TNO innovation for life

Applying Verifiable Credentials in the Base Data Infrastructure

TNO Intern ⟩ TNO 2023 R12443
7 december 2023

ICT, Strategy & Policy

www.tno.nl
+31 88 866 00 00
info@tno.nl

TNO 2023 R12443 – 7 december 2023

Applying Verifiable Credentials in the Base Data Infrastructure

Auteurs	Maaike van Leuken Peter Langenkamp Wout Hofman
Rubricering rapport	TNO Intern
Titel	Applying Verifiable Credentials in the Base Data Infrastructure
Aantal pagina's	48 (excl. voor- en achterblad)
Aantal bijlagen	0
Opdrachtgever	Sjoerd Boot

Table of content

1 Executive Summary

TNO performed research into the applicability of SSI (Self Sovereign Identities), VCs (Verifiable Credentials), and DIDs (Decentralised Identifiers) for two use cases on behalf of the Dutch Ministry of Infrastructure and Water Management (IenW). These two cases were selected from several cases provided by stakeholders on behalf of the Ministry. The cases are the on-boarding of a node to the Base Data Infrastructure (BDI) and authorised pickup of goods at a physical location.

Since the BDI is to be developed according to the FEDeRATED architecture, onboarding is considered in an EU context. It is expected that DTLF will adopt the FEDeRATED architecture and recommend EC DG Move to apply this architecture for development of the European Mobility Data Space (EMDS), at least for freight. Thus, onboarding will be considered for the EMDS (freight).

The organisational structure of applying SSI/DIDs/VCs considers three roles: an issuer, a holder, and a verifier of a VC. The main aspect is that a verifier can authenticate a trusted issuer of a VC presented by a holder. It requires an issuing policy based on agreements adopted by the dataspace, in this context EMDS (freight) with accredited issuers. A VC can irrevocably be associated to a single holder (holder binding) or is transferrable to another holder.

We see an immense potential for VCs in logistics, not limited to the use cases that are explored in this report. Like for physical access, VCs can also be applied to data access. They can contain a claim that represents a permit or a driver's license. Many examples are listed by UN ECE (https://unece.org/sites/default/files/2023-10/WhitePaper_VerifiableCredentials-CrossBorderTrade.pdf). These additional use cases need further exploration.

Many organisations like the EC with the development of eIDAS2.0 and EBSI (European Blockchain Services Infrastructure) and those organisations collaborating in GAIA-X consider SSI/VCs are a pre-requisite for constructing a dataspace, also the EMDS due to its size (millions of potential users): VCs support scalability and can be based on existing developments. Having credentials for on-boarding is also a means for supervision: they enforce an organisation to be compliant with a Regulation before receiving credentials. They can also allow an on-boarded organisation to act as issuer for physical access (second use case).

However, developing an SSI/VC based infrastructure is complex, requires a clear policy, and we are not yet there. We recommend that the Ministry of IenW stimulates and supports the development of an EC framework regulation for EMDS (freight). Such a regulation will provide guidance for (future) investment by business. It is a voluntary regulation. In the context of such a regulation:

- Embedding in eIDAS2.0. An SSI/VC based infrastructure based on eIDAS2.0 is expected to be available by mid 2025. The Architectural Reference Framework (ARF) of this infrastructure leaves room for including specific requirements for the EMDS (freight). This refers to the credential structure for EMDS (freight). EC DG Move, as developer of this regulation for EMDS (freight) should take care of this. Version 2 of the ARF will be available mid 2025.

- **Organizational structure**. There must be issuers implementing an issuing policy. Issuing policies must be specified by an EMDS framework regulation. In the Netherlands, potentially eHerkenning brokers can act as issuers for on-boarding of a node. Enterprises can be issuers of credentials for other types of applications of VCs like the one of physical access. Trust of these latter issuers can be assured by the fact that they have on-boarded in the EMDS.
- **Credential structure**. A credential must contain a proof and can contain a claim. The claim can be a simple statement like being an employee of a company or can be context dependent. The proposed credential structure for the two use cases is specific to the EMDS and relates to the architecture developed by FEDeRATED. A global approach can be stimulated by an EU Regulation as illustrated by the adoption of for instance the GDPR (General Data Protection Regulation).
- **Technical infrastructure**. The various components must be available (and interoperable) for supporting various use cases. This may require wallets on (private) smart devices with holder binding. It also requires organizational wallets with authorised access by employees. Private initiatives like GAIA-X explore the development of an infrastructure with organizational wallets. Our recommendation is to monitor and experiment with these technical developments and apply them when legal code and organizational structure are in place. This means for instance the integration of VCs into the node and the application of VCs for physical access to pick up cargo.

The development and implementation of a solution based on an EMDS framework regulation will take time, three years or more. The implementation of such a solution will be gradual, with a deadline when it must be available. Since it is on voluntary basis, alternative solutions will still exist, even if the proposed solution comes into force.

Since development and support of an EMDS framework regulation by SSI/VCs takes years, intermediate solutions must be developed based on existing initiatives. Our recommendation is (1) the migration of the iSHARE technical scheme and Satellite software to support private - (GAIA-X) and public (eIDAS2.0) technical schemes to prepare itself for an EMDS framework regulation and (2) setup a Living Lab of a node and issuer supporting SSI/VCs for supply and logistics based on the FEDeRATED architecture. The solution can be made operational and will speed up the adoption of an EMDS framework regulation. Developing and applying a framework regulation takes time; support by (eIDAS2.0) based VCs will also take time. In the meantime, authentication tokens can be applied or iSHARE as an intermediate solution governing certificates issued to users. Tokens and an intermediate iSHARE based solution is however difficult to apply and might run into adoption issues for a large data space like EMDS with millions of both public and private users.

2 Introduction

Note to this version: comments of iSHARE and DIL/WP1 are still to be received and processed.

2.1 Problem statement

The application of Self Sovereign Identity (SSI), Decentralized Identities (DIDs), and Verifiable Credentials (VCs) is one of the activities in the support of the Digital Transport Strategy (DTS) and FEDeRATED. The aim of this activity was to provide input for Identification and Authentication (IA). A data user is authorized to access data based on a link that is shared via an event. Access control, which is another component of security, is based on what is called Service Design and its customization (formerly called 'plug and play) by a participant in the BDI.

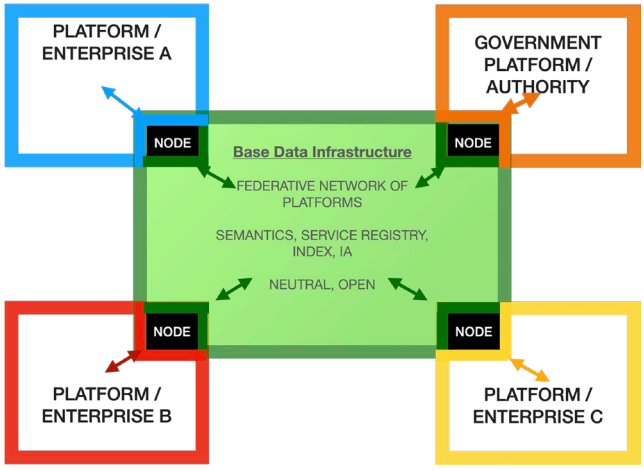
In particular, the questions formulated at the start of the activity for IA were:

- Infrastructure – which infrastructure is required and applicable for international data sharing applications in supply and logistics.
- DIDs – what does a DID look like and how can it be applied.
- Interfaces – how does a solution with SSI, DIDs, and VCs fit into the FEDeRATED architecture.

In the context of SSI/DIDs/VCs, the role and application of iSHARE requires further elaboration, for instance a potentially migration of iSHARE to SSI/DIDs/VCs.

2.2 Background

One of the objectives of the DTS is to create the Base Data Infrastructure (BDI), a 'federated network of platforms' where each participant has its own local interface (expressed by the colours of the arrows for each participant) to the infrastructure and shares data via its node (next figure). The figure shows that IA is one of the main features of this infrastructure.



IA can be implemented in different ways, depending on the technology used for data sharing. Under the assumption of the implementation of a node, Identity and Authentication must be implemented between the nodes.

It has been agreed that the BDI will be constructed according to the FEDeRATED architecture. This architecture is expected to be adopted by the Digital Transport and Logistics Forum, an expert group raised and chaired by EC DG Move. Another expectation is that the DTLF will recommend to EC DG Move to develop the European Mobility Data Space (EMDS) for freight with this architecture. Thus, the BDI can be the basis for EMDS (freight).

2.3 Approach

As part of the project, a peer group was established consisting of the lead architect of the Data Infrastructure in Logistics (DIL) program and one of the product owners of the BDI (Ewout Bouwman), the contact responsible person for BDI of the Ministry (Sjoerd Boot), and the main representative of iSHARE (Gerard van der Hoeven).

The approach taken consists of the following steps:

- Workshop introducing the concepts to the peer group.
- Proposal and selection of use case(s). The peer group members will make proposals for the use case.
- First sprint – the first use case.
- Interim workshop concerning the first sprint.
- Second sprint – the second use case.
- Second workshop of the second use case
- Third sprint for constructing a demonstrator.
- Final reporting.

During its execution, some choices and changes were made to the proposed approach and the problem statemen:

- A primary focus on VCs (see also conclusions). SSI as a concept typically relies on an infrastructure based on VCs, different technologies for which can be used. It also became apparent that there was no real need for DIDs separate from what may be used to facilitate the use of VCs, at least not in the use cases that were selected.
- The opportunity of a hackaton organized by IATA was seized to construct a demonstrator for the first use case. The result is documented and visualized by a video (https://youtu.be/6BRaltYYPd4).

In addition to the peer group, key persons in IAA were approached for consultation on the results. These were: Arjen Ketelaar (business manager IAMConnected, Portbase), and Mitchell Out, Arjen van Hees, and Edwin Platier (all Dutch Customs). The result of the conducted interviews are considered in the conclusions, since these indicate external developments that are relevant to the proposed solution.

With respect to the use cases, the following two were the main priority for the project:

- Identification and Authentication of nodes.
- Physical access to a location for pickup or delivery of cargo.

2.4 Structure of this document

The structure of this document is as follows:

- Section 2 – a general introduction to VCs
- Section 3 – use case ‘Identification and authentication of nodes’ (on-boarding) and positioning of iSHARE in this context.
- Section 4 – use case ‘Physical access to a location’.
- Section 5 – conclusions and recommendations.

In its application to interorganizational identification and authentication, iSHARE is discussed in the context of identification and authentication of nodes.

3 SSI basics

This section provides a common understanding of SSI as a basis for the use cases. .

3.1 Definitions

The following definitions provide background to this report. The list is not complete, but contains the most relevant definitions.

Identification: an act of identifying someone or something.

Authentication: an act, process, or method of showing something (such as an identity, a piece of art, or a financial transaction) to be real, true, or genuine.

Authorisation: the act of having permission (in this context: to access data or a physical environment).

Assurance: pieces of additional information relating to (holder) data, allowing the verifier to have more trust in the data. The verifier should assess whether the data with corresponding assurances is fit-for-purpose.

Verifier unlinkability: the verifier cannot link multiple presentations of the same holder to each other, i.e. the verifier does not know they are communicating with the same holder multiple times.

Issuer unlinkability: the issuer cannot see that the holder is presenting the credential issued by the issuer nor to which verifier the holder is presenting that credential.

Mandate: an authorization to act on behalf of someone else.

Delegating: the process of distributing and entrusting work to another person.

Transactional relationship: ad-hoc, one-time business (commercial) transaction between two parties for a single business activity.

Contractual relationship: a long-term relationship between two parties for outsourcing business activities.

3.2 Decentralised Identifiers

Decentralised Identifiers (DIDs) are globally unique identifiers and are often used in SSI solutions. A DID is associated with a DID document and at least one public-private key pair that is used to control the DID document. DIDs have the following properties:

- Permanent (persistent) - it never needs to change.
- Resolvable - you can look it up to discover metadata.
- Cryptographically verifiable - you can prove control using cryptography.
- Decentralized - no centralized registration authority is required.
- Globally unique.

3.2.1 DID Methods

The DID and accompanying DID document (typically a JSON or JSON-LD file, though other representations may be used) are created, revoked, updated, and deleted (CRUD) based on the DID method. There are currently around 162 different DID methods that work in a variety of ways, each approach having different benefits and drawbacks. The DID methods can be divided into roughly 5 categories:

- Ledger-based DIDs
  - Involves a distributed ledger technology (DLT).
  - Typically, public and globally accessible.
  - Created/updated/deactivated by writing transaction to the ledger, signed with DID controller's private key.
- Ledger middleware DIDs
  - Adds storage layer on top of the base layer ledger (on-chain DID).
  - Multiple DID operations are batched into single ledger transaction, increasing performance and decreasing costs.
- Static DIDs
  - Can be created/resolved, but not updated/deactivated.
  - Tend not to require complex protocols or storage infrastructure.
- Peer DIDs
  - Does not require a globally shared registration layer like a ledger.
  - Created and shared with only one (or small group of) peer(s)
  - Exchanged via peer-to-peer protocol, resulting in private connections between the participants.
- Alternative DIDs
  - A growing number of other innovative DID methods that do not fall into the previous categories.
  - DID identification architecture is flexible can be layered on top of other existing internet protocols.

In practice, the choice of DID method will be guided mostly by the category that is required to satisfy the requirements of the use case.

3.2.2 DID Persistence and Unlinkability

Persistence of DIDs means that you can reuse a previously set up connection and be sure that you are communicating with the same party as last time. This does come with an important caveat: Note that control over DID can be passed on; DIDs can be handed over by the current controller to someone else, somewhat akin to relinquishing control over a telephone number or email address.

Given the persistent nature of DIDs, an interesting scenario occurs when unlinkability is desired, for example for repeat interactions with the same Customs Officer. The straightforward approach is to have the Customs Officer generate a new pairwise DID for

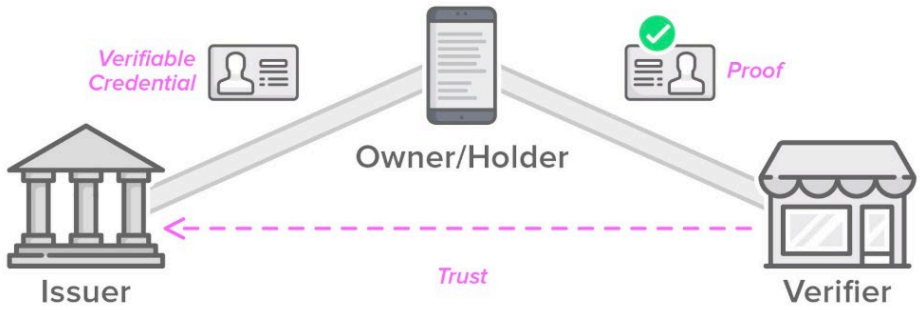
each interaction. This way, no persistent connections are used and the identifiers, keys and signatures are different for each new session, yielding *unlinkability without revocation*.

There's also scenarios where one might want to be able to revoke the unlinkability at a later stage, e.g. if a Customs Officer is subject to an inspection into their behaviour. This *unlinkability with revocation* could be achieved in different ways:

- Pseudonyms.
- Link secrets. A link secret is a unique, random string that serves as a *master identifier*. Only the owner knows the link secret, such that only they can link all variations together. To use a link secret, a *Pedersen commitment* can be made over it, allowing the owner to commit to the link secret, with the possibility to reveal the secret later. Others can then check that the link secret indeed belongs to the owner. To make the link secrets more practically usable, *blinding* can be applied. This allows the owner to reuse the commitment many times, while making them look different for each interaction, such that credentials cannot be linked together.
- Business wallet for VCs (representing for instance permits):
    - Organization as holder.
    - A business wallet stores the permits (VCs) provided by authorities (acting as issuers). Examples of these permits are AEO (Authorised Economic Operator), Declarant (for customs declarations), a permit for transportation of dangerous cargo (issued by ILT – "Inspectie Leefomgeving en Transport"), etc. Permission to act as a node in the network (see use case onboarding) is another permit. This latter permission is applicable to all organizations: enterprises, authorities, platforms, dataspaces (where platforms and dataspaces act on behalf of their users/members and behave as a single node).

3.3 Verifiable Credentials

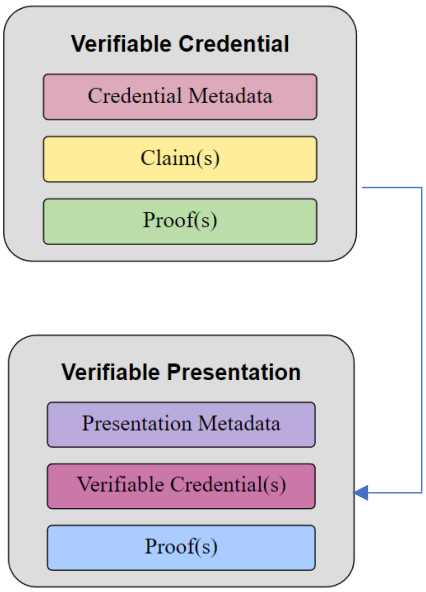
Verifiable Credentials (VCs) are used in the context of a model with three roles: the issuer, holder, and verifier.



In this so-called trust triangle, a holder receives a VC from an issuer. At the verifier's request, the holder is then able to share a verifiable presentation, proving to the verifier the claim(s) made by the issuer if there is trust between the verifier and issuer.

This simple model forms the basis for Self-Sovereign Identity and is broadly applicable. Below we will highlight a couple of important aspects of this type of infrastructure.

3.3.1 VCs and presentations



A verifiable credential consists of the following components:

- Metadata, like
  - Issuer
  - Expiration date
  - Public keys
  - Revocation mechanism, and
  - Any other data required by a use case
- Claim(s): the attestations about the subject
- Proof(s) — a.o. digital signature of issuer

Credentials may be used in different ways, and the kind of information they contain depends on the context:

- *A non-verifiable credential* just containing one claim (e.g. 'company' = 'TNO'). This offers no assurance as it is simply transferring information without assurances.
- *A VC without claims*. For some use cases having a VC with only the issuer information and proof, and no claim, may be sufficient. Possession of such an empty credential signed by a specific party could be enough assurance because the issuer in question only ever issues credentials under specific circumstances. This type of VC is typically unpractical, as parties tend to give out various types of credentials based on different criteria. It is bad practise in terms of scalability.
- *A VC with only a specified type*. Having a VC with only the credential type, issuer information and proof, and no claim. Possession of such an empty credential with a specific type signed by a specific party could be enough assurance if no distinction needs to be made based on credential attributes. Such a VC might be applied for low-assurance interactions.
- *A VC with claims.* The type of claim(s) is context-dependent and the actual information in a claim is transaction-dependent.

As the figure shows, a verifiable presentation or VP is distinct from a VC and normally contains information different from the VC itself.

3.3.2 VCs and wallets – holder binding

VCs are what is called 'tamper-evident: an issuer can be verified (cryptographically). Therefore, a VC can be transferred by a holder to another holder. Many commercial wallets support this transferability. Holder binding is the concept where a VC is irrevocably connected to the wallet of a holder and cannot be transferred to another holder. Holder binding may be a requirement for applications of VCs and thus needs to be specified per application.

3.3.3 Issuer and issuing Policy

An issuer has a certain issuing policy based on which a credential is issued or not. The issued credentials can be reused at a later moment in verifiable presentations.

The issuing policy provides clarity on whether some holder deserves to have the specific credential. It is the issuer that decides the issuing policy, and with that who they give out credentials to. A verifier can verify that the credential was indeed issued by that issuer. However, barring special precautions, they will have to rely on the issuer abiding by an issuing policy. Trust in an issuer is defined by the governance structure of that issuer. For

instance, a dataspace authority governed by its members can specify an issuing policy and certify issuers. This governance structure and its supervision mechanism(s) must be transparent to create trust in an issuer (see also the need of an accreditation mechanism later in this report). In any case the value of a credential to a verifier is determined by their trust in the issuer.

An issuer can provide assurances on who is eligible to receive the credential:

- Based on agreements within an assurance community that verifier and issuer belong to.
- Based on agreements between individual parties.
- Based on legislation or other government interventions.

An issuer can publish its issuing policy and credential types in a *credential catalogue*, including the syntax, semantics, and assurances. An issuing policy can for example include criteria for issuance such as that a credential is issued only after an in-person verification of the holder's national identification document.

In cases where there could be any reason to doubt the diligence or reliability of an issuer it audits could serve as a mechanism to confirm whether the issuer adheres to their stated policy.

3.3.4 Verification and Validation Policy

A verifier (also fulfilling the role of validator) needs certain information with assurances to achieve a certain goal. However, in general a credential will not necessarily have been issued with this specific goal in mind. In principle a credential can be used for a wide variety of goals, and different credentials might be relied upon for the same purpose. A verifier should define its verification and validation policy such that it is clear whether the holder's data and assurances are fit to achieve the verifier's goal.

Based on a validation policy, certain levels of trust can be achieved. Thus, trust is also context-dependent, for example:

- Granting access to public (parts of) networks don't need any assurances.
- For some purposes, like web shops, it is sufficient to know that the interaction is with the same person as last time.
- For more sensitive cases, the verifier might need to know:
    - The holder's identity.
    - The holder's authorisations. For example: is this person allowed to drive a truck?
    - A combination of authentication and authorisation to grant - and log access. For example: if someone picked up a shipment because they were authorised, but later it turned out they shouldn't have been authorised, the verifier might want to know who has picked up the shipment. This could be achieved by using pseudonyms or commitments. Where the pseudonyms could be reidentified later, ar in the case of commitments they could be used to commit to a value (an identifier) while later revealing the value when required.

3.3.5 Mechanisms for Verification of Issuer and Verifier Accreditation

A holder has a certain credential, issued by an issuer. We see the following mechanisms for how verifier V can verify that issuer I is accredited by accreditor A, when a holder H is presenting a credential issued by I:

- V maintains a list of accredited parties. The list is created and maintained by looking at bulletin boards and/or receiving untargeted broadcasts or targeted updates from A. This may result in a large amount of bulletin boards to keep track of. The mechanism is also quite error-prone – if an update is missed the overview is not correct anymore, meaning the accreditation status of parties can be wrong.
- V can consult a list maintained by another party. This party can be A or some other trusted, public party (e.g. Consumentenbond). Examples: VICAL (ISO mdoc spec), trusted issuer list, trusted verifier list.
- V asks I to present a credential issued by A proving its accreditation. This may expose information to I about H. After all, the reason for V to check I's accreditation is that a holder has presented a credential issued by I. This compromises **issuer unlinkability**, the degree to which it does depends on the number of parties issued a credential by I and whether I has other information it can use to narrow down the list of potential holders.
- H's credential contains a claim about the accreditation of I. This claim can be:
  - A link to an accreditation list as named above.
  - The accreditation credential of I. As I is often a large public party, this credential can also be publicly available on a distributed ledger, and the claim can point to it.

Except for maintaining lists of accredited parties or the latter option, these mechanisms work under the assumption that it is public knowledge that I is accredited by A.

To increase assurance for the verifier, it is desirable that the accreditation criteria are also discoverable. By using accreditations, the requirement that a verifier trusts every individual issuer is shifted to trust in a few accreditors. The trust in the accreditor can be guaranteed through, amongst others, audits.

The previous mechanisms are for the verification of the issuer's accreditation. The same mechanisms hold for when the holder H wants to confirm whether verifier V is allowed to ask H for certain information, apart from the roles being different. What information the verifier can ask for, is described in arrangements and/or legislation, e.g. only governmental and healthcare institutions can ask for a citizens social security number, the local supermarket cannot. Being able to check … This is called 'verify-the-verifier'.

3.4 Delegation and Mandates

As an employee, to act on behalf of their organisation, a mandate or delegation can be used to prove that the employee has certain authorisations. We see the following options:

- The organisation issues delegation / mandate credential to employee. Such a nested credential contains a chain of custody, i.e. the owner of the authorisation and the path to the party presenting the mandate. This can be achieved through Chained Credentials, ACDCs, ZCaps or AC nested credentials. To allow a holder to become an issuer, i.e. the original holder passes on the authorisation to another party, the holder

needs an issuer key pair and identifier, but also an issuing policy. The VISMA-NETIS solution allows for this.

- Traditional systems, for example role-based access control (RBAC) can be used. Based on the role an employee has, they get access to certain resources and can obtain certain authorisations. One of the options could be that an employee is provided access to an IT component such as a company wallet containing credential issued to the organization. Based on accounts and roles, different environments might exists giving access to different credentials.

4 Use case 1: Identification and authentication of nodes

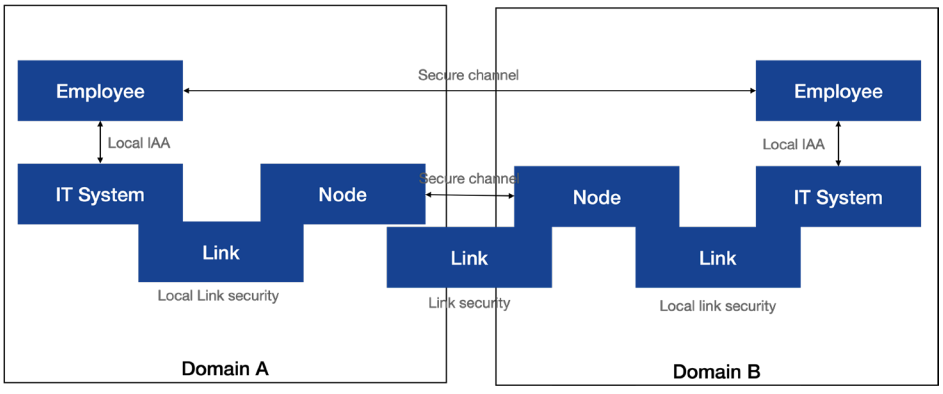
This section describes IA in the context of nodes onboarding in a network, applying the SSI basics explained in the previous section. A node is defined as the implementation of Index functionality as specified by the FEDeRATED Architecture. Thus, in this context it could be called a 'FEDeRATED node' (for brief it will be called 'node').

The FEDeRATED Architecture specifies an open, neutral data sharing infrastructure that can be applied by everyone. Since FEDeRATED provides input to the Digital Transport and Logistics Forum (DTLF), an expert group raised and chaired by EC DG Move that provides recommendations to EC DG Move for data sharing in supply and logistics, its application area is the EU (European Union). This is called the European Mobility Data Space (freight). Mobility of persons is the other dimension of the EMDS.

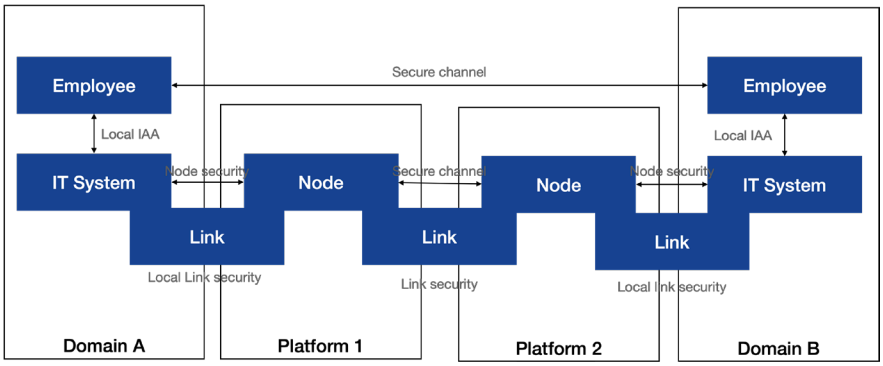
On-boarding of nodes thus can be seen in the scope of EMDS (freight). Since the intention of iSHARE is to be applied by dataspaces (like EMDS), it will be discussed in this section. Other relevant developments are eIDAS2.0 and GAIA-X in this context; these will briefly be explained in this section.

4.1 IA options in the network

There are different options for implementing IA in a network of nodes. The basic objective is to construct a secure channel between any two persons in two domains, where each person is an employee of an organization. This is broken down in the following figure, where domain A and B represent two organizations. It is **peer-to-peer** data sharing between organisations. The assumption is that locally, each organization has organized its IA using its own solutions and nodes have an additional IA mechanism as shown in the next figure. This figure shows that there is only a secure link between an IT system and a node; this link can be secured by for instance an API Gateway whereby employees need to have authorisation to access APIs, even if these are initiated by their own IT system.



An alternative picture shows secure channels between and over platforms, where these platforms locally integrate with organisations. In such a case, a platform acts on behalf of a domain, like the domains A and B in the previous example. A secure channel between platform 1 and domain A is the responsibility of platform 1 and outside scope (same for platform 2 and domain B). We investigate the Identification and Authentication of a platform as a node in a grid; each platform must have an IA mechanism with its users (this might include Authorisation by registering employees of their platform users).



4.2 Acting as node in a network

This section is about node-to-node security, where each node is implemented in a different domain. To admit a node to the network:

- The organization that wants to add a node to the network, selects an accredited issuer from a list. The assumption is that such a list is available and/or accredited issuers can be found.
- An issuer applies an Issuing Policy that is transparent. Selection of an accredited issuer can also consider the applied Issuing Policy of the issuer. The Issuing Policy can be broader than only technical aspects.
- There are two cases to be considered for on-boarding, namely:
    - First registration – an organization did not yet register a 'node'. This node should have minimal capabilities as specified by the Issuing Policy. This could be the support of at least one 'profile' and a 'Service Registry' for discoverability (see the FEDeRATED architecture). Requirements are formulated by an Issuing Policy.
    - Updates – there is already a node registered with at least minimal capabilities required by the Issuing Policy. The capabilities of that node can be extended and/or changed, for instance by including additional profiles.

The high-level onboarding of a node is as follows:

1. There is a BDI network N (i.e. a community) and a node, e.g. 'Node 6' with id_6, wants to join the BDI network.
2. Node 6 interacts with Registration Authority acting as issuer to obtain a $VC(id_6)$. The node has specified its 'profile(s)' which can be certified by an issuer (or a certification authority).
3. Node 6 joins the network, and sets up its own Service Registry (SR).

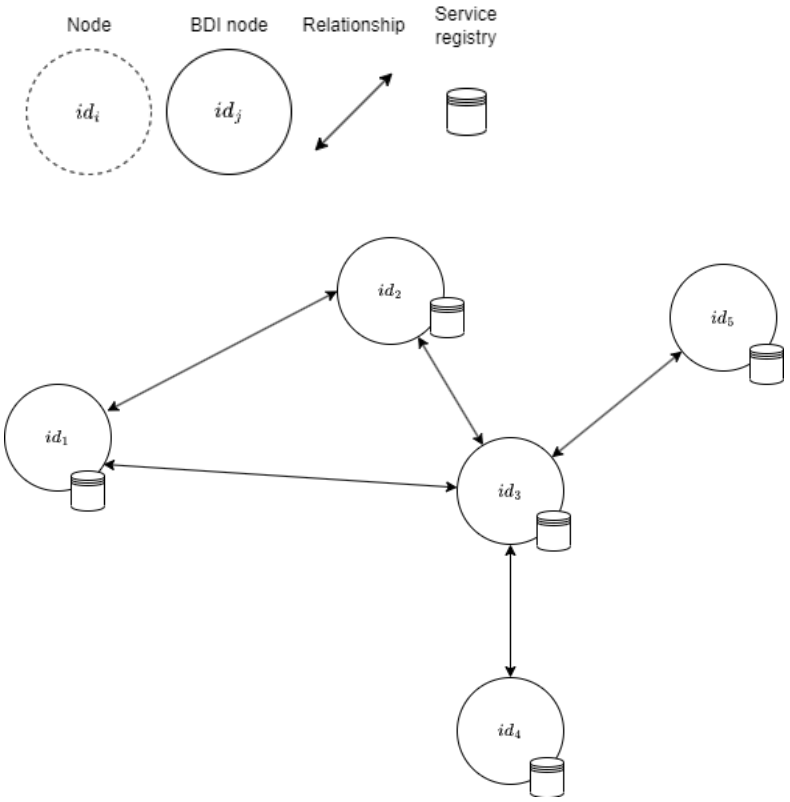
On-boarding will result in data sharing:

4. Node 6 wants to fulfil objective O_6 and uses DNS to find the capabilities of other nodes. Matching algorithm between Node 6 and other nodes → Node 4. From a business perspective, Node 6 discovers other nodes by finding a business service matching its goal.
5. Design-time protocol between Node 4 and Node 6 → agreement.
6. Run-time protocol for fulfilment of agreement between Node 4 and Node 6.

Each step will be discussed in a separate section below.

4.3 On-boarding

We will use the following BDI network N, which Node 6 with id_6 wants to join. Each node i has a SR_i, containing (some connection to) id_i and the (business) capabilities ('business services') of node i C_i. Node i also has objectives O_i.



Node 6 interacts with the Registration Authority (RA) to obtain a Verifiable Credential attesting to its capabilities. Specifically, the credential can take one of the following forms:

- An empty credential, relying on the idea that the RA will only issue this (signed) credential if the node has the required capabilities. The trust a verifier can have in the credential will come from knowing that the RA only issues the credential if the node indeed has the right capabilities.
- A credential with a single claim stating 'accepted to join network N'. This provides high flexibility, as future credentials can have different / more specific attributes.
- A credential with claims for each of the capabilities Node 6 implements. This provides more assurance for other nodes, but also requires a more intensive onboarding and a

process to update the credential should the node's capabilities change after its first onboarding.

- A credential with a claim stating 'accepted to join network N' as well as claims for each of the capabilities Node 6 implements. This is the most versatile option from the perspective of the verifier.

The last option is the preferred one. It is based on the concept 'profile'. As a demonstrator, it will be implemented for a multimodal visibility service (see the specification of 'Multimodal Visibility Service') that will have to be upgraded to support all relevant aspects of 'profile' (see the specification note on 'Profiles'). In the demonstrator, the assumption is that each node will have only one capability (i.e. one profile), but in practice more could be supported.

For demonstration purposes, the capabilities of a multimodal visibility node are expressed as follows in the demonstrator ('**enterprise profile**'):

- Business activity – in the current version 'transport' only. At a later stage extended with others like 'transshipment'.
- Interaction pattern – specification of the agreed pattern that is supported. In this case: 'multimodal visibility pattern'.
- Role – each node must have at least the role of 'customer' or 'service provider' but can have both roles.
- Area of operation – the area in which a business activity is performed or required. For matching purposes, the area of a customer must be fully part of that of a service provider.
- Modality – additional constraints to the modality that can be supported or is required. At least one of the modalities 'sea', 'air', 'road', 'rail', and 'inland waterways' must be given; at most all modalities can be supported. For instance, a forwarder acting as customer or service provider can support all modalities.
- Cargo – the cargo that is offered for transport or can be transported. The following choices are available: trailer, (sea)container, ULD (Uniform Load Device, specific for air transport), goods (pallets, boxes, etc.), parcels (for express delivery), and dry – or liquid bulk cargo.

Later iterations will include additional constraints on the goals or capabilities of an organization. These capabilities are validated by a Certification Authority before being issued as part of a VC by a Registration Authority. Thus, the negotiation and collaboration will be easier (see later).

A node of a governing authority also requires a VC. The claims in this VC may differ from the one of an enterprise node, since the capabilities of an authority will be different. These authority capabilities are specified by its profile properties. A first iteration of an **authority profile** could be:

- Regulation – the regulation by which data access is required. Examples are 'eFTI' (electronic Freight Transport Information) and 'voluntary', where the latter implies that it is up to enterprises to provide access to data. There can be multiple regulations that can be governed by a single authority, each with its own data requirements and interaction pattern.
- Role – the role is always 'authority'.

- Interaction pattern – this is the pattern by which an authority receives duplicate visibility events for a transport movement in its area and has the capability to access enterprise data.
- Reference to a data set – a reference to a data set specification for which access is required. This could be a specific version of the subset of the eFTI data set required by the authority.
- Area of responsibility – the area in which the authority governs the applicable regulation.

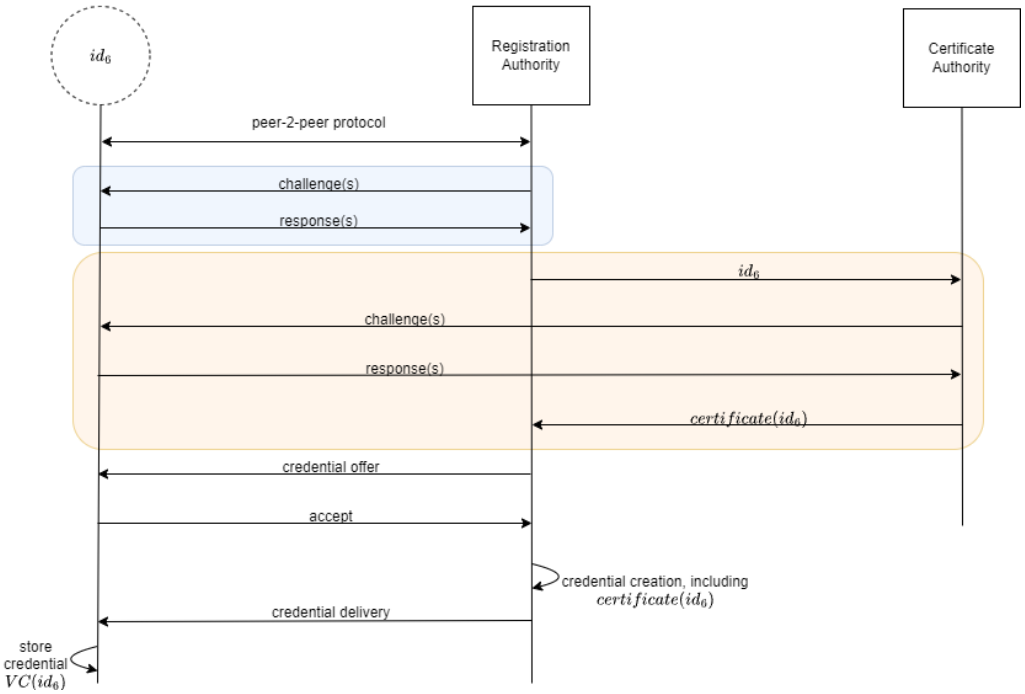
A governing authority can use a VC of an enterprise to validate data received from that enterprise. This data may only contain properties of the concepts of selected modalities and cargo. For instance, if an enterprise indicates support for 'road' it must provide the 'eFTI' data subset required by an authority and that authority is not able to request for instance Air Way Bill (AWB) data.

Next, the on-boarding protocol is described. It will result in a credential signed by RA with metadata included (as a pointer to) RA's public key. In the on-boarding protocol, the capabilities can be checked either by an RA itself (blue flow), or by a CA (orange flow). Both are based on certain challenge-responses. What these challenges entail depends on the capabilities to be tested and can take the form of

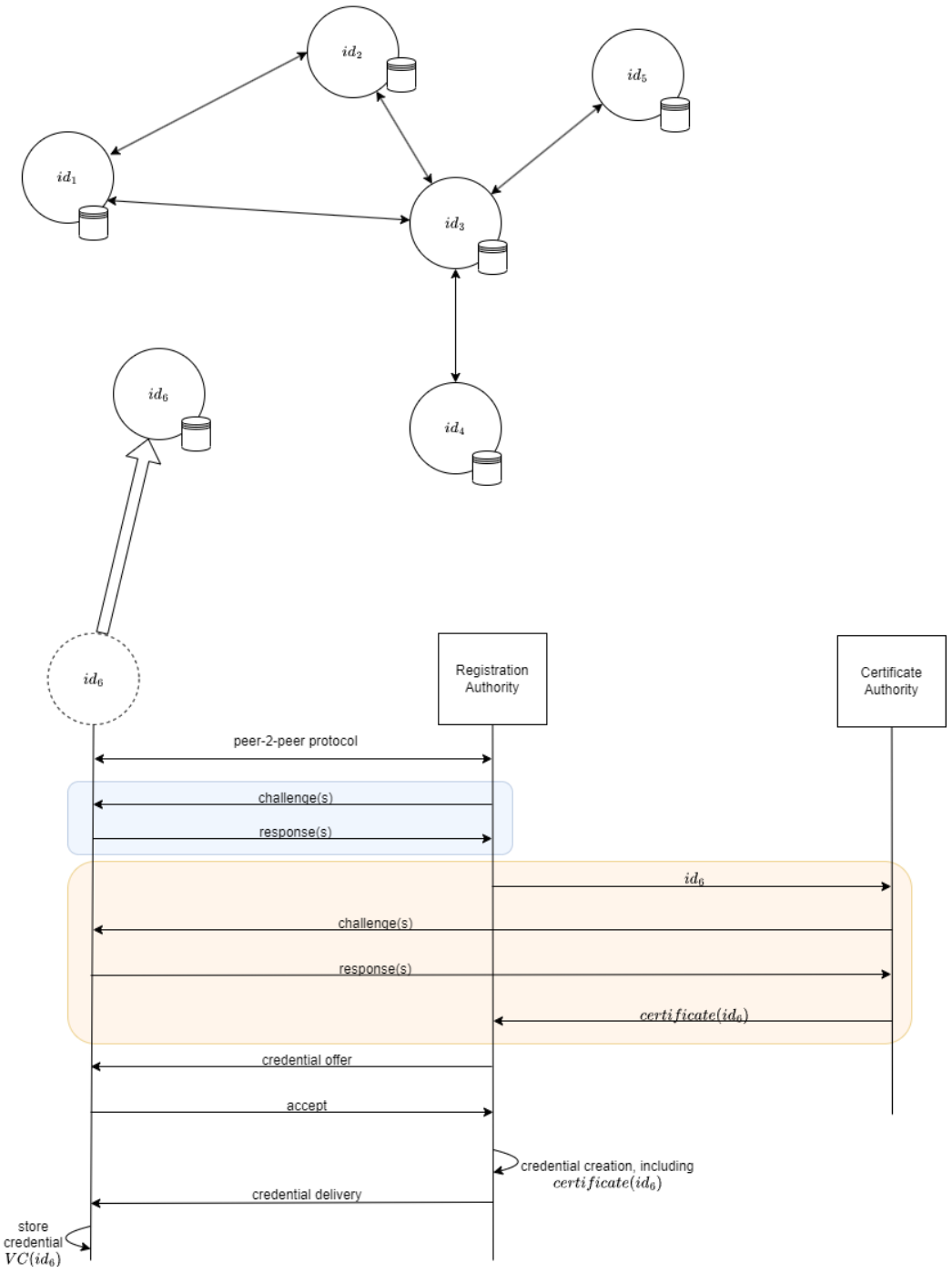
- a request for data;
- a request to fill in a list of information;
- a request to perform a system audit;
- a technical challenge-response, where the node can only form the response if the capability is implemented.

These challenges are specified by the interaction patterns that a node claims to support in the case of the BDI infrastructure.

If these challenges are completed successfully, the RA shall issue the credential $VC(id_6)$.



Node 6 now joins the network by setting up its Service Registry (SR_6). Its SR and therefore capabilities and identifier can now be resolved by other nodes through a DNS-like system and/or business services.



4.4 Data sharing by a node

Node 6 has a certain objective O_6. This objective represents a business goal. To achieve it, the node needs information or a service from another node. To discover the capabilities of other nodes, a DNS-like resolver is used. This resolver mechanism is based on the business service concept. A (goal-business service) matching algorithm is used to match nodes that can

possibly fulfil the needs to achieve O_6. We assume the matching algorithm returns a list of nodes, where the first node is Node 4.

There are other resolving mechanisms than DNS-like resolvers. It can also be done through CORDA network manager. However, as the European Commission has settled on the usage of DNS for eSense Delivery, we will follow this decision in this document.

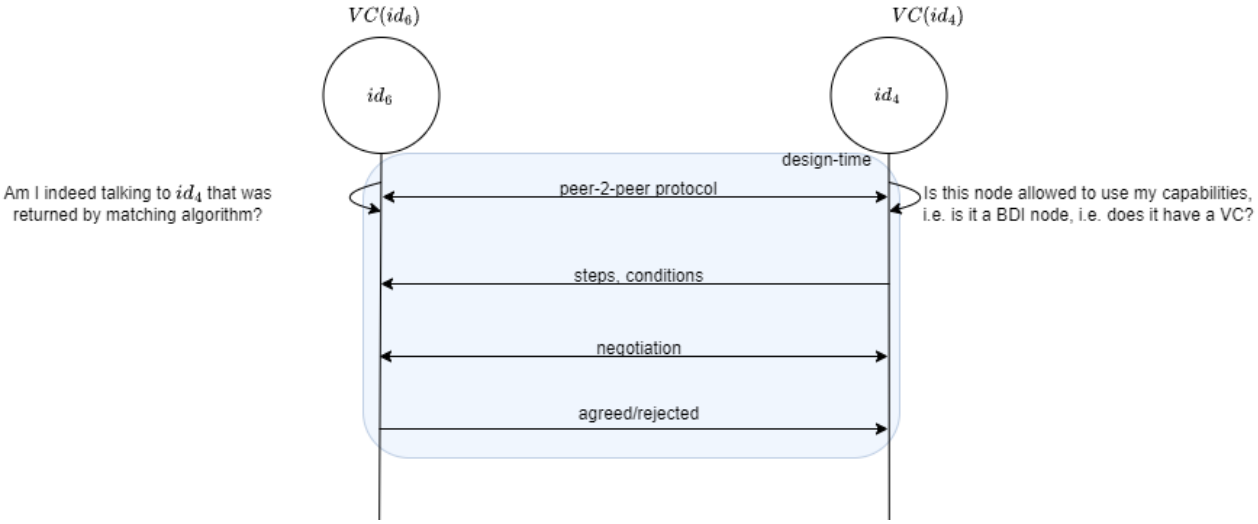
4.4.1 Capability matching protocol

Since goals, business relations, and 'profiles' will change over time, matching will have to be performed for individual goals. In a more static environment of long-term business relations, capabilities can be matched at design time, where the results of capability matching can be considered as a type of design time action. In this context, it is considered dynamically, per individual goal of a customer. Of course, implementations may consider reusing matching agreements for multiple business transactions.

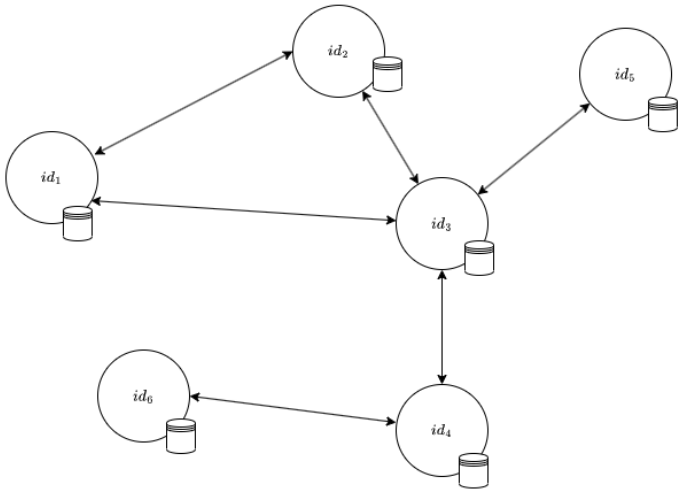
The capability matching protocol is about profile matching of two nodes, in this example Node 6 and Node 4. Each node will have (multiple) profiles formulated as capabilities in VCs. These capabilities identify the interactions and data they can share. Of course, discoverability is already based on goal-business service matching, resulting in a preselection of Nodes that can fulfil a goal.

In this scenario Node 6 will first want to make sure that it is indeed talking to Node 4, the node returned by the matching algorithm. This gives assurance on the capabilities of Node 4, but also that Node 4 indeed belongs to BDI Network *N*. Node 4 needs to verify $VC(id_6)$, to make sure the node indeed belongs to *N*.

As Node 4 is offering the service, it decides the conditions and what the run-time transaction should look like. As Node 6 has the objective, it decides whether it agrees with the conditions and whether the foreseen result of the run-time transaction will satisfy their objective O_6. The result is an agreement between Nodes 4 and 6 that will last for objective O_6.

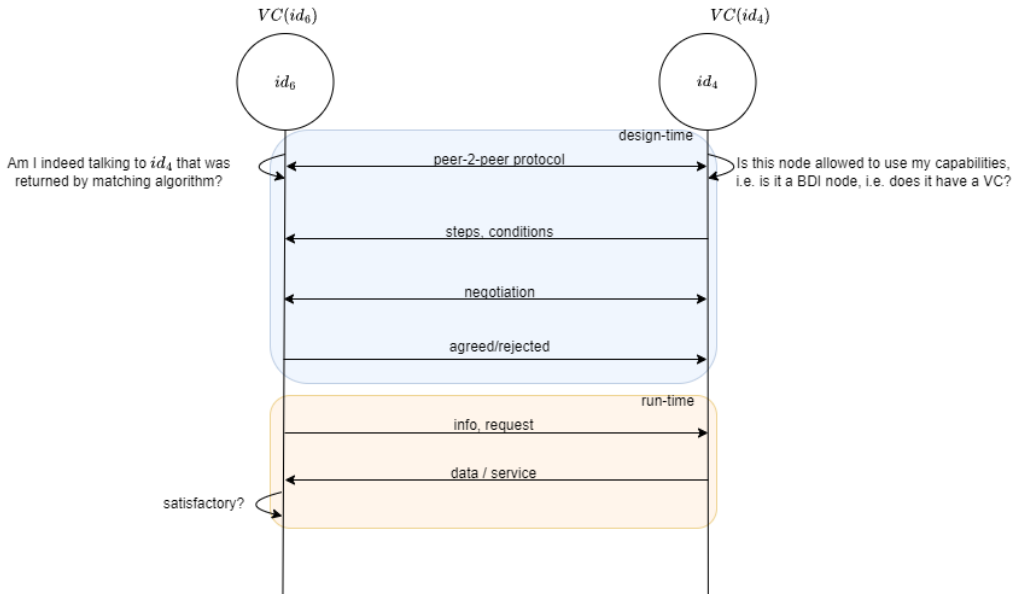


If Node 6 agrees, the nodes then have an agreement and therefore a relationship within the network *N* for a particular goal. This relationship may dissolve after the goal has been fulfilled. In case of framework contracts, a relationship may last for years; in case of a transactional relation it only lasts for the duration of a single business transaction.



4.4.2 Data sharing

Once an agreement is established, data can be shared, for instance concerning events of the multimodal supply chain visibility service. After completion or after a predetermined period, a review can take place.



4.5 Existing mechanisms

This section elaborates existing mechanisms and developments for Identity and Authentication in the context of onboarding of organizations in dataspaces like the EMDS for freight. These are iSHARE, eIDAS2.0, and GAIA-X. A comparison of these mechanisms is made at the end as a basis for exploring the possibilities of migrating iSHARE to an SSI/VC based environment.

4.5.1 iSHARE

According to representatives of iSHARE and DIL, the proposed approach given in this section needs to be supported if the SSI/VC coverage is not sufficient. Whereas the base concepts of iSHARE are similar to SSI/VC, iSHARE does not support them in its current form.

iSHARE consists of the following aspects, which will be elaborated hereafter:

- **iSHARE Foundation** - governance of the iSHARE Trust Framework (type of VICAL for dataspace authorities, creating trust).
- **iSHARE** Trust Framework – data sharing agreements (legal, functional, operational, and technical; independent of the data that is shared).
- **Dataspace Authority** – certified organization acting as an issuer and storing credentials of holders.
- **Credentials** – the structure of credentials is specified in a dataspace.
- **iSHARE Satellite** – reference software for a Dataspace Authority or certification body.
- **Authorization Registry** - referred to via a holder credential, having its own credential, storing authorizations for data/service access, given to third parties by a holder. An Authorization Registry can act as agent on behalf of an entitled party (data owner). This is outside the scope for onboarding.
- **Federation** – re-use of an identity across multiple dataspaces, supported by a ledger.

iSHARE is brief for the iSHARE Foundation or the iSHARE Trust framework, of which the iSHARE Foundation is guardian over through the Foundation governance. The iSHARE Framework consists of agreements enabling data sharing and supporting standards on legal, functional, operational and technical topics. The Foundation itself is Governed by data spaces that apply the iSHARE Trust Framework and implement the iSHARE Trust Framework (link) and that also propose developments to the framework through Change Process of the iSHARE Foundation.

For trusted onboarding of participants, the Foundation delegates credentials to any iSHARE certified organization that acts as Dataspace Authority, supported by the iSHARE Satellite reference software (not mandatory). One data space can have more than one Dataspace Authority. The Foundation maintains a list of trusted organizations running registered (ledger connected) Satellite instances.

Each Dataspace Authority registered by the iSHARE Foundation must comply with the issuing policies of the . The framework is developed and maintained as a collaborative effort to improve conditions for data-sharing by organizations participating in a dataspace. The governance of the iSHARE Foundation is organized in a manner that the iSHARE Network, i.e. the network of Dataspace Authorities, can operate and grow in a sustainable way. At the same time, its governance provides the appropriate checks and balances that will allow Dataspace Authorities to provide input, supervise ongoing activities and collaboratively influence the growth and development of the iSHARE Trust Framework.

In the roadmap a Dataspace Authority issues verifiable certificates (currently in test) to participants and registers those certificates. The Foundation verifies a Dataspace Authority on adherence to the iSHARE Trust Framework through the assessment framework, supported by a Compliance Check Tool (CTT). This requires that a Dataspace Authority provides evidence for implementation of appropriate controls and adherence to onboard

participants with the required trust level (Level of Assurance or LoA). A legal person (organization) is required to be identified with an eIDAS based certificate (for all roles, except the Entitled Party), or as an Entitled Party another trusted IDP according to the . This allows any EU organization to join when adhering to the iSHARE Scheme for the chosen role(s). The identifier used for participants in iSHARE based dataspaces is EORI. In the Netherlands eHerkenning can be used, where the identity of the organization is authenticated via its RSIN, that is converted to EORI (using established procedures).. The underlying trust is equal and guaranteed by the Dataspace Authority. The use of new Identities of Legal persons against the same validation level is under review by the participating data spaces (DID etc. RFC031 - iSHARE Change Management)

In data sharing or requests for data access, legal persons share the references to their certificate. A recipient of this reference can verify the certificate as registered during onboarding (or updated thereafter for renewal) via its Satellite.

A certificate consists of minimal party information. It has a start date and can have an end validity date. There should be policies for defining an end validity date., e.g. a it can have a validity period or can be revoked (via for instance a blacklist) when the owner does not behave according to an applicable issuing policy. A reference to an Authorization Registry can be included in a credential. An Authorization Registry is registered by a Satellite with the certificate of the legal person supporting that role. An Authorization Registry contains access policies and access rights for external stakeholders (Data Owners/ Entitled Parties) and can include delegation evidence. An example of applying the Authorization Registry is for RVO (Rijksdienst Voor Ondernemers) where enterprises can assign access rights to authorities for accessing their energy consumption information hosted by a Service Provider which in this case are the energy companies. In the iSHARE roadmap, also an Authorization Registry is providing verifiable credentials as proof of consent by the data owner.

Each dataspace can include additional data elements, on top of the iSHARE Scheme requirements, to certificates used by their members.

Since there can be many dataspaces, a ledger is applied for dataspace federation of registration of credentials. The ledger stores ‘legal person’ with the Satellite that stores the credential of that legal person. The ledger for dataspace federation is applied to detect duplicate credentials (a member/participant can only be onboarded once). A legal person can attain multiple credentials and (try to) perform illicit behavior within a Dataspace that is not using the ledger for federation.

The extension to the iSHARE scheme under RFC040 Verifiable Credential support and RFC039 EBSI compliance both implemented in the test environment are intended to provide continuity in a bimodal period where the SSI/VC ecosystem is expanding, and organization do not have option to obtain needed VCs from Trusted Issuers.

4.5.2 eIDAS and GAIA-X

There are two major developments relevant for the development, implementation and governance of SSI/VCs, namely that of the private (GAIA-X) initiative and EC developments in the context of eIDAS2.0. These are briefly presented here.

The private GAIA-X initiative develops a technical infrastructure that can be applied by issuers, holders, and verifiers in an organizational setting. Its focus is on creating a so-called organizational – or business wallet for VCs, including interfaces for issuing and verifying these VCs. Such an organizational wallet will require access control based on (internal) authorisations to enable employees to use the credentials stored in this wallet. This type of infrastructure can be applied to support the two use cases of this document.

The EC has various initiatives with respect to IA that might be of relevance. First, there is the legal aspect: development of eIDAS 2.0 supporting VCs. eIDAS 1.0 supports different security levels based on IA infrastructures of Member States, including a central facility for accessing an EC IA infrastructure (UMDS).

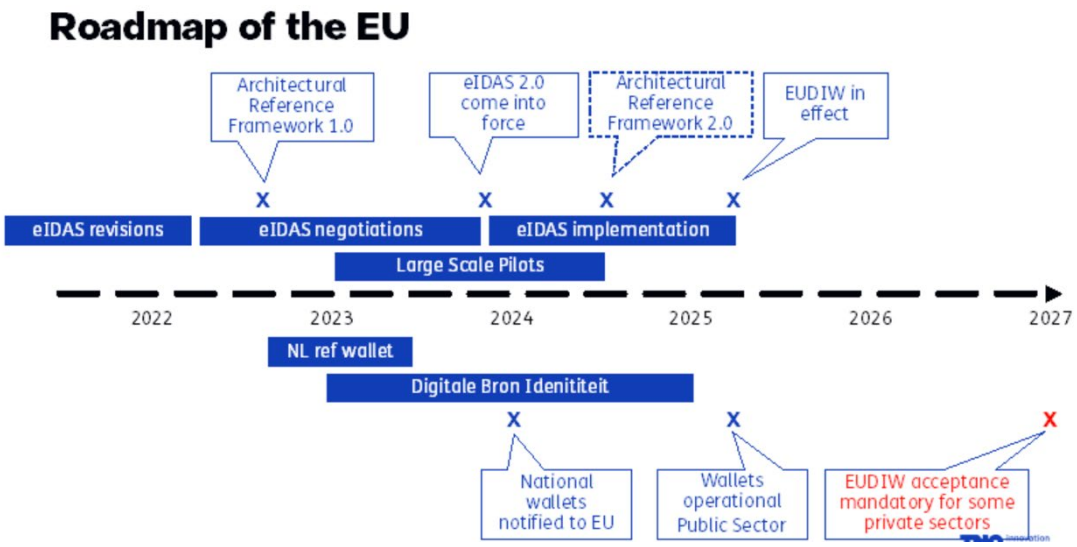
eIDAS1.0 and 2.0 are considered as follows:

- **eIDAS Regulation** – this is about the use of Identity and Authentication for both natural and legal persons in their interactions with authorities (B2G – Business-to-Government).
- **Issuing policy** – as part of the eIDAS Delegating Act, each Member State has its own issuing policy for identities.
- **Data Sharing Agreements** – these are specified by the case in which eIDAS is applied by a MS authority. These can be local (municipality) or EU (e.g. customs, based on the UCC (Unified Customs Code), or an EMDS Regulation (not available (yet))). These data sharing agreements must implement all generic data and privacy related acts like the Data Act, GDPR, etc.
- **Technical scheme** – specification of the technical infrastructure supporting eIDAS. This is part of the eIDAS Implementing Act.
- **Credentials** – the structure of credentials is part of the Architectural Reference Framework (ARF). This structure can be expanded to support for instance EMDS and other initiatives in for instance healthcare and industry.
- **Issuers** – identity providers operating according to the eIDAS issuing policy of a Member State. These are Digid for natural persons and eHerkenning for legal persons in the Netherlands.
- **Federation** – re-use of an identity across multiple MSs is supported by eIDAS(1.0/2.0).

Comparable to the iSHARE Authorisation Register, some MSs and/or authorities may have implemented this type of functionality.

eIDAS 1.0 can be applied both in business-to-government (B2G) applications, but also in business-to-business (B2B). The latter application of eIDAS implementation differs per Member State (MS); not all MSs support B2B with eIDAS 1.0. Secondly, EBSI (EBSI – European Blockchain Services Infrastructure) creates a VC infrastructure with a focus on natural persons. In this context, providers of so-called electronic attestation of attributes (EAA) and qualified electronic attestation of attributes (QEAA) are distinguished. Examples of (Q)EAA are for payments, education, eHealth (like authorisation attributes for health care providers to assess electronic patient records), and others like relevant to travel and social security. These QEAA are expected to be supported by EBSI. These may include digital identities of organisations.

The following figure shows the roadmap for eIDAS2.0. It shows that eIDAS2.0 is expected to come into force by the end of 2023 and will be fully implemented in 2025.



The Netherlands implements eIDAS 1.0 with Digid (natural persons) and eHerkenning (legal persons). There are five so-called eHerkenning brokers that provide certificates to organizations. Authorisation is on employee level, managed by a representative of an organization in a selected eHerkenning broker. This model does not scale and will probably be replaced by eHerkenning brokers issuing VCs. Logius and RVIG currently govern this infrastructure. Together with the Dutch Blockchain Coalition (DBC) they explore future improvements.

Note that the current EC IAA infrastructure of eIDAS for legal persons is to support enterprises in accessing so-called eGov services, where these services are provided via a portal, e.g. to access a national Chamber of Commerce. Lower level eIDAS certificates (on the https protocol level) can be applied for data sharing with authorities (e.g. declarations) and can be adopted for business-to-business. However, https-security is considered insufficient for so-called node-to-node Identification and Authentication.

4.5.3 Comparison of the mechanisms

The comparison of iSHARE with eIDAS requires a better understanding of ‘dataspace’:

- **Dataspace** - a ‘dataspace’ as the governance structure for a data sharing scheme covering all aspects of the European Interoperability Framework (EIF): legal - , organizational -, semantical -, and technical interoperability, including IA.
- **Private dataspace** - a private dataspace is governed by enterprises only;
- **Public dataspace** - a public dataspace is governed by EU -, Member State -, or local (e.g. municipality) authorities, based on EU/MS/local regulations. These regulations are the basis for data sharing agreements.

The International Data Space Association (IDSA) has developed so-called ‘horizontal’ capabilities to rapidly set up a dataspace. The iSHARE Scheme and – Satellite can act as horizontal capability, if recognized as such. In B2G applications, the EC has developed similar ‘horizontal’ mechanisms based on the eIDAS Regulation for public dataspaces.

Implementation of a regulation by a public dataspace is based on an Implementing – and Delegating Act of that regulation. An Implementing Act specifies those aspects that must be implemented by all Member States; a Delegating Act those that are particular to a MS.

The comparison between iSHARE and eIDAS can be made as follows:

Aspect	iSHARE	eIDAS
Governance	iSHARE Participants (Foundation is executing body)	eIDAS Regulation
Data Sharing Agreement (legal)	iSHARE Scheme + dataspace	Public dataspace
Technical Scheme	iSHARE Scheme + dataspace	eIDAS Implementing and Delegating Act
Issuing policy	Dataspace	Public dataspace (Implementing - and Delegating Act, e.g. UCC, eFTI)
Credential structure	Dataspace	EIDAS + extensions for a private dataspacea (logistics, healthcare, industry)
Issuer	iSHARE Foundation certified Dataspace Authority	MS certified Identity provider
Federation	iSHARE roles	eIDAS Regulation

Whereas iSHARE is to be applied to Business-to-Business or private dataspaces, eIDAS is applicable to B2G, but can also be applied to B2B, I.e. EU private – and public dataspaces. Of course iSHARE might also be used for B2G and G2B, but will not be adopted by authorities since it does not have a public legal basis. They have eIDAS. The iSHARE Authorization Register is also applied by an authority in the Netherlands.

GAIA-X develops the technical scheme for implementing organizational wallets in the private sector. This must cover the issuing and verification interactions, and the structure of the credentials.

4.5.4 iSHARE migration strategies

A migration strategy of iSHARE can be considered at various levels:

- **Private dataspace** – this implies the implementation of the technical scheme developed by GAIA-X (under development). The Satellite software needs to be adjusted to support this technical scheme, including its interaction with organizational wallets. Whether the iSHARE data sharing agreements are adopted as 'horizontal' capabilities depends on policies of for instance IDSA and GAIA-X.
- **Public dataspace** – a public dataspace requires the implementation of an issuer that conforms to eIDAS based issuing policies of a MS. In this context, iSHARE has three options:
    - Do nothing and don't act in public data spaces.
    - Act as a credential issuer in the Netherlands implementing eIDAS2.0 (legal, organizational, technical).
    - Become a provider of software for eIDAS conformant issuers, which means competition with commercial providers.

- **Public/private dataspace** – this is the adoption of a public regulation for data sharing and issuing policies by the private sector. The scope of the regulation defines the size of the dataspace, e.g. an EU Regulation is applicable in all EU MS. Such a regulation is on a voluntary basis: the private sector is not forced to implement the regulation. The European Mobility Dataspace (EMDS) is an example of such a dataspace.
  There are two options: either there will be an EMDS Framework Regulation or not. If the latter case, the EMDS is a private dataspace; all public sector data sharing is separately specified and iSHARE can take its role as previously stated. If the former case, such an EMDS regulation will be aligned with the public sector applications of data sharing (e.g. UCC and eFTI; B2G/G2B) and thus needs to be aligned with eIDAS. This implies that iSHARE can act according to its role in a public dataspace.

The Ministry of IenW, DIL, and iSHARE need to consider whether they would like iSHARE (as organization) to have a role in public dataspaces, since this may lead to competition with commercial providers.

Further evolution of iSHARE for private dataspaces is feasible but requires the adoption of its Trust Framework. Technical aspects of this framework may have to be extended to support SSI/VCs. The legal and organizational aspects of the iSHARE Trust Framework might be overtaken by a voluntary regulation for the EMDS, that builds upon eIDAS2. If public - and private sector agree on a common (EMDS) regulation, then iSHARE can potentially only act as issuer. Such a (voluntary or mandatory) Regulation is required in many cases, since private – and public data spaces are intertwined.

Concluding, we propose the following migration strategies:

1. **Private data space support**. Extending or migration of the iSHARE Technical Scheme to support private technical schemes whilst private dataspaces also adopt the other aspects of the iSHARE Trust Framework. The following steps can be taken:
   a. Support of the private (VC-based) technical schemes by extending the current scheme of storing credentials with a Dataspace Authority. It is the implementation of for instance the GAIA-X technical scheme by Satellite software. The GAIA-X technical scheme becomes part of the iSHARE Scheme. Private dataspaces may still adopt the iSHARE data sharing agreements.
   b. Evolving the previous scheme by supporting organizational wallets. The iSHARE Satellite only acts as issuer software and interfaces with organizational wallets. This may require the publication of a DID of an issuer using the iSHARE Satellite software on a public ledger (SSI), depending on the technical scheme developed by for instance GAIA-X.
2. **Public data space support**. Support of the eIDAS Scheme (legal and technical) and extending the iSHARE Satellite to support the eIDAS2.0 technical scheme (Implementing – and Delegating Act)2.0. It will enable iSHARE to become an issuer of credentials in public dataspaces. The eIDAS2.0 technical scheme becomes part of the iSHARE Scheme. The iSHARE data sharing agreements are not part of a public dataspace; the ledger for federation is not applicable in such public dataspaces.
3. **Public/private data space support**. If an EMDS Framework Regulation is adopted, the iSHARE Satellite will have to support additional properties of credentials for EMDS. The iSHARE Scheme is replaced by the data sharing agreements and issuing policies of the EMDS and the technical scheme of eIDAS2.0 with extensions for EMDS is supported.

Alignment with eIDAS2.0 is feasible, but only if private data spaces accept it and require additional extensions for their private use that are not in the Architectural Reference Framework of eIDAS. This is up to a private data space to decide.

4.6 Implications for the existing node

There are existing solutions for onboarding, for instance the use of the mechanism based on Corda technology or OAUTH2.x implemented by a node like the current version developed in FEDeRATED.

With respect to **on-boarding of a 'node'**, these are currently implemented by Corda technology (as prototype). This technology provides an issuer of (Corda) credentials, the so-called Corda Network Manager. Issuing policies can be specific to an implementation of a Corda network and its Network Manager. The Corda Credentials are used to uniquely identify and authenticate a node in the network.

Since Corda has proprietary protocols and a proprietary structure of its credentials, these may have to migrate to generic protocols of a VC-based infrastructure. However, Corda provides additional functionality by its Corda network manager[1] that is not part of a VC infrastructure, like a capability to issue Corda credentials based on an issuing policy and to monitor the functioning of a network of Corda nodes. Corda nodes also share so-called CordApps implementing a type of smart contract[2] functionality, where these CordApps are also part of a Corda message providing the required processing functionality to a recipient without prior distribution of a smart contract to all participants. And of course, Corda also has an implementation of non-repudiation via its Notary Network. Although Corda is based on standard protocols like TLS (Transport Layer Security) and AMQP (Asynchronous Message Queuing Protocol), its functionality is very powerful, but proprietary.

An OAUTH2.x token (or JWT – Java Web Tokens) can be considered as a type of credential. These tokens are issued to natural persons or, a lower level, to software applications requiring access to data in (external) databases. The basic difference with tokens is that VCs don't require centralised functionality like the registration of issuers, so-called IAM Registries (IAM -Identity and Access Management). For token-based security, there must be trusted issuers of these tokens. These issuers are registered by an authority, whereas such an authority may have a mandate of another authority. This is also called a 'federation of IAM Registries, which is supported by iSHARE. In case of applying VCs, these types of federations are not required.

4.7 Conclusion and discussion

Applying VCs for onboarding nodes in EMDS for freight is promising and provides scalability. Including specific properties for EMDS in such a profile is feasible; a proposal is made based on the FEDeRATED architecture.

VCs are also going to be applied in other areas than logistics, for instance private dataspaces according to GAIA-X and public dataspaces based on eIDAS2.0. The underlying Architectural

[1] There is an open source and paid version of the Corda Network Manager; they open-source version is not maintained anymore, and its functionality is too limited for operational use. For prototyping and demonstrations, the open-source solution suffices.

[2] Smart Contracts implement agreements for data processing by software code on a Distributed Ledger or blockchain. In blockchain protocols like Hyperledger and Ethereum, smart contract software is published on the blockchain and thus available to all users of that blockchain.

Reference Framework (ARF) of eIDAS2.0 is expected to support extensions for application areas like logistics, healthcare, and industry.

The current version of a node developed by the FEDeRATED Action still supports a proprietary registration – and credential mechanism. This needs to be replaced by a VC based mechanism, meaning that a node must have an organizational wallet and holder agent software that supports a technical scheme, like the one of eIDAS and/or GAIA-X. This is for further study. Replacing this proprietary mechanism has consequences for the node, since the proprietary solution also supports other functional requirements (like connectivity, discoverability, non-repudiation, and authorisation).

As of currently, there is no public EMDS Framework Regulation and logistics still consists of private dataspaces. Whilst this is still the case, iSHARE can migrate towards the technical scheme developed by private dataspace initiatives like GAIA-X. Since any future EMDS Framework Regulations will be built upon eIDAS2.0, the proposal is to migrate iSHARE also towards the support of the eIDAS2.0 technical scheme.

As the Digital Transport and Logistics Forum (DTLF) concluded in their first mandate (2018), a ‘federated network of platforms’ is required. This recommendation led to the development of a data sharing architecture for supply and logistics and a first prototype of ‘node’ and ‘service registry’ developed by the CEF funded FEDeRATED Action. One of the recommendations of the FEDeRATED Action is the necessity of a Framework Regulation. The recommendation to the Ministry of IenW is to support and stimulate the development of an EMDS Framework Regulation.

There are some considerations regarding the migration of iSHARE towards support of GAIA-X, eIDAS, and any future EMDS Framework Regulation. In all cases, it is about development of a technical solution (based on for instance the iSHARE Satellite software) or credential issuer (e.g. a Dataspace Authority with its issuing policy) competing with open-source software and commercial, certified providers. Only for private dataspaces that adopt the iSHARE data sharing agreements (the legal part of the iSHARE Scheme), the iSHARE Foundation has value as governance structure.

5 Use case 2: Physical access for an action

This section describes IAA techniques in the context of the use case where a customer hires a (sub)contractor to pick up a shipment at a transshipment location like a terminal or airport.

5.1 Description of the Use Case

The use case is based on the following actor roles where each role has responsibilities and constraints:

- Customer (*C*): the customer that wants their shipment, which is a container indicated by *G* containing (for instance) screwdrivers, to be retrieved from the transshipment company (*T*) by the contractor (SP_C). The customer does not know (upfront) whether the contractor hires a subcontractor.
- Transshipment company (*T*): the party that controls the intermediate destination of the customer's shipment. *T* assesses the information presented by the (sub)contractor, to verify that they are allowed to pick up *C*'s goods *G*.
- Contractor (SP_C): the Service Provider directly hired by the customer to retrieve the shipment. SP_C can delegate work to a subcontractor, without communicating this with the customer. The contractor is allowed to pick-up a certain shipment *G*.
- Subcontractor (SP_S): the Service Provider hired by the contractor (SP_C). In this example, the subcontractor cannot delegate work to a sub-tier contractor. The subcontractor is not necessarily allowed to know the identity of the customer *(C)* nor the content of the shipment, i.e. that it concerns screwdrivers. SP_S needs to prove to *T* that they are (indirectly) authorized to pick up *G*, without knowing the type of *G* nor the identity of *C*. After retrieval, SP_S brings *G* to SP_C, who then in turn brings the shipment to *C*.

The following assumptions underly our proposed solution:

- Knowledge about parties
  - The customer knows only *T* and the direct contractor SP_C
  - The contractor knows the customer *C*, transshipment company *T*, and the subcontractor SP_S
  - The subcontractor SP_S knows only the contractor SP_C and *T*
  - *T* knows only the customer *C*
- Knowledge about the shipment
  - The subcontractor SP_S, the contractor SP_C, and the transshipment company *T* are not allowed to know the contents of shipment *G*, e.g. that it concerns screwdrivers.
  - *T* knows the shipment *G* and is holding *G*
  - *T* is already aware that shipment *G* is intended for / property of *C*

Each of these actors *A* has an asymmetric key pair, where *A*'s public key is denoted by pk_A and *A*'s secret key by sk_A. As the names suggest, everyone is allowed to know the public key, whereas only *A* knows their secret key sk_A.

5.2 (Adjusted) chained credentials

This use case being a case of delegation, the obvious approach seems to be to use what are known as chained credentials. However, this approach is not directly applicable for this use case as we will explain.

Chained credentials enable delegation in such a way that a verifier (like transshipment company T) can trace back the chain to the root-of-trust, i.e. the issuer of the credential (customer C in the use case). This ensures that the verifier only needs to trust the issuer, instead of having to trust the delegated party directly (i.e. the (sub)contractor(s) in our case).

The typical approach is to see each delegation as an issuance of a VC that is the encapsulation of the previous VC with the signature of the delegator, with the addition of roles and permissions. For example, a party in the role of 'contractor' is allowed to pick up shipment *G* and delegates the capability of picking up shipment *G* to a party in the role of 'subcontractor'.

Chained credentials cannot be used as-is for our use case since the subcontractor is not allowed to know the customer (its identity and therefore the public key should not be shared with the subcontractor) nor the contents of the shipment. This means that the delegation of VC_1 by the contractor cannot simply be an encapsulation of the previous credential, but it does offer a basis for an approach that does work for this use case.

With slight alterations to the chained credentials approach, we can make sure that the subcontractor can see the information that is relevant to them, whereas the information about the customer destined for the transshipment company will be hidden from the subcontractor. We use the roles and permissions as in the chained credentials but add an encryption with the transshipment company's public key (pk_T) on the information about the customer and the contents of the shipment that the contractor sends to the subcontractor. This way, only *T* can decrypt the information about the customer *C*, as *T* is the only one that knows sk_T. This will be clarified in the structure of the VCs.

This particular use case requires holder binding since a VC is only to be used by a (sub)contractor. It means that the contractor and subcontractor each have their own VC. Holder binding is based on the requirement that only authorized (sub)contractors can pick up containers or goods at a location. A truck driver arriving at a gate to pick up goods, may offer the credential in the organizational wallet of his employer, but has to be authorized for that VC. This may require additional features.

5.3 Information – and physical flows

The next figure shows the information – and physical flows.

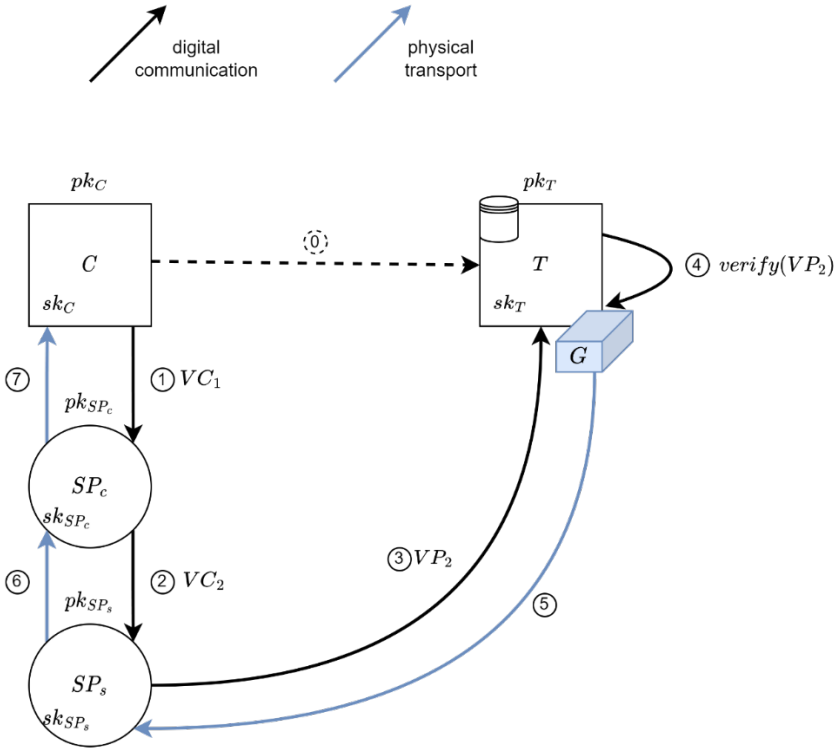


Figure 1 The flow of information and physical shipment for the use case.

The figure shows all roles and interactions between those roles. The structure of the VCs will be described hereafter.

0. [Optional] *C* and *T* communicate about the goods *G*, e.g. that the container is indeed identified by *G*. The communication can take place in a classical fashion or using VCs, this will not be further discussed in this document.
1. *C* creates VC_1 and issues it to SP_C. The contents of VC_1 are described in the following section.
2. SP_c creates VC_2 and sends it to SP_s. The contents of VC_2 are described in a latter section.
3. SP_s creates a VP based on VC_2 and sends this VP_2 to *T*. This presentation contains the (encrypted) claims, the proofs and the metadata from VC_2, additional metadata on when the presentation has been created and where pk_{SP_s} can be found. This is signed by SP_s.
4. *T* verifies VP_2.
5. If VP_2 is accepted, *T* will release *G* to SP_s. In case T cannot accept VP_2, SP_S will not receive G. T may decide to inform C that someone tried to pick up G without proper credentials.
6. SP_s transports *G* to SP_c.
7. SP_c transports *G* to *C*.

5.4 Structure of the VCs

5.4.1 VC_1

C issues a VC of type ShipmentPickupCredential to the contractor SP_C at time '1' (corresponding to step 1 in Figure 1). A graphical display of VC_1 is shown in Figure 2. In the claim, we see that SP_C is allowed to delegate this credential to a subcontractor and has permission to pick up shipment *G*, containing screwdrivers.

The proof is generated simultaneously ('1') by the issuer (*C*). This proof comes in the form of a digital signature (Signature 1 in the next figure) created using *C*'s secret key sk_C. As *C* is the only one who knows this secret key, other parties can be sure that VC_1 was indeed created and signed by *C*. The holder (the (sub)contractor) can prove to the verifier (*T*) that this VC_1 was created by *C*. The verifier needs the public key of the issuer to verify the signature, therefore it is standardly included in the credential proof graph of the credential.

We do not specify here which signature algorithm should be used. Therefore, we also don't generate the signatures and take dummy values for the value of the signature. We will call this proof *Signature 1*. While sending credentials, we assume that the entire credential is encrypted such that only the (sender and the) receiver can see what's inside of the credential.

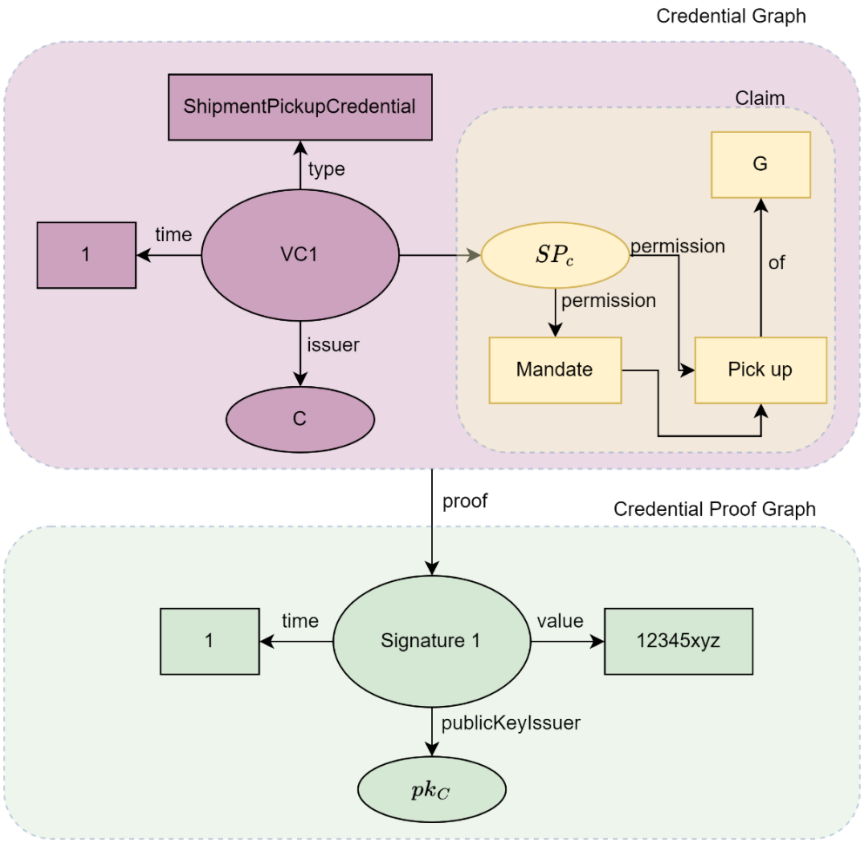


Figure 2 A graphical display of VC_1, consisting of the credential graph and the credential proof graph. The arrows indicate subject-property relationships. The signature value is a dummy value.

The previous figure shows that the claim of SP_C is to pick up G at T, where SP_C also allowed to mandate another actor to pick up G. The value of the proof is an imaginary one; in practice the value is calculated by sk_G, using credential data.

5.4.2 VC_2 and its presentation VP_2

Several steps are being performed for constructing a presentation whereby the subcontractor can pick up G at T. These steps will be explained in more detail:

- Encrypting the private parts of VC1 so that only T can access them
- Issuing a VC to SP_S containing these encrypted parts
- Generating a presentation for T

The contractor first encrypts the private parts of VC_1 with pk_T, generating a derivative credential VC_1^*. These private parts are the identity of the issuer (C) and their public key. This means that only T can decrypt those private parts and know that the subcontractor is to pick up G on behalf of C.

If we display encryption with the public key of T (PK_T) by a lock, we can visualize VC_1^* as in Figure 3. Note that for the subcontractor, VC_1^* is not verifiable, as they cannot check the proof on this credential as they do not know pk_C.

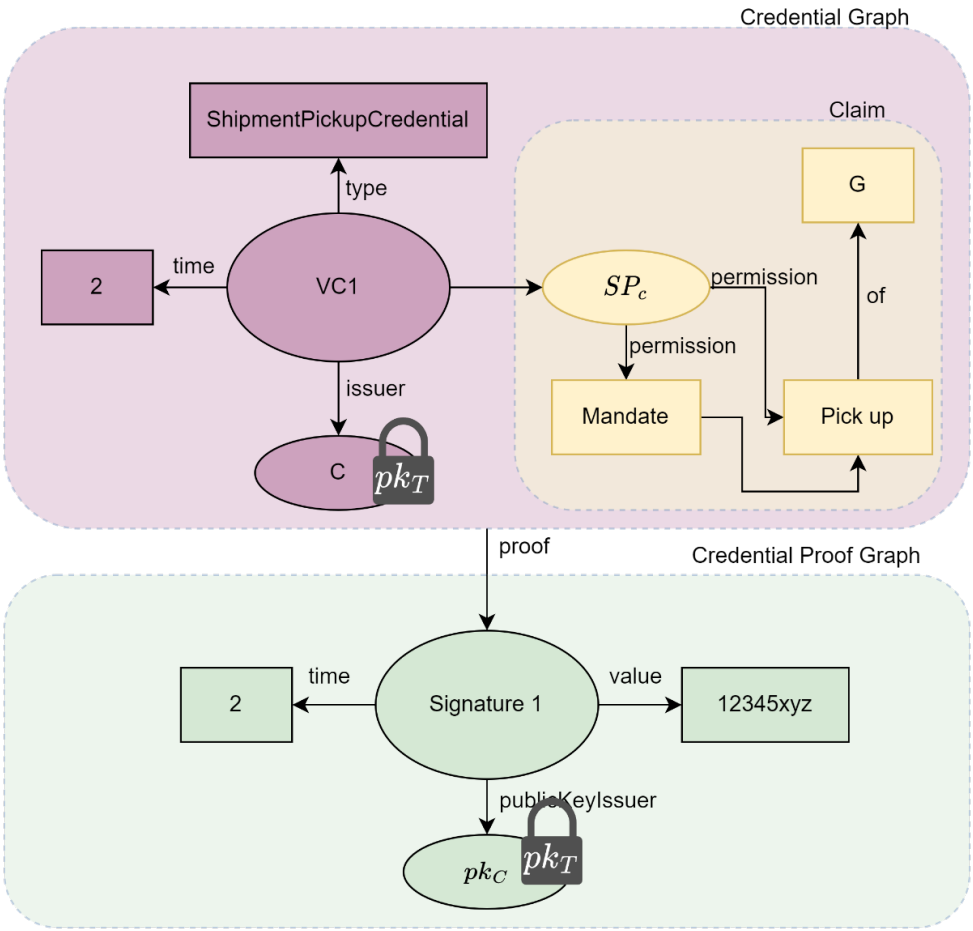


Figure 3 A graphical display of VC_1*. Parts of the credential are encrypted with the transshipment company's public key (pk_T). This is indicated with a lock.

VC_2, which is the credential that will be used by SP_S to pick up G at T, is then constructed by linking to VC_1^* with additional information provided and signed by the contractor about the identity of SP_C and their permissions. This ensures that the contractor indeed delegated this credential to the subcontractor, such that the subcontractor can prove to T that they have a mandate from the contractor.

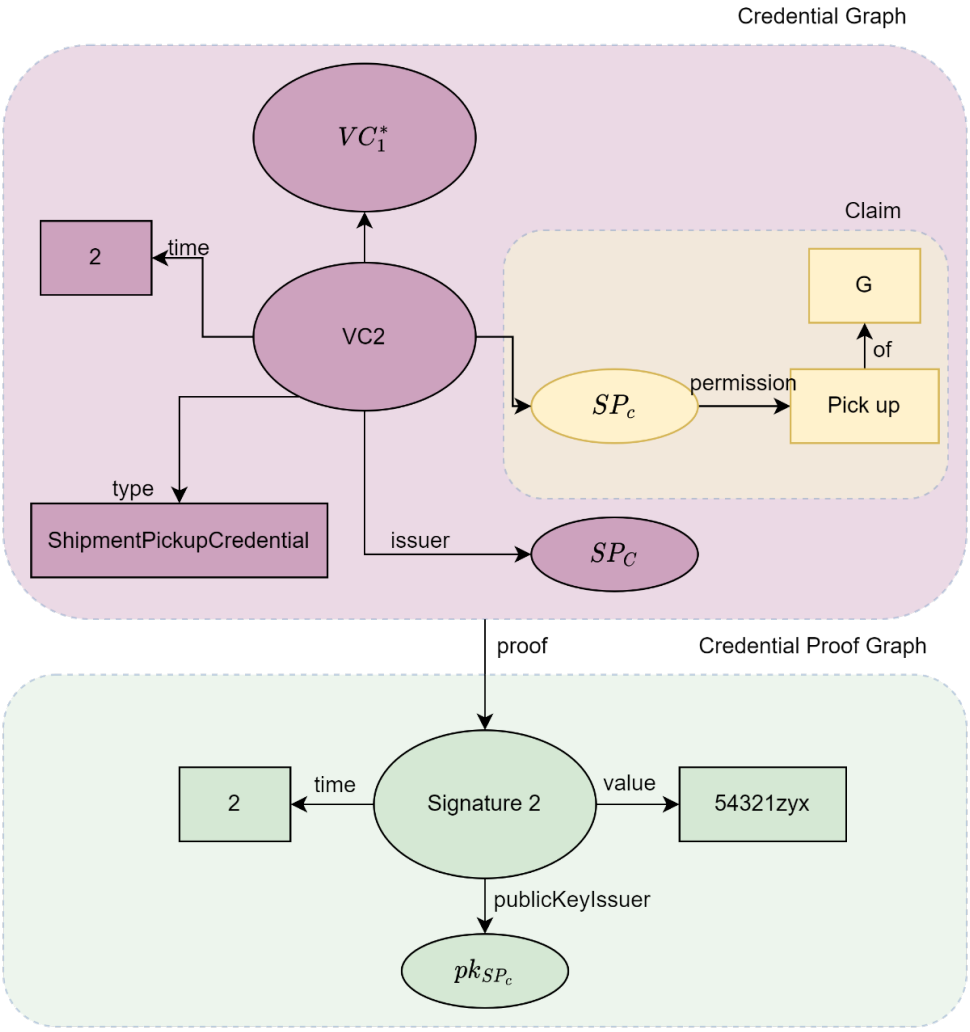


Figure 4 A graphical display of VC_2. The derived credential VC_1^* is included in VC_2. The subcontractor can verify Signature 2 but cannot verify Signature 1 in VC_1^* as it is encrypted with pk_T.

The subcontractor presents VP_2 (the verifiable presentation of VC_2) to T to prove that they are allowed to pick-up G. The subcontractor generates VP_2 by generating a proof over VC_2, while keeping VC_2 as is, which we will call *Signature 3*. The result is displayed in Figure 5.

The previous figure shows that SP_S is not allowed to mandate another carrier to pick up G, as was defined by the use case. If this was allowed, this will be indicated by SP_C in VC_2 and the same mechanism for subcontracting could be used by SP_s as is described here for SP_C.

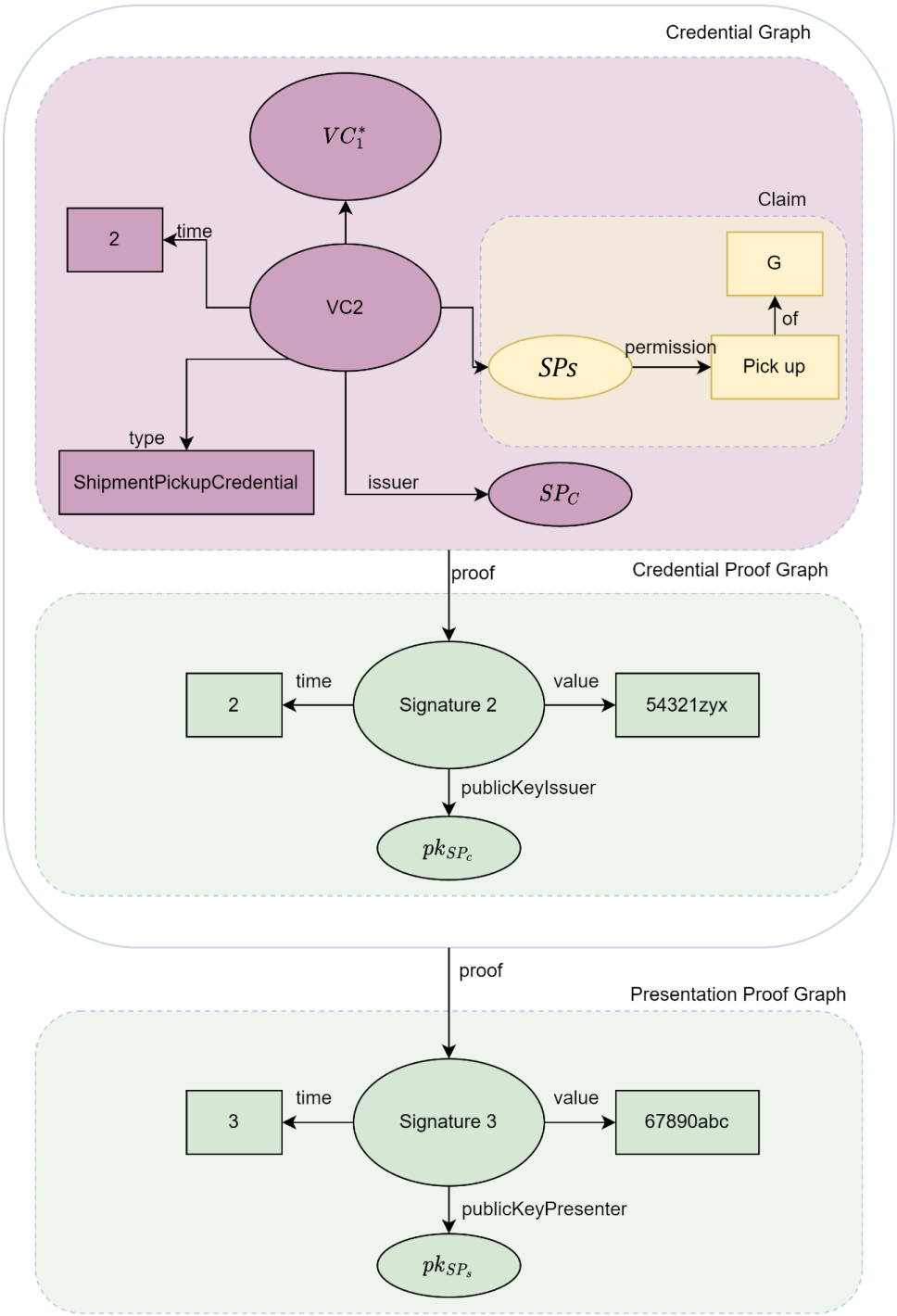


Figure 5 A graphical display of VP_2.

The transshipment company *T* can then verify the credential by:

1. verifying *Signature 3* over VP_2 with public key pk_{SP_S}.
2. verifying *Signature 2* over VC_2 with public key pk_{SP_C}.
3. decrypting *publicKeyIssuer*, *issuer* and *type* of G in VC_1^*, using their secret key sk_T.
4. verifying *Signature 1* over VC_1 using pk_C.

T then validates the information against their validation policy, which will typically consist of:

- Is shipment *G* listed in credentials VC_1 and VC_2?
- Does SP_S have a ShipmentPickupCredential that can be traced back to the client *(C)*?
    - Did SP_C issue VC_2 to SP_S?
    - Does SP_C have a ShipmentPickupCredential issued by *C*?
    - Does SP_C have permission to delegate this ShipmentPickupCredential?

5.5 Discussion

There are other ways of implementing this solution, like applying smart cards. **Physical access** by applying smart cards with biometric applications can only be applied for authenticating the identity of a person. These types of cards cannot be applied for authorisation: which action is allowed. Authorisation, like physical access to a premises, usually takes place after authentication, where the actual action to be performed still requires additional authorisation. These two functions, permission to perform an action on a location, can be combined in a VC. In this case, holder binding is required, where the VC might be stored in a business wallet of a (sub)contractor or the wallet of the truck driver picking up the goods. The use of a personal (truck driver) or organizational wallet requires further attention.

If these authorisation functions combined in a VC are to replace a smart card, there must be support for situations like contracting and subcontracting. A logical way would be to implement chain delegation. Chain delegation can be supported by VCs and does not require any additional registries. It requires however a capability of stakeholders to issue those VCs, whereas these issuers must be trust. Trust will be based on the existence of a business relation for a business activity (like the transport of goods). Even chain delegation by which the identity of a customer is hidden for a subcontractor (commercial sensitivity) can be implemented by VCs as demonstrated in our use case.

Other solutions for delegation are the application of the iSHARE Authorisation Registry in a dynamic organizational network where business relations are based on individual business transactions. Each business transaction could lead to an entry in an Authorisation Registry for only that business transaction, whereas the objective of the Authorisation Registry would be to support longer delegation relations (e.g. contractual relations). A third solution is to directly relate authorisation to the business transaction hierarchy and allow for (federated) querying at a gate to retrieve the authorisation for pickup of goods.

Thus, we potentially have four solutions to this use case, where the one for applying VCs is explored in this section. That latter one may require additional piloting and development for functioning as, in our view, the most secure one since only a driver with the proper VC can enter a gate to pick up goods. Supported by additional federated querying as a way of cross-validation, it may even be more secure. This requires the installation of the data sharing infrastructure with nodes.

6 Conclusions, implications, related developments, and next steps

This section provides conclusions with respect to SSI/VCs, its implications for existing solutions like iSHARE and smart cards for physical access, provides an overview of related public – and private developments and gives recommendation for next steps. Although DIDs are typically used in a VC infrastructure, this aspect is not yet explored and requires further attention.

6.1 Conclusions

This report outlines two potential usages of SSI technologies in supply and logistics, namely for on-boarding of and data sharing between nodes in a network like Base Data Infrastructure and another for physical access to pick up goods at a premises. The selection of these two use cases has been done with input from the lead architect of the DIL project. A demonstrator for the first use case was constructed during the IATA Hackaton in June 2023, Frankfurt. The results are accessible on Youtube.

We see huge potentials in applying SSI technologies in supply and logistics. Applying these technologies decouple Identification and Authentication from Authorisation. IA can be by a VC with a business wallet; authorisation can be arranged by each organization internally. A business wallet requires further integration with internal systems for IAA.

In these use cases, VCs are the obvious solutions, which means that we did not exploit the applicability of DIDs (yet). These are mentioned in our recommendations.

The report does not consider other mechanisms and technologies that may provide the same functionality as required by the use cases but shows the potential of a completely distributed infrastructure with multiple (accredited) Issuers, Holders, and Verifiers of these VCs. A VC based infrastructure is specified conceptually in such a way that it can be applied for various use cases, for instance by introducing terms like ‘capability’ and ‘Issuing Policy’. These abstract concepts need to be made specific for a use case, thus leading to a specific infrastructure to support such a use case. Technically, a VC infrastructure consists of components like a ‘wallet’ with protocols to interface with issuers and verifiers. Since there is standards are under development, like the Architecture Reference Framework 1.0 with a new version mid 2025, we should note that these protocols are not yet fully independent of the wallet that is selected for implementation.

In the first use case, a wallet is associated to a node. Access to that node by an employee, and thus using the wallet, must be restricted via the local interface to that node and the authorisation of the employee to apply that interface. Most applied technology is the implementation of local (open)APIs with an API manager for Role Based Access Control

(RBAC) [3]of these APIs. This is the responsibility of the organization that wants to use the node in data sharing with others. This responsibility can be made part of a voluntary EMDS Framework Regulation to be developed by EC DG Move and be a basis for an issuing policy. Such an issuing policy must consider SMEs (Small and Medium sized Enterprises).

Furthermore, the 'capabilities' in the first use case represent the concept of 'profiles' introduced in the FEDeRATED Architecture to support plug and play. The use case description shows how these capabilities can be applied in data sharing after on-boarding and authentication of a node.

eIDAS2.0 that includes VCs and extensions for a (voluntary) EMDS framework regulation is applicable for onboarding a node in the network. The issue is the speed of development and adoption of a such an EMDS framework regulation. An EMDS framework regulation provides a trust framework that fully overlaps the one iSHARE could develop for an EMDS. As long as an EMDS framework regulation and its support by eIDAS extensions does not exist, iSHARE might act as intermediate solution.

The migration strategy of existing mechanisms like iSHARE and the current version of the node developed by the CEF funded FEDeRATED Action have been assessed.

iSHARE covers various aspects relevant to IA (they also have mechanisms for authorisation, that are out of scope for onboarding a node). These can migrate as follows:

- Private technical schemes – inclusion and implementation of private VC-based technical schemes like developed by GAIA-X in the iSHARE Scheme and by the Satellite software.
- Public (eIDAS2.0) schemes – support by the Satellite software of the eIDAS technical scheme. The iSHARE legal aspects are overruled by eIDAS for public dataspaces.
- Public/private dataspace – this is about adoption of a public regulation by the private sector. Satellite software must support eIDAS2.0 technical schemes plus extensions for a dataspace like EMDS.

Migration of the current version of 'node' is by replacing the Corda Registration and credential mechanism by an open, VC-based infrastructure. It is not clear of Corda will support such an open infrastructure; otherwise Corda has to be replaced by another solution. It also implies that another solution must support functional requirements currently implemented by Corda (e.g. connectivity, discoverability, non-repudiation, and authorisation).

In the second use case, physical access to pick up goods at a location, a presentation of a credential with a claim for picking up those goods is handed over. This presentation is retraceable to the owner (or his agent) of the goods that transported to a destination. The claim is part of the VC, including required proofs. Of course, the claim can be more detailed by adding for instance real world identifications like shipment reference number or container number. The use case does not require any other means of identifying the actor picking up the goods; these are part of the VC presented that is irrevocably associated with the holder. Thus, the holder also identifies themselves and is authenticated as such.

The specification of this second use case is a variant of chain delegation, in such a way that a subcontractor does not know the actual customer. Such may be a requirement where commercial relations are not shared in case of subcontracting. Other solutions provided in

[3] Policy Based Access Control (PBAC) is a new development where rules specify the access control. This may provide more agility in the context of data sharing.

that section are an Authorisation Registry like provided by iSHARE that must support delegation at business transaction level or (federated) querying based on the existence of nodes in a data sharing infrastructure. A combination of VCs and querying is in our view the most secure solution.

6.2 Recommendations

This part provides recommendations for next steps focussing on the long-term establishment of an infrastructure for VCs, proposing extensions of the use case, and proposals for additional use cases. A more general recommendation is to include the results of this study in the FEDeRATED Architecture.

We have the following main recommendations that will be detailed:

1. Stimulate the development of a voluntary framework regulation by EC DG Move for the EMDS (freight and potential persons) with on eIDAS2.0 and EBSI and develop a prototype environment to support the proposed solution.
2. Set up a demonstrator for physical access to a location using VCs.
3. Explore new use cases like data access by VCs and all types of statements issued by authorities (permits, customs release, certificates, personnel screening, etc.) or other trade related organizations (Letter of Credit, commercial release, etc.).

6.2.1 Nodes in the BDI – requirement for a framework regulation for EMDS for freight

Our **main recommendation** is the development of a (voluntary) framework regulation of the EMDS (to be developed by EC DG Move) based on VCs as a crucial element to create an open, neutral data sharing environment (or federated network of platforms) supporting all stakeholders (level playing field) with existing initiatives. These VCs contain profiles which can be tested, certified, and monitored for supervision of this regulation. The Regulation must cover at least issuing policies and governance aspects of the infrastructure. EC DG Move is recommended to investigate how this solution can become part of the next version of the Architectural Reference Framework (ARF 2.0), to be published 2025.

This relates to the use case for onboarding of a node in the infrastructure. It is about the creation of a VC based data sharing infrastructure and the integration of the solution in ARF2.0, making optimal use of existing private – (GAIA-X) and public (eIDAS and EBSI) developments. These private – and public initiatives require further assessment to come to an alignment. Since eIDAS2.0 will be implemented by mid 2025, issuers will be ready before that deadline. Assess the status of these issuers as part of the current eHerkenning solution in the Netherlands.

Our **second recommendation** is to develop a prototype solution consisting of a solution for an issuer, holder, and verifier for a VC-based EMDS Framework Regulation. A node should be complemented by organizational wallet (and its agent) software, both for holder and verifier since a node can have both roles; an issuer might be supported by iSHARE Satellite software for issuing VCs and registering nodes. This should replace the current Corda software implemented by the prototype node.

This last recommendation is in line with the recommendations for iSHARE migration towards its use in VC-based public – and private dataspaces.

Based on this main recommendation, we recommend the following actions, which we will explain hereafter:

1. Stimulate and support the development of an EMDS framework regulation by EC DG Move. Action to be taken by the Ministry of Infrastructure and Water (IenW). The alternative is to develop and finance private solutions that are not adopted by public authorities, since these are bound by public regulations like eIDAS2.0. This leads to separate public – and private dataspaces.
2. Assess the implementation of eIDAS2.0 by eHerkenning and potential others in the EU, propose recommendations for setting up the required organisational infrastructure. Action to be taken by IenW (can be supported by TNO or an external consultant).
3. Assess the development of ARF2.0 and seek for alignment with EMDS, based on the proposal for including 'profile' in a VC of a node. Action to be taken by EC DG Move.
4. Develop a prototype node, Registration – and Certification Authority software to support the framework regulation. This is fulfilling the second recommendation. Setting up a conformance test environment has been part of the original plan of DIL. Action can be taken by IenW, supported by DIL and TNO.
5. Assess the development and relevance of an organizational wallet by GAIA-X. Action to be taken by IenW, supported by TNO.

Implementing these features in data sharing implies that all those that use them, comply with a Regulation for data sharing in logistics that is built upon others like eIDAS 2.0.

With respect to the operation of a VC based data sharing infrastructure, one of the main issues is trust in an issuer. EBSI could assist in this, functioning as a distributed registry of trusted issuers. This could be based on multiple factors like accreditation by an external body, or a transparent Issuing Policies of an issuer.

An **Issuing Policy** can be simple (e.g. based on membership of a community) or more complex (e.g. requiring compliance with a Regulation). To create a viable, open, neutral federated network of platforms like the Base Data Infrastructure, Issuing Policies must overarch an issuer, meaning that many issuers must adhere to the same Issuing Policy.

Such an (international) Issuing Policy requires what can be called legal code: private agreements or a (public) **Regulation**. It is our experience that there will always be multiple private agreements, since various (private) communities will develop data sharing applications in parallel. These private agreements may overlap but can also have conflicts. Therefore, we recommend having a Regulation, preferably spanning as many nations as possible. For now, EU level seems to be the most feasible, since these types of discussions may not yet have started globally. In our view, the EC must develop such a Regulation overarching private law, providing guidance to business, and creating a market for innovation. EU Member States that implement such a Regulation may function as **accreditation** actors providing trust in Issuers.

Once this Issuing Policy is derived from a Regulation, many Issuers can be accredited. This goal could be achieved by approaching organizations that perform a similar function, like for eHerkenning and/or providing services in supply and logistics. Examples could be Dun&Bradstreet, national or International Chamber of Commerce (ICC), or others.

Furthermore, the required **capabilities** for getting issued a VC must be specified in the Issuing Policy. This can be on the one hand compliance of an organization with existing acts and regulations (like the Data (Governance) Act and Cyber Security Act) and on the other hand compliance with the data sharing architecture, i.e. the protocols and capabilities required to share data in a Base Data Infrastructure. A complete chain of trust must be constructed where employees of organizations can be sure that data is not changed or accessed without authorisation. Data sovereignty must be assured.

This last aspect requires integration of the proposed approach for node identification in the **architecture**, including the capability matching protocol and profiles. Second, VCs can be supported by the current prototype node to demonstrate how it works.

The architecture must also prescribe the use of VCs by a platform with multiple users. On the one hand, the platform will have a VC for its node, on the other hand it may have a profile per user or a single profile for all users. The choice between both will most probably relate to whether the platform offers a single service (like visibility) or different services for different roles.

Specification of VCs with their capabilities as part of the architecture will require refinement of specifications for the ‘profile’ and the ‘capability matching protocol’. These are details that will be provided.

Finally, large scale application is not only served by many issuers, but also by providing **test facilities**, whereby organizations (or providers of solutions to organizations) can test their capabilities before requesting a VC. The test facility can be extended by mandatory test runs (and associated data sets) for certification. It is recommended to have web-based test facilities.

Since these facilities will test ‘profiles’ and there are potentially many profiles, the architecture must prescribe how the test functionality must be organized. Certification can be performed by a Certification Authority. These Certification Authorities could also implement a periodic (or real-time) testing based on monitoring data shared by organizations (‘process mining’).

6.2.2 Physical access for an action

With respect to performing a physical action on a location by a non-employee, we recommend using VCs. This is about the second use case. It is first about the capability whereby a customer can provide a service provider with the option of subcontracting. This may be enabled by default because otherwise it implies that a customer controls business decisions of its service provider. But when a service provider is not allowed to subcontract, this limitation could be provided in the VC issued by a customer.

The second recommendation is to install a demonstrator for this use case, whereby also a truck driver (or more generic: an operator of a transport means) is involved. This driver will require the VC in its wallet for an action that is to be performed at a location, like picking up or dropping off goods or container(s). Such a demonstrator will have to be supported by a wallet infrastructure and the capabilities of all relevant stakeholders to issue a VC, potentially included in a business transaction. The latter implies an extension of the architecture, where interaction patterns must be associated with VCs. This will allow for a better integration of the IT environment with the physical world.

6.2.3 Potential other applications

Based on these two use cases, we recommend to further research the following use cases[4]:

- **Federated querying (data access)** – this is a use case whereby an upstream actor requests downstream data, whereby upstream and downstream actors don't have a direct relation (business or legal). An example is where a customs authority requires upstream data of a declarant, the latter needs to request data of its business partners and the declarant is not allowed to read the data provided by its business partners. This will allow for instance the querying of container content by a customs authority to a carrier, where the data of the content is provided by a forwarder. This is a type of chained delegation, potentially like the one of the second use case in this report.

  In business-to-business, this type of VC applications requires further attention, since a customer may not (want to) know a subcontractor (see second use case), whilst a subcontractor may require access to data of that customer.

- **Permits** – such a use case is quite straight forward. An authority issues a permit for a particular type of activity to a logistics stakeholder. A drivers' licence is already an example of such a permit, a permit for transportation of dangerous goods is another example. Examples like a drivers' licence are already developed for education.

  A (customs) **release** or certificate of origin are also a type of permit for goods, whereby it must be clear that an authority is the issuer of this type of permit and integrity of the data can be assured. These are claims issued by an authority about the goods. This differs from a VC that is irrevocably associated with a holder. The role of DIDs could be investigated for these types of cases.

- **Trade related statements** – there are all types of statements made by public – and private organizations like Certificate of Origin and Letter of Credit. These statements are issued for single goods flows and may potentially be held by different organizations; it has to be sure it is issued by a certain organization.

- **Employee screening** (VGB – Verklaring Geen Bezwaar – or VOG – Verklaring Omtrent Gedrag) – this is a use case where a (natural) person receives a claim stating that an authority has investigated the behavior of this person and finds it compliant with a certain security level (VGB) or a claim stating that the person has not been convicted for any crime relevant to the performance of his or her duties (VOG). This would potentially reduce risks for illicit behavior of persons, both employees and others. The person can store this claim in a wallet in the form of a VC, besides other claims such as a VC that they can use to identifying themselves.

When identifying additional use cases, one must bear in mind to make a balance as to which data is in a VC and in IT systems. Conceptually, all data can be part of a claim in a VC (or its presentation), for instance a complete CMR or eB/L data set.

Thus, VCs could be applied for sharing data. However, business collaboration requires adaptation to changes (resilience and agility), whereby data changes. This implies that it may be beneficial to share only linked event data between IT systems of organizations (data at the source) and only store the actual data in the form of VCs when it concerns limited non-volatile data, , e.g. the case of physical operation by a truck driver with a VC per shipment/consignment. Such types of applications for VCs must also be considered in the context of on-board units since these may already contain the data. Furthermore, such

[4] For scalability across the EC (and global), these may have to be included in ARF2.0 (further research).

types of VC applications also require a revocation mechanism at delivery of the goods, where revocation is performed by a consignee (which is a business role, that is not necessarily a verifier).

With respect of eB/L data, such data sets are issued as a claim by a shipping line to its forwarder at exit. This forwarder will have to hand over the eB/L (thus the claim) to a forwarder at entry. This transfer either implies a type of chain delegation since a VC is associated to a single holder, or to apply another technology(-ies).

ICT, Strategy & Policy

Anna van Buerenplein 1
2595 DA Den Haag

www.tno.nl

TNO innovation for life