COVID-19 Credentials Initiative ("CCI") Governance Framework V1

Master Document v01

01 JUNE 2020

This is an official document of the CCI Governance Framework (the "**CCI GF**") V1, as approved by the CCI Rules Workstream.

This document was produced by the CCI Governance Framework Working Group.

Acknowledgements—CCI Governance Framework Working Group: Drummond Reed (convenor), Kelly Cooper (co-chair), Chris Raczkowski (co-chair), Sankarshan Mukhopadhyay (co-geo-lead India), Keerthi Thomas (co-geo-lead EU), Eddie Kago (co-geo-lead Africa), Celia Yeung (co-geo-lead Asia Pacific). Contributors (alpha order): Dele Atanda, Jacques Bikoundou (Florida, USA), Thomas Cox, Rieks Joosten (TNO, Netherlands), Kaliya Identity Woman, Phillip Long, Steve Magennis, Markus Mummert, Orie Steele, Alex Tweeddale,

NOTE: *This document includes or references content of the Sovrin Governance Framework Master Document*[1].

[1] https://sovrin.org/library/sovrin-governance-framework/

1. About this document

Verifiable Credentials, in the form of digital files that follow W3C standards for *Verifiable Credentials*, (a "**VC**" or the "**VCs**") can be used by individuals and organizations to help societies manage and recover from the social and economic impacts of the COVID-19 pandemic. For example, VCs can be used to provide trusted confirmation of a person's COVID-19 test result status, which is easily verifiable back to the issuer of the COVID-19 test and associated VC. Guidance for how this can be achieved is described in this Master Document, as well as associated documents that are identified herein. The core purpose of the CCI Governance Framework (the "***CCI GF***") is to provide open source derived guidance for COVID-19 associated VCs that protects issuers, holders, and verifiers; reduces VC utilization friction; assures regulatory compliance; and shapes best practices for COVID-19 VC use cases.

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

2. Participants

Understanding the human dimensions of the ecosystem comes first. Not all use cases will be modeled; however, the following participants serve as examples: Individual, Government, NGO, Business, Healthcare Provider, Healthcare Worker, Licensor, Health Insurance Companies.

3. Purpose

The Purpose of the CCI Governance Framework (the "***CCI GF***") is to provide minimum governance standards that may be applied to any COVID-19 associated VC used by any individuals, communities, companies, organizations, and governments, anywhere in the world, to issue, hold, and verify a family of interoperable Verifiable Credentials (the "***CCI VCs***"). The CCI GF provides guidance, as contributed by a globally distributed open source committee of VC experts and supporters, for CCI VCs intended to protect issuers, holders, and verifiers; reduce VC utilization friction; assure regulatory compliance; and shape best practices for CCI VC use cases.

4. 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 the UK Government GPG45, NIST Special Publication 800-63-3 Digital Identity Guidelines, or 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. Mistakes and fraud for a Level 1 Claim are not controlled, and a Verifier 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.

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 potential accuracy of such VC Claims. For example, an unknown medical professional, with no verifiable professional license issued by an 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 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.

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.

5. General Principles

5.1. Openness and Interoperability

CCI shall use Open Standards and avoid mechanisms that restrict or prevent Identity Controllers from experiencing interoperability or portability of their Identity Data to other networks and systems.

5.2. Accountability

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.

5.3. Sustainability

VCs that intend to follow the CCI GF should 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.

5.4. Collective Best Interest

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.

5.5. Decentralization by Design

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.

5.6. High Availability

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.

5.7. No Single Point of Failure

The CCI GF credentials should have no single point of failure.

5.8. Maintain Consistent Experience

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

5.9. Censorship Resistant

The CCI GF adopts and implements tools, applications, and services toward credentials that do not discriminate individuals or groups based on race, ethnicity, religion, health, sex life or orientation, membership of organizations (e.g., trade union), or personal beliefs and political opinions.

A CCI GF adopted and implemented requires that a third party cannot modify or revoke credentials, shut-down, or deny access to a credential service without authorization.

5.10. Privacy Preserving

The CCI GF strongly resists any 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.

6. Design and Governance

6.1. General

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:

1. Proactive not Reactive; Preventative not Remedial
2. Privacy as the Default Setting
3. Privacy Embedded into Design
4. Full Functionality—Positive-Sum, not Zero-Sum
5. End-to-End Security—Full Lifecycle Protection
6. Visibility and Transparency—Keep it Open
7. Respect for User Privacy—Keep it User-Centric

6.2. 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.[2] 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).

6.3. 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[3].

[2] This specification is still a work-in-progress in the W3C DID Working Group.
[3] https://www.w3.org/TR/vc-data-model/

6.4. Governance Framework Disclosure by Default

CCI GF Entities, 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.

6.5. 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.

6.6. Anti-Correlation by Design and Default

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

6.7. Guardian 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.

7. Security by Design

7.1. General

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.

7.2. 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.

7.3. Auditability

Transactions in CCI VCs and actions of an application using CCI VCs that require auditing are immutably logged and available for verification processing.

8. Data Protection by Design and Default

8.1. General

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

8.2. 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.

8.3. 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. 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 requires review and approval by an ethical body, such as a Human Subjects or Institutional Review Board.

8.4. 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.

8.5. 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.

8.6. 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.

8.7. Integrity and Confidentiality

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.

9. 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 intentional 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:

1. Digital limitations (e.g., access to connected devices)
2. Physical or cognitive limitations (e.g., disability or incapacity)
3. Political & social status (e.g., stateless individuals; being a child, a woman, an Animal, Natural Thing, etc.)

4. Financial status (e.g., unbanked, unemployed, unemployable)
5. Literacy & language (e.g., low literacy or not speaking a language)

10. Ethical by Default and Design

Data ethics is a branch of applied ethics which describes the value judgements and approaches taken when obtaining, generating, analyzing and disseminating data. This requires a sound knowledge of data protection law and other relevant legislation; the appropriate use of new technologies; and a holistic approach incorporating good practice in computing techniques, ethics and information assurance.

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 organizations.

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. 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::

- 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 that their data be made available to others within a clearly defined set of use restrictions,
- 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,
- Ensure that shared PPOI is treated confidentially by any recipient;
- 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;
- 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;
- Ensure that data activities are respectful of, and do not interfere with, human will/self-determination;
- 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;
- Set out definitions for data privacy, agency and ownership with a specific 'ethical' context;
- Recognize that there may be attributable value to PPOI of other data;
- Adopt principles for allowing transfer of data between data processors and providers at an individual's request, ensuring rights to data portability;
- Adopt principles for an open consent process for the use of PPOI or other data;
- Adopt principles for notification of changes to personal data and change of use of personal data;

- Adopt principles for correcting data;
- Adopt principles for erasure of data and ensure fair rights to be forgotten;
- 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. The CCI GF requires that appropriate techniques be proactively applied to promote ethical data use principles by default.

Resources and Glossary

Definitions

Document Name	Description	Governed By	Normative Location
CCI GF Glossary	Definitions of key terms used in the CCI GF	CCI Governance Framework Working Group	Appendix A of the CCI GF Master Document

Specifications

Document Name	Description	Governed By	Normative Location
CCI Credential Specifications	Credential specifications, and Credential Issuer Policies	CCI Governance Framework Working Group	
Verifiable Credentials Data Model 1.0	Specification for verifiable credentials	W3C Verifiable Claims Working Group	https://w3c.github.io/vc-data-model/

Policies

Document Name	Governs	Governed By	Normative Location
CCI Credential, and Credential Issuer Policies			https://docs.google.com/document/d/1xFyDuoFWt6xD8j5f-3cwcsnhAbOWxUgnUisljb1Sj6Y/edit?usp=sharing

Appendix A: 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 is comprised of a set of Claims.

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.