A Framework for Self-Sovereign Identities

Rieks Joosten {rieks.joosten@tno.nl}

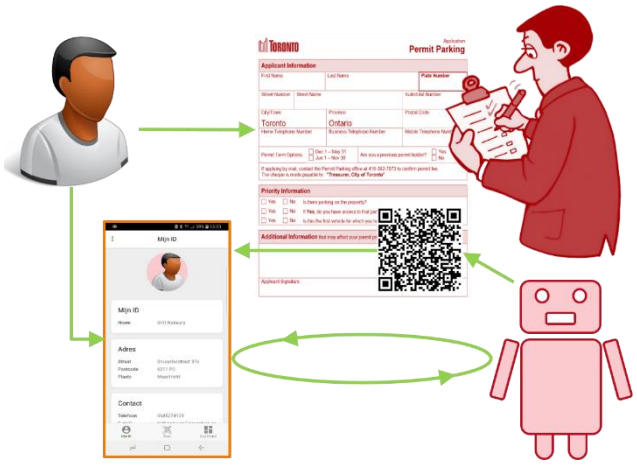
The ability to electronically exchange (personal) data has long been recognized as a key element in administrative processes and conducting business transactions electronically. At the same time, it is acknowledged that such data must be trustworthy, that it has not been altered, that it does not get stolen, that privacy is respected, and so on. Over the last years, the term 'Self-Sovereign Identity' (SSI) has increasingly been used to refer to these properties. So currently, many (technical) SSI solutions exist, and new ones are being developed.

While all of them can show their benefits in one or more use-cases, we are currently far from the situation that such solutions can be used in a generic fashion. One of the causes is that the solutions tend to be quite technical, and do not address business requirements. In order to bridge the business-technology gap, a comprehensive model is called for that we can use to describe the business (i.e. electronic business transactions, legal stuff etc.) and the technological infrastructure in which the SSI solutions have their place. This document is an attempt to come to such a model.

Introduction

Where Self-Sovereign Identity (SSI) is commonly seen as a technical innovation, we are focused on its applications. Perhaps the most important is the electronic filling in of administrative forms.

Here is one of many examples: if you had an accident and require a parking permit for the disabled, , you have to go through various administrative processes of different organizations (municipality, health-insurer, etc.). Often, this means you have to fill in the same data, or that you need a certificate from a specialist stating your medical condition, which you somehow need to get in an electronic (PDF) form and upload to the site of the organization. This may take a lot of time (weeks, sometimes months). It is annoying and frustrating for the consumer, and costly for the parties who have to validate these forms, i.e. check whether the provided data can be trusted in such a way that it can be decided to / do not allow the wheelchair. We estimate that every year, Dutch organizations (companies, government) spend more than 1 billion euros on validation alone.



With SSI we envisage that users get an SSI app on their mobile, that organizations expand their websites with an SSI component, and that they design their (electronic) forms differently – as shown in the adjacent figure.

Here is how it works: the form shows a QR code that can be scanned by the SSI app, which can then 'find' the SSI component of the organization (depicted as a robot). They then 'negotiate' with each other about the kinds of data that should be provided, the assurances that should be given regarding the truth of such data, and more. Assurances consist e.g. of

attestations, data that is signed by a party that the organization trusts, proofs that the data has not been tampered with since it was signed, etc. At the end of this ‘negotiation’, both the SSI app and the SSI component have trustable information that allows them to decide about whether or not to proceed (e.g. issue the parking permit).

In the negotiation phase, both the app and component can tap into their private ‘attestation store’ or wallet, which holds attestations that have been obtained earlier. However, attestations that are required but not available in such a store may be acquired in (near) real time. Thus, the consumer can collect the required information in a matter of seconds / minutes rather than weeks or months. Organizations are now receiving quality data that have been digitally certified by parties they trust, so that validation is not only much faster, but also much cheaper. They can then make faster and better decisions.

The advantages are countless: we already talked about a considerable acceleration of completion and decision making, and about the major cost savings of validation. But there is more: it often happens that consumers do not understand the language in the form, or where they have to get the data from. This frustration, which can lead to 'giving up', can be largely annulled.

Also in the question-and-answer game between SSI app and SSI component other data can be exchanged: the component can tell what the data will be used for (the 'target binding' of the GDPR) the app can keep track of which permissions are given for the processing of personal data, etc . In short: SSI facilitates the exercise of your rights that the GDPR grants you.

Other advantages are use-case specific. A large health insurer with whom we have done some experiments thinks that if GP systems become SSI-aware, the administrative burden will be reduced so that they can spend 20% more time on their patients during a consultation. They also think that far fewer mistakes are made with declarations. Together with the generic benefits, this can be a significant contribution to reducing healthcare costs.

SSI is not yet ready for a large scale roll out. One set of reasons revolves around technology. There are more and more SSI technologies, but at the time of writing, they are not interoperable. We still have to learn how exactly they fit into the picture and how they can then work together. We also need to know more accurately what we expect from an SSI app: what should he do, and what not? How can an app and a component of the other know that they are genuine SSI apps / components?

Another set of reasons is that organizations will need to make their processes and forms 'SSI-aware'. They have to decide which data the consumer must fill in and which ones by the app (for example because it must be attested). This requires decision-making: which parties do I trust in such a way that I can use the data they certify for the decision that I take? They also have to decide whether they want to certify the data they themselves produce for use in third-party transactions: for example, a health insurer must decide whether to make an attestation for insured parties, which includes the relationship number and the type of policy (s) that they or the type of care for which they are insured.

One of the things we need is a safe environment that allows organizations to test and demonstrate their business processes as well as various technologies, so as to develop and validate their own individual business cases, and also to demonstrate what this looks like. The latter is important to arouse interest with parties that are not the fore-runners, but that are instrumental in making SSI a success. TNO in Groningen has started with what is called the SSI-Lab, where SSI does not stand for Self-Sovereign Identity, but for Self-Sovereign *Integration*. The lab is a link between organizations and technologies (you could call it an eco-system) that share the SSI vision mentioned here and in one way or another want to contribute to realizing it.

Another thing we need is a thought model that will help us talk to one another – i.e. all of us different organizations – in a meaningful way. That is to say: that we can determine when we are not talking about the same things, and find a way to become congruent in our discussions.

This document is an attempt to specify such a thought model. This model, which we call ‘Self-Sovereign Identity Framework’ or SSIF, provides a terminology that allows us to precisely model the electronic business transactions of which we have provided an example in the previous paragraphs. It also provides terminology to talk about process- and technology-related topics, as well as their integration. As such, we intend it to be a conceptual model onto which we can map (almost) all technology-specific lingo, enabling us to consistently and coherently discuss their integration.

As with any model, we start by providing the set of assumptions (axions) that we use, and the related terminology. From there, we will further construct the model and develop the necessary terminology. We do not think that this is complete yet; however, we think it is a useful first step.

When developing the terminology, we try to specify definitions in terms of criteria that English speaking people that are interested in SSI are expected to evaluate in the same way. For example, we It is these criteria that are important to us – we do not (really) care about the name we give to whatever satisfies such criteria.

Parties, Knowledge and (Business Transactions)

Let us consider an entity that (a) continuously collects, stores and disseminates information, (b) decides itself what it considers to be valid reasoning/logic, (c) uses this logic to process information that it has, thereby generating new information, and (d) is capable[1] of doing[2] all that in a self-sovereign fashion, i.e. independent of other entities. We will use the term '**party**' to refer to such entities. Typical examples of entities are humans, and organizations.

In our way of thinking, the universe is populated with parties that interact with one another in a self-sovereign fashion, which we take to mean that each of them decides for itself with which other parties to interact, and how to interact with them. Also, we assume that every party acts in a selfish (or self-centered) manner, i.e. for its own benefit[3].

When a party interacts with another party, it uses its (subjective) knowledge for various purposes. First, it uses its knowledge to decide what kinds of information to convey to that other party[4]. Also, it uses this knowledge to interpret data/messages it receives from that other party, to reason with the existing and received information[4], and to decide how to proceed in the interaction. Since the knowledge of a party is subjective, i.e. it differs from one party to another, it is obvious that interactions between different parties will be conducted in a different manner, even if such interactions are of the same kind (e.g. renting a car). We need to understand (the cause of) such differences if we want to electronically support parties as they interact with one another.

We introduce the term '**knowledge (of a party)**' to refer to the information that this party has (either because it was collected, or it was generated by means of reasoning). The knowledge of a party explicitly includes its 'business logic', i.e. the information that it uses for reasoning purposes, and for making decisions. Since every party has its own unique history, perceptions and experiences, we must assume that its knowledge is equally unique – in other words: highly subjective. We assume that the knowledge of a single party is consistent, by which we mean to say that the information it has about itself and the world it lives in makes sense – given the business logic that it applies. Of course, other parties may judge this knowledge of to be inconsistent, but that would then be because they do not use the same business logic.

Interactions between parties can have many forms, of which (electronic business) transactions is a form that is of particular interest for SSI. Using the definition provided by the Merriam-Webster dictionary with a slight modification, we define `**transaction**` as an `exchange or transfer of goods, services, data, or funds`.[5] When a transaction is conducted by (or on behalf of) parties, we classify it as a `**business transaction**` and will refer to each party as a `**participant (of the (business) transaction)**`. The properties that parties have of being both selfish and self-sovereign, lead us to postulate three (selfish) criteria that we assume every party to evaluate, either explicitly or implicitly, before committing to a proposal for a business transaction:

---

[1] The fact that an entity has this capability does not imply that the entity would actually use it.

[2] Further down we will see that some entities that qualify as parties according to this definition, such as organizations, cannot do anything themselves, and also how we can still sensibly interpret phrases that state that they do.

[3] Cialdini et. al. have shown that even so-called 'selfless' actions, e.g. empathy-based helping, can be interpreted 'egoistically', its benefit being that helping reduces the levels of feeling bad.
Cialdini, R. B., Schaller, M., Houlihan, D., Arps, K., Fultz, J., & Beaman, A. L. (1987). Empathy-based helping: Is it selflessly or selfishly motivated? *Journal of Personality and Social Psychology, 52*(4), 749-758. http://dx.doi.org/10.1037/0022-3514.52.4.749.

[4] For readers that like to clearly distinguish between information and data: this includes deciding how to convert between information and data so that it can exchanged in a communication with another party.

[5] Merriam-Webster does not have the 'data'. The Oxford dictionaries stick to `An instance of buying or selling something`, and do not specify what is being bought or sold. The Cambridge dictionary has a lengthier definition, but adds little further (if anything at all) to the previous ones.

1. **clear contract**[6]: the proposal must provide the party with sufficient certainty about its obligations (i.e. what it is going to give/provide), and its expectations[7] (i.e. what it is going to get in return)[8].
2. **net profit**: the *value* of what the party perceives it is going to get must exceed the *value* of what it has decided it will give in return.
3. **acceptable risk**: the party has decided that the level of risk involved in committing to the transaction is acceptable[9].

Thus, a business transaction starts with parties negotiating a contract, i.e. a set of mutual expectations and obligations for the purpose of exchanging goods, services, data or funds between them, in such a way that both of them subjectively profit from that exchange. As soon as every participant has subjectively concluded that all of the above three criteria are fulfilled, they commit to the transaction and start to execute it, meaning that each will provide the other with what was agreed within the agreed constraints (e.g. delivery time, quality, payment, etc.).

During or after this execution phase, participants may continue to converse, e.g. request/report on the progress of the execution, negotiate amendments on the committed-to agreement, etc., which may cause new transactions to be negotiated or disrupt the transaction being executed. Given that each party communicates from its own knowledge, we must expect misunderstandings and disagreements to regularly occur. Also, we must expect cases in which such miscommunications cannot be resolved by the participants.

In such cases, participants need external help to sort things out. One way to do this is that participants anticipate this possibility, and agree to apply a specific conflict resolution mechanism in such cases[10]. But even then, a participant may decide to force the other(s) to accept a particular 'solution'.

[6] A contract can both be tangible, e.g. on paper, or intangible, e.g. an understanding that a participant has.
[7] For humans, this may include moods, feelings, and experiences: for example, if a person may expect to 'feel thrilled' as a result of the proposed transaction, this will be taken into account as (s)he evaluates this criterion.
[8] Obligations and expectations not only pertain to the goods, services, data or funds of which the exchange is proposed, but also to measures that participants need to be in place for the purpose of reducing the risks that are associated with the transaction to an acceptable level.
[9] When deciding about what level of risk is acceptable, it usually takes the expected net profit into account.
[10] For example, participants may agree to bind themselves to the judgement of a specific court.

Actors, Agents And Electronic (Business) Transactions

Every party has objectives and realizing them requires that party to accumulate and maintain relevant knowledge, and to do whatever is necessary. However, not every party is physically capable of actually doing so. Organizations, for example, are incapable of doing things (acting) themselves. They need entities such as machines or humans to do that. We will use the term `**actor**` to refer to an entity that can act (do things). Note that the terms `party` and `actor` are disjunct: a video camera for example is an actor because it can register video images, yet it does not qualify as a party. We have seen that organizations generally qualify as a party, but not as an actor. Humans qualify as both.

While organizations cannot act, it is easy to find statements that state the opposite. An example of this is the phrase 'TNO has made a significant investment in Blockchain Technologies'.[11] What is actually meant here is that some actor that represented TNO at that time, decided to invest in blockchain technologies. But even if sentences such as 'The CEO of TNO has invested in Blockchain Technologies' can be ambiguous, even the the CEO is a person and hence capable of acting: the sentence may use 'CEO' as the person that represents TNO, but also as the person that acts on his own behalf – after all, he is also a party.

To resolve such ambiguities, we start by defining the term `**agent (of a party)**` as `actor that represents that party`. Also, in situations where phrases are required to be unambiguous, we will assume that whenever a party that is also an actor is referred to in a sentence, then it is that party/actor itself that acts. If such a sentence mentions a party that is not an actor, in particular: an organization, we assume the existence of an actor that has not been mentioned in the sentence, and it is valid to ask who or what that actor then is, and whether or not this actor is actually an agent of that party.

That brings us to the (difficult) question of how to decide whether or not an actor is an agent for some party. This question is particularly relevant if we want to conduct electronic business transactions, or better: if we – as parties – want to use electronic components such as apps or webservices as agents that represent us in the digital domain. An insufficient ability to decide whether or not an electronic component is in fact an agent of some party may cause electronic business transactions to go sour in the same way as that we suffer from others impersonating us, or misrepresenting us. For the moment, we will leave this question generically unanswered, which means that whenever a party needs to decide about agenthood, he can do so using its own logic and its own assessments – after all, he is self-sovereign.

A final assumption is that parties not only act in a self-sovereign fashion[12], they also act in a selfish (or self-centered) fashion[13], i.e. for their own benefit. An easy example is buying stuff: a party will buy something if its value (at that point in time, for that party) exceeds the costs. Even so-called 'selfless' actions, e.g. empathy-based helping, can be interpreted 'egoistically', its benefit being that helping reduces the levels of feeling bad[14].

(Electronic) Business Transactions

Under the assumption that SSI aims to electronically support business transactions, we need to describe our understanding of the term `business transaction`. We will use the definition provided by the Merriam-Webster dictionary with a slight modification, and define `**transaction**` as an `exchange or transfer of goods, services, data, or funds`.[15] When a transaction is conducted by (agents of) parties, we classify it as a

[11] Found on https://blockchain.tno.nl/tno-and-blockchains/ on December 5th, 2018.

[12] For parties that cannot act, we assume that their agents are instructed in such a way that they that they engage in transactions that serve to further the objectives of the parties they represent.

[13] We do not (want to) pass any judgement; we simply state what anyone can readily observe in the world we live in.

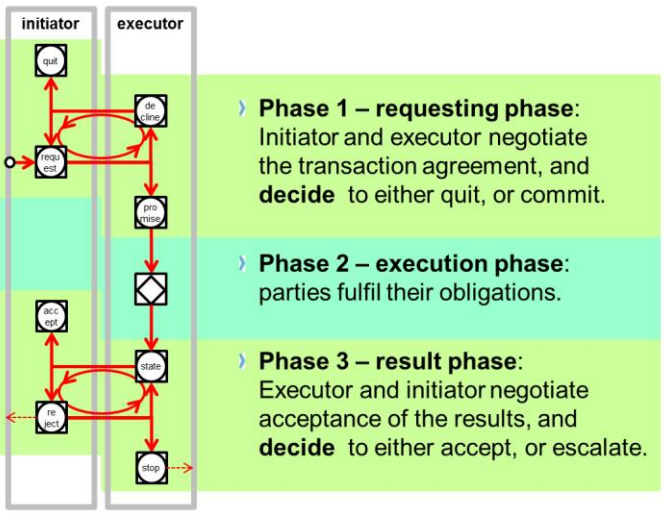
[14] Cialdini, R. B., Schaller, M., Houlihan, D., Arps, K., Fultz, J., & Beaman, A. L. (1987). Empathy-based helping: Is it selflessly or selfishly motivated? *Journal of Personality and Social Psychology, 52*(4), 749-758. http://dx.doi.org/10.1037/0022-3514.52.4.749.

[15] Merriam-Webster does not have the 'data'. The Oxford dictionaries stick to `An instance of buying or selling something`, and do not specify what is being bought or sold. The Cambridge dictionary has a lengthier definition, but adds little further (if anything at all) to the previous ones.

`**business transaction**` and will refer to each party as a `**participant (of the (business) transaction)**`. A business transaction that is (partially) conducted by `**electronic agents**` i.e. electronic equipment that represent the participants of the transaction, will be called an `**electronic business transaction**`.

The properties of being both selfish and self-sovereign, lead us to formulate three (selfish) criteria that we assume every party (agent) to evaluate, either explicitly or implicitly, before committing to a proposal for a business transaction:

4. the proposal must provide the party with sufficient certainty about what it is going to give (which it can decide itself, so that part is always fulfilled), and what it is going to get in return. Note that for humans, this may include moods (feelings, experiences).
5. the value of what the party perceives it is going to get must exceed the value of what it has decided it will give in return; in other words: the party expects a net profit.
6. the party has decided that the level of risk involved in committing to the transaction is acceptable. When deciding about what level of risk is acceptable, it usually takes the expected net profit into account.



Basic Transactions

A business transaction usually consist of several parts, the basic pattern of which is shown in the adjacent figure, and is taken from the Design & Engineering Methodology for Organizations (DEMO)[16]. In its simplest form, this pattern starts with one of the participants (in the role of `initiator`) sending a request to provide a product or service to another participant by one of the participants (in the role of `initiator`) to another participant (in the role of `executor`). This message transfer triggers a negotiation between them, the purpose of which for the initiator is to convince the executor to fulfill the request, while the purpose for the executor is to decide whether or not he should do that. The negotiations continue until the executor decides to fulfill the request, or either decide to quit. If the transaction continues, the executor produces the result (second phase). In the third phase, the result is transferred, and a (often short) negotiation starts of which the golden flow is that the initiator accepts the result.

Note that while this model shows how a buyer (in the role of initiator) may request a product or service from a seller (in the role of executor), it does not show the converse, which is where the buyer pays the seller. This can be included by using a second instance of this model, where the roles are swapped: the seller (in the role of initiator) requests payment for the product or service he will deliver, which the buyer (in the role of executor) may then supply. A business transaction as we have defined it thus consists of multiple instances of the pattern we described in the previous paragraph. Following DEMO terminology, we will refer to such constructs as `**basic transaction**`s.

There are many ways in which basic transactions can be combined to form a business transaction. There is the prepaid model, in which a basic payment transaction precedes the basic transaction in which the product or service is provided. In the postpaid model, the order is reversed.

Depending on what is exchanged in a business transaction, additional basic transactions may be called for. Things are easy when a buyer wants to buy a book in a bookstore: the business transaction consists of two basic transactions that are conducted almost simultaneously: the buyer gets the book and the seller the money. When payment is electronic, additional parties (banks) become involved and additional basic transactions are required. When the business transaction is conducted online, still other parties (transporters) will be involved. In today's world, business transactions are generally a rather complex orchestration of basic transactions.

Electronic Support for Basic Transactions

The importance of the basic transaction model is that it explicitly shows the purpose for which information is being exchanged, which is to decide whether or not to commit to the basic transaction. The context in which a basic transaction lives, i.e. the business transaction of which it is a part, specifies the kinds of business argument (business rules) that the executor may use to decide this.

If a participant of a business transaction assigns an electronic agent as the executor in one of the basic transactions that the business transaction consists of, this electronic agent must be provided with

- the set of business rules that it needs to evaluate in order to make the commitment decision[17]

[16] https://en.wikipedia.org/wiki/Design_%26_Engineering_Methodology_for_Organizations

[17] In the SSIF thought model, we assume that this can be done, even though we are aware of the difficulties this poses in practice.

- specifications that state where the data that is needed to evaluate these rules must come from[18];
- criteria by which it can decide whether or not data is (sufficiently) valid for the purpose of evaluating these rules.

The minimal electronic support for basic transactions therefore consists of the capabilities that allow

- electronic agents in the role of executor to ask for data, and specify criteria by which the validity of such data (within the context of the business transaction) can be determined, and
- electronic agents in the role of initiator to respond to such questions

[18] In a basic transaction, one might say that the data that the executor needs must always come from the initiator. However, we think that it is beneficial to be able to specify that data may (also) originate from other systems, which may or may not use access controls that require the initiator to provide permissions (e.g. by using OAuth).

The Role Of Law

We assume (and emphasize) that all parties are intrinsically free to exercise their capabilities to collect, process (e.g. reason with), store and disseminate information as they see fit. This freedom is not given to people by law, e.g. because Article 9 of the European Convention on Human Rights says that people are free to collect, process and disseminate information. Also, organizations do not lack this freedom because there is no such regulation for them. The intrinsic nature of this freedom is readily observed when reading newspapers: governments, organizations, and individuals can do anything they like, notwithstanding that their actions may cause reactions, e.g. punishment or retaliation.

While laws and regulations do not prevent all anarchy, they are instrumental in limiting it. The phrase “the meaning of a rule/law is the measure by which it is enforced” hints at how this comes to pass. Basically, we can see that groups of parties exist, each of which (a) has a set of rules that govern the behavior of its members and (b) has processes to (i) create/update/delete such rules, (ii) detect violation of such rules and prosecute violators and (iii) pass judgement on violators, i.e. make them suffer the consequences. We will use the term ‘**jurisdiction**’ to refer to such a group. While (national) states are the prototypical examples, enterprises generally also qualify, as will families, sports organizations, etc. As far as we can tell, every jurisdiction that may be relevant for SSI satisfies the criteria for being a party.