COVID-19 Credentials Initiative ("CCI") Governance Framework V2.0

?? SEPTEMBER 2020

This CCI Governance Framework (the "**CCI GF**") V2.0,
was developed and approved by the CCI Governance Framework Task Force.
The CCI GF Task Force operates within the Trust Over IP Foundation.

NOTE: *This document includes references and content from the Sovrin Governance Framework Master Document (https://sovrin.org/wp-content/uploads/Sovrin-Governance-Framework-V2-Master-Document-V2.pdf).*

This page left intentionally blank

INSERT Table of Contents just prior to finalizing V2

Acknowledgements

The CCI Governance Framework (CCI-GF) has been developed through the contributions of knowledge, experience and expertise of a large number of global individuals. The CCI- GF Task Force would like to acknowledge their contributions and participation in the discussions forums. Key contributors include:

Ramon Bernabeu
Jacques Bikoundou
Thomas Cox
Oskar van Deventer
Eric Drury
Rieks Joosten
Eddie Kago
Line Kofoed
Kohei Kurihara
Dennis Landi
Sankarshan Mukhopadhyay
Markus Mummert
Indira Mysore
Ser-Huang Poon
Chris Raczkowski
Robin Renwick
Tony Rose
Jim St. Clair
Keerthi Thomas
Alex Tweeddale
Lucy Yang
Cecilia Yeung

The CCI-GF Task Force would like to especially thank Kelly Cooper for her inputs, suggestions and improvements to the readability and structure of this document; Drummond Reed for his wide-ranging expertise in the principles of Self-Sovereign Identity and how they apply to technology interventions around the COVID-19 pandemic; Scott Perry for his contributions on the topic of Trust Assurance Framework; Paul Knowles and The Kantara Initiative for the work on Blinding Identity Taxonomy; Karl Kneis and Mike Vesey for their assistance as chairs of the Ecosystem Foundry Working Group at the Trust over IP Foundation.

Requirements Notation and Conventions

The following conventions which appear in this document are adopted from the Digital Identity Guidelines (NIST SP 800-63-3[1]) and are to be read alongside IETF RFC 2119[2] to guide adoption of the CCI-GF.

1. The terms "**SHALL**" and "**SHALL NOT**" indicate requirements which are to be followed strictly in order to conform to the intent of the CCI GF and from which no deviation is permitted.
2. The terms "**SHOULD**" and "**SHOULD NOT**" indicate that among several possible approaches, one is recommended. This does not exclude the others or indicate a preference, nor does it state that a course of action is discouraged but not prohibited.
3. The terms "**MAY**" and "**NEED NOT**" indicate a choice that is allowed within the intents and purposes of the CCI GF

[1] https://csrc.nist.gov/publications/detail/sp/800-63/3/final
[2] https://tools.ietf.org/html/rfc2119

4. The terms “**CAN**” and “**CANNOT**” indicate a possibility and capability, whether material, physical or causal or, in the negative, the absence of that possibility or capability.

This page left intentionally blank

5.

1. Introduction

The year 2020 has proven to be a turning point in human history, where a pathogen, SAR-CoV-2, a virus that causes a range of illnesses generally referred to as COVID-19, has significantly and negatively impacted global societies and economies. To facilitate a return to fully functional societies, Verifiable Credentials (a "**VC"** or "**VCs"**) have been identified as a valuable tool. VCs provide a secure, privacy-protecting method for saving valuable and sensitive information as trusted digital data, that can be used to enable individuals and societies to manage and recover from the social and economic impacts of the COVID-19 pandemic.

For example, a COVID-19 test result (e.g. virus test, antibody test, etc.) for an individual can be recorded as a VC, enabling that individual (the VC "**Holder**") to privately and securely prove (a digital "**Proof**") to any other person (a VC "**Verifier**") the result of their COVID-19 test. The VC Proof can be cryptographically linked back to the COVID-19 test administrator and VC Issuer (the "**Issuer**"; for example, a trusted medical professional). In this way, the Verifier is able to place *trust* in a known or otherwise trusted Issuer of a VC, via secure, open-source, cryptographic protocols. This process is represented by the following diagram:

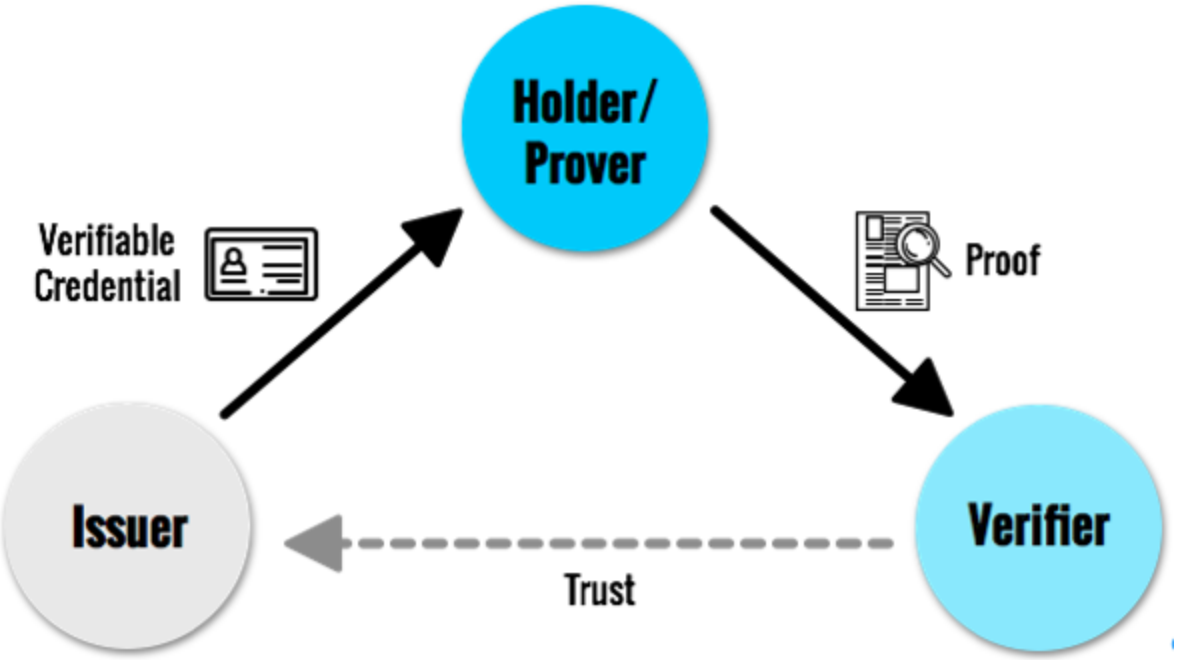

Figure 1: The Verifiable Credentials Trust Triangle

For more information about VC technology and governance, please refer to W3C Verifiable Credentials Data Model 1.0 Terminology, the Trust Over IP Foundation, and The Sovrin Governance Framework Glossary.

The CCI Governance Framework (the “CCI GF”) is an open source document that provides general principles, standards, and guidance for VCs being used for COVID-19 related use cases, with the aim of:

- protecting individuals (issuers, holders and verifiers),
- reducing utilization friction,
- ensuring regulatory compliance,
- shaping best practices.

CCI GF principles reflect the overarching spirit of VCs, which includes individual ownership of their personal data, privacy by design, and inclusivity for all people, organizations and cultures. The CCI GF is intended to be relevant and applicable in many jurisdictions and circumstances. Because global social, legal, and political landscapes are diverse, the CCI GF is primarily a principles-based VC governance standard that can be referenced and adopted as a foundational governance document for the widest possible range of jurisdictions and use cases. The CCI GF primarily provides flexible principles, rather than black-and-white rules, allowing people and organizations around the world to utilize the CCI GF in a manner that is suitable for their situation, while following the founding principles and spirit of VCs, particularly: (1) individual ownership of VCs, (2) privacy and confidentiality by design, and (3) inclusivity for all people, organizations and cultures.

Among the elements this framework addresses, are:

- Guiding Principles
- Design and Governance
- Compliance
- Governance Framework Disclosure by Default
- Identity Owner Controlled Storage by Default
- Anti-Correlation by Design and Default
- Guardian and Delegate Confidentiality
- Security by Design
- Ethical by Default and Design

2. Purpose

The fundamental purpose of the CCI Governance Framework (the “CCI GF”) is to provide an open source set of governing principles and rules to help guide the implementation and use of any COVID-19 associated VCs and their practical application. The document describes an open standards based VC implementation framework to best protect issuers, holders, and verifiers; reduce VC utilization friction; assure regulatory compliance; and shape best practices for implementing COVID-19 VC use cases.

The ultimate goal of the CCI GF is to help mitigate the spread of COVID-19 and strengthen our societies and economies. Additionally, the intended audience of this document includes all individuals, governments, NGOs, businesses, healthcare providers, healthcare workers, health insurance companies, public sector and private sector testing labs, and other organizations.

3. CCI GF Principles - Three Perspectives

This governance framework recognizes three distinct categories of principles and requirements necessary to govern safe, fair and equitable implementation of VCs for COVID-19 use cases. Definitions of these distinct categories stated below.

3.1. Foundational Principles

The Foundational Principles represent the core aspects of the Governance Framework and thus encapsulate the key attributes needed in a holistic system which adopts this framework. These principles indicate the necessary criteria for any implementation of VCs for COVID-19, measured through how they are implemented using technology.

3.2. Technology Principles

The Technology Principles represent the necessary technical choices to be made when transforming the guidelines of the foundational principles into actual end-user centric systems.

3.3. Governance Principles

The Governance Principles are the guidelines which enable the scope and nature of roles, processes and trust systems in an information architecture which is built using aspects of the Technology and Foundational Principles. The Principles provide specific purpose oriented

statements and assertions around the specific roles and process to be put in place in order to enable strong human-centric adoption of the governance framework.

4. Foundational Principles

The CCI GF embodies the following *Foundational Principles*. As stated in section 3.1, these are the core principles of the Governance Framework, which specify the key attributes which must be present in a holistic system which adopts this governance framework.

4.1. Openness and Interoperability

Adoption of the CCI GF SHALL imply adherence with the principles of openness and interoperability as established in this section. The CCI GF strongly advocates, promotes and supports development mechanisms that allow identity controllers[3] to experience interoperability or portability of their identity data to other networks and systems in alignment with " W3C open standards" for VC and DIDs

4.2. Accountability

Identity Controllers and stakeholders that choose to associate VC solutions with the CCI GF SHALL be accountable for conformance to the purpose, and principles documented in the CCI GF. All entities adopting the CCI GF SHALL be responsible for, and within the scope of their abilities, be able to demonstrate compliance with any other requirements of applicable law within their jurisdiction(s) of operations. Nothing in the CCI Governance Framework requires a VC solution to breach applicable laws or regulations as presently enacted for it to perform its obligations under the CCI GF.

4.3. Sustainability

VC solutions that intend to adopt the CCI GF SHOULD strive to be technically, economically, socially, ethically, and environmentally sustainable, and contribute to the improvement of the well-being of people and the environment for the long term.

- Technically: incorporate interoperable and reusable, non-proprietary technologies;
- Economically: VCs should not present an economic burden to obtain and use;
- Socially: VCs should not exclude or dissuade participation by any individual or social groups;
- Ethically: VCs should not preclude ethical concerns or impacts, both potential or real, from being openly and transparently discussed;

[3] This term refers to the subclassifications of Entity that may be held legally accountable. Identity Controllers include Individuals and Organizations but do not include Things. (See Glossary for additional information)

- Environmentally: VCs should contribute to not only minimum impact on the verification process and reduce the carbon footprint of all identity management resources.

4.4. Collective Best Interest

VC solutions that adopt the CCI GF SHALL act in the collective best interests of the CCI Community. It does not favor the priorities or benefits of any single Identity Owner, or group of Identity Controllers, over the mission of the CCI Community as a whole..

4.5. No Single Point of Failure

The CCI GF credentials SHOULD NOT have any single point of failure.

4.6. Maintain Consistent Experience

Developers adopting the CCI GF MAY design comparable experiences for all user communities to include consistent design elements, accessibility, and inclusive language.

4.7. Censorship Resistant

Adopters of the CCI-GF SHALL utilise and implement VC tools, applications, and services that do not discriminate individuals or groups based on race, ethnicity, religion, health, sexual orientation, membership of organisations (e.g., trade union), or personal beliefs and political opinions.

A solution that adopts and implements the CCI-GF must require that a third-party entity cannot inappropriately modify or revoke VCs, shut-down VC services, or deny access to a VC service without authorization.

4.8. Privacy Preserving

The principles of decentralized identity embody the concept that personal identity is “self-sovereign” and the ultimate use of that identity is governed by the credentialed identity owner. As such, the CCI GF SHALL strongly discourage any use of this framework that results in technical or regulatory privacy infraction, such as surveillance, personal tracking, and abuse.

Identity controllers SHOULD respect the privacy, rights, and legal protections of the individuals whose VCs they maintain control of, including clear accountability and transparency mechanisms.An individual’s right to be forgotten (i.e. the right for their personally identifiable data to be erased) MUST be promptly honored ever applicable.

Any VC developer's priority SHOULD include design standards that enable and support the right to privacy for users.

4.9. Protection against coercion

The CCI GF SHALL enable the protection of the users of applications and systems which have adopted the governance framework against forms of coercion. Such coercion can be designed to force the user to act against their own interests. The governance framework MAY encourage adoption of potential counter-measures against coercion. These can include the following:

1. Require authoritative verifier.
2. Require evidence collection.
3. Require enabling anonymous complaints.
4. Require remote/proxy verification.
5. Require complying holder agent.
6. Require what-you-know authentication.

For additional information on the above approaches please see this RFC[4].

4.10. Ethical By Design and Default

The CCI GF promotes generally accepted best practices of ethical data collection, management and use. Ethical data usage is underpinned by principles of privacy, agency and equitability that demonstrate fair, transparent and respectful approaches to the acquisition, storage, processing, publication and commercialization of data. Data ethics provide a set of essential principles dealing with accepted standards of data usage by, within and among professionals and organisations.

Organizations that follow the CCI GF SHOULD determine how their actions could be perceived and avoid potential adverse impacts to stakeholders and their reputation in the future, including how their actions may impact on the perception of the CCI GF itself. Data strategies, processing and acquisition approaches should be adapted to ensure the ethical use of data consistently.

The CCI GF ethical data collection, management and use principles are as follows:

a. Ensure private personal or organizational information (the "PPOI") and the identities of natural persons remain anonymous and private unless otherwise required, unless a PPOI owner otherwise explicitly requests and/or explicitly consents to their data being made available to others, or to further processing, within a clearly defined set of use restrictions,

4 https://github.com/hyperledger/aries-rfcs/tree/master/concepts/0289-toip-stack#countermeasures-against-coercion

b. Ensure that increased levels of subject identifiability are applied carefully, incrementally and appropriately according to reasonable needs and an acceptable level of privacy exposure risk,

c. Ensure that shared PPOI is treated confidentially by any recipient;

d. Ensure that proprietary PPOI is treated as the private property of the appropriate organizations and individuals, with intrinsic value that is respected and protected, with equitable means provided for realizing that value;

e. Provide individuals with a transparent view of data processing activities and the ability to exercise their rights related to any data processing of PPOI that is not required or permitted by law;

f. Ensure that data activities are respectful of, and do not interfere with, human will/self-determination;

g. Ensure that data processing approaches and results do not present unfair or prejudicial biases to individuals or groups of individuals. For example, two individuals with the same COVID test results status should not be subject to different restrictions based on their status;

h. Set out definitions for data privacy, agency and ownership with a specific 'ethical' context;

i. Recognize that there may be attributable value to PPOI of other data;

j. Adopt principles for allowing transfer of data between data processors and providers at an individual's request, ensuring rights to data portability;

k. Adopt principles for an open consent process for the use of PPOI or other data;

l. Adopt principles for notification of changes to personal data and change of use of personal data;

m. Adopt principles for correcting data;

n. Adopt principles for erasure of data and ensure fair rights to be forgotten;

o. Adopt principles for developing policies for arbitration allowing any individual or organization ability to control their PPOI or other data.

Privacy-enhancing techniques, including anonymization and pseudonymization, exist and are evolving. Adopters of the CCI GF MUST employ appropriate techniques to proactively promote ethical data use principles by default.

4.11. Inclusion By Design and Default

Access to CCI Infrastructure that follows the CCI GF must be open to all Individuals and Organizations, on a comparable basis, without exclusion of specific persons, communities, technology limitations, or device availability. Great care for inclusion of underserved populations

SHALL be proactively supported and promoted by individuals and organizations that adhere to the CCI GF. Underserved populations include, but are not limited to:

a. Digital limitations (e.g., access to connected devices)
b. Physical or cognitive limitations (e.g., disability or incapacity)
c. Political & social status (e.g., stateless individuals, being a child, a woman, LBTQ+, an Animal, Natural Thing, homeless, etc.)
d. Financial status (e.g., unbanked, unemployed, unemployable)
e. Literacy & language (e.g., low literacy or not speaking a language)

4.12. Data protection compliance by design and by default

The CCI GF provides guiding principles for the practical implementation of decentralized identity use cases for COVID-19.

For any decentralized identity model to practically work in a real life use case, there must be clarity as to how Decentralised Identifiers (DIDs) and Verifiable Credentials (VCs) fit into global data protection frameworks, such as the General Data Protection Regulation in the European Union.

Given that the VC and DID technical innovations are new, constantly developing, and function in a completely different manner to 'centralized' data management models, it is important to clearly lay out:

a. What constitutes personal data in a decentralized identity model,
b. Who assumes responsibility for managing and controlling this personal data, and
c. Can decentralized identity enable better data protection compliance by default?

The CCI community have created a guiding document which addresses these overarching questions, drawing on guidance from standardisation initiatives (the International Standards Organisation, German Institute for Standardization, Spanish Data Protection Board, and similar) focused on encryption and hashing, blockchain and distributed ledger technologies, and decentralized identity technology. Specific guidance from these bodies is supplemented by guidance from European Entities such as the European Data Protection Board, the European Parliamentary Research Service, and the European Blockchain Observatory.

That document is applicable to any entity designing VCs, and explains how the architecture of a decentralized identity ecosystem SHOULD be designed to ensure best data protection and privacy protection for individuals (data subjects). For any COVID-19 use case, given the sensitive level of data likely to be contained in VCs, the guidance is particularly pertinent.

The document may be summarised by the following:

a. Personal data should be viewed as any information relating to an identified or identifiable natural person. An identifiable natural person is one who can be identified, directly, or indirectly by the data in question, including both presently, and in the future, taking into account reasonable means, available technologies, and resources required.

b. A hash of personal data is viewed as pseudonymised personal data.

c. Encrypted personal data is viewed as personal data regardless of whether the possibility to decrypt the data remains (existence of decryption key). This is due to the potential of identification of the natural person when coupled to additional data sets (time-stamps, encryption/decryption logs, IP addresses, network related data, additional meta-data, etc).

d. It is advised that all personal data is maintained off-ledger in compliance with applicable data protection regulations to ensure adequate privacy and data protection for data subjects.

e. Efforts should be made to ensure that the identity holder maintains control (where feasible) of their credentials. In cases where this is not possible, the identity controller shall adhere to its legal obligations, and shall adhere to a adequate governance framework, such as the one currently being read (CCI GF)

f. Any entity considering deployment of a VC based credential system that includes covid related health information (or related health data) shall conduct, dependent on jurisdiction, either a Privacy Impact Assessment (according to ISO/IEC 29134:2017 Information technology — Security techniques — Guidelines for privacy impact assessment) specifications, or a Data Protection Impact Assessment (as per legal requirement of the GDPR, Article 25).

g. Deployers of CCI should attempt to provide the identity holders with credentials that allow for selective disclosure, and preferably through methods such as Zero Knowledge Proofs to ensure best data protection practice.

https://docs.google.com/document/u/2/d/164S-nNnMHlPZex5lKenuGRhavvt8qeKIdTPHFAD5b_c/

5. Technology Principles

The CCI GF promotes technology principles which support the foundational principles outlined in Section 4. The purpose of the technology principles is to identify necessary technical choices to be made when transforming the guidelines of the foundational principles into actual end-user centric systems.

5.1. Privacy By Design

The design, governance, and operation of CCI credentials SHALL follow the seven principles of Privacy by Design to the greatest extent possible. These principles include:

a. Proactive not reactive; preventative not remedial
b. Privacy as the default setting
c. Privacy embedded into design
d. Full functionality — positive-sum, not zero-sum
e. End-to-end security — full lifecycle protection
f. Visibility and transparency — keep it open
g. Respect for user privacy — keep it user-centric

5.2. Decentralization By Design

Recognizing our role as part of the ToIP Foundation, the CCI GF SHALL promote the principles of decentralization to the extent considered necessary to address the outcomes desired by the CCI GF. As the business, legal, and technical limitations of decentralization may change over time; the CCI GF Working Group shall continuously examine all points of control, decision, and governance to seek ongoing conformance with this principle.

5.3. High Availability

The CCI GF SHALL require any participating Credentials to be designed and implemented within an infrastructure intended to maximize availability for all potential users across multiple output devices ranging from smartphone to paper.

5.4. W3C DID Core Compliant

An agent is a piece of software, either acting on an Identity Controller's device or in a cloud environment, designed to make decisions for the Identity Controller based on permissions set by the Identity Controller. Agents following the CCI GF SHALL be compliant with the W3C DID Core Data Model Specification.[5] In this context, an Agent may be a software program or process used by or acting on behalf of an Entity to interact with other Agents or with distributed ledgers (see Glossary).

[5] This specification is still a work-in-progress in the W3C DID Working Group.

5.5. W3C VC Data Model Compliant

Issuers, Holders, and Verifiers following the CCI GF SHALL issue, hold, and accept VCs that are compliant with the W3C VC Data Model Specification[6].

5.6. Owner Controlled Storage By Default

Agents store private data in decentralized, encrypted data storage, controlled by the Identity Owner by default. Private data storage SHOULD adapt to low- to no-technology environments where control remains with the Identity Owner regardless of device.

5.7. Anti-Correlation By Design and Default

CCI GF designs and implementations SHALL avoid correlation of an Identity Owner, or anything associated with an Identity Owner, without the direct knowledge and informed consent of the Identity Owner.

5.8. Guardianship and Delegate Confidentiality

Utilization of a Guardian or Delegate by a CCI GF Identity Owner MAY be confidential and disclosed with required authorization of the Identity Owner (where possible) and the Guardian or Delegate. All instances of Identity Owner, in this document, may be substituted with an authorized Guardian or Delegate.

5.9. Security By Design

The design, governance, and operation of CCI VCs follows the principles of Security by Design and ensures applicable open standards to the greatest extent feasible consistent with the other CCI principles.

5.10. Least Privilege

Access and authorization of the applications, Agents, and network services that use and comprise the CCI GF subscribe to the concept of least privilege.

5.11. Data Protection By Design and Default

Entities that follow the CCI GF, in the processing of data, SHALL adhere to industry best practice data protection principles to the greatest extent feasible. When additional local or transnational data protections apply, entities MUST make every effort to also be consistent with

[6] https://www.w3.org/TR/vc-data-model/

all CCI GF principles. Compliance with the CCI GF does not exclude the need to comply with existing regulations in relevant jurisdictions.

5.12. Accuracy

CCI GF Entity data must be accurate and, where necessary, kept up-to-date. Every reasonable step must be taken to ensure that where personal data is inaccurate it is erased or rectified without delay.

5.13. Integrity and Transparency

CCI GF Entity data processing provides appropriate, measurable security of the data, including protection against unauthorized or unlawful processing, accidental loss, destruction, or damage, using significant technical and organizational measures.

5.14. Authenticated Access

Secure authenticated access to end-user (i.e holder) CCI GF Entity data must be preserved at all times. CCI GF Entity data must at the minimum be secured via a PIN or password but ideally include biometric authentication mechanisms such as fingerprint verification or facial recognition.

PINs and/or passwords need also be sufficiently strong and implement a timeout feature to withstand brute-force attacks.

5.15. Purpose Limitation

Data is required to be collected for specified, explicit, and legitimate purposes only. Data must not be further processed contrary to this requirement, or repurposed without verifiable approval by a data subject and or Identity Owner. Further processing for archiving purposes in the public interest, scientific and historical research purposes, or statistical purposes, is not considered incompatible with the original processing purposes. However, permission for anonymized, aggregated, or disaggregated data SHOULD require approval and/or explicit consent by Identity Owners.

5.16. Data Minimization

CCI GF Entity data must be relevant and limited to minimum levels of identifiability necessary (starting from a position of anonymity) to the purpose for which it is processed. Data Minimization should ensure that subjects are anonymous by default and that increased levels of identifiability are applied carefully, incrementally and appropriately according to reasonable needs and a consequently acceptable level of privacy exposure risk.

5.17. Storage Limitation

CCI GF Entity data must be kept in a form which permits identification of Entities for no longer than the minimum duration necessary for processing.

6. Governance Principles

The CCI GF embodies the following governance principles. As stated in section 3.3, these principles are the guidelines which enable the scope and nature of roles, processes and trust systems in an information architecture which is built using aspects of the Technology and Foundational Principles. The Governance Principles provide unambiguous statements and assertions around the specific roles and process to be put in place in order to enable a strong human-centric adoption of the governance framework.

6.1. Lawfulness, Fairness and Transparency

CCI GF Entity Data must be processed lawfully, fairly, and transparently to the relevant CCI Entity, or the CCI Entity's Identity Owner, Guardian, Delegate, or Controller.

6.2. Storage Jurisdiction

Data storage for national level CCI implementations must be in compliance with the government policies regarding the geographical locality of the CCI GF Entity data where relevant.

6.3. Governance Framework Disclosure By Default

CCI GF Entities, SHALL, by default, disclose the Governance Framework under which a Connection is created, an Interaction is performed, or a VC is exchanged. Agents, by default, notify the Identity Owner of conflicts among the Identity Owner's privacy preferences, the Governance Framework's privacy policies, and relevant security regulations.

6.4. Data Subject or Credential Holder Rights

Adopters of the CCI GF SHALL accommodate the following rights of any data subject and credential holder:

a. Right of access provided to the holder's or data subject's own personal data

b. Right to rectification

c. Right to be forgotten (deletion)

d. Right to stipulating processing restrictions (refer to 7.5 Purpose Limitation?)
e. Right to be informed who has received or processed my data or credentials
f. Right to data portability allows holders or data subjects to obtain and re-use personal data or credentials
g. Right to object or to stop processing of personal data or credentials
h. Right not to be profiled or subjected to solely automated decisions

NOTE: these are GDPR principles

6.5. Service Provider Attestation to Preserving and Safeguarding Rights

Service providers SHOULD provide clear guidance to users regarding to what level their personal data or credentials are safeguarded or protected. This attestation MAY be legally binding and admissible in a court of law.

Appendix A: Glossary

Glossary (attribution Sovrin Foundation Glossary v3)

Agency

A service provider that hosts Cloud Agents and may provision Edge Agents on behalf of Entities. Agencies may be Unaccredited, Self-Certified, or Accredited.

Agent

A software program or process used by or acting on behalf of an Entity to interact with other Agents or with the Sovrin Ledger or other distributed ledgers. Agents are of two types: Edge Agents run at the edge of the network on a local device; Cloud Agents run remotely on a server or cloud hosting service. Agents require access to a Wallet in order to perform cryptographic operations on behalf of the Entity they represent.

Business

An institution (or sometimes, an individual acting as an institution) that seeks to generate economic value by providing goods and services.

Claim

An assertion about an Attribute of a Subject. Examples of a Claim include date of birth, height, government ID number, or postal address—all of which are possible Attributes of an Individual. A Credential consists of a set of Claims.

Confidentiality

Obligation not to disclose information or the right of an individual to withhold information from others.

Credential

A digital assertion containing a set of Claims made by an Entity about itself or another Entity. Credentials are a subset of Identity Data. A Credential is based on a Credential Definition. The Entity described by the Claims is called the Subject of the Credential. The Entity creating the Credential is called the Issuer. The Entity holding the issued Credential is called the Holder. If the Credential supports Zero Knowledge Proofs, the Holder is also called the Prover. The Entity to whom a Credential is presented is generally called the Relying Party, and specifically called the Verifier if the Credential is a Verifiable Credential. Once issued, a Credential is typically stored by an Agent. (In Sovrin Infrastructure, Credentials are not stored on the Sovrin Ledger.) Examples of Credentials include college transcripts, driver licenses, health insurance cards, and building permits. See also Verifiable Credential.

Data Controller

As defined by the EU General Data Protection Regulation (GDPR), the 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.

Delegate

An Identity Owner that acts on behalf of another Identity Owner. Formally, a Delegate is the Holder of a Delegation Credential.

Entity

A data subject.

Government

A federal/national, state/provincial, or local unit of political governance. Governments make, enforce, and adjudicate laws and regulations. They often have a complex internal structure (bureaus, agencies) and special standing in legal systems.

Guardian

An Identity Owner who administers Identity Data, Wallets, and/or Agents on behalf of a Dependent. A Guardian is different than a Delegate—in Delegation, the Identity Owner still retains control of one or more Wallets. With Guardianship, an Identity Owner is wholly dependent on the Guardian to manage the Identity Owner's credentials.

Guardianship

The legal responsibility of serving as a Guardian. In Sovrin Infrastructure, Guardianship maps to the rights and responsibilities defined in prevailing legal constructs such as parent, in loco parentis, legal capacity, and power of attorney. Note that Guardianship is not Impersonation or Delegation. While the term Guardianship in this glossary applies strictly to natural persons (Individuals) as Dependents, in a more general sense the term can also be applied to Natural Things (such as pets or animals).

Healthcare Provider

An institution, often a Business that delivers healthcare-related goods and/or services.

Healthcare Worker

An Individual employed by a Healthcare Provider. We assume that the interests of Healthcare Workers are colored by their status as individuals; however, the result is not the simple union of the two perspectives. For example, Individuals may want to travel, and when acting as Healthcare Workers, this is rarely a top priority.

Identity Controller or Owner

This term refers to the subclassifications of Entity that may be held legally accountable. Identity Controllers include Individuals and Organizations but do not include Things. The actual legal accountability of an Identity Controller for any particular action depends on many contextual factors including the laws of the applicable Jurisdiction, Guardianship, and so forth.

Individual

A natural person, in a legal sense. Individuals are the locus of human rights. They generally value autonomy and privacy. They have health histories and status, and they are the unit of treatment and decision-making for healthcare. They vote, travel, and spend money. They are held legally accountable. In many cases, Individuals are the Holders of VCs. Some individuals are not capable of self-sovereignty due to circumstances; this raises the issue of guardianship.

Licensor

An institution that accredits or licenses Healthcare Workers and/or Healthcare Providers. The institution may serve as a Government, NGO, or a different type of institution.

Non Governmental Organization (NGO)

A non-governmental organization that exists to provide services, typically without a profit motive. In some contexts (e.g., refugee camps), NGOs may assume a role that has much in common with a local government.

Open Standards

Technical standards that are developed under an Open Governance process; are publicly available for anyone to use; and which do not lock in users of the standard to a specific vendor or implementation. Open Standards facilitate interoperability and data exchange among different products or services and are intended for widespread adoption. Many Open Standards have implementations that are available under an Open Source License.

Privacy

State of being undisturbed or free from public attention.

Appendix B: Practical Examples - Verifiable Credential Use Cases

The CCI Use Case Implementations Workstream at Covid Credentials Initiative has produced a set of use cases around usage of verifiable credentials specific to COVID-19 pandemic. These scenarios are designed to establish the attributes present in a technology architecture created using verifiable credentials and digital identity. A selection of these use cases are included in the appendix to enable the reader to relate the principles and aspects of the governance framework in practical applications of technology interventions.

The listed use cases are not exhaustive but rather to be taken as an indicative one - demonstrating the potential and possibility of a secure, privacy-preserving system based on open standards.

UC 00: Creating and Maintaining Local Assurance Communities (LACs)

[description]

An important part of implementing a Verifiable Credentials based system is the governance authority. This role is undertaken by an organization which has the regulatory authority to direct, control and approve the entire set of workflows involved in enabling a digital identity centric VC based system around health status.

This use case was originally designed by Rieks Joosten (TNO) and Oskar van Deventer (TNO) as part of an effort to focus on the question “what is locally needed for trustworthy (Covid-19 and other) credentials to be actually used”. Credentials may provide privileges, like physical or digital access, there is a risk that untrustworthy credentials provide illegitimate privileges, or that credentials that should provide such privileges do not work.

The concept of ‘Local Assurance Community’ or LAC is introduced to help organize trust ‘locally’ (e.g. within a specific domain, jurisdiction, etc.) by capitalizing on the fact that the parties that will constitute the LAC have already established assurance mechanisms (e.g. based on proximity and familiarity) on which such trust can be based. This enables e.g. issuers to be accredited to issue credentials of type X under the specifics (and governance) of a LAC.

UC 2: Proof of Covid-19 status or, Immunity by Exposure [solution | VC schema]

The adoption of various software patterns to respond to the COVID-19 pandemic include a situation where an individual will need to present their health status upon request. Such a presentation is linked with access to services and this is required by regulations in place locally.

The multiple forms and facets of this scenario was analysed and documented by Antti Kettunen, Michael Corning, Andre Kudra, Dakota Gruener and Markus Mummert. The simplest description of this use case is that Bharat wants to prove, either face-to-face or remotely, that he has recovered from a COVID-19 infection (e.g., so he can drive a car for a rideshare app without being a disease vector).

Documents:

- Antti Kettunen: [use cases CCI] Credential mapping to segmentation
- Michael Corning: CCI Back to Work Verifiable Presentation

UC 11: Verify the Verifier

While the self-governance and management of verifiable credentials makes it very easy to disclose information based on notice/consent mechanism, it is important to validate that the entity requesting the information (in the form of credentials) is actually authorized to do so. This scenario was conceived and designed by Alex Blom (Bloqzone), Sterre den Breeijen (TNO), Oskar van Deventer (TNO), Randy Zhang and Will Abramson (Edinburgh Napier University)

The use case focuses on the question "**how do we reduce the risk that Verifiers make draconian requests for COVID-19 credentials**". COVID-19 credentials may be useful e.g. to health-safely support access to vulnerable elderly in care homes by their family, caretakers and volunteers. However, they are not supposed to be used to harass citizens for them at situations where this would not be needed. It also follows that if adequate verification information is not provided by the verifier the individual can revoke consent and disallow sharing of the information.

Link:
https://docs.google.com/document/d/1PQvDm1ssKypH9X1CV97sStOxfnnSpzLKyDEPJ_bAp7E

Appendix C: Foundational Principles Checklist

The CCI GF espouses guiding principles that shape the development, adoption and implementation of Verifiable Credentials used in the effort to overcome the challenges presented by the COVID-19 pandemic.

Organisations that adopt the CCI GF model are strongly urged to adhere to these same principles.

Below is a checklist that can help an organization evaluate its level of adherence to the CCI GF principles.

1. PRIVACY PRESERVING	**REQUIRED**
The principles of decentralized identity embody the concept that personal identity is “self-sovereign” and the ultimate use of that identity is governed by the credentialed identity owner. As such, the CCI GF strongly resists any use of this framework that results in technical or regulatory privacy infraction, such as surveillance, personal tracking, and abuse. Any VC developer’s priority should include design standards that enable and support the ethical right to privacy for users.	
Can you detail the different tools and approaches you have taken to ensure user privacy?	**Y / N**
If no, please provide **justification** for this decision	

2. OPENNESS & INTEROPERABILITY	**REQUIRED**
Adoption of the CCI GF shall imply adherence with the principles of openness and interoperability. The CCI GF strongly advocates, promotes and supports development mechanisms that allow identity controllers to experience interoperability or portability of their identity data to other networks and systems in alignment with " W3C open standards" for VC and DID. RESOURCES: · W3C standards	
Can you demonstrate openness and interoperability in your solution?	**Y / N**
If no, please provide justification for this decision	

3. ACCOUNTABILITY	**REQUIRED**

Identity Controllers and stakeholders that choose to associate Verifiable Credentials with the CCI GF SHALL be accountable for conformance to the purpose, principles, ethics, and policies of the CCI GF. All Entities participating with the CCI GF SHALL be responsible for, and within the scope of their abilities, be able to demonstrate compliance with any other requirements of applicable law within their jurisdiction(s) of operations. Nothing in the CCI Governance Framework requires a CCI Entity to breach applicable laws or regulations as presently enacted for it to perform its obligations under the CCI Governance Framework.

Can you demonstrate accountability in your solution?	**Y / N**
If no, please provide justification for this decision	

4. SUSTAINABILITY	**RECOMMENDED**
VCs that intend to follow the CCI GF SHOULD strive to adopt technical, economic, social, ethical, and environmentally sustainable best practices, and contribute to the improvement of the well-being of people and the environment for the long term. RESOURCES: · United Nations Sustainable Development Goals	
Can you demonstrate sustainability in your solution?	**Y / N**
If no, please provide justification for this decision	

5. COLLECTIVE BEST INTEREST	**RECOMMENDED**
The CCI Governance Framework Working Group acts in the collective best interests of the CCI Community. It does not favor the priorities or benefits of any single Identity Owner, or group of Identity Controllers, over the mission of the CCI Community as a whole. CCI solutions derive from the most current scientific knowledge.	
Can you demonstrate collective best interest in your solution?	**Y / N**
If no, please provide justification for this decision	

6. DECENTRALISATION BY DESIGN	**RECOMMENDED**
The CCI GF promotes the principles of decentralization to the extent considered necessary to address the outcomes desired by the CCI GF. As the business, legal, and technical limitations of decentralization may change over time; the CCI GF Working Group shall continuously examine all points of control, decision, and governance to seek ongoing conformance with this principle.	
Can you demonstrate the adoption of decentralisation principles in your solution?	**Y / N**
If no, please provide justification for this decision	

7. HIGH AVAILABILITY	REQUIRED
The CCI GF requires any participating Credentials to be designed and implemented within an infrastructure intended to maximize availability for all potential users across multiple output devices ranging from smartphone to paper.	
Can you identify the mechanisms your solution uses to ensure high availability?	**Y / N**
If no, please provide justification for this decision	

8. NO SINGLE POINT OF FAILURE	REQUIRED
The CCI GF credentials should take the strongest measures available to ensure no single point of failure.	
Can you explain how your solution mitigates the risk of a single point of failure?	**Y / N**
If no, please provide justification for this decision	

9. MAINTAIN CONSISTENT EXPERIENCE	RECOMMENDED
CCI Developers should endeavour to design comparable experiences for all user communities to include consistent design elements, accessibility, and inclusive language.	
Can you explain how your solution addresses consistent user experience?	**Y / N**
If no, please provide justification for this decision	

10. CENSORSHIP RESISTANT	RECOMMENDED
The CCI GF supports the development and implementation of verifiable credential tools, applications, and services that cannot be used to discriminate individuals or groups based on race, ethnicity, religion, health, sex life or orientation, membership of organisations (e.g., trade union), or personal beliefs and political opinions. A CCI GF- adopted and implemented framework requires that a third party entity not modify or revoke credentials, shut-down, or deny access to a credential service without authorization.	
Can you explain how your solution is censorship resistant?	**Y / N**
If no, please provide justification for this decision	

Appendix D: Verifiable Credential Levels of Assurance

Users of CCI VCs should have a convenient and transparent system to understand and interpret the reliability of any information (the “Claims”) that might be included in a CCI VC. To facilitate this need, the CCI GF offers a basic guideline for Levels of Assurance (the “LOA”) which may be associated with any CCI VC. This Credentials Level of Assurance Framework intends to interact with transnational General Levels of [Identity] Assurance Frameworks such as: (a) UK Government GPG45, (b) NIST Special Publication 800-63-3 Digital Identity Guidelines, (c) the European electronic identity and trust services regulation (eIDAS).

Level 0

At this level, no VC is produced for a given Claim. Level 0 indicates that the information is not included in the CCI GF.

Level 1

Claims that are self-attested, with no third-party support or verification, are defined as Level 1 claims. The Issuer is also the Holder and the Subject. Mistakes and fraud for a Level 1 Claim are not controlled, and a Verifier must assess for themselves may rely purely on the credibility of the person that issues such Claim in a VC. For example, a person might self-report their weight as 80kg. One value of a Level 1 VC is that it places the Issuer on record. If the Claim is later proved false, this can affect the Issuer’s reputation. Many police departments require officers to make written attestations (Claims) about their own conduct, e.g. “I read the suspect their Miranda rights when I arrested them”. If it is later proved that the officer made a false Claim, the officer can be punished or otherwise held accountable on the basis that they are forbidden by law and their employment contract from making false written Claims. This reduces the overhead on the department of setting up a multitude of elaborate accountability mechanisms specific to each element of officer conduct, relying instead on the “no false Claims” punishment mechanism.

Level 2

Claims made by a third-party about the Subject of a VC, where the third-party is not well known to a verifier, are considered to be Level 2 Claims. In this situation, a Verifier must use their judgement to assess the credibility and potential accuracy of such VC Claims. For example, an unknown self-proclaimed medical professional, with no verifiable professional license issued by any appropriate licensing agency in the relevant jurisdiction, might issue a VC with Claims about a person’s COVID-19 test results.

Level 3

Claims made by a third-party about the Subject of a VC, where the third-party is known (to the Verifier) and can demonstrate that it has met appropriate professional license requirements in the relevant jurisdiction, are considered to be Level 3 Claims. A medical professional that has reliably demonstrated their required professional status and valid licences in a verifiable and auditable manner (such as with an associated personal or organizational identity VC that is reasonably demonstrated to be based on qualifying licenses, etc. issued by relevant authorities in the jurisdiction), would be a trusted source of Level 3 Claims for a CCI VC. For example, a COVID-19 test result VC issued by a doctor licensed to provide such test results in a jurisdiction, and where such licenses are verifiable as part of a VC issued by said doctor. Such COVID-19 test credential VC is considered to have a LOA of Level 3.

Level 4

Extraordinary measures beyond Level 3 may be applied allowing CCI GF participants to establish their own guidelines and requirements for Level 4 Claims. These might include posting of bonds or providing guarantees or warranties.

LOA guidelines above represent minimal standards for any LOA system that may be adopted and reported by a CCI VC issuer. CCI VC Holders and Verifiers must be made aware, by organizations that operate in compliance with the CCI GF, of exact details and implications of what any LOA might mean for CCI VCs they might hold or verify.

Appendix E: Trust Assurance Model

The Governance Principles explained in the document aid in raising the level of trust, assurance and credibility enabled within a system designed to be complying with the Technology Principles. For a digital system design such as the ones to be implemented for COVID-19 related technology interventions, the presence of trust is a key aspect.

Trust can be defined as the "firm belief in the reliability, truth, ability, or strength of someone or something". Digital trust is built from three main components: *Cryptographic Trust; Human Trust and Referential Trust. Referential Trust* is established through a trustworthy entity transferring trust upon a third party[7]. The existence of human trust in the technology implementations around COVID-19 depends heavily on the concept of referential trust - through the creation and existence of specific roles. These roles include Trust Anchor; Credential Registry, Governance Authority, Auditor and Audit Accreditor.

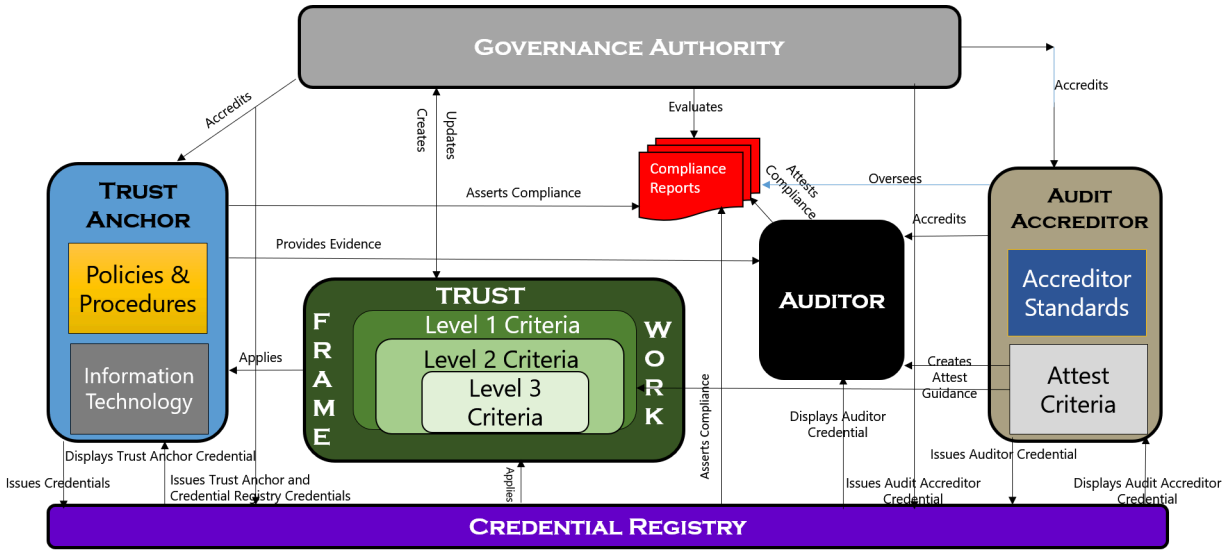

Figure: A Referential Trust Ecosystem (representative illustration)

The ecosystem creates assurance to verifiers, credential holders and relying parties that trust anchors are applying generally accepted trust criteria to their methods and practices by the introduction of accreditation and independent third-party audits that act in their interest. Relying parties acquire trust from the ecosystem based on the ability of the players to follow through on its commitments and the integrity of its decisions. Symbols of this trust are stored on a publicly accessible credential registry it can be propagated throughout the ecosystem.

[7] https://wiki.trustoverip.org/display/HOME/GSWG+Trust+Assurance+Task+Force

Appendix F: Healthcare Data Security and Privacy

Data privacy and security are increasingly a concern in nearly all industries , more so in healthcare. From HIPAA and data breaches to the patient perspective and EHRs, here are some key information to know about data security and privacy issues in healthcare.

HIPAA

1. The Health Insurance Portability and Accountability Act (HIPAA), designed to protect healthcare information security and confidentiality , enacted in 1996, apply to all healthcare providers, health plans and healthcare clearinghouses.
2. Under the HIPAA privacy rule, patients have a number of rights on their protected health information. HIPAA violations can come with both civil and criminal penalties.

Data Breaches

1. The most expensive data breaches occur in the United States and Germany.
2. Data breaches could cost the healthcare industry as a whole $6 billion each year, according to a Ponemon Institute report
3. Criminal attacks are the leading cause of data breaches in healthcare. The number of criminal attacks on healthcare organizations has leapt 125 percent since 2010.
4. There are a multitude of technical issues to consider when safeguarding against data breaches.
5. In addition to addressing the technical side of data security, healthcare organizations must have operational controls in place
6. The high-profile nature of breaches like the Anthem case can drive other healthcare providers to take a second look at their own cybersecurity policies. An Experian Data Breach Resolution and Ponemon Institute found media coverage of data breaches has driven 69 percent of companies to reevaluate and prioritize security.

The Patient side

1. Healthcare providers are not the only ones concerned with data breaches. Depending on the type of information accessed, patients too can be exposed to risk. A Software Advice survey found that 45 percent of respondents were moderately or very concerned about security breaches involving personal health information.
2. Providers have traditionally safeguarded healthcare data, but it is now spreading beyond the four walls of a hospital or physician's office. Wearables are growing in popularity, but not without concern. A PricewaterhouseCoopers report on wearables found that 86 percent of respondents were concerned this technology would make them more vulnerable to security breaches.

A Guardian’s Health Care Decision-Making Authority: Statutory Restrictions

1. State guardianship statutes generally grant guardians broad authority to make health care decisions for incapacitated persons and contain language similar to the Uniform Guardianship and Protective Proceedings Act (“UGPPA”), which states that a guardian may “consent to medical or other care, treatment, or service for the ward. However, the statutes limiting that authority vary broadly between states in the U.S. Local jurisdiction and regional laws and regulations should be consulted as far as guardianship is concerned for VC process , because healthcare VC is another medical record.

Data accuracy related to self-testing for medical conditions - example

1. Covid - There are questions about the general accuracy of available covid antibody tests, potential high rates of false positive and what kind of immunity antibodies might confer. Some in the medical community believe that without professional guidance, it could be easy for a non-expert to jump to the conclusion that they’re immune when they aren’t. If the tests are purely recreational, there’s probably not too much harm that can come from them. But if at-home tests results become the basis for re-entering the workforce or other consequential policy decisions, people might feel pressured to falsify their results. If there’s a lot that depends on the real accuracy of the result, then this has big problems.
2. In general , companies developing verifiable credentials for home-based medical tests need to be aware of these concerns on data integrity and accuracy and implement risk mitigations in the solutions to appropriately capture and communicate these concerns to the users of these VCs.
3. While developers of VC are not medical experts and this GIF is not meant to serve as a medical guidance, it is important to understand the risks in the process and appropriately capture and communicate them to the stakeholders to enable informed decision making.

Appendix G: Blinding Identity Taxonomy

The Kantara Initiative has made available an approach termed as the “Blinding Identity Taxonomy” (BIT) as “*a defensive tool created for the purpose of reducing the risk of identifying data subjects within blinded datasets*”. The purpose of this is to aid schema issuers and data controllers to flag attributes which may contain identifying information. The BIT achieves this by providing a list of elements which can be referred to by the schema issuers and data controllers.

A dataset may be said to be successfully ‘blinded’ when an adversary with access to the dataset cannot identify a significant number of data principles contained in the dataset. The v1.0 of the BIT is available from the Kantara Initiative[8]. This form of preserving privacy against re-identification mechanisms and processes can be useful when designing VC based systems which attempt to address the topics of coercion, disclosure and privacy in the domain of health information data specific to COVID-19 related test and test result status.

[8] https://docs.kantarainitiative.org/Blinding-Identity-Taxonomy-Report-Version-1.0.html

Resources & References

For further exploration of the concepts, technologies and philosophies which converge in the health-related credential ecosystem, please see links below:

Verifiable Credentials

- W3C Verifiable Credentials Data Model 1.0 Terminology
- Characteristics of Safe Credentials: https://www.evernym.com/blog/introducing-safe-credentials/
-

Identity

- Blinding Identity Taxonomy: An approach from the Kantara Initiative to aid schema issuers and data controllers to flag attributes which may contain identifying information.
- https://docs.kantarainitiative.org/Blinding-Identity-Taxonomy-Report-Version-1.0.html

Healthcare Data Security & Privacy

- 50 things to know about healthcare data security & privacy covering HIPAA, data breaches and Electronic Health Records: https://www.beckershospitalreview.com/healthcare-information-technology/50-things-to-know-about-healthcare-data-security-privacy.html
-

Trust

- Trust Assurance Model: Governance Principles to aid in raising the level of trust, assurance and credibility enabled within a system designed to be complying with the Technology Principles of a digital system design: https://wiki.trustoverip.org/display/HOME/GSWG+Trust+Assurance+Task+Force
- Levels of Assurance Framework: convenient and transparent system to understand and interpret the reliability of any information (“Claims”) that might be included in a CCI VC.
    - UK Government GPG45
    - NIST Special Publication 800-63-3 Digital Identity Guidelines
    - European electronic identity and trust services regulation (eIDAS).
-

Organisations & Standards

- Trust Over IP - Trust Over IP Foundation.
- Sovrin - The Sovrin Governance Framework Glossary
- National Institute of Standards and Technology, U.S. Department of Commerce
    - Digital Identity Guidelines - NIST SP 800-63-3

- Internet Engineering Task Force
    - RFC 2119 - Key words for use in RFCs to Indicate Requirement Levels - https://tools.ietf.org/html/rfc2119
- Hyperledger Aries
- International Standards Organisation
- German Institute for Standardization
- Spanish Data Protection Board

Sustainability in Technology

-

Data Ethics

- UK Department for Digital, Culture, Media & Sport - Data Ethics Framework https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/737137/Data_Ethics_Framework.pdf
-