Vision document

Dutch Self-Sovereign Identity Framework (DSSIF)

Dutch Blockchain Coalition

connect and create

www.dutchblockchaincoalition.org

Author:
Tim Speelman

Editors:
Arno Laeven, Jacob Boersma and Peter Verkoulen

Review Board:
Chantal van der Wijst (Tax and Customs Administration)
Simon Sanders (CMS DSB Lawyers)
Rein Schaafsma and Wouter Welling
(Ministry of the Interior and Kingdom Relations)
Sandra van Heukelom-Verhage (Pels Rijcken)
Tina van der Linden (Vrije Universiteit Amsterdam)
Tom Demeyer (Waag)

Illustrations:
Rosa Jager and Tim Speelman

Dutch Blockchain Coalition
connect and create

Table of contents

1 Introduction

Service providers – such as those in healthcare, banking or government – generally need to know something about their users in order to be able to provide their services. Examples include who their users are, what they can do and what they are allowed to do. The administration and exchange of information required for this is becoming increasingly problematic for both the service provider and the users. An example of this can be found in the housing market: potential tenants have to gather and supply an entire file of documents just to prove that they can pay the rent. Landlords must manually check all of these documents for authenticity and then manually assess them. This method is not only tedious, time-consuming and expensive but can also have a serious impact on the privacy and (therefore) the security of the tenant. After all, far more information is shared than is necessary and what happens to all that information afterwards is unclear.

Although digitisation has brought about efficiency gains in such processes, it has also led to greater privacy and (cyber)security risks. People and companies are increasingly the victims of data leaks, which may lead to phishing and other forms of identity fraud. Similar problems occur in many domains. Despite this, a common approach is lacking in most cases. The result is a proliferation of separate identity systems and chains in which privacy, reliability and other values must be considered and safeguarded over and over again. This increases the likelihood of errors and makes it difficult for users and regulatory authorities to understand and monitor those systems and chains and thus to know whether privacy and other values are sufficiently protected. The fragmentation of identity systems and identity chains also results in a lack of interoperability; cultural, organisational, political, legal and economic boundaries hinder the sharing of data and the identification of people and organisations. This is certainly bothersome for the people who have to navigate all these different situations.

This must be and can be improved!

Interoperability can be promoted by means of technical standards and regulations such as the eIDAS Regulation[1], but there is still a need for the technical and organisational implementation of such a regulation. This technology and organisation is needed to facilitate the actual exchange of information and the necessary checks. People – as customers, students, patients or in any other role – also benefit from a joint approach: a single way of authenticating and exchanging (personal) information through which the other party is also directly authenticated. Ideally, a joint approach should therefore consist of shared technology that can be used in a wide range of applications: a digital identity infrastructure. Just like other critical infrastructures – water, electricity, transport – such an infrastructure could add enormous social and economic value. The question is how such a digital identity infrastructure can best be designed to satisfy all of the interests involved in all of these forms of service provision. A proactive approach is required from many more disciplines than technology alone -such as legislation, policy, sociology and ethics- in order to steer these developments in the right direction. Perhaps the most fundamental design question is who will be responsible for the development and management of such a critical infrastructure. To which parties can these critical tasks be responsibly assigned? Where can the data, metadata and behavioural information of all kinds of people and organisations be kept secure? With the

[1] https://www.digitaleoverheid.nl/dossiers/eidas/

Back to Table of Contents

government? Big tech? Big finance? Big telco? Is it at all moral to entrust one or just a few parties with so much power and knowledge?

Self-Sovereign Identity

In the search to answer this question, the term Self-Sovereign Identity (SSI) is being used more and more frequently. The philosophy behind Self-Sovereign Identity is that knowledge of and power over data should rest solely with the data subject itself (person, organisation or even machine). This can be achieved by providing every person and every organisation with a new tool: a digital assistant, also called an agent or wallet in SSI. This digital assistant – probably in the form of a smartphone app for people – makes life easy for the end user and ensures responsible management of identifiers, keys and data at all times. The data subject retains insight and control over data. When service providers ask for data, the subject always sees which data will be shared and with whom in a familiar and consistent interface. The subject will only be asked to allow or deny this request. In addition to the subject, all issuers and verifiers of data have such an assistant. Their agents facilitate safe and efficient data sharing in which the origin and integrity are safeguarded. They also standardise communication with the subject's agent. In this way, the subject becomes the connecting factor between the issuer of a piece of data (such as a government registry) and the verifier of those data (such as a service provider).

Because agents facilitate efficient and secure data sharing and are widely deployable, the friction that goes with data sharing (time, costs and effort) is significantly reduced. At the same time, this position grants the data subject insight and control over the shared data and allows him or her to be completely independent of intermediaries. This means that no third party has any insight into the data or what the data subject is doing with it. The fact that the technology is in the hands of all data subjects creates a decentralised network without central weaknesses. It creates digital identity infrastructure that is not only robust but also more scalable, thereby creating a win-win situation for both service providers and users. This is the aim, at least.

The word 'sovereign' deserves further explanation. Sovereignty makes one think of unlimited control over data – modifying it as desired – which does not fit in with today's society. But this is not the intention of sovereignty in SSI. The idea behind SSI is that the data subject actively controls his or her own data. Some of that data will be self-declared, but most of it will come from trusted third-party sources such as government registries, banks, employers and other organisations and people. With SSI, the data subject cannot alter this data unnoticed, but (just as with a physical passport or security paper) he or she gains real control over who sees the data and when.

A common objection is that people and organisations could not manage such technology and/or data responsibly. In other words, SSI only would work for a small group of privacy experts. However, this does not need to be the case: the software takes all of the complex tasks off their hands and gives them precisely the information that is needed via a comprehensible interface. Having said that, it is true that-in addition to freedom and control- SSI also brings a new degree of responsibility. Therefore we must be careful if we give people full responsibility over their own privacy and (cyber)security. It is important to set up the technology in such a way that it offers sufficient protection by default.

Back to Table of Contents

The development and awareness of Self-Sovereign Identity has increased significantly in recent years. Various (consortia of) large companies are developing technical solutions, some of which appear to be virtually ready. It seems certain that some form of SSI will become part of society in the near future. It is therefore crucial that we are able to assess the value of these developments, adjust them where necessary and, above all, benefit from them.

The Dutch Self-Sovereign Identity Framework

With the Dutch Self-Sovereign Identity Framework, the Dutch Blockchain Coalition aims to create a shared starting point for all stakeholders: what are we talking about and where do we want to go? With this starting point, design choices can be made, substantiated and valued. We also recognise the risks, even though that we cannot assess all of them at this time. Nevertheless, we believe in the enormous potential of (the philosophy of) Self-Sovereign Identity for people and organisations and for the economy and society.

This vision document is structured as follows:

- **Chapter 2** formulates a shared starting point: "What are we talking about?" Firstly, we consider the breadth and depth of the context in which the digital identity infrastructure must play a role. Next, we analyse that context and set out the possible functions of an infrastructure.
- **Chapter 3** formulates a framework of relevant values for assessing the development of an infrastructure and making design choices for that infrastructure. This also makes it possible to determine whether we – as service providers, users and other stakeholders from a broad variety of organisations and sectors – agree on the desired outcomes.
- **Chapter 4** argues for the connecting and controlling role of the subject – the idea of Self-Sovereign Identity – set against alternative designs for a digital identity infrastructure.
- **Chapter 5** addresses the question of how the subject can play that connecting and controlling role. Without discussing specific technologies and developments, we outline a solution and raise relevant design choices, potential risks and open questions.
- **Chapter 6** discusses the next steps: "How do we proceed from here?"
- **Chapter 7** contains a glossary of terms.

This vision document is a guideline and not a manual. It is also a living document that will be adapted and will grow with advancing insights.

Back to Table of Contents

2 A shared starting point

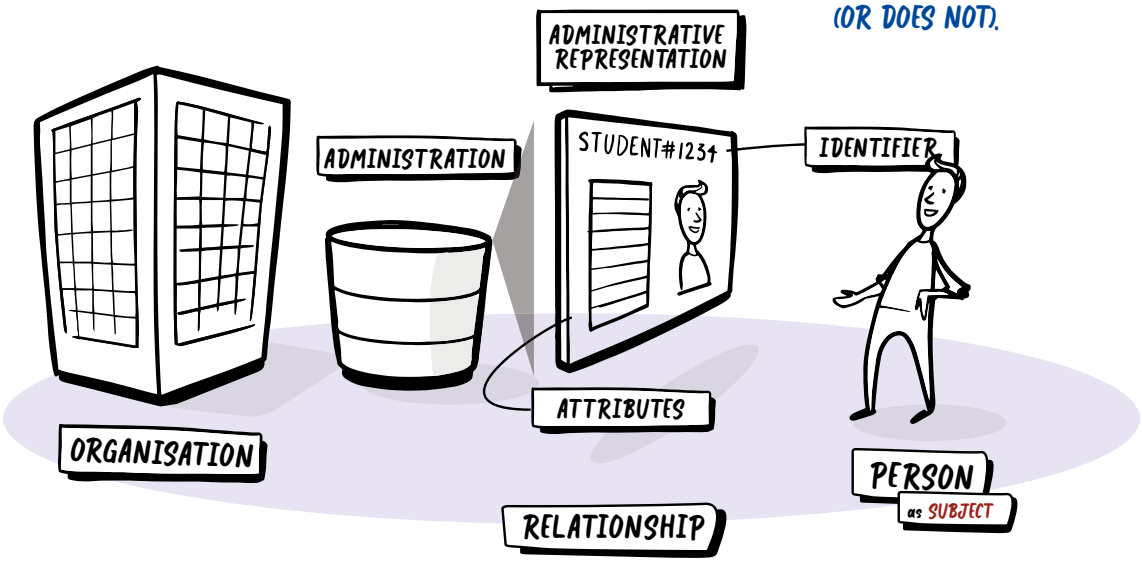
The goal of this vision document is to establish a shared starting point for all stakeholders (with diverse backgrounds and expertise) of the envisioned digital identity infrastructure; what are we talking about and where do we want to go? From this starting point, design choices can be made, substantiated and valued. This chapter describes the context and problems from various perspectives, separate from the technical, legal and policy-related details.

2.1 From 'identity' to 'administrative representation

The term 'identity' can lead to confusion. This is because the various disciplines that have been brought together in this document use different definitions. In information science, identity may refer to a set of data describing a person, organisation or thing. In law, identity may refer to the official registration of a person or organisation as recorded in a civil or commercial register. In the social sciences, identity concerns the complete and unique *being* of a person which can never be captured as *data*. Many more definitions and conceptualisations could be named.

In our context, it is more productive to speak of 'representation. People and organisations form *pictures* of each other according to which they interpret and judge each other. This pictures or rather representations can be mental or emotional but also *administrative*: an **administrative representation** (see Figure 1). Each party has a *different* representation of the same person or organisation which is filled in with other aspects, other attributes. In order to keep subjects apart and to be able to identify them, each subject can be assigned a unique identifying number or datum, an **identifier**.[2] People (and organisations) are usually found in many of these administrative records, such as in their employer's personnel file, their bank's customer database or their government's civil register.

FIGURE 1:
AN ADMINISTRATIVE REPRESENTATION DETERMINES HOW AN ORGANISATION SEES A SUBJECT (OR DOES NOT).



[2] An identifier can also be a (user)name or email address. An identifier is any attribute or combination of attributes that is unique (in a particular context) and can therefore be used for identification.

Back to Table of Contents

It is necessary to recognise that an administrative representation is always a *simplification* and may be incorrect or out of date. The presence of the administrative representation representation should not be confused with the actual *existence* of the person or organisation – 'I am registered, therefore I am'. When the administrative representation in processes and organisational cultures is wrongly assumed to be absolute truth, this can have serious consequences.

Administrative representations – and the processes by which those are created, changed and used – are instrumental to secure and efficient service provision. They are also value-laden; they have an *impact* on service providers, service users and other stakeholders. The design question that follows is: **how can a digital identity infrastructure support these administrative processes and therefore the service provision in a way that does justice to the values of all those involved?**

2.2 A value-sensitive design

The design of a digital identity infrastructure is value-sensitive. Chapter 3 takes a closer look at the values involved. Below is a brief summary so that the reader can keep these values in mind.

Firstly, it is important that the administrative representation fulfils a certain function, that it has a **use** such as securing, supporting or personalising the service provision. This function also determines the required **reliability** of the information. The granting of a loan, for example, involves a higher risk than the granting discount to a customer and therefore requires more reliable information. The **representation** must also be *representative*: an accurate description of the data subject, not only for effective service provision but also for fair treatment of the person or organisation described.

(Administrative) representation formation is, by definition, at odds with **privacy**. Privacy is broadly defined as "the right to be let alone, to go about your business undisturbed." One form of privacy, ***informal* privacy**, concerns the protection of personal data. From this point of view, others should have as *little* knowledge as *possible* about the data subject. For each application, a balance will have to be struck between utility, reliability and informational privacy. In addition to primary (personal) data, **metadata** (with whom and when people and organisations communicate and do business with) must also be regarded as sensitive, for instance because it can say a lot about the behaviour or characteristics of a subject. It is this metadata which is most interesting for targeted advertising. Because administrative representation formation supports communication between people and organisations, **communication privacy** is also relevant: the ability to communicate confidentially without others knowing. Fragmentation also plays an important role: because one infrastructure offers a multitude of applications and contexts, there is a risk that the (meta)data and the subject's behaviour from all these separate contexts can be related to one another, which can lead to an undesirably extensive picture.

Many (vital) processes depend on these administrative representations. When the necessary systems or data are not **available**, this can have serious consequences for people and organisations.
Efficient and effortless processes are generally seen as desirable. From this perspective, **friction** is seen as a

Back to Table of Contents

negative value and the aim is to be able to collect information about data subjects as quickly, easily and as cheap as possible. However, critics point out that friction also has a positive effect: the effort, costs and time required ensure that less data is shared and that people do not have to provide proof for every little thing.

As administrative representation formation inevitably has an impact on the aforementioned values, it is important that the parties involved, particularly the data subject, can have **control** over (the use of) administrative representations. Control can be further specified in terms of transparency, **agency** and **grip**. Transparency is the degree of insight into the use of data. Agency is a certain *right* to have a say in the use of data. And grip is the actual possession and management of data.

2.3 The application space: supporting and connecting islands

In order to achieve a digital identity infrastructure that can be broadly deployed, it is useful to form an image of the application space. The application space extends in various directions: across people and organisations, across domains and sectors, across countries and jurisdictions and also across time. All kinds of cultural, organisational, political, legal and economic 'islands' thus fall within the scope. Each with its own views, problems and values. It is a challenge to not only *support* each of these islands with a single infrastructure but particularly to *connect* them.

Besides the internet and telephony, there are not many infrastructures that operate on this scale. The size of the application space depends on the flexibility and social, technical and economic accessibility of the infrastructure – and vice versa. Wherever the boundary may lie and however large the application space may be, the design of an infrastructure requires a broader view than the organisation itself and a broader view than its own domain and its own expertise.

2.4 A model of the application space

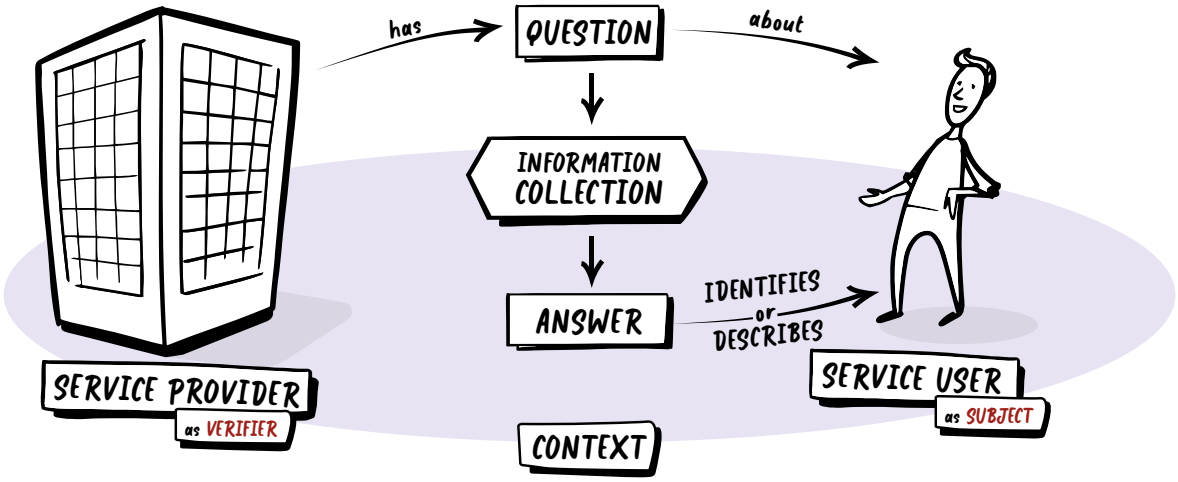
Design of this application space does not work by first achieving a solution on one island and then trying to translate it to the next. Instead, a different approach should be taken: the creation of a **generic model** of the application space based on knowledge and experience from the different 'islands'. Based on this model, solutions can then be developed, tried out in specific applications and refined with the new insights. The model and the solution are in constant development. Over the past two decades, this approach has led to innovations that are now referred to as Self-Sovereign Identity, but also to many of the insights described in this vision document. The generic model in this vision document is not intended to capture all of the expertise but rather to separate it from the details (transcending disciplines) and reach agreement on where we stand and where we want to go.

Back to Table of Contents

2.5 Information collection: from question to answer

Figure 2 illustrates the application of identity information in service provision. The service provider and service user have a common goal: the service. In pursuit of this goal, the service provider has an **information question** about the service user. In this context, both take on a new role: the service provider acts as a **verifier**, the service user as a **subject**.[3] Note that the roles can also be reversed: the service user may want to establish that the service provider is indeed who he says he is. In the further discussion, we consider the verifier to be the party who has the question and the subject to be the party whom this question concerns.

FIGURE 2: THE COLLECTION OF INFORMATION



The information question can be *identifying* (such as "which customer am I talking to?") or *descriptive* ("is this user authorised?" or "where does this person live?"). What follows is an **information collection** process: the verifier may observe something *himself* ("the customer looks 18+") or will have to get the information from his own records, (those of) the subject or (those of) a third party. This collection process results in an **information answer**, which can again be *identifying* ("John") and/or *descriptive* ("yes, 18+"). This answer can then be used by the verifier.

The **context** in which this question, collection and answer plays a role is the interaction, or **transaction**, between the verifier and subject. This can be in a physical context, at the counter or at the door, or in remote communication by mail, telephone or electronic means.

2.6 Link between reality and administration

To be able to collect the desired information, one or more forms of administration are consulted. It is important that the link between reality (the person or organisation in the role of the subject) and administration (the administrative representations about that subject) can be made first and verified later. This link is illustrated in Figure 3.

[3] For the sake of recognisability, the data subject is depicted as a person. However, an organisation can also assume the role of a data subject.

Back to Table of Contents

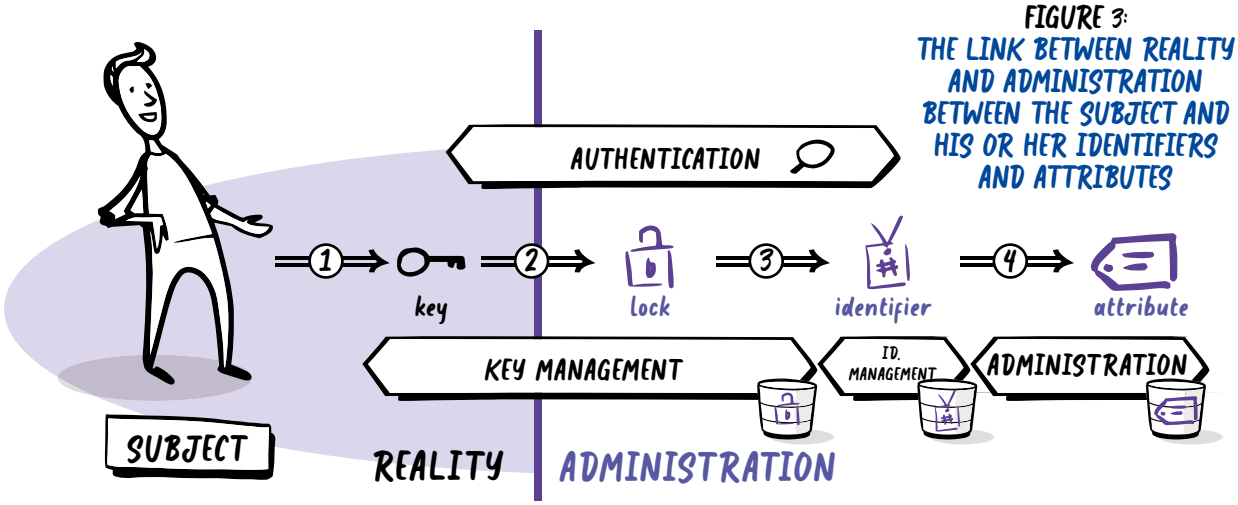


FIGURE 3:
THE LINK BETWEEN REALITY AND ADMINISTRATION BETWEEN THE SUBJECT AND HIS OR HER IDENTIFIERS AND ATTRIBUTES

There are various methods to bridge this gap between reality and administration. Frequently used methods are based on aspects of reality that can be *observed* (such as fingerprints, DNA and faces), *conceived* (such as passwords and PIN codes) or *created* (such as passports and SIM cards). A copy, derivative or other reference material of those keys (symbolised here as a 'lock') is recorded in administrations to establish the link between reality and administration.

The four connections between the five elements of this link (person, key, lock, identifier and attribute) influence the reliability of the information. In the creation and management of this link, we distinguish between three management activities: key management, identifier management and administration. Authentication, the fourth activity, establishes whether the link is correct at the time of information collection. These four activities are briefly explained below.

2.6.1 Administration

The collective term **'administration'** is used in this document to refer to all of the processes and systems involved in recording and managing data. These processes and systems are specialised according to the specific application for which they have been developed. After all, there are substantial differences between the civil register and the commercial register and between the administration of a football club and patient files. The administrative representation, as introduced in Figure 1, is the set of attributes that a party can relate to one data subject. In addition to personal data such as name and date of birth, it can also relate to other things such as the ownership of a car or house, an employment relationship with a company, etc.

In order to be able to overcome cultural, organisational, political, legal and economic barriers, a digital identity infrastructure will have to be independent of the content, form and meaning of data. Attempts to standardise this content, form and meaning therefore fall outside of the scope of this vision. In this view, administration is seen solely as a black box from which answers can be provided to information questions.

Back to Table of Contents

2.6.2 Identifier management

By **identifier management**, we mean the creation, maintenance and destruction of identifiers. The purpose is to be able to refer to individual entities within a certain context in order to be able to identify them. For example, the Dutch government assigns each citizen a single Citizen Service Number ('Burgerservicenummer', BSN), email providers assign one or more email addresses and people can choose their own username on social media. Depending on the purpose, identifier management safeguards certain conditions such as *inclusiveness* (all persons have an identifier), *singularity* (each person has only one identifier), *uniqueness* (each identifier is only used by one person) and *traceability* (the identifier can be traced back to the physical person).

The use of identifiers affects privacy. When one identifier is used by many organisations, in many applications and/or for a long period of time, the risk arises that an extensive image of (the behaviour of) the subject will be created – an image that can possibly be misused. This is one of the reasons to limit the use of the BSN. This privacy impact can be reduced by using disposable identifiers or using a different pseudonym for each of the parties with whom the subject communicates. This makes it more difficult for parties to link their administration or for criminals to do so in the case of data leaks.

Identifiers are an essential connection in the link between reality and administration. Without an identifier, people are invisible and are therefore excluded from (vital) services. The use of identifiers is also value-sensitive. A digital identity infrastructure can support identifier management by standardising various forms of (pseudonymous) identification.

2.6.3 Key management

Key management includes the granting and revoking of keys with which persons (or organisations) can prove that they match their identifiers. Key management must prevent the loss of keys as well as their unauthorised use. When the subject loses the keys, he or she no longer has access to an identifier and all the value that is linked to it in administrations. In such a case, the subject must prove that he or she corresponds to the identifier without being able to show the keys. A digital identity infrastructure could support key management in these challenges.

2.6.4 Authentication

The purpose of **authentication** is to establish that a person matches a particular identifier (that they are who they say they are) during a transaction. The person then presents the previously established key. If this key matches the reference material, there is a good chance that this person is the legitimate data subject. The quality and security of the key management and authentication activities together form the authentication assurance, also known as Level of Assurance (LoA). Without (successful) authentication, identity fraud may occur and may harm the verifier, the actual subject and/or other stakeholders.
Normally, these links are managed by one or more organisations, which makes the subject and verifier dependent on those organisations. Without this link, the subject is practically invisible, as the refugee crisis has

Back to Table of Contents

made painfully clear.[4] If possible, however, this link is guaranteed and is under full control of the subject; a task that could be entrusted to the digital identity infrastructure. In this way, he or she establishes a foothold, so to speak, in the 'administrative world'.

Box 1. An example of the link between subject and administration
Puk wants to claim medical expenses from her health insurer online. The health insurer needs to know which insured person he is dealing with (identification) and uses DigiD to find out. DigiD is responsible for the **key management** and has previously issued Puk two resources (**keys**): a combination of username and password and the DigiD app. **Identity management** is the responsibility of the Personal Records Database ('Basisregistratie Personen', BRP). The BRP has assigned a BSN to Puk. The health insurer keeps its own **records** in which Puk's **identifier** (the BSN or a derivative thereof) is linked to **attributes** such as her policy or payment history. By logging in with DigiD (**authentication**), the healthcare insurer knows which **identifier** matches Puk and therefore which **administrative representation**. Services are provided on the basis of this image.

2.7 Transfer of statements

In some cases, the verifier may not be able to answer the information question but another party can. This creates **identity chains** in which various **chain parties** exchange information about the same subject. When a party shares information about a subject, it is in fact issuing a **statement**. That party therefore assumes the role of **issuer**, see Figure 4.

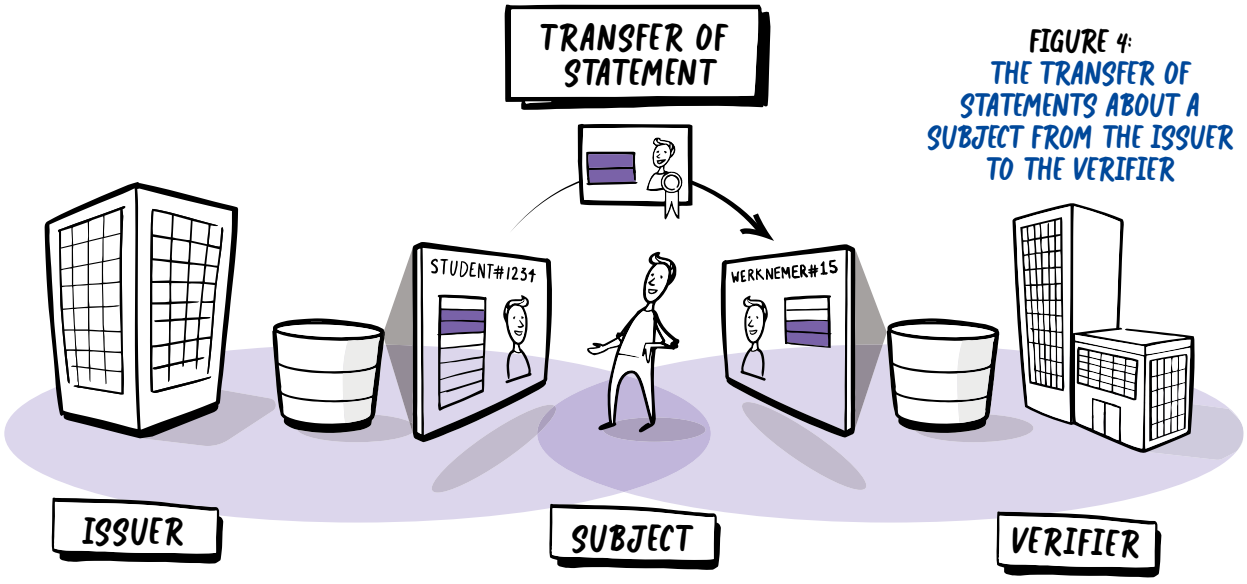


FIGURE 4: THE TRANSFER OF STATEMENTS ABOUT A SUBJECT FROM THE ISSUER TO THE VERIFIER

[4] Refugees who come to Europe without means of identification find it difficult or impossible to use vital services. Source: UNHCR (https://www.unhcr.org/)

Back to Table of Contents

For example, a municipality issues physical statements in the form of a passport, driving licence or identity card. Although the information and application are very different, there are major similarities with the **transfer of statements**.
We have identified three major challenges:

1. **Logistics:** how does the issuer's statement safely reach the verifier?
2. **Issuer authorisation:** how can the verifier *trust* the issuer's statement?
3. **Verifier authorisation:** how does the statement reach only authorised verifiers for the authorised use?

2.7.1 Logistics

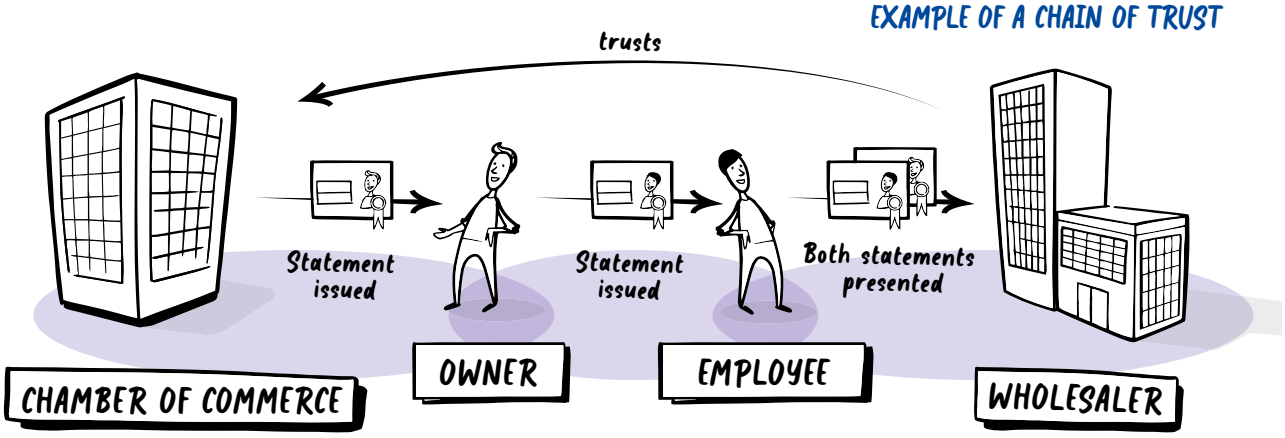
To answer an information question, statements must be transferred from an issuer to a verifier. This can be done, for example, directly or through an intermediary (such as a data vault or safe) or through the subject (as is the case with physical documents). The logistical design affects many values of the subject and verifier if it introduces dependencies on (and possible surveillance and control by) third parties. A digital identity infrastructure can support logistics, among other things, by standardising the statement transfer and reusing the necessary communication channels. This can significantly reduce the friction involved in a statement transfer.

2.7.2 Authorisation of the issuer

The added value of a statement depends on who issues it. For example, the Chamber of Commerce ('Kamer van Koophandel', KVK) may issue (extracts of) statements stating who owns a company. And any Dutch university may issue a WO degree. Basically, the verifier is responsible for (directly or indirectly) authorising the issuer. Before using a statement, the verifier will have to verify the origin of that statement and determine whether it wants to accept statements from that issuer.

From this need arises a new information question: who (or what) is the issuer? The answer to this question can again be determined by another issuer and proven with a statement. This can create a **chain of trust**: a chain of mutually trusting parties that ends with a **trust anchor**, a party which is directly or implicitly trusted by the verifier. The following example (also shown in Figure 5) illustrates how such a chain of trust can work in business:

FIGURE 5:
EXAMPLE OF A CHAIN OF TRUST



Back to Table of Contents

Box 2. Simplified example of a chain of trust
Pim works for Puk and goes to the wholesaler on behalf of Puk BV. The wholesaler wants to establish that Pim is authorised to buy on behalf of Puk BV. Pim produces an authorisation (statement) from Puk. The next question is whether the issuer of that statement is authorised. With a statement from the KVK, an extract from the commercial register, it can be proven that Puk is the owner of Puk BV. As the wholesaler trusts the KVK, the KVK is the trust anchor and the chain of trust is closed.

2.7.3 Authorisation of the verifier

Because the statements contain (sensitive) data, these must not fall into the wrong hands. Prior to each transfer, it must be determined *who* the verifier is and whether this verifier is authorised to process the data within the statement in the intended manner. This responsibility may lie with the issuer, with any intermediary (vault or safe) and/or with the subject.

ssuers usually have a duty of care towards the subject of the statement and will therefore be (partly) responsible for the authorisation of the verifier. However, it may also be undesirable for the issuer to have knowledge of individual transactions between the subject and verifier. With a physical identity card, for example, you can enter any bar or casino without the issuer (the municipality) ever being aware of this. In the digital domain, however, things are different. When someone logs in somewhere using DigiD, DigiD registers the metadata of that log-in attempt and, in theory, the government can look over the behaviour online.

In many cases, a subject may also have control over who may view his or her data and therefore want to have control over the statements that concern him or her. A digital identity infrastructure can help to authorise both the issuer and the verifier for the respective issuing and use of statements. At the same time, such an infrastructure can guarantee that the subject retains control over statements that concern him or her.

2.8 Towards a digital identity infrastructure

A digital identity infrastructure can improve service provision considerably by making it easy for people and organisations to *identify* and *describe* each other at a high level. The interface between the issuer, subject and verifier (statement transfer) and the interface between administration and subjects (key management and authentication) lend themselves well to standardisation. Two *functional* ideals follow from the previous analysis:

1. Ideally, the infrastructure should offer subjects at least one (pseudonymous) link to administration so that they can make themselves known there independently of third parties.
2. Ideally, the infrastructure allows each party, including subjects themselves, to effortlessly issue their own statements and verify those of others while allowing the subject to control the statement transfer.

The rest of this vision document builds on the general description of the context given above and gives form and direction to a digital identity infrastructure.

Back to Table of Contents

3 Shared values

In order to manage and value the development of a digital identity infrastructure, it is necessary to determine what we mean by 'valuable'. Which norms must be adhered to at all times? And what freedom must the users of the infrastructure have in order to find the desired balance between values themselves? The previous chapter introduced nine relevant values. In order to arrive at a weighted framework of values and norms, more research and consideration are required. This chapter is a first step towards a common framework in the form of considerations under each of the nine values.

3.1 Usefulness: a helpful answer

The use of identity resources always serves a certain purpose. For example, a service provider wants to personalise services or protect them against unauthorised users. This purpose is first translated into a specific information question, such as "is the subject 18 years or older?" or "can the subject pay this rent?". Next, it is determined which data, from which source (such as an identity document), should provide *an answer* to that question. The usefulness is the extent to which the verifier can do something with the answer.

a) The answer to the information question – the result from authentication or a statement transfer – serves only the intended purpose.

3.2 Informational privacy: a minimal answer

Informational privacy concerns the protection of (personal) data and is, by definition, at odds with the need to identify (or describe) someone in order to provide a service. A balance must always be struck between the benefit and the impact on privacy. As is also laid out in the GDPR privacy regulation, the following two principles (among others) play a role in this: **proportionality** means that the purpose outweighs the impact on privacy; **subsidiarity** means that if the same purpose can be achieved with an alternative means that has less impact on privacy, this alternative must be used. The envisioned digital identity infrastructure is such an alternative. Considerations:

a) The issuer of a statement determines the (amount of) information it contains. The paper-based credentials, which often contain a collection of data, can be issued one-to-one as a digital statement. The great advantage of digital statements is that they are much cheaper. After all, a digital signature which guarantees the integrity and authenticity of the statement is cheap to produce. This makes it possible to issue statements at an attribute level (or even smaller). Other mechanisms that can limit the amount of transferred information, such as Zero-Knowledge Proofs (ZKPs) can also be used. In addition to facilitating granularity, it is also conceivable that an infrastructure will encourage or even help enforce the keeping of data sharing to a minimum.

Back to Table of Contents

b) It is not possible to guarantee what a party will do with certain information after it has obtained it. However, an infrastructure can help record which party asked for which data at what time and which data were or were not subsequently provided. Such records can serve as proof in the event of a dispute. This can also act as a deterrent against both unlawful requests for data and the unlawful use of data obtained.
c) If the impact on informational privacy can also be reduced, the subject is still asked to prove that he or she meets certain criteria. Removing the obstacles of informational privacy can actually result in more of these types of checks being made. This can harm privacy in its broader definition.

3.3 Representativeness: a precise answer

For fair treatment, it is important that the information question and the answer be representative of the subject. Does the answer cover everything? The danger of an (administrative) image is that it replaces the real person within processes. In other words: the administrative representation may be taken for an absolute truth. In reality, the answer to the information question is never a given (an irrefutable fact)[5] but always a statement by a certain party. Considerations:

a) Is the subject aware of the data and the purposes for which it is used?
Can he or she assess and influence them?

3.4 Checking the answer and the collection

It is important for the subject to have a certain degree of control over the use of his/her administrative representations. This is because these images affect how the subject is handled (in service provision) and their privacy. Considerations:

a) The subject must have insight into the use of his/her administrative representations. Among other things, it must be clear who has obtained which (meta)data and for what purposes. This **awareness** is the basis for the influence that the subject can exert on identity transactions indirectly (e.g. through a judge) or directly (through their own actions). This information must be made understandable. While full transparency towards the subject must be guaranteed, it is also important not to overburden the subject.
b) The **agency** which the subject has over a particular data stream varies by context. 'Consent' is just one of the possible legal grounds on which an organisation may process the subject's data. However, regardless of the legal grounds, it is important to respect the autonomy of the subject. Even if an organisation has the right to receive certain statements, it is up to the subject to transfer those statements. This is comparable to having a grip on money: even if someone has a debt outstanding, the creditor cannot just take this money away. When the subject actually has a **grip** on keys (and therefore identifiers) and data, both awareness and agency are guaranteed to a certain extent.

[5] While it may be treated this way in legislation, it is important to continue to recognise that in reality it is not.

Back to Table of Contents

c) When the subject actually had command of the attributes and identifiers actually lies with the subject, it still has to be considered whether the subject can actually control them. (Some) issuers of statements have a certain duty of care: a responsibility to protect the subject against unlawful or even harmful use of their data. When granting control, attention will have to be paid to the knowledge and skills that the subject needs in order to oversee the consequences and make sensible decisions, both in general as well as in specific contexts. General control could be increased by offering a consistent and familiar interface and providing advice (automatically) at a transaction level, among other things. The users of the digital identity infrastructure must have room to find the desired balance between protection and autonomy.
d) If consent is the legal basis on which data is provided, it is important that the subject retains an overview of all previously granted consent. It is also important that the subject can withdraw this consent immediately with a minimum of effort.

3.5 Reliability: a trustworthy answer

The identifiers and attributes of the subject can be an attractive target for identity fraudsters. Incorrect authentication can lead to substantial damage for both the verifier and the subject, but also for third parties. In addition, the subject must also be able to determine that the verifier is trustworthy and is the right organisation for the transaction at hand. Considerations:

a) In principle, no one other than the lawful subject should be able to prove that he or she belongs to his or her identifiers. When the digital identity infrastructure makes it possible (and easy) for people and organisations to create and manage their own keys, a high degree of certainty can be realised in identity transactions. To achieve this, it is important that the parties involved can verify these keys independently without the intervention of a third party.
b) When authentication is reciprocal by default, the subject is always sure of to whom he or she is authenticating or presenting data. This reduces the chance of phishing, among other things.
c) The reliability of a statement consists of its integrity, authenticity and the extent to which the statement is linked to the subject (subject-binding). If these qualities are guaranteed in the statement itself (in the same way that a physical passport has authenticity features), the statement becomes mobile and retains this value regardless of external factors. The statement itself then contains the proof of authenticity, thus eliminating the need to contact the issuer of the statement.
d) However, it is possible for statements to lose their validity after they have been issued, such as because the original data has changed (like a change of address) or because it was later found that the statement had been issued in error. In summary, the status of a statement may change after it is issued and that status may be relevant to the verifier. The digital identity infrastructure must facilitate the communication of status without infringing on privacy, control or other values discussed here. The considerations regarding change of status require further investigation.

Back to Table of Contents

3.6 Availability: always an answer

Many essential processes depend on authentication and the transfer of statements. If the necessary systems are unavailable, this can have serious consequences for people and organisations. For example, a DigiD malfunction or attack would paralyse a large part of the (digital) communication between citizens and the government. Similarly, if the necessary data are lost or lose their value – such as diplomas that can no longer be verified in the event of the cessation of the educational institution – this is problematic for the subject. Considerations:

a) The pursuit of a widely used digital identity infrastructure means that this will play a critical and therefore indispensable role in the provision of services. If (parts of) the infrastructure become unavailable, people and organisations will no longer have access to (vital) services. It is unacceptable to introduce central weaknesses to the system.
b) It is important for subjects that their access to administrative representations, identifiers and attributes remains available for as long as they wish. This also applies to withdrawn or rectified statements on the understanding that the withdrawal or rectification is always visible to verifiers (a subject cannot present an invalid statement as valid). Which factors threaten the availability of identifiers and attributes? What measures does the digital identity infrastructure take against these threats?

3.7 (Communication) privacy: no leakage of (meta)data

Authentication requires at least communication between the subject and the verifier; transfer of statements also involves a source. Depending on the design of the infrastructure, multiple parties are active during a transaction, such as data processors, data vaults and data safes. It is important for the subject that as few parties as possible have knowledge of (1) the information that is communicated (informational privacy), (2) the metadata of that communication – who communicated with whom and when (metadata/communication privacy) – and (3) the relationship between the subject and verifier. Considerations:

a) When developing a digital identity infrastructure, the aim must be to have the least possible impact on (communication) privacy. The allocation of roles and tasks within the infrastructure contributes significantly to this. What insights into (meta)data follow from each of the assigned roles? Is it possible, for example, for parties to act as data vaults or safes? Does the issuer of statements have insight into how the statements are used and/or with whom they are shared? Such insight (or oversight) may also be labelled as necessary, such as from a duty of care perspective. However, the question is whether such interests (the protection of subjects) can also be achieved by other, less invasive means (the principle of subsidiarity). The aim is that only those parties that are necessarily involved should have knowledge of the relationship or communication (metadata) between subject and verifier.
b) Regardless of the choice, it is important that there is transparency at a system and a transaction level about which parties are involved and the degree of insight they have into transactions. Only with this knowledge can people and organisations protect their own privacy.

Back to Table of Contents

3.8 Friction: an effortless answer

Efficient and effortless processes are typically seen as desirable. From this perspective, the aim is therefore to make authentication and the transfer of statements as quick, easy and cheap as possible. However, critics point out that friction also has a positive effect[6]: the effort, costs and time required ensure that less data is shared and that people do not have to provide proof for every little thing. Friction can therefore be a natural means of protecting the privacy of subjects. However, this is a tool over which one has little control: it is a disadvantage for all applications, not just the undesirable applications of authentication and the transfer of statements. A universal solution may significantly reduce the effort, costs and time, but it does require a new form of (artificial) friction to prevent this negative effect. Considerations:

a) Basically, it is desirable to make the use of a solid identity infrastructure (in which the relevant values are safeguarded) as accessible as possible. This prevents parties from having to fall back on less favourable alternatives.
b) At the same time, it is important that it not be made too easy, such that people (and organisations) are no longer aware of the information collection (and assessment) that is taking place or that they too easily engage in risky practices. The digital identity infrastructure must be visible and/or evident.
c) Prior to the deployment of a digital identity infrastructure, the effect of this friction reduction must be examined and ways of limiting the resulting risks (such as overkill) must be sought out. Refraining from digitising the collection of information is an explicit consideration in this respect.

3.9 Fragmentation: information separated as much as possible

Every organisation (or other person) with whom the subject has a relationship will have its own representation of that subject; the administrative representation formation is thus **fragmented** across all those organisations (and people). This fragmentation is natural because representation formation is fundamentally subjective and personal, and other things are relevant to the nature of each relationship and context. At one extreme, **fragmentation** can be seen as a *positive value*. The other extreme is a comprehensive representation of the subject, which can be used to target or otherwise manipulate them. Such a comprehensive representation is also an attractive target for hackers. On the other hand, fragmentation can be a *negative value* if it prevents the verifier from forming a useful or representative picture. Considerations:

a) Is fragmentation a threat? Is there a risk that naturally separate administrations will be linked together by one party? For example, because data from different administrations are communicated via a single node?
b) Is correlation (of transactions and/or administrative representations) actively being tackled, such as by standard using a unique pseudonym for each relationship instead of using a single identifier in various contexts? And (for whom) can the issuance of a statement be correlated with the presentation of that statement?

[6] https://philipsheldrake.com/2020/11/the-dystopia-of-self-sovereign-identity-ssi/

Back to Table of Contents

4 A shared mechanism

Chapters 2 and 3 outlined an enormous common challenge: a digital identity infrastructure with great potential for both service providers and users and for people and organisations. **An infrastructure that connects cultural, organisational, political, legal and economic 'islands' and in which the subject has control over the exchange of information that concerns him or her.** This application space is much larger than that for which previous trust networks or agreement systems were developed. This is *terra incognita* – unknown territory.

In today's digital domain, trust services play an important role. Figure 6 shows examples in which authentication is mediated by a variety of services or applications, such as (1) an authentication service, (2) the transfer of statements occurring directly between the source and verifier and (3) mediation by a data vault or safe. The dependency, influence and surveillance that these forms introduce – as well as the lack of control by the subject – mean that these forms infringe on the values discussed in the previous chapter. **How can all of these islands be connected without direct communication or mediation by trust services?**

It seems a logical step to let *the subject itself* connect those islands. After all, 'he or she' is the only similarity between all information questions that are about 'him or her'. This corresponds to the SSI philosophy. This idea is not strange: after all, the subject also bridges all these islands with physical passports. But the nature of the *digital* domain is much more complex, dangerous and, above all, elusive; whereas one sees a unique and recognisable human being in front of him or her in the physical world, one showing a legitimate passport with his or her face on it, one sees only a series of zeros and ones in the digital world. The laws of nature limit physical reality and thus make it more transparent and predictable. They form an involuntary contract between all people (and organisations) which does not need to be enforced because it is impossible to violate those laws – regardless of intent or ignorance. Natural laws form a **mechanism** that is lacking in the digital domain.

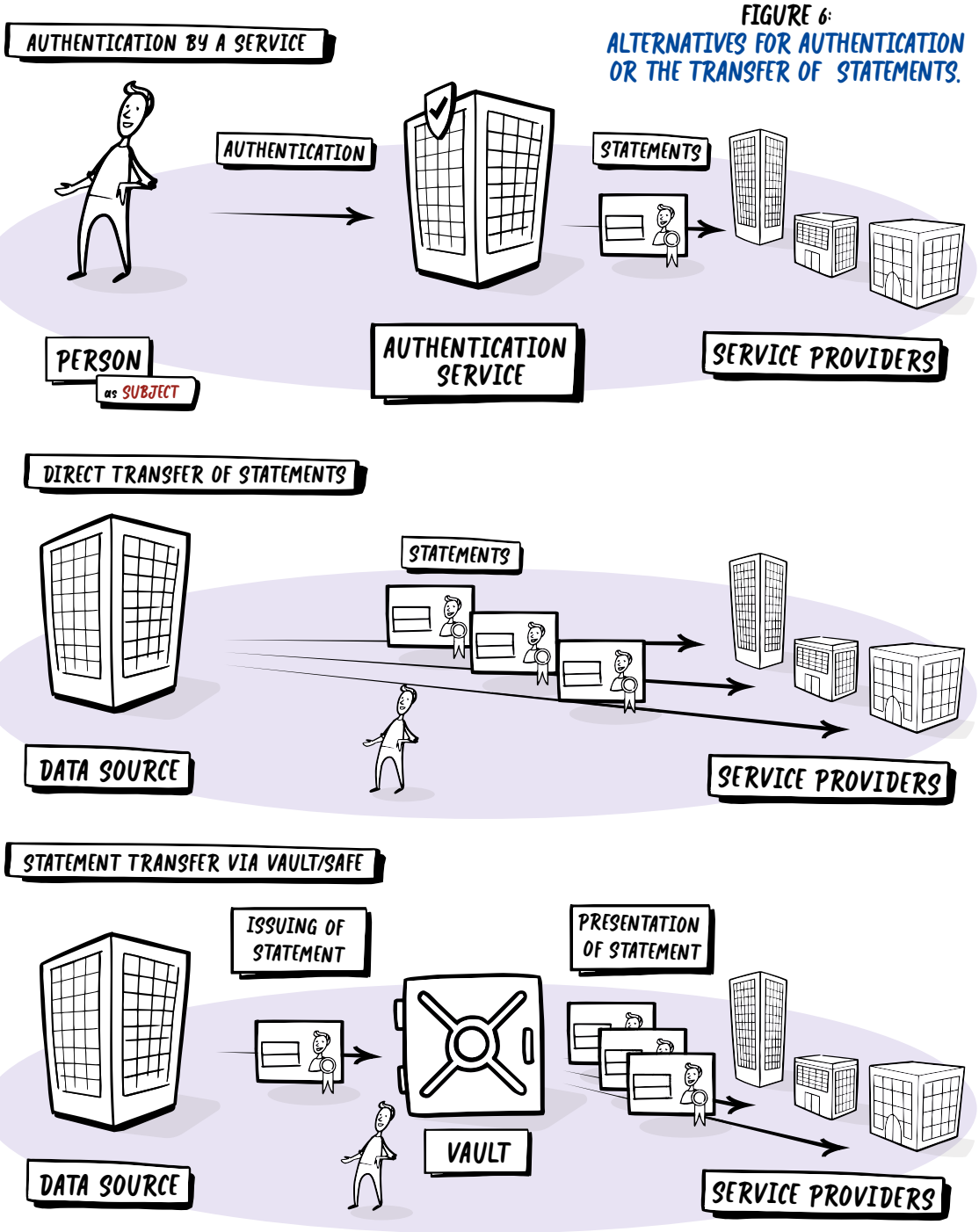
As a result of technological developments that have come together in recent years under the name Self-Sovereign Identity, we now seem to be able to realise an equivalent mechanism in the digital world. **With a transparent and predictable mechanism, *the subject itself* can play the central role in the exchange of information.** Verifiers can consult the subject directly and independently. Everyone gets the same mechanism in the form of standards and software, with which the transfer of statements and authentication become commonplace. **This network of mechanisms forms a decentralised digital identity infrastructure.**

In order to design the mechanism – or put an already designed mechanism into practice – it must be possible to guarantee that it (only) achieves the desired outcomes. The enormous potential and demand for Self-Sovereign Identity comes with a major risk: **recentralisation**. If control over the exchange of information falls into the hands of a small group of organisations – such as big tech, big finance or big telco – instead of being distributed among subjects, this will have the opposite effect. The result is an unprecedented concentration of power and surveillance. **Perhaps the greatest challenge of Self-Sovereign Identity is the permanent guarantee of decentralisation** – that each subject continues to hold the key position in matters that concern him or her. On the one hand, this challenge is technical and organisational (making decentralisation *possible*) but, above all, it is legal and policy-related (making

Back to Table of Contents

sure decentralisation *happens*). Even temporarily, such as in the start-up phase, it can be risky to tolerate central components. **The independence of the subject must be guaranteed in every detail of the technical, legal and policy design.**

FIGURE 6:
ALTERNATIVES FOR AUTHENTICATION OR THE TRANSFER OF STATEMENTS.



Back to Table of Contents

5 How then? A shared building plan

The previous chapter argued that the subject must be central and be able to authenticate and transfer statements independently in order to be sure that their values are safeguarded. At the same time, it is unreasonable to expect every person and organisation to be actively involved in these matters all the time or to have sufficient knowledge and skills to manage this sensitive and important process properly all by themselves. How do we make it possible for (almost) every person or organisation to become the connecting and controlling factor?

The answer is to provide every person and every organisation with a new tool: a digital assistant, also called an *agent* or *wallet*[7] in Self-Sovereign Identity. This digital assistant will probably come in the form of a smartphone app and help people and organisations to manage their identifiers, keys and data responsibly. The assistant ensures that the subject retains both insight into and control over data. Verifiers can ask the subject for all kinds of data via his or her digital assistant. By always presenting this in a familiar and consistent interface, the subject becomes familiar with this type of transaction. The subject will only be asked to allow or deny this request. When 'consent' is the legal ground for this data request, the subject can give informed and uninfluenced consent for the data processing and withdraw this consent at any time. In the background, the assistant takes care of the necessary security checks to protect the subject from injustice and errors. It can also automate other tasks, such as forwarding changes to data (e.g. change of address). In this sense, the digital assistant is a trust service, but is transparent, predictable and under the complete control of the subject[8].

Not only does the subject have such an assistant, but so do the issuers and verifiers. Their agents facilitate efficient and secure data sharing in which the origin and integrity are safeguarded. They also standardise communication with the subject's agent. If these agents are sufficiently generic, they can add significant value in many sectors. The following example illustrates the enormous potential of such an assistant.

[7] The term 'wallet' is often used to suggest a resemblance to the physical wallet that contains identity documents, among other things. Because this analogy does insufficient justice to the (mathematical) power and functionality of the software, we use the term 'agent' or 'digital assistant' here.

[8] To guarantee this transparency and predictability, it is necessary to make the source code of the digital assistant public and to supervise the (further) development of this source code. This makes digital assistants openly verifiable. This is a big step forward but we must consider the fact that few people are capable of verifying the integrity of the source code themselves. The rest will still have to rely on the software (supplier) or on third parties who have verified the source code.

Back to Table of Contents

Box 3. Example of data transfer when renting a house

Pim wants to rent a house. The housing corporation has one question: will Pim be able to pay the rent? Since this cannot be predicted, they base their decision on two aspects: does Pim have sufficient income or capital? And has Pim always paid his debts properly in the past?

It is not uncommon for landlords to request dozens of documents from different agencies in order to answer these simple yes/no questions. The result is that landlords are given an unnecessary amount of personal information. The process is also a considerable burden for both parties: Pim has to manually retrieve all documents from all sources and the landlord has to verify and review them. And there is also the question of what happens to these documents after it has been determined whether Pim can indeed pay the rent with sufficient certainty or not.

If the data sources, the landlord and Pim all have an agent, this process of several days – or even weeks – is cut down to seconds. The landlord's agent sends a detailed data request to Pim's agent, detailing which statements are needed from which agencies and why. Pim's agent can instantly (remotely) access those agencies and collect the requested statements on his smartphone. With Pim's permission and confirmation, the statements are presented to the landlord. Pim has proven – via facial recognition, a password or other means – that he is behind the screen and belongs to those statements. Within seconds and with minimal effort by all parties and the preservation of privacy and self-determination, the registration process is complete and Pim can rent or not.

This example shows that the potential of widely available agents is enormous. It is likely that all parties involved will benefit and that the costs will be significantly reduced. The social and economic benefits justify a considerable effort in the development, regulation and deployment of these agents.

Pim's example can already be achieved with the available technology. The developments and experiments are in full swing, but there are still many questions to be answered. In the domains of policy, legislation and ethics in particular, a lot of effort is required to ensure that this fundamental technology – critical infrastructure in the making – only achieves *desired* outcomes. This chapter discusses some fundamental design choices to provide the insight necessary for responsible development.

5.1 Condition: exclusive possession of devices

The agent is the 'control instrument': the software that performs and keeps track of everything for the subject and 'represents' it, as it were. The agent can represent the subject in a wide range of scenarios. The agent collects, stores and shares all kinds of personal information and also has insight into the metadata: with whom and when the subject conducts transactions. It thus has a particularly intimate view of the subject. The agent also manages the subject's keys with which the subject authenticates itself and possibly also signs all kinds of documents and expressed desires. The agent is thus not only the digital face but also the digital voice of the

Back to Table of Contents

subject. Because the agent has unprecedented power and visibility over the data and keys of the subject, it is essential that the agent remains under the exclusive control of the subject at all times. This is only possible when the device on which the agent is installed – and on which the identifiers, keys and data are stored – is also under the exclusive control[9] of the subject.

This condition raises a number of points of attention, three of which are highlighted here: inclusion, loss & theft, and recentralisation.

5.1.1 Inclusion

Not everyone has a smartphone or any other device of their own. Not everyone is old enough, young enough or otherwise capable of operating one. Not everyone can (or wants to) buy or use a smartphone. Sometimes the smartphone belongs to the employer, so ownership is not exclusive. This condition – exclusive possession of a personal device – risks excluding these people.

On the one hand, all technological developments simply have to deal with this challenge. It would be a missed opportunity to deny the rest of society the enormous potential. Also, it would be unjustified to use this objection to make the trust service central again; if that were used to solve the problem, the risks would be enormous. The question that needs to be asked is how people without smartphones can still reap the benefits.

One answer is (partial) representation. The agent of a parent or guardian can prove that this parent or guardian is authorised to represent a child in certain matters. This is not limited to parent-child relationships: as far as technology is concerned, any person or organisation (or thing) can be represented by any other person or organisation.

Nevertheless, a regular alternative – consisting, for example, of physical (or telephone) counters, guidance and support, and the human touch – is necessary to ensure that everyone can participate.

5.1.2 Loss and theft

Of course, a smartphone or other device is susceptible to theft, damage or loss. To protect against this, identifiers and data should be properly backed up. Also, keys should be deactivated outside the phone to prevent someone else from using them to commit identity fraud. An *emergency plan* for scenarios such as theft, damage and loss falls outside the scope of this vision document. However, it is an essential issue, one that must be approached primarily but not exclusively from a technical perspective. The challenge is to take measures that simply work without the subject doing anything about it and without falling back on centralised solutions.

[9] With the understanding that smartphone security is never foolproof either.

Back to Table of Contents

5.1.3 Recentralisation

Nothing in the (technical) design of agents prevents people from using a cloud-based agent. In other words, with a trust service. Many will see this as an advantage, unaware of (or uninterested in) the dangerous level of power and control they are handing over. For big tech companies, this can be lucrative: they can offer a very attractive *cloud agent* cheaply or even for free and make money from the insights that they thus accumulate on behaviour and relationships or perhaps even personal data. This achieves precisely the opposite effect: all of the data and transactions involving an agent are then held by one and the same party. Even if the service is offered by a non-profit or government organisation, the risks remain. Commercial takeover or privatisation must be out of the question. But such a central service, in whatever form, remains an attractive target for (state) hackers: if not for the theft of keys and (meta)data then certainly for bringing this critical infrastructure to a standstill.

It is not only subjects that are vulnerable. When data sources and service providers outsource their connection to SSI, the same centralisation is threatened. This creates the appearance of a decentralised network in which a small group of processors actually have the power. This technology has great potential for giving control back to the subject but also for taking it away.

Recentralisation is a real danger. This requires an active search for solutions. After all, a new – and, in many ways, better – system should not result in us going from bad to worse.

5.2 Authentication with agents

The subject must be able to prove he or she corresponds to the identifiers and attributes that actually belong to him or her. This must be possible at all times and no one other than the subject must be able to do this. When designing a digital identity infrastructure, it is necessary to look at which factors could threaten these principles. As argued in Chapter 4, intermediaries constitute such a risk because of the dependence, influence and surveillance that can arise as a result of them. The first question is therefore how the service provider can authenticate the subject using their agents and without the intervention of or dependence on a third party. Because this does not appear to be possible in all cases, a second question follows: how should a digital identity infrastructure deal with situations in which it is not possible to authenticate without a third party? An in-depth analysis of these two design questions is beyond the scope of this document. However, this section provides insight into some important considerations.

5.2.1 Complete control over identifiers

If the subject wants to have full control over identifiers and statements, he or she will have to be able to personally create these identifiers. Email providers often allow subjects to choose their own email address as long as it is not already in use. Identifier management is then entrusted to the email provider; this provider thus takes over the role of identity provider. However, the subject – the person behind the email address – always depends on the email provider to prove 'who' he or she is. One alternative is to replace the identity provider with a distributed registry (blockchain). The process is roughly as follows:

Back to Table of Contents

1. The subject claims an available identifier and registers it in the distributed registry.
2. The subject also generates his or her own cryptographic keys and links the verification key (public key) to the chosen identifier in the registry.
3. When the verifier wants to check the subject, the subject presents himself or herself with the identifier chosen in step 1.
4. The verifier consults the registry and finds the verification key with which he or she can authenticate the subject.
5. As long as the subject has the secret key which is mathematically linked to the verification key, he or she can prove ownership of the identifier.

Of course, these tasks are taken care of by the agents of the verifier and subject. Neither people nor organisations need to know about the underlying technology. The main advantage of this solution is that the registry cannot be manipulated just like that and that the verifier and subject can authenticate directly without the need for the intervention of a third party. This alternative – self-claimed identifiers recorded in a distributed registry – can be facilitated with current technology. The applicability of this technology, however, depends on the requirements imposed by the verifier with regard to identification. For cases in which a self-claimed identifier is unsuitable or insufficient, the control of identities and/or keys can (additionally) be entrusted to an external party.

5.2.2 Authentication with third parties

When a third party is involved in authentication, the subject (and the verifier) become dependent on that party. However, by putting the subject at the centre, it is possible to give that subject control of and insight into the authentication process and to prevent the authentication service from having insight into individual transactions or relationships between the subject and the verifier. Figure 7 illustrates how authentication by a third party can work using statement transfer.

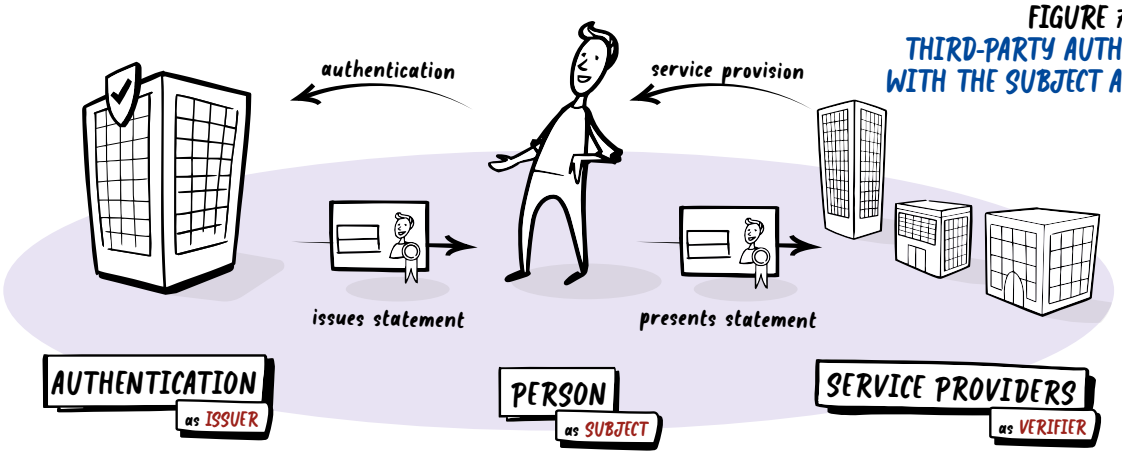


FIGURE 7:
THIRD-PARTY AUTHENTICATION WITH THE SUBJECT AT ITS CENTRE

Back to Table of Contents

The authentication service can authenticate the subject in the usual way (with a password, an SMS or other means) and then issue a statement to the subject showing that he or she was authenticated at that time. The subject can forward this statement to the verifier, who can be confident that the correct subject is behind the agent if this is done in a timely manner.

5.2.3 (Further) development of mechanical identification and authentication

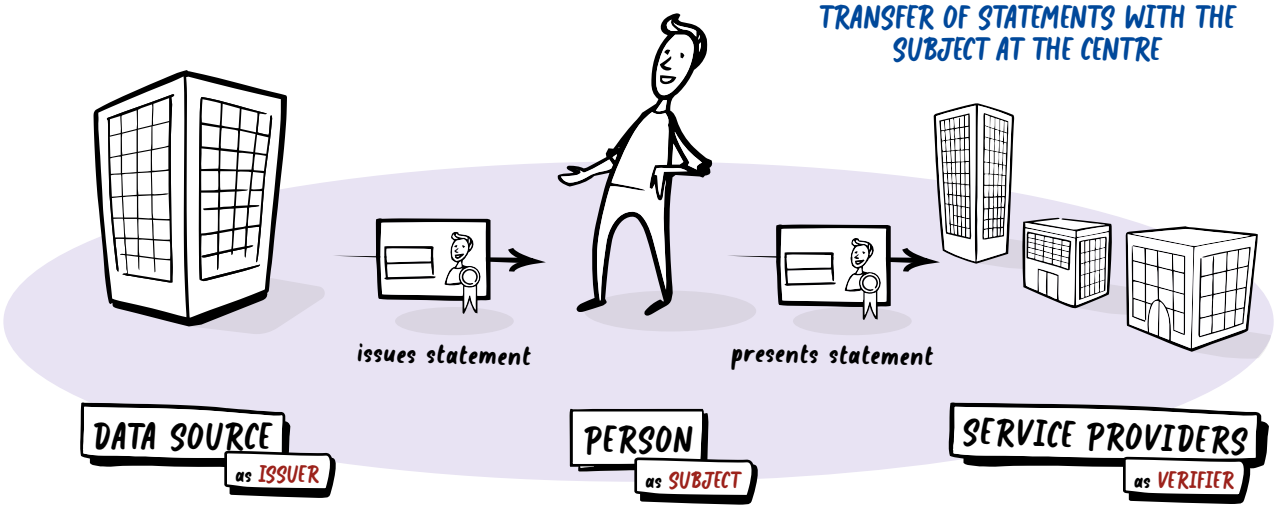
The previous two sections illustrate two ways in which the subject can authenticate itself to verifiers. A combination of these methods can also provide added value. However, the mechanical solution is preferred because it is independent and transparent. To encourage the development of this mechanism, it is first necessary to identify the requirements that verifiers may place on identification and authentication and the mechanical means by which these requirements can be met.

5.3 Transfer of statements with agents

To be suitable for a range of applications, the network of agents must be designed to be sufficiently generic instead of for a specific (set of) use case(s). This is why the problem analysis in Chapter 2 was presented from a general perspective.

If the subject is legally or morally in control of the data sharing, it is desirable to give the subject real **control** over it and, as argued in Chapter 3, to put it at the heart of the process of transferring statements (see Figure 8). This means that the issuer gives the statements to the subject and that the subject can share them with any verifier it wishes. This same pattern can be recognised in the example of Pim: he collects the statements from the different agencies and presents them to the housing corporation.

FIGURE 8:
TRANSFER OF STATEMENTS WITH THE SUBJECT AT THE CENTRE



Back to Table of Contents

Three important points of attention:

1. Can data minimisation be guaranteed?
2. Is it a good idea to let the subject take control of the data?
3. And how can we withdraw statements if they are no longer current?

5.3.1 Data minimisation

For each application, it will be necessary to weigh up whether the usefulness of the information transfer outweighs the impact on privacy. In the interests of privacy, only the minimum required data should be shared for the minimum required duration. An interesting design question is whether it can be structurally – mechanically – guaranteed that only the minimum information is always shared.

There is a prevailing view that yes/no questions, by definition, have a minimal impact on privacy. The game Twenty Questions illustrates why this is not a safe assumption: the challenge is to determine who someone is with a maximum of twenty yes/no questions. Additionally, yes/no questions are too restrictive for many applications, such as when giving an address.

The (developer of the) agent cannot judge the content and the trade-off between privacy and usefulness in advance because this is contextual and subjective. This consideration is made in each case by the parties involved: issuers, subjects and verifiers. However, mechanisms can be designed to support these parties in this consideration, as discussed in the following sections.

5.3.2 Data control: a good idea?

The subject is, within certain limits, in control of data; when a party requests data, it is up to the subject to grant or deny access. The agent can consistently make clear to the subject *who* is asking for *what* data and *why*. The subject can grant permission using the agent and later withdraw it at any time. Still, the risk remains that the subject will make an unwise choice and share too much or too sensitive data with the wrong party. This can prevent issuers who have a duty of care towards the subject from giving him or her control over sensitive data. To reduce the likelihood of unwise data sharing and still achieve control over data, two resources can be used: **control support** and **control restriction.**

1. **Control support:** the agent advises the subject on data sharing, such as by reporting whether or not the verifier is on a list of trusted parties or whether or not the requirements have been satisfied. Such advice can come with different degrees of importance: inform, warn or alarm. However, it remains advice though which the subject, with some effort, may still choose to continue.
2. **Control restriction:** the agent refuses the request, regardless of the subject's wishes, if the verifier cannot demonstrate compliance.

Back to Table of Contents

For each statement (or type of statement), issuers can specify which requirements verifiers must satisfy in order to inspect it and whether those requirements are advisory or restrictive; for example, the BSN may only be shown to government organisations. Of course, issuers must consider the interests of the subject and the applicable legislation. If agents are able to apply this support or restriction independently, this does justice to the duty of care of issuers and thus lowers the barrier to adoption.

5.3.3 Current state

Most data are changeable. Statements based on variable data are always snapshots. If a piece of information changes, statements issued earlier may still be relevant but no longer current. For example, a statement about the ownership of a company is no longer current after that ownership is sold, but it may still be relevant to the tax authorities, for example. In many cases, verifiers need to be able to check how current the data is but cannot contact the issuer for this. After all, doing so would give the issuer knowledge of the transaction between the subject and verifier, which would be detrimental to privacy. However, once statements are issued, an issuer has no control over them. It cannot force the subject to remove or modify the statement. So, how can the verifier still determine with certainty how current the statement is?

A first option is to renew statements each time. When the subject shows an out-of-date statement, the verifier could ask the subject to retrieve that information from the issuer again. If the data has changed in the meantime, the subject will not receive a new statement. The problem with this option is that the statements lose their value within seconds and the subject is again dependent on an issuer that must cooperate, be available and continue to exist.

An alternative is to publicly keep track of the withdrawal of statements in a revocation registry in which the issuer publishes a reference to each issued statement it has revoked without disclosing the identity of the subject. Blockchain technology is increasingly becoming regarded as the solution to this problem. The development and operation of this revocation registry is a separate concern in addition to the development of agents.

Back to Table of Contents

6 And now what?

This vision document is intended to be a common starting point for everyone who is involved with decentralised digital identity in the Netherlands, both from a policy and an operational perspective. This document is therefore a guideline and not a manual. It does not prescribe what a solution should look like but it does help in thinking about the choices that need to be made in the design of an identity system. The vision document is also a living document. This means that it will be supplemented and adapted in response to the practical implementation of SSI and other decentralised digital identity systems. Shared values, a shared mechanism and a shared building plan will enable us to get started.

Practical implementation is therefore an important next step, both in the design of infrastructure such as the Dutch Trust Network (DTN) and in the design of upper echelons of the technology stack such as agents/ wallets. Actual implementation based on cases such as setting up a private limited company, exchanging data on diplomas and certifications obtained or a different interpretation of KYC/AML will provide useful insights through which this document can be further developed and supplemented.
There are also more fundamental questions that are worth investigating. Collaboration with the knowledge partners of DBC is indispensable in this.

In the European context, we want to use the common starting point to help eSSIF and EBSI, for example, but also the framework for European Identity recently announced by the European Commission. One thing is certain: we agree on the starting point but will implement it in practice using different means.

Substantive reactions to this document are very welcome and can be sent in written form to dssif@dutchblockchaincoalition.org. You can also join the discussion by becoming a partner[10] of the Dutch Blockchain Coalition and participating in working groups and/or other meetings.

[10] Partnership of DBC is open to any Dutch organisation from government, business or knowledge institutions. For more information, see https://dutchblockchaincoalition.org/over-dbc.

Back to Table of Contents

7 Glossary

- **Administrative representation** – A set of data/attributes which a party has about a particular subject, characterised by one or more identifiers.
- **Administrative representation formation** – The actions/processes by which administrative representations are created.
- **User | Verifier (Verifier)** – (Role) A party that requests or uses certain data.
- **Agreement system** – collection of agreements that enables a network of parties to provide certain services.
- **Agent** – A software application that represents a party (in the role of issuer, subject and/or verifier) in identity transactions. Synonyms: wallet, digital assistant.
- **Attribute** – A specific piece of data about a subject.
- **Authentication** – A process of determining whether a particular party belongs to a (claimed) identifier.
- **Source** – Synonym for issuer.
- **Cloud agent**– An agent that is hosted in the cloud, as opposed to an agent that runs locally on a private smartphone.
- **Communication privacy** – The ability to communicate confidentially without third parties knowing what is being communicated or that it is being communicated.
- **Verifier** – Synonym for user.
- **Data minimisation** – Keeping the amount of information shared and/or processed to a minimum.
- **Data subject**– (Role) The party about whom certain data are taken. Synonym: subject.
- **Decentralisation** – Spreading power and knowledge among different actors so that it cannot be misused by one actor or create objectionable dependencies.
- **Digital assistant** – Synonym for agent.
- **Digital Identity Infrastructure** – The collection of agreements and facilities that jointly and generically enable authentication and statement transfer.
- **Fragmentation** – The state in which information is dispersed as much as possible to prevent one actor from obtaining an objectionable amount of information.
- **Friction** – Resistance in a broad sense (effort, time and money) that prevents parties from engaging in authentication or statement transfer.
- **Distributed registry (blockchain)** – A database/registry distributed across multiple actors in which the integrity of the registry is ensured by technology.
- **Data source** - Synonym for issuer.
- **Data safe** – A service (provider) that stores data from one or more issuers and, under the direction of the subject, presents that data to verifiers.
- **Gegevenssluis** – A service (provider) that transfers data from one or more issuers to verifiers under the direction of the subject. Unlike a data vault, the data safe does not store data.
- **Data processor** – (Role) A party that processes data. Synonym: processor.
- **Identify/identification**– make an identifier of a person or organisation known
- **Identifier** – A piece of data or combination of data that uniquely identifies a subject.
- **Identifier management** –The creation, maintenance and destruction of identifiers.
- **Identity fraud** – (Unlawfully) impersonating another person or organisation.
- **Identity chain** –A chain of organisations that exchanges identity information.
- **Identity system** – An information system in which identity data are managed.
- **Identity Provider** – A service provider that manages identifiers and authenticates subjects.
- **Issuer** – (Role) A party that issues certain data/statements. Synonyms: source, data source.
- **Metadata** – Data that describes the characteristics of certain data or processes.
- **Revocation Registry** – A registry that records which issued statements have been revoked and are therefore no longer valid.

Back to Table of Contents

- **Self-Sovereign Identity (SSI)** – Intended design of identity systems in which knowledge of and power over data resides solely with the data subject. This can be achieved by providing each subject with an agent/wallet.
- **Key management** - Granting and revoking keys that allow individuals (or organisations) to prove that they correspond to their identifiers.
- **Sovereignty** – In the context of SSI: the ability of the data subject to actively control their own data. Sovereignty does not include modifying the statements of third parties, but it does include controlling who sees these statements and when.
- **Subject** – Synonym for data subject.
- **Verifier** – Synonym for user.
- **Trust anchor** – A party that one naturally trusts.
- **Processor** – Synonym for data processor.
- **Wallet** – Synonym for agent.

Back to Table of Contents

Core partners

Partners

Dutch Blockchain Coalition

connect and create

info@dutchblockchaincoalition.org

www.dutchblockchaincoalition.org