Self-Sovereign Identity and Guardianship in Practice

EJLT European Journal of Law and Technology

Self-Sovereign Identity and Guardianship in Practice

Sterre den Breeijen, Gijs van Dijck, Tobias Jonkers, Rieks Joosten & Katja Zimmermann*

Abstract

With Self-Sovereign Identity (SSI) technologies, individuals use electronic 'wallets' to collect information ('credentials') from various parties about themselves and present this information to (possibly other) parties. The context in which the information is *presented*, or *used*, is often different from the context in which a credential with this information is *created* and *issued*. In this paper, we illustrate this with financial guardianship, which is created by a judge in an official court procedure and which gives the guardian rights and duties that can or need to be invoked vis-a-vis a party not being the court. In this illustration, we explore (i) the application of SSI in the context of financial guardianship, (ii) what is characteristic about the gap between the practical (legal) and technical perspective, and (iii) what needs to be done to overcome the challenges. We observe gaps between the legal and technical reality. We offer insights into how to advance the application of SSI in the context of financial guardianship, and possibly beyond, which may be taken up in future research.

Keywords: Self-Sovereign Identity, SSI, guardianship, law and technology

* Sterre den Breeijen is affiliated with the Ministry of the Interior and Kingdom Relations; Gijs van Dijck is affiliated with Maastricht University (UM); Tobias Jonkers and Katja Zimmermann are affiliated with University of Groningen (RuG); Rieks Joosten is affiliated with Netherlands Organisation for Applied Scientific Research (TNO).

1. Introduction

Examples of Self-Sovereign Identity (SSI) applications include a pilot with hotel check-ins in Germany, where employees of certain companies can use their smartphones to check in with a developed ID wallet,[1] the German ID wallet app with basic ID and proof of a driver's licence,[2] and Turkey, where the Ministry of Foreign Affairs, the United Nations Development Programme, and the Istanbul Chamber of Commerce collaborated to implement SSI in order to increase the employability and financial independence of the more than 3 million refugees in the country. Most would agree that SSI is about individuals that have electronic 'wallets' in which they can collect 'credentials', i.e. information from various organisations about themselves.[3] The individuals can use these credentials with other organisations that need such information in order to provide the individual with a product (e.g. a parking permit) or a service (e.g. entrance to a building). We take it that the 'self-sovereign' part of the term SSI refers to the assumption that individuals and organisations are sovereign over themselves, i.e. autonomous in what they think, how they perceive the world, in making decisions etc. In other words, they can control what they share and whom they share their information with, yet not what others share and whom they share it with. 'Identity' alludes to the idea that what you are is the union of what you and others think you are. It is said that SSI allows individuals to control their own identity, which means in practice they can get credentials about themselves, and use them in electronic business transactions with other parties.[4] Our perspective is that SSI is all technology and other means that are necessary to support the exchange of such 'qualified data' between parties that electronically interact with one another. Therefore, anything that helps – e.g. concepts/ideas, architectures, processes and technologies, is covered by that term.[5]

---

[1] <https://www.bundesregierung.de/breg-de/suche/start-pilot-hotel-check-in-1914392> (last accessed 28 February 2022).

[2] <https://www.bundesregierung.de/breg-de/themen/buerokratieabbau/e-id-1962112> (last accessed 28 February 2022). The app has been criticised for not being properly implemented and tested and for it not being based on international standards, consequently making it not sustainable: https://jolocom.io/blog/id-wallet-ein-debakel-mit-folgen/ (last accessed 28 February 2022).

[3] Various definitions of SSI can be found through websites of different organisations, e.g. Sovrin Foundation https://sovrin.org/library/glossary/, Trust over IP, https://trustoverip.org/wp-content/uploads/sites/98/2020/05/toip_introduction_050520.pdf, or eSSIF-Lab https://essif-lab.github.io/framework/docs/essifLab-glossary#self-sovereign-identity-ssi. A definition can also be found in Drummond Reed & Alex Preukschat, *Self-Sovereign Identity: Decentralized digital identity and veri*
fiable credentials (Manning, May 2021).

[4] This is the vision of eSSIF-Lab, https://essif-lab.github.io/framework/docs/essifLab-vision.

[5] For general information on SSI, we refer to Drummond Reed and Alex Preukschat, Self-Sovereign Identity, Manning, May 2021; Oskar van Deventer, Self-Sovereign Identity - the good, the bad and the ugly; May 2019 | TNO, May 2019.

For the purpose of this article, we assume that SSI will continue to develop and will mature (technologically) over the coming years, in such a way that data processors can simply request for qualified data, i.e. data that comes with assurances (e.g. of provenance and integrity) that make it valid for processing. In addition, SSI technology will enable verification and validation of the responses to be done in an automated fashion. Under this assumption, SSI is already expected to bring several benefits. An organisation that needs to know the yearly income of a citizen, e.g., to establish whether or not it has a right to a social benefit, or to construct a mortgage offer, can simply ask for a credential that contains such data and ascertain it is of the quality it expects it to be (e.g. 'higher than €30,000'). In practice, this would mean that citizens can use their wallet app to fill in the forms that these data processors require them to fill in for certain purposes.

A challenge that is currently not addressed in the literature concerns the interoperability between data that lives at a particular data source in a context/domain that is very different from the context where it is to be used. Financial guardianship is such a context. For example, if a judge creates a financial guardianship, this is some free-format text that nevertheless provides the guardian with rights (and duties), e.g. regarding one or more of the dependent's bank accounts. In an operational setting at a bank – the banking portal – such documents or texts cannot easily be processed, resulting in operational inefficiencies.

A credential is as meaningful as the use that can be made of it. The party that might benefit from a financial guardianship credential seems to be the bank, more particularly one that offers online banking services where account holders have access to their bank accounts and can transfer money through the services. Whenever individuals access the banking portal, they log in, get to see the (possibly multiple) bank accounts that they have a right to access, and can consume the banking services for each of these accounts. Note that from the bank's perspective, a successful login means that the user is identified and associated with a login account to which various rights may be associated, e.g. for accessing bank accounts, insurances, etc.

In this article, we explore how SSI can be applied in the area of guardianship, financial guardianship in particular. As will be further explained below, financial guardianship is a legal phenomenon where a guardian is appointed by the court and who is tasked with making legally valid decisions regarding the assets of another person. A guardian can represent another person and for example transfer money from a bank account or conclude an insurance contract. A third party, the bank or the insurance company, needs to verify the capacity of the guardian: is (s)he authorised to conclude this transaction on behalf of someone else? SSI could help parties, considering that guardianship occurs rather frequently and that its procedure and outcomes are rather standardised. Guardianship can therefore be considered as a 'most likely' legal case study, in that the implementation of SSI is likely to be unsuccessful in other areas if it is unsuccessful in the context of guardianship.

The research question we aim to answer is how SSI can be applied in the context of financial guardianship, and what the challenges are when doing so. For this, we apply SSI to the typical case where an individual is subjected to financial guardianship, as a result of which the guardian will carry the legal responsibilities for the individual's estate and bank account.

This article is structured as follows. We first explain in more detail what SSI (*Section 2*) and financial guardianship (*Section 3*) entails. We then discuss the possibilities and limitations of applying SSI to financial guardianship in the Netherlands (*Section 4*). The findings and their impact are then discussed (*Section 5*). This article concludes with some final remarks (*Section 6*).

2. Self-Sovereign Identity

Over recent years, SSI has become a term that refers to a multitude of ideas, principles and technologies. Currently, SSI technologies and other components are being developed at various places.[6] SSI promises to reap many benefits, yet applications are limited to specific contexts.[7] In addition, interoperability has to be improved, not only at the technology level (that is currently actively worked on), but also at the semantic level (parties need to know what data in the credentials means), at a legal level (e.g. different privacy laws restrict the exchange and use of credential data in different ways), and at a governance level (processors must be able to rely on the data supply processes to be properly governed).

The dialogue about what Self-Sovereign Identity (SSI) really is, which started in the blog 'The Path to Self-Sovereign Identity' by Christopher Allen in 2016,[8] has not

[6] *W3C-CCG*, a W3C working group of 400+ people that explore the creation, storage, presentation, verification, and user control of credentials, and whose tasks include drafting and incubating Internet specifications for further standardisation and prototyping and testing reference implementations. eSSIF-Lab, a project in which tens of small and innovative companies work together to provide an interoperable infrastructure that can be used to address real-world challenges. DIF - Decentralized Identity Foundation is an engineering-driven development-focused organisation that aims to develop the foundational components of an open, standards-based, decentralised identity ecosystem for people, organisations, apps, and devices. ToIP – Trust over IP Foundation is an independent project hosted at the Linux Foundation, working with pan-industry support from leading organisations around the world to provide a robust, common standard and complete architecture for Internet-scale digital trust. Effectively, they aim to implement an SSI stack and the associated governance in (at least) Linux environments.

[7] Laatikainen, Gabriella; Kolehmainen, Taija, and Abrahamsson, Pekka (2021), 'Self-Sovereign Identity Ecosystems: Benefits and Challenges'. *12th Scandinavian Conference on Information Systems*. 10. <https://aisel.aisnet.org/scis2021/10>.

[8] Allen, Christopher, 'The path to self-sovereign identity', <http://www.lifewithalacrity.com/2016/04/the-path-to-self-soverereign-identity.html> (last accessed 28 February 2022).

resulted in a consensus. Even in academic papers, there is not always a general agreement on what SSI is and what it is not.[9] While some see the ten principles of SSI that Allen proposed as the definition of SSI, he formulated them as 'a departure point to provoke a discussion about what's truly important'. In addition, it is obvious that what is important differs per party.

Figure 1: SSI data exchange pipeline

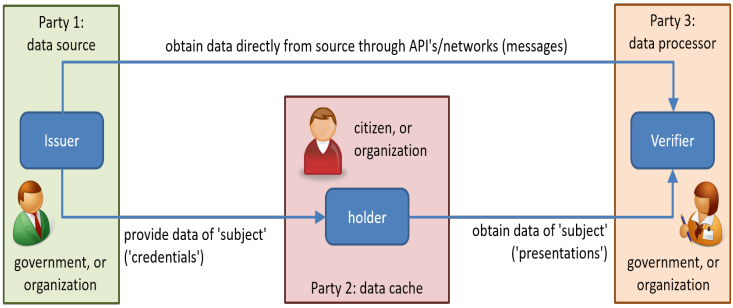

Figure 1 schematically shows how data would typically be exchanged. Party 3 (typically a government or other organisation) requires data for some kind of processing – often to make a decision of some kind. Traditionally, it would obtain the data it needs, such as a yearly income, directly from a data source that it trusts (Party 1 in the figure). This setup requires data sources and data processors to maintain IT-connections through which they can set up sessions (with mutual authentication) for the purpose of exchanging this data. For *n* verifiers and *m* issuers, *n*m* such links would need to be created and maintained.

In SSI, parties with a data source can (electronically) provide data about a citizen or organisation (the 'subject' of such data) to that citizen or organisation, signing it (and providing additional proofs or assurances) such that any party the citizen shows it to, can determine its provenance (and integrity) in a cryptographically sound fashion. We will use the term 'qualified data' to refer to data that comes with such (verifiable) assurances. The citizen will typically use a wallet application (that can be said to serve as a 'data cache') to obtain and store such credentials. Parties that need data for processing can subsequently (electronically) request the citizen to present the data it needs and prove that it originates from the data source and has

[9] Mühle, Alexander, Grüner, Andreas, Gayvoronskaya, Tatiana, and Meinel, Christoph (2018), 'A survey on essential components of a self-sovereign identity', Computer Science Review 80–86. According to this paper, a blockchain is an important component to an SSI architecture; Nauta, Jelle C., and Joosten, Rieks, 'Self-Sovereign Identity: A Comparison of IRMA and Sovrin', TNO 2019 R11011. This paper compares two SSI solutions, which are based on different principles and architecture. However, they are both SSI implementations.

not been tampered with in transit. Note that this setup does not require direct IT-connections between data providers and data processors. Citizens can use the data of providers as they want or need to, without providers knowing citizens' decisions in this regard.

SSI has an impact on the entire IT-stack, i.e. hardware, (system) software, information processes up to business policies. At the lowest levels, SSI relies on cryptography, e.g. for encryption and cryptographic proofs (e.g. about knowing something without actually revealing that knowledge). Such technologies are used to digitally sign digital statements (claims) about various entities, ensure that such claims are obfuscated for parties that have no dealings with them (called 'selective disclosure'), and computing derived statements from fixed data (e.g. if a birth date and the current date are known, a proof can be computed that the bearer is over 18 years old without revealing the actual date of birth). Such sets of digitally signed claims are called credentials. Credentials are typed based on the kinds of claims they may contain. Different parties may issue credentials of the same type. For example, someone can prove his/her home address by presenting a credential issued by the municipality where the person lives, but also a bank can issue a similar credential. One might even issue a credential of himself or herself, stating where s/he lives.
Technological protocols have been devised that allow one:

- To request a credential of a specific kind to be issued. Such protocols provide ways for issuers to make their own decisions regarding whether or not to service such a request, thus enabling them to guarantee that a credential always contains data that it considers true. A party that is issuing a credential is referred to as an 'issuer'; the requesting party is called a 'holder' (as it will hold credentials).

- To request and obtain a 'presentation', i.e. a set of data that originates from specific fields from credentials of a specific type. You can envisage this as a request for providing data to fill in a specific form. Holders may service such requests by creating the requested presentations from credentials they hold and sending that to the requester. The latter then verifies the presentation (and hence is called a 'verifier'), i.e. it checks the cryptographic proofs of provenance, integrity, and other assurances that may have been given. If the checks are all positive, the data in the presentation can be relied on for the purpose that the request was made.

At the (software) application level, provisions have to be made that allow the software to request for presentations and consume the (verified) results. This is something that organisations need to do, and for which there currently are no custom-off-the-shelf solutions. Examples of enterprises taking this on do exist.[10]

[10] Preukschat, A., and Reed, D. (2021), Self-Sovereign Identity - Decentralized digital identity and verifiable credentials. Part 4: How SSI will change your business (Manning), pp 331-407.

At the information level, issuers need to specify the syntax and semantics of the claims they use in the credential that they issue. Such specifications are intended to be used by engineers that write the policies to annotate forms, so that they can decide whether or not, for a specific kind of form, it is valid to map the value of a field in a credential to a field in such forms, or to decide which issuers can be trusted to provide valid data if their credentials based on the processes they say they follow to produce such data. This area is in development. Many syntax and semantic specifications already exist in the form of so-called *schemas* that can be found at various locations (e.g. schema.org, or at data.overheid.nl (Dutch)).

The basic patterns for data flows in SSI can be summarised as follows. The first pattern entails a party that collects data about a person or organisation ('subject' of that data), adds some metadata and digitally signs it all, the result of which is called a 'credential'. This party is called the 'issuer', because it issues such credentials to others ('holders').

The second pattern entails a party that requests data about a person or organisation from that same person or organisation (the holder). The holder checks his/her wallet for relevant credentials, and creates a response to this request (called a 'presentation'). The requesting party then checks the presentation e.g. to see if the credentials are properly signed. This is called 'verification', and as a consequence, the party is referred to as a 'verifier'.

Issuers need to decide what kinds of data to put in a credential. The problem here is that anything they put in there *might* be useful, but there is no way to know upfront whether it will *actually* be useful. This problem is similar to that of a manufacturer that needs to decide what product to make that will actually be used, knowing that many products are brought to the market that (perhaps after an initial success) fail in the end.

Verifiers need to decide what kinds of credentials (from which issuers) they will be requesting from holders for the various purposes it needs them. Again, this is similar to the problem consumers have who need, for instance, a cooking appliance. There are many suppliers, and the differences between them, if not in the type/feature of their products, is in the assurances/warranties they provide. The general problem here is that in the context where issuers (manufacturers) produce credentials (products) that verifiers (customers) need for a variety of specific purposes, both issuers and verifiers have to decide which kinds of credentials to produce c.q. request, and that the type and amount of information that needs to be verified matches what will be produced. It is easy for an issuer to issue credentials that mimic its internal administration in a 1–1 fashion, but that goes with a large uncertainty regarding the usefulness for verifiers. Conversely, an issuer that could issue credentials that are spot on for specific verifiers saddles himself with the burden of managing these 'custom credentials'. The question here is what would motivate issuers to accommodate specific verifiers, as well as what motivates verifiers to start using credentials from a specific issuer.

3. Financial Guardianship

After having discussed the technology behind SSI, we now turn our attention to the legal field in which it might be applied. As explained in the introduction, we have identified the legal concept of guardianship as a promising candidate for the application of SSI technology, as the procedure in which a guardian is appointed, seems to be fairly standardised. We use the term 'guardianship' to refer to situations in which one party (the dependent) is not able to care for or protect itself, and in one way or another is represented by one or more other parties (guardians) that will provide for such care and protection. Examples include parenting (where the child is the dependent and parents the guardians), custodianship, and the execution of the will (by the guardian) of a deceased (the dependent).

Under a guardianship arrangement, interactions can take place where the guardian acts on behalf or in the interest of the dependent. The characteristic property of such situations is that the service provider needs to be convinced that a person claiming to have such rights/duties is in fact a guardian. The grounds (sources) of these rights and duties can be found in, for instance, legislation, and court decisions. The challenges this poses to third parties include keeping track of all such grounds, correctly interpreting such sources (i.e. determine what a guardian should and should not be allowed to do when it interacts with the third party), and to monitor and subsequently accommodate for any changes and updates that are made to these grounds.

Many organisations have operational processes that need to take into account that one or more types of guardianship arrangements must be accommodated. Consider a bank, and its operational processes for account holders to view their bank accounts, transfer money out of it, and provide mandates for such actions to other parties. These processes should accommodate for guardianship arrangements of type 'will execution' (to accommodate situations where the account holder has deceased), 'parenthood' (so that parents can handle the account of minor children), and 'trusteeship'.

In most jurisdictions, several types of guardianship are available to protect an adult who is not capable of taking care of his/her own interests. Legislation differs from country to country, meaning that the terminology used and the powers granted to the guardian vary greatly.[11] What jurisdictions have in common is that a court order is required to make a formal decision, declaring what protective measure is taken and appointing a representative. The procedure is usually conducted before a local court, such as a 'vrederechter' in Belgium, a 'tribunal d'instance' in France or a

[11] For an overview of protective measures in many countries, see Frimston et al. (ed.) (2015), The international protection of adults (Oxford: Oxford University Press) 2015. More information on the protection of adults can be found on the website of the academic network FL-EUR (Family Law in Europe): https://fl-eur.eu/.

'kantonrechter' or 'rechtbank' in the Netherlands.[12] We have no reason to assume that the formulations of the rights and duties in court decisions presumably display similar heterogeneity as described below in Section 4.

In Dutch law, financial guardianship is best represented in the concept of bewindvoerderschap.[13] Unlike a trustee (*curator*: a guardian with full powers), a financial guardian has limited powers over the affairs of another person, the so-called dependent, i.e. the allegedly incapacitated person. Book 1, chapter 19 of the Dutch Civil Code (DCC) regulates financial guardianship. A financial guardian can be appointed by court if an adult is temporarily or permanently unable to take care of his or her financial interests (art. 1:431(1) DCC). This can be due to a physical or mental condition or to problematic debts or spendthrift. The court may order that some or all of the assets of this person, like a bank account or real estate, be placed under the control of the guardian. The guardian is then authorised to administer these assets (art. 1:438(1) DCC) and to represent the adult in matters relating to them in and out of court

Financial guardians receive remuneration for their work (art. 1:447 DCC). They are obliged to take proper care of the assets administered by him/her and they are liable if they fail to do so. Additionally, guardians are obliged to submit periodic reports, usually on an annual basis. When the financial guardianship ends, the guardian must submit a final report to the court. In the meantime, guardians have the power to administer the dependent's assets. This allows them to handle the affairs of the dependent, often including the possibility to make payments through that person's bank account. The basis for this is a court decision issued by the relevant court.

The current process of establishing guardianship is that a specified number of persons, including the dependent, his/her partner, and a family member, submits a request to the court. The request is followed by a court hearing, after which the court makes a decision to grant or reject guardianship. A court decision in which guardianship is granted is usually published in a register,[14] which is publicly accessible, although one needs to know the dependent's last name and date of birth in order to retrieve whether the allegedly incapacitated person has a guardian assigned by the court. The guardian can notify others, for instance the dependent's bank, with the court order serving as the legal basis to obtain certain mandates, for instance the mandate from the bank to control and transfer the client's assets. The

[12] In English law, jurisdiction is granted to the Court of Protection, a specialist court based in London.

[13] On this concept, see e.g. Blankman K (2020) in Vlaardingerbroek et al. (ed.), Het hedendaagse personen- en familierecht (Deventer: Wolters Kluwer), p. 611ff; De Boer, J, Kolkman, WD, and & Salomons, FR (2020), Mr. C. Assers Handleiding tot de beoefening van het Nederlands Burgerlijk Recht. 1. Personen- en familierecht. Deel I. De persoon, afstamming en adoptie, gezag en omgang, levensonderhoud, bescherming van meerderjarigen (Deventer: Wolters Kluwer), p. 688 ff.

[14] <https://ccbr.rechtspraak.nl/> (last accessed 25 May 2021).

register offers the potential to automatically verify whether the alleged guardian is the actual guardian and whether s/he has the rights s/he claims to have.

4. SSI for Financial Guardianship

In this section of the paper, we will apply the SSI technology to the practice of financial guardianship. A credential is formulated by us and applied to Dutch court orders, which were sampled by a survey of case law. First, we elaborate on the semantics and syntax of credentials that somehow serve purposes related to financial guardianship. As already mentioned, a guardian is appointed in a court decision, in which the permissions of the guardian are defined. The permissions are common, and the number of guardianships substantial. The consequence of financial guardianship commonly is that the guardian contacts the bank of the dependent (i.e. the individual to whom the guardianship applies), which subsequently mandates the guardian to provide access to the dependent's bank account. The seemingly standardised process makes guardianship a good candidate for SSI

Obviously, a credential should contain data that allow others to identify the individual people and organisations involved, the roles that they are expected to perform (e.g. a financial guardian), and (references to regulations that determine) their rights and duties. A guardianship credential could look as follows (Figure 2):[15]

Figure 2 – Sample Guardianship Credential

```
{ "financial guardianship": {
        "dependent": {
                "last name": "last name cfm BRP[16]",
                "first names": "first names cfm BRP",
                "date of birth": "date of birth cfm BRP",
                "place of birth": "place of birth cfm BRP",
                "country of birth": "country of birth cfm BRP",
                "gender": "gender cfm BRP"
        },
        "goods": [ <list of goods that fall under the guardianship> ],
        "reasons": [ <list of reasons ….> ],
        "financial guardian": {
                "last name": "last name cfm BRP",
                "first names": "first names cfm BRP",
                "date of birth": "date of birth cfm BRP",
                "place of birth": "place of birth cfm BRP",
```

[15] See figure 4 in the Annex for a Dutch version of the credential.
[16] The BRP ("*Basisregistratie Personen*") refers to the Dutch Key Register of Persons.

```
                    “country of birth”: “country of birth cfm BRP”,
                    “gender”: “gender cfm BRP”
        },
        “remuneration”: {
                    “initial”: “<amount in EUR that …>”,
                    “monthly”: “...”,
                    “yearly”: “...”
        },
        “registration”: “statement specifying the duty to register the
bewindvoering in some register”,
        “action-plan”: “statement specifying the duty to draft and register an
action plan”,
        “entry-into-force”: “statement …..”
}


{ “financial guardianship”: {
        “dependent”: {
                    “last name”: “Puk”,
                    “first names”: “Pieter Jan”,
                    “date of birth”: “01-01-1966”,
                    “place of birth”: “Waterlandkerkje”,
                    “country of birth”: “The Netherlands”,
                    “gender”: “M”
        },
        “goods”: [ “all goods of which the [dependent] is or will become the
owner” ],
        “reasons”: [ “Piet is mentally incapable of managing his finances” ],
        “financial guardian”: {
                    “last name”: “van der Kluns”,
                    “first names”: “Catharina Amalia”,
                    “date of birth”: “01-01-1966”,
                    “place of birth”: “Waterlandkerkje”,
                    “country of birth”: “The Netherlands”,
                    “gender”: “V”
        },
        “remuneration”: {
                    “initial”: “100”,
                    “monthly”: “50”,
                    “yearly”: “400”
        },
        “registration”: “statement specifying the duty to register the
bewindvoering in some register”,
        “action-plan”: “statement specifying the duty to draft and register an
action plan”,
        “entry-into-force”: “statement …..”
}
```

4.1 Decision-Credential

At least in theory it should be possible for a bank, or other entities, to issue an SSI. Using SSI, the court decision may be published as a digital credential and issued to whoever has a legitimate interest (e.g. the guardian). As with all credentials, a decision-credential would ideally be (digitally) signed by, or on behalf of, the judge. The decision-credential must come with 'assurances', i.e. pieces of data that ensure its payload (i.e. the actual data) is indisputably valid, and hence can be relied upon throughout the relevant jurisdiction (e.g. the Netherlands). One example is the assurance that the credential has been issued by, or on behalf of, a legitimate judge. This can be done by embedding a 'judge-certificate' in the decision-credential, which is another credential that may be issued by the Ministry of Justice and that states that the public key that verifiers can use to verify the verdict credential actually belongs to an official judge

Finally, the credential must contain data that allows verifiers to determine which specific real-world entities (e.g. persons, contracts, bank accounts, etc.) fulfil the various roles, which means that a verifier must be able to identify and authenticate such entities. We understand the verification process to be the process of an organisation that, in order to decide whether or not to provide a product or service (e.g. access to a bank account), requests data from the user, i.e. the one that requests the delivery of that product or service, and when such data is provided, not only verifies this data (its completeness, its provenance, and its integrity), but also validates this data (i.e. determines whether or not it may be used in an argument for making the aforementioned decision). Currently, this boils down to a user filling in data in predesigned forms, and (usually an employee of) the organisation doing the verification and validation. While completeness is easily (and often automatically) checked, checking the provenance (and integrity) of the data is much more difficult, and may require the employee to consult registrations of its own, or other organisations (e.g. government citizens' registration, or enterprise registrations). Using SSI, forms can be designed such that they are annotated to require credentials of specific types and provenance, of which the completeness, provenance and integrity can automatically be verified, which makes it easier for users to provide the requested information, and easier (and cheaper) for organisations to verify and validate them.

The difficulty lies in the kinds of credentials that should be involved. The party that defines the structure and meaning of the credentials content (i.e. the party that issues the credentials) is usually not the party that may want to rely on such content. For example, if a court order credential would say: '[the guardian] has the right to control the finances of [the dependent]', and even if the roles were filled in with names, this does not imply that a bank can determine whether or not the user is in fact (the person that performs the role of) 'the guardian', or that the bank can determine to which bank account(s) this right applies

For issuers, the easiest thing to do is to issue credentials in a format that is a 1–1 representation of the otherwise paper artifact, such as a court decision. On the other hand, verifiers are best served by credentials that are customised for use in transactions where a specific product or service is being requested and provided.

4.2 Duties/Rights of the Guardian

A crucial step when creating credentials is to include the rights and duties in the decision-credential. Dutch law only offers a general framework concerning the duties and rights of a guardian. His/her main task is to take care of the assets of an adult who is unable to take care of his or her own interests. The guardian is appointed by the court, and in its decision, the court needs to ascertain which assets are included in the guardianship. The main power the guardian is granted is the exclusive power to administer these assets (art. 1:438(1) DCC). S/he should exercise the 'care of a good guardian' (art. 1:444 DCC) and is liable if s/he fails to do so. It should be noted that these are open norms and that the power to administrate and the duty to take good care do not have a specific meaning and merely give general notions. The power to administrate is very broad and gives a guardian for instance access and control over someone else's bank account.

The actual content or payload of the decision-credential must contain rights and duties that have come into existence as a consequence of the court decision. Depending on the envisaged use, the credential may contain all rights and duties, or only those that are relevant for a specific party (to which such a credential then would typically be issued).

4.3 Homogeneity of Financial Guardianship Orders

A bank that is confronted with a guardian should be able to check the rights and duties of the guardian. It can do so by asking for paperwork, but an automated system that immediately shows the authority of a guardian could save time. For this, it helps if the guardianship orders are homogeneous, as deviations and exceptions are difficult to detect by machines.

In order to determine whether courts currently employ homogenous phrasing in their financial guardianship orders, a sample of such orders was inspected. This sample was retrieved from the website of the Dutch judiciary (uitspraken.rechtspraak.nl) on 2 March 2021 by making use of the following search strategy. First, the search term '*onderbewindstelling*' (financial guardianship) was used to narrow down the court decisions in the database that relate to this type of guardianship. To refine the search results further, only court decisions rendered by

sub-district courts in the area of civil law were selected. This refinement resulted in 348 search results, which were further refined manually by excluding irrelevant search results such as the termination of guardianship, the transformation of trusteeship to financial guardianship, testamentary guardianship, and the appointment of subsequent financial guardians. In the end, a total of 34 financial guardianship orders were distilled.[17] At first sight, this number seems to be relatively low. This can be explained by the fact that not all guardianship orders are published on the website of the Dutch judiciary; case law is only published if they are considered 'special cases', which fit the database's selection criteria.[18] As a result, the analysis has an important limitation given that the reported results are probably an underestimation of the guardianship decisions in the population.

[17] Court of First Instance Midden-Nederland 24 April 2015, ECLI:NL:RBMNE:2015:3502; Court of First Instance Midden-Nederland 24 April 2015, ECLI:NL:RBMNE:2015:3507; Court of First Instance Midden-Nederland 29 November 2017, ECLI:NL:RBMNE:2017:6122; Court of First Instance Midden-Nederland 14 March 2019, ECLI:NL:RBMNE:2019:1113; Court of First Instance Midden-Nederland 21 March 2017, ECLI:NL:RBMNE:2017:1267; Court of First Instance's-Hertogenbosch 11 July 2011, ECLI:NL:RBSHE:2011:BR1380; Court of First Instance Noord-Nederland 11 October 2018, ECLI:NL:RBNNE:2018:4078; Court of First Instance Noord-Holland 24 November 2020, ECLI:NL:RBNHO:2020:11582; Court of First Instance Noord-Holland 18 February 2020, ECLI:NL:RBNHO:2020:1171; Court of First Instance Noord-Holland 12 October 2017, ECLI:NL:RBNHO:2017:8481; Court of First Instance Limburg 15 January 2019, ECLI:NL:RBLIM:2019:249; Court of First Instance Haarlem 1 September 2011, ECLI:NL:RBHAA:2011:BR0306; Court of First Instance Haarlem 10 August 2010, ECLI:NL:RBHAA:2010:BO9125; Court of First Instance Haarlem 22 September 2010, ECLI:NL:RBHAA:2010:BN3545; Court of First Instance Haarlem 22 March 2010, ECLI:NL:RBHAA:2010:BO9330; Court of First Instance Haarlem 22 January 2010, ECLI:NL:RBHAA:2010:BN3339; Court of First Instance Haarlem 26 May 2011, ECLI:NL:RBHAA:2011:BR1295; Court of First Instance Zeeland-West-Brabant 15 February 2018, ECLI:NL:RBZWB:2018:904; Court of First Instance Zeeland-West-Brabant 24 June 2016, ECLI:NL:RBZWB:2016:5844; Court of First Instance Zeeland-West-Brabant 18 September 2013, ECLI:NL:RBZWB:2013:6681; Court of First Instance Zeeland-West-Brabant 19 April 2018, ECLI:NL:RBZWB:2018:2931; Court of First Instance Zeeland-West-Brabant 14 January 2020, ECLI:NL:RBZWB:2020:488; Court of First Instance Zeeland-West-Brabant 14 January 2020, ECLI:NL:RBZWB:2020:489; Court of First Instance Zeeland-West-Brabant 9 May 2018, ECLI:NL:RBZWB:2018:3188; Court of First Instance Zeeland-West-Brabant 13 March 2018, ECLI:NL:RBZWB:2018:1723; Court of First Instance Zeeland-West-Brabant 2 August 2018, ECLI:NL:RBZWB:2018:5048; Court of First Instance Zeeland-West-Brabant 14 January 2020, ECLI:NL:RBZWB:2020:492; Court of First Instance Zeeland-West-Brabant 26 July 2018, ECLI:NL:RBZWB:2018:5036; Court of First Instance Zeeland-West-Brabant 14 January 2020, ECLI:NL:RBZWB:2020:491; Court of First Instance Zeeland-West-Brabant 10 August 2018, ECLI:NL:RBZWB:2018:5065; Court of First Instance Zeeland-West-Brabant 8 September 2016, ECLI:NL:RBZWB:2016:5745; Court of First Instance Zeeland-West-Brabant 14 January 2020, ECLI:NL:RBZWB:2020:492; Court of First Instance Overijssel 25 August 2020, ECLI:NL:RBOVE:2020:2855; Court of First Instance Dordrecht 18 September 2006, ECLI:NL:RBDOR:2006:AY9080.

[18] For an overview of the selection criteria, see: Rechtspraak.nl, 'Besluit selectiecriteria uitsprakendatabank Rechtspraak.nl'. Accessed on March 29, 2021. https://www.rechtspraak.nl/Uitspraken/Paginas/Selectiecriteria.aspx.

A first look at the different guardianship orders revealed that variations regarding the phrasing of the guardianship orders and the type of information that is included in the orders exist. Therefore, it had to be determined on which level(s) these variations occur. Do variations appear solely between the different courts or also in guardianship orders issued by the same court? This second part of the question has proven to be more difficult to assess, given that the 34 guardianship orders were issued by nine different courts, with 15 of the orders made by one court (Zeeland-West-Brabant).[19]

4.3.1 Variations regarding the Components of Guardianship Orders

The dictum of every financial guardianship order consists of several components, such as the appointment of a specific financial guardian and a specification of the goods that fall under the guardianship. However, not all guardianship orders consist of the same set of components. For this reason, it had to be determined which types of components exist and with which regularity they are included in guardianship orders. An analysis of the 34 guardianship orders revealed that such orders can consist of up to eight components:

1. The determination of the goods that fall under the guardianship
2. The reason(s) underlying the guardianship order
3. The appointment of a financial guardian
4. The remuneration of the financial guardian
5. The annual remuneration of the financial guardian
6. The duty to register the guardianship order in the national Guardianship Registry
7. The duty of the financial guardian to submit an action plan
8. The entry into force of the guardianship order

Out of these eight components, only the first and the third component are included in all guardianship orders. Only in one guardianship order issued by the court of

[19] The cases are distributed among the courts is as follows: Court District Dordrecht: 1; Court District Limburg: 1; Court District Noord-Nederland: 1; Court District Overijssel: 1; Court District 's-Hertogenbosch: 1; Court District Noord-Holland: 3; Court Decision Midden-Nederland: 5; Court District Haarlem: 6; Court District Zeeland-West-Brabant: 15.

Haarlem, a financial guardian was not appointed in the dictum.[20] When it comes to the inclusion of the reason(s) underlying the guardianship order, the courts follow different approaches. The courts in Midden-Nederland, Noord-Holland, Overijssel, Noord-Holland, and Limburg seem to merge the reason(s) for the order with the first component, whereas the courts of 's-Hertogenbosch, Noord-Nederland, Haarlem, and Dordrecht seem to not include the reasons in the dictum. The court of Zeeland-West-Brabant takes an intermediate approach; in one case, the reasons were included in the first component, in seven cases, they were stated as a separate component, and in another seven cases, a reason was not provided at all. Moreover, an inclusion of the eighth component in the first component was observed in three guardianship orders of different courts. All other components form separate components that are either fully included or excluded from the courts' dictum. Figure 3 shows to which extent the guardianship orders of the respective courts included the remaining five components:

Figure 3 – Inclusion of Components in Guardianship Orders per Court

Component	Dordrecht	Limburg	Noord-Nederland	Overijssel	's-Hertogenbosch	Noord-Holland	Midden-Nederland	Haarlem	Zeeland-West-Brabant
N	1	1	1	1	1	3	5	6	15
4	0	1	0	1	0	2	3	3	11
5	0	1	0	0	0	2	0	0	12
6	0	1	0	1	0	3	1	0	13
7	0	1	0	0	0	0	0	0	1
8	0	0	0	0	0	0	0	0	5

[20] Court of First Instance Haarlem 10 August 2010, ECLI:NL:RBHAA:2010:BO9125.

Three main findings can be derived from this figure. First, the determination of the goods that fall under the guardianship is included in all of the observed decisions. Second, as has already been established above, not all individual components are included by all courts. Variations therefore exist between different courts. The courts of Dordrecht, Limburg, Noord-Nederland, Overijssel and 's-Hertogenbosch seem to be the most consistent in including and excluding the respective components. Yet, it may not be forgotten that from these courts only one guardianship order could be obtained. Therefore, it cannot be derived whether these courts are consistent in including and excluding certain components. When analysing the (larger) samples from the courts of Noord-Holland, Midden-Nederland, Haarlem, and especially Zeeland-West-Brabant, the findings seem to suggest that variations regarding the type of component included in the dictums of guardianship orders exist not only across different courts but also within the courts themselves.

4.3.2 Variations regarding the phrasing of the components

Variations regarding the phrasing of individual components can exist across courts and within guardianship orders that were issued by a particular court. To the extent that the given sample allows for it, both levels were analysed. To begin with the first component, the determination of goods that fall under the guardianship, it can be observed that the courts generally use the same text modules, but in different sequences. All guardianship orders contain the following text modules: 'specification of the goods', 'name of the person that is placed under guardianship', and 'the fact that this person is placed under guardianship'. In addition, several guardianship orders contained supplementary text modules. For instance, 11 out of 34 orders contained the text module in which a reason for the guardianship was specified. Moreover, three orders provided information on the entry into force of the guardianship. Further, in two orders (one issued by the court of 's-Hertogenbosch and another one issued by the court of Zeeland-West-Brabant), personal information of the person placed under guardianship (i.e. their date of birth and address) were included, while the court of Haarlem in one case specified the temporary nature of the guardianship order. Consequently, due to the existence of different text modules and the fact that they are not used in the same sequence across the courts, variations in the phrasing of this component exist across courts. However, on a court-by-court basis, the phrasing is rather consistent. For instance, when analysing the guardianship orders issued by the court of Midden-Nederland, four out of five cases concern a guardianship that was issued due to a mental or physical condition. In these four cases, the phrasing used is identical. The same holds true for the guardianship orders issued by the court of Noord-Holland; their phrasing of this first component is identical. Even in the largest available sample stemming from the court of Zeeland-West-Brabant, an identical phrasing was used in 87% of all formulations falling in this first component. By contrast, the largest degree of variation was observed in the guardianship orders of the court of

Haarlem, whereby four out of the six court orders were phrased (almost) identically, with minor differences in punctuation.

With regard to the second component, which can solely be found in seven guardianship orders issued by the court of Zeeland-West-Brabant, more variations exist. This has two reasons: first, there are different reasons that have led to the guardianship, which necessarily cause differences in phrasing, and second, in two cases, guardianship was combined with mentorship, which equally influenced the phrasing.

A similar variation can be observed in the phrasing of the third component concerning the appointment of a financial guardian. All information belonging to this component contains at a minimum two text modules: 'the appointment of at least one financial guardian' and 'the name of the financial guardian(s)'. At this level, variations in phrasing occur when formulations were broad enough to accommodate the possible appointment of more than one financial guardian, which occurred in three cases, and when mentorship was installed in addition to the guardianship (which occurred in ten cases). Further variations included the adaptation of the grammatical gender of the term 'financial guardian' by using its female form, the specification that the appointment as financial guardian was of a temporary nature, as well as the use of the more precise description 'protective guardian' (*beschermingsbewindvoerder*), to indicate the specific type of guardianship installed. In addition to this standard set of information, some guardianship orders contained personal information of the financial guardian. In almost half of the cases, the address of the financial guardian was added. Depending on whether the financial guardian was a natural or legal person, this address was the home address, the correspondence address, or the postal address. Furthermore, in two cases, the date of birth of the financial guardian was included and in one case, an indication of the family relationship of the financial guardian with the person placed under guardianship was included.

Variations equally exist within the fourth component, the remuneration of the financial guardian*,* where significant variations can be observed across courts. For instance, while some courts, such as the courts of Midden-Nederland, Limburg, Haarlem, and Overijssel simply refer to the legal act that establishes the remuneration of trustees*,* financial guardians, and mentors, the courts of Noord-Holland and Zeeland-West-Brabant instead refer to an actual sum of money. Furthermore, variations again occur when guardianship is combined with mentorship. Yet, on the level of the individual courts, and excluding those cases that also involve mentorship, identical formulations are employed by the courts of Midden-Nederland and Haarlem. The court of Zeeland-West-Brabant also uses identical formulations apart from the exact sum that is granted as remuneration in each individual case.

The phrasing of the fifth component, the annual remuneration of the financial guardian, is remarkable. This is due to the fact that the phrasing is fairly identical

across the three courts (Zeeland-West-Brabant, Limburg, and Noord-Holland) that have included an order on the annual remuneration in (some of) their guardianship orders. Variations concern the reference to the exact legal provision in the respective legal act, which serves as the legal basis for the annual remuneration, as well as the situation in which guardianship is combined with mentorship because of which also the annual remuneration of the mentor had to be established.

Compared herewith, the sixth component, indicating the duty to register the guardianship order in the national Guardianship Registry, shows a much greater diversity in phrasing across the different courts, while it must be noted that for most courts, apart from the courts of Noord-Holland and Zeeland-West-Brabant, only one guardianship (if any) could be found that included this component in their dictum. Yet, the analysis of the guardianship orders issued by the courts of Noord-Holland and Zeeland-West-Brabant revealed that on a court-by-court basis, the phrasing is identical.

Concerning the seventh component, the duty of the financial guardian to submit an action plan, conclusions on its phrasing could not be drawn, given that this component was included in only two guardianship orders, issued by two different courts. The only observation that could be made was that these courts did not use a similar phrasing, which was partly accounted for by the fact that one of these orders also concerned the institution of mentorship.

Last, the eighth component, the entry into force of the guardianship order, was only included in five guardianship orders issued by the court of Zeeland-West-Brabant. Therefore, it is impossible to determine whether variations exist across courts. Within the given sample, three orders concern the additional installation of mentorship. The eighth component in two of these orders was identical, while the third showed a slight variation, which was caused through the addition of an article before 'mentorship' and which in turn led to a different conjugation of the verb. The remaining two orders, which solely concerned the installation of guardianship, were phrased identically.

To sum up, the foregoing analysis of the variations occurring in the phrasing of the individual components show that variations exist with regard to almost all components. The fifth component is an exception to this general conclusion, because the phrasing was almost identical across the different courts. On a court-by-court basis, and to the extent with which this can be established on the basis of the given sample, it can be generally observed that courts (especially the court of Zeeland-West-Brabant) are fairly consistent in the phrasing of the individual components. To our knowledge, judges within a given local court do not make use of readily available templates or other standard reference works that could account for that consistency, although it is possible, or even likely, that they copy-paste or otherwise recycle phrases used in prior decisions made by themselves or by direct colleagues. Variations are often accounted for by substantive differences (such as the varying reasons that could lead to the placement under guardianship) and

connected herewith, different legal bases. Another main reason for variation was the combination of guardianship with mentorship.

5. Discussion

Based on the analysis, several gaps between the legal, the technical, and the applicability perspective can be identified. A first gap concerns the interpretability of the rights and duties. Every right or duty in a decision-credential must be stated in such a way that it is actually useful in practice. This requirement is difficult to be met, because it entails a mapping of rights and duties that are often phrased in a generic way onto concrete situations they are to be applied in in practice. Such a mapping may not be trivial, in which case a 'translation step' may be necessary that consists of some (trusted) party taking a decision-credential with generic rights and duties, and issuing much more specific credentials that are based on the contents of the decision-credential and other, context specific information. For example, suppose the decision-credential states: '[the guardian] has the right to control the finances of [the dependent]' (where the term within square brackets is a role, i.e. a placeholder for the real-world entity that fulfills that role). This may need to be converted into a set of more concrete statements, e.g. '[the guardian] may access and transfer funds out of any bank account for which [the dependent] is (one of) the account holder(s)', '[the guardian] may void any contract that [the guardian] has committed to'. However, such a translation step requires interpretation of the generic rights and duties that come with the decision-credential, which comes with uncertainty and possibly liability by the interpreter, considering that the party that relies on the content of a credential is commonly not the one that issues it (and defines its content). In addition, guardianships are not easy to operationally handle if they can be tailored to the specific needs of the dependent. For example, a person that is insufficiently capable to manage his/her own finances may be appointed a guardian that oversees such finances and gets the duty to do all major transactions, but a specific arrangement can be made that enables the dependent to spend small amounts of money to a capped maximum. While it would be simple to handle this particular case, it is the wide variety of these simple features that make it all unmanageable to operationally implement.

A second challenge concerns the heterogeneity with respect to how the decisions are worded. The analysis of court decisions reveals that the differences in phrasing and the different sequences seem rather insignificant for humans, legal experts in particular, yet not for machines. Natural language processing and machine learning techniques may correctly classify a large number of sentences or certain types of phrasing under one of the eight components derived from the case law that was analysed, although this is unlikely to be achieved with 100% accuracy. This is an important limitation, considering that particularly false positives can erode trust in the technology and trigger reputational damage or even liability. Moreover, the

number of components might increase with a larger body of court decisions, and courts may introduce more components over time, making the classification models incomplete, unreliable, or not more efficient than a manual (human) verification of the content that would go into a credential.

An alternative to natural language processing is a rule-based approach where courts select the rights and duties from a predefined (but adjustable) list in a predefined form. Differences in court orders may be resolved by the use of orders that allow judges to select which of the predefined components should be included in the decision. One may distinguish between mandatory and optional components in order to ensure machine-interpretability while maintaining flexibility for courts when drafting their decisions. The fact that different courts produce different court orders is not a problem from a legal perspective. A basic requirement for all court orders (or other products) is that it must be fit for use, i.e. it must include the information that may be needed in the various contexts in which it is to be used. If a court order does not specify the reasons that underlie the guardianship, and the order does not need to be used in any circumstance in which such reasons play a role, differences should not be an issue.

Neither issuers nor verifiers are incentivised to bridge the gap between current practice and what is computationally necessary in order to properly detect and process the orders in a way that the order becomes machine-interpretable with 100% accuracy. A solution might be to introduce a third party, such as a notary, whose business objective is to 'translate' credentials that are issued by the judicial system (e.g. courts) into credentials that are tailored for very specific uses. Unfortunately, the introduction of a third party will introduce transaction costs that are unlikely to be covered by the guardian (on behalf of the dependent) or the court. Banks could be interested in this solution, yet it is not clear whether the investment in guardianship credentials will be offset by the savings as a result of automating the process of mandating guardians to control the assets of the dependent.

The third challenge concerns the verification of the credential. In the case of a (new) guardianship, guardians can only successfully login if they are already a customer of the bank (i.e. have a login account, which they may need to create if they do not have one). Then, they must request that the login account be granted access rights to the bank account(s) of the dependent, as per the guardianship decision. Procedures for this vary across banks, and it can be cumbersome finding out what the banks need, how to upload documents (e.g. the decisions), which bank officials need to first validate and then decide what rights should be associated with the guardian's login account, etc. Moreover, bank officials need to be instructed regarding how to validate the various documents, and what arguments to use for deciding to assign the various rights. In addition, the IT systems that provide access to the bank accounts must cater for the various rights involved. Such instructions must be created in such a way that the officials will act in compliance with the applicable laws and regulations. Similarly, the rights in IT systems must have the

effect that when assigned to a login account, its right-holder will be able to exercise them as intended by such laws. It is well known that making such instructions, and adapting IT, can take quite some time and considerable (overhead) costs. In addition, it requires knowledge of the law – not particularly the core business of banks.

Given these observations, a guardianship credential whose contents accurately represents a (guardianship) decision by itself is unlikely to provide much benefit for a bank. We would expect that this analysis is similar for other financial organisations, health organisations, governmental bodies, and in various other contexts, also in other jurisdictions than the one analysed in this article. However, not all is lost. A solution that closes the gap between the 'high-level' credentials that represent a guardianship verdict and the 'low-level' credentials that represent specific rights for its holder in specific contexts (such as banks) could be the involvement of a trusted third party, such as the notary. The idea is that notaries and banks can collaborate to specify the structure of a credential that allows specific rights for a guardian to be expressed for the particular banking contexts. Notaries could be tasked to issue such credentials to guardians, on the basis of a guardianship verdict. Banks would only need to adapt their IT to accept such credentials, which is not expected to be a difficult or costly task. The question, however, remains whether the benefits of SSI credentials outweighs the costs of the additional involvement of a trusted third party.

Future work should explore this, and other ideas, further. The European Commission is currently revising the eIDAS (electronic IDentification, Authentication and trust Services) regulation,[21] as a result of which EU Member States will be required to provide so-called 'wallets' to their citizens that they can use to identify and authenticate, for example by means of credentials. Larger organisations, including banks, will be required to accept such wallets when citizens choose to use them. This may turn out to be instrumental, as it could provide the infrastructure on which such solutions could thrive.

6. Conclusion

In this contribution, we explored what is required to apply SSI in the context of financial guardianship, what is characteristic about the gap between the practical (legal) and technical perspective, and what needs to be done to overcome the challenges. Interestingly, even in a use-case that we, at least from a legal perspective, considered to be one where SSI has a high probability of being

[21] See "Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL amending Regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity".

successful, we identified gaps that question the current usefulness of SSI in the context of financial guardianship. The interpretability of the rights and duties that come with a SSI credential for court decisions on financial guardianship, the heterogeneity of the rights and duties defined in those decisions, and challenges in the verification process raise doubts as to how feasible SSI currently is in the area of financial guardianship. The need for the involvement of different types of stakeholders and the likely investment without a clear return-on-investment disincentivises experiments with SSI.

A solution that closes the gap between the 'high-level' credentials that represent a guardianship verdict and the 'low-level' credentials that represent specific rights for its holder in specific contexts could be the involvement of a trusted third party, such as the notary. The current revision of the eIDAS framework by the European Commission may provide the digital infrastructure for this, but additional work is needed to explore this further.

Annex

Figure 4 - Possible Guardianship Credential (in Dutch)


```
{ "bewindvoering": {
        "onderbewindgestelde": {
                "geslachtsnaam": "geslachtsnaam cfm BRP",
                "voornamen": "voornamen cfm BRP",
                "geboortedatum": "geboortedatum cfm BRP",
                "geboorteplaats": "geboorteplaats cfm BRP",
                "geboorteland": "geboorteland cfm BRP",
                "geslacht": "geslacht cfm BRP"
        },
        "goederen": [ <lijst van goederen die onder het bewind vallen> ],
        "redenen": [ <lijst van redenen ….> ],
        "bewindvoerder": {
                "geslachtsnaam": "geslachtsnaam cfm BRP",
                "voornamen": "voornamen cfm BRP",
                "geboortedatum": "geboortedatum cfm BRP",
                "geboorteplaats": "geboorteplaats cfm BRP",
                "geboorteland": "geboorteland cfm BRP",
                "geslacht": "geslacht cfm BRP"
        },
        "beloning": {
                "initieel": "<bedrag in EUR dat…>",
                "maandelijks": "...",
                "jaarlijks": "..."
        },
        "inschrijving": "verklaring waarin de verplichting tot inschrijving van de
```

bewindvoering in een register wordt gespecificeerd”,
“actieplan”: “verklaring waarin de verplichting tot opstelling en registratie van een actieplan wordt gespecificeerd”,
“inwerkingtreding”: “verklaring …..”
}

{ “bewindvoering”: {
“onderbewindgestelde”: {
“geslachtsnaam”: “Puk”,
“voornamen”: “Pieter Jan”,
“geboortedatum”: “01-01-1966”,
“geboorteplaats”: “Waterlandkerkje”,
“geboorteland”: “Nederland”,
“geslacht”: “X”
},
“goederen”: [“alle goederen waarvan [onderbewindgestelde] eigenaar is of zal worden”],
“redenen”: [“Piet is geestelijk onbekwaam om zijn financiën te regelen”],
“bewindvoerder”: {
“geslachtsnaam”: “van der Kluns”,
“voornamen”: “Catharina Amalia”,
“geboortedatum”: “01-01-1966”,
“geboorteplaats”: “Waterlandkerkje”,
“geboorteland”: “Nederland”,
“geslacht”: “V”
},
“beloning”: {
“initieel”: “100”,
“maandelijks”: “50”,
“jaarlijks”: “400”
},
“inschrijving”: “verklaring waarin de verplichting tot inschrijving van de bewindvoering in een register wordt gespecificeerd”,
“actieplan”: “verklaring waarin de verplichting tot opstelling en registratie van een actieplan wordt gespecificeerd”,
“inwerkingtreding”: “verklaring …..”
}