On Guardianship in Self-Sovereign Identity

Sovrin Guardianship Working Group
April 2023
V.2

sovrin
identity for all

sovrin
identity for all

Executive Summary

Self-sovereign identity (SSI) is a widely supported new model for Internet-scale digital identity that moves beyond centralized "identity providers" by establishing 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 and mental capacity to act for themselves, both online and offline. For SSI to work for everyone, individuals who do not have the appropriate capacity or do not have digital access need another person or organization to serve as their digital identity 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 ID 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 an important feature of SSI[1] 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 commingling of identity data between dependent and guardian. 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 a high-level technical overview on how Guardianship fits the Trust over IP stack[2]. Further guidance is available from two additional documents: one providing Implementation Guidelines[3]; and the second Technical Requirements.[4] These documents, and this whitepaper, are the subject of ongoing work by the Sovrin Foundation's Guardianship Working Group.[5]

---

[1] Principle 2 of SSI: Delegation - *An SSI ecosystem shall empower entities who have natural, human, or legal rights in relation to their identity ("Identity Rights Holders") to control usage of their digital identity data and exert this control by employing and/or delegating to agents and guardians of their choice, including individuals, organizations, devices, and software.* (source: Sovrin)

[2] https://trustoverip.org/toip-model/

[3] Guardianship Credentials Implementation Guidelines V1

[4] Guardianship Credentials Technical Requirements V1

[5] https://sovrin.org/guardianship/

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, augmented and virtual reality, cryptocurrencies, NFTs 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, financial 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 as societies increasingly transition toward digital transactions and depend on digital identities, digital exclusion may become a significant challenge for many. To mitigate this risk, identity systems need a means of connecting with and representing those who cannot act for themselves in the digital world. Today, many guardianship processes are still paper-based, and are difficult to verify in a digital way. For example:

- A power of attorney or third-party mandate can be used to prove to a bank that you can act on behalf of your mother.
- A parent can use their child's birth certificate and proof of their ID to enroll them into elementary school.

These examples of guardianship currently use offline paper credentials and human face-to-face verification. However, they are less secure, less transparent and there are limits to the value of the transactions they can support, especially when these examples are transferred into the digital world.

Self-sovereign identity (SSI) systems, where control of a digital identity is asserted using digital credentials stored in a digital format, present new challenges and opportunities for guardianship. How can we enable everyone to control their digital identity?

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

- Work with 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[6], a status that is well-established in legal systems globally, is this mechanism. Guardianship has always been an essential component of the Sovrin Governance Framework.

This paper, published by the Sovrin Guardianship Working Group, explores the guardianship relationship and how it fits in with the overall SSI "web of trust." It presents risks, benefits and approaches to implementation of Guardianship for SSI use cases.

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 even more so. Therefore, it is essential to provide clear definitions of digital entities and digital relationships defined in the SGF. Table 1 provides essential terms for understanding Guardianship.

[6] Also sometimes referred to by others as proxy access, delegated access, delegated authority, asserted authority or appointed authority.

Table 1, Definitions:

Dependent	an entity for the caring for and/or protecting/guarding/defending of which a guardianship arrangement has been established.
Guardian	a party that has been assigned rights and duties in a Guardianship Arrangement for the purpose of caring for and/or protecting/guarding/defending the entity that is the dependent in that Guardianship Arrangement.
Guardianship Arrangement	Guardianship Arrangement (in a Jurisdiction): the specification of a set of rights and duties between legal entities of the jurisdiction that enforces these rights and duties, for the purpose of caring for and/or protecting/guarding/defending one or more of these entities.
Guardianship Type	a class of guardianship arrangements within the jurisdiction that governs and manages them.
Jurisdiction	the composition of a legal system (legislation, enforcement thereof, and conflict resolution), a party that governs that legal system, a scope within which that legal system is operational, and one or more objectives for the purpose of which the legal system is operated. See also the Jurisdictions pattern.
Legal Jurisdiction	a jurisdiction that is governed/operated by a governmental body.
SSI (Self-Sovereign Identity)	SSI (Self-Sovereign Identity) is a term that has many different interpretations, and that we use to refer to concepts/ideas, architectures, processes and technologies that aim to support (autonomous) parties as they negotiate and execute electronic transactions with one another.
SSI Agent	a digital agent that provides one or more of the SSI functionalities (issuer, holder, verifier, wallet) to its principal.

Audience

This document is for policy and decision-makers, designers, researchers, lawyers, technical architects, 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 some details specific to Sovrin's infrastructure are included, the discussion is relevant for any SSI system. It is, however, important to note that this white paper does not set explicit requirements for guardianship in the context of SSI. The range of guardianship applications is vast; therefore, different norms and standards will be needed for different circumstances.

History and Scope

The initial Guardianship White Paper[7], published in December 2019, was crafted around the technical and conceptual architectures at that time. It provided practical tools, guidelines and designs for implementing guardianship in SSI use-cases. In April 2021, the Guardianship Implementation Guide and Technical Requirements were published. Two Sovrin Stewards have also produced further practical assets which are available to the SSI community for implementing guardianship. These include TNO's eSSIF Lab, terms and mental models, and from Sezoo a series of blog posts looking at specific industry use cases which examine the business impacts and opportunities.

This Guardianship White Paper V2 has been revised based on learnings and insights from real world experiences since its first publication. It provides an overview of guardianship in the round which serves as guidance for applying DIDs/VCs in your jurisdiction within existing Guardianship laws, regulations, and policies.

Example Use Cases

To sharpen our focus, we frame the issue around two fictional people needing guardianship[8] to have trustworthy digital identities so they can access vital services.

Jamie

Jamie was diagnosed with Alzheimer's 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

[7] https://sovrin.org/guardianship/

[8] 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.

attorney[9] to make decisions regarding his healthcare when he is deemed not to have the capacity to make a medical decision.

Mya

Mya is five or six 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 and a woman named Zo who "adopted" her because they recognized her from their home village. Mya arrived in the camp three weeks ago, and none of her extended family are there. She is malnourished and disoriented.

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).

Why SSI Needs Guardianship

The challenge of inclusivity

To fulfill its inclusion principles, SSI must be designed such that guardianship is supported. Jamie and Mya are not alone in being unable to control their lives, both in the physical and digital world. According to the UN, 2.9 billion people, or 37% of the world's population have never used the internet.[10] The World Economic Forum reports an even higher number at 3.7 billion people.[11] This digital divide is not evenly distributed across sex, geography, and circumstance. Women are more likely than men to be digitally disconnected. According to 2019 data from the U.N. High Commission on Refugees, nearly half of all refugees (around 32 million people) don't use the internet.[12]

Challenges of inclusivity extend beyond access and include individuals who don't have the mental capacity to self-assert their identity as well as minors who require adult representation. Globally, about 26 percent of the world is under 15 years of age and some nine percent is over 65 years of age.[13] Of course not all older people will develop dementia however, to quote The Economist

---

[9] Exact terminology will differ across geographies. For example, in England and Wales, this is called a Lasting Power of Attorney.

[10] Reported in the Guardian at https://www.theguardian.com/technology/2021/nov/30/more-than-a-third-of-worlds-population-has-never-used-the-internet-says-un

[11] https://www.weforum.org/agenda/2020/04/coronavirus-covid-19-pandemic-digital-divide-internet-data-broadband-mobbile/

[12] Reported in the Washington Post at https://www.washingtonpost.com/technology/2019/04/24/millions-refugees-need-broadband-too/

[13] Statistica, https://www.statista.com/statistics/265759/world-population-by-age-and-region/

newspaper, this illness is a "global emergency"[14] due to its rising prevalence. In 2020, Alzheimer's Disease International reported that there were over 55 million people worldwide living with dementia and that this number will almost double every 20 years, reaching 78 million in 2030 and 139 million in 2050.[15]

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[16] and gives complete control over their digital identity and related private data.

How can we take care of people that are not capable of acting for themselves, and allow someone else to act on behalf of them? How can both guardians and dependents benefit from the unique properties of SSI? How can we promote the use of SSI to the benefit of all involved?

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

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 or don't want to be self-sovereign—the most challenging gap in the SSI identity model. The exact text of the Guardianship principle is:

> Guardianship: A Party that does not have the capability to directly control (parts of) the Party's Identity Data (a Dependent) shall have the right to be appointed another Party who has that capability to serve as the dependent's Guardian. The Dependent might appoint a Guardian by itself, but it is possible that an authority places the Dependent under guardianship. A Dependent has the right to become an Independent by satisfying all

[14] The Economist, https://www.economist.com/leaders/2020/08/27/the-rising-prevalence-of-dementia-is-a-global-emergency?gclid=CjwKCAiA24SPBhB0EiwAjBgkhjM9CB8yAdX5_A5UjVthOfmCC15rdwCb2oXfuKZ7utzB_2CISagzmxoCgEQQAvD_BwE&gclsrc=aw.ds

[15] Alzheimer's Disease International, https://www.alzint.org/about/dementia-facts-figures/dementia-statistics/

[16] 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 Adrnieu's notes on Functional Identity.

conditions for becoming an Independent. The conditions can differ per Jurisdiction, and per Guardianship Type. 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 allows various legal constructs, including legal guardianship, power of attorney, conservatorship, living trusts, banking relationships, to be used in an SSI-world.

As the text notes, guardianship relies on constructs coming from different jurisdictions. As mentioned above, a jurisdiction can be the legal system of a nation, but also the jurisdiction of a family. This allows guardianship that comes from legal constructs, but also guardianship in situations where social norms underpin roles.

Guardianship does not capture the actual transfer of control of private data and keys from an individual (the dependent) to a guardian (an independent identity owner), only the data that is needed for the guardian to fulfill its rights and duties. The starting time of a guardianship shifts accountability to a guardian, satisfying the rights and duties of their role. If the rights and duties are narrow and rigid, day-to-day use will be difficult; 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:

- Preserve to the maximum extent the self-sovereignty and dignity of those who cannot act for themselves.
- Protect the privacy and security of both parties in the guardianship relationship – dependent and guardian. Offer practical and applicable solutions governed by a protective framework.
- Work in conjunction with and extend existing, non-digital guardianship constructs into the digital world to foster digital inclusion.In short, carefully constructed guardianship is essential to an inclusive SSI world. Without it, SSI solutions will either tend towards centralization 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 formal, they can be founded on legal constructs such as assignments of

guardianship or an adoption certificate, but also based on policies that exist within organizations such as banks. Formally or informally, guardianship helps or protects a dependent person.

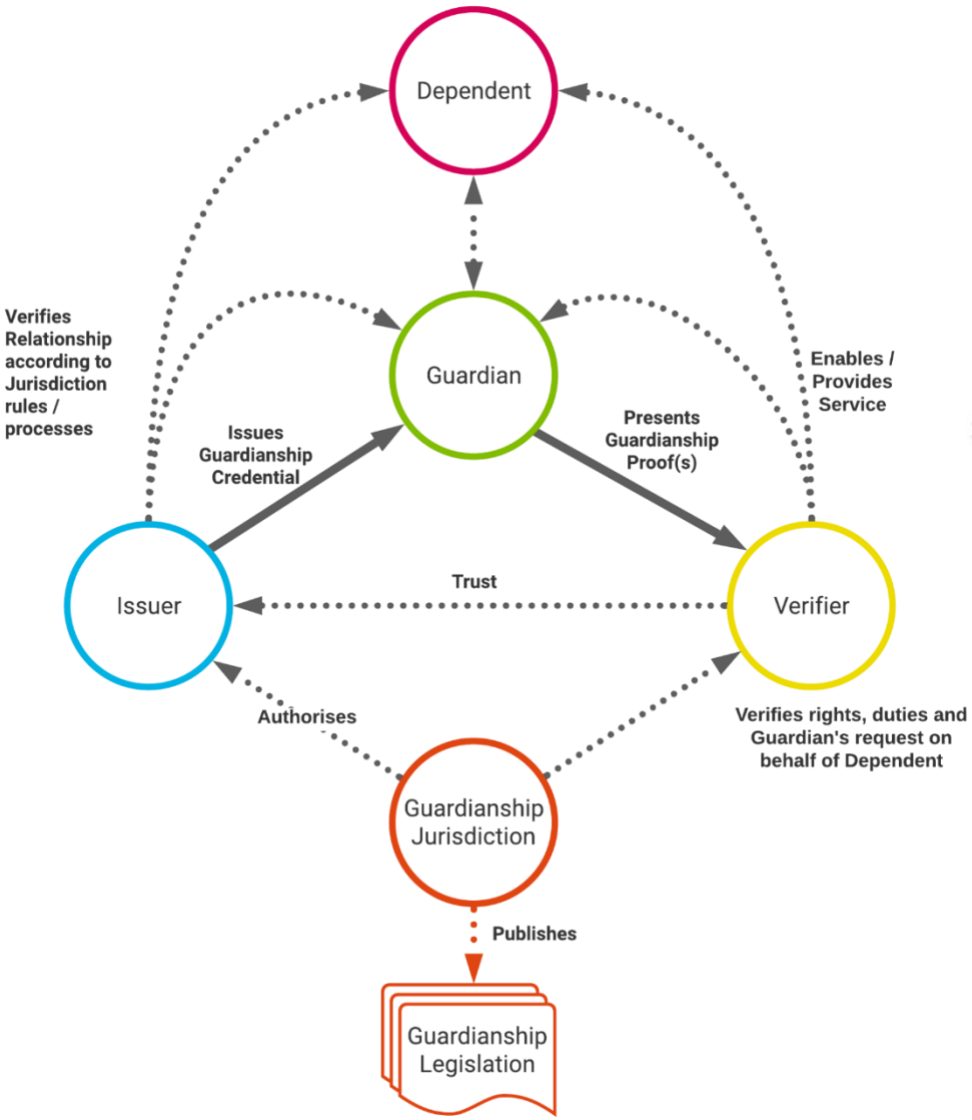

Figure 1: Visual model of how Guardianship works in conjunction with SSI

In SSI, guardianship can be proved using claims that can be issued in the form of a digital credential. Guardians can add this credential to their wallet to prove that they are allowed to act on behalf of someone else. A dependent can still be in control of their own wallet and may be able to access their own data. For example, when a dependent is placed under an administrative guardianship, the dependent might still be allowed to have access to their email account.

With this approach, Guardianship does not demand the control of all or parts of the dependent's digital wallet. This obscures the relationship and risks leading to impersonation since the verifier does not know that the guardian is handling the wallet.

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. This can be done using guardianship credentials where the rights and duties of the guardian are explicitly described, and that is issued to the guardian. Using credentials, it is possible to trace back the origin of the data, and thus a high level of assurance can be obtained[17].

When is guardianship needed?

Guardianship provides access to SSI benefits to people unable to participate in certain transactions. As mentioned above, many guardianship arrangements are imposed by an authority in a jurisdiction. Remember that the term 'jurisdiction' is used in a broad sense, not only referring to the laws in a country, but also to guardianship policies at a specific organization. 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, no commingling of funds, etc. 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.

This conceptual model of guardianship is described in Guardianship Implementation[18] and allows use cases such as a parent acting on their child's behalf when the child is below the age of majority/consent, or when a person assigns guardianship using a legal instrument such as a power of attorney. Another use case is where an individual has no online access. Guardianship allows individuals without digital access, to access online services via their guardian acting as their proxy.

For example, in Mya's case, a humanitarian NGO serves as her guardian, based on the rules that apply within the borders of the refugee camp where Mya is located. 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

[17] Chained credentials: aries-rfcs/README.md at main · hyperledger/aries-rfcs · GitHub
[18] Guardianship Credentials Implementation Guidelines V1

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 acts on behalf of the dependent in a digital world, *the governance framework for setting up and managing a guardianship relationship is critically important*.

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. Lasting Power of Attorney that Jamie established with his wife, Ann. This legal construct usually takes the form of a signed 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.

Examples of different types of Guardianship mandates

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

In all cases, credentials issued to both guardians and dependents must have specific fine-grained permissions under governance frameworks that include rights and duties for both guardian and dependent, as well as 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 financial affairs. It is useful to view these on two key dimensions:

1. **The Temporal Dimension:** These range from ad hoc, to forms of guardianship that extend beyond death in some jurisdictions. The expected duration of the relationship drives key governance considerations, possibly leading to different technical solutions.
2. **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, within this dimension it is useful to consider four main groups:
    a. **Full Guardianship**, where the dependent is considered 'incapable' within a jurisdiction.
    b. **Partial Guardianship**, where the dependent is considered 'incapable' for specific transactions but can transact by themselves for other transactions (for example: a financial guardianship).
    c. **Protective Guardianship**, where the dependent needs to transact together with a guardian.
    d. **Supportive Guardianship,** where the dependent can transact alone but chooses to transact with a guardian.

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 requirements of both dimensions. The realization of guardianship arrangements within digital contexts are intended to supplement, and not necessarily replace, (non-digital) legal constructs or judiciary identification of guardianship relationships.

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. 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 accreditation 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.

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, 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. Mya may not need a guardian for some things, such as eating in the refugee camp food tent.

Differences over time

When Mya first arrives at the refugee camp, she is entirely dependent on her guardian to take care of her. Mya is not able to participate in any transactions regarding her rights and duties, both in the digital and physical worlds. As she grows, receives education, and gains independence, Mya's need for reliance on her guardian diminishes. This growing independence differs from Jamie's

dementia example. While Mya transitions toward an independent person with no need for guardianship, the waning of Jamie's capacity and capabilities sees the transfer of rights and duties to a guardian. Jamie may need more than one guardian or choose to have more than one guardian. For example, in the case of Lasting Power of Attorney in the UK, many donors decide to appoint more than one attorney and often name a replacement attorney.

Differences in permissions

Permissions are directly connected 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) - for example where the Dependent is under the age of 18,
2. **Place** - the jurisdiction(s) and/or geographical locations in which the guardianship arrangement is valid,
3. **Type(s)** - for example legal, medical, educational, travel
4. **Rights and duties** - a list of the responsibilities what the Guardian has on behalf of the Dependent, within circumstances or events. This may include the assessment of a Dependent's capacity to act on their own behalf.
5. **Identity authentication mechanisms** (for both Guardian and Dependent) - visual, biometric, credential verification (physical or digital), etc.
6. **Agents** (what software/devices the guardian can use)

Differences in presentation

Guardianship relationships are authenticated by a verifier during verification and interpretation of presented credentials. The presented credentials may be in the form of:

1. **Credentials** that provide the verifier with sufficient trust that the guardian is in fact the guardian and can carry out what they are requesting, based on the presentation context. The business logic within the verification process, in this case, is the responsibility of the verifier.
2. **Specific, special-purpose guardianship credentials**, with only the necessary data attributes, issued by a trusted source having taken the actors through a specific process. In this form, the guardianship credential is acting as a "good to go" credential with specific usage expectations and contextual limitations. The business logic and process of creating a special-purpose guardianship credential in this type of use case is the responsibility of the issuer and may be specific to one or more jurisdictions.

A few considerations should be noted:

1. The choice of credential model to be adopted is dependent on how the business logic and responsibilities are agreed by the parties involved.
2. In some scenarios, the Issuer and the Verifier could be the same organization (e.g., a bank).
3. The use of both models can be supported within the same jurisdiction.
4. Any specific verification business logic is always the responsibility of the verifier and should not be included in the creation logic for a generic guardianship (good-to-go) credential.

Guardianship and other types of Representation

As illustrated above, guardianship relationships can be complicated, dynamic, and full of blurry lines. What guardianship is and what it is not can be understood by addressing Representation, based on certain relationships. The Sovrin Glossary defines a few potential instances of Representation by addressing the roles of delegate, guardian, and thing controller. The first ideas on these three are captured in Figure 4 taken from Appendix C[19] of the Sovrin Glossary:

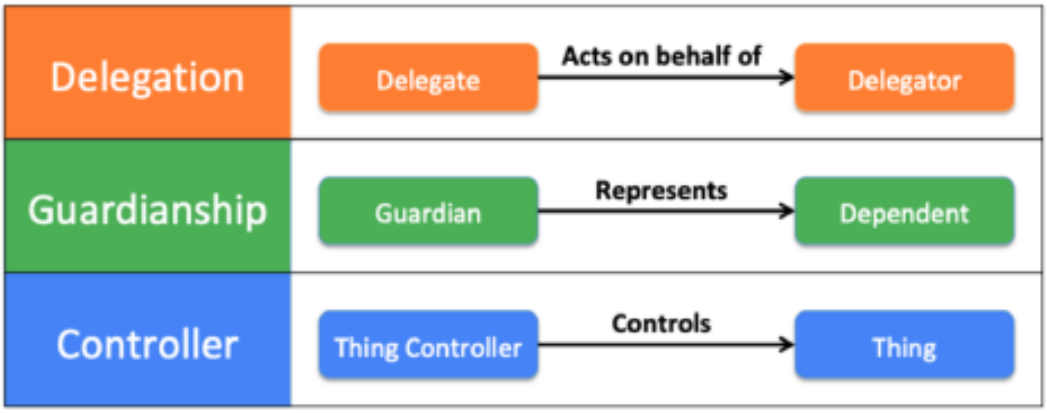

Figure 4: Three types of indirect identity control relationships

[19] https://sovrin.org/library/glossary/

Delegate

In this use case a party in a specific jurisdiction that has laws/rules that state conditions under which that party CAN be represented by another party for the purpose of delegating tasks to the delegator.

Guardianship

In this use case, a person or organization (a party) in a specific jurisdiction that has laws/rules that state conditions under which that party (which we call the 'dependent') MUST (or SHOULD) be represented by another party (called the 'guardian') for the purpose of caring or defending the dependent.

Thing Controller

In this use case, we have a Thing (i.e. not an individual with legal rights) in a specific jurisdiction that has laws/rules that state conditions under which that Thing MUST be represented by a party for the purpose of accountability and taking care of that thing.

Interworking of control relationships

Delegation is one of the most common and useful functions that can be implemented using 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 specific credentials to perform guardianship responsibilities.

Delegation, guardianship, and controller relationships will often work in webs of trust. For example, Ann might delegate her guardianship credentials to a care worker.

The Guardianship Lifecycle

From an implementation perspective, Guardianship is the definition of a specific set of digital credentials for both guardian and dependent, that can be presented in conjunction with other credentials held by either party. The guardianship credential lifecycle is similar to standard credential lifecycle management; however, a Guardianship Credential describes a relationship where at least two Parties are involved, rather than a specific individual. For example, the Guardianship Credential held by the Guardian specifies the Holder to be the Guardian and the Subject to be the Dependent.

Whilst the application of verifiable credentials to guardianship scenarios follows the normal lifecycle and cross-jurisdiction use of credentials for other scenarios, the added complexity in guardianship scenarios comes from the full range of possible and sensitive applications for guardianship and the specific rights and duties required or demanded of the guardian —all of which must mitigate the critical risks of establishing and allowing 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:

- Technical requirements for the cryptographic trust layers of SSI infrastructure (see the final section of the paper).
- Governance and business process mapping for the human trust layers.

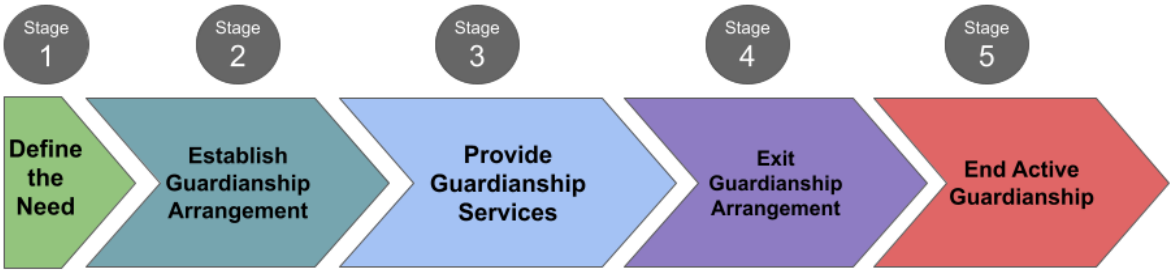

Figure 5: The five major stages in the Guardianship lifecycle

STAGE 1: Define the need

The first stage is to identify the need for a guardian, assess if the need is legitimate and ensure that the parties involved (actors) are known. Setting up a Guardianship Arrangement can be complex, due to legal processes (e.g., Ann's need for a limited power of attorney on behalf of Jamie). By contrast, in a humanitarian emergency case like Mya's, the establishment of guardianship must be done rapidly.

This stage ends with validation by a trusted entity (e.g. Governing Body under a known Jurisdiction) that a Guardianship relationship (the Guardianship Arrangement) can be created, ideally with the informed consent of the dependent. In nearly all cases, this will rely heavily on organizational processes.

Figure 6: A mother and her baby enroll in a biometric identity system.

STAGE 2: Establish guardianship arrangement

The second stage is creating the actual guardianship relationship by issuing the necessary Guardianship and Delegation Credentials to the Guardian, Dependent and any other relevant stakeholders. As described above, from a technical perspective, these are standard SSI credentials that conform to the W3C specification for verifiable credentials. What makes these credentials unique is that they use schemas specially designed for defining the legal and contextual basis and constraints for guardianship. These schemas are typically defined in a corresponding governance framework for guardianship.

This may involve the creation of new schemas and governance frameworks which should appropriately describe the rights and duties of both the Guardian and the Dependent, as well as the limitations of the Guardianship Arrangement by jurisdiction or activities. It is the responsibility of the jurisdiction to maintain these definitions and the appropriate use of the credentials.

As part of this process, a specific person may need to be identified to act on behalf of the dependent, where the formal Guardianship Arrangement is with an organization or government department. This would be achieved by delegating the guardian role specifically to one or more people. These guardianship arrangements are reflected using W3C verifiable credentials.

This stage ends with a Guardian ready to perform (digitally enabled) transactions on behalf of the Dependent.

STAGE 3: Provide guardianship services

This stage covers the real-life usage of the Guardianship Credentials that are issued to the Guardian. In this phase, Zo acts on behalf of Mya, and Ann supports Jamie when he needs help.

The credentials issued to Zo and Ann define the Jurisdiction of validity and the rights and duties of these guardians in supporting Mya or Jamie.

The Jurisdiction under which the credentials are effective can evolve and rights and duties of the guardian can be changed. Where necessary, that might require new credentials to be issued.

Jurisdiction interoperation may allow the guardianship credentials to be used more broadly than initially anticipated. The validity of the presented credentials is the responsibility of the verifier to determine.

STAGE 4: Evolution of guardianship

Like all human lives and 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.”

Depending on the guardianship purpose and scope, the migration to independence might occur either as a gradual process or all at once.

As Mya (or in fact any child) grows older, becoming old enough to take more responsibility for her own actions, Zo’s practical role becomes less critical. As Mya achieves the age of maturity, she would look to be issued and manage her own credentials in the same way as Zo does as the guardian. Mya is issued equivalent credentials for her own use. Zo’s credentials may not be actively revoked, but can be considered to be practically expired, because Mya has reached the age at which Zo cannot act on her behalf. It could be that Zo can have a slowly reducing role as a guardian (as happens with parental guardianship), depending on the jurisdictional rules that apply in various scenarios (medical, educational, social etc.)

In Jamie’s situation, a recovery could cause the limited power of attorney to be annulled. A legal process is required for Jamie to go through to prove his independence and ability to be responsible for his own actions and credentials. Any newly added credentials issued to Ann in her capacity as Jamie’s guardian would have to be revoked and Jamie to be issued his own replacement credentials for the equivalent purposes. Automatic reallocation of capabilities to Jamie might indeed be possible, but the resulting credentials would need to reflect Jamie as both the Subject and the Holder.

STAGE 5: End active guardianship

As described above, the termination of a Guardianship Arrangement may be explicit, with the guardianship credential and guardian-held credentials being revoked or deactivated, or implicit, due to the verifier recognizing the jurisdictional rules that make the arrangement void.

The status update or revocation of guardianship credentials may be governed by many factors—whether defined in law, social practice, commercial process, or a guardianship governance framework. Examples include:

- A formal reassessment of the capacity and the capability of the dependent to control their identity (e.g., the case of Jamie).
- A law or legal judgment changes the status of the guardianship arrangement (e.g., a power-of-attorney is revoked).
- The Dependent is able to have their own commercial arrangements (e.g., Mya has a bank account of her own and no longer needs a trust bank account controlled by Zo).
- A change in the social context is identified or the guardianship is no longer required, which causes a change of guardianship to be reflected in the existing or new guardianship arrangement (e.g., Mya's mother is found, death of the dependent or guardian[20], or Mya leaves for another refugee camp, etc.).
- A change in the organizational rules (within the current guardianship arrangement jurisdiction) needs to be reflected in the guardianship definition. This change typically causes the rights and duties of the guardianship arrangement to change (e.g., Zo's role and duties are changed such that she makes sure that Mya goes to school) or new guardianship arrangements need to be established in other related jurisdictions (e.g. Mya is able to be returned to her mother and this is reflected in the national legal system).

As can be seen, managing Guardianship Arrangements is not a trivial task for the Guardian, the Issuer, or the Governing Body. Verifiers also must be aware of the effect of guardianship credentials and the rules in the use of guardian scenarios.

Where guardianship is provided by individuals (such as Ann acting for Jamie), more than one guardian (as in the parental situation) or by an organization (such as an NGO acting for Mya), guardians must actively manage the Guardianship Arrangement and the resulting credentials that are issued to themselves under specific (and multiple) jurisdictions. Governing Bodies must support the process of establishing and managing guardianship arrangements by establishing and managing the governance rules and operational procedures that underpin the use of credentials that are issued and verified under the jurisdiction of each Governing Body.

[20] A death certificate would be issued in this case, which could support the use of the guardianship arrangement. However, the presentation of supporting credentials isn't necessarily automatic. Therefore, the guardianship arrangement may need to be changed to support digitally those surviving the deceased and assist in managing their affairs—for example, in executing a will or carrying out probate.

Risks of SSI in 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 SSI in guardianship and how they may be mitigated.

The below principles should be considered for Guardianship policies in a governance framework:

A Guardian should:

- Understand, respect, and comply with the rights and duties that are stated by the Jurisdiction under which the Guardianship Arrangement is set up.
- Be particularly careful that a guardian is representing their delegate and not acting on their own behalf.
- Keep detailed records of all actions taken on behalf of the Dependent.
- Not violate the Anti-Impersonation principle (section 2.11.5).
- Be subject to applicable legal structures as defined by the relevant jurisdiction, for example the granting and revocation of guardianships.

Self-Sovereign Identity is primarily concerned with providing control of our digital identity and personal data to the identity owner—in this context, an individual. Ironically, guardianship does precisely the opposite. Guardianship intentionally supports a Guardian (and its delegates) to manage (part of) the rights and duties on behalf of a Dependent who is not able or not allowed to exert such control him/herself.

Risks are inherent in any mechanism that gives control of an individual's identity data to another. It is a critical leap of faith for the power of SSI to be wielded on behalf of individuals who cannot use it directly themselves.

Recentralization

SSI is intended to be 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.

Example mitigations are:

- Prohibiting "bulk load" processes where whole populations are converted to guardianship without involvement or consent.
- Developing governance frameworks in SSI assurance communities that establish best practices for guardianship, including provisions for consent, audit, appeal, and whistleblowing.

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 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 include:

- The guardian making a medical decision that could be said not to be in the best interest of the dependent.
- Self-payment by the guardian for effort provided in caring for the dependent.
- Requiring a dependent to travel for treatment when the dependent does not wish to travel.
- Fraud or inappropriate use or misuse of funds by a guardian, not in the best interest of the dependent.
- Not carrying out a financial 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.

Example mitigations are:

- Careful definition of the rights and duties of the guardian.
- Requiring guardians to be qualified or certified according to either legal standards and/or the requirements of specific guardianship governance frameworks.
- Designing certification and level-of-assurance claims into guardianship credentials.
- Requiring regular and robust requalification and recertification cycles for guardianship credentials.
- Including appeal, objection 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 but use an electricity bill credential in her name.

Enabling guardianship using SSI is a clear step forward for verifiable guardian relationships that do not rely on documents such as birth certificates and enable a guardian relationship to be verified in many contexts. As with a physical birth certificate, it is difficult for a guardian to misuse a verifiable credential because although they are the credential holder, they are not its subject.

Example mitigations are:

- Guardianship laws or governance frameworks should mandate that guardians must clearly distinguish between their own identity data and that of their dependents. This is clearly articulated in the credential itself by distinguishing between the credential holder (the Guardian) and the credential subject (the Dependent). A clear distinction in the Guardianship Arrangement about the scope of guardian's rights and duties, for example between supporting someone, for example with decision making, or acting on behalf of someone.
- Always allow the Dependent to control the wallet and credentials, corresponding to the rights and duties that they still have. The Guardian should control the Guardianship Credentials that they manage, in a wallet that is controlled by the Guardian.
- Make sure that it is clear for the verifier when a Guardian or when a Dependent is acting in a business transaction. This is needed for the verifier to determine whether to accept this transaction.
- Always maintain a cryptographically verifiable audit trail of all transactions from any wallet. This might be needed for an audit of the Guardian.
- Obtain authorization of a (second) guardian/trusted third party for high-value or high-risk transactions on behalf of a dependent.

Complexity, Conflict, and Competition

Guardianship can 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 the guardianship credentials for Jamie during his time in Pakistan.

In this situation, there are multiple guardianship credentials 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. The verifier, in this case the visa issuer, can decide which guardianship arrangement to accept, based on a risk assessment.

Example mitigations are:

- Focus on high-quality user experience design that anticipates these potential conflicts and helps walk guardians and dependents through the choices.
- Design levels of assurance for guardianship credentials to enable evaluation of competing credentials.
- Work towards the maximum interoperability of guardianship governance frameworks.
- Provide additional functionality and trust assurance methods within the credential management layer of SSI infrastructure. For example, using a Trust Registry for schema, issuer, or verifier verification.[21]

Risks at moments of transition

All organizational processes encounter risk at moments of transition. 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 often happen in stressful environments and/or at difficult or emotional times in a guardian and their dependent's 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 after a point of transition.

[21] A Trust Registry is a network service that enables a governing authority for an ecosystem governance framework (EGF) to specify what governed parties are authorized to perform what actions under the EGF. For example: What issuers are authorized to issue what types of verifiable credentials?

Example mitigations are:

- Protect the dependent's ability to maintain continuity in guardianship by allowing the interoperability of physical and digital credentials through the use of biometrics, QR codes, embedded or supporting technologies, and low technology / no technology solutions to support the SSI user experience.
- 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.
- Enable guardianship and digital identity transactions that take place offline to be replicated online, e.g., synchronized within the SSI network.

Guardianship in the SSI Infrastructure

The use of Verifiable Credentials to support digital guardianship and the construction and use of human trust relationships is grounded in Sovrin's architecture and the SSI design approach. The layers of SSI architecture defined in the Trust over IP (ToIP) stack and underpinned by technology solutions, such as Hyperledger Aries RFC 0289, are uniquely suited to support digital guardianship. They combine underlying layers of messaging and cryptographic "technical" trust, the operational or governance requirements for an ecosystem, with higher layers of human trust as represented by legal, business, and social frameworks. This four-layer architecture is shown in Figure 7.

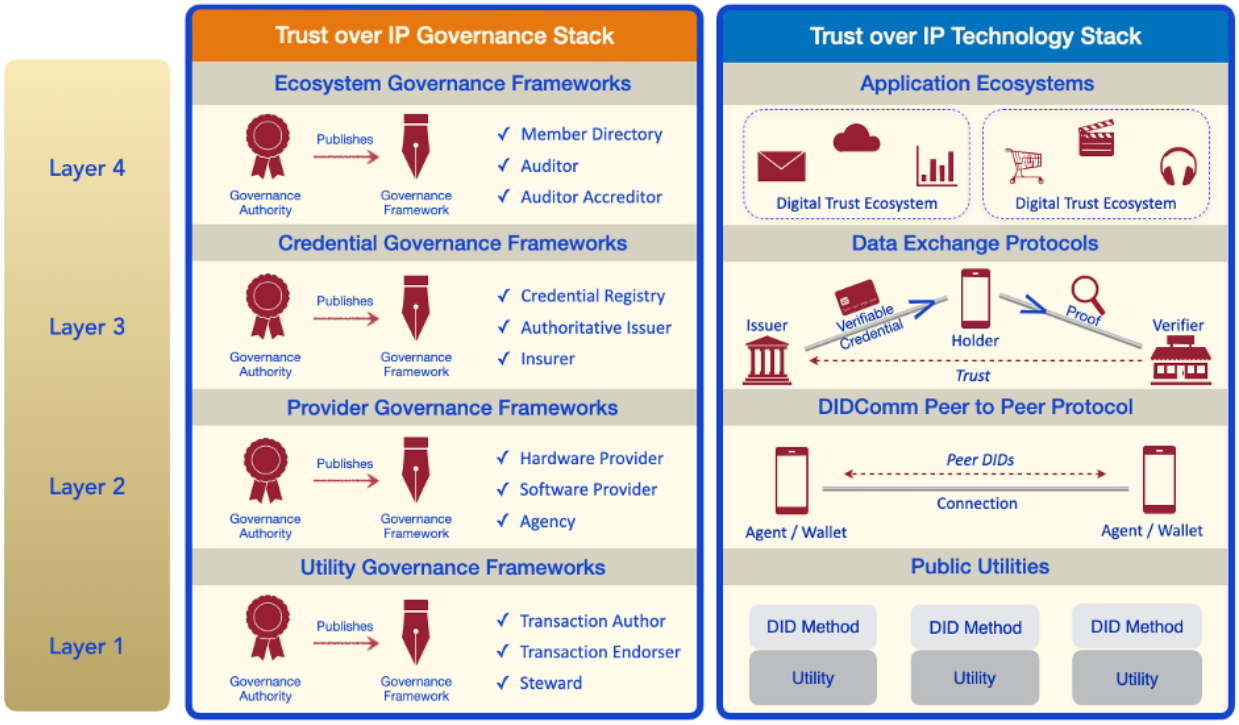

Figure 7: An overview of the Trust over IP Stack, focused on the data exchange layer

LAYER ONE: Public Utilities

This layer consists of the utilities for the definition and storage of Decentralized Identifiers (DIDs), supporting cryptographic solutions, networks and messaging solutions that underpin the use of decentralized networks.

The mechanism of establishing guardianship arrangements should be agnostic of the utility that underpins the DID management. Guardianship interactions are focused on the use of VCs and therefore require accessible DIDs and interaction models that are required by issuers and verifiers.

Specific utilities or other layer one solutions are not anticipated to be required to support guardianship.

LAYER TWO: DIDCOMM PEER-TO-PEER PROTOCOL

Layer Two is defined by SSI agents that use appropriate interaction protocols to establish peer-to-peer and DID-to-DID connections for secure communications and data exchange. At this layer, peer DIDs define the connection and are used for the secure point-to-point communication and the sharing of verifiable credentials.

Guardians are, like any other person in SSI interactions, defined by a DID (layer one) and secure connections are established for the sharing of VCs which are defined at layer three (see below).

Guardians are identified using existing human trust processes (VC-based, login or other mechanisms) and the trusted interactions capability is established. The Guardian does not use the Dependent's DID as part of any of this interaction. The Guardian establishes interactions with others to allow them to issue VCs to the Guardian as the Guardian.

LAYER THREE: Data Exchange Protocols

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 typically 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.

As defined earlier in this document, Verifiable Credentials that define a guardianship arrangement are used to reflect the parties involved (Dependent, Guardian, Delegates, etc.). Relevant information that needs to be included for exchange between the holder and verifier and the rights and duties of the Guardian, should be defined by the Jurisdiction under which the VC was issued. The verifier is required to define the nuances and rules of the VC presentation and the implications of a VC being presented by a Guardian (the holder) rather than the Dependent (the subject in the VC).

Based on the Technical Requirements and the Implementation Guideline documents, it is assumed that guardianship credentials, and digital interactions that exchange them, reflect that the presenting actor, the Holder, is the Guardian. A transparent relationship and activity are therefore assumed.

LAYER FOUR: Governance Frameworks

Layer Four is the layer where the application ecosystem is defined and includes the specification of jurisdictional guardianship types. For example, in a healthcare application ecosystem a guardianship type 'welfare' is defined, and a guardianship arrangement is created for Jamie and Ann for making decisions regarding clinical treatments whereas a guardianship type 'financial' is defined for them for making health insurance claims.

Verifiable credentials include the identification of the jurisdiction and the applicable governance framework (the rules and definitions). This layer is predominantly reflective of the governance process, rules and policies that describe the environments and jurisdictions necessary to recognize the exchanged information, the roles played by participants and the legislative and

trust framework that formalizes the use of verifiable credentials and the mechanisms of their exchange.

Layer Four may be the most critical layer for guardianship as a human right. In many cases, governance frameworks of various kinds (including legislation from jurisdictions such as governments and other commercial entities) will define the legally binding rules and policies for different guardianship types. These specialized governance frameworks should address all the topics in this paper, including all phases of the guardianship lifecycle and all 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 independence, revoking any guardianship arrangement, if necessary.

Conclusion and Next Steps

Guardianship is essential to digital existence and SSI. Guardianship enables individuals or organizations with whom a dependent has trusted relationships to digitally transact on their behalf during times in life when such person requires that assistance.

As vital as it is, digital guardianship is inherently complex due to the multiple relationships it must represent, responsibility for managing sensitive personal issues that may be shared or shifted to a guardian, and the numerous risks it must guard against.

This paper reflects the constant evolution of Sovrin's view on Guardianship and how the maturity of SSI has evolved the integration of guardianship with digital identity. The Implementation Guidelines and Technical Requirements published by Sovrin are an indication of the Foundation's commitment to guardianship and SSI. Deployment of Guardianship credentials for real world applications is happening, and this document aims to support those use cases.

This paper from the Guardianship Working Group is the product of several years of research and exploration on how digital guardianship should work within an ecosystem using SSI solutions. The maintenance of this document along with the newly created Guardianship Credentials Implementation Guidelines[22] and Guardianship Credentials Technical Requirements of Guardianship [23] explains the different types and conditions of guardianship, enumerates the risks, describes the lifecycle and places guardianship in the context of the four layers of SSI infrastructure. It is intended that this effort serves as the starting point for implementing digital guardianship technically, legally, and in governance frameworks designed for this purpose.

[22] Guardianship Credentials Implementation Guidelines V1

[23] Guardianship Credentials Technical Requirements V1

Future Work

The Sovrin Guardianship Working Group[24] continues the work on expanding practical guidance. Future work items were enumerated in the Guardianship Credentials Implementation Guidelines.[25] These include;

- Validation of guardianship credentials / types
- Assurances
- Wallet Take-over
- Transparent vs Opaque guardianship scenarios
- Other representation types
- Updates to existing use cases and new use cases
- Updates based on evolving technology

From a more theoretical and strategic perspective, and in the context of the Sovrin Foundation's *Identity for All* mission, future work items include:

Using Guardianship Credentials for Human Rights & Impact Accounting

There are increasing regulatory and compliance requirements on digital and financial service providers to identify and protect customers from online harms, especially children and vulnerable adults. For example, the UK's Online Safety Bill is set to impose a *duty of care* on service providers with penalties of <10% of global revenues[26]. At the same time, the pandemic has placed increased demands on governments to evidence in data that they have delivered health and social care. All of these are situations where organizations have duties towards individuals which exist in law and are the result of a consent, contractual or legal process. It could be interesting to explore how issuing a guardianship credential from the dependent to the organization as a result of these processes could increase accountability and uphold individuals' rights.

Machines Supporting Guardianship Situations

Artificial Intelligence (AI) and automation are key technical trends to consider for guardianship. Semi-autonomous and autonomous machines may be empowered to help make decisions for people in complex chains of liabilities and duties. Examples may include personal care robots in assisted-living environments, autonomous vehicles in smart cities, etc.

What are the legal, ethical and governance implications of machine supported guardians? Further research and discussions are required.

---

[24] https://sovrin.org/guardianship/

[25] Guardianship Credentials Implementation Guidelines V1

[26] https://committees.parliament.uk/publications/8206/documents/84092/default/

Document Management

Date	Version	Authors
November 2019	V. 1	Guardianship Task Force: 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.
April 2023	V. 2	Guardianship Working Group: Lisa Talia Moretti, Sterre den Breeijen, Nicky Hickman, John Phillips, Jo Spencer, Jamie Stirling, Chris Raczkowski

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.