On Guardianship in Self-Sovereign Identity

Sovrin Guardianship Task Force
November 2019

sovrin
identity for all

sovrin
identity for all

Executive Summary

As a new model for Internet-scale digital identity, self-sovereign identity (SSI) moves beyond centralized “identity providers” by establishing an infrastructure that enables anyone to issue, hold, and verify digital credentials signed with cryptographic private keys. As powerful as this is, it limits the direct use of SSI to individuals who have digital access and the legal capacity to use the technology. For SSI to work for everyone, individuals who do not have digital access, or the appropriate capacity for access, will need another person or organization to serve as their digital guardian.

This whitepaper is for policy and decision-makers, designers, lawyers, software developers, identity professionals and others who want to learn how guardianship is handled in SSI. It examines why digital guardianship is a core principle for Sovrin and other SSI architectures, and how it works from inception to termination through looking at real-world use cases and the stories of two fictional dependents, Mya and Jamie.

The paper explores guardianship as a core principle of SSI and explains the concept through real-world situations; and, after introducing key terms, the paper goes on to posit why SSI needs Guardianship before detailing what the Guardianship relationship is. The paper then explores the contextual nature of guardianship, and looks at the life cycle and design of SSI Guardianship which reflects the complexities of the human condition.

The paper devotes a full section to highlighting the critical risks of guardianship such as impersonation and the commingling of identity data. Ignoring these risks when implementing a Guardianship solution may wipe out any SSI benefits and result in serious adverse effects for dependents.

Finally, the paper includes high-level technical overview on how Guardianship fits the Trust over IP stack. Practical guidance is left for future work to be carried out by the Sovrin Foundation’s new Guardianship Working Group.

Table of Contents

Introduction

Over the last decade, digital identity has enabled the digital transformation of almost every aspect of our lives. New technical advances such as IoT, 5G, and AI promise more digitization for our data-driven futures. New identity and access management technologies (IAM), such as multi-factor authentication, biometrics, and federation protocols have started to improve interoperability and simplify "login" for us all. At the same time, governments, social platforms, credit reference agencies, and enterprise vendors have collaborated to build new online identity verification ecosystems. Their motivation is simple: more trust = less risk = more money.

There is a risk that the more some of us benefit from digital transactions and our digital identities, the more we increase digital exclusion. Identity systems need a means of connecting with and representing those who cannot act for themselves (or wholly by themselves) in the digital world to mitigate exclusion. Today, we use workarounds to solve this problem:

You cannot log in to your computer to approve expenses, so you phone someone else and ask them to log in for you.

Your elderly neighbor now needs to book their doctor's appointments online, so you sit alongside them and fill in all the forms for them or coach them through the process.

A homeless charity creates and manages digital identities for its clients so that it can claim benefits from the state on their behalf.

These workaround examples use offline paper credentials and human face-to-face verification; however, they are not secure, transparent, or auditable, and there are limits to the value of the transactions they can support.

Self-sovereign identity (SSI) systems, where control of a digital identity is asserted using digital credentials stored in a digital wallet, present a further challenge. How can we enable everyone to control their digital identity? By definition, we experience life-stages (e.g., childhood) and conditions (e.g., dementia) where law and social norms dictate we cannot be self-sovereign. This challenge cannot be solved with simple delegation because a child, a person living with dementia, or a refugee without an internet connection cannot delegate something they do not have. Nor is it a simple controller relationship with a thing (e.g., a drone) because unlike a drone, a child progressively gains rights and eventually becomes more self-sovereign. Similarly, the person living with dementia will experience changing capacity over time.

What we need is a mechanism for people who cannot directly access or manage their own digital identity. The mechanism needs to:

- Technically work alongside existing identity and credential management systems.
- Functionally support legal, social, and organizational processes that include those who cannot digitally transact for themselves.
- Support revocation so that each person can reclaim their self-sovereign identity as and when they are able.

Guardianship is this mechanism. Guardianship has always been an essential component of the Sovrin Governance Framework. Without a guardianship mechanism, how will we account for times in our lives when we cannot be fully self-sovereign?

This paper, published by the Guardianship Task Force of the Sovrin Governance Framework Working Group, explores the guardianship relationship and how it fits in with the overall SSI "web of trust." We present the risks and benefits and propose potential approaches to implementation. We hope that the paper serves as a starting point for further work and discussion, beginning with the Sovrin Guardianship Working Group. The paper is accompanied by short, rough-cut demo videos to aid understanding.

Key Terms

This paper considers Guardianship within the context of self-sovereign identity (SSI) and specifically within the context of the Sovrin Governance Framework (SGF), as defined by the Sovrin Foundation. Many terms in this document are defined formally in the Sovrin Glossary, which is part of the SGF. Digital identity is a challenging concept, and SSI is even more so. The Sovrin Governance Framework Working Group finds it essential to provide clear definitions of digital entities and digital relationships defined in the SGF. For this reason, we include Table 1 defining the essential terms for understanding Guardianship.

Definition	Definition
Delegate *(an entity)*	One who receives authority and responsibility to carry out limited tasks on behalf of another. Delegates may represent an independent entity ("self-sovereign") rather than being dependent on another entity; they tend to be more task-oriented than guardians. The power of a Delegate may be limited in scope. *Sovrin Glossary: "An Identity Owner that acts on behalf of another Identity Owner. Formally, a Delegate is the Holder of a Delegation Credential."*

Dependent *(an entity)*	The protected, guarded, or defended person; also *ward*. *Sovrin Glossary: "*An Individual whose circumstances or capabilities, in a given context, requires dependence on a Guardian to administer the Individual's Identity Data. Under the Sovrin Governance Framework, all Dependents have the right (though perhaps not the circumstances or capabilities) to become Independents. Mutually exclusive with Independent."
Guardian (an entity)	An organization or person protecting another person and possibly their property. *Sovrin Glossary:* "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 dependent on the Guardian to manage the Identity Owner's Wallet."
Guardianship *(a relationship)*	The status of being a protector, advocate, or proxy for a person. See *Appendix C of the Sovrin Glossary:* 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 a parent, *in loco parentis*, legal capacity, and power of attorney. Note that Guardianship is not Impersonation or Delegation. While the term Guardianship applies strictly to natural persons (Individuals) as Dependents, in a more general sense, the term can apply to Natural Things (such as pets or animals). Guardianship is one of three types of identity control relationships.
Self-Sovereign Identity (SSI)	An Internet-scale digital identity model based on decentralized identifiers, decentralized digital credentials, and decentralized digital wallets. Sovrin Glossary: "An identity system architecture based on the core principle that Identity Owners have the right to permanently control one or more Identifiers together with the usage of the associated Identity Data. The Sovrin Governance Framework specifies two types of Identity Owners: Independents, who do not need to rely on any external administrative authority; and Dependents, who need to rely on a Guardian." Also see *Sovrin FAQs*
Thing Controller *(an entity)*	One who controls something that is by its nature incapable of self-sovereignty. Examples include a pet owner or a drone operator. Sovrin Glossary: "A Controller that controls the Sovrin Identity Data, including the Private Keys, for a Thing. Every Thing must have a Thing Controller. The Thing Controller may or may not be the legal owner of the Thing; however, the Thing Controller may be legally responsible for actions Agent(s) take on behalf of the Thing."

Table 1: Essential terms for understanding digital guardianship

Audience

This document is for policy and decision-makers, designers, lawyers, software developers, and others who want to learn how guardianship is handled in SSI. It explores the general relationship between guardianship and SSI systems—why it is needed, how it should be modeled, and its risks and benefits. While we include some details specific to Sovrin's infrastructure, the discussion is relevant for any SSI system. It is, however, important to note that we are not setting explicit requirements for guardianship in the context of SSI. We recognize that the range of guardianship applications is vast; therefore, different norms and standards will be needed for different circumstances. This document provides guidance for establishing guardianship practices that endeavor to meet fundamental SSI principles as articulated in the Sovrin Core Principles.

Additional Resources:

https://sovrin.org/faq/what-is-self-sovereign-identity/

https://www.windley.com/archives/2018/09/multi-source_and_self-sovereign_identity.shtml

EXAMPLE USE CASES

To sharpen our focus, we frame the issue around two fictional people needing guardianship to have trustworthy digital identities so they can access vital services.

Jamie

Jamie was diagnosed with Alzheimer's dementia at the age of 60. In the first two years after diagnosis, his periods of confusion and mental capacity fluctuated. His wife, Ann, has a limited power of attorney to make decisions regarding his healthcare when he is deemed not to have the capacity to make a medical decision.

See Jamie's story

Maya

Mya is 5 or 6 years old; she is not sure which. She is alone in a refugee camp in Bangladesh near the Myanmar border. Her parents are either lost or dead. She has an unofficial foster family who "adopted" her because they recognised her from their home village. Mya arrived in the camp three weeks ago, and none of her extended family are there. She is malnourished.[1]

See Mya's story.

Exploring the stories of Jamie and Mya will help us evaluate the relevance of SSI solutions to real-world problems in healthcare, social work, humanitarian aid, finance, law, government, and the Internet of Things (IoT).

[1] The Sovrin Governance Framework Working Group developed these personas. They are deliberately different and challenging. Their potential solutions accommodate the broadest possible set of circumstances.

Why SSI Needs Guardianship

THE CHALLENGE OF INCLUSIVITY

Jamie and Mya are not alone in being unable to control their digital lives. There are 3.3 billion[2] people who cannot access the internet, including 70 million refugees, 50 million adults with dementia[3], and 1.9 billion children[4].

SSI, with its trusted peer-to-peer communication and verifiable digital credentials, opens exciting opportunities to rethink processes, re-calibrate digital relationships, and re-imagine how we interact in an information society. It empowers identity owners[5] and gives complete control over their digital identity and related private data.

How can we give people who are excluded from managing their own identities online access to SSI?

The Sovrin Governance Framework seeks to accommodate real-world constraints without compromising SSI core principles by defining three types of indirect identity control to model reality's complications: **guardianship, delegation, and controllership.** This document details the most delicate of the three—guardianship.

THE PRINCIPLE OF GUARDIANSHIP AS A RIGHT

In the Sovrin Governance Framework, the principle of guardianship immediately follows the principle of self-sovereignty. This order is intentional: guardianship covers situations where we are unable to be self-sovereign—the most challenging gap in the SSI identity model. The exact text of the Guardianship principle is:

---

[2] https://datareportal.com/reports/digital-2019-global-digital-overview

[3] https://www.who.int/news-room/fact-sheets/detail/dementia

[4] https://www.gapminder.org/news/world-peak-number-of-children-is-now/

[5] The term "identity owner" was adopted in the first version of the Sovrin Glossary in 2017. In the intervening period, the concept of data "ownership" of any kind (including identity data) has grown much more controversial. As suggested by Joe Andrieu, co-chair of the W3C Credentials Community Group, the Sovrin Governance Framework Working Group intends to deprecate this term and replace it with a new one in the next version of the Sovrin Glossary. For more about this topic, please see Joe's paper, Functional Identity.

> *Guardianship: An Individual who does not have the capability to directly control that Individual's Identity Data (a Dependent) shall have the right to appoint another Identity Owner who has that capability (an Independent or an Organization) to serve as the owner's Guardian. If a Dependent does not have the capability to appoint a Guardian directly, the Dependent shall still have the right to have a Guardian appointed to act on the Dependent's behalf. A Dependent has the right to become an Independent by claiming full control of the Dependent's Identity Data. A Guardian is obligated to promptly assist in this process, providing the Dependent can demonstrate that the Dependent has the necessary capabilities. Guardianship shall not be confused with Delegation or Impersonation. Guardianship under the Sovrin Governance Framework should map in the proper contexts to various legal constructs, including legal guardianship, power of attorney, conservatorship, living trusts, and so on.*

As the text notes, guardianship relies on formally vetted legal constructs and encompasses situations with little or no legal foundation where social norms or organizational rules underpin roles. It captures the actual transfer of control of private data and keys from an individual (the dependent) to a guardian (an independent identity owner). This control shifts accountability and must be precisely crafted. If too coarse or too rigid, it will not apply to real use cases; if too vague or imprecise, it will degrade and tarnish the promise of SSI by opening backdoors to misuse, abuse, and the centralization of private data.

Within SSI constructs, guardianship should:

- Enable and protect self-sovereignty for those who cannot act for themselves.
- Protect the privacy and security of both parties to the guardianship relationship—dependent and guardian.Offer practical and broadly applicable answers governed by a protective framework.
- Extend existing, non-digital guardianship constructs, both formal and informal, into the digital world to foster digital inclusion.

In short, carefully constructed guardianship is essential to SSI. Without it, SSI solutions will either tend towards centralisation or exclude billions of people.

The Guardianship Relationship

Guardianship is relevant to everyone. It manifests in some of our most important and familiar relationships, including raising a child, caring for a parent, and helping an elderly neighbor. Many guardianships are informal; many are not. Formal ones may be founded on legal constructs such as assignments of guardianship or an adoption certificate. Formally or informally, guardianship helps or protects a dependent person.

In SSI, guardianship involves controlling all or parts of the dependent's digital wallet, including sharing proofs of the dependent's digital credentials with verifiers when required. The contexts in which sharing is required and the controls put in place to avoid abuse (e.g., the guardian impersonating the dependent for the guardian's purposes) must be clearly defined. Although the rules, context, and formality will vary, the same underlying SSI mechanisms of authentication, authorization, and credential exchange support all guardianship solutions. Human and cryptographic trust layers must combine to mitigate the internal risks attached to guardianship.

WHEN IS GUARDIANSHIP NEEDED?

Guardianship provides access to SSI benefits to people unable to manage their own SSI digital wallets. This access means transferring partial or complete control of the dependent's wallet to the guardian. Technically speaking, this means the guardian will have control of the set of cryptographic private keys in the dependent's wallet. Here we consider two scenarios where guardianship is required: 1) no online access, and 2) legally enforced loss or restriction of control.

No online access. First, guardianship allows people that do not have online access themselves to act online via the guardian acting as their proxy. For example, in Mya's case, a humanitarian Non-Governmental Organization (NGO) serves as her guardian. When digital actions are needed on Mya's behalf, such as obtaining a digital certificate of refugee status or sharing a digital credential to prove Mya's eligibility for food aid, an employee of the NGO (technically, a delegate) performs these digital actions for her. The NGO can continue to provide this service until the dependent (Mya) acquires the capacity and capability to take control of her digital wallet. Many humanitarian sector use cases require this type of digital identity mechanism where dependents do not have a smartphone or Internet access or the skills to use them. Because the guardian essentially controls all or some of the dependent's digital life, the governance framework for setting up and managing a guardianship relationship is critically important.

Legally enforced loss or restriction of control. In the second case, guardianship allows for the inclusion of persons whose legal rights to act on their own identity are restricted. A common example is a parent acting on his or her child's behalf when the child is below the age of majority. This form of guardianship is also needed when a person assigns it voluntarily using a legal instrument such as a power of attorney or has it assigned to them by a legal authority. All jurisdictions have legal constructs that map to SSI guardianship even if the specific term used is not "guardian." These typically cover health and welfare (medical guardianship) or financial affairs and property (fiduciary and trustee relationships). Most define specific legal responsibilities of the guardian, such as acting in the dependent's best interests and no commingling of funds. By enabling these relationships and actions to be performed digitally, SSI guardianship can both simplify and increase the value of these real-world legal instruments—a variety of which are shown in Figure 1 below.[6]

6 Based on analysis of a sample of jurisdictions available at https://www.international-guardianship.com/guardianship.htm

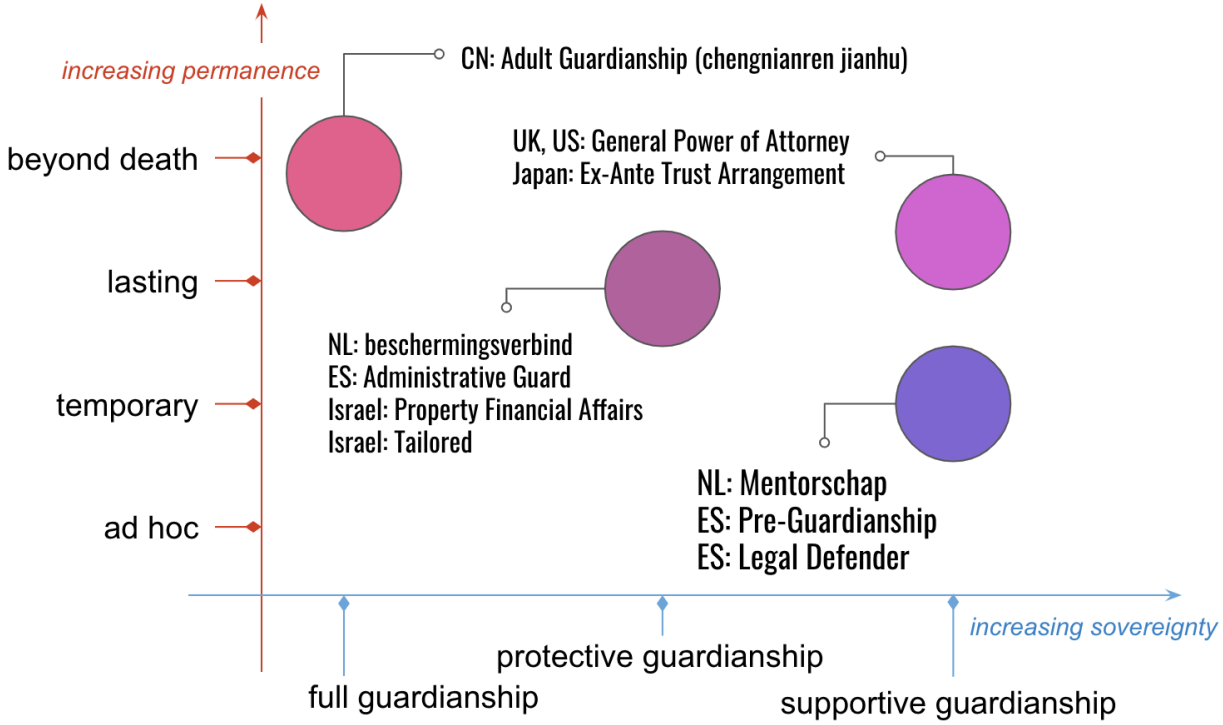


Figure 1: Legal constructs relating to guardianship

GUARDIANSHIP MANDATES

A guardian cannot act in isolation—it must always have a mandate. That mandate can originate from three sources:

1. Legal Construct. Guardianship may be based on a legal construct such as the U.K. Power of Attorney that Jamie gave his wife, Ann. This legal construct usually takes the form of a document, regulation, or court order.

2. Social Norm. Many forms of guardianship are based on a social norm with nothing but custom or circumstance to back it up. An example is the aid worker who found Mya at the border and brought her to the camp.

3. Organizational Governance. This type of mandate is encoded in an industry code of practice, regulation, or domain-specific governance framework.

Table 2 gives examples of different mandates.

Source of Mandate	Type of Mandate	
	Formal	**Informal**
Legal Construct	Ann's Power of Attorney	In loco parents for someone else's child who is having a 'sleepover'
Social Norm	Zo's role as Mya's mother	Jamie's next door neighbor takes Jamie to hospital after a fall
Organized Governance	The NGO at the refugee camp becomes Mya's guardian	Mya is left in the care of the foster family initially

Table 2: Examples of different types of guardianship mandates

In all cases, credentials issued to both guardians and dependents must have specific fine-grained permissions under governance frameworks that include checks and balances necessary to maximize accountability for guardians and self-sovereignty for dependents.

TRADITIONAL APPROACHES

The need for guardianship is present in an extensive range of use cases, legal constructs, and sectors. Most of these concern health and welfare or property and money. It is useful to view all on two key dimensions:

The Temporal Dimension: These range from **ad hoc** (for example, Ann loses her phone and asks their son to act as Jamie's guardian), to forms of guardianship that extend **beyond death** in some jurisdictions. The expected duration of the relationship drives key technical and governance considerations.

The Self-Sovereign Dimension: All forms of guardianship can be categorized on a scale from no self-sovereignty for the dependent and maximum rights and responsibilities for the guardian, to almost complete self-sovereignty for the dependent and minimum rights and responsibilities for the guardian. However, it is useful to consider three main groups:

1. Full Guardianship, where the dependent cannot transact on their own.
2. Protective Guardianship, where the dependent needs to transact together with a guardian.
3. Supportive Guardianship, where the dependent can transact alone but chooses to transact with a guardian.

The two-dimensional canvas in Figure 2 helps to visualize these dimensions:

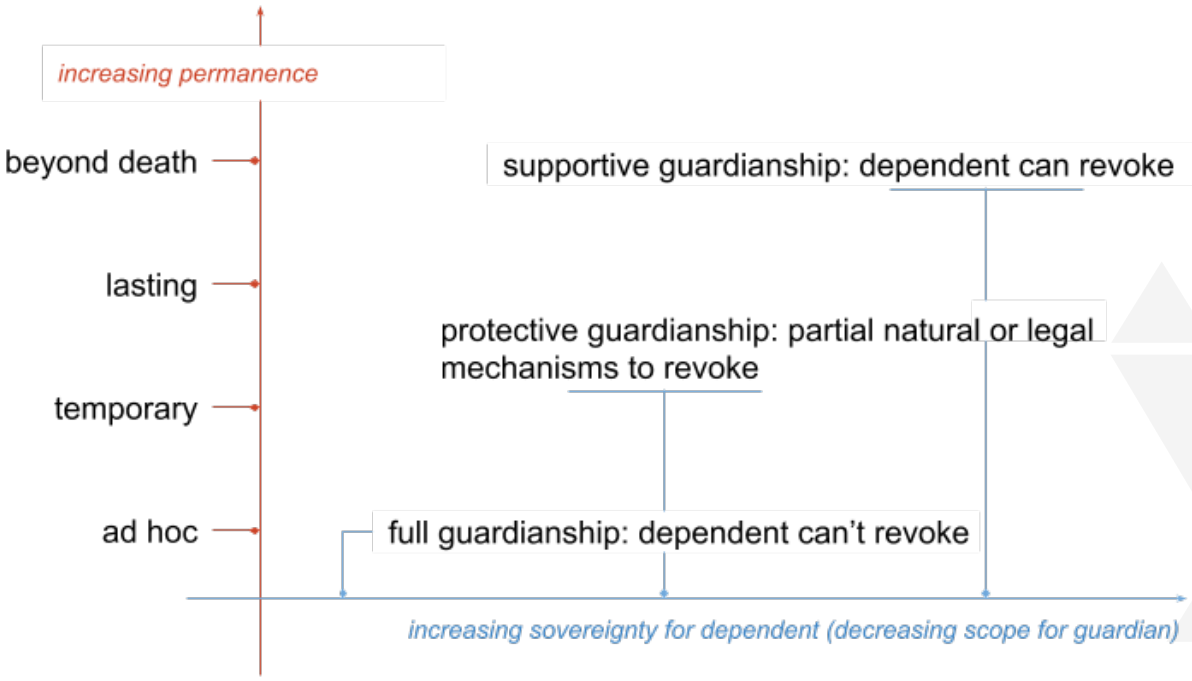


Figure 2: Temporal vs. self-sovereign dimensions of guardianship

Regardless of legal jurisdiction—and variations on these concepts—guardianship maps to these two dimensions. SSI guardianship architecture needs to provide the building blocks to satisfy the requirements of both dimensions. Digital guardianship never intends to fully replace non-digital legal constructs or judiciary enforcement of guardianship.

Even when there is a clear legal construct in place, there are many real-life cases that do not have clear-cut yes or no answers. A common example is divorcing parents who disagree on whom should have child custody. In Mya's case, relatives might compete for her guardianship. In Jamie's case, due to the nature of his condition, there may be good days when he requires some protective guardianship from Ann. In contrast, on bad days, he requires full guardianship.

In these cases, there needs to be some mechanism for evaluating competing claims. This area can be partially addressed via the careful design of guardianship credentials and guardianship governance frameworks. Audit and appeal functions should be embedded in service design. Human relationships are inherently complicated, and circumstances change. Particularly where there is a disconnect between the online and offline worlds.

TRANSPARENT VS. OPAQUE GUARDIANSHIP

The existence of a guardian and the nature of the guardian-dependent relationship must be regarded as a set of self-sovereign identity claims that are only shared with verifiers if required. In some cases, privacy or non-discrimination laws may require the role of the guardian to be opaque to ensure dependent privacy. The Core Principles of the Sovrin Governance Framework, Privacy by Design include:

> *2.10.7 Guardian and Delegate Confidentiality. The use of a Guardian or Delegate may be confidential information and shall only be disclosed with the authorization of the Identity Owner and of the Guardian and/or Delegate.*

However, there are situations where the law requires disclosure of a guardianship relationship, or a verifier's policies require knowledge of the guardianship relationship. There may be a need to verify the identity of the guardian (e.g., when guardianship is legally or organizationally mandated).

These two options for guardianship disclosure are shown in Figure 3:

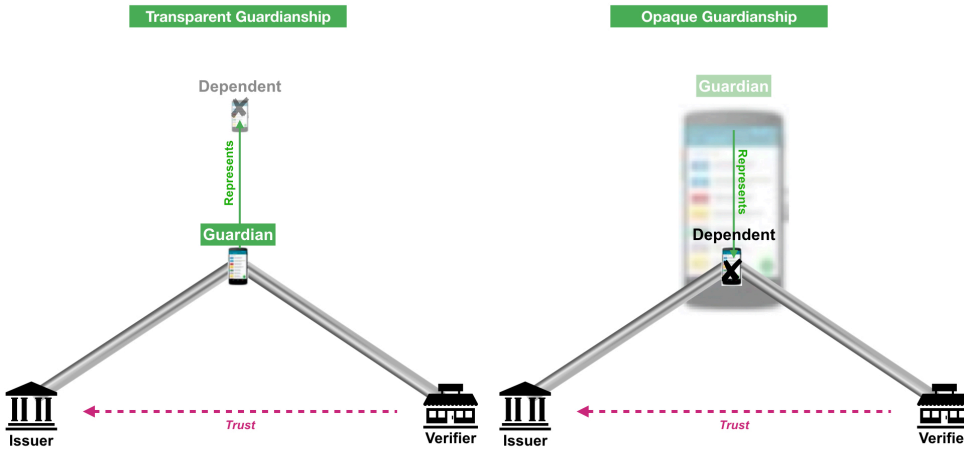


Figure 3: Transparent vs. opaque guardianship

In transparent guardianship, the guardian is a party to a transaction alongside the dependent. For example, when Mya is enrolling at school, the verifier usually confirms the identity of the guardian. If not legally required, social norms dictate a child of Mya's age has an adult taking care of them. As

such, the adult/child guardianship relationship is usually transparent. Transparent guardianship is easy to audit and is less private for both dependent and guardian.

When a guardianship relationship is opaque, verifiers are unaware they are interacting with a guardian. Opaque guardianship has the advantage of enhanced privacy for both dependent and guardian and reduced potential for discrimination or additional friction. However, opaque guardianship is riskier for dependents and verifiers due to limited auditing capacities. This risk effectively informs today's issues for all people who share their usernames and passwords for others to carry out digital transactions on their behalf. Ann may act for Jamie in this way when, for example, she orders his medicines online.

Other examples where opacity may be required for law, dignity, or privacy purposes include:

- Financial guardianship for a gambling addict.
- Mental health guardianship, where revealing the fact of guardianship may lead to discrimination (e.g., renting a property or applying for a job) or a breach of privacy as it reveals that they lack capacity.

Guardianship is Contextual

With all exchanges of identity data, the required credentials and claims depend on context. These requirements include factors such as:

- Why—the purpose of the interaction
- When—the time of the interaction
- Where—the location of the interaction
- How—the means for the interaction (online, offline, voice)
- What—the type of data to be exchanged

The most challenging element]to represent technically is the social context:the relationships between the parties(social, commercial, or legal) and the level of trust between them.

DIFFERENCES IN RELATIONSHIPS AND TRANSACTIONS

The relationship between a guardian and a dependent demands a special kind of trust. As with all relationships, trust develops and changes over time. Consider Jamie, who, as he reaches an advanced age, chooses to entrust decisions about his health and social care to his wife, Ann. Or Mya, who acquires a foster family and, later on, protectors among camp staff. Each of Mya's guardians (or guardian delegates) have different sets of permissions in their relationship with Mya. Transactions like leaving the camp may require the permission of more than one guardian. Some guardian permissions can be delegated (such as signing up at school); others cannot (such as agreeing to vaccines). Mya may not need a guardian for some things, such as eating in the food tent.

DIFFERENCES OVER TIME

When Mya first arrives at the refugee camp, she is entirely dependent on her SSI guardian delegates; they control all of Mya's digital wallet. As she grows, receives education, and gains independence both as a person and digitally, Mya's reliance on her guardian delegates diminishes. This growing independence differs from Jamie's dementia example. Transitioning from a digitally independent person with no need for digital guardianship, transfer of the capabilities of Jamie's SSI digital wallet to a guardian parallels the waning of his capacity and capabilities. Jamie may need more than one guardian—perhaps a neighbour or a friend to watch over him when Ann is away—and he may choose to give different permissions to each.

DIFFERENCES IN ONLINE AND OFFLINE CONTEXTS

Many examples in this paper involve emotional relationships and high-risk transactions that exist completely offline today: Where guardianship is exercised face-to-face at a refugee camp, a war zone checkpoint, a doctor's office, or in a court of law. Designing online guardianship should, therefore, always support existing offline processes. Ideally, online guardianship should share a common governance framework so that guardianship actions take place in either an online or offline context, whichever is more manageable.

DIFFERENCES IN PERMISSIONS

Different contexts demand different permissions for guardians. In traditional identity architectures, this type of complexity can be complicated to model—it requires fine-grained authorisation, risk-based authentication, and a mechanism for dynamic role assignation. In SSI architecture, guardianship credentials, delegation credentials, and dependent credentials can be neatly managed across layers of the SSI stack and implemented across one or more digital wallets.

Permissions can tie directly to specific contextual factors to set limits on guardianship and provide an essential safeguard for dependents. Such limits can include:

1. Time and history (for what period(s) a guardian has that status)

2. Place (in what physical or virtual locations guardianship is valid)

3. Function (e.g., legal vs. medical vs. educational vs. travel)

4. Circumstances (for particular events)

5. Biometrics (for authorization by the dependent or others)

6. Relationships (whom the guardian can connect to)

7. Attributes (data/credentials—what the guardian can prove)

8. Agents (what software/devices the guardian can use)

9. Cooperation (with joint approval)

10.Oversight (audit trail, reporting)

Guardianship and Other Types of Digital Control Relationships

We covered how guardianship relationships can be complicated, dynamic, and often full of blurry lines. What guardianship is and what it is not can be understood by addressing two additional types of indirect identity control relationships. The Sovrin Glossary defines the roles of delegate, guardian, and thing controller. The essential differences among these three are captured in Figure 4 taken from Appendix C of the Sovrin Glossary:

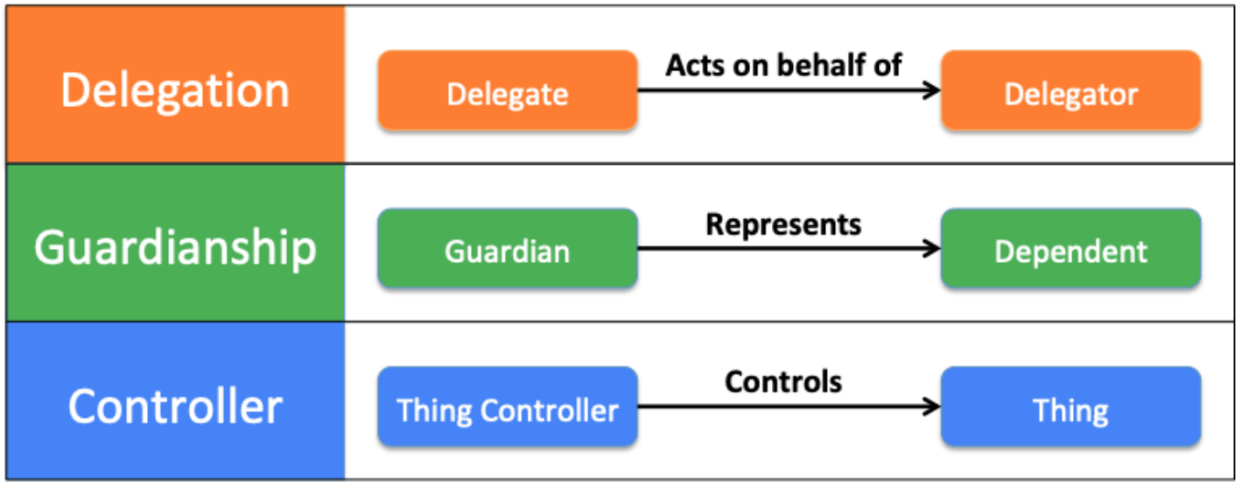


Figure 4: The three types of indirect identity control relationships

DELEGATE

The key difference between delegation and guardianship is that **delegator and delegate act with full self-sovereignty**, i.e., both have full control of their digital wallets and private keys. The delegator is merely delegating some specific set of responsibilities to the delegate by issuing a **delegation credential**. For example, the NGO responsible as Mya's guardian can issue delegation credentials to its staff members to perform specific guardian delegate functions, such as signing Mya up for school or permitting her to leave the refugee camp with the proper supervision.

THING CONTROLLER

Controllership is the Sovrin Glossary term that applies when an SSI identity owner needs to exert control over a **Thing.** A Thing is a physical or digital object with an SSI identity that is not legally capable of taking independent action. Cars, refrigerators, computing devices, and drones are examples of Things that can directly contain or indirectly be represented by an SSI digital wallet. Controllership differs from delegation because **Things cannot be self-sovereign**—so there **must** be another independent entity that ultimately controls the Thing's digital wallet. That entity is called the **controller.**

If a Thing is capable of having a digital wallet, such as a smart medical device like a digital heart monitor, the controller can issue it a **controller credential.** For example, Ann can issue a controller credential to Jamie's digital heart monitor that enables him to view reports and receive alarms without a change in its settings. Ann can issue a different controller credential to Jamie's cardiologist that authorizes permission to change the monitor settings without any other controller credential.

INTERWORKING OF CONTROL RELATIONSHIPS

Delegation is one of the most common and useful functions that can be implemented using SSI digital credentials. It is at the very heart of how most organizations perform their various workflows. As such, many guardianship relationships will also involve delegation relationships. As with delegation, guardians and their dependents will often require controller credentials in order to perform digital guardianship responsibilities.

Delegation, guardianship and controller relationships will often work in webs of trust For example, Jamie delegates his controller credential for his biometric shoe on a 'bad day'. Ann might delegate along with her guardianship credentials to a respite care-worker.

The Guardianship Life Cycle

From an implementation perspective, Guardianship is the definition of a specific set of digital credentials for both guardian and dependent. The guardianship lifecycle is similar to standard credential lifecycle management; however, these credentials describe a **relationship** rather than a specific individual.

The complexity comes from the full range of possible applications for guardianship—all of which must mitigate the critical risks of guardianship (see the following section). To understand these credentials and the risks they must minimize, we will describe the lifecycle of a guardianship relationship from its inception to its termination. This approach represents a comprehensive user experience view from which we can derive:

1. Technical requirements for the cryptographic trust layers of SSI infrastructure (see the final section of the paper).

2. Governance and business process mapping for the human trust layers.

Figure 5 illustrates the four major stages in the Guardianship lifecycle.

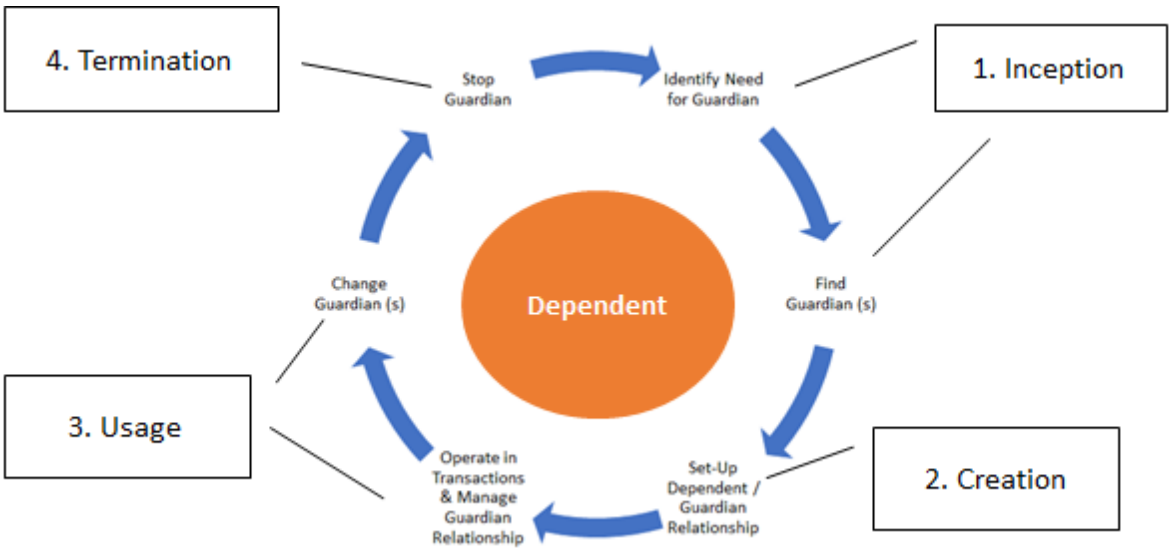


Figure 5: The four major stages in the guardianship lifecycle

STAGE 1: INCEPTION

The first stage is to identify the need for a guardian and assess if the need is legitimate. Setting up a *curatele*[7] type of Guardianship, can be a lengthy process. By contrast, in a humanitarian emergency case like Mya's, guardianship must be done on the fly. This stage ends with validation by a trusted entity that a Guardianship relationship must be created—ideally with the informed consent of the dependent. In nearly all cases, this will rely heavily on offline business processes.

Figure 6 depicts this process underway when a mother enrolls her baby for digital guardianship enabled by iRespond.org, an NGO offering a Sovrin-compatible privacy-respecting biometric ID system used in the refugee camps of SE Asia.

Figure 6: A mother and her baby enroll in iRespond's biometric identity system

STAGE 2: CREATION

The second stage is creating the actual guardianship relationship by creating the digital wallet the guardian will use for the dependent and issuing the necessary guardian, dependent, and delegation credentials. As described above, from a technical perspective, these are standard SSI credentials that conform to the W3C specification for verifiable credentials.[8] What makes these credentials unique is that they use schemas specially designed for defining the legal and contextual basis and constraints

[7] https://en.wiktionary.org/wiki/curatele Means (*law*) legal and financial guardianship under which the ward is an adult.

[8] Â https://www.w3.org/TR/verifiable-claims-data-model/

for guardianship. These schemas are typically defined in a corresponding governance framework for guardianship.

In some cases, this will involve the creation of new schemas and governance frameworks which should appropriately describe:

- The rights and responsibilities of the guardian.
- What identity data (credentials and claims) the guardian controls.
- The limitations on guardianship permissions (see the Guardianship is Contextual section above).

This stage ends with a guardian ready to perform digital transactions on behalf of the dependent.

STAGE 3: USAGE

This stage covers the real-life usage of the digital wallet and credentials the guardian holds on behalf of the dependent. It also includes the maintenance of the guardianship relationship during its operational lifetime (e.g., change of context, new guardians). Those changes will be reflected in the revocation of previously issued guardianship, dependent, and delegation credentials and issuance of new ones.

This stage is open-ended: it lasts as long as guardianship is required. It ends when a termination event is triggered.

STAGE 4: TERMINATION

Like all human relationships, guardianship has a lifetime. The Sovrin Governance Framework Guardianship principle states: Guardians must respect the fundamental right of a dependent to reclaim self-sovereign identity if changes in the dependent's circumstances enable it.

For these reasons, termination is treated as a specific stage in the guardianship lifecycle. The revocation of guardianship credentials may be governed by many factors—whether defined in law, social practice, or a guardianship governance framework. Examples include:

- A formal reassessment of the capacity and the capability of the dependent to control their digital identity (e.g., the case of Jamie).
- A law or legal action (e.g. a child reaches the age of majority; a power-of-attorney is revoked).
- A change of jurisdiction for the dependent.
- The death of the dependent or the guardian.

Note that the death of the dependent may trigger the issuance of additional credentials such as a digital death certificate. These credentials can digitally support those surviving the deceased and assist in managing their affairs—for example, in executing a will or carrying out probate.

This stage ends with the revocation of all guardianship credentials for a given dependent. If termination results in the dependent taking control of their digital wallet, this "cryptographic change-of-control" is accomplished using a specific protocol at the cryptographic layers of SSI infrastructure (see the final section). The result is that the dependent has control of their digital wallet and private keys. And the guardian (and its delegates) no longer have the cryptographic capacity to act on the dependent's behalf.

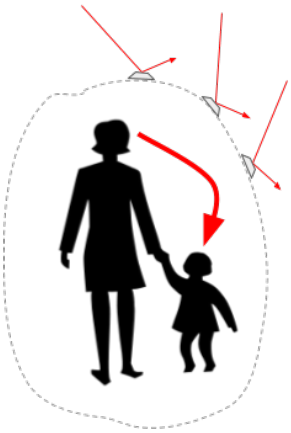
As noted in the guardianship lifecycle analysis, managing guardianship is not a trivial task for the guardian. Whether guardianship is held by one or more individuals (such as Ann acting for Jamie) or an organization (such as an NGO acting for Mya), guardians must manage the dependent's digital wallet and their digital wallet. This wallet management is a demanding user experience challenge, particularly when guardianship is not absolute. For example, when a dependent has their digital wallet and can take some self-sovereign identity actions but not those reserved for the guardian.

Risks of Guardianship

At the start of the paper, we discussed why guardianship is essential for SSI to be inclusive. However, guardianship is not without its risks. Dependents are, by definition, vulnerable people. In this section, we discuss the specific risks of guardianship and how they may be mitigated.

Note that section 3.2 of the Master Document of the Sovrin Governance Framework includes the following overall policies for Guardianship. A Guardian should:

1. Act in the Dependent person's best interest.
2. Exercise good judgment and carefully manage responsibilities.
3. Avoid commingling—keep Dependent's property separate (e.g., separate DIDs, Public Keys, Wallets, Vaults).
4. Keep detailed records of all actions taken on behalf of the Dependent.
5. Not violate the Anti-Impersonation principle (section 2.11.5).
6. Be subject to applicable legal structures regarding the granting and revocation of Guardianships.



INHERENT RISKS

Self-Sovereign Identity is all about returning control of digital identity to the identity owner—in this context, an individual. Ironically, guardianship does precisely the opposite. Guardianship intentionally gives partial or complete control to another party—the guardian (and its delegates)—because the dependent is not able to exert such control himself/herself.

This type of risk is inherent in the nature of SSI and in any mechanism that gives control of one individual's identity data to another. It is the "essential leap of faith" required for the power of SSI to be wielded on behalf of individuals who cannot use it directly themselves.

The specific risks here are:

1. **Dependents becoming too dependent**: In an ideal world, guardianship is a temporary condition before a dependent can manage their own SSI digital identity. Unfortunately, this is not always possible, for example, with Jamie, whose dementia may be progressive for the rest of his life. However, in all other situations, there should be no financial or additional incentive for a guardian to remain in power when the dependent has the capacity to be empowered.

2. **Recentralization**: SSI is inherently decentralized and moves "power to the edge" to eliminate single points of failure, increase security and privacy, and empower individuals to gain greater control and value from their digital identity data. Excessive reliance on guardians can result in "recentralization," e.g., moving power back to a guardian. There is a particular risk that some organizations or governments may try to act as their customers' or citizens' guardians instead of as their peers and delegates.

POTENTIAL MITIGATIONS

Unfortunately, the inherent risks in guardianship are so general that the most effective mitigations may need to occur at the level of legislation or broad social action. Some mitigations at this level include:

1. Requiring informed consent and consent verification processes before issuance of guardianship credentials.[9]
2. Defining precise levels of assurance (and corresponding liabilities) for guardianship and dependent credentials.
3. Prohibiting "bulk load" processes where whole populations are converted to guardianship without involvement or consent.
4. Developing governance frameworks that establish best practices for guardianship, including provisions for consent, audit, appeal, and whistle-blowing.

VIOLATING THE TRUST RELATIONSHIP

As cited above, the first rule of guardianship in the Sovrin Governance Framework—and all forms of guardian and fiduciary relationships—is "Act in the dependent's best interests." However, there are likely to be situations where this is a subjective matter. Although the balance of power in the relationship leans towards the guardian, human relations and the interplay between multiple guardians for the same person make each situation unique.

Examples of such judgment calls:

- Requiring sick, dependent travel for treatment when the dependent does not wish to travel.
- Purchasing medical equipment for a procedure the dependent does not want to take but which medical professionals advise is best for the dependent's health.
- Not carrying out a transaction that the dependent has requested if the guardian believes it is not in the dependent's best interests.

These differences of opinion on what an individual's best interests are—and what constitutes "good judgment"—expose risk to the welfare of the dependent. The reverse is also true, although less likely. For example, a dependent may ask a guardian to lie about a health condition, thereby exposing the guardian to liability.

[9] See this post on iRespond's informed consent process https://medium.com/id2020/unbundling-informed-consent-lessons-from-mae-la-24bdd19e7bbd

POTENTIAL MITIGATIONS

1. Requiring guardians to be qualified or certified according to either legal standards and/or the requirements of specific guardianship governance frameworks.
2. Designing certification and level-of-assurance claims into guardianship credentials.
3. Requiring regular and robust requalification and recertification cycles for guardianship credentials.
4. Including appeal and whistle-blower mechanisms in guardianship regulations or governance frameworks.

IMPERSONATION AND COMMINGLING OF IDENTITY DATA

Another longstanding risk of guardianship is the guardian using their position to benefit themselves, even if the guardian believes this does not directly violate the dependent's trust or interests. For example, a guardian may pretend to be the dependent without the dependent's knowledge to qualify for a merchant discount when making their online purchases. Or a guardian might commingle the dependent's credentials with the guardian's credentials. For example, Ann may be tempted to apply for a loan on Jamie's behalf to move their bedroom downstairs but use an electricity bill credential in her name.

POTENTIAL MITIGATIONS

Digital guardianship laws or governance frameworks should mandate that guardians must:

1. Always maintain separate digital wallets and credentials for their dependents.
2. Always maintain a cryptographically-verifiable audit trail of all transactions from the dependent's wallet.
3. Obtain authorization of a trusted third party for high-value or high-risk transactions on behalf of a dependent.
4. Disclose their guardianship relationship to a verifier any time a transaction might involve a conflict of interest on the part of the guardian.

COMPLEXITY, CONFLICT, AND COMPETITION

Guardianship can get easily get messy. For example, imagine that Jamie wants to visit family in Pakistan, where the rights and responsibilities of guardianship are different. Ann cannot make the trip, so Jamie will need a separate guardian who will maintain a separate digital wallet for Jamie during his time in Pakistan.

In this situation, there are multiple guardian wallets and potentially multiple guardianship governance frameworks in operation. These guardians and their guardianship credentials may compete in the context of specific transactions, for example, completing a visa application and then extending that visa.

POTENTIAL MITIGATIONS

1. Focus on high-quality user experience design that anticipates these potential conflicts and helps walk guardians and dependents through the choices.
2. Design levels of assurance for guardianship credentials to enable evaluation of competing credentials.
3. Work towards the maximum interoperability of guardianship governance frameworks.
4. Provide mediation or brokerage functions within the credential management layer of SSI infrastructure (see the last section).

RISKS AT MOMENTS OF TRANSITION OR CHANGE

All business processes encounter risk at moments of transition or change. With Guardianship, these risks have an impact on the relationship between guardians and their delegates because they arise from real-world situations outside the scope of the SSI as a technical system. . Transitions in guardianship s often happen in stressful environments and/or at difficult or emotional times in a guardian and their dependents' lives.

The frequency of change in guardianship can be high; for example, doctors must legally assess Jamie's mental capacity at the start of each healthcare interaction to determine if his cognitive abilities change as his condition progresses. Risk management for such change should be structured around the guardianship lifecycle, focus on informed consent at Inception, and ensure that a dependent is not "digitally stranded" with no guardian at Termination.

POTENTIAL MITIGATIONS

1. Protect the dependent's ability to maintain continuity in guardianship by embedding the physical in the digital through the use of biometrics, embedded technologies, and voice in the SSI user interface.

2. Encourage or require guardian organizations to design, implement, test, and maintain a high-quality business operating model and SSI architecture with an end-to-end process framework that includes online and offline processes.

3. Enable guardianship and digital identity transactions that take place offline to be replicated online, e.g., synchronized within the SSI network (this is critical for the humanitarian sector).

4. Develop machine-based guardians (or guardian assistants) that learn from guardians and/or dependents what their actions/choices should be—and empower guardian assistants to act as a guardian in moments of transition or change if there is a breakdown in the real world.

Note that this last recommendation has precedent in the offline world today—it is similar to how a living will is implemented as a legal and medical document.

Guardianship in the SSI Infrastructure

Although digital guardianship is fundamentally a construct of human trust relationships, it is also grounded in Sovrin's architecture, or "technology stack. The layers of SSI infrastructure called the Trust over IP (ToIP) stack and defined by Hyperledger Aries RFC 0289, are uniquely suited to support digital guardianship. They combine underlying layers of cryptographic or "technical" trust with higher layers of human trust as represented by legal, business, and social frameworks. This four-layer architecture is shown in Figure 7.

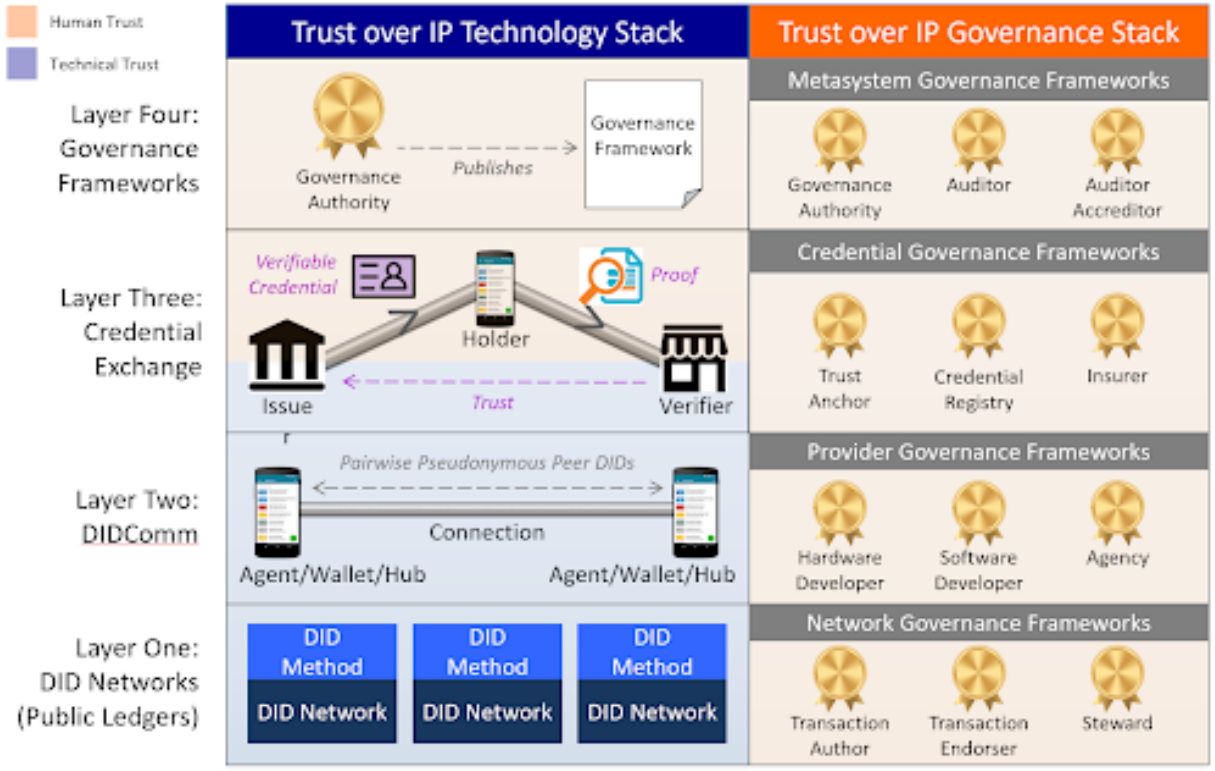


Figure 7: The four layers of the Trust over IP stack

In this section, we explain the specific support for digital guardianship at each of the four layers.

LAYER ONE: DID NETWORKS

This layer consists of the public blockchains or other decentralized networks that support Decentralized Identifiers (DIDs), an open standard for cryptographically-verifiable identifiers that do not require centralized registry services. Layer One is how we can have a wide variety of strong cryptographic roots-of-trust that do not depend on single authorities.

Although many guardians will have DIDs rooted in a Layer One DID network such as the Sovrin Network, those entities serving as guardians are opaque to this layer. For privacy and security reasons, DID ledgers do not hold digital credentials and hence do not contain information on whether a given DID represents a dependent or an independent identity owner. Layer One is essentially purely cryptographic distributed networking infrastructure

LAYER TWO: DIDCOMM

Layer Two is defined by SSI digital wallets, agents, and hubs that speak the DIDComm protocol to establish peer-to-peer, DID-to-DID connections for secure communications and data exchange. At this layer, default DIDs are called peer DIDs because they are generated and exchanged directly between the digital wallets of the two peers and are not rooted in a public ledger at Layer One. Layer One DIDs are needed primarily for credential issuers (Layer Three) whose digital signatures, based on their DIDs, need to be widely verifiable.

This layer is where the fundamental task of guardianship takes place: management of a digital wallet (and the private keys it contains) by the guardian on behalf of the dependent. This management is what gives a dependent access to SSI infrastructure without the dependent needing to have their own SSI-capable devices or network access.

Guardians must perform this task in a way that avoids the commingling of their identity data with the dependent's identity data. This strict oversight avoids many potential problems. It enables a dependent who transitions out of guardianship in the future to have a clean transition to control of their wallet. The best practice is for a guardian to use two different identity wallets to enforce this separation. At a minimum, the guardian must use a multi-user digital wallet that enables complete separation of the guardian's and dependent's DIDs, private keys, and other identity data.

Figure 8 is an illustration of the separation of the digital wallets for a mother acting as a guardian for her child.

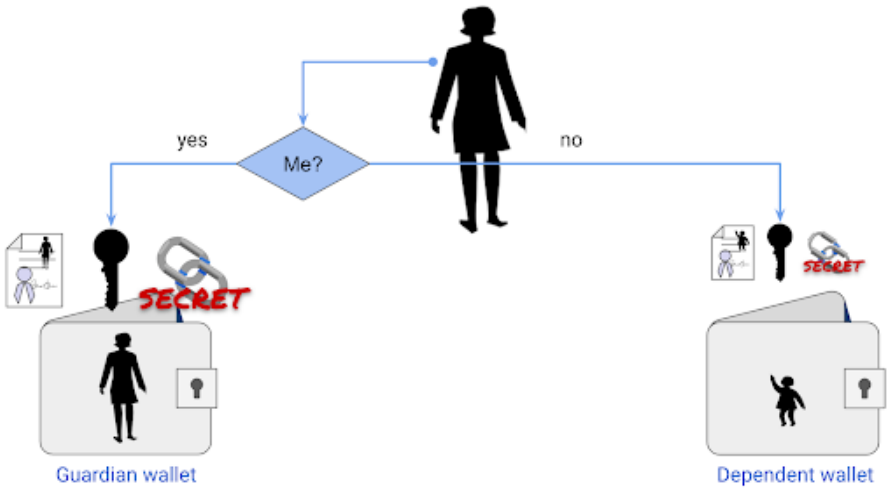


Figure 8: Digital wallets for guardian and dependent

The mother has her digital wallet on the left, and the digital wallet she maintains as a guardian for her child on the right. When the mother is managing her own identity, she uses the wallet on the left. When she is managing her child's identity as her guardian, she uses the wallet on the right.

LAYER THREE: CREDENTIAL EXCHANGE

Layer Three is where human trust enters the ToIP stack in the form of the "trust triangle" among issuers, holders, and verifiers of digital credentials based on the W3C Verifiable Credentials Data Model 1.0 open standard. These credentials are exchanged over peer-to-peer DIDComm connections at Layer Two and, as a rule, are signed by the issuer using the private key associated with a DID rooted in a public ledger such as the Sovrin ledger at Layer One, so that any verifier can easily verify the issuer's public key.

From the standpoint of guardianship, this layer is critical for two functions:

1. **Guardianship, delegate, and dependent credentials:** These express the complex and nuanced permissions management required to support guardianship. As described in the earlier sections of this paper, guardians (and their delegates) and dependents need credentials that capture respective rights and responsibilities, including the conditions under which guardianship can be revoked before the guardianship relationship can be considered to be valid.

2. **Standard verifiable credentials needed by the dependent:** Part of the beauty of the ToIP stack is with the addition of the special credentials described above (and Layer Four governance frameworks to support them), SSI identity management for dependents **functions like SSI identity management for independents**, e.g., everyone else. There is no difference. Although the guardian operates the digital wallet, the dependent can still obtain, hold, and prove digital credentials like anyone else. And these are the credentials that the dependent will "take over" when and if the dependent transitions to independent status.

LAYER FOUR: GOVERNANCE FRAMEWORKS

Layer Four is the layer where human governance is added to the first three layers. The only technology at this layer is the definition of a small set of special verifiable credentials used by governance authorities to publish governance credentials. These credentials are used to provide proof that an SSI entity is performing one or more of the roles in the ToIP Governance Stack on the right. For more information on these roles, and how governance frameworks can be developed for any layer of the ToIP stack, please see the description of the ToIP Governance Stack in the Trust over IP RFC.

Layer Four may be the most critical layer for guardianship as a digital right. In many cases, governance frameworks of various kinds (including legislation from actual governments) will define the legally-binding rules and policies for different forms of guardianship. These specialized governance frameworks should address all of the topics in this paper, including all phases of the guardianship lifecycle and all of the business, legal, and technical policies and processes necessary to mitigate the online and offline risks associated with guardianship. Above all, they should ensure a dependent's right to revoke guardianship.

The Guardianship Task Force of the Sovrin Governance Framework Working Group has already begun work in this area: see http://bit.ly/sample-guardianship-tf for an example governance framework, credential, and schema. The Sovrin Guardianship Working Group will continue this work (see below).

Conclusion and Next Steps

Guardianship is essential to SSI. Guardianship enables people with whom we have trusted relationships—rather than central authorities—to digitally transact on our behalf for those times in life when we cannot act for ourselves. As vital as it is, digital guardianship is inherently complex due to the multiple relationships it must represent and the numerous risks it must guard against.

This paper from the Guardianship Task Force of the Sovrin Governance Framework Working Group is the product of a year's research and exploration of how digital guardianship should work within an SSI ecosystem. We have attempted to define the core concepts, explain the different types and conditions of guardianship, enumerate the risks, describe the lifecycle, and place guardianship in the context of the four layers of SSI infrastructure. We hope that this effort serves as the starting point for implementing digital guardianship technically, legally, and in governance frameworks designed for this purpose.

GUARDIANSHIP DEMOS

To accompany this paper, the Guardianship Task Force developed short demos of guardianship that offer some examples of how it can work in practice:

- Link to Mya's demo - Child refugee use case
- Link to Jamie's demo - Dementia use case

Please note these are preliminary, rough-cut demos designed to teach basic concepts and advance discussions. Further collaboration and community effort are needed to develop and deploy working solutions.

THE SOVRIN GUARDIANSHIP WORKING GROUP

The work of the Guardianship Task Force, including this paper and the demos above, have progressed to where the Sovrin Foundation is ready to create a formal working group to begin implementing the technical, legal, and governance components of digital guardianship. To that end, all readers are invited to join the Sovrin Guardianship Working Group <<insert link>> . Membership is voluntary and open to anyone who wishes to support the work.

Document Management

AUTHORS

Aamir Abdullah, Sterre den Breeijen, Kelly Cooper, Michael Corning, Octavia Coutts, Rick Cranston, Heather Dahl, Daniel Hardman, Nicky Hickman, Noelannah Neubauer, Darrell O'Donnell, Philippe Page, John Phillips, Drummond Reed, Chris Raczkowski, Peter Simpson, Jamie Stirling, Scott Warner.

With thanks to members of the Sovrin Guardianship Task Force, Sovrin IoT Task Force and Sovrin Governance Framework Working Group for their time, knowledge, and expertise in bringing the paper and guardianship demos to life.

WHITE PAPER REVISION HISTORY

Date	**Version**	**Author(s)**
June 2019	Original Version	Sovrin Guardian Task Force (1)
July 2019	Split out Practical Guidance	
September 2019	0.3 - draft for team & critical review	
October 2019	0.4 - clean view for final reviews & intro!	
October 23, 2019	0.5 - updated with exec summary and conclusion	
November 13, 2019	0.7 - copyedited	Trevor Butterworth
November 20, 2019	0.8 - graphic layout	Helen Garneau

Disclaimer

PLEASE NOTE: THE INFORMATION PROVIDED BELOW IS FOR INFORMATIONAL PURPOSES ONLY AND MAY NOT BE RELIED UPON BY ANY PARTY AS LEGAL ADVICE. PARTICIPANTS IN THE SOVRIN NETWORK SHOULD CONTACT THEIR COUNSEL TO OBTAIN ADVICE WITH RESPECT TO THE POTENTIAL APPLICABILITY OF THESE, AND OTHER LAWS TO THEIR INTERACTION WITH THE SOVRIN NETWORK.

Copyright