ResearchGate

See discussions, stats, and author profiles for this publication at: https://www.researchgate.net/publication/348325716

# Decentralized SSI Governance, the missing link in automating business decisions

**Preprint** · January 2021

DOI: 10.13140/RG.2.2.35491.68640

CITATIONS
0

READS
1,088

**3 authors:**

Rieks Joosten
TNO
**34** PUBLICATIONS **60** CITATIONS
SEE PROFILE

Sterre den Breeijen
TNO
**2** PUBLICATIONS **0** CITATIONS
SEE PROFILE

Drummond Reed
Evernym
**9** PUBLICATIONS **734** CITATIONS
SEE PROFILE

**Some of the authors of this publication are also working on these related projects:**



Self-Sovereign Identity: A Comparison of IRMA and Sovrin View project



Networked Risk Management (NRM) View project

All content following this page was uploaded by Rieks Joosten on 08 January 2021.

The user has requested enhancement of the downloaded file.

# Decentralized SSI Governance, the missing link in automating business decisions

Authors: Rieks Joosten (TNO)
Sterre den Breeijen (TNO)
Drummond Reed (Evernym)

Publication date: January 6th, 2021

Reviewers: Daniel Hardman, Eugeniu Rusu, Jan Lindquist, Jim St. Clair, Kalyan Kulkarni, Kai Wagner, Oskar van Deventer, Sankarshan Dhiway, Scott Perry, Steve McCown, Steven Milstein, Victor Golubkov, Victor Syntez, Wenjing Chu

## Summary

This whitepaper explores a set of related ideas that we collectively refer to as “decentralized SSI governance”. The purpose of such governance is to support organizations as they transform their IT, their business-process artifacts, such as forms, and their policies to reap the benefits of SSI. This paper introduces SSI Assurance Communities (SSI-ACs) and identifies three specific governance topics: credential-types, accreditation and decision tree support. Tools and services are suggested that help with these topics. Furthermore, a distinction is made between what the business primarily cares about (business and business applications), and the technology and other things that are just expected to work (which we call "SSI-infrastructure").

Here are the main takeaways:

- Self-sovereign identity could save time and money on bureaucratic processes (form filling and validation) by automating business decisions.
- Business decisions require governance to ensure the data used for making them qualifies (is valid) for that purpose, and continuously remains compliant with laws, regulations, and company policies (which regularly change).
- Companies could share this governance burden by supporting communities that support the provisioning of SSI-related assurances for their specific purposes.
- Such (focused) assurance communities could be supported by tools like credential catalogues and accreditation credentials.

We hope this paper inspires SSI proponents to develop not only real SSI infrastructure, but also assurance mechanisms for exchanging qualified data.

# Table of Contents

# Why SSI - Saving time and money on bureaucracy

SSI promises big benefits: better data quality, faster and cheaper data validation and decision-making, higher conversion rates and customer satisfaction, less churn, fewer IT-links[1], and operational costs, et cetera.

We estimate that in the Netherlands alone, monetary benefits are over 1Bn euro[2], waiting time for information can be reduced from hours (days, weeks) to seconds (minutes), and many IT-links can be dismantled.

SSI allows individuals to store and exchange qualified data when they want to, making it easier to fill in (digital) forms. This improves the individual's interaction experience with the system. Currently, there are many problems that an individual can experience. Examples are not understanding what is being asked for, where to get the data or documents, and challenges and/or errors when entering data into the form. Moreover, sometimes you need to physically go somewhere to get a (signed) document, or scanning documents and uploading PDFs. The Dutch National Ombudsman has shown that everyone - including people with academic degrees, or lots of IT experience - faces these challenges.

On the other side, organizations can also benefit from the use of SSI. At this moment, organizations need to deal with unqualified data (e.g. typed or uploaded, without any assurances about anything), errors and unsatisfied customers. SSI can provide them with assurances (e.g. regarding the provenance and integrity of such data, required accreditations of the data source, etc.) they need to qualify the data for the purposes they intend to use it.

Indirectly, yet nonetheless important for (some?) governments, is that SSI may help to reduce the 'digital divide',[3] People in lower socio-economic classes tend to find filling in forms more difficult, yet have to fill out most of the forms as they apply for social benefits and support. Typically, these forms are not the easiest to understand. As a result, these people give up, often for very good reasons, and therefore do not get benefits they are entitled to. Moreover, they do not file complaints if things go wrong. With SSI technology as their companion, all this can change.

---

[1] IT-links connect IT-systems that are governed/managed by different parties (internal or external to an enterprise or government). It usually requires the setup and maintenance of a business contract, implementation of 'connectors' to convert data, authentication/authorization mechanisms, and a technical communications channel.

[2] This is a rough estimate that TNO did a few years ago. While there is no solid underpinning of these figures, representatives of various organizations (public notaries, banks, insurers) consent that this is a lower bound. Whether or not the figure turns out to be actually correct is less important than the fact that there is a wide consensus that we're talking big savings here.

[3] Representatives of various governmental bodies in the Netherlands have identified as a concern they take quite seriously.

# The challenge: automating business decisions based on qualified data

While most business decision makers can see the benefits and even want to reap them, acceptance is still an issue. Since SSI is still in its infancy, we would only expect 'innovators' and 'early adopters' to be interested.[4] So what issues are being raised for (currently) not engaging?

First, the technology still is not sufficiently mature. While many vendors are already developing SSI components and/or solutions, they do not yet (easily) interoperate with business applications or SSI components of other developers. Standardized specifications for APIs, credential exchange protocols, and other fundamental processes are still lacking.

Fortunately, these technical issues are being addressed and we expect to see them being resolved over the coming years. As a result, we foresee a generic SSI-infrastructure that is accessible for all (SSI-enabled) business applications, equally pervasive as the Internet IP-infrastructure. The main difference from a business point of view between the two is that the IP-infrastructure can be used to exchange *any* data, while the SSI-infrastructure will specifically be used for providing, requesting and obtaining *qualified* data. This is data that comes with assurances regarding its provenance and integrity, and that can be combined electronically in semantically valid ways.

> *Qualified data*: data that comes with assurances, at least regarding its provenance and integrity, and that can be combined electronically in semantically valid ways.

Second, business managers need to create and maintain the (machine readable) policies for the SSI infrastructure to provide such services. For verifiers, these policies can specify the kind of credentials that are needed for the different business transactions, and the issuers that can be trusted to give certain statements. For issuers, the policies can specify to whom, and under which conditions the party will issue credentials, together with the kind of assurance it is willing to offer to whom. Also, policies could give requirements to holders, on how to use specific credentials, etc. These policies can be hierarchical. For example, small policies of small business need to fit into the bigger policies of the country the business is in.

This puts a burden on business governance processes: creating and maintaining the (machine readable) policies for the issuance, storing, verification and validation of credentials wasn't required before. Reliable processes are required to develop and maintain machine readable policies that are clear, unambiguous, complete, consistent, coherent and precise, as machines cannot deal with incompleteness, inconsistencies, incoherence, impreciseness or ambiguities the way humans (often) can.

Finally, many managers do not want to take the risk of being or becoming non-compliant. This means that the new SSI IT, the processes that use them and all related (digital) policies have to be made explainable to third parties such as auditors (who are expected to have sufficient prerequisite knowledge) and judges (who generally do not).

---

[4] This would be in line with Rogers' Diffusion of Innovations theory.

# Towards SSI Adoption And Transformation

We expect that more organizations will adopt SSI and transform their business processes and IT systems when it becomes easier for them to do so.

For now, let's assume that the technology issues of interoperability, scalability etc. have been addressed, and that SSI infrastructure technology is a commodity, in the same way as the Internet IPv4/IPv6 infrastructure currently is. This would mean a set of standardized protocols exist (analogous to HTTP and FTP) for issuing credentials and obtaining them, for combining credentials from different issuers into a new credential and present that to others, and for requesting such 'presentations' because you need the data.[5] Also, we would see applications from various vendors (analogous to web clients/browsers and servers) that use these protocols in pretty much the same way, but for different purposes. For example, a 'user wallet' would focus on obtaining credentials and constructing presentations upon request. Vendors compete on UX, security, features, etc., but the basic functionality is the same. In a similar fashion, we expect to see components that serve a party's needs for issuing credentials (the 'issuer component'), and components that serve to collect data from different issuers, usually for the purpose of making a decision of some kind (the 'validator[6] component').

Once SSI is a (commodity) infrastructure as described above, organizations will expect it to properly function on a 24/7 basis, just like any other infrastructure (e.g. for energy, transportation, the Internet etc.). They expect to be able to buy devices, appliances etc. that properly work with such infrastructures, and they do not want to be required to know all technical details.

The crucial component that organizations (as well as individuals) will need is what we will call the 'SSI-gateway' (which is a currently non-existent component[7]). Its function is to ensure that data being exchanged is qualified, i.e. the data is valid to be used as business information for the intended purposes. Specifically, it allows businesses to

- provide arbitrary data-sets to others that request them, adding proofs of provenance and integrity in a way that the requesting party can process, thereby making and issuing 'qualified data'. Such qualified data may come in different forms, e.g. as Verifiable Credentials (VC), X.509 attribute certificates, SAML tokens, Attribute-Based Credentials (ABC), OpenID Connect scopes, etc.
- request a data-set, the contents of which is constructed in a semantically valid way from a number of credentials, each of which is provably issued by a party that the business trusts in that, and hasn't been changed in transit. The response to such a request can be used to automatically fill in forms with qualified data that needs no further validation activities.

It helps organizations to reduce the time and effort spent on validating information to the bare minimum. It allows them to focus on the contents (payloads) of credentials, the 'qualified data', rather than the 'envelopes' that the various kinds of credentials specify. This is similar to TCP/IP, the main interest of which is sending and receiving (unqualified) data, without being bothered by the 'envelope' (the IP-header).[8]

---

[5] This is the mission of the Trust over IP stack from the ToIP Foundation. https://trustoverip.org/

[6] This might appear to be the 'verifier component' but it is actually validation. See 'The Validator Perspective" below."

[7] A proof of principle for such a component is being developed in e.g. in TNO's SSI-Lab and further developed in the eSSIF-Lab project.

[8] Extending this analogy, there might well be a business cases for 'SSI-providers', that, in analogy to Internet providers, provide their customers with SSI-gateways (internet routers/gateways) that it can use (after

However, organizations *do* take an interest in, and pay attention to

- the actual (kinds of) qualified data (credential payloads), insofar they may serve purposes of an organization's business or its information processes;
- the kinds of qualified data that the organization itself might create and issue credentials with, insofar that fits with its business strategy/purposes;
- assurances that it needs to designate data as being qualified, i.e. assurances that help mitigate any (unacceptable) risk that the organization perceives to run as a result of using such data in its information processes;
- how to construct arguments using this qualified data, insofar such arguments lead to qualified decisions (i.e. decisions that are based on qualified data) that are relevant to the organization - irrespective of such decisions are to be made by the organization itself or some other party.

Let's look at each of these more closely.

# Three perspectives on qualified data: issuer, validator, and holder

As with credentials, qualified data can be looked at from different perspectives: the 'issuer perspective', the 'validator perspective'[9] and the 'holder perspective'. In the following sections, an explanation is given what these perspectives are and how the different roles can act in a decentralized governance.

## The Issuer Perspective

In its issuer role, a party is interested in creating value from sharing the knowledge it has about (other) entities (people, organizations, or things). Various business models exist for different organizations. For example, a government may decide to create credentials with citizen data (not just name and address, but also marital status and children, data concerning taxes, various permits, ownerships, guardianships, mandates, etc.). This may result in savings on bureaucracy that outweigh the costs of implementing credential issuing.

In order to reap the benefits expected by the business model, issuers should provide data that others will actually use, and do so with proofs of provenance, integrity and perhaps other assurances. This means that the issuer must communicate (advertise) the existence of such data in such a way that others can not only find it, but also decide whether or not that data is beneficial (for *them*) to use. An 'advertisement' not only needs to say 'what' the data is about, but also what its characteristics are (e.g. that this issued data is guaranteed to be 1-1 equal to the registrations of the issuer, unless the credential in which it is contained has expired or has been revoked), the liability (if any) that the issuer is prepared to take, conditions of use, etc.

From the issuer perspective, it isn't all that important what the 'envelope' is in which the data is conveyed, as long as the assurances for provenance and integrity (and perhaps some others) for the data are in place. Verifiable credentials are good, but so are X.509 attribute certificates, Attribute-Based Credentials (ABCs), etc. Parties may want the ability to specify which of these (not) to use, but that's a secondary concern.

---

appropriate 'configuration' (policy specifications)) to provide (issue), store (hold), request and obtain (verify/validate) qualified data.

[9] in the section on the validator perspective it is explained why we do not call this the 'verifier role'.

In short, as an issuer, a party is interested in creating value from sharing knowledge about other entities. A party's "issuer" governance process is concerned with making (and continually reviewing and updating) decisions about e.g.:

- the kinds of qualified data it is willing to provide (what they consist of, what characteristics are to be ensured, liability to take, etc.;
- the kinds of credentials ('envelopes') it is willing to use for providing that data;
- under which conditions such credentials may be issued (e.g. only to a party that is mentioned in the qualified data);
- how all this is communicated: published, advertised and marketed (both in machine-readable and human readable form, for different purposes/audiences).

## The Validator Perspective

In its role as a validator[10], a party is seeking to create value by efficiently obtaining data that is valid[11] for further processing for specific purposes. Such processing includes doing computations with the data, or using it as a value for a variable/placeholder in a rule that needs to be evaluated for the purpose of making some decision. In this document, we will generically think of this as that the party has various 'formulae'[12] that it needs to be processed or evaluated for specific purposes, and doing so requires the 'variables' (fields) of these formulae to be assigned a value.

The validator perspective is about obtaining such data (through the SSI infrastructure or otherwise), determining whether or not evaluation of the formula would be valid if the data were assigned to specific variables (validation), and if so, assign the obtained data to such variables.

Obtaining data through the SSI infrastructure requires that the party first needs to track down which issuers exist and what kinds of credentials they issue, i.e. the kinds of data that they contain, and further characteristics. It is needed to create and maintain a mapping between (fields) from credentials from specific issuers and 'variables' in the formulae that it uses in its business processes. Such a mapping would also include 'validation criteria'[13], i.e. formulae whose variables can be populated by the meta-data of credentials, such the expiration date, and that are used to decide whether or not data from a credential can serve as the value of a variable in the formula. We will refer to such mappings (and their validation criteria) as a 'validation policy'.

Machine-readable validation policies enable generic IT to collect data for populating a formula using the SSI infrastructure, with the guarantee that such data is valid for the purpose in which the

---

[10] in the SSI world, people would expect this to be the 'verifier role'. However, in the Verifiable Credentials Data Model document, 'verification' is defined as "*the evaluation of whether a verifiable credential or verifiable presentation is an authentic and timely statement of the issuer or presenter, respectively. This includes checking that: the credential (or presentation) conforms to the specification; the proof method is satisfied; and, if present, the status check succeeds*". It doesn't say anything about whether or not that statement can be used by a party in a way that is valid.

[11] In the Verifiable Credentials Data Model document, 'validation' is defined as "*The assurance that a verifiable credential or a verifiable presentation meets the needs of a verifier and other dependent stakeholders.*" and subsequently declares it out of its scope, for the obvious reasons that different stakeholders have different criteria for deciding what assurances they require, as they are in different situations and run different risks that these assurances serve to mitigate..

[12] We see a 'formula' something that implicitly or explicitly specifies the transformation between a set of typed data (with names/placeholders to identify the various 'variables') and a result, and is specific for one or more kinds of 'processors'. Example: an (HTML or paper) application form for a parking permit (to be evaluated by a civil servant); this implies the 'transformation' of such data into a parking permit or a rejection.

[13] For example, China requires that an applicant for a visa has a valid (= unexpired) passport that must remain valid for at least X months after the projected visit has terminated. This would be a validation criterion, as it uses meta-data (the expiration date) of the credential (passport).

formula is used. Human-readable validation policies enable the designated employees of the organization to do the same, using other kinds of infrastructure (e.g. Internet, phone, mail, …).

In short, as a validator, a party creates value by obtaining data that is valid for processing in specific cases. A party's "validator" governance process is concerned with making (and continually reviewing and updating) qualified decisions about e.g.:

- the mapping between variables in formulae, and fields from credentials of specific issuers;
- validation criteria for each of these mappings;
- what risks it runs in case the claims made within the credential are not true, and what assurances may be called for in order to reduce such risks to an acceptable level

### The Holder Perspective

In the holder role, a party is seeking to create value by collecting and managing (qualified) data for later use, by itself, or by presenting it to others e.g. within the context of a business transaction. The value comes mainly from the fact that handling such data is done electronically, using the SSI infrastructure, thereby avoiding most of the (costly, time consuming and annoying) problems that people face if they had to do this by hand (as explained earlier).

In the holder role, a party is predominantly concerned with how to respond to presentation requests that it receives from other parties that collect data (for populating a formula) and making qualified decisions. Such requests would state which fields of specific kinds of (possibly multiple) credentials are needed, and might also state the validation criteria. Collecting the requested (meta-)data, wrapping it into a presentation format and 'issuing' it to the requester suggests that the party is actually performing in an issuer role. Note that collecting and presenting data in the requested format does not mean that the data needs to be changed.

However, in this (holder) role a party may also want to know more about the party that it receives presentation requests from, e.g. who it is, whether it is registered as an enterprise with the national Chamber of Commerce, etc, and it may also need assurances. That would mean that it would simultaneously/intermittently also have to perform the verifier role[14].

In this sense, a holder seems to combine both issuer and verifier/validator perspectives. The holder takes the issuer mindset when presenting the asked qualified data, possibly from multiple sources. The verifier viewpoint is taken when a holder checks whether it trusts the validator enough to share the qualified data with.

## Automated decision making requires argument construction

The Issuer and Validator perspectives show that (support for) decision making is one of the important contributions of SSI. We see a decision as "the acceptance of one (qualified) proposition (the conclusion) on the basis of a set of other (qualified) propositions (premises)", according to the (business) logic used by the party that makes the decision. We will use the term 'argument' to refer to the set of premises and the business logic on which the conclusion is based; we use the term both for situations where premises can be evaluated, or (still) contain 'variables', i.e. placeholders that need to be replaced with actual data.[15]

---

[14] some might recognize this as the 'verify the verifier' expression from CCI Use-Case 11.

[15] This is a common figure of speech: we can say "I am going to buy a bottle of wine" and 5 minutes later "I have bought a bottle of wine". In the first case, 'bottle of wine' works as a variable, referring to a still unknown member of a class, and in the latter case it is a value that represents the actually existing element of that class.

A well-designed argument is characterized by the fact that it is as simple as possible for making the decision it is used for. A ‘qualified argument’ is an argument that comes with (specifications for, or the actual) assurances that a party needs to reduce the risk of making an erroneous decision to an acceptable level.

> *Qualified argument*: Argument of a party that comes with (specifications for, or actual) assurances, such that the risks this party runs when using the result of evaluating the argument, are acceptable within the context of such use.

Designing and establishing the policies that specify which arguments are to be used for what kinds of decisions is perhaps *the* core element of a party’s governance. Such argument specifications can take the form of a tree, where the root-node represents the final conclusion, and other nodes represent sub-arguments that their parent node combines using a function such as ‘AND’ or ‘OR’.

This breaking down of the argument in sub-arguments, in a tree-like structure, makes its governance more manageable. For example, deciding whether or not a person should be given access to some digital service may be broken down in an argument for deciding this in case the person is an employee and the case in which (s)he is a customer.

## Arguments for automated decision making require governance

The governance of arguments may be done in a distributed fashion, meaning that the task of establishing some (set of) sub-arguments can be assigned to the people that are best suited for that. For example, the basic argument to decide whether or not someone may access a particular bank-account might be “authenticated person owns bank-account”. There may however be legal situations in which someone else should also be given access. This can be done by introducing “authenticated person has a legal right to access bank-account”. We leave the governance of the argument that establishes whether or not this is the case up to the legal department.

The ability to break down arguments and distribute their governance can also help mitigate the risk of making wrong decisions. In high-risk situations, the governance of specific sub-arguments can be delegated to (e.g. risk and compliance) officers that have the skills to construct these arguments such that they provide the necessary assurance to reduce the risks to an acceptable level. An example is given in the section ‘Tools and Services That Support Decision Making’

For completeness sake, we mention that a distinct part of the governance of arguments is the specification of the assurances that must be in place for data to qualify as valid for the position where it is applied in the argument. This has already been covered earlier, when we discussed validation policies. Basically, qualified data (for some argument) is data that comes with the assurances that are specified in the appropriate validation policy.

## Arguments for automated decision making require assurances

Assurances can be all sorts of things, as long as they contribute to the mitigation of risks of parties that make decisions. A party that wants to sell a house needs assurances that enable him to sue the buyer in case he doesn’t pay. A proof of the buyer’s identity that is acceptable to the courts in which he may sue that person would be an example of such an assurance. Another kind of assurance would be a downpayment.

Note that assurances are subjective. Something that would provide you with assurance in a certain case may not do so for me in that case.

For SSI, we have specific things that might serve as assurance. One such thing is cryptographic proofs. One can use such proofs e.g. to establish the integrity of a credential (i.e. that it hasn't been changed since it was issued), or its provenance. Also, such proofs may be used to establish links between credentials, and much more. Good cryptographic proofs have a solid mathematical basis that gives them the property that they cannot be denied.

As is in the name, the SSI-ACs care about assurance between the parties that are part of the community. The parties can decide for themselves what assurance means for them, what kind of credentials are needed, and how they want to express this. A possibility for expressing this is a 'Level of Assurance' or LoA. A LoA can be an integer in the range of 1-4 or 5, which identifies a set of (objective) statements that allegedly apply to some situation or equipment, where these statements are designed to provide assurance. LoAs are typically claimed by one party, within a certain context, and such statements can be trusted by other parties, just as any other claim. Examples of how LoAs are currently used, are the NIST 800-63, that provides levels of assurance for identity proofing (IAL), authentication (AAL) and strength of an assertion in a federated environment (FAL), and the ISO/IEC 29115, that provides a framework for managing entity authentication assurance, including 4 LoA's (for entity authentication).

In general, a statement can be (part of) an assurance for a specific party if this party can use the statement to contribute to risk mitigation. SSI allows us to request any statement, including assurance statements that are needed for decision making.

For example, a party that is electronically negotiating a transaction with another party, and that wants to mitigate the risks of that party using a rogue digital agent, may request an accreditation credential (issued by a well-known/trusted accreditor) that states the set of security requirements that this agent satisfies.

There is a business in providing credentials that contain statements that are valued in the market as providing assurance. For example, it is conceivable that a party runs a digital service that allows digital agents to be registered when installed, and that at a later time can remotely test the digital agent for any (rogue) modifications, and issue an (ephemeral) credential stating the results of such checks. If properly designed and implemented, such services may contribute significantly to the uptake of SSI, particularly if they also were to take on some liability in case things go wrong.

# Outsourcing assurance to SSI Assurance Communities (SSI-ACs)

The difficulties that the governance of information processes bring along, particularly when the result of such processes should be (digital, machine-readable) policies and regulations that are fit for use by computers, is a major obstacle for organizations to adopt SSI, and transform their business processes and IT. This is nothing new. Since computers have been used by businesses, the existence of this business-technology gap has been recognized, and people have tried to come to grips with it.

This document proposes several additions to the tools that have up till now been used for this. These tools assume the existence of an operational SSI infrastructure. Also, they capitalize on existing mechanisms for providing trust and assurance by observing that trust and assurance work best in a

community of parties that have some common objectives, and because of that, find it more beneficial to work together in some areas than having to do all the work themselves.

They do not seek to provide rules/standards that should be followed world-wide, but rather they consent to a set of rules that they can all work with, for the particular purposes that they share and the concerns they collectively want to address. They will often allow others to join if they find that beneficial. We will use the term 'SSI Assurance Community' or SSI-AC to refer to such communities.[16]

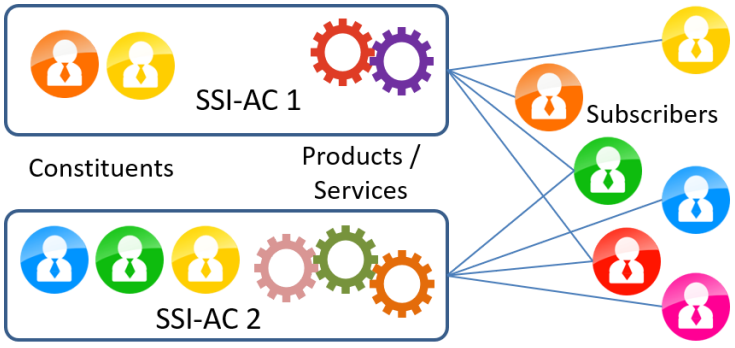


Figure 1: Constituents and Subscribers of an SSI-AC

An illustrative example of such SSI-AC could be the Dutch "Outbreak Management Team" (OMT) that consists of people from the National Institute for Public Health and the Environment, research institutions, medical societies, etc. The OMT is a standing organization, that only convenes when "existing scenarios offer too little guidance" (to government, the public, or enterprises regarding the ways in which to behave in situations with specified health risks) in the outbreak of an infectious disease. It is their task to propose additional guidance for specific situations. In the current COVID-19 crisis, their advice to the Dutch government deals with what citizens should (not) do, what kinds of enterprises are to be temporarily shut down, etc. This task makes them ideally suited to also become a SSI-AC that specifies the necessary SSI support that organizations and citizens need, e.g. the kinds of credentials that citizens should be issued after having been tested, accreditation credentials for trusted testing facilities, etc.

A SSI-AC is constructed and maintained by (representatives of) organizations - which we will call its 'constituents' - which perform the governance. They specify its scope (what (not) to consider), the products and services that the SSI-AC will govern (and perhaps also realize) for the purpose of facilitating organizations to obtain assurances and build or maintain trust.

A SSI-AC may typically provide products and services that organizations need to adopt SSI and transform their business processes and IT, such as:

- Credential Type support, e.g. in terms of specifying their structure and semantics, supporting the advertisement of such specifications and the searching/finding of them;
- Accreditation support, e.g. in terms of maintaining lists of 'trusted issuers/verifiers/holders', specifying accreditation schemas and providing for the issuing and use of accreditation credentials associated with such schemes,
- Decision-Tree support, e.g. defining arguments for certain types of decisions, specifying validation policies for the data that such arguments need, providing a service that can push updates of such arguments and validation policies to subscribers, and perhaps even a generic (locally deployable) service for the evaluation of such arguments in given contexts.

[16] The term "SSI-AC" roughly corresponds to the combination of what the Sovrin Glossary and ToIP call a governance authority (SSI-AC Constituents) that serves on behalf of a trust community (SSI-AC members). What we propose in this paper is a more generalized form of this concept that goes into more details.

Organizations that use products and/or services of a SSI-AC are called ‘subscribers’. Organizations are self-sovereign in deciding which SSI-AC(s) to subscribe to. They may want to subscribe to multiple SSI-ACs.[17] We use the term ‘SSI-AC member’ as a party that engages with the SSI-AC, either as a constituent or a subscriber.

We like to think of a SSI-AC as a service-oriented community that has a limited focus, such as in the example of the Dutch OMT, exists for the benefit of its members, and realizes that it is just one of many such communities. The latter means that a SSI-AC may decide to become a member of another SSI-AC, reaping the benefits associated with that SSI-AC. For example the Dutch OMT may decide to become a constituent of some European Covid-19 SSI-AC, together with similar SSI-ACs from other EU countries. There, they could support credential types, accreditations and decision-tree support that would allow e.g. for EU cross-border use of credentials as they are governed by the different constituents.

In other words, a SSI-AC is a formal or informal, temporary or persistent organization that consists of different constituents (individuals, enterprises, governments) whose task is to at least govern[18] the SSI-AC (and optionally providing one or more of the products/services that it governs). This includes:

1. **define and maintain its scope**, i.e. the set of credential-types, jurisdiction(s), and domain(s) within which the SSI-AC aims to function, and the objectives it aims to pursue. This helps the Assurance Community to remain focused;
2. **define the services and products that the SSI-AC governs**[19], examples of which are given above;
3. **define restrictions, artifacts etc. that are necessary for the provisioning of such products and services.** Restrictions include e.g. liabilities of issuers under the SSI-AC, specific choices in semantics, credential mappings (i.e. stating the list of alternative credentials that can be used if a certain credential is being requested), defining credential lifecycle, defining audit processes, etc.
   Artifacts include e.g. the mechanism/process scheme by which it is determined if an organization qualifies as a ‘trusted issuer’[20] within the SSI-AC;
4. **the operational details of producing such products and services**, e.g. which organizations will, or are allowed to perform these operations, endpoints of e.g. **CI/CV**s where products and services can be obtained, etc.

[17] The discovery of SSI-ACs is a non-technical topic that resembles the way you discover the kinds of laws and regulations that apply to you(r business). You do that, e.g. by talking to peer organizations, governmental bodies (e.g. chamber of commerce), business associations, company lawyers, etc. It is conceivable that a SSI-AC exists, or will be created, that will maintain a register of SSI-ACs (that may be accredited as such by some scheme).
[18] See also the COVID-19 Credentials (“C19C”) Governance Framework.
[19] This does not necessarily mean that the SSI-AC itself provides such products/services; it may also outsource this.
[20] The idea is that verifiers may decide to trust any issuer in the trusted-issuers list of particular SSI-ACs, effectively (partially, at least) outsourcing the vetting work of what would be trusted issuers.

# Tools for Supporting SSI-ACs

In this chapter, we present a vision for tooling that allows SSI-ACs to support SSI in (at least) three major ways that were explained in depth in the previous section:

1. support the use of specific kinds of credentials;
2. support the accreditation of parties as they perform the roles of issuer, verifier/validator, or holder for (a subset of) such kinds of credentials;
3. support the creation and maintenance of (sub-)arguments, and provide technological services that allow subscribers to considerably simplify their business-information and business-decision governance processes.

The tooling needs to satisfy the following assumptions:

- The sovereignty of parties implies that each of them can issue any kind of credential. Other parties, also when they are referred to as an authority of some kind, cannot deprive parties of this ability. Therefore, we do not elaborate on what are called 'trusted issuers'. Rather, we provide support for accreditation against arbitrary accreditation schemes, which can be used to address the 'trusted issuers' issues, as well as several other/related issues.
- A credential consists of an 'envelope' and a 'payload'. The payload is a set of statements that parties issue (and other parties are interested in). The 'envelope' is just another (yet possibly standardized) means of transporting that payload with some basic assurances. For example, a bare passport document (as it comes from the printing house) is an 'envelope', and the payload is whatever is added (statements, photo, fingerprints) etc. The VC data model spec specifies an envelope where the payload/contents are to be put in the `credentialSubject`[21] section. There are many more kinds of envelopes, e.g. X.509 attribute certificates, attribute-based certificates, OpenID tokens, etc.
- Parties are typically interested in the payload (and they assume that the envelope is properly 'managed' by the infrastructure). They may choose to (not) use certain kinds of envelopes for issuing a payload, or to (not) accept certain kinds of envelopes. The policies for specifying such preferences to the (commodity) SSI infrastructure that we assume will exist are out of scope for this paper.

## Tools for Credential Markets

We expect various tools to become available that support credential markets, and the related governance. We will elaborate on two tools we think will be indispensable, but they will undoubtedly be complemented with others.

### Credential Catalogues

We will use the term '**Credential Catalogue**' to refer to a functional component, or an operational service, that parties can use to advertise the payloads of credential types that they issue in a human readable way. After all, the purpose of this advertising is to inform other parties that seek to use credentials about the characteristics that credential-payloads of such types have, which such parties need to determine whether or not (and if so, under which conditions) parts of these payloads can be used in the arguments they use for making specific kinds of decisions.

The exact nature of the information that parties may want to publish in payloads will depend on the (needs of their) prospective users. Obviously, it will contain a (JSON, XML or other) schema that

[21] This may be a bit confusing because 'subject' usually refers to some entity, whereas 'credentialSubject' is a set of statements about different entities.

specifies which statements are in the payload, and what they mean (semantics). Also, it would specify the kind(s) of 'envelope'(s) that may be used.

Other information might include the process that the issuing party has followed to verify the data that it puts in such payloads, standards or regulations that it has followed, constraints for use, pricing/payment mechanisms, applicable accreditations, liabilities it is willing to accept, etc.

A very simple credential-catalogue (proof-of-principle) was built for the Odyssey hackathon (november, 2020), for the purpose of experimenting, and the elicitation of further functional requirements.

SSI-ACs may use credential catalogues to document and advertise the types of payloads that they govern. They can use it as a platform

- to inform parties that may want to join the SSI-AC, or subscribe to its services,
- to store, or link to documentation about appropriate accreditation schemes,
- to inform verifiers how it can determine which parties have been accredited for some accreditation scheme (see section 'Supporting Accreditation Schemes']),
- to inform parties how they can get certified against such schemes, the kinds of payloads they can then obtain that certify this, etc.

### Yellow Pages service

We will use the term '**Yellow Pages service**' to refer to a functional component, or an operational service, that parties can use to search for and discover payload-types that other parties may govern and/or issue (in a variety of 'envelopes').

Typically, such a service would allow various kinds of search mechanisms, e.g. allow searches based on specific contents (e.g. an addresses, or names), assurance levels, issuers, analogues, keywords/categories etc.
A very simple yellow pages service (proof-of-principle) was built for the Odyssey hackathon (november, 2020), for the purpose of experimenting, and the elicitation of further functional requirements.

Parties that operate a credential catalogue and those that run a yellow pages service will find ways to cooperate, as it is obvious that in general, both benefit from each other's existence. However, the specifics of the credential catalogue services and yellow-pages services, such as the expected needs of their respective customers (e.g. the kinds of credentials, or kinds of characteristics they will be looking for), will determine what arrangements between them will be beneficial, and impose requirements e.g. on the credential type advertisements. This is an area for further market-research.

## Supporting Accreditation Schemes and Certification

In the section on the validator perspective we explained that a party makes decisions by evaluating associated arguments that have been populated with validated data[22], i.e. data that it considers valid to be used in such arguments. It is up to the individual parties to decide what data is (in)valid

[22] 'validation' is the process that parties use to determine whether or not a specific data element can be used in a specific argument. These processes are not only subjective - they are unique for every party, but they also depend on the kind of argument that is under consideration. Data that a party considers valid for one kind of decision may not be valid for another, and vice versa.

for what kinds of decisions. Its “validator” governance process is concerned with making (and continually reviewing and updating) such decisions.

Data is valid (to be used in some kind of argument) if the party ‘trusts’ it. That is to say: if the party has come to believe it is true. It is easier to believe this when the data comes with assurances, which come in various flavors (as discussed in the section on assurances).

SSI-ACs may play a significant role in providing a specific kind of assurance, namely ‘accreditations’. Accreditation is the formal recognition of a party’s competence to conduct a specific activity such as issuing, holding and/or verifying a specific kind of credential, or certifying parties. Such recognition is based on that party demonstrating compliance with a set of criteria (the accreditation scheme) to another party that is properly qualified (accredited) to conduct compliance assessments.

SSI-ACs are in an excellent position to define accreditation schemes that serve the (shared) purposes of its members, and any party that sees benefits in being accredited against such a scheme could apply for an accreditation assessment.

Accreditation schemes come in various flavors. They can be quite extensive, examples of which are ISO/IEC 27001 (requirements for running an information security management system), and ISO/IEC 27006 (requirements for bodies providing audit and certification of such systems).

But they can also be very simple. Many organizations with professional accreditations would be registered (in a database, or on a ledger), which are easily checked (similar to VONx).

There’s nothing new here - everything already exists, and SSI-ACs can readily use the existing practices in the existing communities. What may differ is the certification: since SSI-ACs operate in the ‘SSI world’, it makes sense to link accreditations with (verifiable, or other kinds of) credentials.

## Accreditation Credentials

Let’s consider the use of credential payloads for certification and validation purposes. We will use the term ‘accreditation credential’ to refer to a credential (payload):

- for which a SSI-AC has established and published a credential type specification (using its Credential Catalogue);
- that states (implicitly and/or explicitly[23]) at least:
    - the party to which the accreditation credential has been issued;
    - the accreditation scheme whose requirements have been fulfilled by that party[24];
    - the credential-types to which the accreditation credential applies;
    - the (cryptographic) proof methods and associated data that allow the proofs to be verified for the assurances that the accreditation scheme specifies. This obviously

[23] Implicitly: by describing in the accreditation credential type specification what this trust consists of, i.e. what it has decided to believe about the (issuer) organization, and what assurances it has obtained (and perhaps also: how it has obtained these assurances) that convinced it to hold this trust/belief.
Explicitly: by including claims in the accreditation credential that state the obtained assurances for this particular issuer organization.

[24] The accreditation scheme implies the functions that the party can be trusted to properly execute. So you might have a ‘trusted issuer’, or ‘trusted verifier’ accreditation schemes for specific kinds of credentials, as well as of certifying parties against such schemes.

includes the proof of provenance and integrity (signature), as well as other proofs that may be required under the accreditation scheme[25];
- the party that has audited the accredited party[26], the date of the audit, and perhaps some other audit-related attributes;
- … (etc.)

Parties can be accredited for different functions, against different schemes[27]. We may have schemes not only for accrediting 'trusted issuers', but also 'trusted verifiers'. A party that has been certified against a trusted verifier scheme of a SSI-AC would be trusted, at least within the scope of that SSI-AC, to request and use credentials of specific kinds only for specific purposes.[28] Similarly 'trusted holders' (i.e. wallet equipment[29]) that will interact in specified ways with 'trusted verifiers' and/or 'trusted issuers')[30].

If SSI-ACs were to provide accreditation credentials for well-designed accreditation schemes, this will be of enormous help for their subscribers to reduce the complexity of requesting credentials. A party that needs credentials for making a particular decision, and that can simply request that the issuing party must have a specific (issuer) accreditation credential of some SSI-AC, doesn't even have to know the name of the issuing party. For example, a party that requests a credential from a user that states the result of a Covid-19 test does not need to know about each and every (accredited) test-lab; it only needs to know that the credential was issued by a party that has the corresponding accreditation by the appropriate SSI-AC.

## Trustworthy Credentials of a SSI-AC

We introduce the term 'Trustworthy Credential (of a SSI-AC)' for a credential,
- whose type is specified by (and published in the Credential Catalogue of) that SSI-AC;
- of which the 'envelope' (metadata) includes one or more accreditation credential payloads, one of which is issued by, or on behalf of that SSI-AC, and is of a type that is specified (and published) by that SSI-AC.

---

[25] Doing this, and including the payload of the accreditation credential in every credential that is issued under this regime, enables verifiers to check the trustworthiness of the issuer based on the SSI-ACs assessment without needing to know who the actual issuer is. The exact/preferred ways of doing this remain to be determined. Candidates include using (pseudonymous) DIDs, and also with ZKP VCs.

[26] If a SSI-AC decides to outsource its accreditation process, it should make sure that the associated accreditation credential types that it specifies make verification and validation as easy as possible. There are several possibilities: the SSI-AC can allow organizations to use its 'accreditation credential signing service' if they present a credential that states they are a SSI-AC accreditor (so every accreditation credential is signed with a single key that is owned/controlled by the SSI-AC). Alternatively, accreditors may issue accreditation credentials that also include the accreditation credential of the accreditor (there is recursion here…). And there are more ways.

[27] As with ISO certification: different management systems of an organization may be certified: the quality management system (ISO 9001), environment management system (ISO 14001), the information security management system (ISO 27001), etc.

[28] In the Netherlands, the Burger Service Number (BSN - i.e. the Dutch social security number) may only be legally used within the government, for health purposes, and by banks. Certifying other organizations against a 'trusted verifier' scheme might provide sufficient assurances to allow them to use government issued credentials that contain this number.

[29] Note that where 'trusted issuers' and 'trusted verifiers' refer to parties (individuals, organizations), for the holder role we need the actual equipment (wallet app, edge/cloud agent) to be certified, because it is that equipment that will do the actual receiving of credentials, and creating presentations.

[30] In order to enforce a SSI-AC policy that states that trusted credentials may only be issued by trusted issuers and requested/used by trusted verifiers, we need realize ourselves that the holder agent (wallet app) does not just perform the holder role, but also the verifier role because it should be capable of asking 'the verifier' for its accreditation credential, and only use a trusted credential (under that SSI-AC policy) if the verifier has one (this is also referred to as the 'verify the verifier' capability).

The fact that such credentials contain an accreditation credential of the SSI-AC means that it comes with the particular assurances as stated in the associated accreditation scheme. The credential is 'trustworthy' for any party that appreciates the assurances provided by that accreditation scheme.

## Example for Trustworthy and Accreditation Credentials.

Here is an example of what a simple Accreditation Credential, in the form of a VC, might look like. This credential (of type `DHACAccreditationCredential`) has been issued by a SSI-AC named `DHAC`. It has been issued to a party called ACME and asserts that ACME is a trusted issuer for credentials of type `DHAC:Covid19TestResult`.

```
{
  "@context": [
    "https://www.w3.org/2018/credentials/v1",
    "https://www.w3.org/2018/credentials/examples/v1"
  ],
  "id": "http://DHAC.org/accreditationCredentials/1872",
  "type": ["VerifiableCredential", "DHACAccreditationCredential"],
  "issuer": "https://DHAC.org/issuers/4",
  "issuanceDate": "2020-04-30T11:17:24Z",
  "credentialSubject": {
    "id": "did:example:ebfeb1f712ebc6f1c276e12ec21",
    "name": "ACME, Inc.",
    "trustedIssuerCredentialType": "DHAC:Covid19TestResult",
    "trustedIssuerProofType": {
      "type": "RsaSignature2018",
      "verificationMethod": "https://acme.com/issuers/keys/1"
    }
  },
  "proof": {
    "type": "RsaSignature2018",
    "created": "2019-06-18T21:19:10Z",
    "proofPurpose": "assertionMethod",
    "verificationMethod": "https://DHAC.org/issuers/keys/3",
    "jws": "eyJhbG...GHSrQyHUdBBPM"
  }
}
```

Figure 2: Simple example of Accreditation Credential

Figure 3 shows an example of a Trustworthy Credential as it might have been issued by ACME to a person called Wayne Dodge. It states that Wayne has been tested on April 30th, 2020, and that the result of the test was negative[31]. It also contains ACME's accreditation credential that allows a verifier to obtain assurance that, according to SSI Assurance Community DHAC, ACME is a trusted issuer for this credential.

[31] This credential content is fictitious, and may be replaced with whatever else may be appropriate.

```
{
    "@context": [
      "https://www.w3.org/2018/credentials/v1",
      "https://www.w3.org/2018/credentials/examples/v1"
    ],
    "id": "http://acme.com/credentials/DHAC_Covid19TestResult/172",
    "type": ["VerifiableCredential", "DHAC:Covid19TestResult"],
    "issuer": "did:example:ebfeb1f712ebc6f1c276e12ec21",
    "issuanceDate": "2020-05-01T12:13:14Z",
    "credentialSubject": {
      "id": "did:example:2bdcc0b259683e194e48037ea21e15d3",
      "name": "Wayne Dodge",
      "covid19TestResult": {
          "tested": "2020-04-30T11:19:10Z",
          "result": "negative"
      },
      "accreditationCredential": [ {
        "@context": [
            "https://www.w3.org/2018/credentials/v1",
            "https://www.w3.org/2018/credentials/examples/v1"
        ],
        "id": "http://DHAC.org/accreditationCredentials/1872",
        "type": ["VerifiableCredential", "DHACAccreditationCredential"],
        "issuer": "https://DHAC.org/issuers/4",
        "issuanceDate": "2020-04-30T11:17:24Z",
        "credentialSubject": {
            "id": "did:example:ebfeb1f712ebc6f1c276e12ec21",
            "name": "ACME, Inc.",
            "trustedIssuerCredentialType": "DHAC:Covid19TestResult",
            "trustedIssuerProofType": {
                "type": "RsaSignature2018",
                "verificationMethod": "https://acme.com/issuers/keys/1"
            }
        } ],
        "proof": {
            "type": "RsaSignature2018",
            "created": "2019-06-18T21:19:10Z",
            "proofPurpose": "assertionMethod",
            "verificationMethod": "https://DHAC.org/issuers/keys/3",
            "jws": "eyJhbG...GHSrQyHUdBBPM"
        }
    },
    "proof": {
      "type": "RsaSignature2018",
      "created": "2019-06-18T21:19:10Z",
      "proofPurpose": "assertionMethod",
      "verificationMethod": "https://DHAC.org/issuers/keys/3",
      "jws": "eyJhbG...GHSrQyHUdBBPM"
    }
  }
```


Figure 3: Example of a Trustworthy Credential

# Tools and Services That Support Business Decision Making

Whenever a party wants to make a well-considered decision, it needs to establish the argument on which to base it. As we explained earlier, an argument can be seen as a tree where each node can be seen as a variable whose value is the result of doing some computation with (the values of the nodes of) its branches, or if it has no branches, it may simply be assigned some value (boolean, integer, date, …).

Nodes, particularly when they have multiple branches, can be assigned a name that acts as a variable that can be evaluated, i.e. assigned a value. For example, a node called “authenticated person owns bank-account” might evaluate to ‘true’, ‘false’ or ‘non-evaluable’. A node called “personnel” may evaluate to a list of people (identifiers) that are considered personnel (employees, or hired staff).

Here is a fictional example of what a tree might look like for dealing with a request for accessing a bank account. The root node, called ‘bankaccount’, will evaluate to the account that the requestor has selected from all bank accounts that (s)he has a right to access. In its simplest form, that would be the bank accounts that (s)he owns:

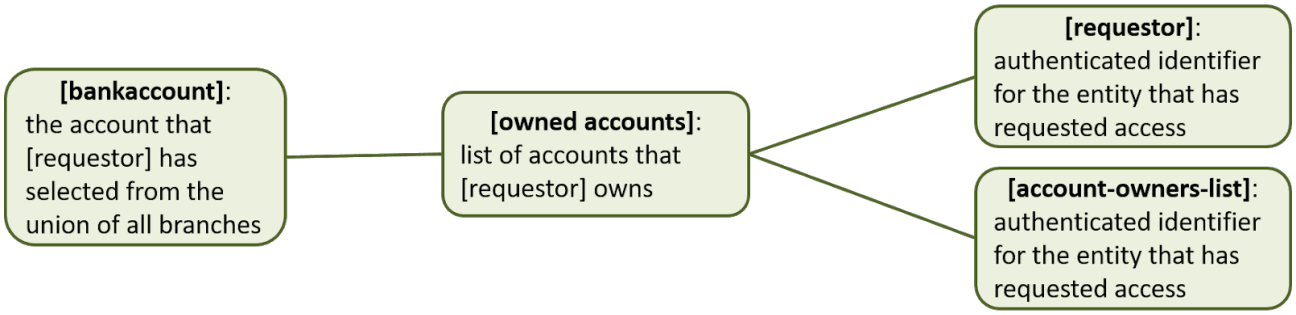


Figure 4: Fictional example of decision tree for accessing a bank account.

However, if the bank provides the owner of a bank account with the service to mandate other people to access their bank account, this has to be reflected in the decision tree as well: a requestor then also gets to select from the accounts for which (s)he is a mandatee, as follows:

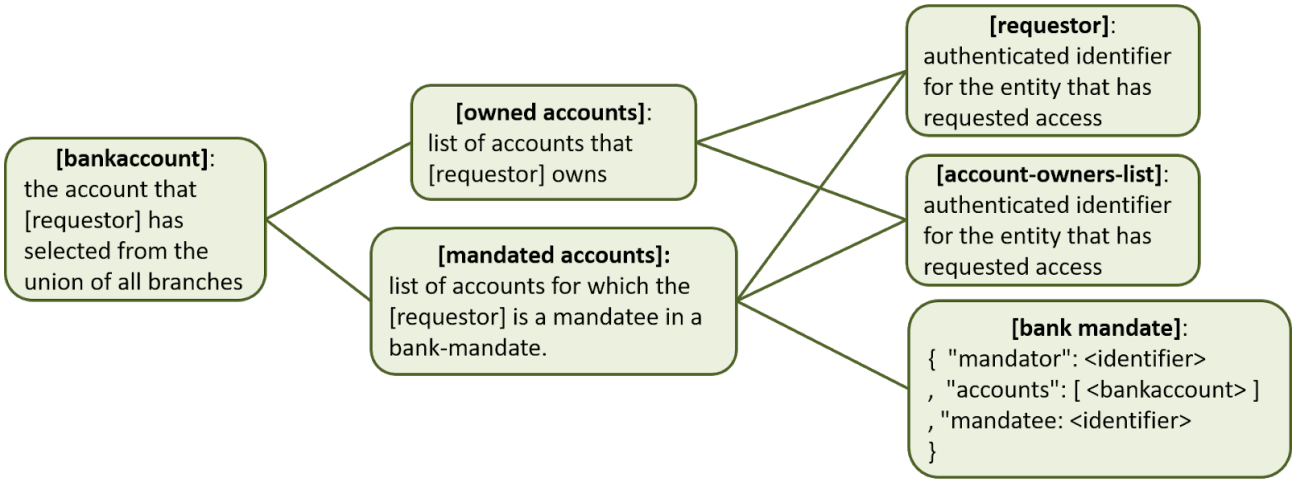


Figure 5: Grafting a new branch on the decision tree.

As time progresses, all sorts of other situations will pop up that cause subtrees to be grafted (added to one of the existing nodes), causing the decision tree to become ever more complex over

time. Moreover, since the proper design of these subtrees may require ever more specialized expertise, their governance quickly becomes unmanageable. An example is dealing with legal rights that people may have to access a bank account of others. For example, if your partner, parents or child has died, if you have been appointed as a guardian of someone that is incapable of doing its own financial administration, if you are a police officer that is tasked with tracking down bank frauds, etc. Such a decision tree might then look like this:

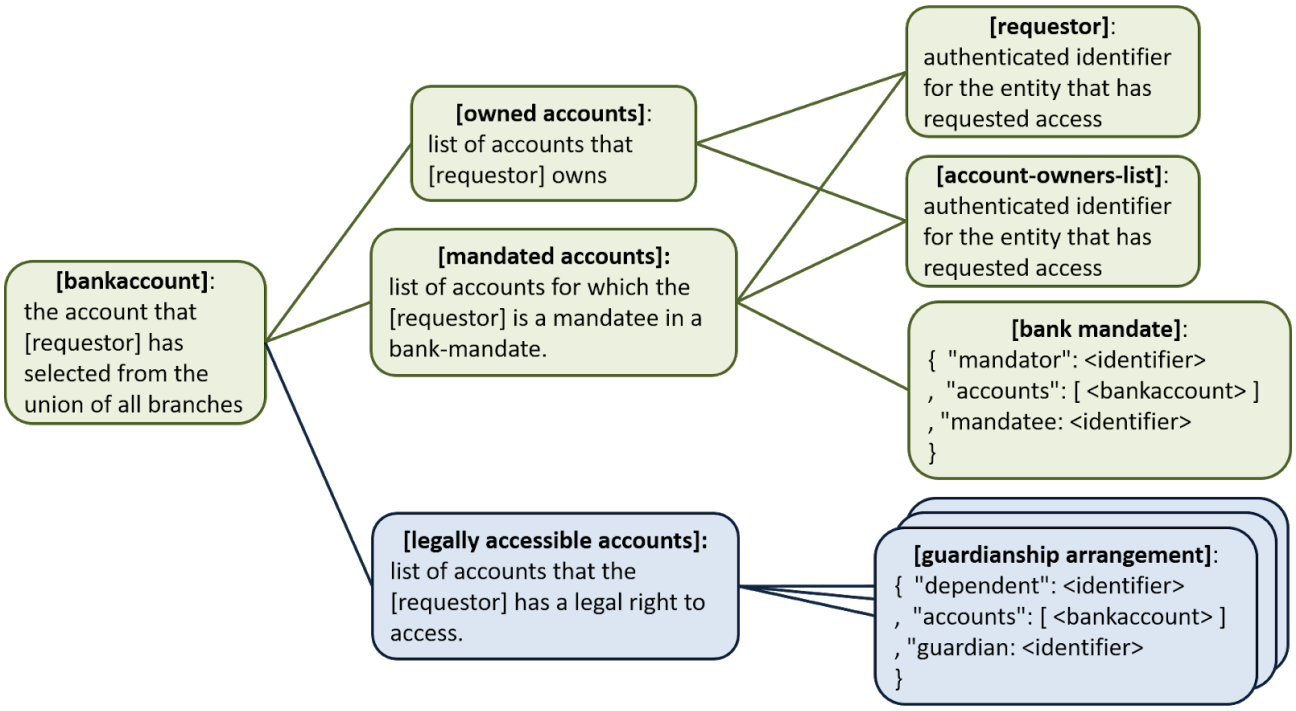


Figure 6: Grafting a branch the execution of which may be outsourced.

As we explained earlier, we can outsource the governance and design of individual nodes to parties within or outside of our own organization that have the specific knowledge and experience to design them.

We propose that SSI-ACs can provide such services, i.e. design decision trees that others can use as a node in their own decision trees. In the above picture, the decision tree with node ‘legally accessible accounts’ could be designed by a SSI-AC that has in-depth knowledge of the law, and since that would be the same for every bank in that jurisdiction, all of them could use that tree as a node in their own decision trees.

The SSI-AC can provide various services for this. One would be that it would provide code that subscribers can download and install in their own IT equipment. Such code could come with various assurances regarding its correctness, efficiency etc. Alternatively, the SSI-AC could provide an IT service and endpoint where subscribers could request the evaluation of the node, where the result could contain proofs of execution correctness.

We can also foresee that such trees can be provisioned through a new capability that we propose the SSI infrastructure to have, being the requesting and provisioning of qualified (sub)decisions. The SSI infrastructure then not only goes after some qualified data, but also actually processes it into the result of evaluating a decision tree with such data.

Obviously, the SSI-AC would then also need to have a ‘decision-tree catalogue’ in which it can advertise the kinds of decisions that the various decisions-trees can produce, the kinds of (qualified) data that are involved, the ways in which subscribers can use such trees (in-house or as-a-service), properties (e.g. ‘guaranteed to be compliant with current legislation’), etc.

# Conclusions

We have explored a set of related ideas that we collectively refer to as “decentralized SSI governance”, the main purpose these concepts is to help organizations transform their IT, business-process artifacts and policies to enable them to use SSI and reap its benefits.

We have identified several of such benefits, not just saving time and money, but also that using SSI may contribute to diminishing the ‘digital divide’, because it prevents people from giving up on filling in digital forms as they encounter all sorts of difficulties.

We have also identified obstacles to the adoption of SSI by organizations, postulating that the electronic exchange of qualified data - using an SSI infrastructure - should be just as easy as the electronic exchange of arbitrary data - using the Internet, i.e. TCP/IP infrastructure. We have assumed that over time, such an SSI infrastructure will become available as a commodity and use the current trust networks as a basis.

The adoption and transformation challenges that remain have to do with

- **qualified data**, i.e. data that comes with assurances regarding provenance, integrity, and possibly others. We have described the related concerns from the perspective of providing such data (issuer perspective), obtaining and using such data for further processing (validator perspective), and holding such data (holder perspective). We conclude that organizations need governance processes that establish and maintain policies for providing and validating such data.
- **argument construction**, i.e. governance processes for establishing arguments, which is the reasoning by which decisions are being made in an organization, and the possibility to outsource the (partial) design of such arguments, particularly in cases where specific (expert) knowledge and experience is required.
- **assurances** related to qualified data, other than those regarding its provenance and integrity. We have identified various sources of such assurances as well as different ways to communicate them in terms of (un)qualified data.

Then, we have introduced the idea of a SSI Assurance Community, that is a (often already existing) community of organizations that already work together for some purposes and have established trust mechanisms that they can rely on. We propose to leverage such communities and their trust mechanisms for the purpose of furthering the adoption of SSI, and the related transformation of organizations.

We do so by proposing the development of tools to support

- **Credential markets**. One example is ‘credential catalogues’, that organizations and/or SSI-ACs can use to advertise the definitions of the payloads of credentials that they govern, providing all information that other parties may need to determine whether or not using such credentials would be beneficial for them. Another example is the ‘yellow

View publication stats

pages service', which is a service that allows such parties to find the various credential catalogues that may be of interest to them.
- **Accreditation schemes** that can be used for the accreditation of parties as they issue, hold, or verify credentials as well as for the accreditation of IT that performs such functions. Specifically, we proposed a generic kind of accreditation credential, and we show how it can be used in a way that is integratable with SSI infrastructure.
- **Decision tree development and execution**, where such trees can be used as nodes in the decision trees of SSI-AC subscribers, thus freeing them from difficult governance tasks and the implementation of the resulting decision policies. While we expect this to potentially become a huge benefit, more work is needed to explore this idea.

Taking it all together, SSI-ACs propose to help the adoption of SSI, so that the current bureaucratic information exchange processes are easier, both for individuals as well as organizations. Using the SSI-ACs, it is possible to leverage the present trust communities and corresponding mechanisms, while at the same time automating the business decisions that are experienced as cumbersome. Different credential types, accreditation, machine readable policies and decision tree support are an essential part in decentralized governance. To reach these potentials that the SSI-ACs can offer, different tooling and services are suggested. Such tools and services will need to be better specified, and some perhaps also standardized.

---