GHP solutions.

The Privacy by Design and Security by Design recommendations included in this document provide a robust framework for GHP solutions to achieve Privacy by Design and Security by Design. GHP providers **MUST** comply with all relevant security, privacy and data protection laws and regulations and **MUST** be designed and implemented to enhance privacy, support data minimization and other fundamental privacy and security principles.

Privacy by Design and Security by Design is a collective responsibility of all actors in the health pass ecosystem; privacy, data protection, and security is as strong as the weakest link of the entire ecosystem. Therefore it only works if all actors have the same vision on privacy, data protection, and security of data.

5.3 Recommendation #3: Identity Binding

5.3.1 Introduction to this Interoperability Challenge

For a health credential to be trustable at the point of presentation, the verifier **MUST** be able to determine the level of confidence that the presenter of the health pass is the legitimate subject of the health pass (i.e. is it really Jane Doe presenting Jane Doe's health status?).

This challenge may seem trivial for the credentials that are carried in wallets and purses to identify ourselves (e.g., driving licenses or passports). That is because we go through elaborate in-person identity proofing processes to obtain those credentials. As a result, those credentials end up carrying a great deal of personal data (e.g., name, address, birthdate, hair color, eye color) including biometric data (e.g., 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 any form of legally-recognized identity at all.

While the International Health Regulations recommend binding the identity of an individual to their International Certificate of Vaccination (or "yellow card") by their name, date of birth, gender, nationality and national identification document, in the context of the COVID-19 pandemic, few health authorities are mandating 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.

This raises critical questions about how best to manage identity proofing from the point of healthcare delivery through to point of presentation, and how best to mitigate risks associated with identity fraud.

5.3.2 Objective of this Drafting Group

This section provides recommendations for identity binding across three zones in the Good Health Pass (GHP) ecosystem. We also address identity disambiguation – the concept that not all issuers will know all verifiers' identity requirements – to enable a flexible framework for trust.

Identity authentication is performed by the health provider to capture the necessary identity binding data

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 bind the holder's identity to the verifiable credential

Figure 5: Identity binding and authentication zones in the Good Health Pass ecosystem

Specific identity binding challenges must be solved in each of the three zones:

1. In Zone 1, the GHP 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 electronic health record (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, GHP 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, GHP 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 GHP ecosystem **MUST** support:

- Low-tech or no-tech identity binding solutions alongside high-tech means.
- Options for supervised remote proofing using secure video conferencing services.
- 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, GHP-compliant credentials **MUST** be able to describe any level of identity proofing at the time of testing – from none to fully verified biometrics.

5.3.3 Background

Identity binding is the ability to link the presenter of an identity claim to the claim itself. In the context of verifiable health credentials this is typically done when:

5.3.3.1 Issuing an identity credential

In many instances this is a government function where an identity proofing process is used to:

- Resolve a claimed identity to a single, unique identity within the context of the population of users
- Validate that all supplied evidence is correct and genuine
- Validate that the claimed identity exists in the real world
- Verify that the claimed identity is associated with the real person supplying the identity evidence

The rigour of the identity proofing process is quantified in the Level of Assurance (LOA) (see ISO/IEC 29115, Section 8.1.2) and often correlates with the Identity Assurance Level of the credentials provided and their underlying identity proofing processes (refer to NIST 800-63A Section 4.7 or ISO 29115 Section 6.5 for examples of IALs).

Identity credentials with relatively high enrollment LOAs are jurisdictional ID cards and national passports where identity proofing is done in-person, typically with biometric identifiers to deduplicate within the population, and breeder documents are source-checked. Conversely, shoppers' affinity cards require a very low enrollment LOA. The acceptable enrollment LOA for an identity credential is a business decision based on the risk appetite of the relying party for the credential's primary purpose.

5.3.3.2 Presenting an identity credential to receive a service

In the context of verifiable health credentials, this **MAY** be at the point of vaccination or test, the border crossing point, at an employer's facility, at an educational institution, etc.

The viability of the verifiable health credential relies on the accreditation of the issuer AND their ability to authenticate the identity of the subject to the level required by verifiers.

Authentication, like identity proofing, has varying levels of assurance depending on the methods used. See ISO/IEC 29115 Section 6.5 for examples of Authentication LOAs or Assurance Levels.

Authentication processes with relatively high Authentication LOAs are in-person (or remote supervised). They **MAY** include one or more biometrics, and one or more cryptographic devices. Conversely, a 4-digit PIN corresponds to a relatively low Authentication LOA. The Authentication LOA best suited for authenticating an identity claim is a business decision based on the risk appetite of the relying party.

5.3.4 Levels of Assurance

ISO/IEC 29115 Entity Authentication Assurance Framework provides a framework for managing authentication assurance in a given context. In particular, it:

- specifies four levels of authentication assurance;
- specifies criteria and guidelines for achieving each of the four levels of authentication assurance;
- provides guidance for mapping other authentication assurance schemes to the four LOAs;
- provides guidance for exchanging the results of authentication that are based on the four LOAs; and

- provides guidance concerning controls that should be used to mitigate authentication threats.

There are four LOAs defined in **ISO/IEC 29115** which are:

LOA 1	There is minimal confidence in the asserted identity of the entity, but some confidence that the entity is the same over consecutive authentication events. This LOA is used when minimum risk is associated with erroneous authentication. There is no specific requirement for the authentication mechanism used; only that it provides some minimal assurance. A wide range of available technologies, including the credentials associated with higher LOAs, can satisfy the authentication requirements for this LOA. This level does not require use of cryptographic methods.
LOA 2	There is some confidence in the asserted identity of the entity. This LOA is used when moderate risk is associated with erroneous authentication. Single-factor authentication is acceptable. Successful authentication **SHALL** be dependent upon the entity proving, through a secure authentication protocol, that the entity has control of the credential. Controls **SHALL** be in place to reduce the effectiveness of eavesdropper and online guessing attacks. Controls **SHALL** be in place to protect against attacks on stored credentials.
LOA 3	There is high confidence in an asserted identity of the entity. This LOA is used where substantial risk is associated with erroneous authentication. This LOA **SHALL** employ multi-factor authentication. Identity proofing procedures **SHALL** be dependent upon verification of identity information. Any secret information exchanged in authentication protocols **SHALL** be cryptographically protected. There are no requirements concerning the generation or storage of credentials; they **MAY** be stored or generated in general purpose computers or special purpose hardware.
LOA 4	There is very high confidence in an asserted identity of the entity. This LOA is used when a high risk is associated with erroneous authentication. LOA 4 provides the highest level of entity authentication assurance defined by this standard. LOA 4 is similar to LOA 3, but it adds the requirements of in-person identity proofing for human entities and the use of tamper-resistant hardware devices for the storage of all secret or private cryptographic keys. Additionally, all personally identifiable information (PII) and other sensitive data included in authentication protocols **SHALL** be cryptographically protected.

Levels of assurance are described in other national and international standards documents including: 1) Pan-Canadian Trust Framework; 2) eIDAS; 3) the NIST 800-63 series; 4) the Trusted Digital Identity Framework; and 5) UK GPG-45. However, we will refer to the ISO guidance throughout this document, which can be mapped to other standards.

5.3.5 Case Study: Identity Binding for COVID Health Passes in the United Kingdom

Taking a high-level look at enrollment and authentication processes in the United Kingdom highlights how identity is used in healthcare today, both generally and in the context of COVID-19.

It is important to note that other countries' health care systems work very differently. Identity binding for health passes needs to operate within these different constructs.

5.3.5.1 Patient enrollment

Patients in the U.K. obtain first-line healthcare through a General Practitioner (GP). GP surgeries are private businesses contracted to the National Health Service through their local Clinical Commissioning Group. Patients are enrolled onto the list of their local GP surgery. While GPs will often ask for proof of identity and address, there is no formal requirement for identity verification. Indeed, GPs cannot decline to register a patient due to a lack of proof of identity or address[3].

Once enrolled, when attending an appointment in-person, the patient will be required to confirm their name and date of birth. Again, there is no requirement for identity verification nor any authentication other than matching the self-asserted information with the patient record.

5.3.5.1.1 Why is this important?

1. Vaccinations obtained in the course of public health programmes, such as the COVID-19 vaccination rollout, **MAY** have no demonstrable identity verification for some users.
2. Health pass providers cannot assume users have been rigorously authenticated at the point of care.

5.3.5.2 Digital Health Records

Patients are able to access online services such as:

- contacting their GP for advice and support
- ordering repeat prescriptions
- seeing parts of their health record, including information about medicines, vaccinations and test results
- seeing communications between their GP surgery and other services, such as hospitals
- booking, checking or cancelling appointments

There are two ways in which patients can enrol for access to online services.

1. They enroll for an NHS ID online by proving their ID using a government document – their verified data is then matched against their patient record, and they get credentials (username, password and mobile one-time passcode) for future access.
2. They go via their GP who registers them for online access, making the link to their patient record and issuing them with credentials for access.

5.3.5.2.1 Why is this important?

Credentials obtained from a health record should contain identity data that can be matched with the identity proofing undertaken by the health pass provider.

---

[3] https://www.nhs.uk/nhs-services/gps/how-to-register-with-a-gp-surgery/

5.3.5.3 COVID-19 Vaccinations

In the U.K., COVID-19 vaccinations are offered for free, with rollout prioritising the most clinically vulnerable. Patients are contacted by their GP surgery as, based on their patient record, they fall into the priority grouping being called forward on a national basis. Once invited, patients register either online or by phone giving their details to match to their patient record. Vaccinations are being provided through:

- local hubs covering multiple GP surgeries
- mass vaccination centres
- satellite locations in premises such as pharmacies

This means that for the majority of patients, they will be vaccinated somewhere other than the GP surgery they are registered at.

The NHS has produced a COVID-19 vaccination record card which is issued to the patient when they attend for their vaccination. The card acts as a reminder for their second appointment for a two-dose regime. It is not intended to be used as evidence of being vaccinated. The name of the patient is the only identity binding on the record. The name of the vaccine given, the batch number and the date given is recorded.

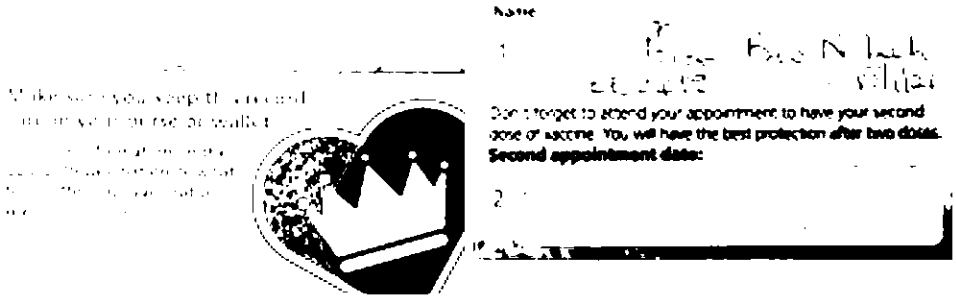

Figure 6: Vaccination card

As well as being provided with the physical card, the details are electronically recorded against their NHS patient record.

5.3.5.3.1 Why is this important?

1. The use of identity tools provided by health pass applications **SHOULD NOT** expect to be included within a public healthcare process.
2. Proof of vaccination **MAY** be obtained from the healthcare systems post the point of treatment.

5.3.5.4 COVID-19 Testing

Public health testing is available through an online or phone booking system. This is available through a network of testing centers offering drive-up or walk-up service, additionally home testing is provided by post. In areas with surges of cases or where new variants are of concern, testing with no prior appointment is also available. Patients applying online must provide their name, plus a mobile number to receive their results. An email address is also required for a home testing kit. Public health testing is not to be used for activities that require proof of a negative test.

Testing for proof of a negative result for international travel purposes is provided by the private sector. Governments have published criteria for providers of these tests to develop "Trust Lists" that passengers must obtain their test results from[4][5].

These private sector providers offer both in-person and at home testing services. The personal data required varies from provider to provider. Some require only limited contact information, name and email, where others also request passport details.

5.3.5.4.1 Why is this important?

1. Public health testing **SHOULD** be assumed to be for the identification of positive cases rather than proof of a negative test. Therefore, the requirements for identity binding **MAY NOT** be of primary concern should a credential be issued.
2. Health pass providers **MAY** need to provide the ability for private sector testing providers to authenticate the user of the Health Pass (e.g., by securely displaying a photo, name and date of birth of the user).
3. Private sector health providers **MAY** need to align their own identity proofing and authentication processes, where used, with those of the health pass providers.
4. Health pass providers **MAY** need to support the use of identification evidence related to the use case for which the credential is being obtained (e.g., a passport for a travel use case, a proof of age card for a hospitality use case, matching attributes such as name and age for an event use case).
5. Health pass providers **MAY** need to support facial biometric binding to the individual where the technology requirements allow to include those without provable identity.

5.3.5.5 Coronavirus testing before you travel to England

International arrivals to England (other nations within the U.K. may have different rules) are required to complete a Passenger Locator Form.

Passengers are required to have proof of a negative test result. This proof can be in the form of a printed document or an email or message that can be shown on a phone. The test result must be in either English, French, or Spanish. Translations are not accepted.

The original test result notification must include the following information:

- your name, which should match the name on your travel documents
- your date of birth or age
- the result of the test
- the date the test sample was collected or received by the test provider
- the name of the test provider and their contact details
- confirmation of the device used for the test, or that the test was a PCR test

https://www.gov.uk/guidance/coronavirus-covid-19-testing-for-people-travelling-to-england

5.3.5.5.1 Why is this important?

Health pass providers should be able to meet the identity binding policy of the use case for which the health credential is being used.

---

[4] https://www.gov.uk/guidance/self-declare-as-a-private-sector-covid-19-testing-provider
[5] https://www.cdc.gov/coronavirus/2019-ncov/travelers/testing-international-air-travelers.html

5.3.6 Achieving Interoperability for Identity Binding Across the Zones

In order for identity binding of digital health credentials and passes to be interoperable, participating ecosystem partners **MUST** either all agree on processes for identity binding within each zone and how those processes will be represented digitally (as was done by ICAO and its members for passports, e-passports, and Digital Trave Credentials), or because different countries, regions, or other jurisdictions may have differing requirements, there **MUST** be a way for verifiers to publish their requirements so that issuers can obtain country-specific requirements and update their process accordingly.

5.3.6.1 Zone 1: Identity authentication at the point of COVID-19 Vaccination or Testing

As we have seen from the example of the United Kingdom, identity authentication processes vary at the point of COVID-19 vaccination or testing.

Even though passports or government-issued IDs are required for international travel, and even while verifiers may hope for high-assurance, robust identity proofing processes at the point of vaccination or testing, this may not be in the best interests of the health care provider or the patient. It would be exclusionary – and could potentially run contrary to public health aims – to require patients to present a passport in order to access testing or vaccination.

As such, 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 for a refugee who may not have official identity documentation to authenticating a patient, in-person, with full biometrics using a tamper-resistant hardware device for cryptographic keys and an extensive Electronic Health Record at a modern hospital.

This said, where test results or vaccination status is being sought specifically for the purposes of international travel, the ID document intended to be used for international travel should be presented to the healthcare provider.

Regardless of what form of identity proofing is performed, the **Identity Assurance Level MUST** be recorded in the transaction so that verifiers can assess the corresponding risk of identity fraud.

5.3.6.1.1 Why is this important?

1. It is the responsibility of the verifier to convey its identity assurance requirements to the pool of Issuers so they can determine whether to change their issuance processes. These identity requirements are enumerated as Levels of Assurance (LOA) associated with the identity document issuance process (Enrollment Phase per ISO/IEC 29115; Identity Assurance Level per NIST 800-63A) and with the authentication process (Authentication Phase per ISO/IEC 29115; Authenticator Assurance Level per NIST 800-63B).
2. Health pass providers **MUST** augment the deficiencies of identity binding in public healthcare processes for the fulfilment of private sector use cases that need greater assurance.
3. Health pass providers **MAY** support differing assurance levels no or low identity and authentication provided that this information is conveyed to the Verifier.
4. The Issuer **SHOULD** provide the enrollment LOA of the identity document used in **Zone 1** along with associated Authentication LOA of the authentication process where:
    4.1. enrollment LOA – reflects the level of identity proofing and identity verification that is performed when enrolling with an identity provider which typically results in the issuance of an identity credential (e.g., Passport Agency)

4.2. Authentication LOA – reflects the level to which the subject can demonstrate that they are in possession and/or control of a credential in order to establish confidence in a claim of identity.

5.3.6.2 Zone 2: Identity authentication at the point of COVID-19 credential issuance

In some jurisdictions, credential issuance could occur contemporaneously with the vaccination or test. If conducted in a single uninterrupted process (i.e. the person administering the vaccine in a patient's arm also being the identity authenticator and credential issuer), there would be limited possibility for the credential to be issued to the wrong individual.

But, often, these processes will be distinct, with issuance of the credential occurring after the health process undertaken. As described in the U.K. example, a record of vaccination may exist within the health system. A patient should be able to access their own health record and obtain a credential as proof of prior vaccination.

If **Zones 1 and 2** are separated, the identity binding process is referred to as "late binding", it is incumbent on the process to ensure chain of custody – that the health information is bound to the correct individual across zones. Having performed identity proofing in Zone 1, authentication is then used in Zone 2 to ensure that the health credential is being issued to the correct individual.

In **Zone 2**, GHP credential issuers **MUST** perform identity authentication of the holder to a sufficient Authentication LOA [based on the destination country's rules – where applicable] prior to issuance of the credential. The level of authentication assurance will vary depending on how these steps are administered.

It is recommended that the GHP credential **SHOULD** include identity document information and both the enrollment LOA of the document presented and the Authentication LOA achieved when authenticating the identity claim; i.e. identity binding, for zone 1 and 2, even if it's the lowest possible level on zone 1, to enable a trusted risk assessment for zone 3.

Health care providers **MAY** issue the credential using technology integrated into the health pass provider (e.g., a QR code scanned by the health pass application), via SMS or email, via the health care systems (e.g., digital health records), or using paper records.

With home testing, strong identity authentication could be required in order to obtain the test kit, though the chain of custody is far weaker as to who the kit is used on. Without remote supervision being used for the entirety of the process, there is scope for fraud to occur. This can be mitigated to some degree by requiring authentication of the user to accept the test kit. For example, using possession of a mobile device as an authentication factor so that the results of the test are only issued to a specific device.

The use of multi-factor authentication that includes a biometric factor such as the photo from a passport may be desirable for an international travel use case. To enable such a scenario, biometric information (e.g., facial image) **MAY** be added to the credential data. Performing biometric authentication in Zone 3 and validating the custody chain will enhance assurance while minimizing the impact on the user's privacy in the process.

Consideration should be given to the required technology to do this. While biometric authentication is readily available for individuals with smartphones, additional technology investments might be required for individuals with little or limited access to smartphones.

5.3.6.2.1 Why is this important?

1. Health pass providers **MAY** need to match the identity data from their own proofing process with identity data in a credential obtained from a health system.
2. Health pass providers **MAY** need to account for the chain of custody in the information presented to the verifier in order that they can implement their own risk mitigations.

5.3.6.3 Zone 3: Identity authentication at the point of COVID-19 credential validation

In **Zone 3**, GHP credential verifiers validate the GHP credential by checking the authenticity, integrity, and revocation status of the credential and then determining if the presenter of the credential is the legitimate subject of the credential. Being able to determine what has occurred – from the point of health care provision to the issuance of the corresponding GHP credential – enables the implementation of business/operational policies within the verifier domain.

This can be done with digital or physical identity credentials where the verifier **MAY** use biometric information in the credentials and **MAY** also review the issuer's levels of assurance during the identity process to ensure that it meets the required enrollment LOA and Authentication LOA – where applicable.

Leveraging the authentication used to issue the credential at the time of presentation can ensure that the subject of the credential is known and can be trusted. If issuers have established multi-factor authentication using a biometric factor bound to the holder, the verifier can require the holder to authenticate using the same means in order to prove they are the subject of the credential.

Alternatively, verifiers can use the identity information bound to the credential to match with their own data or the additional presentation of an identity document. For a travel use case, this could be the passenger named on the boarding card or the details of a passport or regional travel document.

While tools exist to provide high levels of assurance, such as biometric authentication, it should be recognized that the following primary considerations for healthcare may make such tools difficult if not impossible to implement:

- inclusion and accessibility needs mean that low, or no tech solutions **MUST** work alongside high-tech means
- those with limited evidence of their identity **MUST** be served with equivalence to those with the strongest forms
- public health needs **MAY** require remote and self-administered testing to provide greatest impact and reach
- primary systems for recording data are established health systems that extend far beyond the purpose of a health pass service

Given this, verifiers **MAY** choose to adopt additional risk mitigation practices and, where suitable, accept a degree of risk associated with lower identity assurance levels.

5.3.6.3.1 Why is this important?

1. Health pass applications **SHOULD** allow the verifier to understand, to the extent possible, what identity binding has occurred in **Zones 1 and 2.**
2. Verifiers **SHOULD** expect to fill gaps in the identity binding process, particularly for no/low assurance and no/low technology implementations. For example, manual cross reference of the health credential with a physical identity document at the point of acceptance.

3. If countries specify minimal identity assurance levels (enrollment and authentication), those countries **SHOULD** publish those requirements, making it possible for individuals to bring the requisite identity information to the point of healthcare delivery and for healthcare providers and credential issuers to perform the requisite identity authentication and binding – and record it in the GHP credential.

5.3.7 Problem #1: Health pass solutions must work with the existing diverse healthcare system

5.3.7.1 Problem Description

Identity binding is primarily a concern of the providers of health pass solutions. Healthcare providers need to prioritise access to healthcare, and if health passes are to be inclusive, it **MUST** be recognised that:

- Healthcare providers, particularly in the public health domain, cannot present unjust barriers based on a patient's ability to prove their identity, or their access to or capability to use technology
- Access to health care is the primary concern, ability to provide proof downstream is secondary. This may create undesired circumstances for the verifier of a health pass credential that they will have to mitigate. Health pass providers need to give them the information to enable them to do so.
- There is more ability to influence identity binding for health credentials obtained for the specific purpose of the verifier use case – for example, obtaining a COVID-19 test prior to international travel.

5.3.7.2 Good Health Pass Design Requirements & Considerations

Healthcare infrastructure (e.g., IT, processes) is mature and diverse, and changes needed to support Good Health Passes may be cost and/or time prohibitive. The recommendations that follow will allow for these constraints while focusing on steps to facilitate the safe resumption of international travel.

5.3.7.3 Recommendations

5.3.7.3.1 Overall Recommendations

Providers of health pass solutions **SHOULD** perform identity binding between the identity credential presented and the subject of the health pass where possible. The use of biometric authentication **MAY** provide a useful foundation from which identity binding can be layered as required for the use of the health pass.

Health pass providers **MUST** operate with the healthcare system, not the other way round. This means that they will have to fill gaps in identity proofing and authentication undertaken in the healthcare domain through innovative controls in their own domain. They **MAY** fill these gaps by providing matching of identity data from their own proofing process with the identity data received from the healthcare systems.

Health pass solutions **SHOULD** implement identity binding by offering identity proofing and authentication capabilities to fulfill variations and gaps that exist in healthcare providers and verifiers across the three zones described.

5.3.7.3.2 Phase One (30 Day Horizon)

Health pass solutions **SHOULD** document the existing identity binding process including what information is recorded and/or reviewed at health pass issuance and/or verification.

5.3.7.3.3 Phase Two (90 Day Horizon)

Health pass solutions **SHOULD** review guidance on GHP-certified issuance or verification sub-systems (e.g., APIs) that can augment existing IT to meet GHPC identity binding recommendations.

5.3.7.3.4 Phase Three (180 Day Horizon)

Health pass solutions **SHOULD** implement GHP-compliant issuance or verification sub-systems (e.g., APIs) that meet GHPC identity binding recommendations which includes documenting the full name, date of birth, identity document type, country of issuance, and identity document number[6] presented to the healthcare provider which **SHOULD** be the passport the subject plans to use for international travel. If not the passport to be used for international travel, another government-issued identity document with a photo **SHOULD** be used so that the healthcare provider can ensure that the presenter of the photo ID is the authorized holder of the ID and the identity information matches what is in the health record. Electronic passports (e-passports) themselves are supposed to align to ICAO's Traveler Identity Programme (TRIP) process and, where the photo is taken live, have a high LOA. Where the photo is captured by the subject and mailed to the issuing authority, the e-passport has a lower (i.e., medium) LOA.

5.3.8 Problem #2: Identity Binding must support low or no technology solutions

5.3.8.1 Problem Description

Recognition is needed that solutions requiring higher-end technology need to interoperate with low- or no-technology solutions at the issuer and verifier(s) points of the journey. The same is true for solutions that provide higher standards of identity proofing and authentication, these **MUST** equally interoperate with low assurance implementations.

If lower assurance identity binding was used at issuance, the verifier **MAY** be required to take additional actions, such as cross referencing the identity details of the subject of the health credential. Solutions leveraging tools such as smartphones, document verification and biometric facial matching can provide a more seamless and reliable verifier experience. Health pass solutions offering this three-way binding between the user, their identity evidence and the health credential are desirable, though need to allow for interoperability with more simple health passes, including those utilising paper as the means of presentation.

5.3.8.2 Good Health Pass Design Requirements & Considerations

Because the goal is to integrate with low- or no-technology health solutions, the health pass validity related to identity binding MUST be self-contained. Therefore, health pass solutions **SHOULD** document the identity binding process at the time it was issued and share the related identifying attributes as part of the health pass so that verifiers can assess risk of identity fraud.

There are two scenarios that **SHOULD** be considered:

---

[6] Per recommendations in ICAO DOC 10152

1. The no technology use case, where a paper-based health pass is presented and the identifying attributes contained in the health pass are validated with some form of official ID such as a passport or driver's license.
2. The off-line use case, where a digital or paper-based health pass is presented that can be digitally verified using cached public key information from a trust registry. The identifying attributes contained in the health pass are validated with some form of official ID such as a passport or driver's license.

5.3.8.3 Recommendations

5.3.8.3.1 Overall Recommendations

Verifiers **SHOULD** be provided with information on the identity binding that has taken place. This allows identity binding activities to be stepped-up by the verifier from no or low levels of identity binding as required to meet their use case.

5.3.8.3.2 Phase One (30 Day Horizon)

Health credential and pass solutions **SHOULD** document the existing identity binding process, including what information is recorded and/or reviewed, at health pass issuance and/or verification points.

5.3.8.3.3 Phase Three (180 Day Horizon)

Health pass solutions **SHOULD** implement GHP-compliant credential issuance or verification sub-systems (e.g., APIs) that meet GHPC identity binding recommendations.

5.3.9 Problem #3: Globally agreed standards for the levels of confidence in identity binding are required

5.3.9.1 Problem Description

GHP solutions operate at an international level. There are multiple local, national and international standards on Identity Proofing LOAs and Authentication LOAs that are already established across the different jurisdictions.

In order to work with the currently established standards that different governments and identity providers use today rather than forcing them to adopt a new standard, the GHP EGF needs to work with multiple standards and enable interoperability across them. So for example a GPG-45 Authentication LOA 2 medium identity binding for zone 1 & 2 in the U.K. can be accepted by a verifier in zone 3 in the U.S. where they require an equivalent Authenticator Assurance Level (AAL), as defined in NIST 800-63B, or lower (i.e., AAL 1).

5.3.9.2 Recommendations

5.3.9.2.1 Overall Recommendations

To create consistency and full disclosure, the degree of identity assurance and authentication is highly **RECOMMENDED**. In reviewing generally accepted standards for levels of identity assurance and authentication, we **RECOMMEND** adopting ISO/IEC 29115:2013 (revised as intact in 2020) to categorize distinct levels of assurance for identity proofing and authentication. While we believe that other standards have advanced ISO/IEC 29115 as it directs specific jurisdictional applications, this standard is established

to be the most widely used at an international level. The standard also provides guidance for mapping other authentication assurance schemes to the four levels of assurance, providing for the most flexible option (satisfying our GOOD objective).

While other standards **MAY** be used in a particular jurisdiction, they **MUST** map their established standards to the international ISO/IEC 29115 identity and authentication levels of assurance as defined in their respective standards to ensure interoperability.

Both the identity proofing and authentication LOAs used in the identity binding process **SHOULD** be present across the three zones.

Health pass providers **MAY** also offer tools and services to the healthcare provider, such as the ability for the user to show or share their verified identity details in an easy to integrate way. Similarly, they **SHOULD** provide ease of integration into the verifiers' systems.

Healthcare is a multi-provider domain. Health pass providers **SHOULD** ensure that documentation of identity binding is implemented consistently across GHP-compliant solution providers so that Issuers in both the public and private healthcare sectors and verifiers in all sectors can reliably utilise whichever health pass solution a user presents.

5.3.9.2.2 Phase One (30 Day Horizon)

Health Pass solutions **SHOULD** identify which identity and authentication assurance framework(s) are applicable and what LOAs are possible to reach with the current system.

5.3.9.2.3 Phase Two (90 Day Horizon)

1. Health Pass solutions **MUST** map their existing identity and authentication assurance framework(s) to ISO/IEC 29115
2. Health pass solutions **MAY** extend or modify the IT systems and verification processes to achieve the desired Levels of Assurance within ISO/IEC 29115.

5.3.9.2.4 Phase Three (180 Day Horizon)

Health pass solutions **SHOULD** achieve a certification of compliance from GHP to the LOAs supported. This **MAY** be achieved by providing GHP with evidence of a valid third party audit when available.

5.3.10 Interoperability Testing Recommendations

1. Health pass solutions **MUST** ensure that they are able to consume identity binding information for the commonly adopted standards defined above from credential Issuers.
2. Health pass solutions **MUST** ensure that they are able to interpret identity binding information for the commonly adopted standards defined above for use in their business processes.
3. Health pass solutions **MUST** ensure that they are able to convey identity binding information for the commonly adopted standards defined above to verifiers.

5.3.11 Additional Recommendations

5.3.11.1 Regulators (Governments)

Governmental jurisdictions **SHOULD** establish acceptance policy for identity proofing and authentication by taking measures to ensure that Individuals are not excluded due to a lack of provable identity or access to technology when defining requirements for presentation of health credentials

5.3.11.2 Standard Developing Organizations (SDOs) / Industry Groups (e.g. WHO, ISO, W3C, VCI, LFPH, ID2020, ToIP, DIF, IATA, ICAO, HL7)

1. Global standards bodies and industry groups **SHOULD** map to the ISO/IEC 29115 levels of assurance.
2. Use of other jurisdictional standards **MAY** be used provided that they are mapped to the globally interoperable standard recommended by GHPC.

5.3.11.3 Issuers – Public (Public health providers)

Public health providers **SHOULD** include identity information of the subject to comply with data standards for health credentials issued to Good Health Passes.

5.3.11.4 Issuers – Private (Private health providers)

Private health providers **SHOULD** align their own identity processes with health passes by utilising identity processes provided by or aligned to those of the GHP providers. They **SHOULD** include identity information of the subject to comply with data standards for health credentials used to create Good Health Passes.

5.3.11.5 Verifiers / Buyers of Health Pass solutions (Airlines; Airports; Border control)

Verifiers of health pass solutions **SHOULD** establish risk mitigation practices that consider the complexities for issuance of health credentials and the variations in the level of confidence they can take from identity binding. Their identity binding practices **SHOULD** be in compliance with the requirements of a governance framework.

6 Credential Recommendations

6.1 Recommendation #4: Standard Data Models and Elements

6.1.1 Introduction to this Interoperability Challenge

COVID-19 health data comes from multiple sources and in different formats, based on who, where, and how that data is collected in a given jurisdiction. But as with passports and payment cards, fully interoperable digital health pass systems need to support a common data model for data exchange, including specifying standard attributes and forms that can be supported by specific use case implementations.

The Good Health Pass Data Models & Elements recommendations are grounded in the work put forward by several cross-industry efforts, including:

- COVID-19 Credentials Initiative (CCI) [Linux Foundation Public Health (LFPH)], which has established a task force to develop form and schema specifications, Codes of Practice, technical guidelines, JavaScript Object Notation (JSON) code, and related components. This CCI work includes full reference to the eHealth Network's guidelines for COVID-19 certificates.
- W3C Credentials Community Group (CCG)'s Vaccination Certificate Vocabulary
- Smart Vaccine Certificate Working Group at World Health Organization (WHO)
- Canadian COVID Credentials Consortium (C4)
- International Air Transport Association (IATA): IATA Travel Pass Initiative
- International Civil Aviation Organization (ICAO)
- FHIR Focus Group at Trust over IP Foundation (ToIP)
- Vaccination Credential Initiative (VCI): SMART Health Cards Framework
- Centers for Disease Control and Prevention (CDC): COVID-19 Vaccination Reporting Specification (CVRS)
- UK's National Health Service (NHS): Testing for coronavirus (COVID-19) / Coronavirus COVID-19 vaccine
- ISO/IEC 18013-5 mdoc for eHealth

The Good Health Pass Collaborative (GHPC) would like to applaud the global efforts of all of these initiatives – each of which reflects vast participation and collaboration from public health authorities, private health vendors and consortiums, electronic health record (EHR) providers, pharma companies, and major pharmacy chains (US).

Through an extensive evaluation of the above cross-industry initiatives, this group worked to develop a set of data element recommendations that can accommodate requirements of different countries and jurisdictions around the world.

6.1.2 Objective of this Drafting Group

Given the global nature of health pass credentials and passes, the Good Health Pass ecosystem **MUST** be technologically agnostic to all data ingestions. As such, this document focuses recommendations predominantly on data elements, semantic harmonization, and common models for data exchange that can help us work toward interoperability without putting an undue burden on existing health systems and workflows.

6.1.3 Problem #1: Data Elements – Certificates, Credentials, and Passes

6.1.3.1 Problem Description

In healthcare contexts, data is held in a number of places, such as laboratories, health information systems, and clinical trial registries. In order for an issuer to create a credential or pass, based on the requirements of the activity they're undertaking, these institutions must make a version of that data available to that person in the form of a certificate or credential.

When creating standards for a globally-useable health pass, agreement on a minimum-necessary set of data, including how the data is named, organized, etc. is critical to ensuring interoperability. This is of particular importance when considering that the sources of the data (e.g., the aforementioned institutions) may collect or code data differently.

In general, a Good Health Pass (GHP) should only include the minimal set of information necessary to verify and confirm the holder's vaccination, testing, or recovery status as required for a verifier to make a particular trust decision. This is reinforced by Figure 7 from the Good Health Pass Guide to Key Concepts and Terminology:

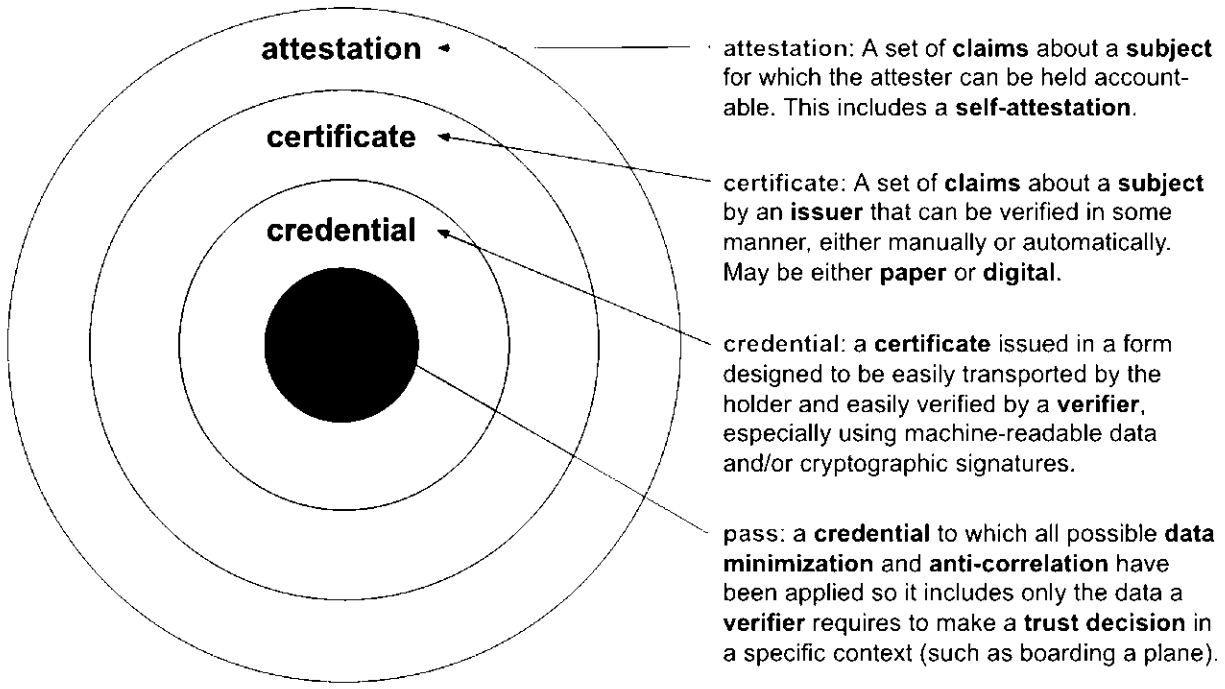

Figure 7: The four core terms for describing data containers for health data used for travel

6.1.3.2 Good Health Pass Design Requirements & Considerations

Within the Good Health Pass ecosystem, a health credential attests that a COVID-19 test event or vaccination event occurred and a health pass attests to the minimal set of data from one or more health records required for a specific verifier or class of verifiers to make a particular trust decision.

In February 2021, the COVID-19 Credentials Initiative (CCI) Schema Task Force began comparing data set recommendations from the cross-industry efforts listed above (see cross-reference links in Appendix

B for more details). This landscape began with the CDC's Technical Standards and Reporting Data – comprehensive documentation that contained recommendations beyond the minimum data requirements for credentials and passes.

When the World Health Organization published its core data set for the Smart Vaccine Certificate in March 2021, and when the EU's eHealth Network published its Value Sets for Digital COVID Certificates in April 2021, these were cross-referenced with the CDC standards to determine common attributes across the three entities, creating the foundation for the recommendations below.

6.1.3.3 Recommendations

6.1.3.3.1 Overall Recommendations

Based on this cross-review process, the GHPC RECOMMENDS that solution providers include the following minimum viable value sets for COVID-19 credentials for global interoperability. Because the GHPC focuses on credentials and passes for both vaccination and testing, these recommendations most closely resemble the EU specification. (The EU specification was also informed by WHO's core dataset, which focuses exclusively on vaccination).

Note that GHPC also recommends that CVX code and state/province of vaccination be included as additional data fields for North America only (these two fields are not currently in EU recommendations).

6.1.3.3.2 Health Certificates

Verifiable Vaccination Certificates

These guidelines aim at preparing for interoperability between attestations of vaccination for medical purposes (also known as vaccination certificates). Other purposes of non-discriminatory use (e.g., in particular for travel purposes) **MAY** be decided upon by jurisdictional authorities, with attestations of vaccination reserved for ongoing global legal, ethical, scientific and societal discussions.

COVID-19 Antigen Test Certificate

A common list of COVID-19 rapid antigen tests, including those of which their test results are mutually recognised, and a common standardized set of data to be included in COVID-19 test result certificates.

6.1.3.3.3 Health Credentials

Vaccination Credential

Vaccination credentials are to be used primarily as a standardized and interoperable form of proof of vaccination for medical purposes. For other use cases, such as for the purpose of travel, one could consider situations where a person arrives in a country and a verifying authority confirms whether the person has been vaccinated against an infectious disease.

The following data fields **SHOULD** be included in the vaccination credential:

(a) name: surname(s) and forename(s), in that order;
(b) date of birth;
(c) disease or agent targeted;
(d) vaccine/prophylaxis;
(e) vaccine medicinal product;
(f) CVX code* *(North America only; not currently in EU recommendations)*;

(g) vaccine marketing authorization holder or manufacturer;
(h) number in a series of vaccinations/doses;
(i) date of vaccination, indicating the date of the latest dose received;
(j) state/province of vaccination* *(North America only; not currently in EU recommendations)*;
(k) country of vaccination;
(l) certificate issuer;
(m) a unique certificate identifier.

Test Credential

Robust testing strategies have been – and will continue to be – an essential aspect of preparedness and response to the COVID-19 pandemic, allowing for early detection of potentially infectious individuals and insight on infection rates and transmission within communities. They are also a prerequisite to adequate contact tracing that can help limit the spread through prompt isolation.

The unequal rollout of COVID-19 vaccines underscores the importance of continued, widespread COVID-19 testing as an essential public health tool – one that must continue alongside vaccination to ensure an equitable return to public life. Additionally, with increasing concerns over the circulation of SARS-CoV-2 variants, testing – and variant-specific testing – will continue to be vital for controlling and suppressing further spread of the virus.

The following data fields **SHOULD** be included in the COVID-19 antigen test credential:

(a) name: surname(s) and forename(s), in that order;
(b) date of birth;
(c) disease or agent targeted;
(d) the type of test;
(e) test name *(optional for NAAT test)*;
(f) test manufacturer *(optional for NAAT test)*;
(g) date and time of the test sample collection;
(h) date and time of the test result production *(optional for rapid antigen test)*;
(i) result of the test;
(j) testing centre or facility;
(n) state/province of test* *(North America only; not currently in EU recommendations)*;
(k) country of test;
(l) certificate issuer;
(m) a unique certificate identifier.

Recovery Credential

According to current evidence, although still testing positive for SARS-CoV-2, infected individuals who have recovered from COVID-19 may still be infectious. In those particular cases, negating the virus may not be viable, with a limited risk of transmission to others.

However, by not presenting a negative test result for unrestricted movement, jurisdictional authorities would prevent those individuals from crossing borders. On balance, the evidence suggests that those who have recovered from COVID-19 have a reduced risk of infection.

The following data fields **SHOULD** be included in the COVID-19 citizen recovery credential:

(a) name: surname(s) and forename(s), in that order;
(b) date of birth;
(c) disease or agent the citizen has recovered from;
(d) date of first positive test result;
(e) state/province of test* *(North America only; not currently in EU recommendations)*;
(f) country of test;
(g) certificate issuer;
(h) certificate valid from;
(i) certificate valid until *(not more than 180 days after the date of first positive test result)*;
(j) a unique certificate identifier.

6.1.3.3.4 Good Health Passes

While the above health credentials attest that a COVID-19 test event or vaccination event occurred, one could consider situations where a person may be required to provide proof of COVID-19 status and may not want – or should not be required to – share all of the information that is captured in a credential.

In these scenarios, such as for international travel, a health pass **MAY** be used to attest to the minimal set of data from one or more health records required for a specific verifier or class of verifiers to make a particular trust decision.

A Good Health Pass **SHOULD** only include the minimal set of information necessary to verify and confirm the holder's vaccination, testing, or recovery status as required for a verifier to make a particular trust decision. For travel, this **SHOULD** include the following basic elements:

(a) name: surname(s) and forename(s), in that order;
(b) date of birth;
(c) event status

All defined semantic content **MUST** be uniquely identified by cryptographic hash functions to ensure that the same message always results in the same hash.

6.1.4 Problem #2: Data Exchange – Common Data Model

6.1.4.1 Problem Description

Common data models are used to standardize and facilitate the exchange, sharing, or storing of data from multiple sources. They are frequently used in healthcare, where there is a need to share data from disparate sources for a particular use, such as clinical research. Common data models can also help avoid the need to share patient-level data – a privacy preserving feature with great relevance for the Good Health Pass ecosystem.

Common data models are designed to promote interoperability between systems that encode healthcare data in different ways. At the same time, there are a multitude of common data models designed for specific contexts – necessitating thoughtful choices based on the proposed use case.

6.1.4.2 Recommendations

The EU, World Health Organization (WHO), and Vaccine Credentialing Initiative (VCI) have all recommended FHIR as the common data model of choice for COVID-19 credentialing initiatives. To further promote interoperability, the GHPC also RECOMMENDS that health credentials and passes

SHOULD use the **HL7 FHIR data model** as described below. In doing so, credential and pass developers can guarantee that data elements included will represent the necessary data requirements covering specific jurisdictions and usage types.

Figure 8: HL7 FHIR Logo

Fast Healthcare Interoperability Resources (FHIR) is a standard for health care data exchange that ultimately aims to get legacy EHRs (electronic **health records**) to a point where they can be interoperable. FHIR allows EHRs the versatility to be used in mobile devices, web-based applications, cloud communications, and EHR data-sharing using modular components. This makes it easier for third-party developers to integrate medical applications into existing systems.

While the FHIR data model aligns Good Health Pass implementers with the data format selected by the EU/WHO/VCI initiatives, it **SHOULD** be recognized that FHIR's adoption is still uneven and there are many healthcare systems that have not, or could not adopt this data model. To address this, the GHPC RECOMMENDS that solution providers **SHOULD** provide guidelines and/or tools to convert non-FHIR formatted EHR data into FHIR formatted records as a pre-processing step. Example guidance on importing csv data into FHIR can be found here.

This RECOMMENDATION assumes that the candidate source EHR data meets the minimum data field requirements called for in the Health Credentials: Vaccination Credential, Test Credential, Recovery Credential sections above.

6.1.5 Problem #3: Semantic Harmonization

6.1.5.1 Problem Description

In exploring the minimal datasets required to differentiate between certificates, credentials, and passes, it is clear that COVID-19 related data will often come from disparate, siloed sources.

When data for credentials and passes comes from multiple sources, it can be difficult to facilitate efficient processing during verification, use an automated rules engine and/or decision support system for pass issuance (based on jurisdiction requirements), and support multiple languages. All of these are key considerations for any proposed solution that would be used to support international travel. Further, dictionary coding differs across jurisdictions, underscoring the importance of having flexible overlays.

As such, data and semantic harmonization are critical to ensuring interoperability of health credentials and passes. Data harmonization involves transforming datasets to fit together in a common architecture. Semantic harmonization is the process of ensuring that – as part of data harmonization – the meaning and context of data remains unaltered for all interacting actors, regardless of how the data was collected originally. This also means that transient objects such as credentials and passes can be more easily resolved into multiple languages.

6.1.5.2 Good Health Pass Design Requirements & Considerations

Advances in decentralized data modeling can enable data harmonization across different models and representation formats. The introduction of decentralized technologies in identity, semantics, and governance has the added benefit of providing a safeguard against online exploitation, surveillance, or potential abuse by redistributing digital control away from centralized platforms and placing control back in the hands of a person – a key principle of the GHPC.

6.1.5.3 Recommendations

6.1.5.3.1 Overall Recommendations

The GHPC RECOMMENDS using Overlays Capture Architecture (OCA) as a solution for semantic harmonization between data models and data representation formats that has been specifically devised for data object interoperability, acting as a catalyst for standardized credential issuance (See Appendix C for more information).

OCA offers an optimal level of both efficiency and interoperability in alignment with FAIR principles (Findability, Accessibility, Interoperability, and Reusability). The architecture provides a stable infrastructure to facilitate seamless semantic harmonization and interoperability processes, not only between internal departments and functions but also between external organizations working under an **ecosystem governance framework (EGF)** (e.g., **Good Health Pass Ecosystem Governance Framework (GHP EGF)**) as defined by an industry collaborative or consortium.

The GHPC is also aware of other semantic architectures being developed in open source communities, which will be continuously evaluated and may feature in future GHPC publications.

6.1.5.3.2 Processing Recommendations

The GHPC RECOMMENDS using the FHIR-OCA data processing pipeline (see Appendix D). The FHIR-OCA tool provides for the conversion of COVID-19 vaccination, testing, or recovery JSON formatted resource bundles via a FHIR JSON-LD context that enables FHIR resource elements to be represented in JSON-LD.

This conversion has several advantages, including allowing the FHIR element definitions to be referenced in a linked data vocabulary, enabling purpose-of-use data framing, and allowing the application of Zero Knowledge Proof and linked data signature encryption techniques to the health certificate and related verifiable credentials. Details of this pipeline can be found in Appendix C.

6.1.6 Phased Approach

With the publication of this document, implementers would take a phased approach toward adoption of recommended standards. These phases would be defined along timelines measured in 30-, 90-, and 180-day segments and further accounted for across industries with different levels of agility based on established development cycles.

The standards and technology patterns being developed in this specification, and broadly as part of the GHPC activities, are designed to be used not just for the immediate needs of this phase of the COVID pandemic but to be a potential framework to handle a variety of verifiable credential use cases that may arise in the future. To that end, for implementers that require a longer lead time, (e.g., larger companies),

announcements of participation via product road maps, with regular updates until official launch, would demonstrate their commitment to GHP principles to the community as a whole.

6.1.6.1 Phase One (30 Day Horizon)

1. The GHPC **RECOMMENDS** that solution providers, issuers and attesters start setting the minimum viable value sets for COVID-19 credentials required for global interoperability.
2. The GHPC also **RECOMMENDS** that CVX code and state of vaccination be included as additional data fields for North America only.
3. To further promote interoperability, the GHPC **RECOMMENDS** that health credential and pass solution providers/issuers/developers **SHOULD** start using the HL7 FHIR data model. For healthcare systems that have not, or could not adopt the FHIR data model, the GHPC **RECOMMENDS** that solution providers **SHOULD** provide guidelines and/or tools to convert non-FHIR formatted EHR data into FHIR formatted records as a pre-processing step.

6.1.6.2 Phase Two (90 Day Horizon)

1. The GHPC **RECOMMENDS** that solution providers enable semantic harmonization between data models and data representation formats to create health certificates, health credentials, and GHPs for jurisdictions they are affiliated with.
2. The GHPC **RECOMMENDS** using the FHIR-OCA data processing pipeline for the conversion of COVID-19 vaccination, testing, or recovery JSON formatted resource bundles via a FHIR JSON-LD context that enables FHIR resource elements to be represented in JSON-LD.
3. The GHPC **RECOMMENDS** that solution providers start testing their health certificates, health credentials and GHPs against rules engines for interoperability with other jurisdictions.

6.1.6.3 Phase Three (180 Day Horizon)

The GHPC **RECOMMENDS** that solution providers work with jurisdictions rolling out health certificates, health credentials and GHPs.

6.2 Recommendation #5: Credential Formats, Signatures, and Protocols

6.2.1 Introduction to this Interoperability Challenge

Technical interoperability of digital health passes rests on use of a singular set of formats, digital signature suites, issuance protocols and presentation protocols.

However, although the promise of **digital credentials** is enormous, the W3C open standard data model for cryptographically verifiable digital credentials – widely referred to as **verifiable credentials** – is only 18 months old. So there are already many **non-W3C verifiable credentials** in existence, including several defined expressly for proof of COVID-19 health status (such as the EU COVID-19 Certificate and the proposed WHO Smart Vaccination Certificate). Furthermore, even those verifiable credentials that do follow the W3C standard may use different representation formats and digital signature types because the W3C specification supports multiple options.

In addition, the W3C standard does not cover any standard protocols for **issuance** of credentials to **holders** or **presentation** of **proofs** of those credentials to **verifiers**. It only covers the data model for representing and signing credentials in a digital format.

So the essence of this interoperability challenge is to specify the precise set of formats, digital signature suites, issuance protocols, and presentation protocols that will enable maximum interoperability of Good Health Pass–compliant digital credentials and passes while still meeting the other requirements of the **GHP Interoperability Blueprint**.

6.2.2 Objective of this Drafting Group

Based on the goals described above, the objective of this Drafting Group is to specify the following for **GHP-compliant** digital **health credentials** and **health passes**:

1. **The data format(s).**
2. **The digital signature suite(s).**
3. **The issuance protocol(s).**
4. **The presentation protocol(s).**

Ideally, only one choice should be recommended for each of these. The reason, in the words of Brian Behlendorf, General Manager of Blockchain, Healthcare, and Identity at the Linux Foundation, is that "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.

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

- Performance requirements at airports, airlines, and for 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 and
- Cost and availability.

6.2.3 Problem #1: Specify how GHP-compliant credential systems can interoperate with non-GHP credential systems

6.2.3.1 Problem Description

As explained in the Background section, there are many different systems and processes for issuing digitally-signed health data. The GHP ecosystem needs to be able to accept certificates and credentials from issuers who are not following our recommended standards for verifiable credentials.

Figure 9 illustrates conceptually how other non-GHP certificate and credential systems – whether or not they are compatible with the W3C standard – should be accepted as inputs used to produce a GHP-compliant health pass.

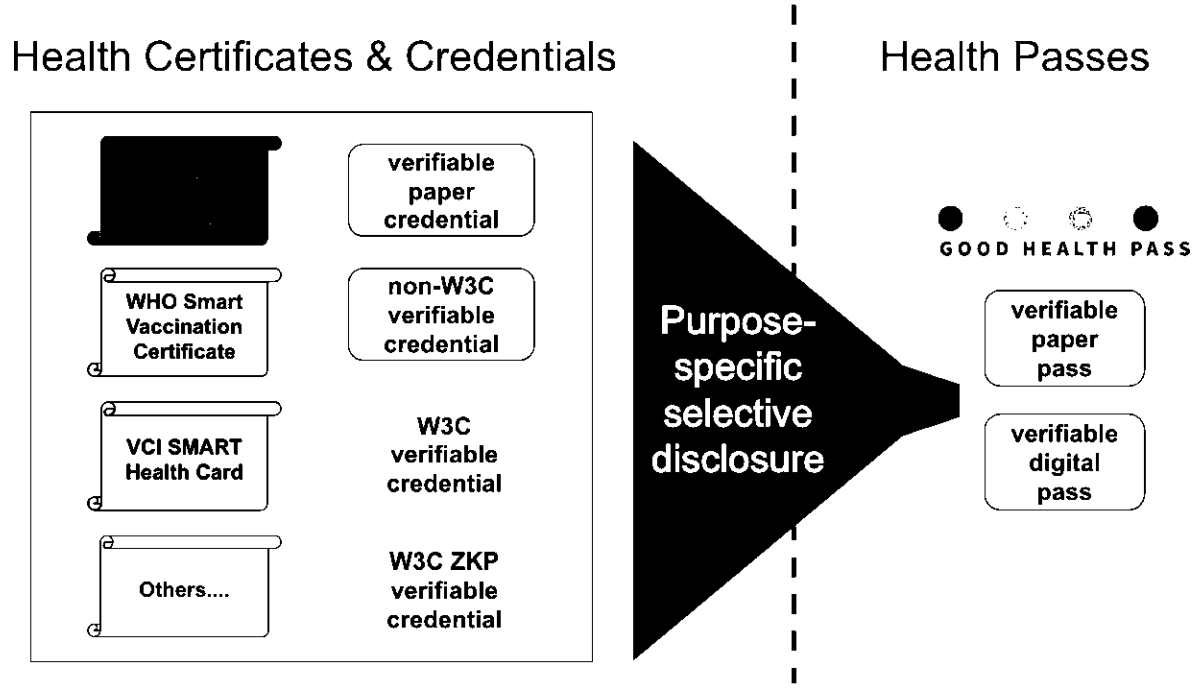

Figure 9: Health certificates and credentials that are not GHP-compliant can all be used as inputs to general a GHP-compliant health pass

6.2.3.2 Good Health Pass Design Requirements & Considerations

Good Health Pass architecture is explicitly designed to accommodate other inputs of verifiable health data. The primary design consideration is that issuers of GHP-compliant health credentials and passes who wish to ingest other health credential formats need to integrate the necessary verification services – sometimes called "universal verifiers". These issuers will also typically need to implement a rules engine and/or decision support system to apply the necessary verification and re-issuance rules.

In addition, non-GHP certificates or credentials might not use W3C Decentralized Identifiers (DIDs) or the digital signature suites recommended in this document. For example, both the WHO Smart Vaccination Certificate and the EU Digital COVID Certificate plan to use public key directories (PKDs) based on conventional X.509 PKI public key certificates. This contingency has been recognized by the GHP Trust Registries group. See Recommendation #8 for their proposals, which envisage a global trust registry network using an open standard protocol supporting both DID-based and X.509-based public key verification.

A universal verifier **MAY** also need to accept other credential presentation protocols besides those recommended in this document. Of particular interest is the OpenID Connect (OIDC) protocol and specifically the Self-Issued OpenID Provider (SIOP) protocol under development at the OpenID Foundation in collaboration with the Decentralized Identity Foundation. This is an active, ongoing effort to define how the OIDC protocol can be used for the issuance and presentation of W3C Verifiable Credentials.

Furthermore, OIDC and OAuth2 can already be leveraged in the issuance process by providing an authentication solution for consumers to access their health records in an electronic medical record (EMR) or similar system using the HL7 Fast Healthcare Interoperability Resources (FHIR) standard as shown in Figure 10.[7]

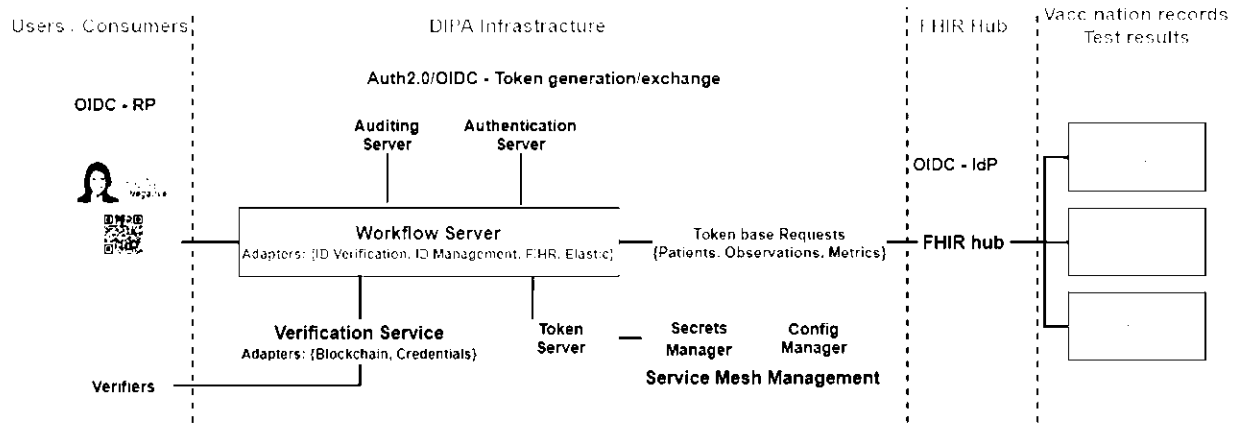

Figure 10: Holder authentication to a FHIR-enabled health record system using OAuth 2 and OIDC

6.2.3.3 Recommendations

1. Issuers of GHP-compliant digital credentials and passes in the travel domain SHOULD also serve as verifiers accepting non-GHP-compliant health credentials.
2. Issuers who choose to serve as verifiers of non-GHP credentials MUST follow the GHP Interoperability Blueprint recommendations for GHP-compliant verifiers.
3. The Good Health Pass digital trust ecosystem SHOULD support the development of open source universal verifier code for processing and verification of these non-GHP credentials. (Some companies have already developed such code.)

6.2.4 Problem #2: Determine the precise open standards necessary for interoperability of GHP-compliant digital credentials

6.2.4.1 Problem Description

As described above, interoperability requires that we make specific choices among the myriad of formats, signatures, and exchange protocols in use. Our interoperability recommendations will address these in the following categories:

- W3C Verifiable Credential formats and signatures,
- W3C Verifiable Credential **issuance** protocol, and
- W3C Verifiable Credential **presentation** protocol.

[7] https://arxiv.org/ftp/arxiv/papers/2103/2103.04142.pdf

6.2.4.2 Good Health Pass Design Requirements & Considerations

For maximum interoperability, GHP-compliant digital credentials should be designed whenever possible to use:

1. A single format compliant with the W3C Verifiable Credentials standard.
2. A single digital signature suite that meets GHP security and privacy requirements.
3. A single protocol for issuance (issuer-to-holder) and presentation (holder-to-verifier).

Other key considerations in arriving at our recommendations include:

- **User control:** GHP-compliant digital wallet apps need to provide the holder with maximum control of how and when the credentials are shared.
- **Privacy:** GHP-compliant solutions **SHOULD** not "phone home" or implement other designs or features that allow for tracking or surveillance. They **SHOULD** also apply data minimization via selective disclosure. And they **SHOULD** minimize correlation risks.

> ***What is the "phone home" problem?***
>
> Digital identity systems built for enterprise Identity and Access Management (IAM) and federation operate using an architectural pattern often referred to as "phoning home". When individuals enroll in a federated identity system (usually through an entity called an identity provider or IdP), they are assigned an identifier and register one or more ways to authenticate (prove) they are in control of this identifier, such as an ordinary password, one-time password (OTP) token, or a biometric that is enrolled and matched against. If, in the process of authenticating with some other entity within that federated identity system, the enrolled individual is redirected back to the entity that issued the original identifier, that is called "phoning home". This is a privacy problem within all federated identity systems because it allows the IdP to track the individual's activity within the network. For example, in a government context, it creates a way for governments to track usage of citizens within the system.

These design considerations make it clear that a GHP-compliant health credential format **SHOULD** ideally use a **zero-knowledge proof** (ZKP) cryptography because its ability to support **selective disclosure** means the holder can produce any number of context-specific GHP-compliant health passes that meet the requirements of a specific verifier at a specific point in time. This is illustrated in Figure 11.

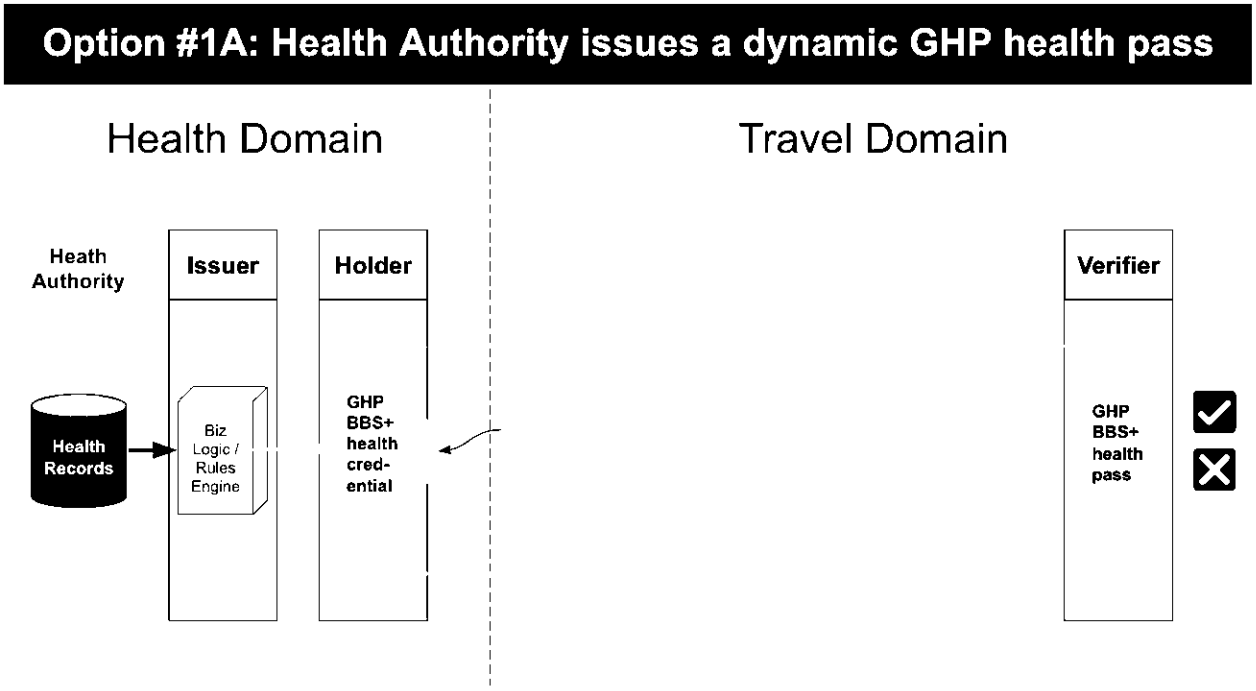

Figure 11: A zero-knowledge proof credential can support dynamic generation of any number of context-specific GHP-compliant health passes

6.2.4.3 Recommendations

6.2.4.3.1 Overall Recommendations

1. Implementers **MUST** implement the following open standards according to the timelines specified below:
   1.1. JSON-LD formatted W3C Verifiable Credentials
   1.2. BBS+ LD-Signatures
   1.3. WACI PEx Protocols for issuance and verification as defined by the DIF Claims and Credentials WG.

   IMPORTANT: We recognize that we are recommending a protocol that is still a work-in-progress, but we do so for a specific reason: each of the current options on the market were designed with different architectural assumptions and do not yet have broad adoption. The emergence of JSON-LD ZKP with BBS+ signatures as a common format and signature suite represents an inflection point. Developers of the different technology stacks are willing to adopt it. This has spurred the Good Health Pass community and other stakeholders to converge first on a presentation protocol and secondly on an issuance protocol that will work across these different technology stacks.

   The work on WACI Pe-X draws on DIDComm, Aries Proof Request, Aries Credential Issuance, DIF Presentation Exchange, WACI (Wallet and Agent Credential Interaction), and VC-HTTP-API. Because this emerging protocol is merging the best and simplest elements of these together, this is what we are recommending.

2. If a GHP-compliant digital wallet app or rules engine/DSS supports sharing digital health credentials in other formats, **the app or rules engine/DSS MUST display an explicit warning**

to the holder about the privacy implications if a verifier requests a presentation of an entire credential – thus requiring the holder to share all the data – instead of presenting (or asking a rules engine/DSS to generate) a privacy-preserving GHP-compliant health pass.

6.2.4.3.2 Phase One (30 Day Horizon)

Purpose: To converge on a common data model.

1. **MUST** publicly document your existing credential formats, signatures, and exchange protocols.
2. **SHOULD** use W3C Verifiable Credentials which leverage the JSON-LD format and BBS+ signature scheme.
3. **SHOULD** have a transition plan in place (for existing implementers) or begin building toward (for new implementers) to comply with the recommendations in this document.
4. If possible within 30 days, implementers SHOULD use W3C Verifiable Credentials as follows:
   - 4.1. Formats and Signatures: JSON-LD, with BBS+
   - 4.2. Issuance Protocol:
     - 4.2.1. Existing implementers with an existing issuance protocol: adapt that protocol as needed to work with JSON-LD with BBS+ credentials
     - 4.2.2. New implementers: implement support for EITHER Aries Issuance Protocol OR CCG Issuance Protocol
   - 4.3. Presentation Protocol: WACI Pe-X for presentation

6.2.4.3.3 Phase Two (90 Day Horizon)

Purpose: To enable interoperable presentation of GHP-compliant credentials. That means regardless of which credentials were issued, to which kinds of digital wallets, those credentials will be able to be presented to any verifier.

MUST have transition plan in place for moving to the recommended formats, signatures, and exchange protocols

SHOULD use W3C Verifiable Credentials as follows:

- **Formats and Signatures**: JSON-LD, with BBS+
- **Presentation Protocol**: WACI Pe-X for presentation

If implementers are able to within 90 days, they SHOULD use W3C Verifiable Credentials as follows:

- **Issuance Protocol**: WACI Pe-X for issuance

6.2.4.3.4 Phase Three (180 Day Horizon)

Purpose: To enable interoperable issuance of GHP-compliant credentials. That means regardless of which digital wallet an individual possesses, credentials from any GHP-compliant issuer can be issued to that wallet and accepted by the individual. This prevents user experience challenges associated with downloading multiple apps (e.g., imagine needing to download app A to travel to a country and download app B to travel home) and enables user choice of wallet.

MUST use W3C Verifiable Credentials as follows:

- **Formats and Signatures**: JSON-LD, with BBS+
- **Issuance Protocol**: WACI Pe-X for issuance
- **Presentation Protocol**: WACI Pe-X for presentation

6.2.5 Problem #3: Determine the precise open standards necessary for interoperability of GHP-compliant digital passes

6.2.5.1 Problem Description

A GHP-compliant digital pass is simply a GHP-compliant digital credential to which data minimization and anti-correlation have been applied for privacy-preservation as illustrated in Figure 1. Therefore the interoperability requirements in this section overlap with those of Problem #2.

6.2.5.2 Good Health Pass Design Requirements & Considerations

Our JSON-LD / BBS+ recommendation for a GHP-compliant health credential in the previous section will automatically produce a GHP-compliant health pass in response to a GHP-compliant verifiable presentation request from a verifier.

However, what if a holder either has a *non-GHP-compliant digital wallet* – or does not have a digital device at all? In this case the holder is not capable of accepting a BBS+ credential since it requires a digital interaction with the holder.

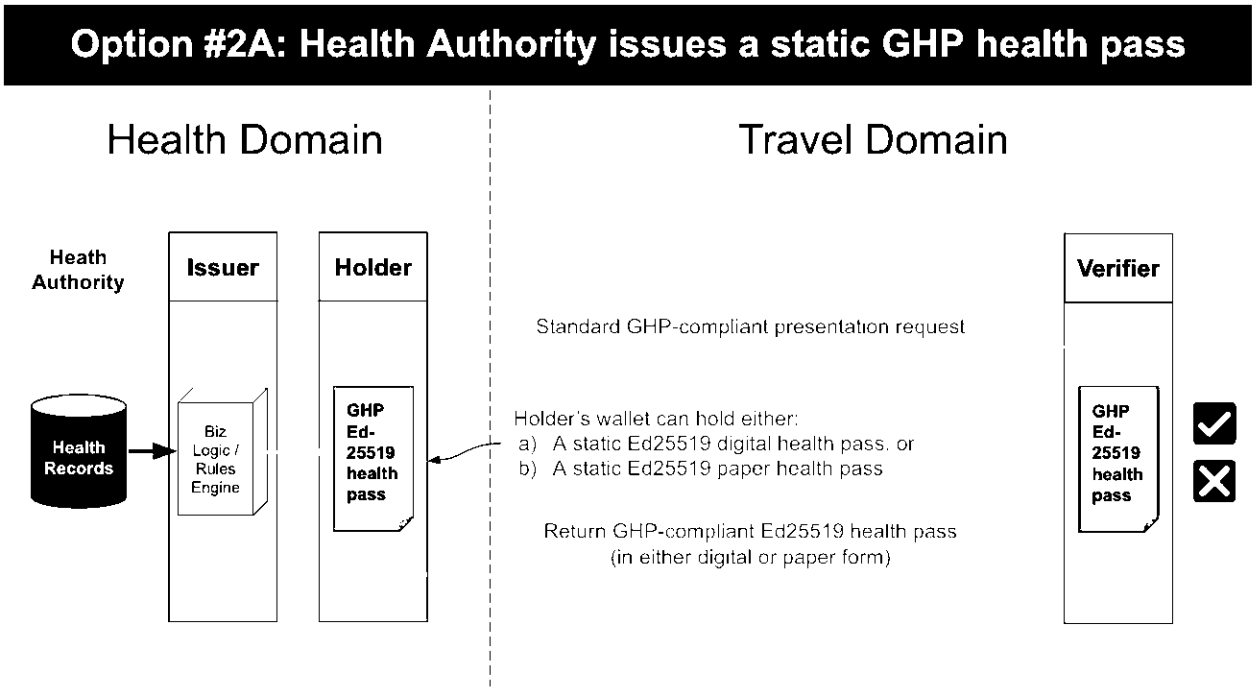

Figure 12: A static GHP-compliant health pass does not require an advanced digital wallet and can be printed on paper, but it does not support selective disclosure

So the Good Health Pass Interoperability Blueprint requires a second recommendation for *non-ZKP health credentials*. Since such a credential is static and does not support selective disclosure, it effectively functions as a **health pass** that can be displayed either in a simple digital format (such as a QR code displayed by a simple digital wallet or mobile web app) or printed on paper. This static GHP-compliant health pass is illustrated in Figure 12.

6.2.5.3 Recommendations

6.2.5.3.1 Overall Recommendations

1. For dynamic GHP-compliant health passes, the recommendations in Problem #2 apply.
2. For static GHP-compliant health passes, an implementer **MUST** implement JSON-LD formatted W3C Verifiable Credentials with ED25519 signatures and using the same issuance and presentation protocols as in Problem #2.

6.2.5.3.2 Phase One (30 Day Horizon)

MUST publicly document your existing credential formats, signatures, and exchange protocols.

SHOULD have transition plan in place for moving to the recommended formats, signatures, and exchange protocols

SHOULD use W3C Verifiable Credentials where:

1. **Formats and Signatures** are: JSON-LD, with either BBS+ (for passes derived from GHP-compliant credentials) or ED25519 signatures (for passes directly issued)
2. **Issuance Protocol** is: WACI Pe-X
3. **Presentation Protocol** is: WACI Pe-X

6.2.5.3.3 Phase Two (90 Day Horizon)

MUST have transition plan in place for moving to the recommended formats, signatures, and exchange protocols

SHOULD use W3C Verifiable Credentials where:

1. **Formats and Signatures** are: JSON-LD, with either BBS+ (for passes derived from GHP-compliant credentials) or ED25519 signatures (for passes directly issued)
2. **Issuance Protocol** is: WACI Pe-X
3. **Presentation Protocol** is: WACI Pe-X

6.2.5.3.4 Phase Three (180 Day Horizon)

MUST use W3C Verifiable Credentials where:

1. **Formats and Signatures** are: JSON-LD, with either BBS+ (for passes derived from GHP-compliant credentials) or ED25519 signatures (for passes directly issued)
2. **Issuance Protocol** is: WACI Pe-X
3. **Presentation Protocol** is: WACI Pe-X

6.2.6 Problem #4: Agree on implementation requirements for security, privacy, and data protection of GHP-compliant digital credentials and passes

6.2.6.1 Problem Description

Digital credentials, especially digital health credentials, contain sensitive personal information that requires continuous safeguards to prevent unauthorized or unintentional disclosure. The prospective credential ecosystem for health passes means that credentials **MUST** be supported by a comprehensive trust assurance framework that not only supports all jurisdictional compliance requirements for security and privacy, but incorporates open standards, accepted cryptographic methods, and internationally recognized security processes to minimize risk to the credential holder. General security, privacy, and data protection guidance is provided in Recommendation #2 – Security, Privacy, and Data Protection; here we will focus on corresponding characteristics specific to Formats, Protocols, and Signatures.

6.2.6.2 Good Health Pass Design Requirements & Considerations

The world has a very large patchwork of different security and data protection requirements, some of which are regional in nature. As this blueprint is intended to be usable worldwide, it does not require specific approaches, but instead directs policy makers and practitioners to appropriate standards with some supplemental direction in terms of desired outcome objectives.

6.2.6.3 Recommendations

6.2.6.3.1 Overall Recommendations

Digital credential issuers and verifiers **MUST** demonstrate adherence to all jurisdictional security and privacy requirements, and provide evidence of their implementation of recognized standards and best practices in information security and privacy, such as ISO 2700X, ISO 29100, ENISA, HIPAA, NIST CSF, or Canadian ITSG-33, as examples.

All credential issuers and verifiers **MUST** possess certifications or independent party assessment documentation that demonstrates compliance with an internationally recognized cybersecurity standard.

6.2.6.3.2 Phase One (30 Day Horizon)

1. Current and prospective issuers and verifiers **MUST** conform to the GHP ecosystem governance framework requirements for certification with supported evidence.
2. GHP-compliant passes **SHOULD** apply data minimization and anti-correlation regardless of what technology is used. Please refer to the other recommendations in this section as well as the security, privacy, and data protection recommendations for more detail.

6.2.6.3.3 Phase Two (90 Day Horizon)

1. Current and prospective issuers **SHOULD** have a self-assessment, risk assessment, and plan of action and milestones (POA&M) to demonstrate the intended path for compliance and certification.
2. GHP-compliant passes **SHOULD** support selective disclosure and non-correlating signatures by following the recommendations in Problem #2 and Problem #3.

6.2.6.3.4 Phase Three (180 Day Horizon)

1. Issuers **MUST** have a self-assessment, risk assessment, and Plan of Action and Milestones (POA&M) to demonstrate the intended path for compliance and certification.

2. GHP-compliant passes **MUST** support selective disclosure, non-correlating signatures, and non-correlating holder binding.

6.2.7 Problem #5: Specify how GHP-compliant implementations can support offline usage of digital credentials and passes

6.2.7.1 Problem Description

There are a number of different circumstances under which digital credentials and passes may be used. While some of these circumstances allow for the use of the Internet for actions such as connecting to trust registries, verifying public keys, etc., this is not always the case. For example, many border crossings do not allow Internet access for either the holder or the verifier.

GHP-compliant implementations need to work in environments that do not allow Internet access. This affects both holders and verifiers.

6.2.7.2 Good Health Pass Design Requirements & Considerations

This section identifies key areas where system providers need to pay special attention to the challenge of offline usage, and where providers will need to architect appropriately. For example, offline use requires trust registries to support the caching of data needed for verification.

6.2.7.3 Recommendations

6.2.7.3.1 Overall Recommendations

1. A mechanism **MUST** exist whereby holders can present credentials and passes without the support of the Internet.
2. A mechanism **MUST** exist whereby verifiers can verify the validity of the presented credentials and passes without the support of the Internet. It is recognized that this means verifiers **MAY** be using outdated information to perform this task.
3. A mechanism **MUST** exist whereby holders can present credentials and passes to the verifier without the support of the Internet. This process **MAY** include the request from the verifier to the holder.

6.2.7.3.2 Phase One (30 Day Horizon)

The solution **SHOULD** support offline use with W3C Verifiable Credentials.

6.2.7.3.3 Phase Two (90 Day Horizon)

The solution **MUST** support offline use with W3C Verifiable Credentials. It SHOULD support offline use with privacy-preserving capability.

6.2.7.3.3 Phase Three (180 Day Horizon)

The solution **MUST** support offline use with W3C Verifiable Credentials and privacy-preserving capability.

6.2.8 Problem #6: Determine the formats and signatures for the payload of GHP-compliant paper credentials and passes

6.2.8.1 Problem Description

The previous problem statements have applied to digital credentials and passes, where the assumption is that the credential or pass is issued directly to the holder's digital wallet and then presented to a verifier, when needed, in the same all-digital manner.

However for purposes of equity and inclusion, GHP-compliant health credentials and passes also need to support being transmitted in a non-digital version that does not require a digital device or an Internet connection. We call this a **paper credential** or **paper pass** because it is physically printed in some manner, but the underlying medium can be any non-digital medium capable of carrying information (e.g., plastic, metal, or cloth).

6.2.8.2 Good Health Pass Design Requirements & Considerations

Once a paper pass is scanned by a digital scanning device of some kind, it is converted back into a digital representation. At that point it would be ideal for this representation – or an algorithmic transformation of it – to be directly processable according to the previous recommendations in this document.

However there is a specific challenge in the case where the paper pass has been produced directly by an issuer without the holder having a digital wallet. In this case, the pass cannot be digitally signed by a BBS+ signature because the holder has no mechanism for generating and sharing the BLS private key or link secret needed by the issuer to issue a JSON-LD with BBS+ credential. This is why problem #3 recommends issuing a static GHP-compliant digital pass that still uses the JSON-LD format but with the Ed25519 digital signature suite. This format can be printed directly as a static paper pass.

6.2.8.3 Recommendations

1. The output of scanning a **GHP-compliant paper credential** or **paper pass MUST** be a digital representation that is either directly conformant with or or is algorithmically transformable into one of the digital credential representation formats recommended in this document.
2. In the case that the holder is not capable of supporting the recommended BBS+ digital signature type, the issuer **MUST** digitally sign the paper credential or pass with a linked data signature using the Ed25519Signature2020 signature suite.
3. The 30, 90, and 180 day phased recommendations **SHOULD** follow the recommendations of the Paper Credentials group (see Recommendation #6).

6.2.9 Problem #7: Determine a two-way transformation between the paper versions and the digital versions of GHP-compliant credentials and passes

6.2.9.1 Problem Description

The preceding problem described how a paper credential or pass can be converted into a digital representation conformant with the recommendations in this document for purposes of verification. But it would be ideal for holders to be able to complete a full two-way "round-trip" from digital credentials and passes into their paper versions and back again.

6.2.9.2 Good Health Pass Design Requirements & Considerations

We have already recommended the overall process for transforming from a digital format into a paper format. The precise algorithm to follow to produce a print document containing a QR code will be a recommendation from the Paper Credentials group (see Recommendation #6).

The remaining challenge is to transform from the paper version back into the digital version such that the credential or pass can be stored in the holder's digital wallet and used in the same manner as if it had been issued directly into the holder's digital wallet app.

6.2.9.3 Recommendations

6.2.9.3.1 Overall Recommendations

There are two types of digital health information described here that can be transformed into a paper version: GHP-compliant digital credentials, and GHP-compliant digital passes. Paper versions of these **MAY** be produced, but they have different qualities and intended uses. The algorithm by which this transformation is performed is specified in Recommendation #6 – Paper Credentials.

6.2.9.3.2 GHP-Compliant Digital and Paper Passes

A paper version of a GHP-compliant digital pass is intended to be shared with a verifier, just as a digital pass would be. All of the recommendations around data minimization and context-specific production apply here.

1. A GHP-compliant digital pass **MAY** be converted into a GHP paper pass.
2. The resulting GHP-compliant paper pass **MAY** be converted back into a GHP-compliant digital pass.
3. An Issuer **MAY** directly issue a GHP-compliant paper pass to a holder.
4. If conversion between paper and digital passes is supported, it **MUST** be lossless (i.e. the artifact that exists as a GHP-compliant digital pass **MUST** be indistinguishable from the result of converting that GHP-compliant digital pass into a GHP-compliant paper pass and back again).

6.2.9.3.3 GHP-Compliant Digital and Paper Credentials

A paper version of a GHP-compliant digital credential is **not** intended to be shared with a verifier in the travel domain because it contains a full set of health and other personal attributes. Additionally, since it contains the issuer's BBS+ signature for the holder (which requires input from the verifier to whom the signature will be presented), a different verifier would not have the information needed to verify it.

Instead, a paper version of a GHP-compliant digital credential is intended to provide a means of storing the credential *until it may be converted back into digital form*. This is necessary before the GHP-compliant paper credential can be used by the holder.

1. A GHP-compliant digital credential **MAY** be converted into a GHP-compliant paper credential.
2. A GHP-compliant paper credential converted from a GHP-compliant digital credential **MAY** be converted back into a GHP-compliant digital credential.
3. If such transformation between paper and digital credentials is supported, it **MUST** be lossless (i.e. the artifact that exists as a GHP-compliant digital credential **MUST** be indistinguishable from the result of converting that GHP-compliant digital credential into a GHP-compliant paper credential and back again).
4. If a holder is not able to accept a GHP-compliant digital credential or pass, rather than issue a GHP-compliant paper credential to a holder, it is **RECOMMENDED** to issue a GHP-compliant

paper pass to the holder.

4.1. It is **RECOMMENDED** to apply as much data minimization and anti-correlation as possible to still meet the holder's and verifier's requirements.

6.2.10 Interoperability Testing Guidance

Good Health Pass-complaint credential testing suites SHOULD be created based on W3C Verifiable Credential JSON-LD, ZKP with BBS+ signature format and the WACI Pe-X issuance and presentation protocols. Test suites already exist for Hyperledger Aries (the open source project often used as the wallet/agent component for the issuance, verification, and sharing of W3C Verifiable Credentials) and the open source Verifiable Credentials test suite hosted by W3C CCG originally developed for the U.S. DHS S&T Silicon Valley Innovation Program.

1. Within Phase 1 (30 days), we recommend producing an analysis of the existing test suites to identify the gaps and formulate a plan and resources for addressing them.
   1.1. The test harness **MUST** test both issuer to holder systems and holder to verifier systems.
2. Within Phase 2 (90 days), we recommend:
   2.1. Completing the work for the test suites to test the requirements of the **Good Health Pass Interoperability Blueprint**.
   2.2. Commencing NxN matrix testing of implementations seeking GHP-compliance.
3. Within Phase 3 (180 days), we recommend:
   3.1. Development and execution of a GHP-compliant certification program and trust mark.

6.3 Recommendation #6: Paper Credentials

6.3.1 Introduction to this Interoperability Challenge

Inclusion is a fundamental principle of the Good Health Pass Collaborative (GHPC): health pass solutions **MUST** be designed to serve everyone, including those who may be socially, financially, digitally, or otherwise excluded. To enable universal accessibility, Good Health Pass (GHP) solutions need to serve all people in a variety of issuing and verification situations, including those that do not have guaranteed connectivity or a high degree of digital infrastructure. Additionally, not all people have smartphones, the physical ability to use them, or the desire to use them for this purpose.

As such, the GHP ecosystem **MUST** support proofs of vaccination or test status that are paper-based and offline. The challenge is to maintain consistent privacy and security measures offered by digital approaches, including Verifiable Credentials (VCs), while adapting to the potential lack of connectivity during holding and verification.

By virtue of being paper-based, some aspects of a paper credential's user experience (UX) will be notably different from its smartphone-based equivalent. Where possible, though, we desire a unified experience so people can broadly use the same approaches and rely on the same mental models no matter if a health credential or pass is on a smartphone or on paper.

In making our recommendations, the GHPC recognizes its responsibility for helping guide emerging data privacy practices in this space. In many parts of the world, information related to COVID-19 health status is deemed to be personally identifiable information (PII) or sensitive PII, not public information. There should be explicit awareness that we are shaping people's understanding of how they should treat the privacy of their information.

The tradeoffs associated with a paper-based design or the lack of connectivity for verifiers **SHOULD** be clearly laid out so individuals and policy makers may consider them. While time to implement a solution is a key factor for all decisions relating to the present COVID pandemic, compromises **MUST** be carefully considered, as they may be irreversible or have long term implications and consequences.

6.3.2 Background

Before COVID-19, proofs of vaccination tended to be paper-based and "low assurance"; this also tended to matter less because people rarely needed to prove this information, and the risk or incidence of fraud was relatively small – or at least, not broadly known or considered.

In the United States, for example, parents enrolling their children in school may request a paper print-out of their child's vaccination status from the state-level Immunization Information System (IIS) and share that with the school. This would need to happen typically once per school year. In the international travel case, the use of vaccination cards such as the WHO Yellow Card was used in times where proof of immunization was required.

Today, the scale and importance of proving COVID-19 status requires improvements to data privacy, data integrity, and confidentiality in disclosure.

Innovations in VCs, such as new W3C standards for a VCs data model and Decentralized Identifiers (DIDs), have lent themselves to improved privacy preservation. They make it easier to protect the sharing

of health status. However, paper-based considerations were not in the W3C's original scope. For this reason, the community has done additional work to harmonize these principles with a paper-based approach.

All these efforts must be considered in a global context. No matter the sector of the economy, confirming the authenticity of information now primarily uses digital technologies. This is true of payments, passports, and all manner of Internet-connected systems. The abuses of, and attacks against, any existing or new paper or digital design are unrelenting – the challenges around Internet payments and advertising's global unique identifiers are two notable examples.

While details vary, digital systems often include safeguards that have evolved in order to support system integrity and trust. These include avoiding persistent and global identifiers, using short-lived pairwise and session-based identifiers, preventing replay of a transaction, using good cryptography, data minimization, selective disclosure, zero-knowledge proofs, and guarding against abuse from an actor-in-the-middle of a transaction flow.

Although the world is already set up to support paper-based solutions, many of the above safeguards cannot be implemented in paper-based designs. Additionally, paper-based implementations have different design constraints than digital implementations – which become particularly pronounced at scale. For example, paper-based solutions:

- are statically printed and cannot directly implement time-limited, session-specific, dynamic data features that aid in privacy, security and integrity;
- must include, in verification situations without supporting documents or connectivity, all of the data and personal information that may be needed, introducing the potential challenges of global unique identifiers, data spills, and uncontrolled replays;
- may be altered or faked, and cannot match smartphone security and biometrics;
- may be stored by someone for a long time with data that does not change, rather than digitally deleted and re-issued as needed;
- may be able to be presented multiple times, rather than being restricted to a single use;
- may not be as easy to revoke if issued in error, if the data changes or situations of use change;
- are not easily bound to the person that holds them, unlike online solutions that can use digital signing and cryptography to prove the intended holder.

These are important trade offs and compromises that must be balanced alongside considerations around ease of use, equity, and time to implement. The massive scale and importance of providing COVID-19 status underscores the need for digital means to streamline this process – which, in turn, necessitates an upgrade from unverifiable paper evidence of health status to verifiable paper evidence.

The recommendations in this document are the result of collaboration between many organizations with expertise in QR codes, encryption, compression, W3C VCs, and W3C DIDs.

(Note that in this document we talk specifically about using QR codes for paper credentials, but the same ideas and recommendations work for any other machine-readable code.)

6.3.3 Objective of this Drafting Group

To explore the unique challenges presented by paper credentials and make recommendations as to how they can be supported in a way consistent with the overall principles of the Good Health Pass Collaborative. Since paper credentials experience the same interoperability challenges of digital

credentials, albeit with unique constraints, we have chosen to break down our investigation into the same set of challenges. We have also attempted, wherever possible, to minimize divergence between digital and paper strategies, and make recommendations for a more cohesive implementation strategy – allowing paper credentials to participate in the digital ecosystem and vice-versa.

6.3.4 Problem #1: Consistent User Experience

6.3.4.1 Problem Description

Paper credentials, and passes, present a unique set of challenges that impact credentialing, presentation, and verification, which if not carefully considered could result in a divergence in the benefits, protections, and user experiences of those holding paper compared to those holding digital.

This will add complexity for organizations implementing credential-driven business processes and raise the barrier to adoption. It will also add complexity for those individuals holding paper credentials, not least of all because it is reasonable to assume that individuals will migrate from physical to digital over time, and could hold a combination of physical and digital at any point in time, particularly in the case of multi-generational households. It is also reasonable to assume that holders of a paper credential may need to present online as well as in-person, such as requesting a boarding pass, and therefore need flexibility for how they can use their paper credential.

The main user experience challenges with paper credentials or passes relate to:

1. The method by which the Issuer issues the credential to the holder; including layout, privacy protections, techniques to reduce the risk of fraud, and minimum requirements for QR codes.
2. The method by which the holder presents the credential to the verifier; including in-person, online.
3. The method by which the verifier verifies the credential; scanning technology and verification process.

If we want to create a consistent user experience for holders of paper credentials, we need to make recommendations that will address these challenges.

We have focused on general considerations that are specific to paper credentials. We have not considered the broader user stories that are already described in the Recommendation #1: Consistent User Experience, as these are broadly applicable to both digital and paper credentials. No conflicts have been observed between our two sets of recommendations.

6.3.4.2 Good Health Pass Design Requirements & Considerations

An optimal implementation needs to take the following into consideration:

1. The format of a paper pass or credential for machine scanning and human readability.
2. Constraints in the techniques by which paper credentials can be scanned; specifically to address legacy scanning devices, older phones, and other constraints on QR code size, compression and encodings.
3. Interoperability between paper and digital credentials and passes, where individuals may want to migrate from one to the other.
4. Hashing, signing algorithms need to be secure but make small outputs
5. Data fields need to respect global languages and names
6. Spec **MUST** be implementable on low-powered hardware

7. Support as many programming environments as possible
8. Fully offline operation has to work – online maybe once a week at most

The decision to use QR codes was made because:

- QR codes can store more data, both in terms of number of "bits on paper" and in terms of efficiency of recording non-ASCII data. PDF 417's smaller ASCII-based encoding is likely not capable of encoding the size and types of payloads we expect;
- QR codes have consumer recognizability compared to other encoding formats; and
- QR codes are well supported by well-tested production-deployed libraries in popular programming languages.

Unlike a digital credential where the holder has options to choose what data to disclose at presentation time, with a paper credential the selective disclosure options need to be set up when the credential is issued. Selective disclosure can be implemented through a card design that can include multiple QR codes. For example; by providing multiple QR codes, each with different levels of disclosure. With multiple options, an educated user can choose what to share by presenting the QR code with the most appropriate information set for the occasion.

6.3.4.3 Recommendations

6.3.4.3.1 Format of a Good Health Pass

A GHP-compliant paper credential or Good Health Pass:

1. **MUST** allow individuals who do not have a smartphone or do not want to hold a digital credential to participate in business processes that require proof of COVID status. NB: "Paper" stands for any physically-printed, non-electronic medium (e.g., plastic).
2. **MUST** use QR codes, to provide a simple and broadly used mechanism for exchanging credential data.
3. **MUST** format the QR code message as a URI.
4. **SHOULD** display all fields found in the QR code legibly on the paper credential/pass, so that the person can see exactly what is stored in the machine readable QR code.

6.3.4.3.2 Issuance of a GHP-compliant paper credential or Good Health Pass

1. **MUST** offer selective disclosure options when issuing/printing out, to ensure that the person only needs to share the minimum amount of information for a specific business process; such as retrieving your boarding pass.
2. **MUST** include, in the QR code, all information needed to cryptographically verify the credential and perform the use case, to support an offline use case where there may not be Internet access at the point of credential exchange.
3. **MUST** provide the holder with clear guidelines on how they can recover their credential, if recovery is available.
4. **MUST** provide the holder with a clear description of what happens when they present their credential to a verifier.
5. **MUST** provide the holder with information about their rights as it relates to the credential being issued to them.
6. **MUST** provide the holder with clear guidelines on how they can keep their information secure and private.

6.3.4.3.3 Presentation of a Good Health Pass

See "Recommendation #5: Credential Formats, Signatures, and Protocols" for the recommended QR code technical specifications.

1. **MUST** ensure the QR code is machine readable when printed from or displayed on low-end devices.
2. **MUST** support a number of different QR code scanning options to address legacy devices, older phones, and other constraints on size, CPU performance (when using compression), and encoding.
3. **MUST** specify the expected QR code reading distance, where some QRs are made to be displayed in large displays to be read at a distance, others in small form-factors to be read at close distance.
4. **SHOULD** support decode and verification directly in low-end QR scanning devices.

6.3.4.3.4 Verification of a GHP-compliant paper credential or Good Health Pass

1. **MUST** collect electronic consent from the holder if personal data is being harvested from the QR code being presented.
2. **MUST** provide means to download and cache all needed information to cryptographically verify the credential so that verification can happen offline.
3. **MAY** collect electronic consent from the holder when verifying a credential.

6.3.4.3.5 Participation in Online Processes

1. **MUST** be able to participate in a digital transaction, such as an online check-in system.
2. **SHOULD** be able to be converted into a digital credential, so that a person who has received a paper credential can choose to migrate to digital. It would be optimal if paper credentials could be a paper-based version of their digital cousin, but that may not always be the case due to various constraints, such as QR code size or selective disclosure constraints. For example, paper credentials **MAY** need to apply minimization or compression techniques that do not easily facilitate backward mapping to their digital alternative.
3. **SHOULD** be able to be generated from a digital credential, so that a person who has received a digital credential can choose to convert into a paper credential so they can use it through more traditional paper-based QR code scanning

6.3.5 Problem #2: Standard Data Models and Elements

6.3.5.1 Problem Description

Paper credentials cannot participate in privacy-preserving presentation requests and proof exchanges: whatever is in the credential is presented as a whole to the verifier. By contrast, a presentation request from a digital credential is able to selectively request information or a Zero Knowledge Proof from the credential. For example, only asking for the first and last name from a driver's license, or a proof that the holder is over the age of 21 without requiring the birth date.

For this reason there are specific requirements that we need to call out for how paper credential schemas may differ from digital ones. For example, a paper credential could allow some level of identity obfuscation by only providing incomplete demographic information, such as the first and last letter of a name.

Paper credentials are built on the work of other GHP working groups. Thus, to some degree a large part of our recommendation here is "encode the data the way they specify it elsewhere in GHP".

Because there may be use cases where verification will be done without access to the Internet, paper credentials and passes **SHOULD** be as "self-contained" as possible, meaning that all data that is external to the credential can be cached in advance.

We request GHP implementers to specify with maximum detail each of their fields and field types in a schema. Knowing minimum and maximum sizes for each field allows an implementer to estimate the minimum QR size where every payload can be represented. Specifying the precision of the field and encoding value sets into fixed enumerations significantly reduces the size of the field in bytes. Long field types, like DIDs and UUIDs **MUST** be encoded in Base32URL to make sure they use the minimum amount of space in the QR.

Defining data type recommendations can significantly improve the size of the QR. If possible with the use case, fields with Latin alphabets should encode their text only in UPPERCASE. This simple choice represents ~50% savings of the field size in represented bytes. Virtually every paper credential existing today, from government IDs and passports, to credit cards and member cards, etc., uses UPPERCASE only fields.

If the schema happens to have multiple dates and/or datetimes, a good option is to encode all datetimes as positive integers representing the time passed since a chosen epoch (e.g. 1/1/1970). Ideally, the new datetime format has a flag that marks the scale (days, hours, minutes, seconds, milliseconds or ticks) and uses an integer number of that scale between the given time and an arbitrary epoch. This method can save a significant amount of space when compared to ISO8601 dates.

URLs or QRs with simple identifiers where more data can be downloaded directly from the issuer or a centralized server/blockchain, and thus allow tracing from that server, are **not Good Health Passes.**

6.3.5.2 Recommendations

6.3.5.2.1 Fit for Purpose

Paper credentials are being designed for use cases where the Internet is not available, but there is the expectation that public keys and similar can be cached and refreshed occasionally.

A GHP-compliant paper credential or Good Health Pass:

1. **MUST** include the complete information set for the use case inside the QR.
2. **MUST** be designed with minimum data.
3. **MUST** be digitally signed using a method recommended by GHPC.
4. **MUST NOT** be a URL or a simple identifier.
5. **SHOULD** limit the inclusion of URLs into the payload.
6. **SHOULD** follow the W3C Verifiable Credentials data model.

6.3.5.2.2 QR Code Compatibility

There is a limit to how much data can be reasonably stored within a QR code, and generally speaking the smaller the size of the QR code, the better. QR codes internally have multiple encoding methods and respond better to certain data encodings. Please see the "QR Image Specs for Printing/Displaying" section for further considerations.

A GHP-compliant paper credential or Good Health Pass:

1. **MUST** specify the maximum payload size and estimate minimum printed QR size.
2. **SHOULD** encode highly random data, such as DIDs and UUIDs, in Base32URL.
3. **SHOULD** encode Latin-alphabet text as UPPERCASE ASCII.
4. **SHOULD** encode dates as differences in time since a given epoch.
5. **SHOULD NOT** duplicate information in the payload.

6.3.5.2.3 Formal Data Field Definitions

It is worth noting that the EU Digital COVID Certificate[8] specifies this information using JSON Schema[9].

A GHP-compliant paper credential or Good Health Pass, for each field:

1. **MUST** specify optionality, minimum and maximum bounds.
2. **MUST** specify a format (date format, decimal number formats).
3. **MUST** specify an alphabet (UTF-8, UTF-16, numbers, ASCII, uppercase letters).
4. **MUST** specify a unit of account (celsius, meters, etc.).
5. **MUST** specify the precision (floating points, rounding methods, cropped names, etc.).
6. **MUST** specify normative simplifications (enumeration mappings, options, etc.).
7. **MUST** specify a formal semantic definition that SHOULD be a linked data URI.
8. **SHOULD** specify a regular expression to validate the field.

6.3.6 Problem #3: Credential Formats, Signatures, and Minimization Functions

6.3.3.1 Problem Description

Paper credentials are severely constrained by QR code size limitations, which means that credential formats **MAY** need to be compromised in order to meet the requirements of paper based exchange. There is a limit to how much data can be reasonably stored within a QR code, and generally speaking the smaller the size of the QR code, the better. QR codes internally have multiple encoding methods and respond better to certain data encodings. Please see the “QR Image Specs for Printing/Displaying” section for further details.

In order to enhance interoperability of all components, we are strongly advising Good Health Passes to use the URI specification, where the schema type implies the minimization function used, as a defining element for the rest of the QR message. URI encodings are extremely common data types for the QR community. The adoption of this battle-tested standard guarantees stable deployment of the protocol and easy compatibility with most if not all scanning devices and applications out there.

Choices of formats, signatures and minimization functions should be optimized for ease of implementation in high- and low-end devices while using the minimum amount of software dependencies with preference for low-resource-consuming algorithms that have mature libraries available in many programming languages. In order to guarantee that Verifiable Credentials are indeed "verifiable", the GHP specification recommends all elements of the credential (keys, schemas, minimization functions, etc.) to

---

[8] https://ec.europa.eu/health/sites/health/files/ehealth/docs/digital-green-certificates_dt-specifications_en.pdf

[9] https://json-schema.org/

be made free of cost, publicly available, well-defined and patent unencumbered, with wide access in multiple programming languages.

QRs are by definition not human readable. But there is a difference between reading a QR with the phone's default camera app and reading the same QR with apps from the app stores (verifiers). How do holders know the apps available to decode the QR are not exposing their information to unwanted parties? How can holders be sure such apps are not using the information in their favor? Having to trust an app to decode a QR just to verify if the sensitive information there is correct or existing is a bad user experience design. We recommend implementers to create easily reviewable QRs, with directly legible fields using the default camera apps on available devices.

6.3.3.2 Recommendations

GHPC has designed this recommendation such that it can be implemented with free of cost, publicly available, well-defined and patent unencumbered code, in multiple programming languages.

A GHP-compliant paper credential or Good Health Pass:

6.3.3.2.1 Fit for Purpose

1. **MUST** support issuing and verification of credentials in offline environments.
2. **MUST** include a unique reference to download public keys for verification.
3. **MUST** include references (not necessarily a direct link) to any other element that is needed to process, verify and understand the payload (conversion templates, minimization functions, schema definitions, etc.).
4. **MUST** be formatted as a URI (RFC3986), where the schema type implies the minimization function.
5. **SHOULD** be easily readable by the holder, to confirm the information in the QR matches their privacy expectations.

6.3.3.2.2 Cryptography

1. **MUST** include a cryptographic signature.
2. **SHOULD** use the signature suite(s) recommended in "Recommendation #5: Credential Formats, Signatures and Protocols".
3. **SHOULD** use signatures that minimize space and are easy to compute by low-end devices.

6.3.3.2.3 Data Minimization and Encoding

1. **MUST** apply a data minimization function to adjust encoding of available W3C VC syntaxes (JSON, XML, YAML, CBOR) to the QR; or use a VC syntax already designed for QR compatibility.
2. **MUST** define or reference all steps of the data minimization function being used and make it freely available. Any holder or any verifier may revert the function and obtain the original payload.
3. **MUST NOT** use plain or unencoded Unicode strings on QRs. QR expects ISO 8859-1; use of Unicode will likely cause faulty decoding and cryptographic verification failure.
4. **SHOULD** be optimized for ease of implementation in high- and low-end devices while using the minimum amount of software dependencies with preference for low-resource-consuming algorithms that have mature libraries in many languages.

6.3.3.2.4 Minimization Functions

Choosing a Minimization Function

1. Decoders **MUST** support Option 1 and Option 2.
2. Encoders **SHOULD** use the option which encodes the smallest payload size.

Option 1: CBOR-LD encoded Base32

Note that all JSON-LD contexts **MUST** be available at encoding time.

1. Encode the JSON-LD message using CBOR-LD. (https://digitalbazaar.github.io/cbor-ld-spec/)
2. Encode the CBOR-LD message as Base32.
3. Prefix with **`CBLD:`** (UPPERCASE strongly preferred).
4. Create the QR code, with at least 25% error correction preferred.

The URI at step 3 is a valid URI according to RFC3986. When decoding:

- the prefix **MUST** match CBLD: with a case-independent match.
- the last colon section separated component of the URI is always the encoded payload (this allows for other components in the future, but their meaning is undefined).

Option 2: JSON-XT

JSON-XT is described here: https://jsonxt.io/. JSON-XT requires a template which describes all the data being encoded.

1. Choose the template "resolver", name and version.
2. Encode the JSON-LD (or any JSON) as JSON-XT. A valid RFC3986 URI is produced with the prefix **`JSONXT:`**.
3. Create the QR code, with at least 25% error correction preferred.

Phase One (30 Day Horizon)

GHPC will recommend standard templates for JSON-XT encoding, including resolver name, template name and version.

6.3.7 Problem #4: Security, Privacy, and Data Protection

6.3.7.1 Problem Description

Paper credentials cannot participate in privacy-preserving selective disclosure and zero-knowledge presentation request and proof exchanges: whatever is in the credential is presented as a whole to the verifier. For this reason are there specific considerations that we need to call out for how paper credential schemas may differ from digital ones. For example, a paper credential could allow some level of identity obfuscation by only displaying incomplete demographic information, such as the first and last letter of a name.

A Good Health Pass gives full control to holders and it is generally the legal property of the holder. The holder should be able to review the data encoded on the credential or pass and control the physical document. Implementations **MUST** comply with local regulations on data retention and transmission (e.g.,

GDPR, HIPAA) which may impact any or all parties using the pass or credential. The holder **MUST** have access to information about the security and privacy implications of the data on the credential or pass, and make decisions about which information to disclose to verifiers based on these implications

Implementers **MUST** consider implicit information sharing consent opportunities and risks. The holder can, for instance, display parts of the pass or credential to a handheld scanner while obfuscating another part of the credential. In this case, the consent is sufficiently well defined by physically masking the information the holder does not want to expose. Implementers **MUST** make sure that desire cannot be circumvented by verifiers and/or additional cameras recording the holder.

If the implementation explicitly includes a path to destruction/revocation of a credential or pass, the implementation should specify whether destruction/revocation will prevent recovery/replacement of that pass. If the information in the pass or credential may be used to defraud or otherwise harm the holder, the pass or credential **MUST** incorporate security measures (such as a PIN or password) to mitigate this risk.

All multi-use Verifiable Credentials are traceable through data sharing between colluding verifiers. If traceability is an issue for the use case, we recommend providing holders with a tear-off book of Verifiable QRs that contain a nonce. This design element turns a multi-use element into a single-use, give away card. If this is implemented, verifiers need to make sure to properly secure or destroy the evidence of the physical QR in the same way they would protect and destroy the digital QR.

6.3.7.2 Recommendations

To meet the expectations of a Good Health Pass, a QR paper credential or pass:

1. **MUST** provide as much control of the physical document as possible to the holder.
2. **MUST** comply with local regulations on data retention and transmission.
3. **MUST** give information to holders about the security and privacy implications of the data.
4. **MUST** only reveal information with the consent of the holder.
5. **MUST** use encryption if the Verifiable QR can defraud or otherwise harm the holder.
6. **SHOULD** specify whether destruction/revocation will prevent recovery/replacement.
7. **SHOULD NOT** combine multiple information classes such as health and financial information.
8. **SHOULD NOT** include information not necessary to support the desired use case.
9. **MAY** print multiple different single-use paper QRs that are designed to be given away to each verifier if verifier traceability is an issue.

6.3.8 Problem #5: Minimum Identity Binding

6.3.8.1 Problem Description

Typically, paper-based credentials that should be verifiable without contacting the issuer act as bearer instruments, where the holder of the instrument is assumed to be its subject. While this is good for privacy reasons, it does cause an issue with regards to potential misuse of credentials, for example by being presented by a person that is not the subject of the credential. Due to the static nature of paper-based credentials, another issue is that they generally could allow for replay attacks, allowing for repeated usage (e.g., through copies). This is especially problematic in a situation where there is no unique identifier for credentials that may originate from different issuers, using a variety of issuance processes and/or systems.

In order to address these problems and reduce the risk of misuse, a minimum form of identity binding should be implemented in paper-based credentials in such a way that it can be independently established that the holder of a paper-based credential is also the subject of the credential. As the more information is stored in a Verifiable QR code, the more likely the QR code can be used to uniquely track a person; therefore we recommend the less information stored the better, including less precise individual fields. For example, instead of storing a person's full name and date of birth, it could store only the person's initials and year of birth, adding ambiguity to reduce traceability. Instead of storing the issuance date in milliseconds, which can be used as an identifier, it could store in seconds. However, we recognize that this may cause a conflict with the requirements of verifiers and the potential for creating a credential that could be reused by someone it was not issued for.

When used in combination with other credentials (e.g., a ticket), the identity binding should remain independent and bound information from the health-pass should not be propagated into any other credential which serves a different purpose. While it may appear this is good for usability, the linked PII (Personally Identifiable Information) and/or PHI (Protected Health Information) significantly changes the regulatory status of those credentials, posing large challenges to the processors and controllers of those credentials.

6.3.8.2 Good Health Pass Design Requirements & Considerations

Since paper credentials cannot participate in automated digital identity verification protocols, implementers **MUST** bind the record to an independently verifiable identifier of the person. The binding can be strong (e.g., exact name, government-issued ID numbers, e-mails, phone numbers, biometric information) or weak (e.g., initials of the user's name, public database's member ID), but it **MUST** be in the credential payload or be linked to that payload.

The chosen method **MUST** allow manual identity checks by verifiers and should not rely on IDs that are not openly accessible to independent verifiers (e.g., company controlled member/employer cards) or identification mechanisms that allow a third party to control access to them. Weak binding is key for vulnerable populations such as undocumented immigrants, persecuted populations, and other minority classes. It also enables easier implementation across a wide variety of issuers.

In order to strengthen the binding with the holder, authenticators such as passwords or PINs **MAY** be used, with the consideration that this could prevent misuse in cases where the original holder is not actively involved. As such, it will generally not increase the level of assurance of the credential.

Paper credentials **MAY** have a second user binding mechanism using a digital multi-factor authentication. By including contact information (e-mail, phone numbers, etc.) in the Verifiable QR, a verifier can send a message to verify the control of the contact information and authenticate the owner without the need for an additional identity document. The same procedure can be used to unencrypt sensitive parts of the Verifiable QR.

6.3.8.3 Recommendations

To meet the expectations of a Good Health Pass, a QR paper credential or pass:

1. **MUST** minimally bind to identifying information of the rightful holder.
2. **MUST** be independently verifiable with another form of identifying information.
3. **SHOULD** bind using commonly-used, publicly accessible, identifiers.
4. **SHOULD** allow for flexibility in assurance levels through its identity binding.
5. **MAY** bind to a multi-factor authentication option.

6. **MUST** ensure identifying information remains independently verifiable.

6.3.9 Problem #6: Trusted Physical Card Design

6.3.9.1 Problem Description

QRs require physical space, either on a card or on a display. The following recommendations are intended to describe what features such cards should consider.

6.3.9.2 Good Health Pass Design Requirements & Considerations

The card **MUST** allow the holder to understand what is in their Verifiable QR. A good practice that is implemented in virtually every other form of barcode-based paper credential is to expose the fields inside the QR around the QR itself, as much as possible. However, sometimes the information in the QR might not fit on the card or might not be desirable to be human-readable (e.g., a password). Due to such fringe use cases, even though we believe all fields SHOULD be on the card, we are choosing to not require this.

Cards can include security features (e.g., branded cards, select materials, serial numbers, etc.) that add protections to the cryptographic signature. We are particularly concerned about use cases where massive unauthorized cloning can create a Denial of Service attack on the identity check procedures of verifiers. Vendors **MUST** carefully understand the risks of cloning the QRs and adopt measures accordingly. Additional materials can provide protection against unwanted/unauthorized scanning, such as privacy filters, folding designs, protective sleeves, etc. If labels/stickers are to be used, "tamper-proof"/"tamper-evident" labels can be implemented for scenarios where added security is required (where the risk/incentive of fraudulent activity is high).

Good Health Passes tend to be multi-use elements and **MUST** be designed with a specified longevity in mind. Certain materials (e.g., thicker papers, labels or PVC card) can also improve the speed of scanning due to the need to keep the Verifiable QR flat during scanning.

For cards that contain more than one Verifiable QR, the design of the card **MUST** make obvious to the holder what each QR contains and how/where to use it. The same design **MUST** also allow holders to hide parts of the card, including other QRs and/or human-readable fields they don't want to show to a verifier, especially if each QR contains different data classes (e.g., health information, financial information, personally identifiable information).

When providing Verifiable QRs as independent stickers to be placed on cards, implementers **MUST** print the information in the QR in human-readable fashion on the stickers themselves. This builds up the confidence of holders by clarifying which QR has what data even before placing them on a card.

In case of using weather-sensitive printing mechanisms (e.g., thermal printers, soluble inks), holders must be aware of the risks of losing the credential by temperature or water damage. If possible, card designers should avoid such materials to enhance user experience. Card/label/paper printers should be capable of catering for large scale printing and simplicity of user experience (changing ribbons, etc.) at point of issuance.

6.3.9.3 Recommendations

To meet the expectations of a Good Health Pass, a QR paper credential or pass:

1. **MUST** define minimum and maximum physical space for the Verifiable QR.
2. **SHOULD** design the card avoiding potential folding marks through the Verifiable QR.
3. **SHOULD** display all fields found in the QR Code legibly on the Card.
4. **SHOULD** be durable and/or easily reprintable.
5. **SHOULD** use thicker materials to enhance machine readability.
6. **SHOULD** label each QR to instruct holders what exactly it contains and how to use it.
7. **SHOULD** be designed for and/or use materials that block unauthorized reading.
8. **SHOULD** provide protections to enhance durability, resist abrasion, crumbling, tearing, scratching, temperature and water damage.
9. **MAY** use tamper-evident materials, for example, so a QR sticker could not be removed and reattached.

6.3.10 Problem #7: QR Image Specs for Printing/Displaying

6.3.10.1 Problem Description

QRs require physical space, either on a card or on a display. The following recommendations are intended to facilitate the scanning and set up minimum requirements for low-end devices.

6.3.10.2 Good Health Pass Design Requirements & Considerations

Understanding what information can fit into a readable QR code takes into consideration the allowable space in the card, the quality of the printer, and the expected distance between the QR code and the QR scanner. We stress that by carefully defining the fields available for the issuer and the minimization function, a vendor **MUST** be able to build the minimum and maximum payload configurations and verify if both fit the available space, given the printing processes available, and are easily readable by the lowest-resource QR scanner supported.

We recommend a minimum QR resolution as the following: each QR bit (each black and white square of the QR) is composed of at least a 3x3 grid of printed dots or display pixels and a minimum of 0.4mm per QR bit. Implementers should keep in mind that QR scanners have a maximum and minimum focusing ability and if the QR bit is too small for the expected distance, the scanner will not be able to read. For error correction, we recommend level Q (~25%) and require a minimum of level M (~15%).

The GS1 2D Barcode Verification Process Implementation Guideline[10] design document provides a comprehensive overview of all the metrics implementers should review before deploying their solution. The printed QR should be optimized for Symbol Contrast, Fixed Pattern Damage, Axial Nonuniformity, Grid Nonuniformity, Modulation, Unused Error Correction.

6.3.10.3 Recommendations

To meet the expectations of a Good Health Pass, a QR paper credential or pass:

1. **MUST** follow the QR Code specification (ISO/IEC 18004:2015).[11]
2. **MUST** follow the GS1 2D Barcode Verification Process Implementation Guideline.
3. **MUST** be printed or displayed on a size where the QR's bits per inch is at most a third of the printer's dots per inch or the display's pixels per inch.

---

[10] https://www.gs1.org/docs/barcodes/2D_Barcode_Verification_Process_Implementation_Guideline.pdf
[11] *ibid.*

4. **MUST** be printed/displayed with a margin/quiet zone with the size of 4 QR bits.
5. **MUST** specify minimum QR printing size for given printing/displaying resolutions.
6. **MUST** be able to print the maximum payload in the minimum QR printing size.
7. **MUST** use a minimum Level M (15%) error correction.
8. **SHOULD** use a Level Q (25%) error correction.

6.3.11 Problem #8: Public Testing Suites

6.3.11.1 Problem Description

Every solution provider for verifiable credentials and passes should provide ways to test implementations against their designs and allow implementers to determine compliance with the specifications.

6.3.11.2 Recommendations

To meet the expectations of a Good Health Pass, a QR paper credential or pass:

1. **MUST** design a Test Policy.
2. **MUST** create a Test Suite.
3. **MUST** allow implementers to INDEPENDENTLY claim compliance to the vendor's mode of operation if their implementation passes all tests.
4. **MUST** offer a complete set of credentials and passes for testing purposes that explore all variables, formats, optionalities and the limits of the proposed credentials, including all variants of cryptographic algorithms, signatures, minimization functions, QR images, and complete card images and electronic display screenshots.
5. **MUST** offer a complete set of testing credentials signed with development and production keys that can be verified with development and production environments on a frequent basis.
6. **MUST** offer the Test Suite in a programming language-independent way.
7. **MUST NOT** require implementers to purchase specialized equipment or licenses from the vendor to validate the correctness of an implementation.
8. **SHOULD** offer an locally-runnable implementation of the test suite in the vendor's preferred language.
9. **SHOULD** provide meaningful feedback to implementers when a QR paper credential or pass does not satisfy the requirements of the specification (beyond pass/fail).
10. **SHOULD** provide example data sets for minimum and maximum size that **MUST** be supported by implementers.

6.3.12 Problem #9: Interoperability between Paper and Digital Credentials

6.3.12.1 Problem Description

Paper credentials **MUST** be given equal weight in the GHP ecosystem. For equity and other reasons, no one should be required to have an electronic device to use GHP. We also foresee the need for credentials in highly constrained environments, and also the possibility that people **MAY** need to move between these worlds (highly constrained and less constrained).

6.3.12.2 Good Health Pass Design Requirements & Considerations

We are allowing for two possibilities for transcribing the "original" digital credentials into paper credentials:

- Two-way, which will be convertible back into the original digital form
- One-way, which will not

One-way paper credentials do not have to be convertible back into their original digital form. We are not making a recommendation whether these be even exchangeable for a digital credential.

6.3.12.3 Recommendations

Problem #3 outlines the data minimization function requirements, so we will not duplicate that information here.

6.3.12.3.1 Fit for Purpose

1. A GHP-compliant implementation **MUST** support a paper credential option, **MAY** be one-way or **MAY** be two-way
2. A two-way paper credential **MUST** be losslessly convertible back into its original digital form.
3. The one-way and two-way transformations **MUST** be well defined, as per Problem #3.
4. All verifiers that accept GHP-compliant digital credentials **SHOULD** also accept GHP-compliant paper credentials
5. **MUST** expect and allow for the importation of the same credential/pass wallets that might have other information for this record and might not be in sync with each other.

7 Operational Infrastructure Recommendations

7.1 Recommendation #7: Rules Engines

7.1.1 Introduction to this Interoperability Challenge

Airlines are subject to many rules that govern every part of their operations. There are rules from the airport, from government agencies, and from the countries they fly between (and over). If an airline fails to comply with any of these hundreds of rules, they may be subjected to fines and/or negative financial impact due to operational delays.

In addition to the rules for operating aircraft, there are also rules specific to each passenger, including rules around travel restrictions, disabilities, or other regulated accommodations.

Travel restrictions based on country of origin or health status have become commonplace during the pandemic. These rules may change often and are often time-bound, complicating adherence by passengers and air carriers alike. For example, a requirement that passengers must have tested negative for COVID-19 within a certain time frame before arrival may impose its demands afresh every time there is a flight delay/cancellation or an airport closure.

Additionally, governments do not publish those rules consistently through specific channels or in a standard format. Rules are published using various means like circulars, website updates or a Notice to Airmen (NOTAM).

Most airlines choose to outsource this complexity and the expense of tracking all the rules to other companies who keep track of ongoing changes and can serve multiple airlines with the same data to achieve an economical benefit to all parties. One of the key products these rule-tracking companies offer is called a Rules Engine. The Rules Engine stores the required rulesets and applies them on demand to ensure airlines satisfy the regulatory requirements for the specific circumstances of each traveler.

The job of a Rules Engine is not only to determine compliance with rules, but also to determine both what is additionally necessary to reach compliance and under what circumstances a non-compliant state may be reintroduced after compliance is satisfied (e.g., visa expiry).

As COVID-19 has put air travelers and airline employees at greater risk, the requirement to manage that risk through the interpretation of health screenings, medical documents, and passenger attestations in addition to the weight of public opinion and protecting personal privacy necessitates an integrated approach.

7.1.2 Objective of this Drafting Group

Health screening is now just as much a part of air travel as the boarding pass. The current question is no longer whether or not health screening should be done, but how it should be done for the benefit of all participants. With that in mind, the Rules Engine section of the document will describe issues with the contemporary system of asserting health status to satisfy Rules Engine requirements, and proffer a series of recommendations and standards for advancing the status quo toward an efficient system that meets the needs and respects the rights of all parties.

7.1.3 Scope of this Drafting Group

Rules Engine systems are mature and in use today for most airlines. Their scope goes far beyond passenger and flight crew health. Therefore we have focused our recommendations only on what can be improved with respect to the accurate determination of traveler health status in the context of a Rules Engine.

The following diagram is a subsystems view of how Rules Engines regarding health status might be integrated into contemporary Rules Engines. The diagram is not meant to be representative or complete with respect to Rules Engines. It is also not meant to imply that these subsystems or activities cannot be integrated into a single system. However, a monolithic implementation may reduce a system's agility in the face of the constantly developing rules seen during the pandemic. The grey boxes are out of scope for the Rules Engine section of this document but are represented for context.

7.1.3.1 Recommended Rules Engine Subsystems

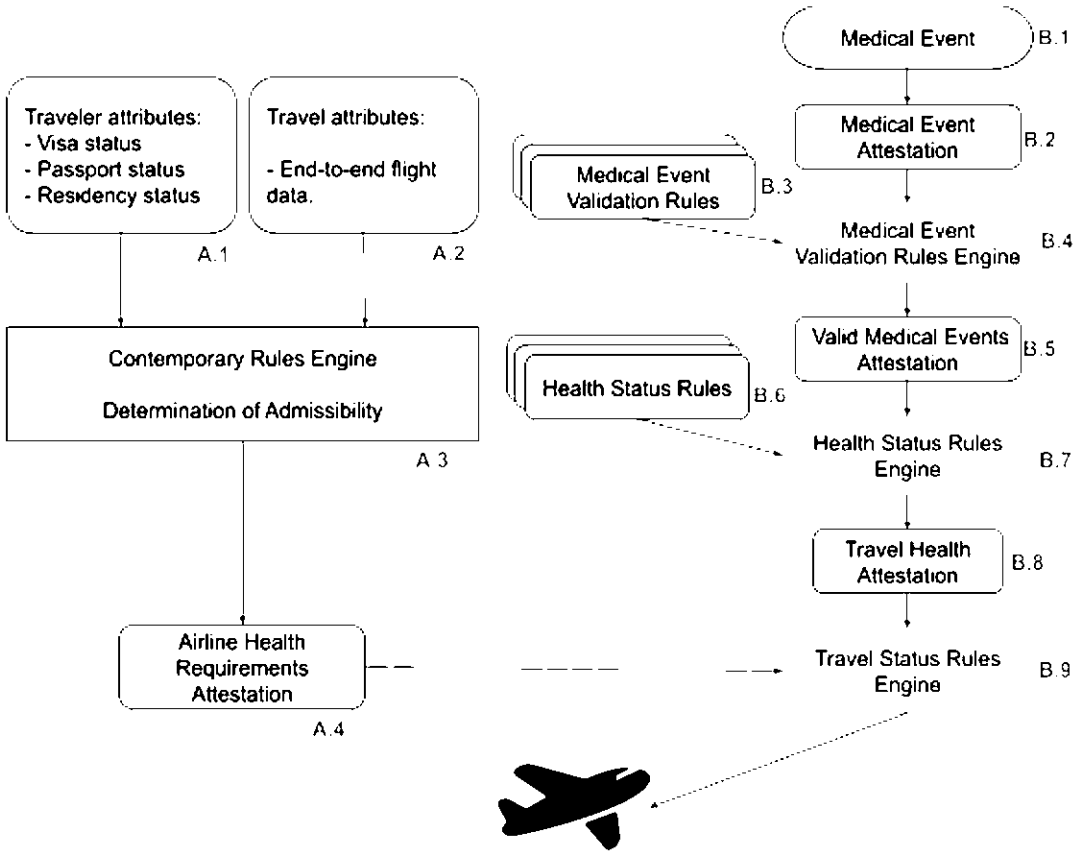

Figure 13: Subsystem view of Rules Engine Processes

7.1.3.1.1 Series A: Contemporary System

A.1: Traveler attributes include any documentation or data that is specific to the traveler. This includes any demographic information, travel documents, or personally identifiable information

collected by the airline to facilitate compliance. Some of this is self attested by the traveler if required like country of residence, or type of visit (i.e. business or leisure).

A.2: Travel attributes include any information about the flights a traveler plans to take including any rescheduling, diversions, or other changes in itinerary on a per passenger basis.

A.3: The Contemporary Rules Engine analyzes the data from A.1 and A.2 in order to determine if a traveler has what they need to travel in terms of compliance with pre-pandemic regulations and controls.

A.4: The Contemporary Rules Engine makes a health status determination based on customer attestations of their own health, screening for elevated temperatures, and other methods to reduce the risk of disease transmission. For future versions, A.5 will become the place where ad-hoc rules are applied which cannot be accommodated elsewhere including but not limited to passenger attested attributes.

7.1.3.1.2 Series B: Health Status Subsystem Additions

B.1: The medical event that helps a passenger qualify for travel. This could be a vaccination, a test, or something else.

B.2: The Medical Event Attestation is an authoritative document (paper or digital) that has the required information to determine if the passenger meets the health related requirements for travelling according to their itinerary. It is not self-attested by the passenger. This attestation can be in the form of a credential, pass, or physical verification via paper or other means.

B.3: The Medical Event Validation Rules are used to decide which presented medical event attestations are considered sufficient for use in determining health status.

B.4: The Medical Event Validation Rules Engine applies the Medical Event Validation Rules to all presented Medical Event Attestations and produces a single attestation that includes all valid evidence valuable for the determination of Health Status. This **MAY** be done for a specific context such as air travel or it can convert the many forms of Medical Event Attestations into a convenient machine readable format.

B.5: The Valid Medical Event Attestation is issued by the Medical Event Validation Rules Engine to the holder in decoupled systems or provided directly to the Health Status Rules Engine in tightly coupled systems. The Valid Medical Event Attestation **MAY** be used in multiple contexts.

B.6: The Health Status Rules are highly contextual and may come from multiple sources. They must therefore be combined and deconflicted based on their context. For air travel, the context is specific to each passenger's itinerary.

B.7: The Health Status Rules Engine determines if the passenger meets the health related requirements for traveling according to their itinerary. This is usually a complex decision based on sound medical advice or opinion and may result in either a pass/fail or a probability/risk score.

B.8: The Travel Health Attestation can be used at various stages of travel by various entities related to the specific passenger's itinerary. This includes but is not exclusive to the airline. It is not self-attested by the passenger. This attestation can be in the form of a credential, pass, or physical verification via paper or other means.

B.9: The Travel Status Rules Engine determines if all the requirements have been met for the passenger to travel under current or expected conditions.

7.1.3.2 What Does the Recommended Architecture Change?

The architecture in Figure 13 is representative of changes that have already been made, and so represents the current status quo. However, by breaking apart the subsystems and showing the component subsystems, it is both easier to understand which subsystems need the most attention, and they can be decoupled to decrease the scope of changes needed in each subsystem. Furthermore, each of these subsystems represent different areas of expertise and innovation that are necessary to implement Good Health Passes as quickly as possible.

7.1.3.3 Why Have Separate Subsystems for Medical Event Validation, Health Status, and Travel Status?

Splitting the functions of validating medical event attestations, evaluating health status and travel status in system design acknowledges several facts.

1. There is no universal Medical Event Attestation [B.2] format or requirement. Vaccination records, for example, might be digital or on paper as prescribed by the traveler's health system, local government, national government, or even the World Health Organization (WHO). Each of these formats has different risk profiles for fraudulent use. Determining the validity of any given Medical Event Attestation [B.2] will require some specialization and will rely on different data sources than the subsequent Rules Engines [B.7 and B.9]. Ideally, improvements in Medical Event Attestations [B.2] will reach a point where a Medical Event Validation Rules Engine [B.4] becomes unnecessary, but until that is universally true, those attestations [B.2] **MUST** be validated.
2. Evaluating health status is a constantly evolving task as more data becomes available with which to evaluate risks. Making the Health Status Rules Engine [B.7] a separate subsystem allows for quicker adoption of fit-for-purpose software such as Clinical Decision Support (CDS) systems to evaluate health status and provide an interoperable Travel Health Attestation [B.8] to the Travel Status Rules Engine [B.9].
3. Sometime in the near future, it will be possible for travel rules to be executed in a trusted and verifiable way on the traveler's phone without revealing any private information to the verifier. However, it is unlikely (and possibly undesirable) that this new privacy preserving capability will eradicate the need to depend on less technical solutions such as paper records. Therefore, it should be expected that the Health Status Rules Engine [B.7] **MUST** continue to handle private information that is regulated differently across national boundaries and should then remain a separate subsystem.
4. By separating the Health Status Rules Engine [B.7] from the Travel Status Rules Engine [B.9], we acknowledge that the solutions for assessing health status do not necessarily belong with the travel industry and that the healthcare industry or some other party may be better suited to create the Health Status Rules Engine [B.7].
5. Separating the Health Status Rules Engine [B.7] from the Travel Status Rules Engine [B.9] enables better portability of health passes between travel providers as long as the Travel Health Attestation [B.8] enables that portability with consistent data elements.

7.1.4 The Health Status Rules Engine

7.1.4.1 Challenge 1: Passenger Privacy

7.1.4.1.1 Problem Description

As health status requirements become more onerous for airlines and travelers, the technical simplicity of providing airlines with direct access to patient records makes it a tempting solution. This option has historical precedent. Vaccination cards have been used for decades as a medical provider's attestation regarding a health event. These health event attestations were functionally credentials because they could be used in various contexts to assert that a particular health event (a vaccination) took place.

Digital credentials, however, cannot simply be a digitized paper credential because the Internet is the world's largest copy machine. Digital credentials **MUST** have additional properties to protect the people and information they represent, prevent the inevitable copies from being usable by unauthorized entities, and prevent forgeries. The ideal digital credential should prove the holder meets entry requirements without revealing any additional information about the person or being correlatable to other contact events with the holder.

In the near term, the Health Status Rules Engine will be the subsystem most consequential to privacy outcomes. Passengers may provide Medical Event Attestations in many forms, but the Health Status Rules Engine **MUST** be able to validate those attestations through inspection or verification and produce its own attestation in the form of a pass that will be machine readable by the Travel Status Rules Engine. This pass **MUST** protect the passenger's private information while also protecting the airline from regulatory penalties due to the misuse of private information or the failure to comply with regulatory standards for traveler health status.

7.1.4.1.2 Good Health Pass Design Requirements & Considerations

In this section, we will not cover inputs to the Health Status Rules Engine. While these Health Event Attestations would ideally be digital credentials imbued with all the privacy protecting features of a Good Health Pass, this cannot be controlled nor expected by the Health Status Rules Engine. In fact, if that ever becomes a global standard, there will be no need for the Health Status Rules Engine.

7.1.4.1.3 Health Status Rules Engine Privacy Requirement:

A good Health Status Rules Engine **MUST** not collect, store, process, analyze, or retransmit data that is unnecessary for follow-on transactions with the passenger to which the data refers unless it is maintained on behalf of and with the consent of that passenger or their guardian.

7.1.4.2 Challenge 2: Health Status Rules

7.1.4.2.1 Problem Description

Establishing rules to apply within the Health Status Rules Engine is a complex issue on its own. First, one must determine what the authoritative source of rules is in a specific context. Second, one must interpret those rules and place them in a machine readable format. Finally, one must apply those rules consistently across multiple types of health event attestations (vaccination records, tests, etc.).

Providers of Rules Engines will recognize these challenges as their raison d'être. However, there are special circumstances that make health status evaluations more complex. The line of authority is not always clear as recommendations from health institutions are subjected to differing interpretations of clinical guidelines and mercurial political proclamations. This complexity is deepened by the constant

misinformation fueled by pay-per-click advertising and the malevolent intentions of state sponsored information warfare. However, Health Status Attestations are too important to allow interference from a noisy information environment. Therefore, for Health Status Attestations to have the desired efficacy, the rules that generate them should be authoritative and verifiable. Ideally, these rules would also be machine readable in a way that would facilitate automated combination and deconfliction.

Finally, it is imperative that public trust be maintained. Transparency is the only tolerable course for the application of access controls to the public. Rules being used to determine travel eligibility based on health status **MUST** be made public in both the plain language and machine readable forms. Doing so will go a long way in maintaining the trust of the public, and help the public understand what they need to do before a travel decision is funded. Eventually, rules published in a Verifiable Presentation Request format along with Medical Event Attestations in a Verifiable Credential format that supports selective disclosure could enable passengers to generate their own verifiable Health Status Attestation without ever sharing any medical or personal information.

7.1.4.2.2 Good Health Pass Design Requirements & Considerations

1. A good Health Status Rules Engine **MUST** publish both the plain language and machine readable rules along with references to the authoritative sources of those rules.
2. A good Health Status Rules Engine **SHOULD** use an open standard or published rules language.
3. A good Health Status Rules Engine **SHOULD** be able to verify the sources of the rules it is applying to passengers.
4. A good Health Status Rules Engine **SHOULD** execute rule assessments in a trusted execution environment utilizing cyber security best practices.
5. A good Health Status Rules Engine **SHOULD** provide passengers with the rules that are being applied to them either in writing or by reference.

7.1.5 The Travel Status Rules Engine

7.1.5.1 Challenge 3: User and Passenger Experience

7.1.5.1.1 Problem Description

The Travel Status Rules Engine depicted in Figure 13 represents the final decision gate regarding a passenger's eligibility to travel. The output of this Rules Engine starts when the passenger signals an intent to travel and ends when the itinerary has been completed. The Rules Engine's customer is the airline and this customer pays for the reductions in internal complexity and external risk provided by the Rules Engine. However, a Rules Engine must also consider its customer's customers. The passenger also desires less complexity and risk.

The status quo of person-to-person self-attested regulatory compliance is untenable if the regulations are to have their desired effect. Not only does the person-to-person model increase expenses and slow throughput, but it also risks the safety of passengers and employees by creating more vectors of infection. Additionally, the earlier a health status assessment can be made while still being usable for the passenger's itinerary, the more costs are reduced for airlines and passengers. Early status decisions also prevent the more frustrating late stage congestion and itinerary interruptions.

7.1.5.1.2 Good Health Pass Design Requirements & Considerations

A good Travel Status Rules Engine **MUST** accept Health Status Attestations compliant with the Good Health Pass requirements.

7.2 Recommendation #8: Trust Registries

7.2.1 Introduction to this Interoperability Challenge

Trust in the Good Health Pass (GHP) digital trust ecosystem depends on **the ability to verify that issuers – and in some cases verifiers – are authorized under a GHP-compliant governance framework**. As simple as that may sound, being able to do this securely – at scale, online or offline, across diverse jurisdictions and governance frameworks – is a non-trivial problem. This is the challenge of designing and implementing GHP-compliant **trust registries**.

7.2.2 Background

As decentralized digital trust infrastructure based on **decentralized identifiers** (DIDs) and verifiable credentials has emerged, it has introduced a new problem: how to extend trust across the trust boundaries that have traditionally been established either by: a) firewalls and internal networks, or b) hierarchical or federated public key infrastructures (PKIs).

The atomic building blocks of this new decentralized trust infrastructure are decentralized identifiers (DIDs). Currently in the final stage of standardization by the W3C (see the W3C DID Core 1.0 Specification), a DID is a new type of URI—the open standard globally unique identifiers (specified by IETF RFC 3986) that are the foundation for the World Wide Web. The big difference is that a DID is generated *cryptographically*. This means:

1. A globally unique DID can be generated without the use of a centralized registration service (such as is required with domain names, phone numbers, IP addresses, etc.)
2. Each DID can be cryptographically bound to exactly one **DID document** that contains the associated public key(s) or other metadata under the control of the DID controller.
3. The entity (person or organization) in control of a DID—called the **DID controller**—can cryptographically verify control of the DID without the use of an external service provider.
4. DIDs can be free or extremely low cost.

All of this means DIDs can be generated quickly, easily, and in volume, either by individuals or organizations as needed.

So the question becomes: how do you establish trust between entities—in particular individuals or organizations—when they each control their own DIDs?

With traditional PKI systems, such as those based on X.509 public key certificates, this is accomplished via a **public key directory** (PKD) model. In a PKD, the root of trust is a top-level directory, typically run by a **certificate authority** (CA). The root CA self-signs its own public key certificate together with the certificates of its delegates. The delegates, in turn, sign the certificates of their delegates, and so on. To verify a public key certificate in this **X.509** certificate chain, the verifier must follow the delegation links and verify the digital signatures in each of these certificates ("walk the chain") back to a root CA to establish cryptographic trust. (To establish human trust, the verifier needs to decide if it trusts the root CA.)

This same type of delegated trust infrastructure can be implemented with DIDs, only it can be simpler and more flexible. Since every DID controller generates their own DIDs and can cryptographically verify control over them, centralized CAs are no longer required to serve as roots of trust. Instead, any DID

controller can serve as its own root of trust by establishing its own **governing authority** and publishing its own **governance framework**. Then that governing authority can make the list of DIDs it trusts available to the members of its ecosystem via a network service called a **trust registry**.

Figure 14 provides a conceptual overview of where a trust registry fits into the GHP ecosystem:

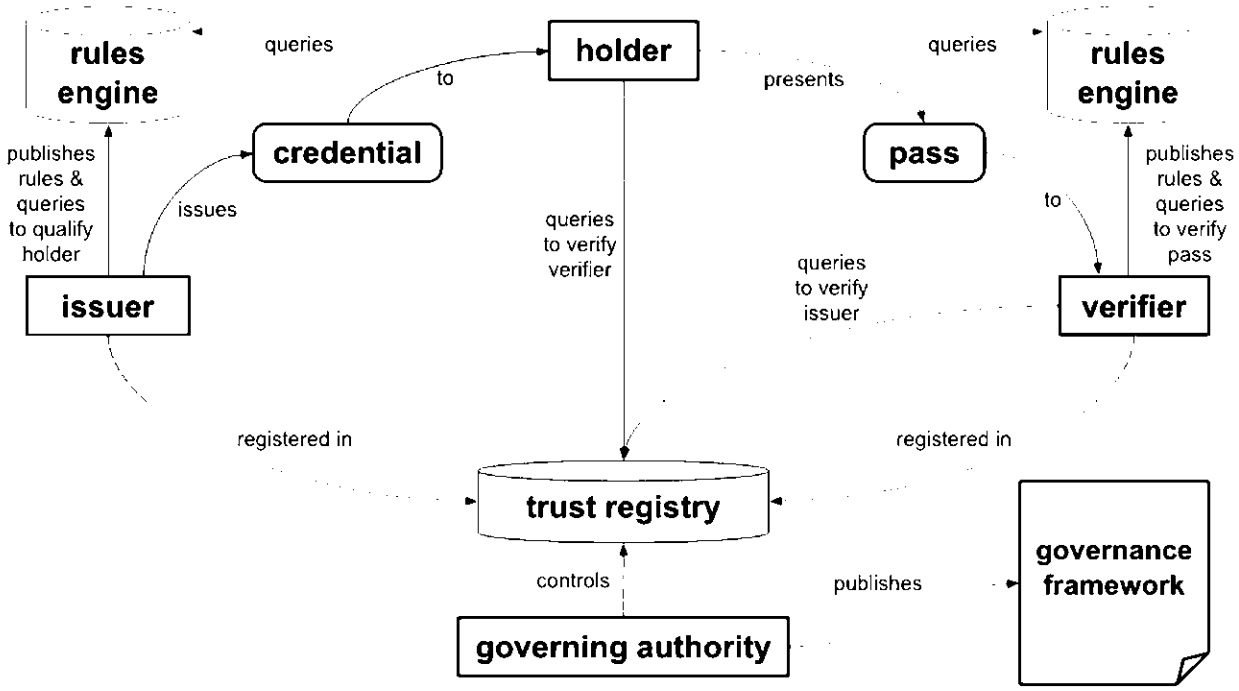

Figure 14: Conceptual overview of the Good Health Pass digital trust ecosystem showing the core role of a trust registry

It is critical to note that Figure 14 is a diagram of just one participating governing authority and its associated trust registry. The Good Health Pass digital trust ecosystem can have as many governing authorities and trust registries as are necessary to serve the overall **ecosystem of ecosystems** (see "Recommendation 9: Governance and Trust Frameworks") for more details of this governance architecture). As shown in Figure 15, all of these governing authorities and trust registries are *peers*—there is no "top-level" root of trust.

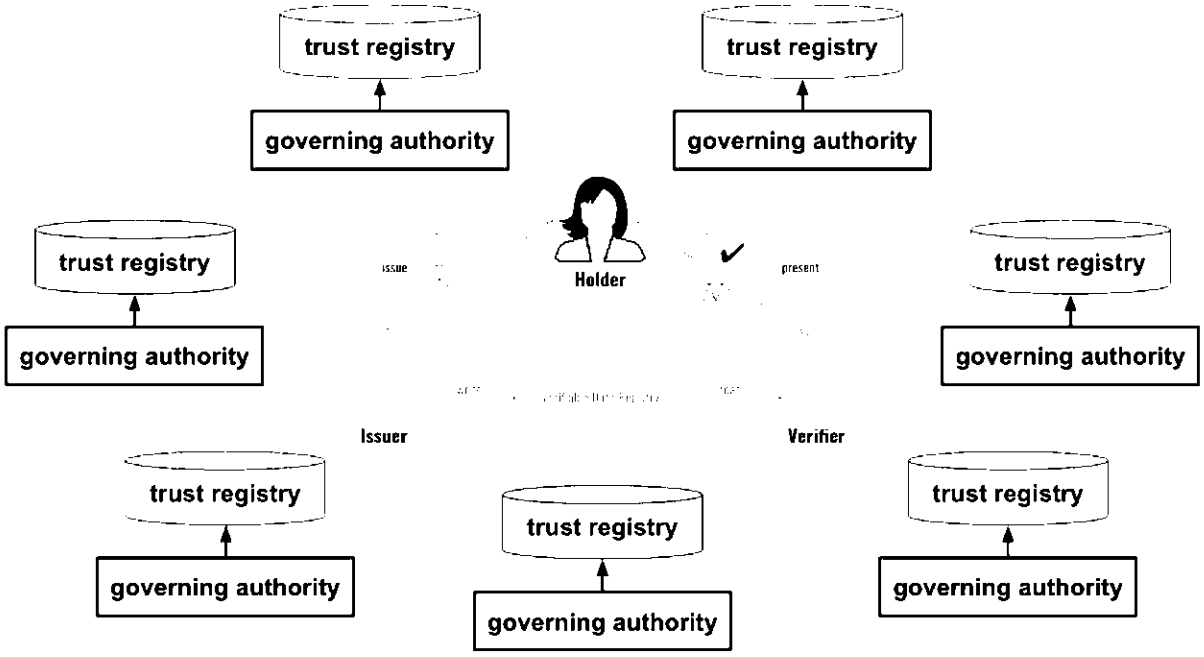

Figure 15: The peer trust architecture of the GHP decentralized PKI

Furthermore, with this **decentralized PKI** architecture, trust registries are not restricted to just supporting DIDs and DID chains—they can be designed to support both DID chains and X.509 certificate chains, thus providing a bridge between these two worlds. Architects of decentralized digital trust infrastructure at the ToIP Foundation and other industry organizations are developing specifications for this hybrid architecture.

While this hybrid trust registry architecture is the long-term ideal for the Good Health Pass digital trust ecosystem, the initial recommendations in this document only need to encompass **GHP-compliant trust registries** as shown in Figure 16 (see "Recommendation 5: Credential Formats, Signatures, and Exchange Protocols" for more about this diagram). In other words, only direct issuers of GHP-compliant health passes are required to be registered in GHP-compliant trust registries. Issuers of other non-GHP health credentials **MAY** or **MAY NOT** use GHP-compliant trust registries.

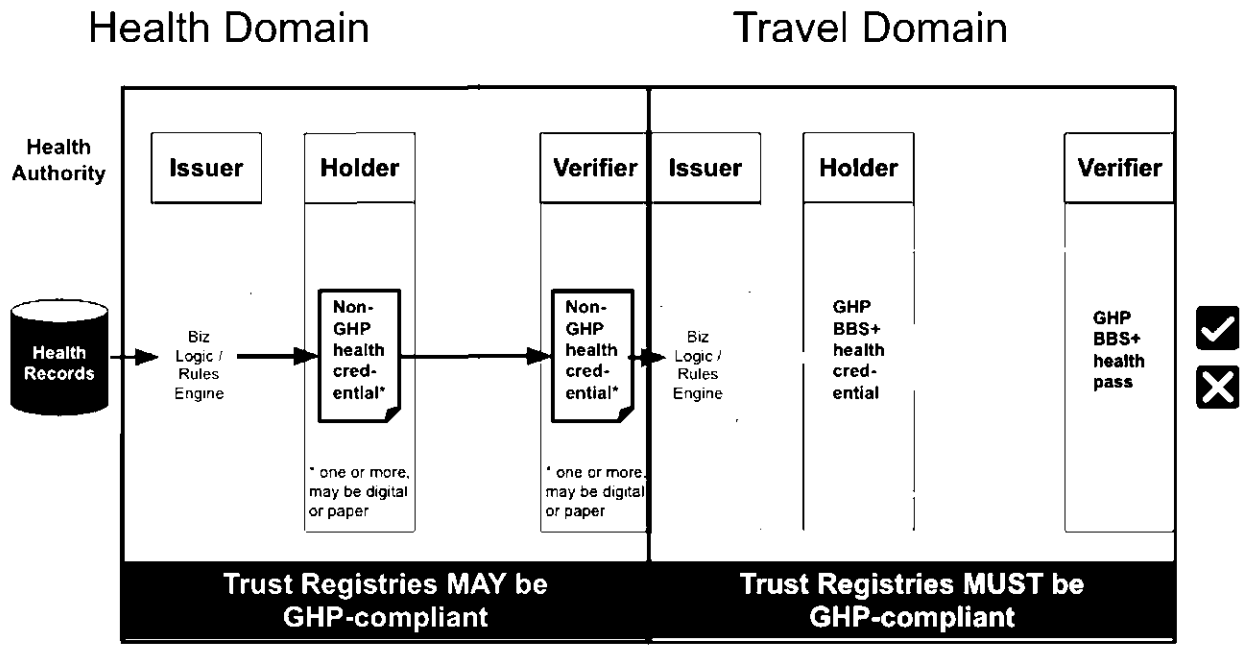

Figure 16: Direct issuers of GHP-compliant health passes **MUST** *use GHP-compliant trust registries. Issuers non-GHP health credentials are encouraged to use GHP-compliant trust registries but may use other trust registry solutions that can be verified by GHP-compliant health pass issuers.*

The "bridge" between GHP-compliant trust registries and other non-GHP trust registries (such as X.509-based PKDs) can be provided by issuers in the travel domain who choose to act as verifiers of **non-GHP health credentials** from issuers using **non-GHP trust registries**. The travel domain issuers can then issue **GHP-compliant health passes** that are verifiable using a GHP-compliant trust registry.

7.2.3 Objective of this Drafting Group

The objective is to recommend solutions for each of the key challenges in delivering a globally interoperable decentralized trust registry network, including resolving and accessing peer GHP-compliant trust registries, establishing a common trust registry protocol, verifying both authorized issuers and authorized verifiers, supporting offline verification, and providing sufficient trust assurance. These objectives will be met if the recommended design is: a) compatible with the GHP Principles, b) consistent with the other GHP recommendations, and c) enables GHP ecosystem members to answer two basic questions:

1. Is an issuer authorized to issue a specific type of credential or pass under a specific ecosystem governance framework (EGF)?
2. Is a verifier authorized to request a specific type of credential or pass under a specific EGF?

7.2.4 Problem #1: How can a verifier know an issuer is authoritative in the GHP digital trust ecosystem?

7.2.4.1 Problem Description

To verify a proof of a GHP-compliant digital health credential or pass from a holder, a verifier needs to answer the following questions:

1. Was the credential or pass issued by an issuer authorized under a **GHP-compliant specific ecosystem governance framework** (EGF) to issue that type of credential or pass at the time it was issued?
2. Is the digital signature on the proof verifiable using the issuer's public key?
3. Does the proof contain the data necessary for the verifier to make a **trust decision**?

GHP trust registry architecture is designed to answer the first question. Strictly speaking, the second question is out of scope, however our proposed DID-based design will also enable the verifier to obtain and verify the issuer's public key. The third question is out of scope for GHP.

7.2.4.2 Good Health Pass Design Requirements and Considerations

To be consistent with the rest of the GHP recommendations, the Trust Registries group established the following high-level design principles:

1. **Decentralized peer trust**. The design **MUST** not require a single root of trust, but rather support a peer trust model between all participating governing authorities that enables each authority to determine its own policies for registering:
    a. Issuers.
    b. Verifiers.
    c. Other peer trust registries.
2. **Simplicity**. The design **SHOULD** be as simple as possible to encourage rapid development, a minimal attack surface, and broad adoption. GHP **SHOULD** not push design constraints on implementers beyond the most basic requirements.
3. **Open standard**. Although the design **MAY** enable access control for governing authorities who require it, it **MUST** be based on easy-to-implement open standard royalty-free specifications.
4. **Protocol-based**. The design **MUST** not specify or rely on any specific trust registry implementation, but rely only on a common interoperable trust registry protocol. How a governance authority implements the back-end system for a trust registry (e.g., database, directory, or distributed ledger technology; administration; redundancy; backup; scalability, etc.) is out of scope for these recommendations.
5. **Performant**. The design **SHOULD** respond to trust registry queries with approximately the same performance as high-performing commercial websites.

7.2.4.3 Recommendations

7.2.4.3.1 Governing Authorities

A GHP-compliant governing authority:

1. **MUST** publish at least one **trust registry DID** in their specific EGF.

2. **MUST** specify at least one **trust registry service endpoint** for issue authorization in the associated DID document using the **trust registry service endpoint type URI** specified in the **GHP Trust Registry Protocol Specification**.

7.2.4.3.2 Trust Registries

A GHP-compliant trust registry:

1. **MUST** be identified by a trust registry DID generated using a GHP-compliant DID method.
2. **MUST** support all mandated requirements of the **GHP Trust Registry Protocol Specification**.
3. **SHOULD** incorporate throttling, DDOS protection, etc.
4. **MAY** limit the DID methods permitted to be used for the registered DIDs to a subset of the GHP-compliant DID methods.

7.2.4.3.3 Trust Registry Protocol

The GHP trust registry protocol:

1. **MUST** be an open standard royalty-free specification.
2. **MUST** be specified in either:
    2.1. A GHP Trust Registry Protocol Specification.
    2.2. A more general purpose trust registry protocol specification if it meets all the requirements in these recommendations.
3. **MUST** support trust registry service endpoint resolution using GHP-compliant DID methods.
    3.1. **SHOULD** support the **GHP X.509 Subject Alternative Name URI Specification**
4. **MUST** provide a registration method.
5. **SHOULD** provide a revocation method.
6. **SHOULD** provide a verifier access request method.
7. **MUST** support queries consisting of the following parameters to enable issuer authorization:
    7.1. Trust registry DID
    7.2. Issuer DID
    7.3. Verifiable credential type URI
8. **MUST** support queries of the following parameters for cross-registration of peer trust registries
    8.1. Trust registry DID
    8.2. Verifiable credential type URI
    8.3. Verifiable credential issuance date
9. **MUST** return exactly one of the following status values:
    9.1. Not found
    9.2. Current
    9.3. Expired (not renewed after the previous valid registration period)
    9.4. Terminated (voluntarily terminated by the issuer)
    9.5. Revoked (involuntarily terminated by the governing authority)
10. **MUST** return exactly two date values (formatted to comply with RFC3339, as UTC/Z - with no offset):
    10.1. AuthorizationStartDate - which indicates the data that the Issuer's authorization started.
    10.2. AuthorizationEndDate - which may be null for Issuers that are currently, at time of the query, an Authorized Issuer. If an Issuer is not currently an Authorized Issuer, the date that they lost that status will be returned.

7.2.4.3.4 Issuers

GHP-compliant issuers:

1. **MUST** be identified by an **issuer DID** generated using a GHP-compliant DID method.
2. **MUST** register the issuer DID in the trust registry of any specific EGF under which the issuer wishes to issue GHP-compliant credentials.
3. **MUST** issue GHP-compliant verifiable credentials that meet the following requirements:
   3.1. The verifiable credential includes a claim specified in the GHP Verifiable Credentials Specification whose value is the **trust registry DID** for the specific EGF under which the credential or pass was issued.
   3.2. The value of the verifiable credential issuer ID is the **issuer DID** registered in the trust registry identified by the trust registry DID.
   3.3. The value of the verifiable credential type is a **GHP credential type URI** specified in the GHP EGF.

7.2.4.4 Recommended Timelines

7.2.4.4.1 Phase One (30 Day Horizon)

GHP-compliant specific governing authorities:

1. **SHOULD** manually maintain a list of authorized issuers in a DID document using a did:web: URL as specified GHP Trust Registry Protocol Specification.
2. **SHOULD** participate in development of the GHP Trust Registry Protocol Specification.
3. **SHOULD** publish their trust registry development plans.

7.2.4.4.2 Phase Two (90 Day Horizon)

GHP-compliant specific governing authorities:

1. **SHOULD** publish their trust registry policies and specifications in their specific EGF.
2. **SHOULD** have their trust registry implemented.
3. **SHOULD** pass a GHP-compliant trust registry protocol test suite.
4. **SHOULD** maintain a list of the trust registry DIDs of other GHP-compliant peer governing authorities.

7.2.4.4.3 Phase Three (180 Day Horizon)

GHP-compliant specific governing authorities:

1. **MUST** have implemented a GHP-compliant trust registry.
2. **MUST** meet all requirements in their specific EGF.

7.2.5 Problem #2: How can a holder verify an authorized verifier in the GHP digital trust ecosystem?

7.2.5.1 Problem Description

In some cases, the governing authority for a specific EGF **MAY** wish to support a specific privacy and data protection feature for holders using GHP-compliant digital wallets within its ecosystem: verifier authorization. This can take one of two forms:

1. **Required authorization of verifiers**. In this case the trust registry for the specific EGF will not allow access to unauthorized verifiers, so they are unable to fully verify a GHP-compliant credential issued under that specific EGF.
2. **Holder warning of unauthorized verifiers**. In this case an unauthorized verifier still has access to the trust registry, but a GHP-compliant wallet will automatically warn the holder when it receives a presentation request from an unauthorized verifier.

This capability, often referred to as "verifying the verifier", is illustrated in Figure 17.

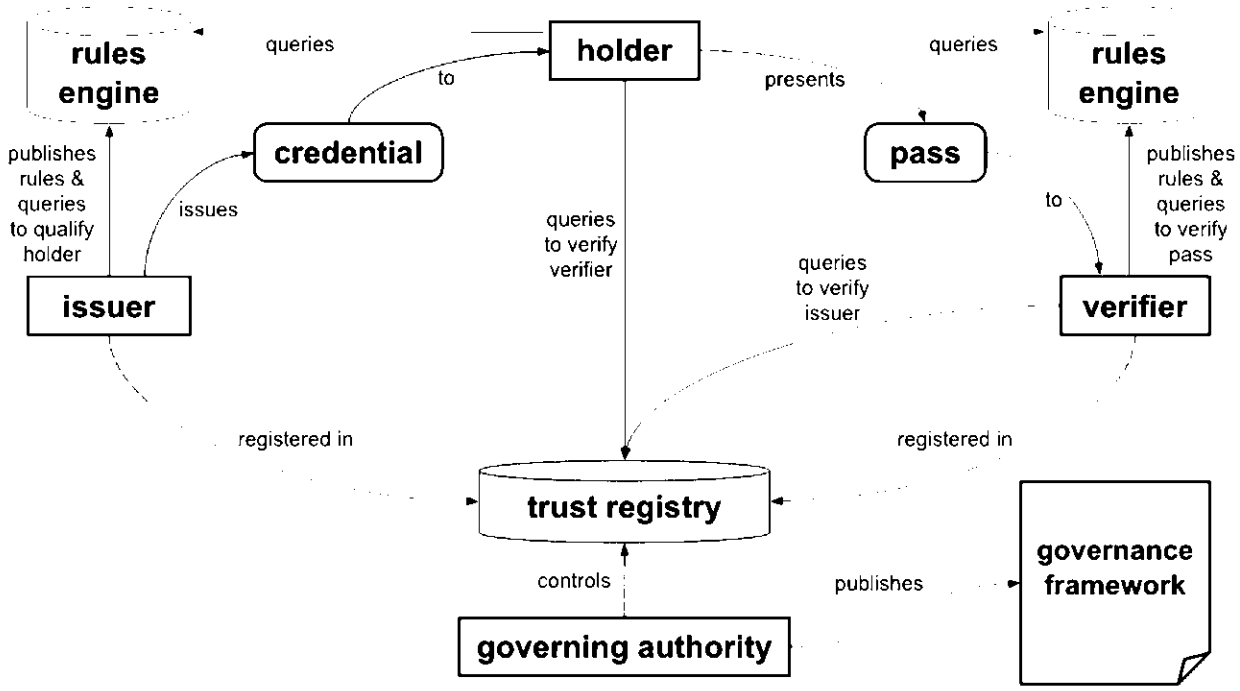

Figure 17: If supported in a specific EGF, a holder's digital wallet can query the trust registry for that ecosystem to verify that a verifier is authorized

7.2.5.2 Good Health Pass Design Requirements and Considerations

The preceding requirements for the GHP Trust Registry Protocol Specification are easily extended to include verifier authorization.

7.2.5.3 Recommendations

7.2.5.3.1 Governing Authorities

A GHP-compliant governing authority:

1. **MAY** specify requirements for verifier authorization in their specific EGF.
2. **MAY** specify a separate **trust registry service endpoint** for verifier authorization in the associated DID document using the **trust registry service endpoint type URI** specified in the **GHP Trust Registry Protocol Specification**.

7.2.5.3.2 Trust Registry Protocol

The GHP trust registry protocol:

1. **MUST** support queries consisting of the following parameters to enable verifier authorization:
   1.1. Verifier DID
   1.2. Presentation definition type URI
   1.3. Request datetime
2. **MUST** return exactly one of the following status values:
   2.1. Not found
   2.2. Current
   2.3. Expired (not renewed after the previous valid registration period)
   2.4. Terminated (voluntarily terminated by the issuer)
   2.5. Revoked (involuntarily terminated by the governing authority)

7.2.5.3.3 Verifiers

GHP-compliant verifiers:

1. **MUST** comply with the verifier authorization requirements of a specific EGF if the verifier wishes to request GHP-compliant credentials issued under that specific EGF.
2. **MUST** be identified by a **verifier DID** generated using a GHP-compliant DID method.
3. **MUST** make a GHP-compliant presentation request that meets the following requirements:
   3.1. The presentation request includes the **verifier DID** and the **GHP presentation definition URI**.
   3.2. The presentation request is digitally signed by the verifier using the private key associated with the **verifier DID** (See section 4.5 of DIF Presentation Exchange v1.0.0).

7.2.5.3 Recommended Timelines

This trust registry feature **SHOULD** be implemented by the specific governing authorities who require it on the same timeline as issuer authorization (Problem #1).

7.2.6 Problem #3: How can a GHP-compliant trust registry support offline verification if needed?

7.2.6.1 Problem Description

In some situations, verifiers may not have access to online trust registries. Examples include poor or lapsed connectivity (e.g., remote border crossings), firewall restrictions, or networks that are air-gapped for security reasons. In other cases offline caching may be required for performance reasons. For all these reasons, GHP trust registry architecture **SHOULD** support offline verification of authorized issuers. (Offline verification of authorized verifiers by holders is considered such a small edge case that it will not be addressed).

7.2.6.2 Good Health Pass Design Requirements and Considerations

Offline replication of directories and PKDs is a well-understood problem space. Furthermore, the simplicity of the GHP trust registry design and GHP Trust Registry Protocol Specification should make it relatively straightforward to add support for offline verification. However any data synchronization protocol that also needs to be secure and reliable is non-trivial to implement.

7.2.6.3 Recommendations

7.2.6.3.1 Governing Authorities

A GHP-compliant governing authority:

1. **MUST** specify their specific EGF whether their trust registry service supports offline verification.

7.2.6.3.2 Trust Registries

If required by its governing authority, a GHP-compliant trust registry:

1. **MUST** implement support for data synchronization as specified in the **GHP Trust Registry Protocol Specification**.

7.2.6.3.3 Trust Registry Protocol

The GHP trust registry protocol:

1. **MUST** specify at least one data synchronization method (such as batch downloading) for offline usage.

7.2.6.3.4 Verifiers

GHP-compliant verifiers::

1. **MAY** implement offline verification if supported by a trust registry.
2. **MUST** follow cache refresh or other offline verification policies specified in the specific EGF.

7.2.6.4 Recommended Timelines

Offline verification **SHOULD** be implemented as demand arises in the GHP ecosystem.

7.2.7 Problem #4: How can a GHP-compliant trust registry provide a high level of trust assurance?

7.2.7.1 Problem Description

Trust in a GHP trust registry is rooted in its governing authority, its specific EGF, and most concretely in the **trust assurance framework** section of the specific EGF. The challenge is how GHP-compliant trust registries and their associated trust assurance frameworks should be designed to provide high levels of trust assurance.

7.2.7.2 Good Health Pass Design Requirements and Considerations

The design of a trust assurance framework for a trust registry is a complex problem that depends on many factors unique to the governing authority, the trust registry implementation, and the digital trust ecosystem being served. There is no single path to managing trust, rather it is a layered process that involves intent, activities and controls. Aspects of managing trust that are particularly important to the implementation and operation of a GHP-compliant trust registry include:

- Credibility
- Reputation

- Protection of trust registry participants
- Operational performance
- Indemnification and operation within a trusted legal jurisdiction

7.2.7.3 Recommendations

NOTE: Implementing these recommendations can vary from trivial to very complex depending on the risk exposure associated with the trust registry operator(s) and users. The following is intended to be an essential list of items to consider, but **SHOULD** be addressed at a level appropriate for each implementer. There are very few **MUSTs**, and a wide latitude is allowed for how they are addressed.

7.2.7.3.1 Governing Authorities

In a GHP-compliant specific EGF, a governing authority:

1. **MUST** follow industry best practices to the extent possible in the design, implementation and operation of the technical components of the trust registry.
2. **MUST** define the operational constraints, obligations, authority and other permitted actions of the trust registry operator
3. **MUST** define the relationship(s) between the trust registry operator and parties allowed to make changes to the registry
4. **MUST** define the relationship(s) between the trust registry operator and the consumers of the data maintained by the registry
5. **MUST** establish policies providing sufficient monitoring and enforcement of the requirements of the specific EGF that apply to the trust registry operator.
6. **MUST** clearly identify who holds legal liability for the data contained in registries and properly indemnify the trust registry operator for its role in maintaining the registry.
7. **SHOULD** promote transparency, peer review, ongoing awareness of system flaws and correction of important flaws.
8. **SHOULD** ensure the trust registry operator has sufficient capital and resources to maintain levels of operational availability that are appropriate for the participants of the trust registry ecosystem.

7.2.7.3.2 Trust Registry Operators

Operators of GHP-compliant trust registries:

1. **MUST** employ detection and prevention controls to restrict and log participants creating and updating entries in the registry.
2. **MUST** be able to enforce accountability of the parties permitted to alter the registry in conformance with trust registry requirements.
3. **SHOULD** seek to maintain reputational trust by continuously and vigorously addressing both internal and external issues that would serve to diminish the perception of the operator, including public relations issues, solvency issues, accuracy issues, security issues, system performance issues, inappropriate actions by executives, employees, partners and participants, as well as others.
4. **SHOULD** establish and maintain criteria to identify and screen candidates for participation that align with the goals and expectations of the trust registry.
5. **SHOULD** establish and maintain criteria for expected performance memorialized in a formal service level agreement between the operator and external participant.
6. **SHOULD** have formal mechanisms in place to:

6.1. Limit the possibility that private or proprietary information may be leaked to unauthorized parties.
6.2. Remediate the effects of leaked information identified in breaches and address root causes.
6.3. Periodically audit the accuracy and integrity of data maintained by each role defined in its trust assurance framework.
6.4. Remediate control deficiencies identified within audits.

7. **MUST** set expectations with participants regarding operational availability.
   7.1. It is anticipated that ecosystem availability needs **MAY** vary widely. Some trust ecosystems **MAY** require global 24/7 operation of a trust registry to meet the needs of its participants whereas others **MAY** only require part-time or intermittent operation. The key is that the level of operations **MUST** sufficiently match the expectations of the participants.
8. **SHOULD** minimize operational downtime and performance degradation resulting from issues that could be reasonably anticipated (e.g., funding, political, infrastructure, technical, process and people).
9. **SHOULD** implement operational practices to minimize impact, mitigate damages and hasten recovery of anticipated potential downtime or performance degradation events.
10. **SHOULD** put technical controls in place with system users to protect the system from low and inconsistent performance and responsiveness.
11. **SHOULD** have actionable plans in place to mitigate the impact of sub-optimal capital and resources.
12. **SHOULD** have plans in place to limit the duration of any negative impact.
13. **SHOULD**, in the event that operations can no longer be sustained or a decision is made to cease operations, either:
    13.1. Seek an orderly transfer of data and operations to another GHP-compliant trust registry operator, or
    13.2. Seek an orderly shutdown which includes proper disposition of data according to jurisdictional requirements and notification of the originators and consumers of registry data.

7.2.7.4 Recommended Timelines

Governing authorities **SHOULD** follow the recommendations in this section as they apply to the each of the trust registry implementation phases recommended in Problem #1.

7.2.8 Interoperability Testing Recommendations

1. A test suite for implementations of the **GHP Trust Registry Protocol** described in these recommendations **SHOULD** be developed in parallel with the specification of the protocol itself.
2. Implementations of GHP-compliant trust registries **SHOULD** begin testing against this test suite as soon as possible.
3. A GHP Trust Registry Technical Implementation Guide **SHOULD** be developed in conjunction with the development of the specifications and test suite.

7.3 Recommendation #9: Governance and Trust Frameworks

7.3.1 Introduction to this Interoperability Challenge

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 policies and rules they will follow to achieve their trust objectives. This collection of policies, rules, and specifications is called a **governance framework** – a term that includes a **trust framework** (as that term is generally used in public key infrastructure (PKI) and federated identity systems) along with additional governance components needed for **transitive trust** across independent digital trust ecosystems.

As decentralized digital trust infrastructure has evolved, governance frameworks are also being specialized for each layer of infrastructure. In particular, the Trust over IP (ToIP) Foundation is developing standard models and best practices for governance frameworks for each of the four layers of the **ToIP stack** as shown in Figure 18.

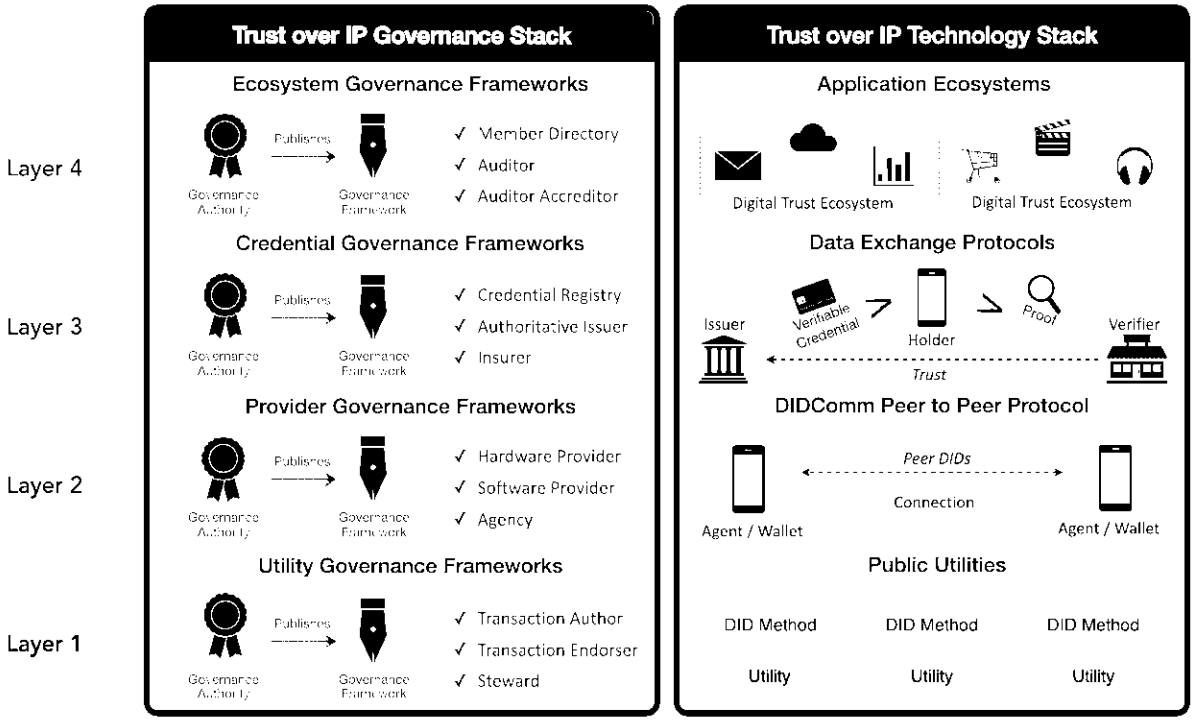

Figure 18: The four layers of governance in the ToIP stack for decentralized digital trust infrastructure

From this perspective, the goal of the Good Health Pass Collaborative (GHPC) is to create a complete ToIP Layer 4 **digital trust ecosystem** that is governed by an **ecosystem governance framework**. Given the global scope, multiple stakeholders, overall complexity, and urgency of the task, development of this governance framework is one of the most critical tasks for the GHPC. This document will convey the overall recommendations of the Governance Framework Drafting Group for the development and deployment of the **Good Health Pass Ecosystem Governance Framework**.

7.3.2 Background

The COVID-19 pandemic and its devastating effects on societies and economies are well documented – governments worldwide have adopted various restrictions on mobility and public gatherings to limit the virus' spread. Vaccination campaigns are underway globally, and health systems or solutions meant to alleviate the pandemic's effects have been pressed into service with the goal of safely reopening society as soon as possible.

To prevent these initiatives from operating as a series of unconnected solutions that enable siloing, vulnerability, and mismanagement of user health data, the GHPC has focused on solving the key challenges to interoperability – the problems we need to solve to standardize information sharing mechanisms and achieve scalability, greater efficiency, heightened privacy and transparency, and a seamless experience for individuals.

Many of those problems are technical, and some involve agreement on user experience and education. But the remaining challenges all fall into policy – the business, legal, and operational policies that are needed to turn the technical solutions into full production-ready, scalable market solutions.

Designing those policy frameworks to work together – to fit with each other like Lego blocks as smoothly as the technical pieces fit together – is the job of governance framework standards such as those under development by the Governance Stack Working Group at the ToIP Foundation. This is what provides the overall solution architecture for the governance frameworks required for the Good Health Pass digital trust ecosystem.

7.3.3 Objective of this Drafting Group

The **Good Health Pass Interoperability Blueprint** (GHP Blueprint) and the **Good Health Pass Ecosystem Governance Framework** (GHP EGF)together provide a vision for the Good Health Pass digital trust ecosystem. This vision is rooted in the premise that the challenges of transitive trust across all of the jurisdictions and stakeholders in international travel is sufficiently complex that it constitutes an **ecosystem of ecosystems** in which each constituent ecosystem needs its own ecosystem governance framework. The objective of this Drafting Group is to recommend how to establish this worldwide infrastructure of collaborating governance frameworks.

7.3.4 Good Health Pass Digital Trust Architecture

The GHP EGF is a ToIP Layer 4 ecosystem governance framework developed according to the ToIP Governance Metamodel defined by the ToIP Governance Stack Working Group. The metamodel reflects five years of industry experience about the categories of policies needed to support transitive trust within and across multiple digital trust ecosystems – the same kind of trust that we exercise constantly in legal, business, and social relationships in the real world. Development of ecosystem governance frameworks based on the ToIP governance metamodel also follows best practices developed by the ToIP Ecosystem Foundry Working Group.

The GHP EGF plays a special role in the **Good Health Pass digital trust ecosystem**: it is a **general ecosystem governance framework** (**general EGF**) that specifies the requirements for any number of specific ecosystem governance frameworks (specific EGFs) that serve different **trust communities** within the overall ecosystem. It is very important to note that this is not a hierarchical "delegation" relationship. A

general EGF is simply a "class" that defines the overall requirements for all of the "instances" just like all class/instance relationships as shown in Figure 19.

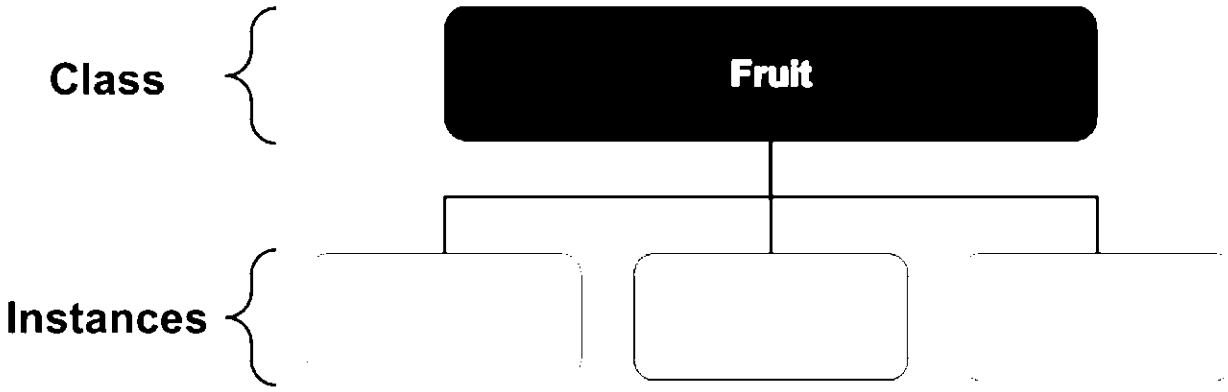

Figure 19: Class/instance relationships are inheritance, not hierarchy

In any large digital trust ecosystem, the stakeholders can follow this class/instance pattern to collaboratively develop a general EGF as their "class", and then all of the stakeholders can develop their own specific EGF as an "instance" as shown in Figure 20.

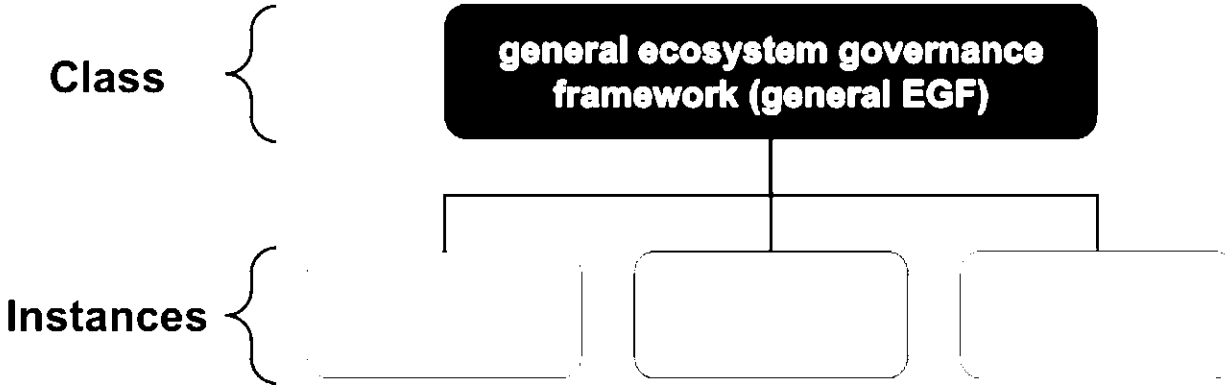

Figure 20: The class/instance relationships of general and specific EGFs

Applying this ecosystem of ecosystems governance framework architecture to the Good Health Pass digital trust ecosystem yields the governance framework relationships in Figure 21.

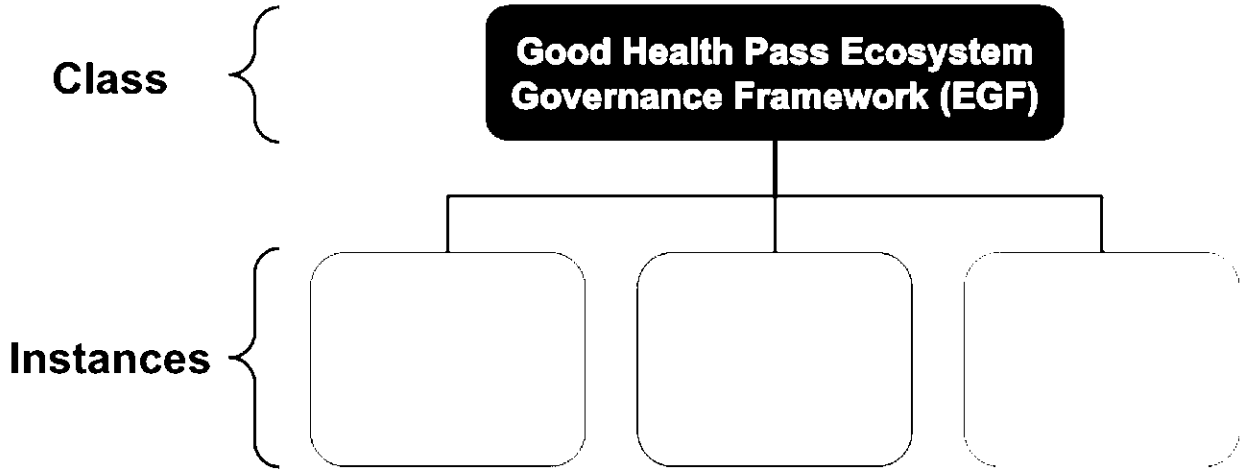

Figure 21: The relationship of the GHP EGF as a general ecosystem governance framework and the specific EGFs that conform to it

Each specific EGF is developed, published, and maintained by a specific governing authority to meet the requirements of a specific jurisdiction, industry, or other trust community. This architecture embraces local law, culture, and diversity while still enabling interoperability and transitive trust across the overall ecosystem.

Again, the relationship of the GHP EGF as a general EGF to the GHP-compliant specific EGFs is not a hierarchical delegation relationship. In other words, the governing authority for the GHP EGF does not have any direct authority over the governing authorities for each of the specific EGFs. Rather the only power the general EGF governing authority has is to make revisions to the general EGF. As these revisions are made, each of the specific EGF governing authorities can make their own decisions about complying with those revisions if they have sufficient incentive to continue to maintain interoperability across the ecosystem of ecosystems.

7.3.5 The GHP Governance Framework Development Process

The vision of the **GHP Blueprint** and the **GHP EGF** Recommendation cannot be realized solely by its cross-industry group authors. It will require building a community of ecosystems and parties within them committed to adopting these recommendations and creating **GHP-compliant** solutions. It will also require forming an official **governing authority** for the GHP EGF whose job is to:

1. Complete and approve the official first version of the GHP EGF derived from the EGF Recommendation.
2. Publish and maintain a dedicated website hosting the official GHP EGF documents.
3. Gather feedback and develop future versions based on the "in-the-field" experience of implementing V1 as well as changes in other external factors such as regulations and health authority guidelines.

In keeping with the principles of good governance, the Governance Framework drafting group recommends that the GHP governing authority be formed and governed by the primary stakeholders in the GHP digital trust ecosystem. For purposes of this document, we will refer to the official governing authority resulting from this process as the **GHP Foundation**. *However this is just a placeholder name*

and we are soliciting feedback about the role of this governing authority organization during the public review of these recommendations. We recommend that the initial process of bootstrapping the GHP Foundation be the responsibility of the **Good Health Pass Collaborative** (**GHPC**).

7.3.5.1 Stages of EGF Development

Based on the input of the ToIP Governance Stack Working Group and the IEEE 2145 Blockchain Governance Standards Working Group, both of whose members participated in the GHP Governance Framework drafting group, we RECOMMEND the following bootstrap process:

1. Initially, the GHPC will serve as an **interim EGF governing authority** responsible for stewardship of development of the GHP EGF, and convening the first set of governing authorities committing to implement the GHP EGF.
2. These governing authorities will implement the GHP EGF by creating their specific EGFs in conformance with the requirements of the GHP EGF Recommendation. Each of them will build and support their community of participating stakeholders (issuers, verifiers and auditors) under their EGF.
3. These governing authorities will formally organize to create the GHP Foundation for long term governance of the GHP EGF. The GHP Foundation will develop the governance policies for the GHP Foundation itself – for example, requirements for who can join the GHP Foundation, who is authorized to make decisions about membership, and approval of the deliverables such as new versions of the GHP EGF.) The GHP Foundation will also be entrusted to grow the GHP Foundation membership of participating specific EGF governing authorities.
4. The GHP Foundation will approve the official GHP EGF V1, maintain subsequent versions, and support the GHP Foundation members as they continue to implement the GHP EGF and create their specific EGFs.

Figure 22 shows the progression across four stages of development and the division of responsibilities at each stage between **GHPC**, the **specific governing authorities** who represent the primary stakeholders creating specific EGFs, and the **GHP Foundation** that will take on the long-term governance of the GHP ecosystem and deliverables.

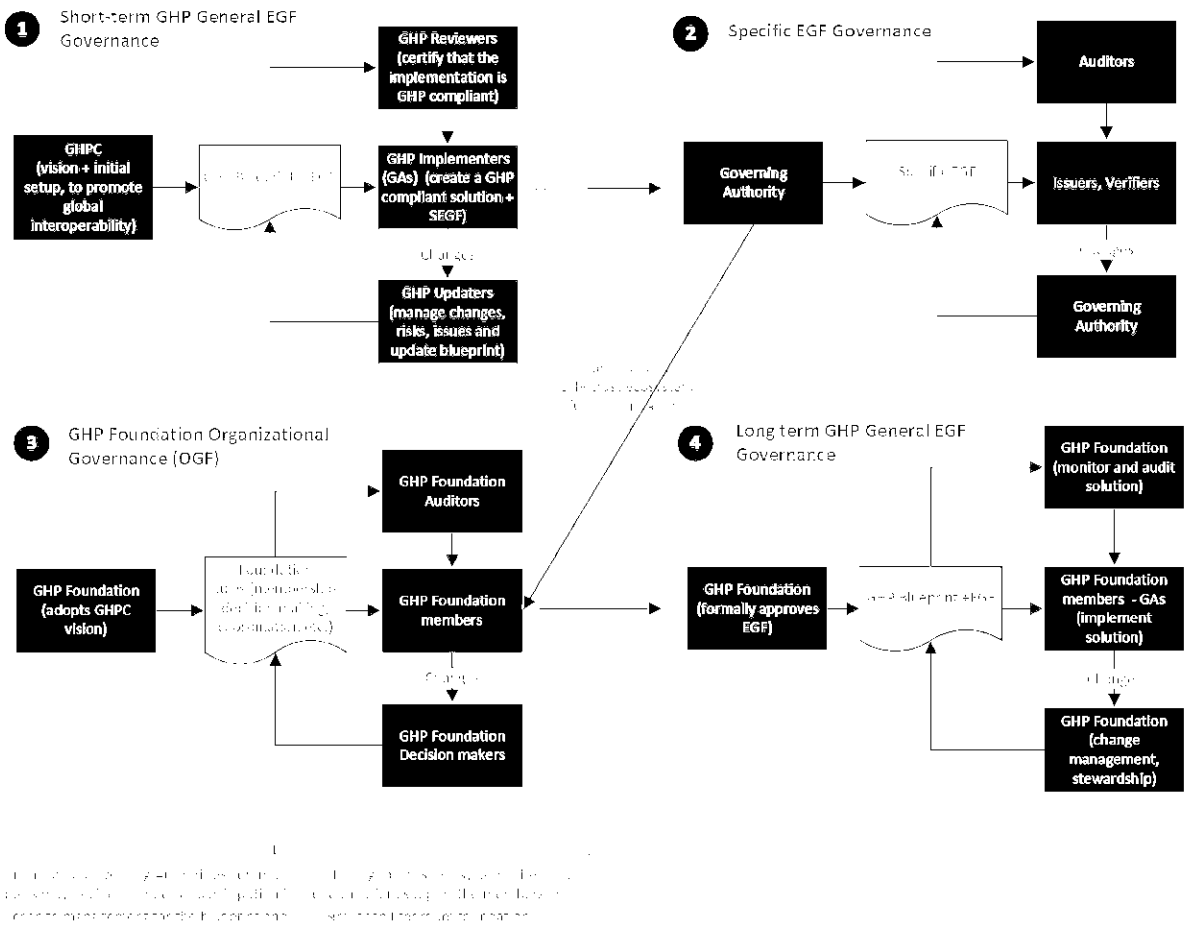

Figure 22: The four stages of development of governance for the Good Health Pass digital trust ecosystem

7.3.6 Recommendations

Following are specific recommendations for progressing through each of the four stages.

7.3.6.1 Stage 1: Initial GHP General EGF Governance

1. GPHC **SHALL** publish the GHP Blueprint and GHP EGF Recommendations.
2. Simultaneously, GHPC **SHALL** invite specific governing authorities to participate in the establishment of the GHP Foundation and create their specific EGFs.
3. GHPC **SHALL** assist in onboarding the participating governing authorities as early adopters and facilitate coordination and collaboration amongst them.
4. Specific governing authorities **SHALL** comply with the GHP Blueprint and GHP EGF Recommendations to create GHP-compliant specific EGFs.
   4.1. GHPC **SHOULD** support these early adopters to help establish baselines and benchmarks for the global ecosystem.
5. Specific governing authorities **MUST** self-attest their compliance with the GHP EGF Recommendations.
   5.1. GHPC **SHOULD** review the self-attestations and certify compliance.

6. Specific governing authorities **MAY** report issues faced during the implementation and propose changes to the GHP EGF.
    6.1. GHPC **SHOULD** adopt proposed changes judged to be beneficial to the Good Health Pass digital trust ecosystem.

7.3.6.2 Stage 2: Specific EGF Governance

1. Participating specific governing authorities **MUST** complete their V1 specific EGFs in compliance with the requirements in the GHP EGF.
2. Governed actors such as issuers, verifiers, and trust registries participating in a specific EGF **SHOULD** complete their implementations in compliance with the GHP EGF.
    2.1. The governing authority **SHOULD** establish a support structure to assist the governed actors.
3. If the specific EGF specifies conformance auditing:
    3.1. The governing authority **MUST** appoint auditors meeting the requirements in the specific EGF.
    3.2. Auditors **MUST** perform the audit function for a governed party as specified by the trust assurance framework.
    3.3. If a governed party is in compliance, the auditor **MUST** provide an attestation of compliance as specified by trust assurance framework.
    3.4. If the governed party is not in compliance, the governed party **MUST** remediate non-compliances in accordance with the trust assurance framework.
4. Revisions to the EGF **MAY** be made for any of the following reasons:
    4.1. Governed parties raise risks, issues, or improvements.
    4.2. Changes due to external factors such as new regulations.
    4.3. Changes due to a revision of the GHP EGF.
5. Governing authorities **SHOULD** create a Risk/Change Management Board or similar governing body to address risks, issues and changes to its specific EGF.

7.3.6.3 Stage 3: Formation of the GHP Foundation

1. Participating governing authorities **MUST** formally organize and create the GHP Foundation.
2. The GHP Foundation **MUST** replace the GHPC's interim governance role and take on the following responsibilities:
    2.1. Building a strong GHP digital trust ecosystem of ecosystems.
    2.2. Administering and revising the GHP EGF, including monitoring and revising governance of the GHP Foundation itself.

7.3.6.4 Stage 4: Ongoing GHP EGF Governance

1. Once it is officially established, the GHP Foundation **MUST**:
    1.1. Onboard initial members.
    1.2. Approve the GHP Ecosystem Governance Framework V1.
2. The GHP Foundation **SHOULD** provide support for members implementing GHP-compliant specific EGF.
3. The GHP Foundation **SHOULD** perform a risk assessment and generate a risk treatment plan to address identified risks.
4. The GHP Foundation **SHOULD** establish a certification process for GHP-compliant specific EGF as part of the trust assurance framework of the GHP EGF.
    4.1. The trust assurance framework **SHOULD** include a trust mark.

4.2. This process **MAY** include self-attestation.

5. The GHP Foundation **SHOULD** follow a change management process to review proposed changes, assess the impact and make revisions to the EGF, if necessary.

7.3.7 Governance Matrix for the EGF Development

The four stage GHP EGF development process above shows multiple parties collaborating at each stage to meet the objectives. To facilitate governance decisions across these stages, we are recommending the Governance Matrix tool created by the IEEE P2145 Blockchain Governance group (see below). The Governance Matrix shows the governance considerations (down) that need to be addressed across different stages of an ecosystem's lifecycle (across).

The governance considerations include the key questions about who is being governed (governed parties), who governs (governing authorities), process of governance (how decisions get made), and incentives and accountability. Each of these can be different at each stage.

The GHPC has used the Governance Matrix in development of our initial governance recommendations during the initial stage. The Matrix can be used in similar fashion for subsequent stages.

Governance Dimensions

Defition: Governance is about decision making for direction and control of a dynamic system

Governance Considerations

Governance Structure

Who is involved in Governance?

Members

Who are the members? Governed members/ Governing Authority?

Decision makers (Governance Authority)

Who are decision makers? What is the structure of decision making team (if it is a team)? Centralized, Federated, Decentralized?

Organization

How are the members organized? Are there any formal / informal communities (e.g., Working groups, committees)?

Governance Process

How do members work together to make Governance decisions (policies)?

Membership

What is the process for membership management, communities / decision making bodies membersh ps?

Communication / Coordination

How communities communicate / coordinate? What tools/processes they use?

Decision making

What is the process of decision making (including decisions for memberships, scope, objectives, deliverables, and any other unanticipated decisions)?

Governance Decisions

What are the outcomes (deliverables) of Governing process? What decisions (rules, policies or other) are made? Where are they published? (this will depend on what the Governance is for)

Incentives / Accountability

What are available incentives for different roles?

Financial

Are there financial incentives? (for example cost reduction with compliance or increased costs with non-compliance)

Social

Are there social incentives such as social recognition or other?

Governance Framework (GF)

Governance for the Governance Framework Development lifecycle.

Envision EGF	Execute EGF			Enhance EGF
	short-term - setup (build community of early adopters)	**medium-term - create (early adopters create governing authority)**	**long-term - operate (governrning authority operational)**	
Business need / Purpose - Create a globally interoperable ToIP Layer 4 digital trust ecosystem that operates according to the Good Health Pass Principles. Refer to Good Health Pass Ecosystem Governance Framework Recommendation for scope, objectives, principles and requirements.	**Implement** - Invite Governing Authorities to imp ement the EGF (the participating authorities/early adopters will create the SEGF based on General EGF); Provide support for and review of the early implementations; Change mangement for EGF	**GHP Foundation formation** - Early adopters collaborate to form the GHP Foundation, define the organizational governance for the GHP.	**GHP Foundation operational** - GHP Foundation becomes officia. Governing Authority for the GHP EGF, and assumes the role of supporting and auditing GHP compliant solutions, maintaining EGF, risks and issues.	**GHP Foundation change management** - identify issues, accept and process change proposals, considering the impact of change, communication and adoption of change etc.

Figure 23: Governance Matrix

Glossary

Purpose and Scope

The purpose of this glossary is to support the recommendations of the Interoperability Working Group for Good Health Pass hosted by the ToIP Foundation and the Good Health Pass Collaborative hosted by ID2020. It includes the most relevant terms from related glossaries including:

- W3C Verifiable Credentials Data Model 1.0
- W3C Decentralized Identifiers (DIDs) 1.0
- W3C CCG JSON-LD 1.1
- W3C CCG Linked Data Proofs 1.0
- eSSIF-Lab Glossary
- EU General Data Protection Regulation (GDPR)
- HIMSS Healthcare Interoperability

The scope of this glossary is terms that are required to enable interoperable implementations of the software and systems required by issuers, holders, and verifiers of GHP-compliant health passes together with the governing authorities and governance frameworks under which these parties will be interoperating. Within this scope, unless explicitly declared otherwise, terms defined in this glossary are only used in the meaning provided herein. Outside of this scope, these terms may have other meanings.

Formatting

1. Terms that are used, and whose meaning is defined in this glossary, and whose meaning is included in this glossary, appear in **bold**. When a term that is defined in this glossary appears as regular text (not bolded), it is to be interpreted as usual (e.g. according to well-known dictionaries).
2. In some cases, where a term is imported from another scope, its definition will use supporting terms that are hyperlinked to their definitions in that scope. Those hyperlinks have only been replaced with terms in **bold** only if the supporting term is included in this glossary.
3. The definition of terms imported from other scopes are prefixed with the name of that scope (and a link where applicable). All definitions without a prefix are considered to be defined in this **GHP Glossary**.
4. If a term is cited from Wikipedia, the link is the Wikipedia permalink.
5. If a term is used in more than one scope that applies to the **Good Health Pass digital trust ecosystem**, multiple definitions are shown. The authoritative definition in the context of this glossary is the one prefixed with **GHP Glossary**.

Terms

1-way paper credential

A **paper credential** that is either issued directly to the **holder** or generated from a **digital credential** in such a way that it is not possible to transform it back into the original digital credential without contacting the **issuer** for re-issuance.

1-way paper pass

A **paper pass** that is either issued directly to the **holder** or generated from a **digital pass** in such a way that it is not possible to transform it back into the original digital pass without contacting the **issuer** for re-issuance.

2-way paper credential

A **paper credential** generated from a **digital credential** in such a way that it can be losslessly transformed back into the original digital credential by following a published algorithm.

2-way paper pass

A **paper pass** generated from a **digital pass** in such a way that it can be losslessly transformed back into the original digital pass by following a published algorithm.

AAL

Abbreviation for **authenticator assurance level**.

actor

(ESSIF Lab Glossary) An **entity** that can act (do things), e.g. people, machines, but not **organizations**. See the eSSIF-Labs Parties, Actors, and Actions pattern for more information.

administering authority

(ToIP Glossary) The **party** responsible for administering a particular **governance framework**. The administering authority may or may not be the **governing authority**. For example, an NGO may be the administering authority for a governance framework governed by a government as the governing authority.

anti-correlation

(ToIP Glossary) A technique for privacy preservation that eliminates any unnecessary correlators from a message and its data payload, such as a **credential**. Anti-correlation applies specifically to digital

cryptography, where public keys and digital signatures can serve as globally unique identifiers for the **subject** and/or **holder**. One solution for this type of anti-correlation is to use **zero-knowledge proof** cryptography.

attestation

A set of data asserted about a **subject** for which the attester can be held accountable. This includes a **self-attestation** from the subject itself.

auditor

(ToIP Governance Glossary) A **person** or **legal entity** that assesses the conformance of a **governed party** to the **requirements** of a **governance framework**. The auditor may itself be required to follow the requirements of a **trust assurance framework**.

auditor accreditor

A **certifying party** for **auditors**.

authentication

(W3C Decentralized Identifiers 1.0) Authentication is a process by which an entity can prove it has a specific attribute or controls a specific secret using one or more verification methods. For example, with **DIDs**, a common authentication method is to prove control of the cryptographic private key associated with a public key published in a **DID document**.

authenticator assurance level (AAL)

The term is used in the NIST 800-63B standard for what the ISO/IEC 29115:2013 standard calls **authentication LoA**.

authentication LoA

The **level of assurance** achieved in an **authentication** event in any **identity authentication zone**. For example, in **zone 2** an **issuer** can assign an authentication LoA based on the strength of authenticating the **holder** against the available **identity binding** data at the time of issuing a **credential** or **pass**. In **zone 3** a verifier can assign an authentication LoA based on the strength of authenticating the **holder** against the same **identity binding** data. Note that the verifier's authentication LoA cannot exceed the issuer's authentication LoA. Note: This term is from the ISO/IEC 29115:2013 standard; the NIST 800-63B standard uses the term **authentication assurance level** (**AAL**).

authoritative issuer

(ToIP Glossary) An **issuer** that is either inherently trusted by some set of **verifiers** (for example, a trusted government agency) or that has been explicitly authorized by a **governing authority** in a **governance**

framework to issue one or more **verifiable credential types**. Authoritative issuers are often listed in a **trust registry** controlled by the governing authority.

authority

(ESSIF Lab Glossary) a **party** of which certain decisions, ideas, rules etc. are followed by other **parties**. A centralized authority uses its powers to further its own **objectives** by imposing its decisions, ideas, rules etc. on other **parties**. A decentralized authority uses its power to further the **objectives** of the **parties** that have given it these powers of their free will as they find it beneficial for themselves to do so. An authority can be anywhere in this spectrum.

barcode

(Wikipedia) A method of representing data in a visual, machine-readable form.

base32URL

Base32URL is used to represent a Base32 encoding (https://tools.ietf.org/html/rfc4648) without the padding ('='), which is not a character of the Alphanumeric QR alphabet. The use of the suffix "URL" matches the technique used for the Base64URL variation.

business rule

(ToIP Glossary) A **rule** that is under business **jurisdiction**, and is used to express business logic. For details, see the Semantics of Business Vocabulary and Business Rules (SBVR) standard from the Object Management Group.

CA

Abbreviation for **certificate authority**.

card

(GHP Glossary) The physical object on which a **QR credential** is printed. A card can enhance the cryptographic security or reduce the needs for stronger cryptographic securities by including physical security features to avoid counterfeiting and cloning. Although the term “card” is used in a Good Health Pass context, a QR credential can also be printed on a booklet, a label, a sticker, or any other physical medium.

(Smart Health Cards) A synonym for a **digital credential** that uses the metaphor of a physical card such as a credit card, business card, or health insurance card. See **Smart Health Card**. A card is *not* a synonym for a **pass**.

certificate

A set of data asserted about a **subject** by an **issuer** that can be verified in some manner, either manually

or automatically. A **credential** is a type of certificate, and a **pass** is a type of credential. See also **health certificate**.

In the context of Public Key Infrastructure (PKI), a **public key certificate** or **X509 certificate** is a digitally signed structured document binding the subject's public key to one or more identifiers for the subject. The signer is usually a **certificate authority**, however a certificate may also be self-signed.

certificate authority (CA)

(ToIP Glossary) The **legal entity** responsible for issuing a **public key certificate**.

certificate chain

See **X.509 certificate chain**.

certification

(Wikipedia) The formal attestation or confirmation of certain characteristics of an object, **person**, or **organization**. This confirmation is often, but not always, provided by some form of external review, education, assessment, or audit. Accreditation is a specific organization's process of certification.

(GHP Glossary) The process that a **certifying party** performs to assess conformance of a **governed party** to the requirements of a **governance framework**. The certification process follows the policies and procedures defined in a **trust assurance framework.**

certifying party

A **governed party** that performs **certification**.

claim

(W3C Verifiable Credentials Data Model 1.0) An assertion made about a **subject**.

(ToIP Glossary) An assertion about a **subject** made within the context of a **verifiable credential**. Also known as an *attribute* or *property* of the subject.

consent

(ToIP Governance) Permission granted by a **subject** for some set of the subject's personal data to be processed by another **party**. Under Article 7 of the EU General Data Protection Regulation (GDPR), consent must be freely given, specific, informed, and unambiguous.

consent receipt

(ToIP Governance) A verifiable record of the granting of **consent** by a **subject**. See the Kantara Consent Receipt Specification.

controlled document

(ToIP Glossary) A component document of a **governance framework** that follows the modular architecture of the **ToIP governance metamodel**. All controlled documents must be listed in the **primary document**.

credential

(W3C Verifiable Credentials Data Model 1.0) A set of one or more **claims** made by an **issuer**. See also **verifiable credential**.

(GHP Glossary) A **certificate** issued in a form designed to be easily transported by the **holder** and easily verified by a **verifier**, especially using machine-readable data and/or cryptographic signatures. In most cases a credential also uses one or more **identity bindings** that enable a verifier to **authenticate** the **subject** and/or **holder**. A credential may be either a **paper credential** or a **digital credential**. Either form may be a **verifiable credential** according to various standards, including the **W3C Verifiable Credentials Data Model 1.0**. See also **health credential**, **identity credential**, and **card**. A **pass** is a specific type of credential.

custodial wallet

(ToIP Glossary) A **digital wallet** in which the private keys are held by a **trusted third party** and not directly by the **holder**. The third party is called the **custodian**. In most cases a custodial wallet is hosted in the cloud as a service provided by the third party and accessed by the holder using a secure web browser. Mutually exclusive with **non-custodial wallet**.

custodian

A trusted third party operating a **custodial wallet**.

data controller

(EU General Data Protection Regulation) A natural or legal **person**, public authority, agency, or other body which, alone or jointly with others, determines the purposes and means of the processing of **personal data**.

data processor

(EU General Data Protection Regulation) A natural or legal **person**, public authority, agency, or other body which processes **personal data** on behalf of a **data controller**.

data minimization

(W3C Decentralized Identifiers 1.0) The act of limiting the amount of shared data strictly to the minimum necessary to successfully accomplish a task or goal.

decentralized identifier (DID)

(W3C Decentralized Identifiers 1.0) A globally unique persistent identifier that does not require a centralized registration authority and is often generated and/or registered cryptographically. The generic format of a DID is defined in § 3.1 DID Syntax. A specific DID scheme is defined in a DID method specification. Many—but not all—DID methods make use of **distributed ledger technology** (DLT) or some other form of decentralized network.

decentralized PKI

Public key infrastructure based on **decentralized identifiers** (**DIDs**).

decision support system (DSS)

(Wikipedia) An information system that supports business or organizational decision-making activities. DSSs serve the management, operations and planning levels of an organization (usually mid and higher management) and help people make decisions about problems that may be rapidly changing and not easily specified in advance—i.e. unstructured and semi-structured decision problems. Decision support systems can be either fully computerized or human-powered, or a combination of both.

(GHP Glossary) See also **rules engine**.

DID

Abbreviation for **decentralized identifier**.

DID chain

(ToIP Glossary) A set of **DIDs** linked in a hierarchical model where each DID (except the root) digitally signs the next DID in the chain. DID chains can be verified for cryptographic trust by "walking the chain" back to the **root of trust**. See also **trust registry**. Contrast with **X.509 certificate chain**.

DID controller

(W3C Decentralized Identifiers 1.0) An entity that has the capability to make changes to a **DID document**. A **DID** might have more than one DID controller. The DID controller(s) can be denoted by the optional controller property at the top level of the DID document. Note that a DID controller might be the **DID subject**.

DID document

(W3C Decentralized Identifiers 1.0) A set of data describing the **DID subject**, including mechanisms, such as cryptographic public keys, that the DID subject or a DID delegate can use to **authenticate** itself and prove its association with the **DID**. A DID document might have one or more different representations as defined in § 6. Representations or in the W3C DID Specification Registries [DID-SPEC-REGISTRIES].

DID method

(W3C Decentralized Identifiers 1.0) A definition of how a specific DID method scheme is implemented. A DID method is defined by a DID method specification, which specifies the precise operations by which **DIDs** and **DID documents** are created, resolved, updated, and deactivated. See § 8. Methods.

DID scheme

(W3C Decentralized Identifiers 1.0) The formal syntax of a **decentralized identifier**. The generic DID scheme begins with the prefix `did:` as defined in § 3.1 DID Syntax. Each **DID method** specification defines a specific DID method scheme that works with that specific DID method. In a specific DID method scheme, the DID method name follows the first colon and terminates with the second colon, e.g., `did:example:`

DID subject

(W3C Decentralized Identifiers 1.0) The **entity** identified by a **DID** and described by a **DID document**. Anything can be a DID subject: person, group, organization, physical thing, digital thing, logical thing, etc.

DID URL

(W3C Decentralized Identifiers 1.0) A **DID** plus any additional syntactic component that conforms to the definition in § 3.2 DID URL Syntax. This includes an optional DID path (with its leading / character), optional DID query (with its leading ? character), and optional DID fragment (with its leading # character).

dispute resolution

(Wikipedia) The process of resolving disputes between **parties**.

distributed ledger (DLT)

(W3C Decentralized Identifiers 1.0) A non-centralized system for recording events. These systems establish sufficient confidence for participants to rely upon the data recorded by others to make operational decisions. They typically use distributed databases where different nodes use a consensus protocol to confirm the ordering of cryptographically signed transactions. The linking of digitally signed transactions over time often makes the history of the ledger effectively immutable.

digital credential

A **credential** in digital form that may be stored in a **digital wallet.** A digital credential may be either an **online credential** or an **offline credential**. It may be stored in a high-end or low-end device, may be transmitted from an **issuer** to a **holder** and presented from a **holder** to a **verifier** via various protocols, including barcodes on a screen, Bluetooth API, HTTPS call, and so on. Mutually exclusive with **paper credential**.

digital pass

A **pass** in digital form that is stored in a **digital wallet app.** A digital pass may be stored statically or generated in response to a **presentation request.** A digital pass may also be issued directly by an **issuer**—or a **rules engine** acting as an issuer. See also **verifiable digital pass**.

digital trust ecosystem

(ToIP Glossary) An ecosystem of **governed parties** that interoperate to achieve a set of **trust objectives** online. Layer 4 of the **ToIP stack** is designed to support digital trust ecosystems.

digital wallet

(ToIP Glossary) Software used by a **holder** to store the cryptographic private keys necessary to exert control over **DIDs**, **digital credentials** of any type, and digital value stores such as cryptocurrencies. Digital wallets are also commonly used to store **digital credentials** and **passes** issued to the holder. See also **custodial wallets** and **non-custodial wallets**.

digital wallet app

A mobile app used by a **holder** to perform the functions of a **digital wallet.**

DLT

Abbreviation for **distributed ledger** technology.

DSS

Abbreviation for **decision support system**.

ecosystem governance framework (EGF)

(ToIP Governance) A **governance framework** for governing an entire ToIP Layer 4 **digital trust ecosystem.** An EGF may be either a **general EGF** or a **specific EGF**.

ecosystem of ecosystems

(ToIP Governance) A **digital trust ecosystem** (usually of significant scale or complexity) that is governed by a **general ecosystem governance framework** (**general EGF**) for which there are multiple conforming **specific ecosystem governance frameworks** (**specific EGFs**). An example is the **Good Health Pass digital trust ecosystem**.

EGF

Abbreviation for **ecosystem governance framework**.

entity

(W3C Verifiable Credentials Data Model 1.0) A thing with distinct and independent existence, such as a person, organization, or device that performs one or more roles in the ecosystem.

(ESSIF Lab Glossary) Someone or something that is known to exist.

EU Digital COVID Certificate

(European Union) A particular type of **health credential** issued by an EU member state to facilitate travel of EU citizens within the EU according to regulations specified by the European Union. Even though an EU Digital COVID Certificate is designed to enable travel across borders within the EU, it is *not* a **pass** as defined by the Good Health Pass glossary because it does not apply the data minimization or anti-correlation required to be **Good Health Pass-compliant**.

event record

(ToIP Glossary) A **record** of the data inputs associated with a particular event.

form

(ToIP Glossary) A domain-agnostic data structure used to collect data. A form may be either a paper form or a digital form. A form can contain attributes from one or more **schema**.

foundational interoperability

(HIMSS) The first of the four levels of **interoperability** defined by HIMSS. This level establishes the inter-connectivity requirements needed for one system or application to securely communicate data to and receive data from another. See also **structural interoperability** (level 2), **semantic interoperability** (level 3), and **organizational interoperability** (level 4).

general ecosystem governance framework (general EGF)

(ToIP Glossary) An **ecosystem governance framework** (EGF) that is intended to only be directly binding on a **governing authority** defining a **specific ecosystem governance framework**. An example of a general EGF is the **Good Health Pass Ecosystem Governance Framework**.

general EGF

Abbreviation for **general ecosystem governance framework**.

GHP

Abbreviation for **Good Health Pass**.

GHPC

Abbreviation for **Good Health Pass Collaborative**.

GHP-compliant

Abbreviation for **Good Health Pass-compliant**.

GHP EGF

Abbreviation for **Good Health Pass Ecosystem Governance Framework**.

GHP Foundation

Abbreviation for **Good Health Pass Foundation**.

GHP Glossary

This document.

Good Health Pass (GHP)

A generic class of **health passes** that conform to the requirements of the **Good Health Pass Ecosystem Governance Framework**.

Good Health Pass Collaborative (GHPC)

A project of ID2020 to specify and advocate for the **Good Health Pass**.

Good Health Pass community

The **trust community** of stakeholders in the **Good Health Pass Ecosystem Governance Framework**.

Good Health Pass-compliant (GHP-compliant)

The condition under which a **governed party** has been determined to conform to the **trust assurance** requirements of the **Good Health Pass Ecosystem Governance Framework** (GHPEGF) or a **specific EGF** based on the GHPEGF.

Good Health Pass digital trust ecosystem

The **digital trust ecosystem** governed by the **Good Health Pass Ecosystem Governance Framework** (GHP EGF) and all **specific EGFs** based on the GHP EGF.

Good Health Pass Ecosystem Governance Framework (GHP EGF)

The **general ecosystem governance framework** that governs the **Good Health Pass digital trust ecosystem**. This glossary is a **controlled document** of the GHP EGF.

Good Health Pass Foundation

A proposed name for the official **governing authority** for the **Good Health Pass Ecosystem Governance Framework**.

Good Health Pass implementation

An implementation of any component of the **Good Health Pass digital trust ecosystem** for which requirements are specified in the **GHP EGF**. This includes hardware, software, and network services used by **issuers**, **holders**, and **verifiers** of **GHP-compliant health credentials** and **health passes**. It also includes **digital wallet apps**, **rules engines**, and **decision support systems**.

Good Health Pass Interoperability Blueprint

The final recommendations from the ToIP Interoperability Working Group for Good Health Pass as compiled and approved by the **Good Health Pass Collaborative**.

governing authority

(ToIP Glossary) The **legal party** responsible for governing a particular **governance framework**. The governing authority may or may not be the **administering authority**. For example, a government may be the governing authority for a governance framework administered by an NGO as the administering authority.

governance framework

(ToIP Glossary) A set of business, legal, and technical definitions, policies, specifications, and contracts by which the members of a **trust community** agree to be governed in order to achieve their desired **trust objectives**. In governance frameworks that follow the ToIP governance metamodel, a **governance framework** is divided into a **primary document** and a set of **controlled documents**. A governance framework is itself governed by a **governing authority** and in some cases may be administered by a separate **administering authority**. A **trust framework** is a specialized form of a governance framework. See also **ecosystem governance framework**.

governed party

(ToIP Glossary) A **party** that plays a role in a **governance framework**.

health attestation

An **attestation** about a **subject's** health, such as the subject having had a COVID-19 test or vaccination.

health authority

An issuer who is authoritative for at least a portion of a **subject's health records** and therefore is trusted by at least one **governing authority** to issue **health credentials** and/or **health passes**.

health certificate

A **certificate** containing **claims** from one or more one or more **health records**. Also known as a *medical certificate.* This term is often used to refer to an official document issued by a government agency, public health authority, or other accredited issuer. Examples include the EU Digital COVID Certificate and the WHO Smart Vaccination Certificate.

health credential

A **credential** containing **claims** from one or more one or more **health records**. In the context of the Good Health Pass, a health credential attests that a COVID-19 test event, vaccination event, or recovery verification event occurred. The **claims** are the data inputs associated with the health record, such as the test results or the type and dosage of vaccination given. See also **identity credential**.

health record

A **record** of a health event for a **person**. In the Good Health Pass context, health events include COVID-19 test events, vaccination events, and recovery verification events.

health pass

A **pass** that contains the minimal set of data from or about one or more **health records** that is required for a specific **verifier** (or a class of verifiers, such as airlines) to make a particular **trust decision**.

holder

(W3C Verifiable Credentials Data Model 1.0) A role an **entity** might perform by possessing one or more **verifiable credentials** and generating **presentations** from them. A holder is usually, but not always, a **subject** of the verifiable credentials they are holding. Holders store their **credentials** in credential repositories.

IAL

Abbreviation for **identity assurance level**.

identity authentication

The process of providing assurance about the identity of an **entity** interacting with a system.

identity assurance level (IAL)

The term used in the NIST 800-63B standard for what the ISO/IEC 29115:2013 standard calls **identity proofing LoA**.

identity credential

A **credential** whose **claims** describe attributes of an **entity's identity**. Identity credentials can be used to perform **identity binding** with other credentials such as **health credentials**.

identity

(W3C Verifiable Credentials Data Model 1.0) The means for keeping track of **entities** across contexts. Digital identities enable tracking and customization of entity interactions across digital contexts, typically using identifiers and attributes. Unintended distribution or use of identity information can compromise privacy. Collection and use of such information should follow the principle of **data minimization**.

identity authentication zone

A phase in the lifecycle of a **credential** or **pass** describing a health event (such as a COVID-19 test or vaccination) during which the **subject's** identity may need to be **authenticated** to some **level of assurance**. **Zone 1** is at the time of vaccination or testing, **zone 2** is at the time of **issuance** of the credential or pass, and **zone 3** is at the time of **presentation**.

identity binding

The method by which a **subject** is linked ("bound") to a **credential** or **pass** issued to that subject. There are different methods an **issuer** can use to perform identity binding and that a **verifier** can use to **authenticate** the subject against that identity binding. In the Good Health Pass digital trust ecosystem, the processes involved in creating and authenticating an identity binding takes place across three zones: **zone 1**, **zone 2**, and **zone 3**.

identity proofing

The process of verifying the claimed identity of a **subject** by **authenticating** the identity source documents and other information provided by or obtained in relation to the subject.

identity proofing LoA

The **level of assurance** an **issuer** has in the strength of the **identity proofing** used for **identity binding** in the issuance of a **credential** or **pass**. This term comes from the ISO/IEC 29115:2013 standard; the NIST 800-63A standard uses the term **identity assurance level** (**IAL**).

individual

See **natural person**.

interoperability

(Wikipedia) A characteristic of a product or system, whose interfaces are completely understood, to work with other products or systems, at present or in the future, in either implementation or access, without any restrictions.[1]

(HIMSS) The ability of different information systems, devices and applications (systems) to access, exchange, integrate and cooperatively use data in a coordinated manner, within and across organizational, regional and national boundaries, to provide timely and seamless portability of information and optimize the health of individuals and populations globally. The four levels of interoperability defined by HIMSS include **foundational interoperability** (level 1), **structural interoperability** (level 2), **semantic interoperability** (level 3), and **organizational interoperability** (level 4).

issuance

The act of an **issuer** issuing a **credential** or **pass** to a **holder**.

issuer

(W3C Verifiable Credentials Data Model 1.0) A **role** an **entity** can perform by asserting **claims** about one or more **subjects**, creating a **verifiable credential** from these claims, and transmitting the verifiable credential to a **holder**.

jurisdiction

(ESSIF Lab Glossary) The composition of a legal system (legislation, enforcement thereof, and conflict resolution), a **party** that governs that **legal system**, a scope within which that legal system is operational, and one or more objectives for the purpose of which the legal system is operated. For full context, see the full ESSIF Lab Jurisdictions pattern.

legal entity

(GHP Glossary) Any type of **entity** that has legal rights and responsibilities except a **natural person**. Examples of legal entities include corporations, partnerships, sole proprietorships, associations, governments, and non-governmental organizations (NGOs). See also **party**.

(ESSIF Lab Glossary) An **entity** that is known by, recognized to exist, and registered in a specific **jurisdiction**.

Legal Entity Identifier (LEI)

(Wikipedia) A unique global identifier for **legal entities** in the form of a 20-character, alpha-numeric code based on the ISO 17442 standard.

legal person

An entity that is not a human being but is still endowed with legal rights associated with personhood in a jurisdiction (such as enterprises). See also **person**, **legal entity**, and **party**.

legal system

(ESSIF Lab Glossary) A system in which rules are defined, and mechanisms for their enforcement and conflict resolution are (implicitly or explicitly) specified.

level of assurance (LOA)

(ToIP Glossary) A measure—often on a numeric scale—of the confidence one **entity** has in an assertion about another entity based on a defined set of criteria for evaluating that confidence. LoAs are often defined in or referenced by **governance frameworks** and **trust assurance frameworks**. The **Good Health Pass Interoperability Blueprint** follows the ISO/IEC 29115:2013 standard which defines four LoA. Each LoA describes the degree of confidence in the processes leading up to and including the authentication process itself, thus providing assurance that the entity claiming a particular identity (i.e., the entity) is in fact the entity to which that identity was assigned. See also **authentication LoA** and **identity proofing LoA**.

linked data

(W3C CCG JSON-LD 1.1) A set of documents, each containing a representation of a **linked data graph**.

linked data graph

(W3C CCG JSON-LD 1.1) A labeled directed graph, i.e., a set of nodes connected by edges, as specified in the Data Model section of the JSON-LD specification [JSON-LD11CG]. A linked data graph is a generalized representation of an RDF graph as defined in [RDF-CONCEPTS].

linked data proof

(W3C CCG Linked Data Proofs 1.0) A set of attributes that represent a **linked data** digital **proof** and the parameters required to verify it.

linked data signature

(W3C CCG Linked Data Proofs 1.0) A type of **linked data proof** that involves cryptographic signatures.

LoA

Abbreviation for **level of assurance**.

mandate

The set of **requirements** defined in IETF RFC 2119 that use the keywords **MUST, MUST NOT, SHALL, SHALL NOT** or **REQUIRED**.

minimization function

A sequence of steps used to compact a **verifiable pass** or **credential** and then encode it into a URI-compliant and QR-friendly format. Each minimization function uses a combination of methods in a pre-defined order, for example: manual and automated templating (e.g. PathCheck, JSON TX), canonicalization, serialization, normalization and binarization (e.g. CBOR, RDF), data compression (e.g. ZLIB, GZIP, 7-Zip), character encoding (e.g. Base32, percent encoding), final formatting (e.g. URI documents, MIME types, File headers, etc).

natural person

(GHP Glossary) A person that is known, for example through some form of legal registration, in a **jurisdiction**. See also **legal person** and **legal entity**. See the eSSIF-Labs Parties, Actors, and Actions pattern and the eSSIF-Lab Jurisdictions pattern for more information.

non-custodial wallet

(ToIP Glossary) A **digital wallet** in which the private keys are held directly by the **holder** and not by any **trusted third party** acting as a **custodian**. In most cases a non-custodial wallet operates as a **digital wallet app** on a mobile phone or other local device. Mutually exclusive with **custodial wallet**.

non-GHP

A qualifier used before any term in the **GHP Glossary** (e.g., credential, pass, issuer, verifier, rules engine, trust registry, etc.) to mean that the referent of the term is not **GHP-compliant**.

non-W3C verifiable credential

A **verifiable credential** that does not conform to the W3C Verifiable Credentials Data Model 1.0 standard. Mutually exclusive with **W3C verifiable credentials**.

objective

(ESSIF Lab Glossary) Something toward which a **party** directs effort (an aim, goal, or end of action).

(ISO 27000) result to be achieved.

offline credential

A **credential** designed to work entirely offline, i.e., without an Internet connection. An offline credential may be either a **paper credential** or a **digital credential** but it is always stored in a **non-custodial**

wallet. In both cases the credential can be presented and verified with full functionality using local resources, i.e., without access to the internet. An offline credential can be transmitted via a **QR code**, Bluetooth APIs, or other near-range technologies. Mutually exclusive with **online credential**.

online credential

A **digital credential** designed to work online, i.e., that requires Internet access to achieve full functionality. An example of an online credential is one that is stored in a **custodial wallet**. Mutually exclusive with **offline credential**.

option

The set of **requirements** defined in IETF RFC 2119 that use the keywords **MAY** or **OPTIONAL**.

organization

(ESSIF Lab Glossary) A **party** that is associated with a group of **actors** that work to realize its **objectives**. See the eSSIF-Labs Parties, Actors, and Actions pattern for more information. See also **legal entity**.

(ISO 27000) person or group of people that has its own functions with responsibilities, authorities and relationships to achieve its **objectives**.

organizational interoperability

(HIMSS) The fourth of the four levels of **interoperability** defined by HIMSS. This level Includes governance, policy, social, legal and organizational considerations to facilitate the secure, seamless and timely communication and use of data both within and between **organizations**, **entities** and **individuals**. These components enable shared consent, trust and integrated end-user processes and workflows. See also **foundational interoperability** (level 1), **structural interoperability** (level 2), and **semantic interoperability** (level 3).

paper credential

An **offline credential** printed on a physical medium (such as paper) so that when it is read by a scanner, it can be converted back into a **digital credential** of some type. Mutually exclusive with **digital credential**. A paper credential may or may not be a **verifiable credential**. Even though it has "paper" on the name, any other non-electronic material can be used. A paper credential must use a **QR code** or similar data transfer protocol due to the lack of electronics.

paper pass

A **pass** rendered in a paper format that contains at least some data in a machine-readable format such as a **QR code** or **barcode**. Mutually exclusive with **digital pass**. A paper pass may or may not be a **verifiable pass**.

party

(ESSIF Lab Glossary) An **entity** that sets its **objectives**, maintains its **knowledge**, and uses that knowledge to pursue its objectives in an autonomous (sovereign) manner. Humans and **organizations** are the typical examples. See the eSSIF-Labs Parties, Actors, and Actions pattern for more information.

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 **subject's** name, place and date of birth, photograph, signature, and other relevant identifying information. Contrast with **pass**.

pass

A **credential** to which **data minimization** and **anti-correlation** protections have been applied and any relevant **travel data** has been added so it discloses only the data a **verifier** needs to make a **trust decision** in a specific context (such as boarding an airplane). Contrast with **credential**, which includes all relevant data from a **record** and is not required to apply data minimization or anti-correlation. A pass may be: a) issued directly from the **issuer's** authoritative data records, b) issued by a **proxy issuer** on the basis of other **attestations**, **certificates**, or credentials presented by the holder, or c) derived directly from a **verifiable credential** that supports **selective disclosure** to produce a particular **verifiable presentation** with only the data required by a verifier. A pass may be either a **digital pass** or a **paper pass**. See also **verifiable pass**.

person

A human being. See also **natural person**, **legal person**, **legal entity**, and **party**.

personal data

(EU General Data Protection Regulation) any information relating to an identified or identifiable **natural person**.

PKI

Abbreviation for Public Key Infrastructure.

presentation

(W3C Verifiable Credentials Data Model 1.0) Data derived from one or more **verifiable credentials**, issued by one or more **issuers**, that is shared with a specific **verifier**.

presentation definition

(DIF Presentation Exchange v1.0.0) An object that articulates what **proofs** a **verifier** requires. These help

the verifier to decide how or whether to interact with a **holder**. Presentation definitions are composed of inputs, which describe the forms and details of the proofs they require, and optional sets of selection rules, to allow holders flexibility in cases where many different types of proofs may satisfy an input requirement.

(ToIP Glossary) A digital object defining what **proof(s)** a **verifier** requires from a **holder** in order for the verifier to make a **trust decision**. See the DIF Presentation Exchange specification.

presentation request

(ToIP Glossary) A data structure sent from a **verifier** to a **holder** to request a particular **presentation definition**. Also known as **proof request**.

presentation submission

(DIF Presentation Exchange v1.0.0) An object embedded within target **claim** negotiation formats that unify the presentation of **proofs** to a **verifier** in accordance with the requirements the verifier specified in a **presentation definition**.

(ToIP Glossary) A digital object providing the **proof(s)** a **holder** has selected to submit to a **verifier** in response to a **presentation request**. See the DIF Presentation Exchange specification.

primary document

(ToIP Glossary) The starting point document of a **governance framework** that follows the modular architecture of the **ToIP governance metamodel**. In this metamodel, the primary document is required to include a list of all other **controlled documents**.

protected health information (PHI)

(Wikipedia) Any information about health status, provision of health care, or payment for health care that is created or collected by a healthcare provider and can be linked to a specific individual.

public key certificate

(Wikipedia) An electronic document used to prove control of a public key.

proof

(ToIP Glossary) Cryptographic verification of a **claim** or a **credential**, typically provided by the **issuer**, but may also be generated by the **holder** based on the original proof(s) provided by the issuer. A digital signature is a simple form of proof. A cryptographic hash is also a form of proof. **Zero knowledge proofs** enable **selective disclosure** of the information in a credential.

proof request

See **presentation request**.

proxy issuer

An **issuer** who is not authoritative for the source data for a **certificate** or **credential**, but who serves as a **verifier** of one or more certificates or credentials as part of the process of issuing a **verifiable pass**. A proxy issuer may function as a **rules engine** and/or **decision support system**. A proxy issuer may perform other processing including applying business logic, performing data validation and normalization, and applying data minimization and anti-correlation.

QR code

(Wikipedia) A type of machine-readable two-dimensional **barcode** that can be read by an optical scanner to convey information defined in the ISO/IEC 18004:2015 specification (full name: "*Information technology — Automatic identification and data capture techniques — QR Code 2005 bar code symbology specification*).

recommendation

The set of **requirements** defined in IETF RFC 2119 that use the keywords SHOULD, SHOULD NOT, or RECOMMENDED.

record

(ToIP Glossary) A collection of domain-specific data inputs, possibly of different data types, typically in a fixed number and sequence within a database.

relying party

(ToIP Technology) A **party** who chooses to rely on a **credential** once it has been verified. The **W3C Verifiable Credentials** community uses the term **verifier** for this role. Other specifications, particularly those defining federated identity management systems, use the term "relying party".

(ToIP Governance) A **party** who relies on the assertions or attestations of a **governed party** over conformance with all or part of a **governance framework**, often as measured against a **trust assurance framework**.

repository

(W3C Verifiable Credentials Data Model 1.0) A program, such as a storage vault or personal **verifiable credential wallet**, that stores and protects access to **holders'** verifiable credentials.

requirement

Any statement in a governance framework or one of its controlled documents that uses one of the keywords defined in IETF RFC 2119. Requirements are either **mandates**, **recommendations**, or **options**.

revocation

(ToIP Glossary) The act of an **issuer** asserting that a **credential** it issued is no longer valid.

revocation registry

(ToIP Glossary) A network service available from one or more **service endpoints** specified in a **governance framework** that can be queried by a **verifier** (or other relevant party) to check whether a **credential** has been **revoked**. For verification of **offline credentials**, the entries in a revocation registry may need to be periodically downloaded by the verifier.

risk

(ESSIF Lab Glossary) the deviation of the expected realization (e.g. results) of a **party**'s **objective**.

(ISO 27000) effect of uncertainty on **objectives**. An effect is a deviation from the expected - positive or negative. Uncertainty is the state, even partial, of deficiency of information related to, understanding or knowledge of, an event, its consequence, or likelihood.

risk analysis

(ISO 27000) process to comprehend the nature of **risk** and to determine the level of risk (**risk level**).

risk assessment

(ToIP Glossary) A process of evaluating threats to the purpose, scope and **objectives** of a **governance framework** and categorizing them so that risk treatment options (mitigation, avoidance, acceptance or transference) can be considered and applied. A risk assessment can evaluate threats of any type: external attackers, insider threats, information technology limitations or failures, market risks, legal risks, and so on.

(ISO 27000) overall process of **risk identification**, **risk analysis** and **risk evaluation**

risk evaluation

(ISO 27000) process of comparing the results of **risk analysis** with **risk criteria** to determine whether the **risk** and/or its magnitude (**risklevel**) is acceptable or tolerable.

risk identification

(ISO 27000) process of finding, recognizing and describing **risks**

risk owner

(ISO 27000) person or entity with the accountability and authority to manage a **risk**.

risk level (or: level of risk)

(ISO 27000) magnitude of a **risk**, expressed in terms of the combination of consequences and their likelihood.

risk treatment

(ISO 27000) process to modify **risk**. Risk treatment can involve:

- avoiding the **risk** by deciding not to start or continue with the activity that gives rise to the **risk**;
- taking or increasing **risk** in order to pursue an opportunity;
- removing the source/cause of the **risk**;
- changing the likelihood (chance) of the **risk** materializing;
- changing the outcome of a security event, affecting **objectives**;
- sharing the **risk** with another **party** or **parties** (including contracts and risk financing);
- retaining the risk by informed choice.

risk treatment plan (RTP)

A component of a **trust assurance framework** that states how identified risks shall be treated, e.g. mitigated, avoided, accepted or transferred.

role

A set of rights, responsibilities, and **requirements** that apply to a particular **governed party** in the scope of a **governance framework**.

root certificate

(ToIP Glossary) The first **certificate** in a **certificate chain** that represents the **root of trust** for that chain.

root DID

(ToIP Glossary) The first **DID** in a **DID chain** that represents the **root of trust** for that chain.

root of trust

(ToIP Glossary) The starting point for a **certificate chain** or a **DID chain**.

(GHP Glossary) A **trust registry** designated by a **governing authority** in a **specific ecosystem governance framework** by specifying the **root certificate** or **root DID** and the trust registry service endpoint.

RTP

Abbreviation for **risk treatment plan**.

rule

(ToIP Glossary) A deterministic machine-readable conditional statement that evaluates to an outcome. See **business rule**.

rules engine

(Wikipedia) A software system that executes one or more **business rules** in a runtime production environment.

schema

(ToIP Glossary) A machine-readable definition of the semantics of a domain-specific data structure.

selective disclosure

(W3C Verifiable Credentials Data Model 1.0) The ability of a **holder** to make fine-grained decisions about what information to share.

self-attestation

An **attestation** made by a **subject** about itself. An example is a self-attestation by a **person** about a lack of COVID-19 symptoms within a specified period, or a self-attestation by a **legal entity** about conformance to a **governance framework**.

semantic interoperability

(HIMSS) The third of the four levels of **interoperability** defined by HIMSS. This level provides for common underlying models and codification of the data including the use of data elements with standardized definitions from publicly available value sets and coding vocabularies, providing shared understanding and meaning to the user. See also **foundational interoperability** (level 1), **structural interoperability** (level 2), and **organizational interoperability** (level 4).

service

(W3C Decentralized Identifiers 1.0) Means of communicating or interacting with the **DID subject** or associated entities via one or more **service endpoints**. Examples include discovery services, agent services, social networking services, file storage services, and verifiable credential repository services.

service endpoint

(W3C Decentralized Identifiers 1.0) A network address, such as an HTTP URL, at which **services** operate on behalf of a **DID subject**.

Smart Health Card

(Microsoft) A specification from Microsoft Health for producing **verifiable credentials** from Fast Healthcare Interoperability Resources (FHIR) health records. See https://smarthealth.cards/

Smart Vaccination Certificate (SVC)

(World Health Organization) A **vaccination certificate** is a medical document that records a vaccination service that an individual has received. Digital vaccination certificates, or cards, refer to digital immunization records that are accessible by the vaccinated person, and serve the same purposes as traditional home-based records: they provide a tool to ensure continuity of care and a proof of vaccination. A smart vaccination certificate (SVC) can be purely digital and stored, for example, on a smartphone application or a cloud-based server. Alternatively, it can be a "digital twin" of a traditional paper home-based record. A smartphone is not required to have an SVC. The link between the paper SVC record and the digital record can be established by a barcode , for example, that is printed on the paper vaccination card. The SVC only documents that a vaccination event has occurred.

(GHP Glossary) An SVC is one form of a **verifiable credential** that can be used as a **health credential**. An SVC is *not* designed to be used as a **verifiable pass**.

specific ecosystem governance framework (specific EGF)

(ToIP Glossary) An **ecosystem governance framework** that complies with the requirements of a **general ecosystem governance framework (general EGF)**. A specific EGF is designed to govern a specific **trust community** within the larger **digital trust ecosystem** established by the general EGF with which it complies.

specific EGF

Abbreviation for **specific ecosystem governance framework**.

structural interoperability

(HIMSS) The second of the four levels of **interoperability** defined by HIMSS. This level defines the format, syntax and organization of data exchange including at the data field level for interpretation. See

also **foundational interoperability** (level 1), **semantic interoperability** (level 3), and **organizational interoperability** (level 4).

subject

(W3C Verifiable Credentials Data Model 1.0) A thing about which claims are made.

(ToIP Glossary) The **entity** identified by a **DID** and/or described by a **verifiable credential**. See also **DID subject**.

SVC

Abbreviation for **Smart Vaccination Certificate**.

TAF

Abbreviation for **trust assurance framework**.

TIP

Abbreviation for **ToIP Interoperability Profile**.

ToIP

Abbreviation for **Trust over IP**.

ToIP Foundation

(ToIP Glossary) A non-profit project organized under the Joint Development Foundation model hosted by the Linux Foundation for defining interoperable decentralized digital trust infrastructure based on the **ToIP stack**.

ToIP governance metamodel

(ToIP Glossary) The model for structuring a **governance framework** developed by the **ToIP Foundation**. See https://wiki.trustoverip.org/display/HOME/ToIP+Governance+Metamodel. GHP-compliant governance frameworks **MUST** follow the ToIP governance metamodel.

ToIP Interoperability Profile (TIP)

A collection of **ToIP Standard Specifications**, other open standard specifications, and associated **recommendations** and best practices for how a particular set of **trust communities** agrees to interoperate technically across the four layers of the **ToIP stack**.

ToIP trust model

(ToIP Glossary) The model for achieving **transitive trust** across **trust communities** using the **ToIP stack** defined by the **ToIP Foundation**. See the ToIP white paper.

ToIP stack

(ToIP Glossary) The four-layer dual stack of technology and governance defined by the **ToIP Foundation** that enables **transitive trust** across **trust communities**. See the ToIP white paper.

ToIP Standard Specification (TSS)

A specification for decentralized digital trust infrastructure approved and published by the **ToIP Foundation**.

transitive trust

(ToIP Glossary) The ability of one **trust community member** to make a **trust decision** about another trust community member in that same trust community or a different one.

travel authority

An **issuer** who is not authoritative for a **subject's health records** but is trusted by at least one **governing authority** to access those health records with the consent of the subject for the purpose of issuing **health credentials** and/or **health passes** for enabling freedom of travel.

travel context

A specific juncture in a traveler's journey where the traveler might be required to present a relevant **credential** or **pass**. Examples include border crossings, ticket bookings, airline boardings, health facility visits, and so on.

travel data

Data describing a traveller's journey, such as itineraries, declarations, restrictions, and so on.

travel document system

An information processing system designed to automate the workflow and production of travel data into either digital or paper travel documents such as boarding passes, itineraries, passenger locator forms, and so on.

trust community

(ToIP Glossary) A set of **parties** who agree to cooperate and interoperate to achieve a set of **trust**

objectives online. In the **ToIP trust model**, such agreement is formalized in a **governance framework**. **Actors** and **parties** may participate in any number of independent trust communities and may use the ToIP trust model to achieve **transitive trust** across those communities.

trust community member

(ToIP Glossary) A **governed party** within a **trust community**.

trust decision

(ToIP Glossary) A decision by a **party** about whether or not it will engage in an interaction or transaction with another **party**, which includes a determination by the first **party** whether the **risk** it runs is acceptable (given its risk appetite).

trust assurance framework (TAF)

(ToIP Glossary) A set of specialized roles, **policies**, and processes defined by a **governing authority**—usually as a subcomponent of a **governance framework**—to specify how **governed parties** can be held accountable for compliance to a stated level of assurance.

trust framework

(ToIP Glossary) A specialized form of a **governance framework** specifying how a set of **governed parties** agree to cooperate and interact to achieve their **trust objectives** at specified **levels of assurance**.

trust mark

(ToIP Glossary) An official seal, authentication feature, certification, license, or logo that is provided by a **governing authority** (or its delegate) to a **governed party** as authorized under its **trust assurance framework** to signify that the party is in compliance with the **governance framework**.

trust objective

(ToIP Glossary) An **objective** of one or more **parties** to make successful **trust decisions**. In the **ToIP trust model**, the trust objectives shared by the members of a **trust community** are formalized in a **governance framework**. Note that individual members of a trust community may have different trust objectives than those of the community as a whole, however there is enough overlap to provide sufficient incentive for all members to join the trust community.

Trust over IP

An architecture for decentralized digital trust infrastructure developed and specified by the **ToIP Foundation**. The core of the architecture is the **ToIP stack**. See the ToIP white paper.

trust registry

(ToIP Glossary) A network service available from one or more **service endpoints** specified in a **governance framework** that can be queried to determine if a **party** is authorized to perform a specific **role** or **action**. A common example is a verifier querying a trust registry to determine if the issuer of a verifiable credential is an **authoritative issuer** for a specific **verifiable credential type**. Another example is a **holder** querying a trust registry to determine if a verifier is authorized to make a specific **presentation request**. If a trust registry serves multiple governance frameworks, the trust registry data may also include the governance framework(s) under which issuers and verifiers are authorized. A trust registry can host any data or metadata that assists the querying party in making a **trust decision**. To support **offline credentials**, the records in a trust registry may need to be periodically downloaded by the verifier.

trusted third party (TTP)

(ToIP Glossary) A third **party** who is trusted by two parties to facilitate interactions or transactions between the two parties.

TSS

Abbreviation for **ToIP Standard Specification**.

TTP

Abbreviation for **trusted third party**.

URI

Abbreviation for **Uniform Resource Identifier**.

Uniform Resource Identifier

(W3C Decentralized Identifiers 1.0) The standard identifier format for all resources on the World Wide Web as defined by IETF RFC 3986. A DID is a type of URI scheme.

VC

Abbreviation for **verifiable credential**.

vaccination certificate

A **health certificate** describing a vaccination event.

vaccine passport

A misnomer for a **health credential** or **health pass**. IT IS VERY STRONGLY RECOMMENDED TO NEVER USE THIS TERM.

validation

(W3C Verifiable Credentials Data Model 1.0) The assurance that a **verifiable credential** or a **verifiable presentation** meets the needs of a **verifier** and other dependent stakeholders. This specification is constrained to verifying verifiable credentials and verifiable presentations regardless of their usage. Validating verifiable credentials or verifiable presentations is outside the scope of this specification.

verification

(W3C Verifiable Credentials Data Model 1.0) The evaluation of whether a **verifiable credential** or **verifiable presentation** is an authentic and timely statement of the issuer or presenter, respectively. This includes checking that: the credential (or presentation) conforms to the specification; the proof method is satisfied; and, if present, the status check succeeds.

verification method

(W3C Decentralized Identifiers 1.0) A set of parameters that can be used together with a process to independently verify a **proof**. For example, a cryptographic public key can be used as a verification method with respect to a digital signature; in such usage, it verifies that the signer possessed the associated cryptographic private key.

verifiable credential (VC)

(W3C Verifiable Credentials Data Model 1.0) A tamper-evident **credential** that has authorship that can be cryptographically verified. Verifiable credentials can be used to build **verifiable presentations**, which can also be cryptographically verified. The **claims** in a credential can be about different **subjects**.

(GHP Glossary) A verifiable credential may be either a **digital credential** or a **paper credential**.

verifiable credential type

A URI used as the value of a **verifiable credential** `type` property to identify its specific type as defined in section 4.3 of the W3C Verifiable Credentials Data Model 1.0 specification.

verifiable data registry

(W3C Decentralized Identifiers 1.0) A system that facilitates the creation, verification, updating, and/or deactivation of **decentralized identifiers** and **DID documents**. A verifiable data registry might also be used for other cryptographically-verifiable data structures such as **verifiable credentials**.

verifiable presentation (VP)

(W3C Verifiable Credentials Data Model 1.0) A tamper-evident **presentation** encoded in such a way that authorship of the data can be trusted after a process of cryptographic verification. Certain types of verifiable presentations might contain data that is synthesized from, but do not contain, the original **verifiable credentials** (for example, **zero-knowledge proofs**).

(GHP Glossary) A **presentation** that conforms to the requirements of a **verifiable presentation** in the W3C Verifiable Credentials Data Model 1.0 standard.

verifiable QR code

A **QR code** that contains a **verifiable credential** or a **verifiable pass**.

verifiable pass

A **pass** that can be cryptographically verified in the same manner as a **verifiable credential**. A verifiable pass may be either a **digital pass** or a **paper pass**.

verifier

(W3C Verifiable Credentials Data Model 1.0) A role an **entity** performs by receiving one or more **verifiable credentials**, optionally inside a **verifiable presentation** for processing. Other specifications might refer to this concept as a **relying party**.

VP

Abbreviation for **verifiable presentation**.

W3C

Abbreviation for the World Wide Web Consortium.

W3C Decentralized Identifiers (DIDs) 1.0

The W3C standard for DIDs published at https://www.w3.org/TR/did-core/.

W3C verifiable credential

A **verifiable credential** that conforms to the W3C Verifiable Credentials Data Model 1.0 standard. Mutually exclusive with **non-W3C verifiable credentials**, such as ePassports, which are cryptographically verifiable but do not conform to the W3C Verifiable Credentials Data Model 1.0 standard.

W3C Verifiable Credentials Data Model 1.0

The W3C standard for **verifiable credentials** published at https://www.w3.org/TR/vc-data-model/.

WHO

Abbreviation for the World Health Organization.

WHO Smart Vaccination Certificate

See **Smart Vaccination Certificate**.

X.509 certificate

(ToIP Glossary) A **public key certificate** issued following the X.509 standard.

X.509 certificate chain

(ToIP Glossary) A set of **X.509 certificates** issued in a hierarchical model where each certificate (except the root) is signed by the parent certificate it was derived from. Certificate chains can be verified for cryptographic trust by "walking the chain" back to the **root of trust**. See also **trust registry**.

zero-knowledge proof (ZKP)

(ToIP Glossary) A **proof** that uses a particular branch of cryptography to support **selective disclosure** of information. A zero knowledge proof provides cryptographic verification about some or all of the data in a set of **credentials** without revealing the actual data or any other information about the holder. ZKP-based credentials can be used with different **presentation requests** to dynamically produce **verifiable passes**.

ZKP

Abbreviation for **zero-knowledge proof**.

zone 0

The "zone" prior to any other **identity authentication zone** during which the person planning to travel may need access to a **rules engine** or **decision support system** in order to determine what **health records** will be needed to obtain the necessary **health pass(es)** for a particular journey.

zone 1

The first **identity authentication zone** in which the health event resulting in a **health record** takes place, e.g., a COVID-19 test, vaccination, or proof of recovery test. If the patient is already enrolled in a healthcare system, the patient will typically need to be **authenticated** prior to the health event. If the patient is not enrolled, the healthcare system will typically need to collect the identity information

necessary to do **identity binding** so the patient can be authenticated in **zone 2**. However this may or may not be possible for some health events (such as vaccinations given during a pandemic).

zone 2

The second **identity authentication zone** in which a credential or pass is issued to the **holder** by an **issuer**. If **identity binding** data was collected in zone 1, the holder must be **authenticated** by the issuer to whatever **level of assurance** is supported by the available identity binding data. If identity binding was not performed in **zone 1**, or if it was not performed to an adequate level of assurance, in zone 2 it may be possible to supplement the patient identity data and increase the level of assurance beyond what was collected in zone 1. However this depends on the capabilities of the **issuer** and **attestations** of the patient or other witnesses to the health event.

zone 3

The third **identity authentication zone** in which a credential or pass is presented by the **holder** to a **verifier**. In this zone the verifier **MUST** use the **identity binding** data from **zone 2** to **authenticate** the holder to the **level of assurance** required by the verifier (but this level cannot exceed the level of assurance achieved in zone 2).

References

About the Semantics Of Business Vocabulary And Business Rules Specification Version 1.5
https://www.omg.org/spec/SBVR

Accreditation - Wikipedia
https://en.wikipedia.org/wiki/Accreditation

Adopt | Human Colossus Foundation
https://wiki.colossi.network/en/Technologies/OCA/Developer/Adopt

Airport Health Testing and Travel Information Standard - APIs
https://acris.aero/api-travel-health-information-standard/

Apache License, Version 2.0
http://www.apache.org/licenses/LICENSE-2.0.html

Audit - Wikipedia
https://en.wikipedia.org/wiki/Audit

Barcode - Wikipedia
https://en.wikipedia.org/w/index.php?title=Barcode&oldid=1016784379

BBS+ Signatures 2020
https://w3c-ccg.github.io/ldp-bbs2020/

Biometric passport - Wikipedia
https://en.wikipedia.org/wiki/Biometric_passport

Business logic - Wikipedia
https://en.wikipedia.org/wiki/Business_logic

Business rules engine - Wikipedia
https://en.wikipedia.org/w/index.php?title=Business_rules_engine&oldid=923067160

Call for public comments: Interim guidance for developing a Smart Vaccination Certificate – Release Candidate 1
https://www.who.int/news-room/articles-detail/call-for-public-comments-interim-guidance-for-developing-a-smart-vaccination-certificate-release-candidate-1

CCCC4
https://cccc4.ca/

CCI Schema Reference Documents
https://drive.google.com/drive/u/1/folders/1h4vF79KzUY6KipBt3A6kMEboiqcSYtv7

Certification - Wikipedia
https://en.wikipedia.org/w/index.php?title=Certification&oldid=1005115412

Consent Receipt Specification – Kantara Initiative
https://kantarainitiative.org/download/7902/

Core data set for the Smart Vaccination Certificate
https://www.who.int/publications/m/item/core-data-set-for-the-smart-vaccination-certificate

Coronavirus (COVID-19) - NHS
https://www.nhs.uk/conditions/coronavirus-covid-19/

Coronavirus (COVID-19) testing before you travel to England
https://www.gov.uk/guidance/coronavirus-covid-19-testing-for-people-travelling-to-england

Coronavirus (COVID-19) vaccine - NHS
https://www.nhs.uk/conditions/coronavirus-covid-19/coronavirus-vaccination/coronavirus-vaccine/

Coronavirus disease (COVID-19)
https://www.who.int/emergencies/diseases/novel-coronavirus-2019

COVID-19 Credentials initiative
https://www.covidcreds.org

COVID-19 Response and Recovery Platform
https://www.icao.int/covid/Pages/default.aspx

COVID-19: Digital COVID certificates | European Commission
https://ec.europa.eu/info/live-work-travel-eu/coronavirus-response/safe-covid-19-vaccines-europeans/covid-19-digital-green-certificates_en

COVID-19 Vaccination - Clinical Resources for Each COVID-19 Vaccine
https://www.cdc.gov/vaccines/covid-19

Creative Commons — Attribution 4.0 International — CC BY 4.0
https://creativecommons.org/licenses/by/4.0/

Credentials Community Group
https://www.w3.org/groups/cg/credentials

Cryptographic hash function - Wikipedia
https://en.wikipedia.org/wiki/Cryptographic_hash_function

Cybersecurity Best Practices
https://www.cisecurity.org/cybersecurity-best-practices/

Decentralized Identifiers (DIDs) v1.0
https://www.w3.org/TR/did-core/

Decision support system - Wikipedia
https://en.wikipedia.org/w/index.php?title=Decision_support_system&oldid=1009221582

Decision-making - Wikipedia
https://en.wikipedia.org/wiki/Decision-making

DIF Presentation Exchange
https://identity.foundation/presentation-exchange/

Digital Identity and Federation in Health Care
https://www.carinalliance.com/wp-content/uploads/2020/12/LPCA_CARIN-Alliance-Federated-Trust-Agreement_FINAL-12.3.2020.pdf

Digital signature - Wikipedia
https://en.wikipedia.org/wiki/Digital_signature

Dispute resolution - Wikipedia
https://en.wikipedia.org/w/index.php?title=Dispute_resolution&oldid=1015333922

DIVOC - Digital Infrastructure for Vaccination Open Credentialing
https://divoc.egov.org.in/

Ecosystem Foundry Working Group
https://wiki.trustoverip.org/display/HOME/Ecosystem+Foundry+Working+Group

eHealth and COVID-19 | Public Health
https://ec.europa.eu/health/ehealth/covid-19_en

eHealth Network - Guidelines on COVID-19 citizen recovery interoperable certificates - minimum dataset
https://ec.europa.eu/health/sites/health/files/ehealth/docs/citizen_recovery-interoperable-certificates_en.pdf

eHealth Network - Guidelines on Value Sets for Digital COVID Certificates
https://ec.europa.eu/health/sites/health/files/ehealth/docs/digital-green-certificates_dt-specifications_en.pdf

eHealth Network - Guidelines on verifiable vaccination certificates - basic interoperability elements
https://ec.europa.eu/health/sites/health/files/ehealth/docs/vaccination-proof_interoperability-guidelines_en.pdf

eHealth Network | Public Health
https://ec.europa.eu/health/ehealth/policy/network_en

eSSIF-Lab Glossary
https://essif-lab.pages.grnet.gr/framework/docs/essifLab-glossary

EU health preparedness: a common list of COVID-19 rapid antigen tests, including those of which their test results are mutually recognised, and a common standardised set of data to be included in COVID-19 test result certificates
https://ec.europa.eu/health/sites/health/files/preparedness_response/docs/covid-19_rat_common-list_en.pdf

EUR-Lex - 52021PC0130 - EN - EUR-Lex
https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021PC0130

FHIR v4.0.1
http://hl7.org/fhir/

FHIR Focus Group
https://wiki.trustoverip.org/display/HOME/FHIR+Focus+Group

General Data Protection Regulation (GDPR) Compliance Guidelines
https://gdpr.eu/

General Data Protection Regulation - Wikipedia
https://en.wikipedia.org/wiki/General_Data_Protection_Regulation

Global Reference Docs
https://drive.google.com/drive/u/1/folders/1y-nr-YlacLvv7P54N6EUYVrBNt7YA51T

Good Health Pass - A Safe Path to Global Reopening
https://www.goodhealthpass.org/wp-content/uploads/2021/02/Good-Health-Pass-Collaborative-Principles-Paper.pdf

Good Health Pass Collaborative
https://www.goodhealthpass.org/

Good Health Pass Working Group
https://wiki.trustoverip.org/pages/viewpage.action?pageId=73790

Governance Framework-GHP-Execution
https://docs.google.com/spreadsheets/d/18WVtpVcyyh2NDsvi48FkxtbXKf49c62d/edit

Governance Stack Working Group
https://wiki.trustoverip.org/display/HOME/Governance+Stack+Working+Group

GS1 2D Barcode Verification Process Implementation Guideline
https://www.gs1.org/docs/barcodes/2D_Barcode_Verification_Process_Implementation_Guideline.pdf

Guidance on Levels of Assurance
https://ec.europa.eu/cefdigital/wiki/download/attachments/40044784/Guidance+on+Levels+of+Assurance.docx

Health Level Seven International - Wikipedia
https://en.wikipedia.org/wiki/Health_Level_Seven_International

How to prove and verify someone's identity
https://www.gov.uk/government/publications/identity-proofing-and-verification-of-an-individual

How to register with a GP surgery - NHS
https://www.nhs.uk/nhs-services/gps/how-to-register-with-a-gp-surgery/

IATA - COVID-19: All resources
https://www.iata.org/en/programs/covid-19-resources-guidelines/

IATA - Travel Pass Initiative
https://www.iata.org/en/programs/passenger/travel-pass/

ICAO
https://icao.int/

ID2020 | Digital Identity Alliance
https://id2020.org/

Importing CSV data into a FHIR server | Hay on FHIR
https://fhirblog.com/2019/03/25/importing-csv-data-into-a-fhir-server/

Information Commissioner's Office
https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-rectification/

Information system - Wikipedia
https://en.wikipedia.org/wiki/Information_systems

Interim guidance for developing a Smart Vaccination Certificate
https://www.who.int/publications/m/item/interim-guidance-for-developing-a-smart-vaccination-certificate

Interoperability - Wikipedia
https://en.wikipedia.org/wiki/Interoperability

Interoperability in Healthcare | HIMSS
https://www.himss.org/resources/interoperability-healthcare

Introducting the Trust Over IP Foundation
https://trustoverip.org/resources/intro-to-toip/

ISO - ISO 17442:2012 - Financial services — Legal Entity Identifier (LEI)
https://www.iso.org/standard/59771.html

ISO - ISO/IEC 18004:2015 - Information technology — Automatic identification and data capture techniques — QR Code bar code symbology specification
https://www.iso.org/standard/62021.html

ISO - ISO/IEC 29115:2013 - Information technology — Security techniques — Entity authentication assurance framework
https://www.iso.org/standard/45138.html

ISO Online Browsing Platform
https://www.iso.org/obp/ui/

ISO/IEC 18013-5 mdoc for eHealth - Internationally standardized protocols for vaccination certificates
https://github.com/18013-5/micov/blob/main/ISO_IEC_18013_5_for_eHealth.pdf

Joint Development Foundation
https://www.jointdevelopment.org/

JSON Schema | The home of JSON Schema
https://json-schema.org/

JSON-LD 1.1
https://json-ld.org/spec/latest/json-ld/

Jurisdiction Specific Reference Docs
https://drive.google.com/drive/u/1/folders/1Gmapb1ktvm-v3NDH65AZEUJ-__-ouvcg

Jurisdictions
https://essif-lab.pages.grnet.gr/framework/docs/terms/pattern-jurisdiction

Legal Entity Identifier - Wikipedia
https://en.wikipedia.org/w/index.php?title=Legal_Entity_Identifier&oldid=1016164326

Linked Data Proofs 1.0
https://w3c-ccg.github.io/ld-proofs/

Linux Foundation - Decentralized innovation, built with trust
https://www.linuxfoundation.org/

Linux Foundation Public Health – Collaborating to battle COVID
https://www.lfph.io

Machine Reaadable Travel Documents - Technical Report - VDS-NC - Visible Digital Seal for non-constrained environments
https://www.icao.int/Security/FAL/TRIP/PublishingImages/Pages/Publications/Visible%20Digital%20Seal%20for%20non-constrained%20environments.pdf

Machine-readable data - Wikipedia
https://en.wikipedia.org/wiki/Machine-readable_data

NIST SP 800-63 Digital Identity Guidelines
https://pages.nist.gov/800-63-3/

NIST Special Publication 800-63A
https://pages.nist.gov/800-63-3/sp800-63a.html

NIST Special Publication 800-63A - Digital Identity Guidelines - Enrollment and Identity Proofing
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63a.pdf

NIST Special Publication 800-63B
https://pages.nist.gov/800-63-3/sp800-63b.html

NIST Special Publication 800-63B - Digital Identity Guidelines - Authentication and Lifecycle Management
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63b.pdf

NOTAM - Wikipedia
https://en.wikipedia.org/wiki/NOTAM

oca-fhir-cli
https://github.com/SemanticClarity/oca-fhir-cli

On an innovative architecture for digital immunity passports and vaccination certificates
https://arxiv.org/ftp/arxiv/papers/2103/2103.04142.pdf

OpenID Connect | OpenID
https://openid.net/connect/

Overlays Capture Architecture — The Human Colossus Foundation
https://humancolossus.foundation/blog/cjzegoi58xgpfzwxyrqlroy48dihwz

P2145 - Standard for Framework and Definitions for Blockchain Governance
https://standards.ieee.org/project/2145.html

P2145 Blockchain Governance Standards Working Group - IEEE 2145
https://sagroups.ieee.org/ieee2145/

Parties, Actors and Actions
https://essif-lab.pages.grnet.gr/framework/docs/terms/pattern-party-actor-action

Permalink - Wikipedia
https://en.wikipedia.org/wiki/Permalink

Personhood - Wikipedia
https://en.wikipedia.org/wiki/Personhood

Privacy by design - Wikipedia
https://en.wikipedia.org/wiki/Privacy_by_design

Protected health information - Wikipedia
https://en.wikipedia.org/w/index.php?title=Protected_health_information&oldid=1023641320

Public key certificate - Wikipedia
https://en.wikipedia.org/w/index.php?title=Public_key_certificate&oldid=1018062037

Public key infrastructure - Wikipedia
https://en.wikipedia.org/wiki/Public_key_infrastructure

QR code - Wikipedia
https://en.wikipedia.org/w/index.php?title=QR_code&oldid=1020475188

RDF 1.1 Concepts and Abstract Syntax
https://www.w3.org/TR/rdf11-concepts/

Requirement for Proof of Negative COVID-19 Test or Recovery from COVID-19 for All Air Passengers Arriving in the United States | CDC
https://www.cdc.gov/coronavirus/2019-ncov/travelers/testing-international-air-travelers.html

RFC 2119 - Key words for use in RFCs to Indicate Requirement Levels
https://tools.ietf.org/html/rfc2119

RFC 3986 - Uniform Resource Identifier (URI): Generic Syntax
https://tools.ietf.org/html/rfc3986

RFC 4648 - The Base16, Base32, and Base64 Data Encodings
https://tools.ietf.org/html/rfc4648

Secure by design - Wikipedia
https://en.wikipedia.org/wiki/Secure_by_design

Self-declare as a private COVID-19 testing provider
https://www.gov.uk/guidance/self-declare-as-a-private-sector-covid-19-testing-provider

Self-Issued OpenID Connect Provider DID Profile v0.1
https://identity.foundation/did-siop/

Semantic Domain - Trust Over IP
https://trustoverip.org/working-groups/decentralized-semantics/

SMART Health Cards Framework
https://smarthealth.cards/

Smart Vaccination Certificate Working Group
https://www.who.int/groups/smart-vaccination-certificate-working-group

Software system - Wikipedia
https://en.wikipedia.org/wiki/Software_system

Technical Standards & Reporting: COVID-19 Vaccination | CDC
https://www.cdc.gov/vaccines/covid-19/reporting/requirements/index.html

Testing for coronavirus (COVID-19) - NHS
https://www.nhs.uk/conditions/coronavirus-covid-19/testing/

The FAIR Guiding Principles for scientific data management and stewardship
https://www.nature.com/articles/sdata201618

The Trusted Digital Identity Framework | Digital Transformation Agency
https://www.dta.gov.au/our-projects/digital-identity/trusted-digital-identity-framework

ToIP Governance Metamodel - Home - Confluence
https://wiki.trustoverip.org/display/HOME/ToIP+Governance+Metamodel

Trust Framework | Digital ID & Authentication Council of Canada
https://diacc.ca/trust-framework/

Trust Over IP - Defining a complete architecture for Internet-scale digital trust
https://trustoverip.org/

Trusted execution environment - Wikipedia
https://en.wikipedia.org/wiki/Trusted_execution_environment

Vaccination Certificate Vocabulary v0.1
https://w3c-ccg.github.io/vaccination-vocab/

VCI
https://vci.org/

Verifiable Credentials Data Model 1.0
https://www.w3.org/TR/vc-data-model/

W3C Patent Policy
https://www.w3.org/Consortium/Patent-Policy-20040205

Wallet And Credential Interactions
https://identity.foundation/waci-presentation-exchange/

World Wide Web Consortium (W3C)
http://www.w3.org/

X.509 - Wikipedia
https://en.wikipedia.org/wiki/X.509

Zero-knowledge proof - Wikipedia
https://en.wikipedia.org/wiki/Zero-knowledge_proof

Acknowledgments

To be compiled

Appendix A: Example User Flows for Obtaining a Health Pass

Testing

1. Individual goes to lab > presents an identity document (e.g., government issued ID) > healthcare provider authenticates identity claim > healthcare provider conducts test/vaccination > receive SMS or email > receive QR code embedded in PDF or printed test/vaccination report
2. Individual goes to lab > presents identity document (e.g., national health number) > healthcare provider authenticates identity claim > results pushed to national or regional central repository > receive SMS or email (can be stored on paper or for vaccination at digital wallet/app)
3. Individual downloads app > registers appropriate information (including flight details, if not connected via API from airline booking system) > gets specific test requirements for trip (via API connection to TravelDocs or Timatic, etc.) > links to booking platform for test centre/lab to schedule test > go to test centre > healthcare uses verifier app and verifies identity document (in person, not remote) > healthcare takes sample, performs test and pushes results to individual app > ([lab should be high attestation]; can have for self certified attested [low attestation]) > result pushed to/pulled by departure control systems for at-airport clearance to fly > individual retains their results on app [and has ability to print a digitally signed "certificate"]
4. Individual goes to lab > individual fills (or has autofilled) information for a compliant border crossing including their picture and identity information > this information is hashed > the lab creates a (presumably) negative result > this information is hashed > the user checks a common cryptographic database for the mutual hash and confirms the digital credential is approved and verifiable. (The architecture here is a bit more complex than described and the user flow varies depending on the airport, but this is essentially the case) ***there is no central processor of identifiable information, all hashing is done locally.

Vaccinations

A person who is fully vaccinated decides to travel internationally and determines that a COVID-19 health pass is required. They should be able to request the issuance of a GHP after authenticating themselves to the issuer at the required authentication LoA against a pre-enrolled identity (or identity document) at the required identity proofing LoA.

Note: Below examples focus on steps involving software, which will work in parallel with a standalone or digitally-linked paper credential.

1. Digital, Semi-automated: Individual receives appointment and any prerequisite instructions (e.g., for setting up a credential app/health pass) > individual initialises a digital credential app, provides consent and personal information > individual identifies themselves at health facility > health facility follows procedure to administer vaccine and collect data (including vaccine data, individual's personal data, dosage information, hospital records) > relevant data stored in the health facilities system, and/or synchronised to a government/state central immunisation database > credential may be issued containing record of 1st vaccination (following individual's consent) if 1st dose > credential may be issued to certify individual is vaccinated following 2nd dose (or data added to credential if one already exists) following consent from individual.

2. Digital, Fully-automated: Individual follows health facility process for vaccination including identification and consent for digital credential > issuance handled by authorised entity back-end system (e.g. country/state immunisation database) > individual installs and sets up credential app/health pass (can be at a previous stage) > receives notification to accept vaccine credential > individual provides consent to data process/transfer.
3. Digital, Manual (for low-tech health facilities): Individual receives appointment and any prerequisite instructions (e.g., for setting up a credential app/health pass) > individual initialises credential app, provides consent, personal information, and identification document/data > individual identifies themselves at health facility > health facility verifies identity, follows procedure to administer vaccine and collects data into issuer version/area of credential app (including vaccine data, dosage information, signature of issuer entity or medical personal) > credential may be issued containing record of 1st vaccination (following individual's consent) if 1st dose > credential may be issued to certify individual is vaccinated following 2nd dose (or data added to credential if one already exists) following consent from individual.

Appendix B: COVID-19 Credentials Initiative (CCI) Schema Task Force Data Specification Repositories

CCI Schema Reference Documents:
https://drive.google.com/drive/u/1/folders/1h4vF79KzUY6KipBt3A6kMEboiqcSYtv7

Global Reference Documents:
https://drive.google.com/drive/u/1/folders/1y-nr-YlacLvv7P54N6EUYVrBNt7YA51T

Jurisdiction Specific Reference Documents:
https://drive.google.com/drive/u/1/folders/1Gmapb1ktvm-v3NDH65AZEUJ-__-ouvcg

Appendix C: OCA Background

OCA presents a schema as a multi-dimensional object consisting of a stable capture base and interoperable overlays. Overlays are task-oriented linked data objects that provide additional coloration to the capture base. This degree of object separation enables issuers to make custom edits to the overlays rather than to the capture base itself. In other words, multiple parties can interact with and contribute to the schema structure without having to change the capture base definition. With capture base definitions remaining stable and in their purest form, a common immutable base object is maintained throughout the capture process, which enables data standardization.

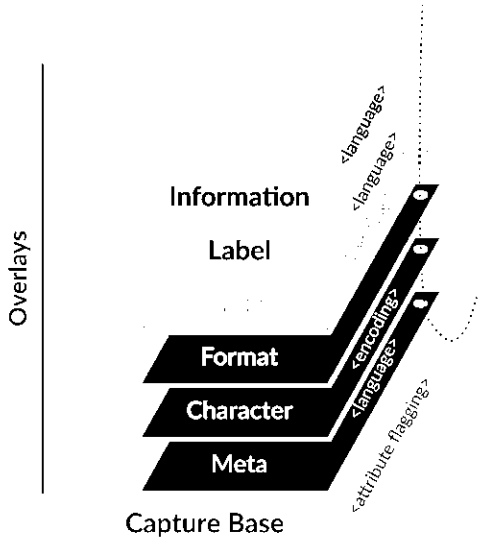

Figure 24: Overlay Stack

Explainer on OCA Objects:

Capture Base

A capture base is a stable base object that defines a single set of data in its purest form thus providing a standard base from which to decentralize data.

Attribute names and types are defined in the capture base. The construct also contains a blinding block which allows the issuer to flag any attributes that could potentially unblind the identity of a governing entity. With these attributes flagged at the base layer, all corresponding data can be treated as sensitive throughout the data lifecycle and encrypted or removed at any stage thus reducing the risk of identifying governing entities in blinded datasets.

Meta Overlay

A meta overlay is a core linked object that can be used to add contextual meta-information about the schema, including schema name, description and broad classification schemes.

Character Encoding Overlay

A character encoding overlay is a core linked object that can be used to define the character set encoding (e.g. UTF-8, ISO-8859-1, Windows-1251, Base58Check, etc.). This overlay type is useful when implementing solutions that facilitate data inputs across multiple languages.

Format Overlay

A format overlay is a core linked object that can be used to add formats, field lengths, or dictionary coding schemes to schema attributes.

Entry Overlay

An entry overlay is a core linked object that can be used to add predefined field values in a specified language to schema attributes. To minimize the risk of capturing unforeseen PII, the implementation of free form text fields is best avoided. This overlay type enables structured data to be entered thereby negating the risk of capturing and subsequently storing dangerous data.

Label Overlay

A label overlay is a core linked object that can be used to add labels in a specified language to schema attributes and categories. This overlay type enables labels to be displayed in a specific language at the presentation layer for better comprehensibility to the end user.

Information Overlay

An information overlay is a core linked object that can be used to add instructional, informational or legal prose to assist the data entry process.

https://wiki.colossi.network/en/Technologies/OCA/Developer/Adopt

Appendix D: FHIR-OCA Data Pipeline

HL7 FHIR formatted data is being specified as a preferred exchange format for EHR data being processed into vaccination, test or recovery certificates for the EU DGC, WHO SVC, VCI and other initiatives. The respective FHIR communities are creating FHIR Implementation Guides that provide technical direction on how to create and structure the relevant FHIR resources to be processed. This support from the FHIR communities helps to ensure that FHIR formatted record sets will be widely available for processing. HL7 has several other formats for health data exchange, these formats 2.x, 3.x, and CDA have libraries and mappings to support the conversion of data formatted from their respective formats into a FHIR format.

Being that FHIR EHR data records represent clinical information from the clinical application source, there are compliance, security and audit features available via FHIR that facilitate the accurate capture of state for the health event being described. This in turn provides for a transparent usage of the data keeping it aligned with the original reason for its extraction and capture. The FHIR-OCA approach to processing assumes that these mechanisms have been applied by the clinical application.

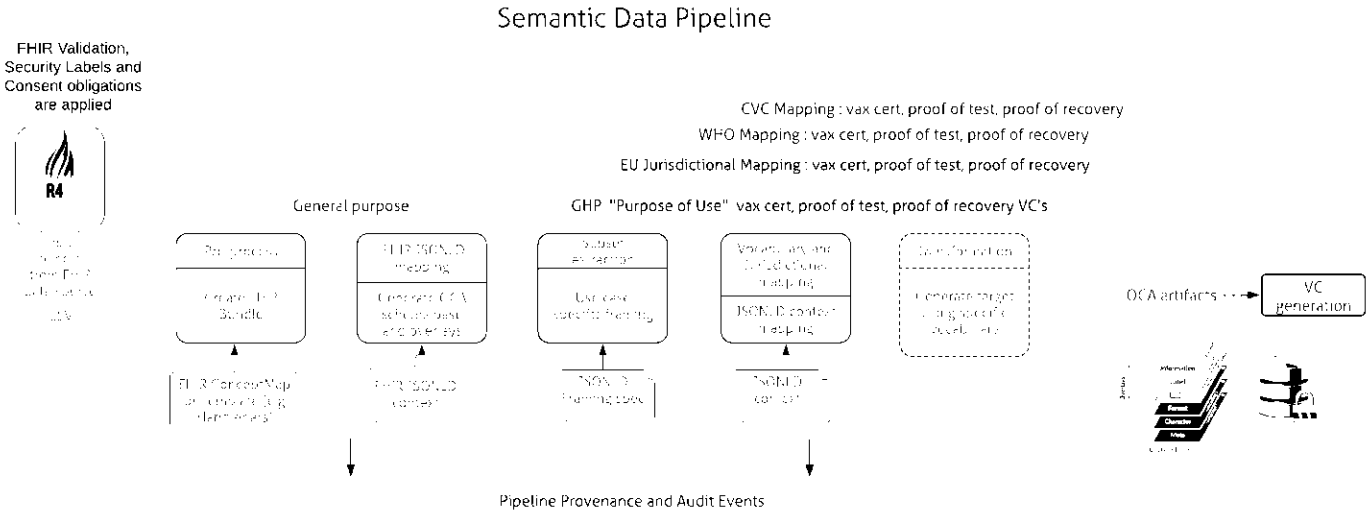

Figure 25: Semantic Data Pipeline

In the FHIR JSON-LD (JavaScript Object Notation for Linked Data) transform, the data elements are also structured into an OCA capture base. Next, the capture base elements have application context extracted and transformed into a set of overlay capture objects, the set of overlay objects are pre-defined to align with the purpose of use of the data set.

Finally, based on the purpose of use, jurisdictional and vocabulary mappings are applied and the target specific OCA artifacts are created. This set of OCA artifacts are then available for further encryption and persistence processing.

https://github.com/SemanticClarity/oca-fhir-cli

Appendix E: About the Good Health Pass Collaborative

Launched by ID2020, the Good Health Pass Collaborative is a multi-sector global initiative to establish principles and standards for digital health passes for international travel.

The Good Health Pass Collaborative is unique in that it is neither developing its own nor promoting any specific technology solution or product. Rather, the Collaborative has brought together more than 120 companies and organizations from across the travel, health, and technology sectors – including all of the major solution providers – in an attempt to dramatically streamline a standards-setting process which, under normal circumstances, might take years or even decades to complete.

Learn more at goodhealthpass.org.