EUROPEAN
FEDERATION
OF BUILDING AND
WOODWORKERS

FIEC
EUROPEAN CONSTRUCTION
INDUSTRY FEDERATION

Technical Feasibility Report on Social ID Cards

in the Construction Sector across the European Economic Area

Social identity cards in construction (SIDE-CIC) project – Technical experts

A Joint-Project of the European Social Partners for the Construction Sector on Social Identity Cards in Construction

ABSTRACT

The Technical Feasibility Report developed under the SIDE-CIC project assesses the potential to establish an interoperable Social ID Card information-exchange system across EU Member States in the construction sector. FIEC and EFBWW have commissioned this study not to set out a policy position but to examine the technical feasibility of interoperability in a neutral manner and to explore how existing national schemes could voluntarily exchange data without altering their underlying structures. The study proposes a new approach to addressing the current and growing challenges related to workforce mobility. Creating an interoperable data network or data space would support more efficient cross-border mobility and provide stronger tools for compliance enforcement. The report examines various technical options for achieving interoperability, along with the associated obstacles and risks, and also considers organisational, financial, and governance implications. In addition to outlining a roadmap from the current state to the desired future state, the study presents relevant benchmarks from comparable cross-border systems. The report concludes that no major common technical barriers prevent the implementation of such an information-exchange system. Existing EU funded frameworks and support structures for establishing Data Spaces could significantly reduce the time, effort, and resources required for system development and operations. This would, however, require strong stakeholder commitment and collaboration to address organisational and potential political issues. Overall, the report finds that a European-wide information-exchange network would bring significant benefits, and that with a step-by-step approach building on existing interoperability frameworks, its implementation is achievable.

AUTHORS

Lars Albäck (Certapartners Oy)
Dalius Mašalas (Moxy Identity Services AB)
Claes Rydin (Moxy Identity Services AB)

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or of the DG for Employment, Social Affairs and Inclusion. Neither the European Union nor the granting authority can be held responsible for them.

Table of content

1 Introduction

1.1 PURPOSE AND SCOPE OF THE STUDY

The SIDE-CIC project aims to strengthen EU rule enforcement, support fair worker mobility and boost transparency in Europe's rapidly evolving construction sector.

The industry stands at a crossroads: the workforce is becoming increasingly cross-border, especially with rising numbers from other EU and third countries — making enforcement and fairness harder to guarantee. At the same time, modern digital tools open up new opportunities to meet these challenges through real-time, trusted and context-specific data sharing.

The problem? Crucial data is scattered across multiple stakeholders, with no existing interoperability or connected system to bring it all together.

The goal of the SIDE-CIC technical study is to map out how existing national Social ID card schemes could interoperate across Member States and how a secure, governed data exchange network, could be built. A SIDE-CIC network would be the environment where Social ID Card information would flow between the participating members. This work builds on the project's earlier mapping and is closely coordinated with the legal team's findings.

To truly understand feasibility, the scope was expanded to include network organization and legal-technical overlaps. One key insight: legal, technical and organizational elements are deeply interconnected and must be addressed together.

This report focuses primarily on technical aspects, evaluating feasibility, exploring solution options, identifying risks and highlighting best practices that can inspire a shared European approach.

The purpose is not to create a policy position or discussion. This topic is however interrelated to ESSPASS and ongoing discussion in Member States where cards are in development like the Netherlands and Romania.

The purpose of this report is to examine if Social ID Card systems across Member States can be made interoperable to enable seamless data exchange and deliver real value to all stakeholders?

1.2 METHODOLOGY AND INTERVIEWS

The technical analysis has been carried out by using the following methods and frameworks:

1. Interviews of Social ID Cards service providers and data interoperability and data exchange experts
2. Execution of 3 workshops with all key stakeholders in the project
3. Study of appropriate and applicable technical solutions
4. Demonstration of Data Exchange flow between 2 countries
5. Outline of technical services to be provided by the network which will help assess the technical interoperability model
6. Benchmarking of similar cross country data exchange networks and data spaces
7. Application of an EU Commission aligned feasibility study framework
8. Application of key questions per feasibility area model from Sitra Data Rule Book 3.0[1]
9. Review of studies on key subjects (ex. User consent or permissioning).

The work has been coordinated with the Legal experts, Spark Legal and Policy Consulting, as well as with the project responsible from EFBWW and FIEC. In addition, the technical team has attended and presented in the project steering committee meetings during the project. All relevant stakeholders have been invited to the workshops.

[1] The „Sitra Data Rule Book," developed by Sitra, the Finnish Innovation Fund, provides a framework for building trust and facilitating data sharing in various sectors (https://www.sitra.fi/en/publications/rulebook-for-a-fair-data-economy/).

1.3 PROJECT PLAN, WORKSHOPS AND PROOF OF CONCEPT (PoC) DEMONSTRATION

The project plan proposed in the Tender for the technical analysis has been carried out with the following tasks and milestones as illustrated in the graphic below.

The workshops have been a key aspect of the study as they have provided a possibility to gain further insights, different opinions and verification of the key aspects evaluated and concepts created.

The workshops can be summarised as follows:

- **Workshop #1, Define:** purpose to verify the mapping stage findings and assumptions regarding interoperability and governance solution
- **Workshop #2, Create:** review of the flow demonstration demo between Vastuu Group Finland and Statreg Lithuania. Evaluation of possibilities to organise the data exchange network as a Data ecosystem creating a Data Space
- **Workshop #3, Verify:** evaluation of alternatives, obstacles and feasibility assessments as well as risk analysis.

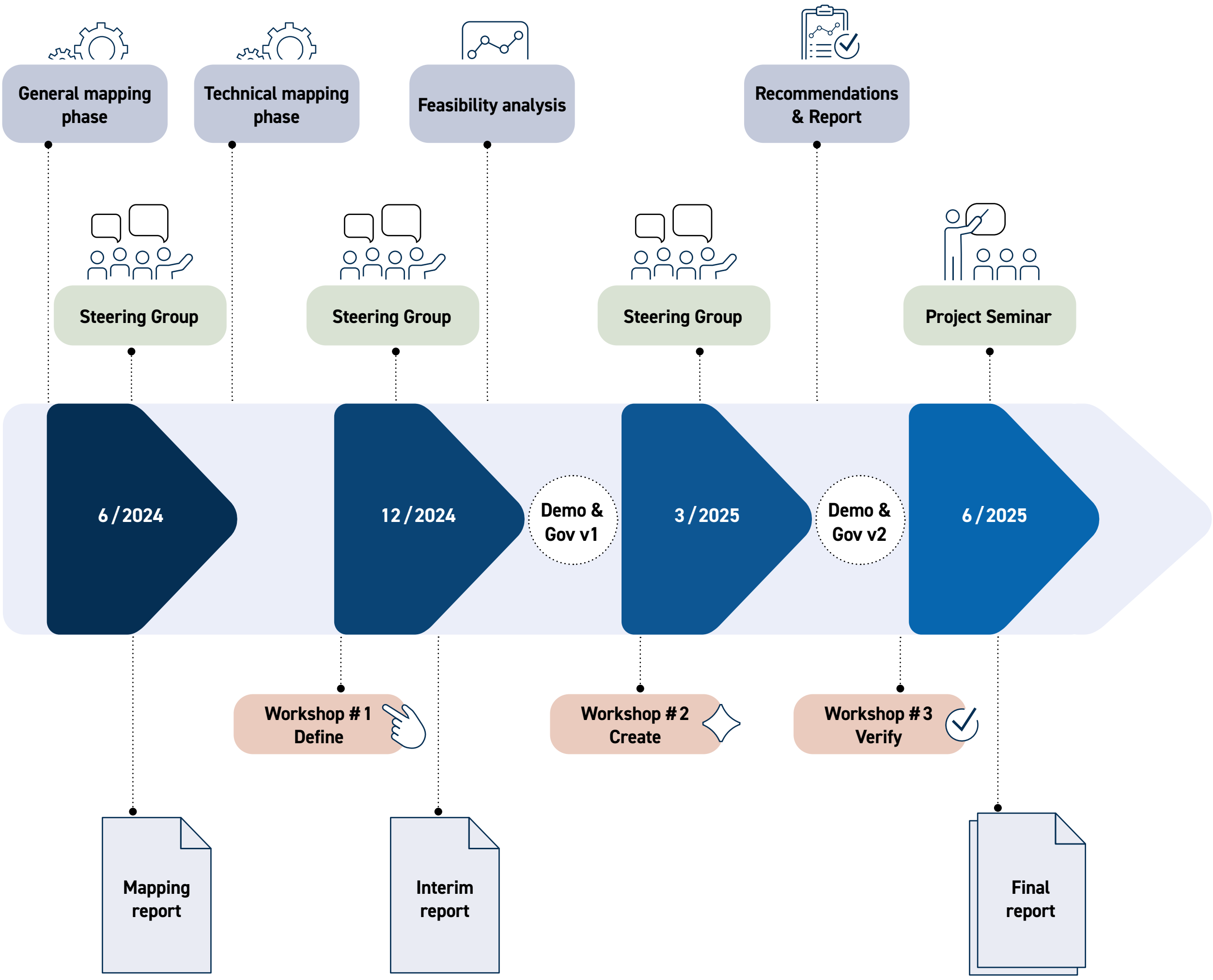
1.4 STRUCTURE AND LOGIC OF THE REPORT

The technical report is divided into 3 main sections:

- Technical mapping
- Technical feasibility
- Conclusions

The sections follow a logical path in the sense that the summary from the previous part serves as the input to the next chapter. In this way it is possible for the reader to follow the logic behind certain decisions and assumptions.

Graphic 1 Project Plan



1.5 GLOSSARY

API: Application Programming Interface, enabling systems to interact and exchange data based on predefined protocols.

Connector: A technical component used to facilitate secure and standardized data exchange between nodes.

Data Mapping: The process of matching fields from one database to another to ensure accurate data transformation.

Data Ontology: A structured framework to define data elements and relationships, ensuring semantic interoperability.

Data Space: An infrastructure enabling data transactions among different data ecosystem parties governed by a shared framework.

DC4EU: Digital Credentials for Europe initiative supporting interoperable digital service infrastructures.

eIDAS: EU regulation for electronic identification and trust services, crucial for digital identity verification.

ESSPASS: European Social Security Passport, a digital wallet for cross-border social security credential verification.

Gaia-X: A European initiative and framework for creating interoperable and sovereign data infrastructures.

Governance Framework: A set of rules and procedures that govern the operations and dispute resolutions within the data space.

Interoperability: The ability of different systems and organizations to exchange and use information coherently.

Level of Assurance (L0, L1, L2): Classifications of data reliability based on source verification and update mechanisms.

OID: Object Identifier (OID) — A globally unique identifier used to name or classify objects in a standardized, hierarchical way, commonly applied in information systems, cryptography, and data schemas.

PDA1: A portable document used to verify social security rights of posted workers across EU countries.

Social ID Card: A digital or physical identity card used in the construction sector to verify workers' identity, employment, and compliance.

Trust Network: A consortium of entities that ensure secure and reliable data exchange through shared trust principles.

2 Background and need analysis

2.1 BACKGROUND AND LANDSCAPE IN THE CONSTRUCTION SECTOR

One of the biggest drivers for EU was and still is the creation of an EU single market and the free and effective mobility of goods, services and people. In the construction sector it is important, at the same time, to ensure worker's rights and prevent social dumping. One of the key enablers of a single market is the availability of trustworthy and good quality data. In the construction sector, to enable mobility, reliable information about cross-country workers and their employing companies is key.

The graphic below highlights the changes in the industry leading to more mobility in the sector, an increasing demand for workforce from other EU and 3rd countries and the subsequent challenges it creates as well as the potential solutions. The main point is that all stakeholders must work together and find a common model for exchanging data to find a long-term sustainable solution. The current model where work is mostly happening in "silos" i.e. separate from each other, is not sustainable.

In the construction sector, most of the workforce related challenges are linked to mobile workers that are deployed either cross country or that are represented by a seemingly domestic company and employer. The reason for this is simply that it is much more difficult to ensure that rules and regulations are followed in relation to workers from other EU and 3rd countries.

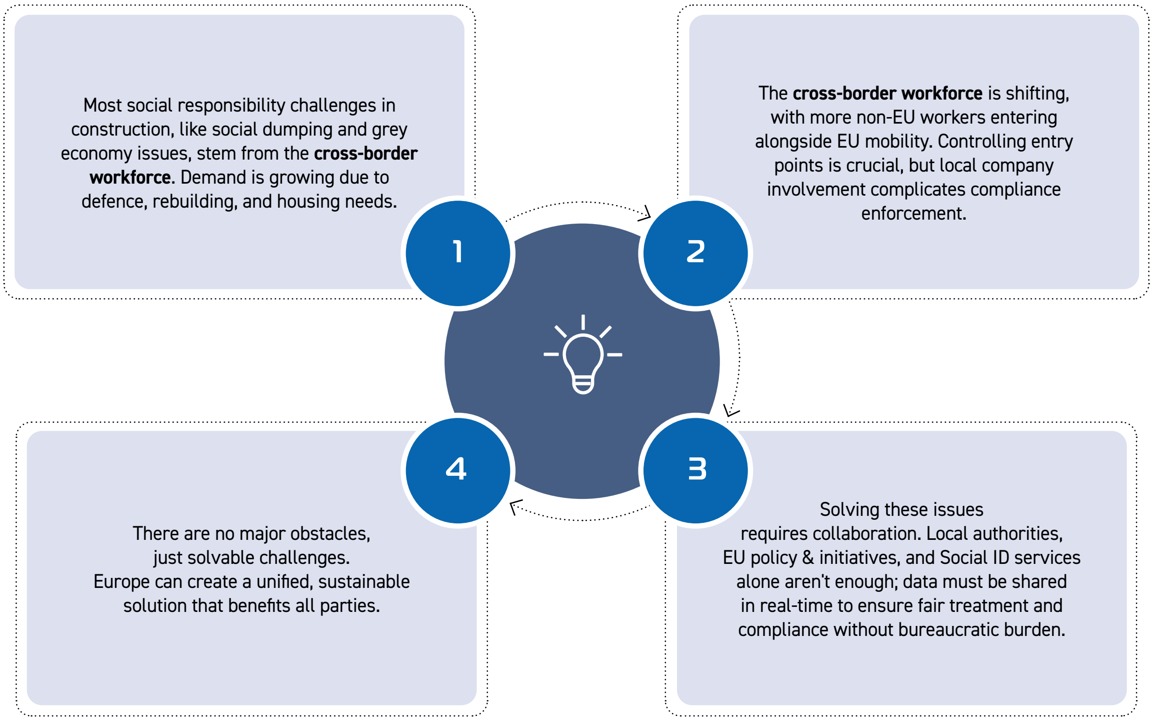
The need for workforce from other EU and 3rd countries is increasing with heavy investments in green transition industry solutions, military and defence facilities and factories as well as the re-building of war or natural catastrophe areas.

Over the past decade the demographics of workforce mobility has changed from a scenario where Inter-EU mobility (e.g. from Eastern Europe to Western Europe) was the most usual scenario to a scenario where non-EU workforce is increasing rapidly. At the same time companies from other EU and non-EU countries set up subsidiaries that seem like local companies to minimize the scrutiny in relation to the origin of the company and the workforce they are deploying.

This situation calls for a joint solution, where all stakeholders can work together and have access to the right data and tools. Authorities and private actors in the construction industry must work together and have access to the same information and tools.

To enable the flow of cross-country workers in the most effective and purposeful way with respect for the individual needs, is the premise for the creation of a Social ID Data Exchange Network. EU is investing heavily in the creation of a prosperous data economy based on EU values. To enable this transition EU has created frameworks for Data Spaces enabled by Data Ecosystems to emerge in different industries.

Graphic 2 Background story for the conclusions and recommendations


1
Most social responsibility challenges in construction, like social dumping and grey economy issues, stem from the **cross-border workforce**. Demand is growing due to defence, rebuilding, and housing needs.
2
The **cross-border workforce** is shifting, with more non-EU workers entering alongside EU mobility. Controlling entry points is crucial, but local company involvement complicates compliance enforcement.
3
Solving these issues requires collaboration. Local authorities, EU policy & initiatives, and Social ID services alone aren't enough; data must be shared in real-time to ensure fair treatment and compliance without bureaucratic burden.
4
There are no major obstacles, just solvable challenges. Europe can create a unified, sustainable solution that benefits all parties.

To respond to the challenges mentioned above, the idea to create a Pan-European Data Exchange Network has emerged. This would enable both construction workers and employers to work in other members states with minimum bureaucracy and waste of time and resources but with maximum social security and worker rights protection.

In addition, a Data Exchange Network in the form of an Ecosystem which would form a Construction Social ID Data Space could provide benefits for all parties involved. Companies employing workforce from other EU and 3rd countries and national enforcement and inspection authorities as well as private inspection companies would benefit.

An alternative with a data driven approach could create benefits for member state Social ID solution providers and their customers as well as governing authorities. The other alternative is to rely on declared data from the construction companies which is not favourable and creating a lot of waste for all parties involved.

2.2 MAPPING OF STAKEHOLDERS AND INCENTIVES

The stakeholders for the implementation and operation of data exchange between the Social ID card schemes across the European Union's construction sector can be grouped as shown in Graphic 3.

To enable the co-operation intended in SIDE-CIC the stakeholders mentioned above would need to co-operate and enable exchange of data through novel solutions like accreditation of privately issued Social ID Cards. Currently, as stated earlier the stakeholders do work in vertical silos instead of working horizontally.

Motivation to develop more interoperability between social ID cards schemes for different parties:

Social ID Card service providers

- Trustworthy, verified and better-quality information would enable the provision of better services to both construction service providers and buyers in the local market (e.g. PDA1).
- Possibilities to provide additional service schemes that enable the digitalisation of the whole value chain and life cycle of acquiring workforce from other EU and 3rd countries.
- Possibilities to co-operate with peer organisations to influence key stakeholders such as Social Security Institutions.

Social Partners – Trade Unions

- Reliable and high-quality information of workforce from other EU and 3rd countries would enable effective tools to combat grey economy and social dumping.
- It would also create a level playing field between all players by providing digital possibilities to inspect and prevent fraudulent behaviour.
- In addition, it would provide possibilities to add information on Collective Bargaining Agreements and assure that workers' rights are respected.
- Agreements both for workforce flowing into the country and workers going abroad.
- The possibilities of workers being left out of social security and proper insurance schemes would be reduced significantly.

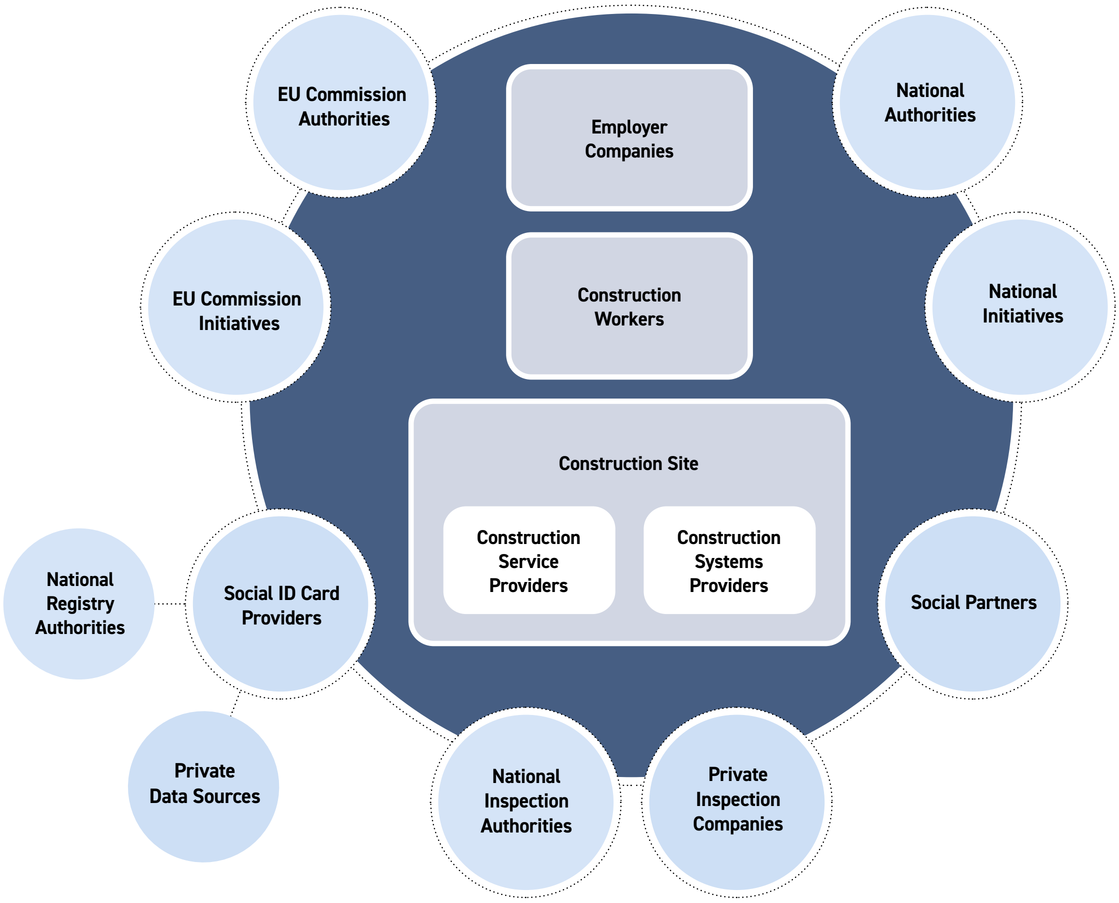
Social Partners – Employers organisation

- The possibility to ensure member organisations with the accessibility to workforce from other EU and 3rd countries without the risk of breaking regulations and local rules.
- The possibility to reduce the bureaucracy involved in the whole life cycle of acquiring workers from other EU and 3rd countries.
- Minimizing risks related to workforce from other EU and 3rd countries and ability to prove compliance to their buyers.
- Enabling sustainability and compliance with ESG Social responsibility by ensuring that the wellbeing of workers in the construction delivery chain is ensured (ESRS: S2).

EU authorities and services

- Wider deployment of initiatives and related tools and systems.
- Example of successful data driven co-operation in accord with the European Union fair data economy principles and the European Data act.

Graphic 3 SIDE-CIC Stakeholders


EU Commission Authorities
Employer Companies
National Authorities
EU Commission Initiatives
Construction Workers
National Initiatives
Construction Site
Construction Service Providers
Construction Systems Providers
National Registry Authorities
Social ID Card Providers
Social Partners
Private Data Sources
National Inspection Authorities
Private Inspection Companies

- Ensuring of the needed workforce for EU wide construction needs but with respect to worker's rights and minimising bureaucracy.

National authorities

- Better compliance with EU and local regulations when all parties can share relevant and timely information.

- Better inspection tools to combat fraud, grey economy and social dumping by enabling inspectors with best possible data combined from both authority and Social ID Card services.

- Possibilities to use Data Mining and AI anomaly detection to better focus the inspection activities.

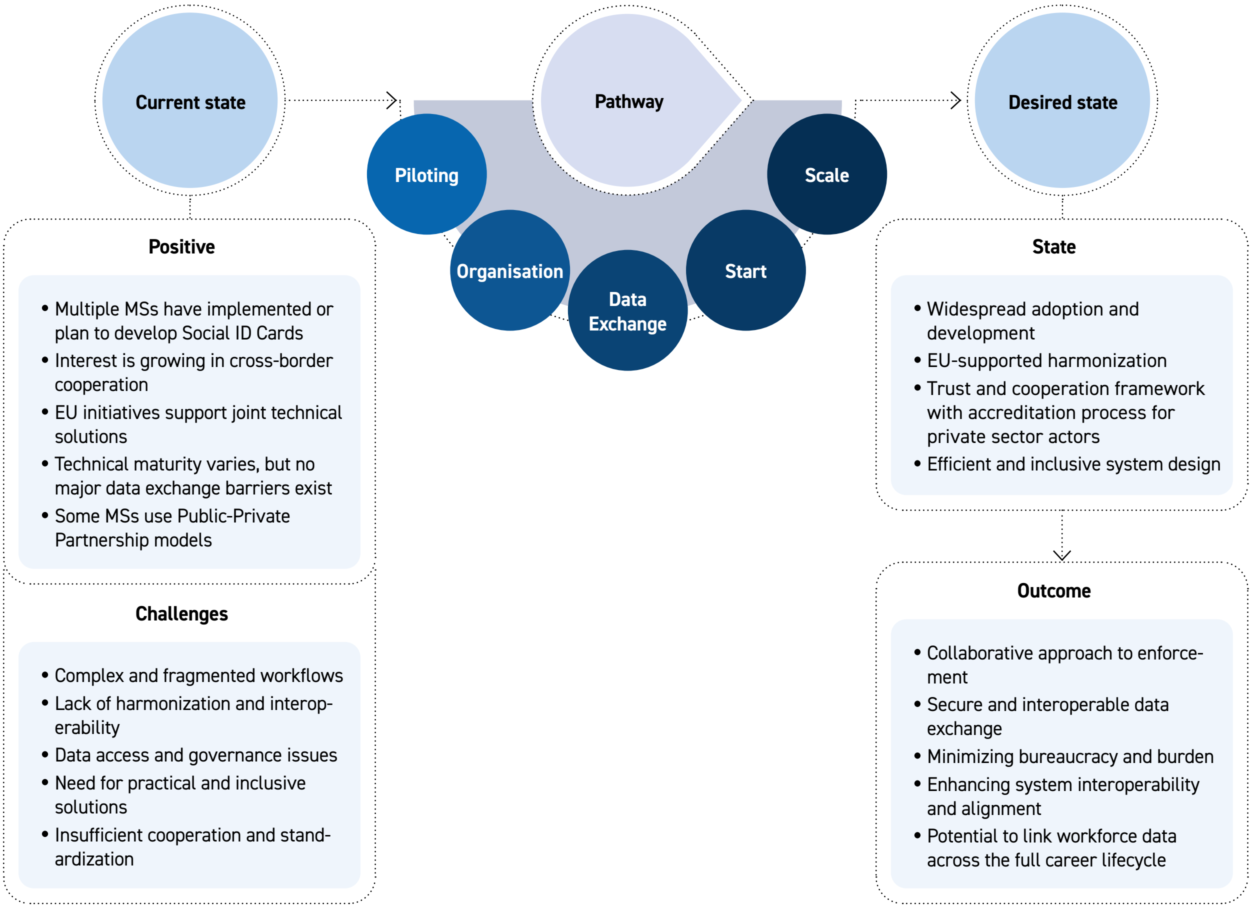
In our opinion, there is no reason why authority-based and private or social partner-driven Social ID services could not exchange data, provided that the trust framework and related data profiles are accepted by both parties. Equally the data exchange could provide benefits for both Social Partners. Employer organisations would benefit from being able to provide a more level playing field for their members and Trade unions can use data to ensure that workers' rights are not abused. One concrete example that would serve both Social Partners is the integration of Collective Bargaining Agreements in the Social ID Data Profile. This works very well for example in Finland. A data driven approach could be added to current member services.

2.3 CURRENT VS. DESIRED STATE ANALYSIS

During the project the lack of a common goal and desired state for SIDE-CIC was highlighted many times. To provide a common ground as basis for analysis of the different outcome scenarios a Current state vs. Desired state analysis was conducted and evaluated in the workshop #3.

The following graphic summarises the outcome of this analysis (Graphic 4).

Graphic 4 Current state vs. Desired state analysis



Positive

- Multiple MSs have implemented or plan to develop Social ID Cards
- Interest is growing in cross-border cooperation
- EU initiatives support joint technical solutions
- Technical maturity varies, but no major data exchange barriers exist
- Some MSs use Public-Private Partnership models

Challenges

- Complex and fragmented workflows
- Lack of harmonization and interoperability
- Data access and governance issues
- Need for practical and inclusive solutions
- Insufficient cooperation and standardization

State

- Widespread adoption and development
- EU-supported harmonization
- Trust and cooperation framework with accreditation process for private sector actors
- Efficient and inclusive system design

Outcome

- Collaborative approach to enforcement
- Secure and interoperable data exchange
- Minimizing bureaucracy and burden
- Enhancing system interoperability and alignment
- Potential to link workforce data across the full career lifecycle

A Current state vs. Desired state analysis typically evaluates the differences between the end goal and the current situation and the steps that are needed to bridge the gap.

In the workshop #3 this analysis was conducted with the participants. The comments regarding the positive aspects of the current state were:

"Social ID Cards are viewed positively by EU authorities, particularly for their role in enhancing service provision across borders through interoperable systems, in line with Article 56 TFEU. The diversity of existing schemes is considered valuable for identifying effective practices. Additionally, regulatory frameworks support their use in improving labour monitoring, safety enforcement, company verification and legal compliance."

2.3.1 Long-term goals

The Desired State points can be summarised as follows. The envisioned future centers on the widespread adoption of Social ID Cards and continuous development of an efficient, inclusive system for managing workforce-related data across the EU. This future is supported by a harmonized Data Space framework, backed by EU institutions, enabling consistency and mutual recognition across Member States. A key pillar of this vision is the establishment of a trusted and cooperative environment, underpinned by a formal accreditation process that facilitates the involvement of private sector actors in a transparent and secure manner.

Realizing this desired state results in a collaborative approach to enforcement and governance, where all stakeholders actively contribute to maintaining system integrity. Secure and interoperable data exchange becomes the norm, significantly reducing administrative burdens and minimizing bureaucracy. This streamlining not only enhances operational efficiency but also ensures broader accessibility and fairness within the system. Ultimately, the outcome is a fully interoperable and aligned infrastructure that holds the potential to link workforce data across the entire career lifecycle—from education and onboarding to retirement—providing long-term value for individuals, institutions, and governments alike.

2.3.2 Summary of Challenges Related to Social ID Cards

Here is a structured summary of the key challenges identified in relation to Social ID Cards:

1. Fragmentation of Responsibilities and Workflows

a. Multiple authorities are involved in the lifecycle of Social ID Cards—declaration, issuance and control—often across different national and EU levels.
b. The absence of a unified reconciliation mechanism makes it difficult to assess the system's effectiveness in tackling social fraud and illegal work.

2. Lack of Harmonisation across Member States

a. Different technologies, databases, issuing authorities and data types are used across schemes, creating complexity.
b. There is no standardisation in data collection, storage or access protocols, which leads to inefficiencies and legal uncertainty.

3. Interoperability and Autonomy Tensions

a. While interoperability is essential, it must respect each Member State's autonomy in designing and managing their schemes—both technically and politically.

4. Inspection and Enforcement Challenges

a. Labour inspectors face difficulties due to varying technologies and standards, requiring tailored training and tools.
b. Fraud is often transnational, making enforcement and inspections more complex without coordinated or connected systems.
c. There is a need for real-time data verification to effectively enforce regulations.

5. Data Governance and Privacy Concerns

a. Clear rules are needed on who stores the data and under what legal mandates it can be accessed.
b. Ensuring workers' consent in data exchange is crucial, particularly under privacy regulations.

6. Institutional and Stakeholder Coordination

a. Differences in mandates between public authorities, social partners and contractual bodies hinder seamless data sharing.
b. Social partners need access to relevant data to fulfil enforcement roles where applicable.

7. Usability and Administrative Burden

a. The system must remain simple and practical, particularly for SMEs and end users.
b. Without a harmonised approach, the risk of parallel systems may increase bureaucratic obligations for stakeholders.

8. Infrastructure Gaps

a. National registration systems differ significantly, and data is often held by different actors, complicating interconnection.
b. Technical differences can be bridged through "connectors," but these add another layer of complexity.

It is worth noticing that the Social ID Card services in the Member States have been developed to serve the local market and to meet the local requirements. Therefore, there is also a long-term need to enabling harmonisation of technical features and data handling as well as exchange capabilities. The benefits of a Data Ecosystem with common services are that many of these differences can be tackled without major changes to the local systems. This is very important as it is directly related to the political will of the potential Member State Social ID Card services that consider joining a joint ecosystem.

Equally, it is important to recognise how the national solutions and their autonomy is respected in the right way. This is why the idea of voluntary Data Profiles is described in chapter 5.

2.4 ALIGNMENT WITH EU POLICIES AND INITIATIVES

It is important to review EU initiatives in this context for two reasons. Firstly, the aim is not to create parallel solutions to EU initiatives but rather to complement them. Secondly, by using EU initiatives integrated into the SIDE-CIC based solution we can potentially get a basis for EU wide adoption and ready solutions will be possible to help deploy critical capabilities or provide critical data.

2.4.1 EU Data Act

The Data Act aims to maximise the value of data in the economy by ensuring that a wider range of stakeholders gain control over their data and that more data is available for innovative use, while preserving incentives to invest in data generation.

The Data Act complements the Data Governance Regulation proposed in November 2020, the first deliverable under the European strategy for data.

The Data Act provides the platform for creating data driven solutions and supports and funds the concrete work with Data Spaces and Ecosystems.

2.4.2 ESSPASS

The European Social Security Passport ESSPASS is defined as follows (Sascha Garben, 2023, EMPL Study[2]):

1. A 'digital wallet' used by mobile individuals to store social security credentials issued by trusted authorities and verifiable online across borders;

2. Mobile individuals are in control of their own personal data;

3. More efficient cross-border verification and reduction of fraud.

The availability of a European solution for digital social security credentials and in a later phase the European Health Insurance Card (EHIC) would provide a platform for verifying first and foremost posted workers. This could be done at a later stage.

For the second workshop a demonstration including ESSPASS was presented. The idea is that ESSPASS makes it possible to exchange the PDA1 document between the different Social ID Card services and make it possible for the posted country inspectors to verify that the document is not compromised and that the posting is still valid or not revoked.

Graphic 5 illustrates how the basic process i. e. without Social ID Cards would work between two countries. The principle is that the holder is in control of the information called a credential and thus can give consent to who can access the information. This applies to both authority-based inspectors and privately driven organisations like Social ID Card services or inspectors (Graphic 5).

In the centre of the concept is that the solution would be based on using the EUDI Digital Wallets as the vehicle to display and control the information. This also opens the possibility to use the Wallet for displaying the information in the Social ID Card and thus enabling a full Social ID Card profile for multiple countries.

In the demo it was shown how connecting the ESSPASS solution with technical interfaces (APIs) the Lithuanian workers could provide the PDA1 information to Finland as part of the Social ID profile in the posted country. As the PDA1 is currently one of the biggest challenges for the Social ID Card service providers, the integration with ESSPASS could solve this in a very practical and easy way. The only constraint identified is the possible delay in deploying Digital Wallets in member states.

2.4.3 eIDAS regulation and DC4EU

The objectives of the eIDAS[3] regulation are:

- Simplifying cross-border transactions by focusing on a smoother user experience.

- Enabling a unified system for reliable digital IDs.

- Enhancing security and reliability of electronic transactions.

- Providing a legal framework for electronic signatures and identification.

The Level of Assurance descriptions used in chapter 5 provides a framework to evaluate the level of trust in the data profiles provided by the Member State's Social ID Card services. The regulation is a key component to bring trust and confidence in digital processes and identities used in them.

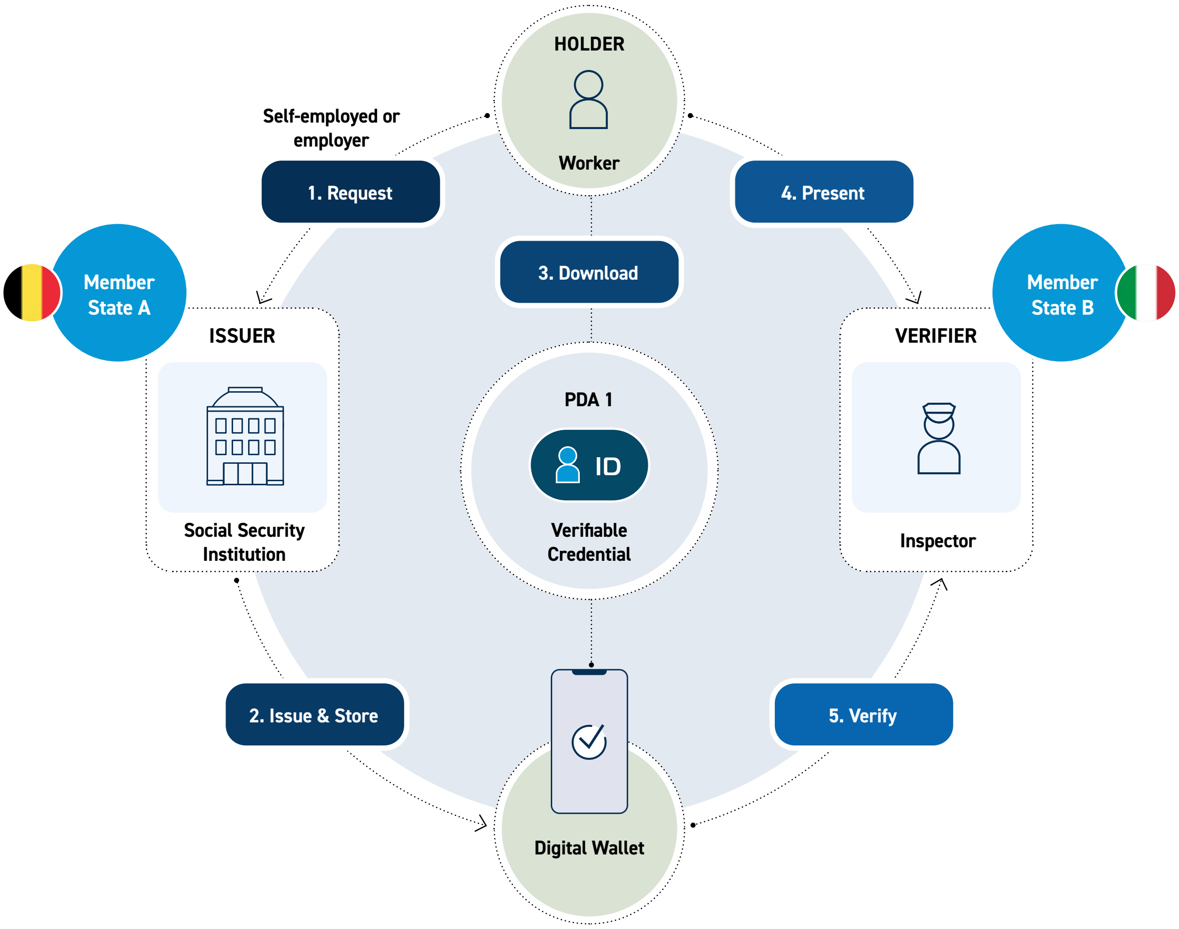
Digital Credentials for Europe (DC4EU)[4] provides tangible support to the public and private sectors in the educational and social security domains by deploying

[2] The study is available at: https://www.europarl.europa.eu/thinktank/en/document/IPOL_STU(2023)754194

[3] eIDAS or "Electronic Identification, Authentication and Trust Services". It's an EU regulation that aims to create a single digital market by establishing a framework for electronic identification, authentication and trust services across the EU.

[4] DC4EU, or "Digital Credentials for Europe", is a project that aims to enhance the interoperability and scalability of digital educational credentials and social security documents within the European Union.

Graphic 5 ESSPASS stakeholders and process



Source: European Commission

and accessing state-of-the-art trans-European interoperable digital service infrastructures and their integration in a cross-border trust framework.

If Social ID Card systems could be accredited as members of Member States' eIDAS nodes and use DC4EU created Digital Wallets, the cross-border data exchange would be significantly supported. The use of Digital Wallets is a pre-requisite for ESSPASS and many other solutions like Digital Passport Credentials to be deployed.

2.4.4 IMI

The Internal Market Information System (IMI) digitally connects national, regional and local authorities across the EU (EEA) by allowing them to quickly and easily communicate with their counterparts abroad. In some cases, it also allows companies to submit information to the national authorities via a portal powered by IMI. This cooperation and swift exchange of information are essential for people and businesses to benefit from their Single Market rights.

If Social ID Card systems could be accredited as data providers and receivers of IMI it would be possible to access data from local registries of countries that are exporting a lot of workforce but lack a Social ID card. One example of this is Italy needing better information about workforce from the neighbouring countries.

2.4.5 BRIS

The Business Registers Interconnection System (BRIS) is an infrastructure that enables the cooperation and interoperability of Business Registers across Europe. The service allows users to search for information on companies registered in EU and European Economic Area (EEA) countries and enables the connected registers to share information on foreign branches and cross-border mergers of companies. The company search functionality is available through the e-Justice Portal.

BRIS would provide a platform for checking the employers background information from other EU countries and thus be integrated into the SIDE-CIC system to provide better Company Screening Profiles (CSDs).

2.4.6 EESSI

The Electronic Exchange of Social Security Information (EESSI) DSI is a central platform to which national social security institutions connect to exchange information between each other. The exchanged information covers all 8 branches of social security coordination, which are sickness benefits, accidents at work and occupational disease benefits, family benefits, old-age pensions, pre-retirement and invalidity benefits, unemployment benefits. The institutions use the system to route structured electronic documents to their counterparties following agreed business processes (also known as "Business Use Cases").

The inability to co-operate with National Social Security Institutions has been a major challenge for all Social ID Cards. Only the Estonian solution which is authority issued can access this information. The exchange of PDA1 is most probably best deployed via ESSPASS, since the system is enabling the worker and employer to decide where the data is distributed with consent that is revokable later.

2.5 USE CASES & SCENARIOS

The use case drivers identified for Social ID Card ecosystem are highlighted in the graphic below.

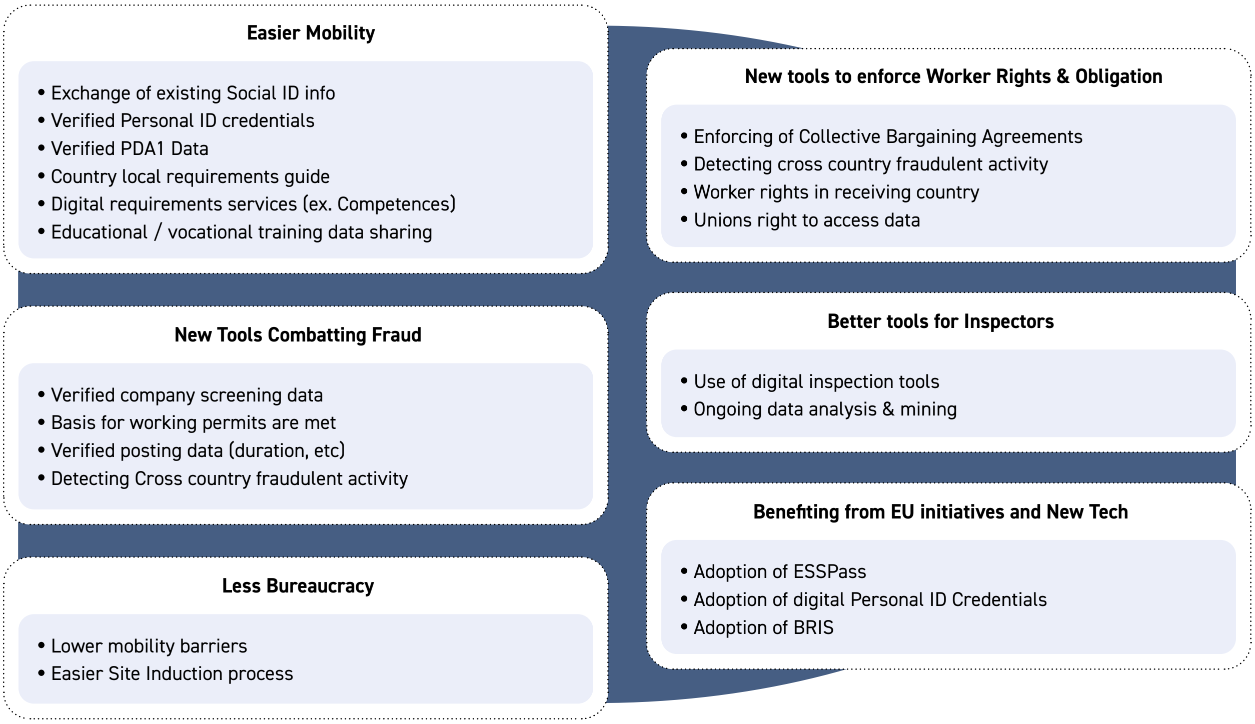
Based on the drivers we have outlined some combined use cases below.

2.5.1 Use case 1: Easier mobility and less bureaucracy

- less bureaucracy and lower costs of mobility
- faster end-2-end process with digital services
- local guides for cross-country workers
- data integrated solutions provide value for local employing construction companies when data is integrated to operative systems
- possibilities to continuously access updated sending country data from local authorities
- possibility to co-operate on how to gain access to 3rd country verified data.

This use case is a big driver for Data Exchange since it is a big challenge and hurdle for many employer companies and main contractors alike. The Proof-of-Concept demonstration between Finland and Lithuania highlighted this as currently the complexity of Finnish and Swedish regulations force Lithuanians to use external consultants to comply.

Graphic 6 Drivers and use cases



Easier Mobility

- Exchange of existing Social ID info
- Verified Personal ID credentials
- Verified PDA1 Data
- Country local requirements guide
- Digital requirements services (ex. Competences)
- Educational / vocational training data sharing

New Tools Combatting Fraud

- Verified company screening data
- Basis for working permits are met
- Verified posting data (duration, etc)
- Detecting Cross country fraudulent activity

Less Bureaucracy

- Lower mobility barriers
- Easier Site Induction process

New tools to enforce Worker Rights & Obligation

- Enforcing of Collective Bargaining Agreements
- Detecting cross country fraudulent activity
- Worker rights in receiving country
- Unions right to access data

Better tools for Inspectors

- Use of digital inspection tools
- Ongoing data analysis & mining

Benefiting from EU initiatives and New Tech

- Adoption of ESSPass
- Adoption of digital Personal ID Credentials
- Adoption of BRIS

The essence of this use case is that processes for all stakeholders could be automated and digitalised gradually. Naturally all construction companies and their workers would reap the biggest benefits.

2.5.2 Use case 2: New tools combatting fraud and better tools for inspectors

As described in Graphic 6, this use case is important since it would provide all stakeholders better tools to combat fraud, social dumping and other major social security and compliance challenges in the construction sector. This includes the following points:

- Authorities gain access to data enabling more effective targeting and execution of inspections.
- Enabling cross-authority data exchange.
- Enabling private service provider inspections.

The challenge today, is that each stakeholder has only part of the information. If all stakeholders would have access to the same Data Space, innovative solutions like data mining and anomality analysis supported by AI/Machine Learning could be deployed. Thus, authorities could target their inspections more effectively and private actors could automatically verify compliance as part of their normal processes like for example purchasing and induction routines.

For inspectors both authority and privately driven this would provide possibilities for digitalising inspections. In practice the targeting, preparation, execution and reporting could be data driven and digitalised. Thus, the value per inspector would drastically increase. In some Nordic countries discussions regarding co-operation has been discussed since Social ID Cards have been assisting authorities in investigations.

2.5.3 Use case 3: Improved workers' rights

- Transparency regarding workers' social rights
- Easier to verify if social security and insurance is properly organised
- Possibility to guide workers regarding rights and obligations in target country

In practice this would mean that workers' rights would be visible in their digital profiles verified by their digital identities. This means that domestic and foreign additions to statutory rights like Collective bargaining Agreements would be part of the Social ID Profile. In addition, Insurances and other forms of social protecting could be tagged from the Employer company data profile. The employer relationships would be integrated to the data profile.

2.5.4 Use case 4: Benefitting from EU initiatives and new technology

A major issue today is that benefits from EU initiatives, systems and platforms are not implemented as a Private-Public-Partnership (PPP). This is understandable since deployment in Member States on national level is a big enough and complicated task. Our point with this use case is the deployment of EU initiatives to applicable industries like the construction sector could be paved by co-operation with Social ID Card services. Equally, the integration with EU initiatives would provide common and EU wide building blocks for Social Partner driven services.

2.6 SUMMARY OF BACKGROUND ANALYSIS

The fragmentation of the Construction Industry is a well-known fact. This applies also to the data and information related to Social Identities of workers in the industry and the companies employing them. The need for better holistic management of intra-EU mobility and third country national workers is increasing. The solution is based on better co-operation between all stakeholders. There are crisp use cases that demonstrate the benefits of this kind of co-operation and exchange of data. In the next chapters this will be examined closely.

3 Technical mapping study of current Social ID card schemes

3.1 TECHNICAL MAPPING STUDY

When looking at existing social ID cards in different countries, one might notice a lot of differences in what is the legal background, responsible entity, technologies used to implement the cards, processes for card issuance and card usage. Most implemented cards have some centralised database where information is stored, but some do not have it. And it would be nearly impossible or would take a lot of time if the EU would want to harmonise on the card technology and processes across different countries and markets. Social ID cards that are in use are deeply trenched in respective markets and usually have a lot of use cases attached to them, like opening work site gates, tracking work time, proving competences and training, OSH certifications. As experience in countries show evolving a card in one country is a project that can last years, as these cards are used by hundreds of thousands of people and it affects the whole ecosystem of 3rd party system vendors of hundreds of applications available on the market to support various use cases built over years. To coordinate such change in multiple countries would require years of discussions to come to single standard, enormous political will and years of implementation making the task unfeasible.

However, there is a lot of commonalities in different countries when we look at data used in social ID profiles. All of them follow the basic principle of identifying a person, a company and an employment relationship between the two. In many countries, card providers are verifying various data points (such as company name and number, official company officers, tax debt, etc.) during card issuance and some even monitor those parameters during card lifecycle. However, degrees of data reliability vary among countries as there are different regulations in place, different approaches are used to fight grey labour. And within a single country, there are differences in data reliability when it comes to local vs. other EU or 3rd countries companies with great struggles on verifying foreign company and foreign worker data. One of the most often cited problem was getting reliable posting information, as it is quite common, that private companies are tasked with verifying possession of PDA1 form from each worker coming from other EU country. In many countries verified digital PDA1 data is available via systems accessible by government actors only.

Findings on data attributes and data reliability from each country are collected in the table below. The table also helps to see compatibility and differences of social identity profiles from different countries. For example, let's consider a company from Lithuania (registered and having social ID cards from Lithuanian STATREG) willing to go to work in Finland. When comparing two columns, we can see that almost all data is already in STATREG at trust level required by Valtti or higher. Additional information that Lithuanian company needs to submit to Vastuu is company and employees' registration at Finnish tax inspection number (Tax IDs) and posting (PDA1) data.

When mapping data, reliability of data was analysed. As there are various means of data verification used in different countries, a grouping into 3 levels of data veracity assurance is proposed, as described in section 5.1.

3.2 TECHNICAL LANDSCAPE OF SOCIAL ID CARD SERVICES IN EUROPE

In stage 1 of the project i.e. the mapping stage interviews with countries both having an operational Social ID Card service and countries planning a service were conducted. In addition, expert interviews were conducted to gain perspective regarding solution alternatives and how to organise a co-operation of the planned Trust Network of Social ID Card service providers. Interviews with ELA and DG EMPL were also conducted to assess possibilities to use current and future EU initiatives.

A workshop was organised at the end of the technical mapping stage. The objectives with the workshop were the following:

- Verify the results of the mapping phase
- Test and get feedback on initial concepts presented
- Present the next steps and get confirmation on how to proceed

The summary of stage 1, confirmed in the workshop, is that there are both benefits and possibilities to create a European wide Trust Network of Social ID card services that would enable the exchange data between the country nodes in a trustworthy way. It was also confirmed that EU ESSPASS and EUDI Wallet initiatives (DC4EU) can be used to gain access to valuable information like PDA1 in the context of posting and Digital Personal ID credentials with the individuals being in control of the data sharing.

Mapping phase showed there is a lot of commonalities in different countries when we look at data in social ID profiles. All of them follow the basic principle of identifying a person, a company and an employment relationship of the two. Card providers are also making efforts to ensure data is valid in the cards issued.

Table 1 Technical mapping of Social ID Cards

	Austria BauID	**Belgium** ConstruBadge	**Estonia** UWC
Local person data			
Person name	L1	L2	L2
Gender			
Date of birth			L2
Place of birth			
National identity number	L1	L2	L2
Nationality			
Home state / Country of Tax residency			
Photo	L1	L2	L0
Health insurance status	L2		
TaxID (person registration with Tax authority)			
Registration in construction workers state registry			
Status (posted, temp agency, etc.)			
Employment type: Paid Employer / Independent Contractor / Unpaid Worker			
Is Employment status declared to state before employment and is verified by card provider?		L2 at card issue, but no card revocation afterwards	L2
Competences			
Person consent is collected during card issuance?	No	No	No
Employment duration is consistent with card validity?		No. Card is valid until end of year	L2
Person from other EU country, working for non-domestic company			
Posting data or A1 for workers from other EU country	L2		L2 (in rare cases, manual addition of person's details)
Registration of worker from other EU or 3rd country with the state (if required)	L2?	L2	L2

	Finland Valtti	France Carte BTP	Lithuania STATREG	Norway HMS	Sweden ID06
	L2	L0	L2	L2	L2
		L0	L2	L2	L2
	L2	L0	L2	L2	L2
		L0			
	L2	L0	L2	L2	L2
	L1	L0			L2?
	L0	L0	L2	L0	L0
	L2				
			L2		
		L1			
			L2	L2	
			L2 At least 1 competence is mandatory		Optional
	Yes	No (legal obligation)	Yes	No?	Yes
	L0 (card can be terminated by both parties when employment ended)	L1	L2 (verified nightly against SODRA, cards terminated automatically)	L2 NAV Aa and OAR checked	L0 (card can be terminated by both parties when employment ended)
	L0	L2 Posting data: dates, client name and client's registration ID		L2?	L0?
	L2 (Tax ID)			L2 Dnummer	

	Austria BauID	**Belgium** ConstruBadge	**Estonia** UWC
3rd country national			
Residence / work permit for 3rd country nationals	L2		L2
Local employer company			
Company name	L2	L2	L2
Company registration number	L2	L2	L2
Company VAT number			
Company full mail address (including country)	L2	L2	L2
Company registration as employer			
Company tax debts	L2		L2
(some other company information ...)	Fraudulent company list, etc.		Any state data can be accessed via X-road
Additional data for company from EU count.			
Registration with destination Tax inspection			
Additional data for company from 3rd count.			
Unspecified			
Card			
Card validity dates	L2?	L1	L2
Card number	L2	L2	L2

Furthermore, it was discovered that challenges regarding interoperability can be solved technically with various mapping models. The main question is whether a centralised or de-centralised data exchange model should be used.

The organisation of the Trust Network and how governance is performed remains an important question.

To our understanding, all the interviewed Social ID Card service providers were positive both towards a Proof of Concept (PoC) and participating in a potential Pilot phase given that a mandate would be granted and other potential individual conditions are met.

To verify the feasibility of the Trust Network and how to organise the interoperability it is proposed by the technical team that a PoC should be conducted. The objective would be to make an end-to-end demonstration on how the process could work. The PoC would provide a great test ground for different ideas and work as a pre-stage to a potential Pilot project following this project.

3.3 GAP ANALYSIS

Based on the general mapping study and the technical mapping study there are differences between the Member States Social ID card solutions. One of the major differences is the mandate of the Social ID Card:

- Statutory defined
- Compliant with legislation but privately driven
- Voluntary

Equally, the issuer can be an authority, a social partner owned company or a private company. Table 2 groups the current landscape of Social ID Card schemes based on these distinctions.

	Finland Valtti	France Carte BTP	Lithuania STATREG	Norway HMS	Sweden ID06
	L0	L0 (optional)		L2	L2 at issuance
	L2	L1	L2	L2	L2
	L2	L1	L2	L2	L2
			L2	L2	
	L2	L1	L2	L2	L2
					L2 (F skatt nummer)
			L2		L2?
		L1 (address, contact details), operating sites)	Up to 60 parameters from various state and private sources		
	L2 Tax ID				
	L2	L1	L2	L2	L2
	L2	L2	L2	L2	L2

Table 2 Social ID Card comparisons

Category	Issuer Authority	Issuer Social Partner	Issuer Private
Statutory Card is Law based	HMS Card Norway, Estonian Card	Constructiv Belgium, CBT Card France	
Compliance Card is compliant with legal framework		Valtti Vastuu Group, ID06 Sweden, BAU-ID Austria, CIBE Italia, Latvia	
Voluntary Card is based in industry needs		Statreg Lithuania	ISHAP Austria

Table 3 Social ID Card comparisons

	Austria BauID	**Belgium** ConstruBadge	**Estonia** UWC	**Finland** Valtti	**France** Carte BTP
Legal Basis	Law	Collective agreement	Law	Law	Law
Participation	Voluntary	Voluntary	Compulsory	Compulsory	Compulsory
Issuance	Centralised	Centralised	Centralised	Decentralised	Centralised
Issuing body	Paritarian	Paritarian	Gov	Employer / other	Employer association
Main objectives					
Combat undeclared work	Yes			Yes	Yes
Identify worker and employee	Yes	Yes		Yes	Yes
Verify site access			Yes	Yes	In practice yes, but not as a goal
Training and work experience	Yes				
OSH training compliance					
Work time tracking			Yes	Yes	Yes
Data access					
Visual data access	Yes	Yes	Yes	Yes	Yes
QR/bar code at the control of the worker	Yes				Yes
Central DB	Yes	Yes	Yes	Yes	Yes

The differences can also be analysed by the objectives of the Social ID Card and the access to data as described in the table above (Table 3).

Based on the general and technical mapping studies the technical team has conducted the feasibility study to evaluate the possibilities and potential solutions to create interconnectivity and interoperability between the existing Social ID Card schemes and those in planning phase.

3.4 ALTERNATIVES AND CHOSEN WORKING HYPOTHESIS FOR FEASIBILITY ANALYSIS

The working hypothesis for the feasibility is that despite the differences between the Social ID Card schemes there is a clear possibility to create a network of interconnected and interoperable nodes that exchange data in a trustworthy way with proper governance. Based on the mapping study we cannot find a technical or legal obstacle that cannot be solved given enough will by the parties founding the network.

It is however very important to select an organisational model based on which the network can be created. This is crucial since choosing the right model will create the trust factors in the network, will alleviate the existing differences and enable the possibilities to both create and operate the service needed to enable the technical capabilities needed.

The potential scope and framework alternatives are summarized in the table on the right (Table 4).

	Lithuania STATREG	Norway HMS	Sweden ID06	Denmark	Iceland	Italy	Netherlands	Romania
	Voluntary	Law	Law	Municipal solution in CPH	Law & Collective agreement	Collective agreement	Collective agreement	
	Voluntary	Compulsory	Compulsory		Compulsory	Compulsory		
	Centralised	Centralised	Centralised		Decentralised	Centralised		
	Employer association	Gov	Employer association		Employer	Paritarian		
	Yes		Yes		Yes		Yes	
			Yes	Yes		Yes		
			Yes			Yes		
	Yes	Yes	Yes			Yes		
	Yes		Yes			Yes		
	Yes		Yes	Yes				
	Yes	Yes	Yes	Yes	Yes	Yes		
	Yes	Yes	Yes					
	Yes	Yes	Yes					

Table 4 Alternatives for Scope and framework

Area	Alternative	Description	Feasibility	Impact	Score	Assessment
Scope	EU	EU wide geographical	2	5	7	**The desired outcome since it would add value and impact for many workers and companies**
	Areas (Nordics)	Areal or regional	3	3	6	Easier to accomplish than EU wide but adding only marginal impact and scalability
	Bilateral	Bilateral countries	4	2	6	Simple solution but not easily scalable
Framework	Data Space	Political, legal, economic or other reason	3	4	7	**Use of proven multistakeholder and country framework would improve feasibility and add impact**
	Bilateral /Regional agreements	Some members do not get mandate to join due to legal, economical or other reason	4	1	5	Not desirable since it only adds value to small part and is not copyable to other countries

Based on the scope and framework alternatives analysis, the combined alternatives for organising the network are the following:

1. Bilateral agreements
2. Regional ecosystem
3. EU organised network and solution
4. EU supported Data Ecosystem and Data Space-model

3.4.1 Bilateral agreements

A bilateral agreement model meaning that two countries benefiting from data exchange would make a data exchange agreement. If many Member States make agreements, a sort of network could emerge. This model however is not scalable and does not provide enough benefits for the stakeholders involved. It is also the most expensive model, in relative sense, since all solutions are point-to-point and therefore not re-usable. This alternative is also the least beneficial for the end users i. e. workers and construction companies since there is no underlying standard.

3.4.2 Regional model

A regional model is an alternative to the bilateral model that could provide some form of joint solutions and standards as well as joint governance. The challenge is however, like in the bilateral model, that it only solves part of the problem in a specific region and does not provide a scalable model that can be applied by all stakeholders and parties needed. It would create regional models that are not interoperable and thus create an opposite direction than intended.

3.4.3 EU organised network and centralised solution

An EU organised model supported by a centralised technical solution is not feasible since the Social ID Cards have so many local requirements that need to be considered. Also, a sector specific solution with local differences is not the responsibility of EU level. It would not be feasible from a timewise and political standpoint.

3.4.4 EU supported Data Ecosystem and Data Space-model

Based on all evaluations and expert recommendations the creation of a Data Space resulting in a Data Ecosystem would be the best solution. **A data space is an infrastructure that enables data transactions between different data ecosystem parties based on the governance framework of that data space. A data space should be generic enough to support the implementation of multiple use cases.**

The reason for this is that it is a model that can be supported and funded by the EU Commission in creating a fair data economy which is one of the key aspects in sustaining a competitive European Union. There are several alternatives and frameworks for organising Data Spaces and Ecosystems. Gaia-X[5] is one of them and is a framework supported by the EU Commission. It provides a framework with support functions for creating a technical, agreement and governance models that supports the creation of network of parties that wants to exchange data to the benefit of the members. Alternative frameworks are International Data Space Association, IDSA (https://internationaldataspaces.org/) or iShare (https://ishare.eu/home/ecosystem/ishare-in-data-spaces/). The technical experts would recommend selecting Gaia-x as it is specifically intended for cross country data exchange not based on a specific industry but on a general model suitable also for non-profitable organisations and initiatives.

Gaia-x also provides the best compliance with EU regulation (EU Data Act) and therefore a good platform for creating cross country data ecosystems. In summary, it would be the most legally, technically, financially and scalable solution. The different alternatives will be examined closer in chapter 7 and 10.

We have also found a benchmarkable ecosystem DS4SKILLS that corresponds to the objectives of SIDECIC. It will be examined closer in chapter 11.

3.5 SUMMARY OF THE MAPPING STAGE

The key learnings from the mapping stage are:

- The Member States Social ID Cards have big variation in terms of issuing party, mandate, objectives and technical deployment.

[5] Gaia-X is a European initiative to build a federated, secure cloud-and-data infrastructure that empowers users and organizations to retain full control over their data while fostering interoperability and digital sovereignty. For more information: https://gaia-x.eu/.

- However, there is clear common ground since the challenges are the same despite that the priorities might vary.

- The technical and data set differences can be managed over time and do not provide a major obstacle.

- The main challenge is to cater for a mandate for all current and future Social ID Cards to co-operate and exchange data.

Our conclusions from this stage are:

- Data is key not the Card.

- Member States' differences must be respected.

- Data profiles that are voluntary to use is the right way forward.

- Organisational framework is key to create trust.

We will elaborate on this in the next chapters in the feasibility analysis.

4 Technical Feasibility analysis

The Technical Feasibility Analysis chapter explores the trust factors, data exchange models and the alternative implementation models needed to enable the interoperability from a technical perspective. They are central components of how a SIDE-CIC data exchange model could work in practice.

4.1 TRUST FACTORS FOR INTEROPERABILITY

Interoperability between the different nodes in the Trust Network is fundamentally based on the Trust Factors that are important in the context of Social ID Cards. The technical team have identified three basic Trust Factors:

1. **Data:** The data comes from reliable sources like authority registries, and the data has not been tampered with. If data is self-declared it can be verified with external sources to verify validity. Data which is prone to change frequently is updated regularly, and the update process is verified.

2. **Technical:** Data in the system cannot be changed or tampered with, and all changes are logged. The identification and authentication methods are strong so that the person ordering and receiving the card can be verified. Ideally there is an ISO certification for the operation.

3. **Security:** The system is protected from external intrusion by relevant security measures. The security of the system has been audited by an external third party and the system has a security responsible.

For inspiration on trust factors one can look at eIDAS 2.0. One could think that social identity card providers operating in different countries could operate as Attribute Service Providers. One could also look at UK's Digital Identity and Attributes Trust Framework for examples of standards and governance related to attributes service providers.

The technical mapping provides an overview of the Trust Factors for each country Social ID service. The technical standard outlines the minimum level of trust factors that can be accepted by a Social ID Card service (see next chapter 4.2).

4.2 DATA EXCHANGE MODELS

The data exchange models that are needed to provide interoperability are:

- Data mapping
- Technical exchange mapping
- Requirements mapping

By using these models there is no need to strive for exactly the same models but rather to identify the differences that are to be covered in for example local data additions.

The different data exchange models are outlined below.

4.2.1 Data mapping

The data mapping means that the data profiles regarding individual data (Social ID Profile, SIP) or Company Data (Company Screening Data, CSD) are compared. The comparison between two systems can result in a deficit of for example 25%. This means that the sending country's profile contains 75% of the information that the receiving country requires. The deficit 25% is handled by local additions to complete the profile and print the card. It is important to consider required data assurance level in the receiving country when comparing profiles.

This model was highlighted with Lithuania and Finland as examples in the Miro Board serving as a basis for the workshop #1 (see section 3.1).

4.2.2 Technical exchange mapping

When the data is mapped, the next step is to assure that the technical exchange can function. This is done in the way that the two nodes do a mapping of the data models and how they are reflected in the API-description that provides the outgoing interface for data. In practice, the APIs are integrated, and the data models are harmonised so that despite different attribute level differences the same data can be interpreted in each system.

This can be compared to a "translator-service" between the systems. Once the technical mapping is done the network nodes need to exchange API-keys that allow the exchange of the data in a secure way and only concerning the data aimed for this purpose.

4.2.3 Requirements mapping

In addition to data and technical mapping, it is highly recommended that the network nodes do a requirement mapping. The objective is to map the requirements that a sending country company must abide by in the receiving country. By providing detailed instructions in local language to the companies the Social ID

Card service provides a reduction of bureaucratic burden for their customers doing cross-country work.

4.3 ALTERNATIVE IMPLEMENTATION MODEL

The actual implementation model has two distinct alternatives highlighted in the graphic below (Graphic 7).

The differences in the models are described below.

4.3.1 Centralised model

In the centralised model the harmonisation between the data models and the technical integration is done on the platform level once for each node. A universal machine-readable data model i.e. an ontology is then created. This means that interpretations of all data models are mapped and interpreted so that all systems are interoperable and can exchange data via the platform. The platform also assures that the data agreements between the nodes are followed and that quality assurance is met in the communication.

A centralised approach is easier to implement as it does not need point-to-point integration and harmonisation. The challenge is that in terms of organisation and governance it might be more difficult to achieve. It requires agreement on joint funding and administration including purchasing of necessary technical services from independent 3rd parties.

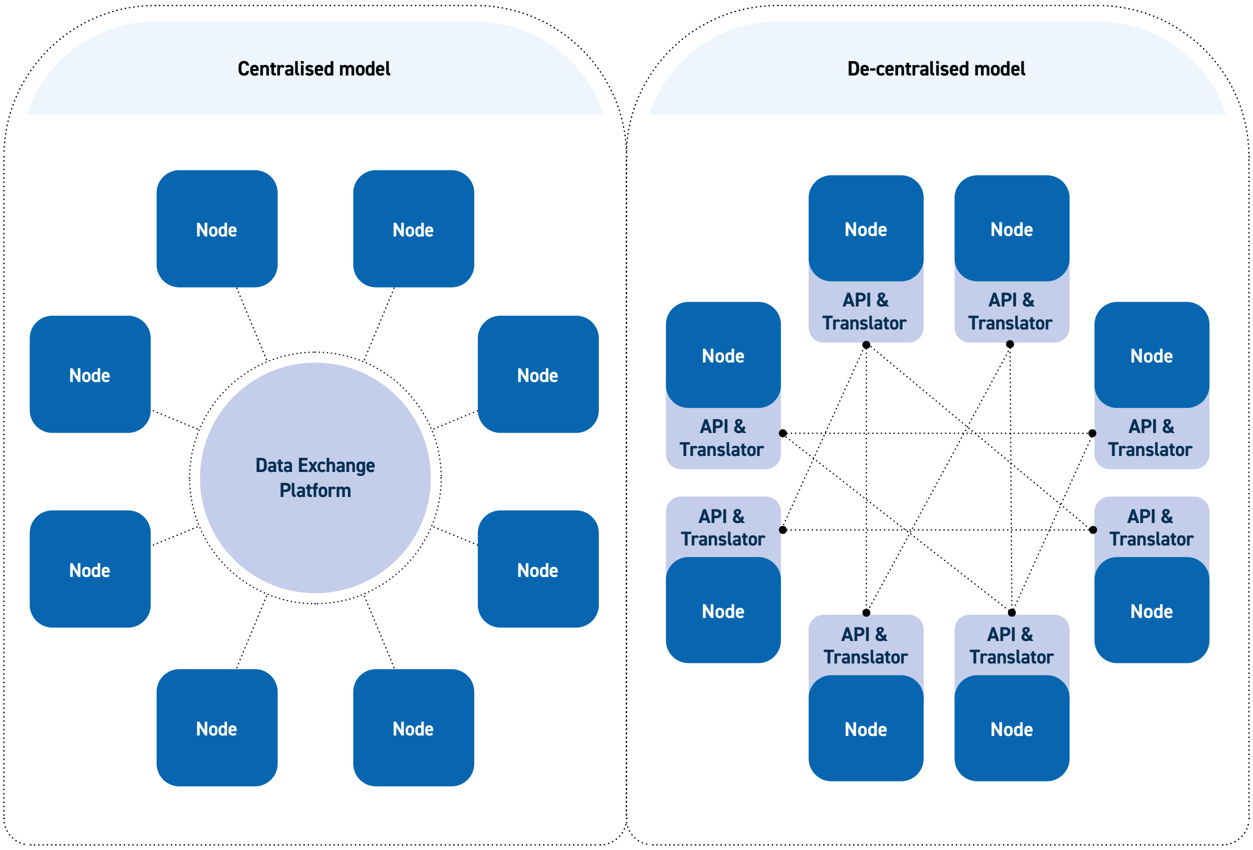
There are multiple solutions that would provide the foundation to create a centralised data platform:

- Commercial platform solutions like MS Azure[6] and Amazon AWS[7]. The MS Azure DataFactory solutions are used by many public authorities.

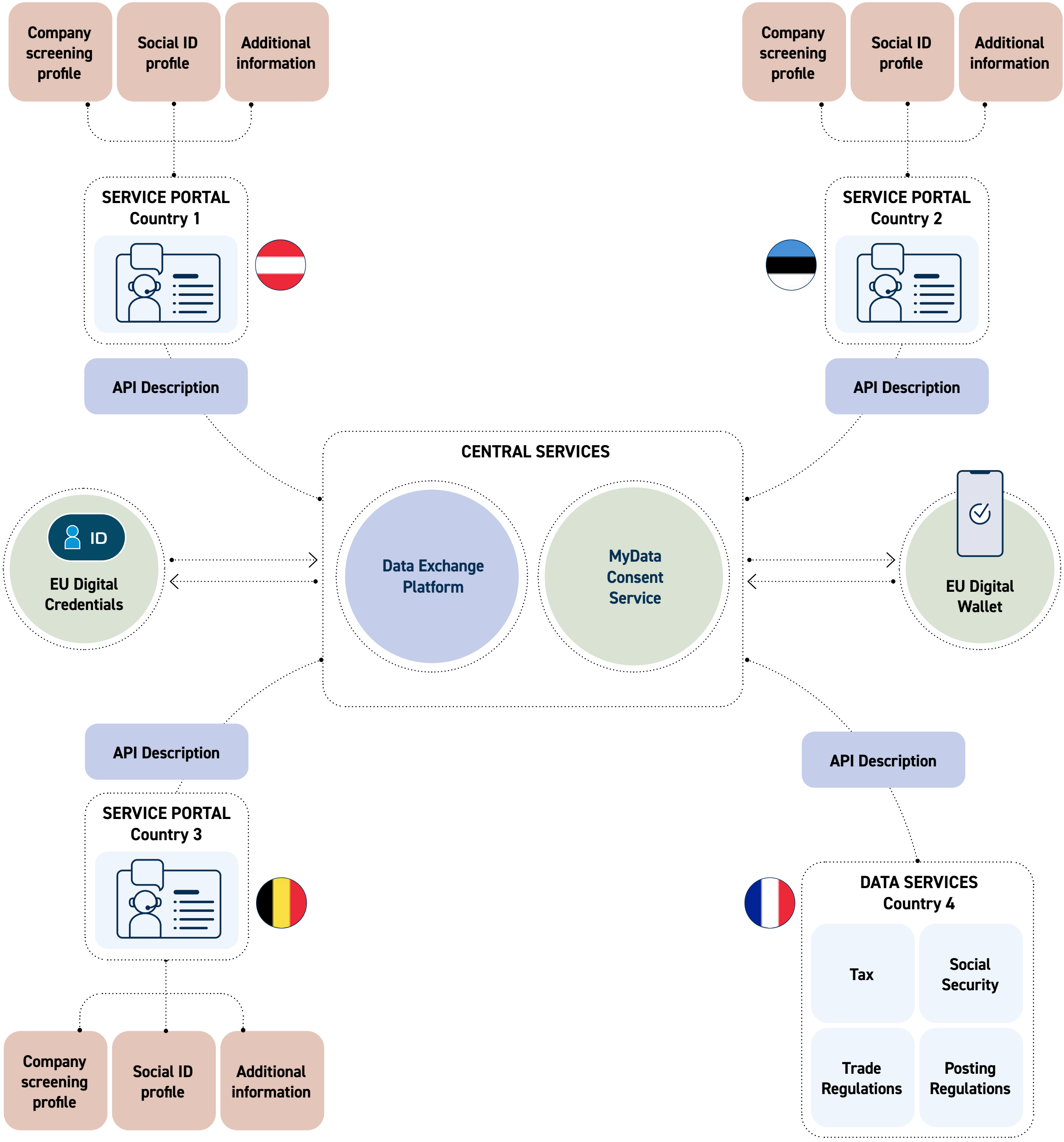
[6] Microsoft Azure is a comprehensive cloud computing platform offering infrastructure, platform, and software services for building, deploying, and managing applications through Microsoft-managed data centres (https://azure.microsoft.com/).

[7] Amazon Web Services (AWS) is a widely used cloud platform providing on-demand computing power, storage, and a broad set of tools to help organizations scale and innovate securely (https://aws.amazon.com/).

Graphic 7 Alternative implementation models



Graphic 8 Centralised Data interoperability model



- Specific construction industry platforms like the French Dawex[8] and the Finnish Platform of Trust[9] are examples of industry data exchange solutions

- EU funded solutions like FIWARE[10] is an example of an open-source platform that could be deployed

4.3.2 De-centralised model

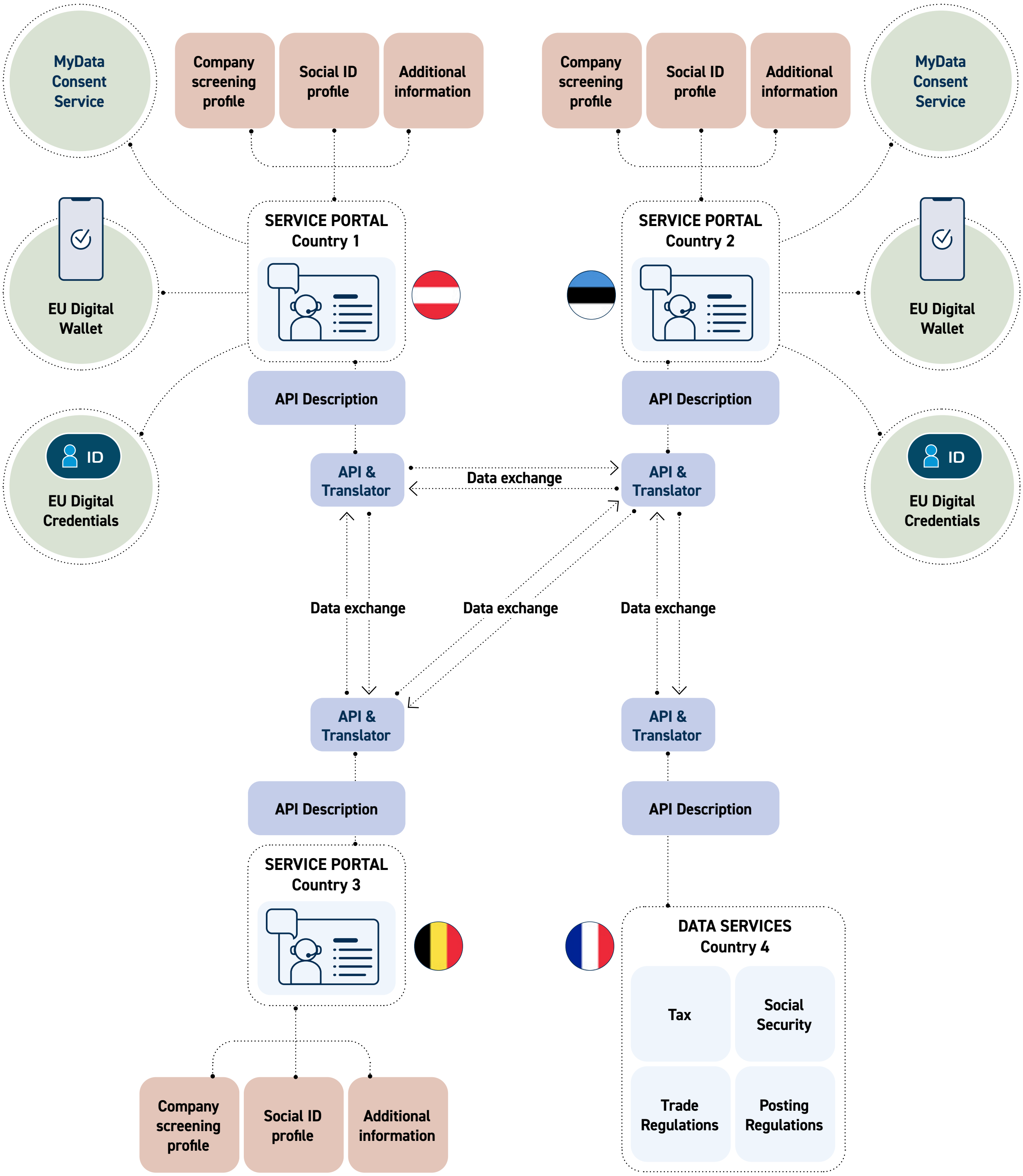
A de-centralised data exchange approach means that each node must be integrated and harmonised point-to-point. In practice this means that all nodes wishing to connect must do the mapping steps.

[8] Dawex is a French company offering a secure and compliant data exchange platform that enables organizations to publish, discover, license, and distribute data products across trusted ecosystems (https://www.dawex.com/).

[9] Platform of Trust is a Finnish data exchange platform focused on the built environment, enabling secure, interoperable, and authorized data flows between systems, applications, and stakeholders (https://www.platformoftrust.net)

[10] FIWARE is an open-source, EU-funded framework of modular software components and APIs (originally funded under the EC's Future Internet PublicPrivate Partnership 2011–2016) designed to accelerate interoperable and scalable smart solutions for domains like cities, industry, and water through context data management and standard data models (https://www.fiware.org).

Graphic 9 De-centralised Data interoperability model



Technically the harmonisation must be done in the API-integration (creating technical interface) so that the systems can interpret the data being exchanged. Fortunately, each node can publish a data model attribute table as part of the API-technical integration description. This helps the technical work and reduces the time of integration. A joint standard can be formed for this purpose. The benefit with the de-centralised model is that it requires much less common agreements and governance models than a centralised model. It also does not require joint funding. The challenges are that it takes longer and costs more to implement between the nodes and is more complicated to audit.

The current trend within Data Spaces is to deploy architectures that are using approved Connectors, credentials identification and consent management components that can be deployed with the many-to-many principle. This means, in practice that it is the responsibility of the members of the ecosystem to deploy the components provided in the way described in the technical standards. The benefit of this model is that it scales very well and does not require any action by the orchestrator of the Data Space.

In the EU there are numerous examples of approved Connectors. Here is a list of some connector solutions:

1. **Dataspace Connector (DSC)**
   Developed by Fraunhofer ISST, the DSC provides a modular and open-source entry point into IDS-compliant data spaces. It supports the enforcement of eight usage condition classes and has been tested for the Base certification level, facilitating cross-industry data exchange (https://international-data-spaces-association.github.io/DataspaceConnector/).

2. **FIWARE Data Space Connector (FDSC)**
   An open-source suite developed by the FIWARE Foundation, the FDSC integrates components for identity management, contract negotiation and data exchange. It aligns with DSBA Technical Convergence recommendations and supports protocols like NGSI-LD and the Dataspace Protocol (https://github.com/FIWARE/data-space-connector).

3. **Eclipse Dataspace Connector (EDC)**
   Part of the Eclipse Foundation's initiatives, the EDC offers secure and reliable access to data, ensuring data sovereignty through a decentralized architecture. It's utilized in projects like the Mobility Data Space and supports integration into various systems (https://mobility-dataspace.eu/data-catalogue).

4. **VTT Data Space Connector**
   Developed by VTT Technical Research Centre of Finland, this connector is the second globally to receive IDSA certification. It plays a significant role in advancing Europe's vision for a unified data market by facilitating secure data sharing (https://www.vttresearch.com/en/news-and-ideas/vtt-paving-way-data-sharing-2nd-certified-data-space-connector-world).

5. **OneNet Connector**
   Included in the IDSA Data Connector Report, the OneNet Connector is designed to support energy sector data exchange, aligning with IDS standards to ensure interoperability and data sovereignty (https://www.onenet-project.eu).

Some references on the subject include:

- **IDSA Data Connector Report:** For an extensive overview of existing data connector implementations, including their development status and usage, refer to the Data Connector Report (https://international-dataspaces.org/data-connector-report/).

- **Academic Survey:** For a detailed analysis of data-space connector architectures, data models and usage control mechanisms, consider reviewing the academic paper titled "A Survey of Dataspace Connector Implementations" (https://arxiv.org/pdf/2309.11282).

In chapters 5, 6 and 11 the subject of connectors will be elaborated further.

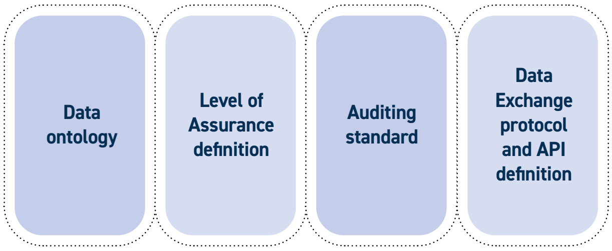
4.4 SUMMARY OF TECHNICAL FEASIBILITY STUDY

Creating functional data exchange between the Social ID Card systems is possible by creating processes and models to manage the Data Profiles each member provides. The main question is to choose which general model is deployed. The implications are both technical, legal, political and financial. Irrespective of the decision regarding the model there are some technical solutions and services that need to be deployed as general capabilities and tools for the members and orchestrator of a Data Ecosystem. The solutions and services will be described in the next chapter.

5 Technical Solutions and Services proposed

5.1 COMMON STANDARDS

Graphic 10 Common standards needed



Data ontology
Level of Assurance definition
Auditing standard
Data Exchange protocol and API definition

A set of common standards is required to facilitate data exchange among countries.

5.1.1 Data ontology

When looking at different Social ID profiles in different countries it is important to understand, when data points have the same meaning (semantic interoperability). For example, "Personnummer" (Swedish) and "Asmens kodas" (Lithuanian) means the same – personal identification number issued to a person by the state. To enable data mapping, data ontology could state, that personal identification number in any social ID profile could have Object Identifier (OID) reference 2.5.4.5. OID reference 2.5.4.4 could be used for surnames and OID reference 2.5.4.42 for persons first name and middle names. This way automatic data mapping between different profiles can be enabled, even when data items are named differently in different countries.

An ontology needs to cover all the data points that are going to be exchanged among countries. Object Identifier (OID) Repository (https://oidref.com) or X.501 recommendation could serve as a basis to unambiguously identify terms and ease automatic mapping.

5.1.2 Levels of assurance definitions

When mapping, reliability of data was analysed. As there are various means of data verification used in different countries, a grouping into 3 levels of data veracity assurance is proposed. These levels were inspired by eIDAS levels of assurance of identity[11]. Standards on Levels of assurance need to be defined for each class of data, for example what is L2 level when it comes to person nationality or company-employee relationship.

Each participating node would define its own profile of what data can be shared (with references to OIDs of each data attribute) and what level of assurance is achieved for each shared data attribute.

A country willing to receive data, would also define what data attributes are of interest (with references to OIDs) and what level of assurance is acceptable for each data attribute.

5.1.3 Auditing standard

Set of requirements each participant would need to comply with in technical and organisational security

[11] eIDAS term "level of assurance" refers to the degree of confidence in the claimed identity of a person – how certain a service provider can be that it is you the one using your eID to authenticate to the service, not someone else pretending to be you. In other terms, it refers to the difficulty one would have tried to use someone else's eID to access an online service.

Table 5 Level of Assurance descriptions

Level of assurance	Description
L2	• Data comes digitally from (national) registries in a secure way with high degree of assurance that data was not tampered with. • Data that is prone to changes (like person employment or company status) is verified and kept up to date by regular data verification process. • When data comes from a document (like passport), the document has counterfeit measures and there is traceability of who verified this information and when.
L1	• Data is self-declared, but there are some checks with external sources of data validity. • Data might have come from verified sources, but in case it is prone to changes (like person employment or company tax debt status) is NOT verified and kept up to date by regular data verification process.
L0	• Self-declared data.

measures. The auditing standard could be used by third parties when auditing data exchange participants. By successfully passing an audit a participant would show to others that it is safe to share data with and data that is received from such participant corresponds to the declared assurance levels.

5.1.4 Data Exchange protocol and API definition

Data exchange protocol is an agreement on common way of exchanging data: who initiates the exchange, what methods are called to perform actions and in what sequence.

One example of such sequence could be the one below.

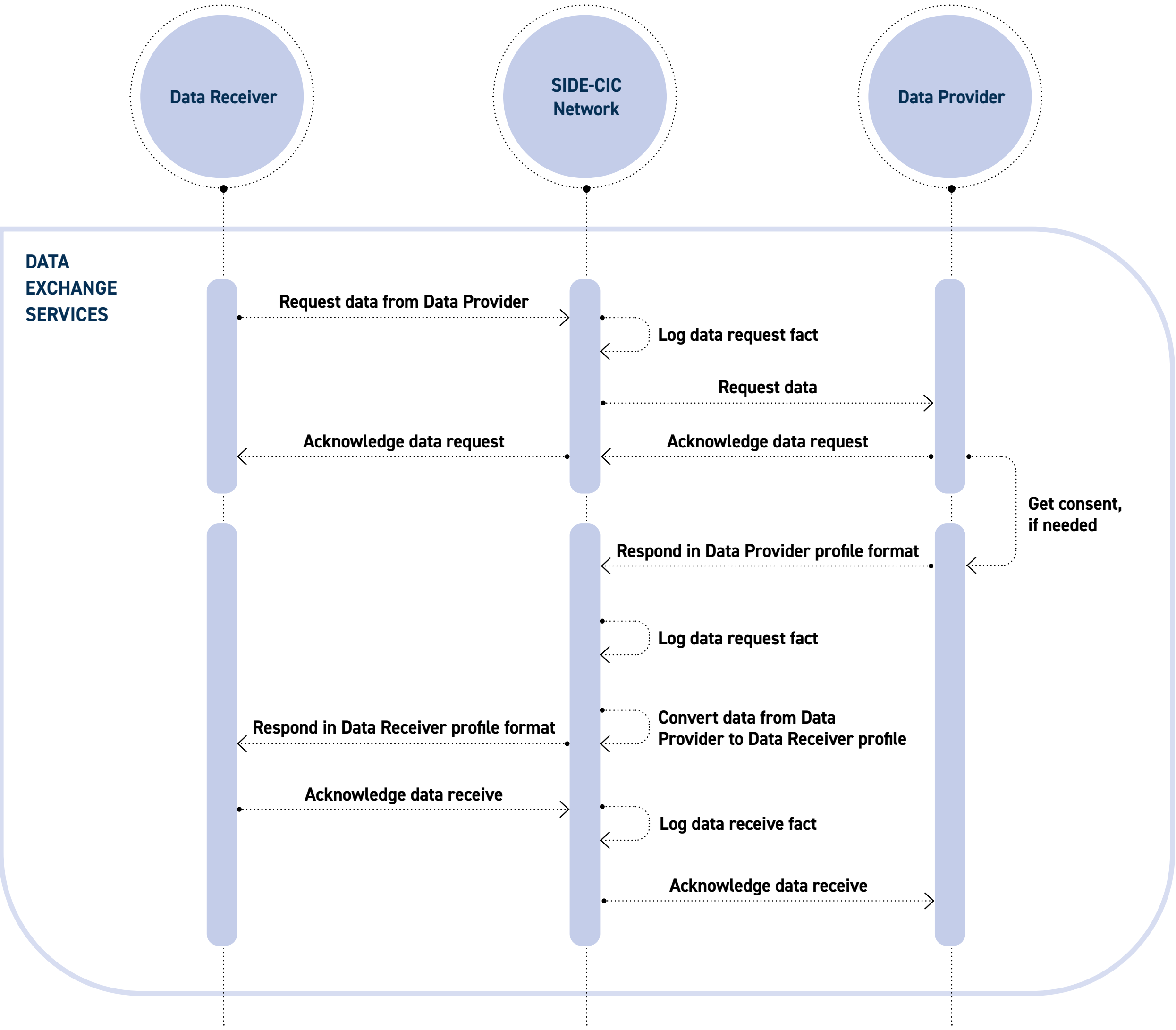
5.2 TECHNICAL CAPABILITIES AND SERVICES

Several technical capabilities and services are needed for data interoperability (See Graphic 12).

5.2.1 Register and authenticate network participant, Data provider discovery

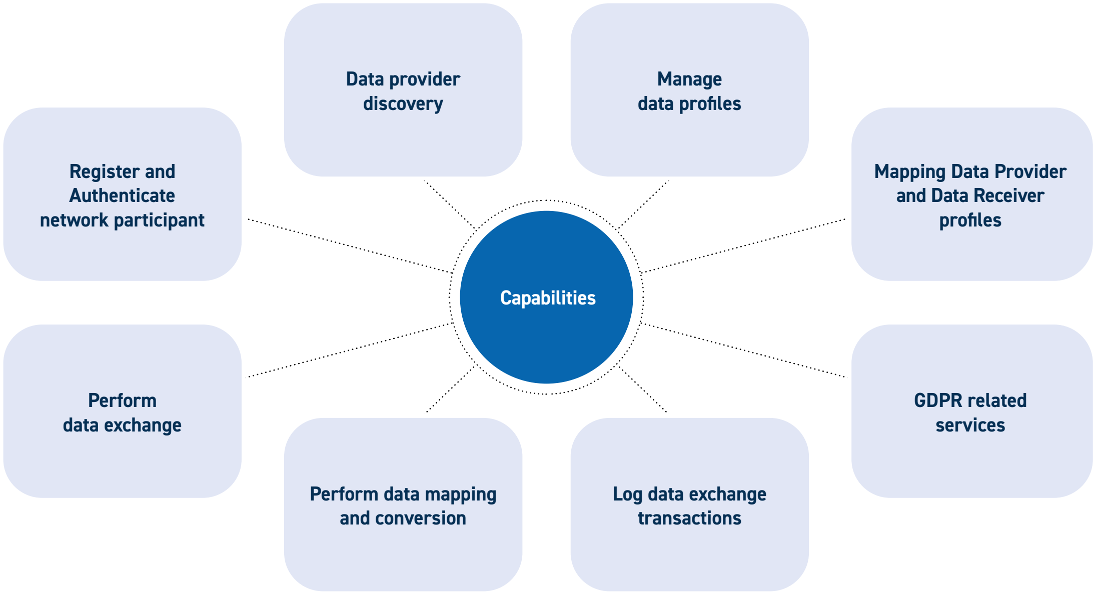
All participants of data exchange network will need to be registered, so that other network participants would know what participants are and where to direct their data requests. Naturally, all the network participants must authenticate themselves, – i.e. data exchange must be performed in the safe environment where every participant is sure whom they are exchanging data with.

Graphic 11 Sequence of Data Exchange



Note: For easier comprehension sequence diagram uses "SIDE-CIC network" actor in the middle. The same sequence works well in direct "Data Provider" to "Data Receiver" exchange.

Graphic 12 Technical capabilities and services


Capabilities
Data provider discovery
Manage data profiles
Register and Authenticate network participant
Mapping Data Provider and Data Receiver profiles
Perform data exchange
GDPR related services
Perform data mapping and conversion
Log data exchange transactions

5.2.2 Managing data profiles

Social ID cards have their own data attributes that are relevant to their local context. Data profile management service will allow them to publish their data attributes, declare their levels of assurance. This service would also allow them updating the profiles independently as they evolve over time.

5.2.3 Mapping profiles

Based on profile definitions, requirements for data level of assurance and use of common ontology an automatic profile mapping can be performed.

5.2.4 Perform data mapping, conversion and exchange

An orchestrating service, which would handle data exchange initiation, receiving data from data sender, calling data mapping and conversion service and delivering data to the data receiver in receiver's data profile format. This component would insulate data sender and receiver from need to handle all the different profiles.

5.2.5 Log transactions

Log of all the data exchange operations performed would be collected. Further investigation on the logging requirements is needed, but as an example, the log could contain data sender, data receiver, time stamp of request and data send, hash of whole set of data attributes, hash of person identifier, hash of company identifier, etc. ("Hash" is the result of applying a "hash function", which produces a short unreadable representation. Any change in data produces different hash result. It is not possible to decrypt original content from the hash).

Such log would not only ensure traceability of who exchanged data and when but would also allow data exchange parties to verify if data was modified after the send operation without disclosing personal data. The logs are conducted by the orchestration party appointed jointly by the steering group for the ecosystem. It is important that log administration is managed by an independent and trustworthy party.

5.2.6 GDPR related services

Services that help ensuring person's rights to own data as per GDPR, such as right to consent revocation, right to be forgotten, right to access data, etc. When original data holder receives a request from data subject, that member could propagate such request to every other participant, whom data was shared with.

Note, that data exchange does not introduce new ways of fraud, since only data of existing Social ID profile would be shared. Anomality reporting would need to continue be done on the local level.

5.3 INTEGRATION WITH EU INTEROPERABILITY FRAMEWORK

According to the Data Space Support Centre, interconnected Interoperability is the ability of different organizations and participants within a data space to share, understand and utilize data seamlessly. It is essential for effective data sharing and maximizing the value generated in a data space. The Rulebooks of the Data Space frameworks mentioned in 3.4.4 offers valuable insights into interoperability within and between data spaces. The design principle focuses on aspects like data modelling, data exchange and traceability.

The European Data Spaces Interoperability framework (EIF), referenced in the Data Act, establishes harmonized rules for fair data access and usage. This framework, aligned with the EIF and ISO/IEC 19941 standards, identifies four key facets of interoperability: technical, semantic, organizational and legal. Technical interoperability is supported by the Data Space Protocol (DSP), which defines a standardized set of specifications for data sharing.

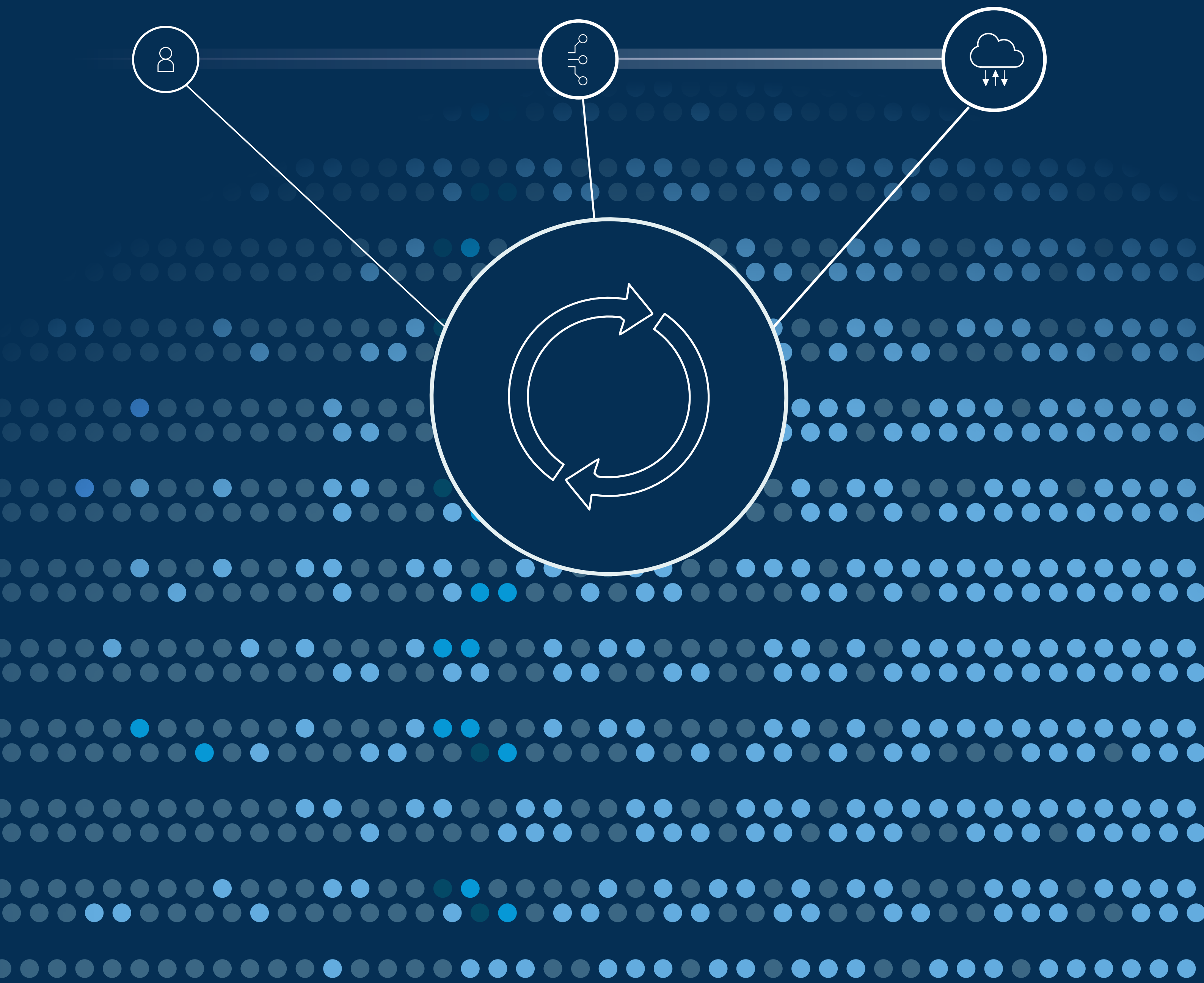
Data interoperability is crucial for efficient exchanges between data providers and recipients, enhancing agility, reducing errors and ensuring consistency across systems. Data Space Participants must integrate interoperability into their designs from the start to ensure these benefits. This design principle addresses data models, exchange protocols and features like provenance and traceability, ensuring that data sharing adheres to protocols mandated by the Data Space Governance Authority.

Metadata plays a crucial role in supporting data interoperability. It helps describe data and services within data spaces, covering aspects such as quality, formats, schema, provenance, access control and technical details. Quality metadata evaluates the reliability of exchanged data, while schema metadata assists in data interpretation and integration. Provenance metadata tracks the lineage and origins of data, helping maintain its reliability and compliance. Access control metadata defines permissions and aligns with security and privacy policies.

5.4 SUMMARY OF TECHNICAL SERVICES AND SOLUTIONS

As noted, a set of common standards, services and technical solutions are required to facilitate data exchange among countries. These common factors create the foundation of Trust that the data interoperability and exchange is built on. Adherence with EU standards and frameworks will add scalability. In the next chapter data flow and exchange alternatives will be examined closer.

6 Data flow, responsibilities & Data Exchange alternatives



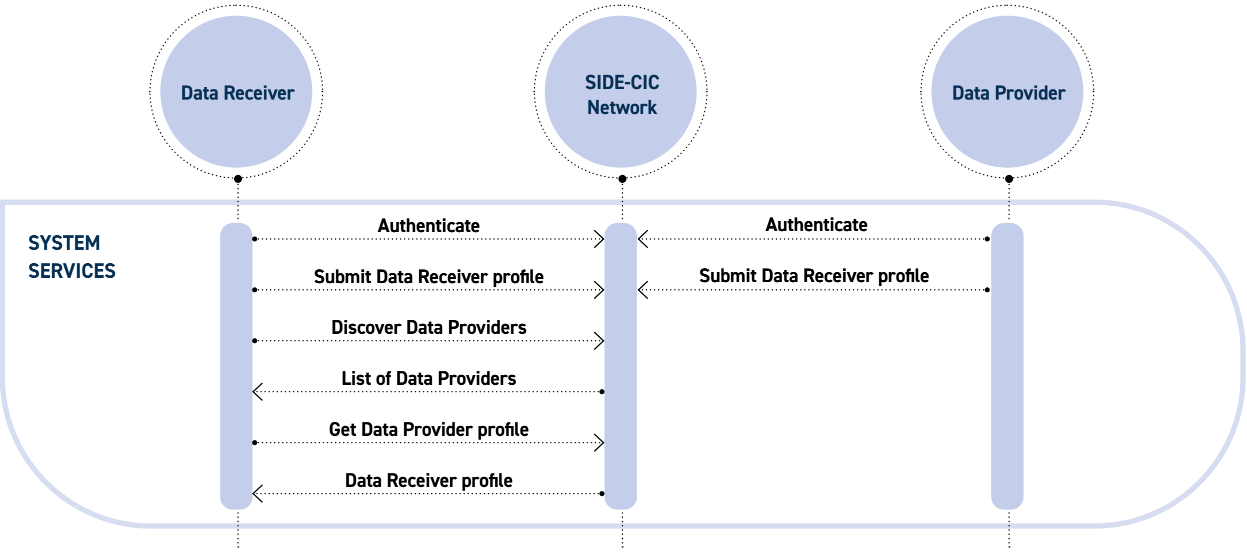
6.1 DATA FLOW

In this section an abstract (independent of implementation) workflow schema of how data exchange could function is proposed.

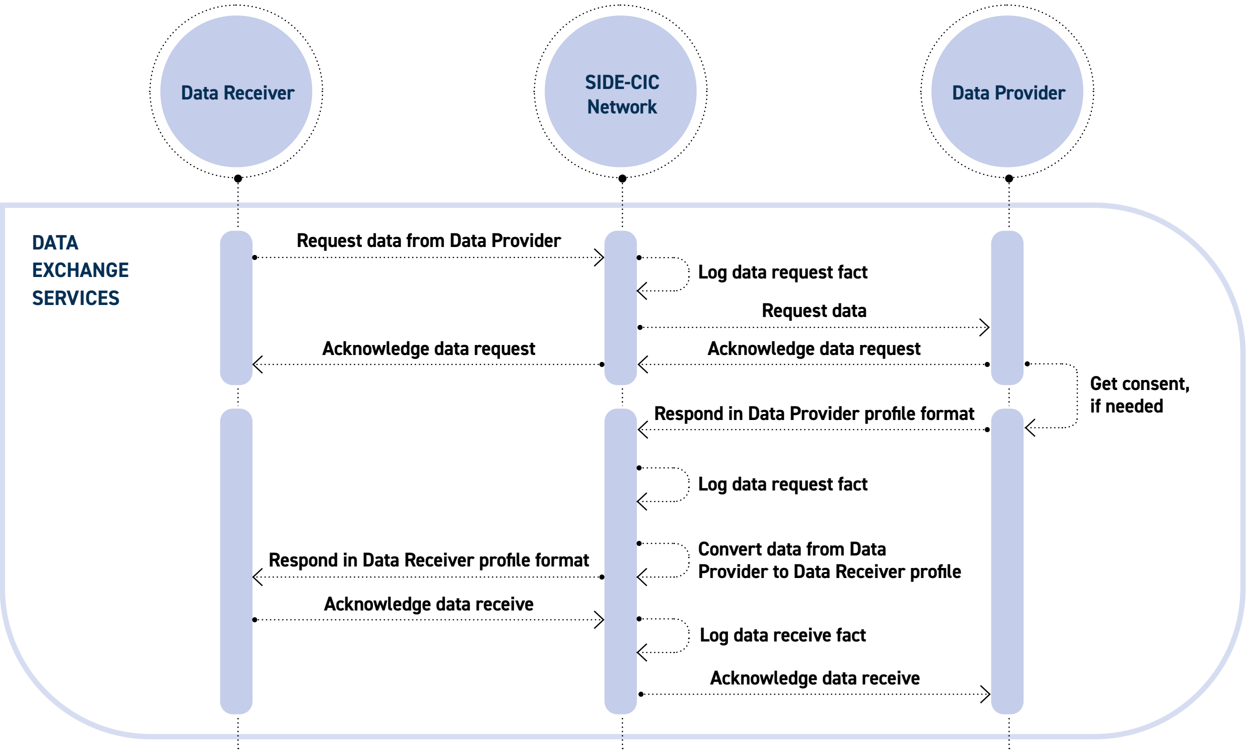
All members of the data exchange ecosystem should be able to securely authenticate themselves. Also, there should be a way to discover which other members participate in the data exchange, as well as understand what data other members are willing to provide, declare own data profiles of what a member wants to share (See Graphic 13).

Data exchange could be performed according to the workflow as depicted below (See Graphic 14):

Graphic 13 Data Flow example



Graphic 14 Workflow of data exchange



Main steps would be:

- Data Receiver requests data from the Data Provider.
- Data Provider would get a consent for data sharing from Data Subject, when needed.
- Data Provider would share data with Data Provider.
- An ecosystem would automatically convert and map data from Data Provider profile to Data Receiver profile. This way neither party needs to know implementation details of the other party.
- The data exchange fact would be logged for traceability purposes.

Furthermore, the data space could also facilitate data monitoring – receiving periodic updates on data such as other EU country company tax debts or legal status. It could be done by registering Data Receiver's interest on some data with the Data Provider and Data Provider would inform Data Receivers, when there are changes to the data of interest as depicted below (Graphic 15).

6.2 ROLES AND RESPONSIBILITIES

Data Space would have three main roles: Data Provider, Data Receiver and the SIDE-CIC network – an Entity responsible for Data Space creation and development. Depending on the scope decided by the Entity actors in the Data Provider and / or Data Receiver roles would need to define their own data profiles of what data they want to send and what data they need to receive. Data Providers and Data Receivers would also need to implement technological solutions based on standards proposed by Data Space (Table 6).

SIDE-CIC Network, as a minimum would need to propose standards for data ontology, technology and security, but could also implement data exchange components for data space members to use.

6.3 DATA EXCHANGE IMPLEMENTATION ALTERNATIVES

The alternatives for implementation could be as provided in the table below on the spectrum from "do nothing" to "create centralised solution with least effort required from participating members" and with some options in between.

When looking at implementation of the data exchange, one can look at different possibilities depending on how de-centralised vs centralised solution would be. Simplified logical schemas with possible options are depicted in Table 7.

Graphic 15 Data Monitoring services

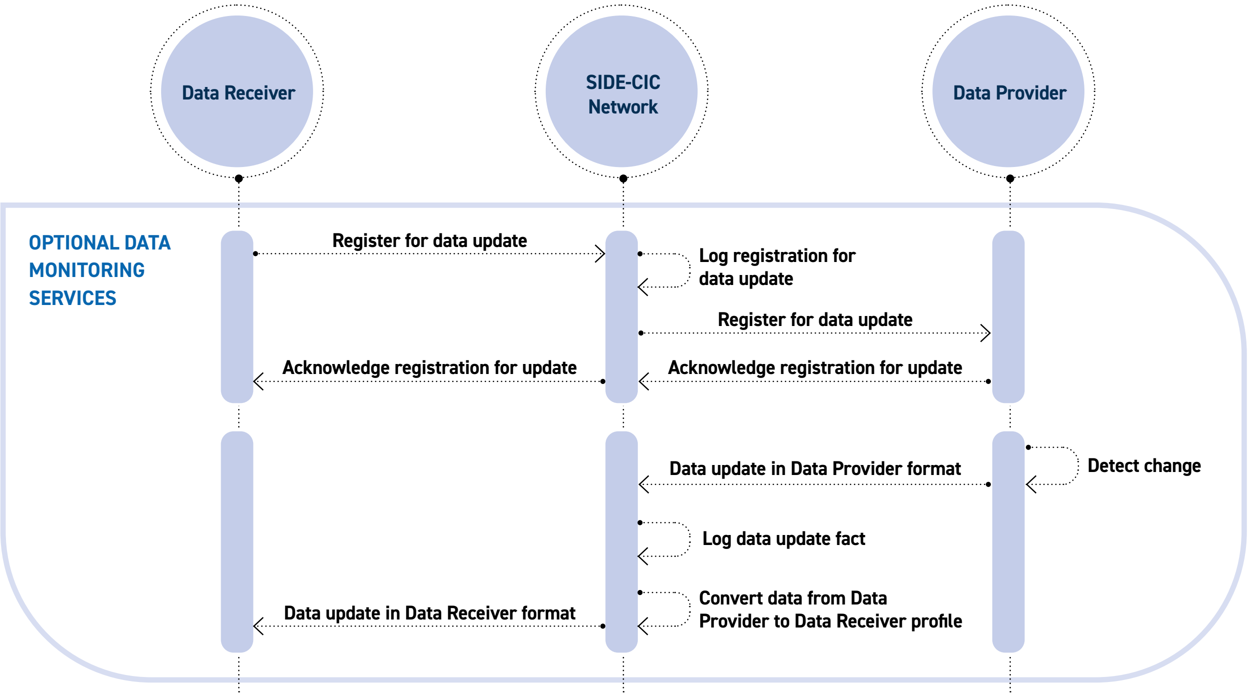

Data Receiver
SIDE-CIC Network
Data Provider
OPTIONAL DATA MONITORING SERVICES
Register for data update
Log registration for data update
Register for data update
Acknowledge registration for update
Acknowledge registration for update
Data update in Data Provider format
Detect change
Log data update fact
Convert data from Data Provider to Data Receiver profile
Data update in Data Receiver format

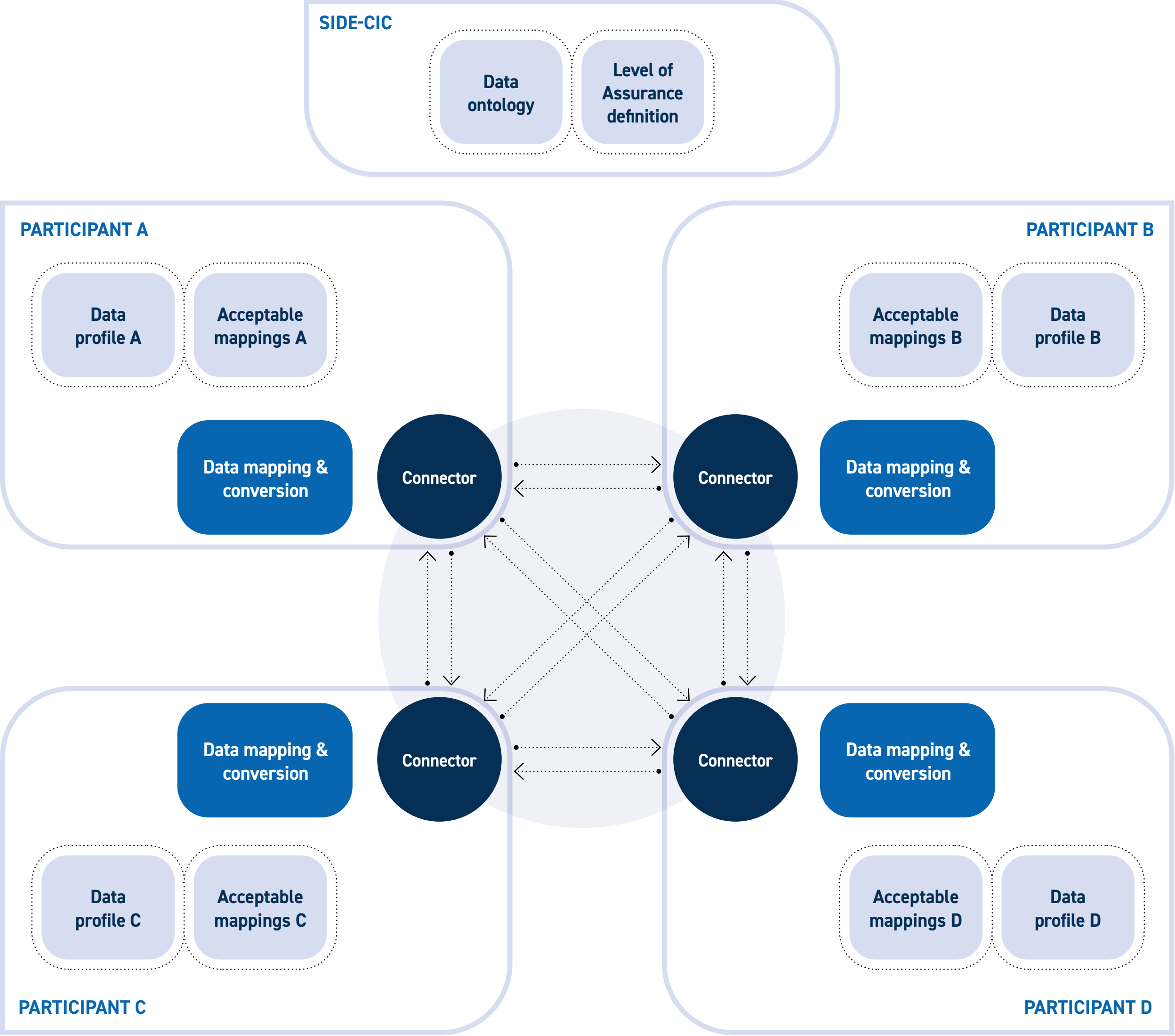
Table 6 Roles and Responsibilities members and network/ecosystem

	Data sender	SIDE-CIC Network	Data Receiver
1.	Define Social ID Profile	Propose data, technology (API) and security standards of the network	Define Social ID profile
2.	Implement connection to the SIDE-CIC network	Implement network infrastructure and technology	Implement connection to the SIDE-CIC network
3.	Collect consents, if needed. Respond to data sharing requests	Perform data exchange and mapping. In case of centralised – logging	Request data on behalf of construction company
4.			Collect additional data from the construction company

Table 7 Data Exchange alternatives

Alternatives	Benefits	Drawbacks	Services & components required
Leave it to countries to agree on everything and implement their own solutions	As it is now. No investments centrally.	Situation is not ideal. Would require re-inventing the wheel in multiple countries willing to improve situation	None
Create standards or recommendations on data sets, data exchange standards. Leave implementation to each individual country.	There would be guidance on: • data ontology and data naming for countries to "speak same language", • technical data exchange standard – so it would be easier for countries to implement it and there would be a single voluntary standard to follow. No need to have any infrastructure or operations centrally.	Countries would implement their solutions individually, establish peer-to-peer agreements and connections which involves a lot of repetitive work.	Data ontology and naming recommendations. Technical standard of API (documentation).
Create standards or recommendations on data sets, data exchange standards. Make an implementation (for example using block chain technologies) that each individual country could run.	There would be guidance on • data ontology and data naming for countries to "speak same language", • technical data exchange standard, and • centrally developed components/software that countries could take and run on their own infrastructure (hence less implementation costs locally, faster deployment, less misunderstandings and errors during implementations). No need to have any infrastructure or operations centrally.	There is a need to develop some software centrally and that needs investments. Cooperating countries would need to establish peer-to-peer agreements. Countries would need to run some centrally developed software which could differ from their own chosen software architecture, and it might need new competences to run it. There would be a need for central Technical Support function to help participating countries running centrally developed components.	Data ontology and naming recommendations. Technical standard of API (documentation). Implementation of components and services, that would then be deployed locally by each participating member. Technical support helping running the components locally.
Create standards or recommendations on data sets, data exchange standards. Implement a central data exchange system, that could perform data conversion and data exchange among countries. Countries need to implement single connection to a central system to exchange data with all members.	There would be guidance on • data ontology and data naming for countries to "speak same language", • technical data exchange standard, and • centrally developed components/software run by central organisation. Countries would implement one connection to the central system to exchange data with all connected MS's. Cheaper for each participating member, comparing to other alternatives. Single contract would be sufficient to start data exchange with multiple countries. NO PERSONAL DATA stored at a central system (it could operate like a phone company: keep records on data exchange fact, but not the actual content)	There is a need to develop some software centrally and that needs investments. There is a need to operate central system and it needs financing for as long as data exchange is in place. A data ecosystem technically is more difficult to set up comparing to a single peer-to-peer agreement.	Data ontology and naming recommendations. Technical standard of API (documentation). Implementation of centralised data exchange system. Technical support helping participants to connect to central system.

Graphic 16 Decentralised solution



6.3.1 Decentralised solution

De-centralised solution built with DSSC ideas in mind. Data ontology and other standards would be developed and maintained centrally. Connector, Data mapping and conversion component and several other services and components would also be developed (opensource components from Gaia-X could be reused) centrally, however these services and components would run locally on each participant's infrastructure. In addition, members would define their own Data profiles for sharing and Acceptable mappings for receiving data.

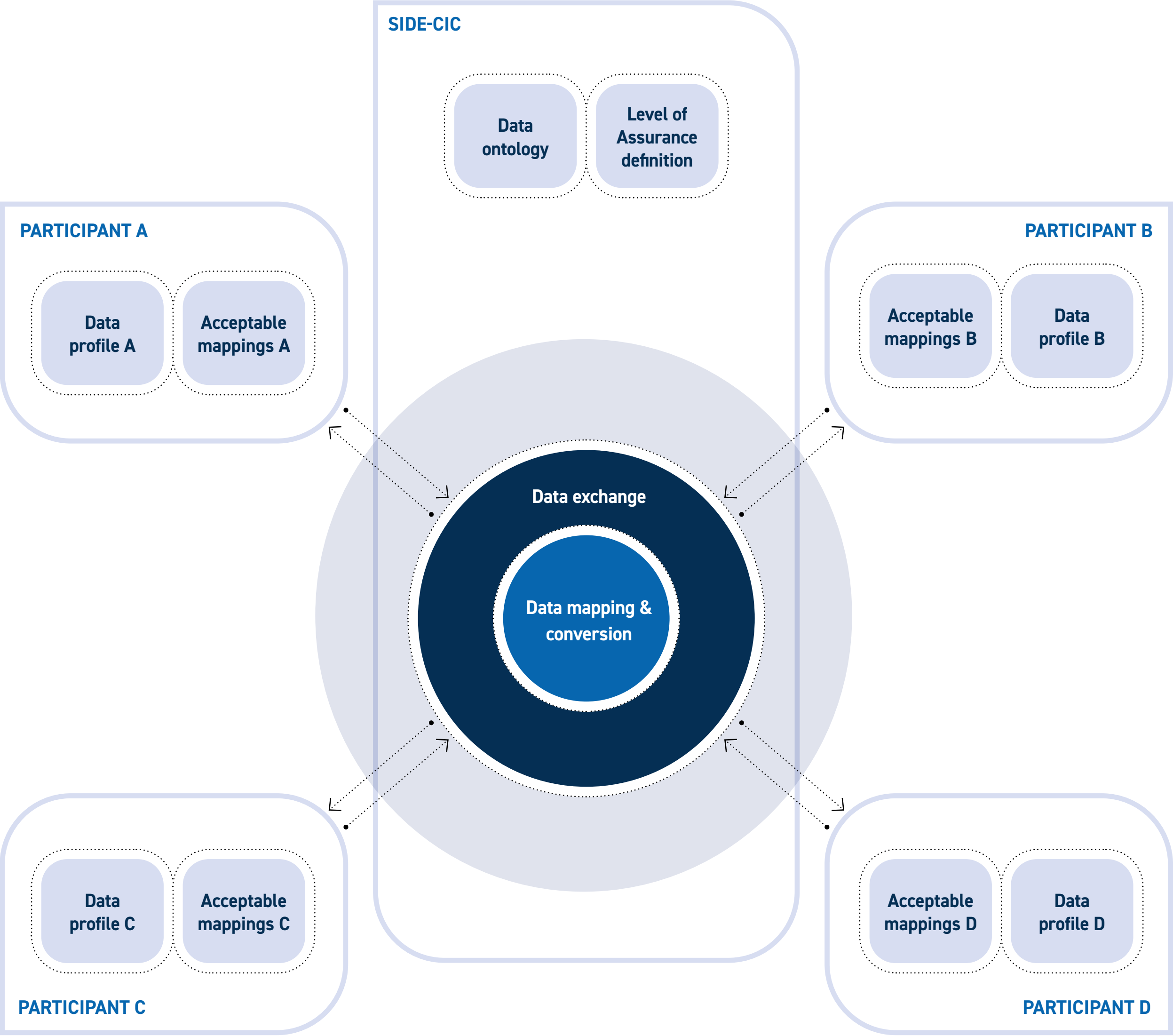
6.3.2 Centralised solution

If centralised solution would be selected, members would define their own Data profiles for sharing and Acceptable mappings for receiving data; would connect their locally run systems to the central system via API. But they would not need to run any additional software on their local infrastructure. Data exchange system would be developed and deployed centrally on a centrally managed infrastructure.

6.3.3 Summary of Data flow and exchange alternatives

There are different alternatives of making the Data Exchange in practice and the decision will have implications on many factors. To get the full picture a closer look at how to organise and what organisational entity model could be suitable is needed. This is explored in the next chapter.

Graphic 17 Centralised solution



7 Organisational & Operational Feasibility

7.1 COMPONENTS OF THE ORGANISATIONAL AND CONTRACTUAL FRAMEWORK

According to our expert interviews, a Data Ecosystem needs to have an organisational or governance framework and an agreement framework in place. These frameworks combined provides the necessary rules of engagement and dispute mechanism to run the Ecosystem. If the frameworks are well defined all parties can trust that the data exchange with each member is trustworthy and rely on the fact that possible indifferences will be resolved. These frameworks form the fundament of the Ecosystem.

In addition, a way to manage the service providers and subsequent services (see section 6) for the Ecosystem is needed. The services provided help to both execute the data exchange and provide support services needed for both members and the Ecosystem.

Furthermore, technical standards need to be set to make sure that the auditing of existing members and onboarding of new node members is systematic. Finally, the policies and practices for 3rd party auditing needs to be formulated.

All the separate documents are part of the Data Ecosystem Agreements framework which all parties need to sign before becoming members of the network. In practice however, the founding members sign a constitutive agreement and the new members an accession agreement.

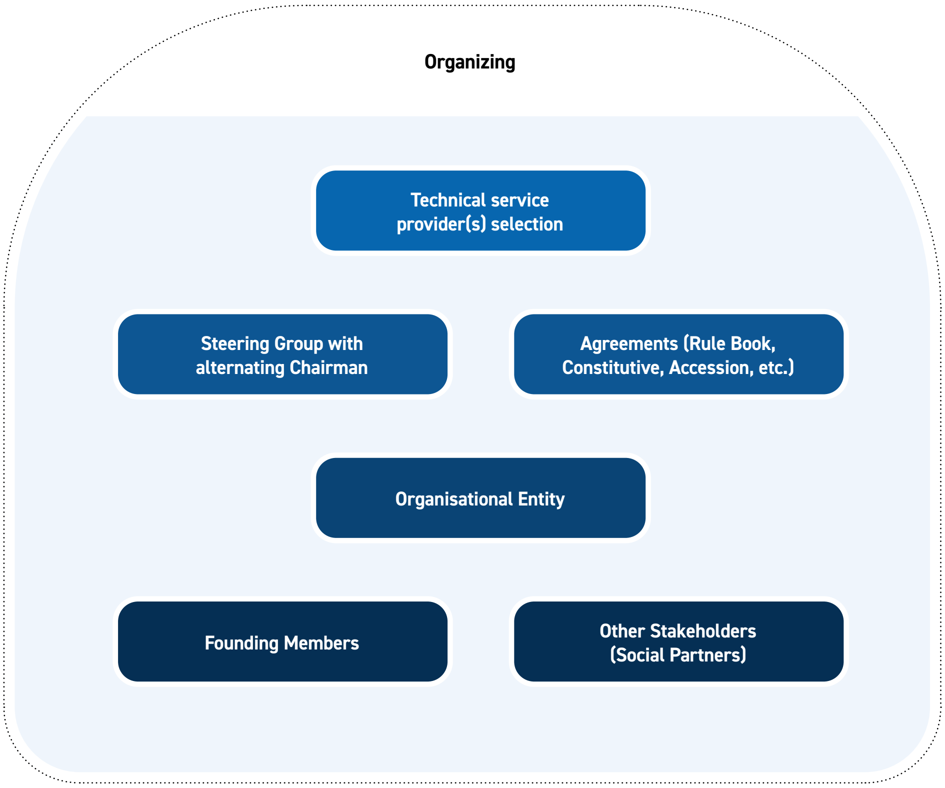
All the components form the framework upon which the Ecosystem is organised and governed. The components are described in more detail below. The graphic below summarises the different components.

7.2 ORGANISATIONAL FRAMEWORK

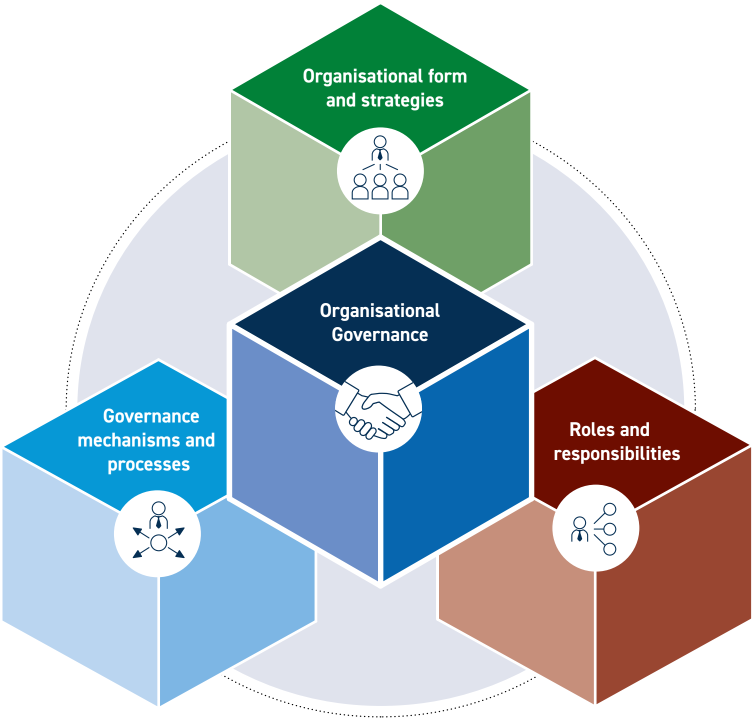
According to the Data Space Support Centre the organisational framework needs to consider the following aspects:

- **Organisational form and strategies:** This element encompasses factors such as the legal structure and applying the overarching strategies for the data space
- **Roles and responsibilities:** This element defines and assigns roles within the data space. The governance authority defines role descriptions, assigns tasks, establishes reporting structures and sets performance expectations for these roles.

Graphic 18 Components of the governance model


Organizing
Technical service provider(s) selection
Steering Group with alternating Chairman
Agreements (Rule Book, Constitutive, Accession, etc.)
Organisational Entity
Founding Members
Other Stakeholders (Social Partners)

Graphic 19 Organisational framework building blocks


Organisational form and strategies
Organisational Governance
Governance mechanisms and processes
Roles and responsibilities

Source: Data Spaces Support Centre (dssc.eu)

- **Governance mechanisms and processes:** This element includes procedures for fair dispute resolution between data space participants, performance monitoring, continuous improvement through innovation and continuity planning to ensure business functions in the event of disruption.

The key components constituting the organisational framework are:

- Organisational entity
- Steering group
- Technical and security standards

These components are discussed in more detail below.

7.2.1 Organisational entity alternatives

The organisational entity was discussed in the workshop #2. The alternatives are highlighted and evaluated in the table below:

The view of the workshop #2 participants was that a normal company model is not the best option. In practice the preferred model would be to form a Co-operative or a new separate federation. The co-operative model is interesting since there is an EU form called European Cooperative Society (SCE), an optional legal form of a co-operative. It aims to facilitate co-operatives' cross-border and trans-national activities. The members of an SCE cannot all be based in one country. The SCE is required to unite

Table 8 Alternatives of organisational entities

Area	Alternative	Description	Feasibility	Impact	Score	Assessment
Organisational entity	Co-operative (Normal or SCE/EU)	EU or member state based cooperative	2	3	5	**The model used most often in Data Ecosystems where the assurance of equal treatment is fundamental. European alternative (SCE) would take away jurisdiction question.**
	Federation	A new federation is created	2	3	5	Same model as FIEC or EFBWW but not suitable for an organisation providing services and handling substantial financials
	Company	A specific company is established	2	4	6	Not suitale in this context as it will easily lead to inequal treatment and unnecessary bureacracy and legal challenges since it has to be based in one country and follow that jurisdiction

residents from more than one EU country. A legal entity that allows its members to carry out common activities, while preserving their independence. Its principal objective is to satisfy its members' needs and not the return of capital investment. Members benefit proportionally to their profit and not to their capital contribution.

7.2.2 Steering group

There is no single alternative for a governance model. It is dependent on the size and specifics of the Data Space. In an ecosystem like the SIDE-CIC stakeholders the best way would be to work with a steering group much like a board in companies. The Data Space Support Center defines the following activities for the governing function as follows:

- **Dispute resolution:** Addressing operational issues and disputes that may arise between participants promptly and impartially. This could be done by providing a mechanism for reporting and resolving disputes.
- **Feedback mechanisms:** Establishing feedback mechanisms to gather input from participants and stakeholders on the effectiveness of the governance framework and using this feedback to drive continuous improvement.
- **Rulebook maintenance:** Ensuring the data space rulebook is up to date by revising rules, procedures and mechanisms to adapt to changing requirements and evolving technologies.
- **Scale for growth:** As the data space grows or evolves, adapting the governance framework to accommodate new stakeholders, services and requirements while maintaining guiding principles.
- **Compliance Enforcement:** Ensuring that all data space participants comply with the governance framework and implementing enforcement mechanisms, e.g. penalties or sanctions for non-compliance.
- **Risk management:** Continuously assessing and managing risks associated with data space operations, including data breaches, cybersecurity threats and regulatory compliance risks. Developing and maintaining contingency plans for potential disruptions.
- **Stakeholder engagement:** Promoting effective channels of communication and opportunities for stakeholder engagement.
- **Transparency and reporting:** Providing regular and transparent reporting to data space participants, stakeholders and relevant oversight bodies. Maintaining transparency in decision making processes and activities to build trust and accountability.
- **External audits and reviews:** Arranging for periodic external audits or reviews of the governance authority's performance and adherence to best practices. Addressing findings and recommendations for improvement.
- **Contingency planning:** Developing and maintaining contingency plans to mitigate potential disruptions or crises that could affect the operation of the data space. Ensuring that participants are prepared to respond to unforeseen events.
- **Legal and regulatory compliance:** Staying informed of relevant legal and regulatory changes that may affect the operation of the data space (see Regulatory Compliance building block). Ensuring that the governance framework remains compliant with all applicable laws and regulations.

For the steering committee to function effectively, the preparation work would need to be done by some persons that are operational in the Ecosystem. Based on the feedback in the workshop #2 the wish of the participants is that the governance model would be inclusive and thus involved stakeholders should be included rather than excluded. Naturally, the founding members of the Data Space who are engaged in

Table 9 Alternatives of participation models

Area	Alternative	Description	Feasibility	Impact	Score	Assessment
Participation model	Open with acceptance process	Model that fits current Social partner driven initiatives where all parties can participate	3	4	7	**Model that fits current Social partner driven initiatives where all parties can participate**
	Closed for Data Processors only	Only parties that process data participate	4	2	6	Though easier to implement with less parties to accomodate not feasible from impact perspective since many questions still need social party discussions

the data exchange must be given influence but equally Social Partners could play an important role in the governance model. It was however noted that financing should not be a basis for more influence and thus create indifference. In summary, an equal model was preferred. See analysis of the preferred model above (See Table 9).

7.2.3 Technical and security standards

It is finally important to form underlying technical and security standards that form a basis for trust and a framework for 3rd party auditing of members technical solutions. The technical standards are usually related to credentials and data protocols defining how data sets are deployed. Data Space frameworks like Gaia-x provide good guidelines relating to these matters.

7.3 CONTRACTUAL FRAMEWORK

The contractual framework is described in detail in the legal part of the feasibility study in section 4.2. In this section we want to highlight matters that have a technical implication (See Graphic 20).

7.3.1 Constitutive and Accession Agreements

The constitutive agreement is formed by the founding parties. From a technical perspective it is important to define the objective and functions of the data space, i.e. the basis and purpose for founding the data space. **The most important point is however to describe the use cases in great enough detail.** The use cases are the foundation on which the Data Space is built and therefore at the core of the governance framework. This sets the base for the future operations and is thus a document that will guide the future decisions. The accession agreement is signed by the members joining later. Thus, the point above made regarding the constitutive agreement is important.

7.3.2 Rule Book

The rule book is the most important legal document from a technical perspective. The key aspects to consider in the rule book are usually the following:

- Access & Control
- Data Ownership & Responsibilities
- Liability & Risk Management
- Confidentiality & Data Protection
- Sustainability & Futureproofing

The rule book is often called a Data Rule Book since it handles the key aspects that forms the legal framework regarding the data exchange in the data space. From a technical standpoint, the rulebook is where the important decisions are made that guide the needed technical capabilities for compliance to EU legislation. Since Gaia-x is an EU supported framework the model data rule books contain relevant aspects regarding the Data Act and General Data Protection Regulation or GDPR. The GDPR aspect is important since member states interpret GDPR differently. In a data space with SIDE-CIC context solutions for consent management regarding workers data are of utmost importance and one of the key legal obstacles to overwin.

Data ownership or data usage rights is one other key aspect of the rule book. The data space must provide solutions how this is monitored and audited. The rules regarding who has access to what data is also a key aspect.

7.3.3 Enabling services agreements

The data space needs supporting services to function and parties providing these services both in the setup phase and further in the operational phase. The technical team's view is that this should be a part of the legal framework discussed in the founding stage and not considered as a separate operational matter. The reason is that the discussion would highlight important aspects related to how to organise the data space and ecosystem.

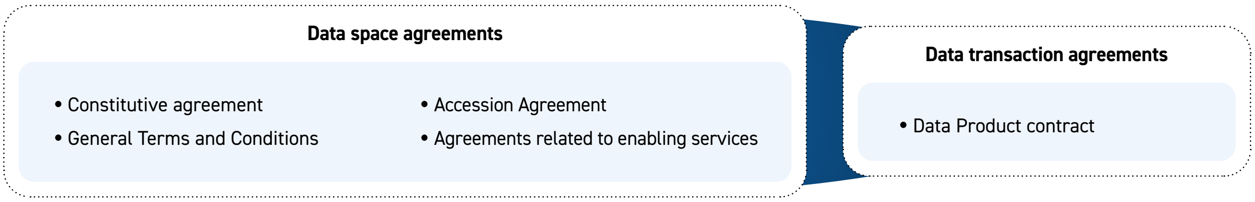
7.3.4 Data transaction agreement

The data transaction agreement usually provides descriptions how formal data products should be produced. In the SIDE-CIC context it would concern the data profiles like SIP and CSP – profiles described in section 4.2.1. The benefit would be that all members would have a legal guideline how to form the proposed data profiles to other members. This would significantly add trust to the equation.

7.3.5 Node Audit and compliance monitoring

The final aspect of trust is created by conducting 3rd party audits and creating a service for automated compliance monitoring and anomaly detection. These functions are important to enable potential participants with statutory or legal mandate to join and exchange data with members that have a mandate only being compliant with legislation but having a private mandate like for examples Social Partners joint or individually.

Graphic 20 Contractual framework



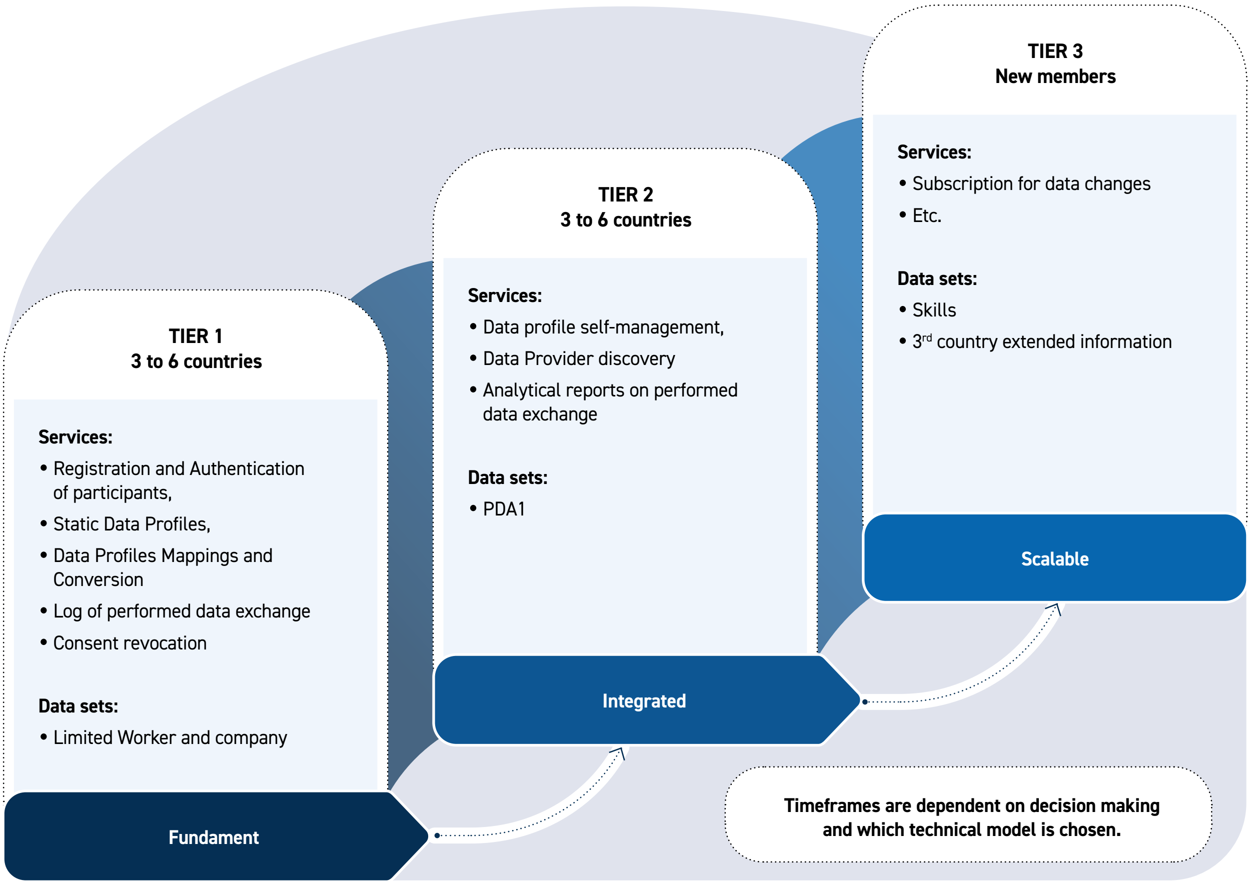
Data space agreements

- Constitutive agreement
- General Terms and Conditions
- Accession Agreement
- Agreements related to enabling services

Data transaction agreements

- Data Product contract

Graphic 21 Implementation roadmap with tiered approach



TIER 1
3 to 6 countries

Services:

- Registration and Authentication of participants,
- Static Data Profiles,
- Data Profiles Mappings and Conversion
- Log of performed data exchange
- Consent revocation

Data sets:

- Limited Worker and company

Fundament

TIER 2
3 to 6 countries

Services:

- Data profile self-management,
- Data Provider discovery
- Analytical reports on performed data exchange

Data sets:

- PDA1

Integrated

TIER 3
New members

Services:

- Subscription for data changes
- Etc.

Data sets:

- Skills
- 3rd country extended information

Scalable

Timeframes are dependent on decision making and which technical model is chosen.

7.4 IMPLEMENTATION ROADMAP

From a perspective of the parties joining the ecosystem, the services deployed, and data sets included we have made a tiered implementation roadmap (Graphic 21).

The idea would be to start quite small in each section and expand as maturity on all levels is reached. In this way the foundation can be created before more members and service offering and data is expanded.

The benefit of the tiered approach is that there would be a major learning experience for all parties and initial mistakes and wrong assumptions could be corrected. The need and benefits of a tiered approach was mentioned frequently in the workshops.

7.5 SUMMARY OF ORGANISATIONAL AND OPERATIONAL FEASIBILITY

One of the most important questions in creating a data space or ecosystem, is to gather enough political will. Therefore, the way a data space is organised plays a big role. Fortunately, there are good models and support functions in place to help those who aim to create a data space. There are also implications on the financial feasibility which will be discussed in the next chapter.

8 Financial feasibility

A financial feasibility study is very difficult to do in exact terms while the size, scope and implementation model is not clearly defined. However, it is possible to analyse what the technical development areas could be before deploying the data space and the different functions that would contribute to the running costs. It is also worth noting that EU provides substantial funding possibilities for creating data spaces.

8.1 COSTS OF CREATION OF ENABLING TECHNICAL SERVICES

The technical services needed to deploy a SIDE-CIC data space are described in chapters 5 and 6. The areas and factors can be summarised in Graphic 22.

8.2 COSTS OF RUNNING SERVICES

The running costs are divided into two major categories:

1. Management orchestration services
2. Technical orchestration services

They can be described as follows.

8.2.1 Management

Participant Onboarding & Governance

- Identity verification and credential management.
- Role-based access control and participant registry.
- Establishing and enforcing participation rules.

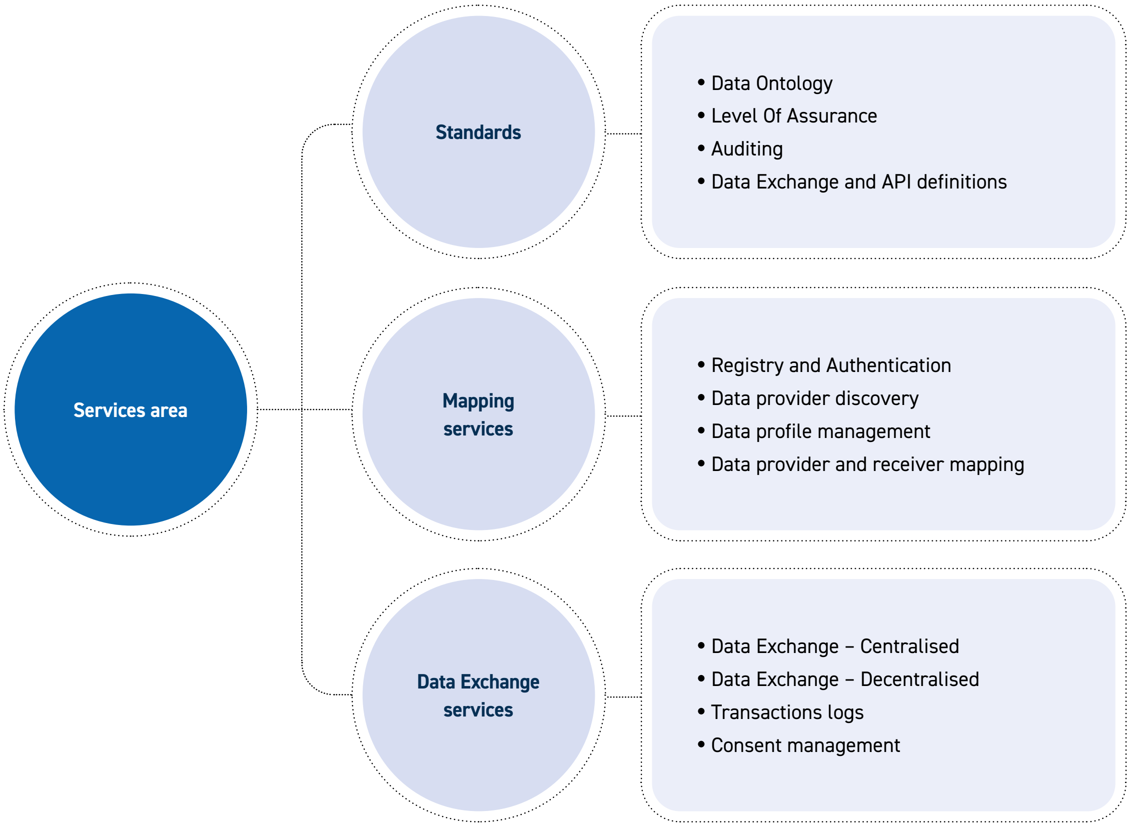
Trust Framework & Policy Enforcement

- Managing and enforcing data usage policies and contracts.
- Ensuring data sovereignty through governance mechanisms.
- Enabling trust anchors (e.g. via certifications, trust levels).

Discovery & Matchmaking

- Maintaining metadata catalogues for data/service discovery.
- Matching data consumers with appropriate providers.
- Managing service-level agreements (SLAs) and consent mechanisms.

Graphic 22 Cost components of development phase


Services area
Standards
Mapping services
Data Exchange services
• Data Ontology
• Level Of Assurance
• Auditing
• Data Exchange and API definitions
• Registry and Authentication
• Data provider discovery
• Data profile management
• Data provider and receiver mapping
• Data Exchange – Centralised
• Data Exchange – Decentralised
• Transactions logs
• Consent management

Compliance, Audit & Transparency

- Logging and monitoring of data transactions.
- Ensuring compliance with legal and contractual obligations (e.g., GDPR, data usage terms).
- Providing audit trails and transparency reports.

8.2.2 Technical Functions

Interoperability & Standards Enforcement

- Supporting common data models, APIs, and communication protocols.
- Enabling semantic and technical interoperability.
- Supporting federated identity and metadata standards.

Data Flow Orchestration

- Coordinating secure, policy-compliant data exchange between participants.
- Managing connections via data connectors, brokers, and routing services.
- Supporting data transformation, filtering, or enrichment where needed.

Infrastructure Services

- Hosting or coordinating shared services (e.g., connector registries, policy engines).
- Providing discovery, authentication, authorization, and negotiation mechanisms.
- Supporting scalability and availability of core services.

Monitoring & Automation

- Enabling real-time monitoring of data transactions.
- Automating workflows for contract negotiation, data access, and policy checks.
- Integrating with logging and alerting systems for incident management.

8.2.3 Summary of Financial Feasibility

In summary, the costs are fully dependent on the size, scope and choices made in the next steps. When considering the costs of developing and running a data ecosystem, it is worth noting that there are possibilities to get funding. The following chapter makes a summary of the different feasibility areas.

9 Summary of feasibility study

The summary of the feasibility stage consists of a summary of the different feasibility areas and an analysis of the factors creating trust as well as potential innovative solutions described in the feasibility chapters.

9.1 SUMMARY

As noted in the previous section, to get a comprehensive feasibility analysis, other than purely technical aspects needed to be assessed. Thus, the summary of the feasibility study is divided into the following sections:

- Purpose and need
- LegalTech
- Technical
- Organisation and governance
- Financial

The result of the feasibility assessment can be summarised in the following graphic:

Based on the figures shown in the graphic the workshop participants (#19 persons) were thinking that a data exchange ecosystem between the interested parties was a good idea and that it can be organised and

Graphic 23 Key terms used throughout the Report

Services area	Definition	Score in workshop (average)	Score by Technical team
Purpose and need	What is the urgency and real need?	8.4	8
LegalTech	Can critical legal related technical questions be solved?	6.9	7.5
Technical	Can technical challenges be solved?	6.6	8.5
Organisation & governance	Can the organisational and governance challenges be solved?	7.5	8
Financial	Can the operations and needed technical services be financed?	7.7	8

financed. On the other hand, participants saw that it will be difficult to deploy from a technical and from a LegalTech standpoint.

9.1.1 Purpose and need

The feasibility of the purpose and need is the starting point of the feasibility analysis. Based on our interviews and the feedback and scoring in workshops it seems like all participants agree that there is a clear need for interoperability and data exchange between both Member States Social ID Card services and between authorities and private sector stakeholders. The landscape is turning more difficult, and the fragmentation of the data is hindering everyone from getting the information they would need to carry out their tasks (Graphic 24).

9.1.2 LegalTech

The technical questions that are legally connected are challenging to evaluate in terms of feasibility because it depends on interpretations by the viewer. The most difficult question is no doubt regarding personal data protection and GDPR legislation since the Social ID Profile (SIP) contains personal information regarding the worker and the connection to the employer (Graphic 25).

The other big aspect to consider is the differences in mandates and legal frameworks in the Member States which makes implications on how the technical capabilities need to be designed to ensure a maximum level of trust. Based on our research, there are today existing solutions to solve these challenges. Personal Data Intermediaries (PDIs) and consent management tools compliant with GDPR regulations are applicable.

9.1.3 Technical

The technical feasibility which is the core of this study is an area which at first can seem rather complex but with close examination is rather structured and possible. In terms of deployment the decision to adopt the needed capabilities in a centralised or de-centralised model is important. Both models are possible and there are a lot of ready technological solutions available even as open source i.e. free of charge (Graphic 26).

The fact that the Social ID Card services have different technical maturity levels is not a big obstacle as they can gradually be improved with reasonable investments.

One of the biggest revelations during the project is that we do not need one data or technical profile for all services. The differences in data and technological solutions can be harmonized on ecosystem level with modern technology. It is however important that the technological investments can be done gradually so that initial investment does not become an obstacle.

The fact that there are Data Spaces that have faced the same challenges as SIDE-CIC is also re-assuring since many of the challenges have been solved by others before.

9.1.4 Organisation and governance

During the workshops it was repeatedly pointed out that the Member States' services and legal differences must be respected when forming the potential joint solutions. Therefore, the organisational and governance models must respect this request. In practice this means that the model must be open and inclusive as well as based on equality between the members (Graphic 27).

Graphic 24 Feasibility Purpose and need

Key Questions	Justifications	Obstacles	Risks	Tools
Purpose • What is the need for data sharing? • What is the key problem? **Motivation to join** • What motivates participants to join? **Use cases** • What are the use cases? • What problem justifies the data sharing?	• With all the crises and security threats workforce mobility will increase • Social ID services biggest challenge is data regarding foreign workforce • Without an ecosystem or data space everybody needs to solve things individually • The use cases are concrete and options are rare	• Participants with regulated data sets can have difficulties to approve mandate • Authority based participants might have difficulties to get mandate • New participants have challenges getting go to start	• Too few participants in pilot and founding phases • If multiple regions cannot be formed the EU dimension and funding is not justifiable • If arguments, pay back and ROI figures are not crisp justification for investments might be hard	• Data Space sales deck • Social ID Card sales deck with figures • Benchmark visits to multi-stakeholders in many countries • Purpose, need and use case presentations

Graphic 25 Feasibility LegalTech

Key Questions	Solutions	Obstacles	Risks	Tools
Consent How to enable consent management in a way that enables use by all members? **Conversion** How to convert Data Profiles so that legal differences are harmonised as good as possible?	• Choice of consent management tool(s) with a method and an application that is accepted across Europe • Focus on legal differences in mapping stage and providing solutions with connector technology and guidelines	• Non-voluntary consent dilemma might be dependent on local interpretations • Data profiles might need amendments at source level to be accepted	• Time delays in the process due to consent issues • Difficult legal questions where interpretations vary might slow down process	• Consent management tool research and selection • Close co-operation with legal experts to form acceptable solutions • Utilize solutions by other data spaces

Graphic 26 Feasibility Technical

Key Questions	Solutions	Obstacles	Risks	Tools
1. What are the requirements for the network? (i.e. scope of capabilities needed) 2. What level of technical expertise could solve demand locally? 3. Who (people, organisation) is going to make decisions on requirements and technical alternatives?	1. Provision of adequate support for countries in need of technical assistance 2. Careful evaluation of technical model (centralised. vs. de-centralised) to verify capabilities to implement by all parties 3. Development and testing in pilot phase	• Technical maturity variations among countries, for some might be difficult to use distributed solution • Technical investments potentially needed for some parties to join • Technical security levels too low by some parties Profiles to be accepted	• Needed investments slow down the joining of some parties • Lack of security makes profiles cold • Slowness of adoption of some members makes the whole process drag out in time	• Ecosystem provided tools and support • Strong pilot phase where provided tools are tested by all parties • Consideration of centralised tech model

Graphic 27 Organisation and governance

Key Questions	Solutions	Obstacles	Risks	Tools
1. What is the most suitable organisational entity alternative? 2. How to organise a multi-stakeholder / inclusive model without making decision making too slow and political? 3. How to balance the rule book and steering group governance role?	1. Make use of established Data Space models and templates 2. Use experts to facilitate the creation of the ecosystem legal and governance frameworks if necessary 3. Benchmark similar ecosystems for reference and learnings	• Lack of understanding by external to project decision makers why a separate entity is needed • Discussions regarding semantic governance issues due to political standpoints	• Discussion regarding a new joint entity slows down process • Governance and legal framework process becomes tedious due to differences of opinion on details	• Data Space tools, templates and support centres • Clear arguments why certain decisions are needed • Use of benchmarks

Graphic 28 Feasibility Financial

Key Questions	Solutions	Obstacles	Risks	Tools
1. How to finance the development of common tools and capabilities? 2. How to finance the operational phase? 3. What funding / financing instruments should be used?	1. Make solid cost calculations of funding needed for each phase 2. Use pilot phase to develop and test potential technical solutions 3. Consider multiple financial and funding instruments and sources	• Funding needed grows too big per participant due to low number of funding members • Difficulties on agreeing on funding instruments • Difficulties of estimating total costs on capex and opex levels	• Mandate challenges reduces the number of founding members and slows down the process • Difficulties of getting commitments due to complexity and lack of understanding of calculations	• Focus on getting good funding and allocating as much as possible development work to pilot phase • Use pilot phase to learn and make accurate budgets regarding development and operational expenses and estimations of income

The choice of organisational entity must reflect the stakeholders represented and the values stated above. Similarly, the objective should not be to make a too detailed agreement framework but rather create a good and practical way to solve possible challenges and resolve issues and disputes that may arise. A functioning Data Space needs an orchestrator function that can run and operate the ecosystem as well as manage the governance and auditing functions.

9.1.5 Financial

The financial feasibility is directly linked to the options regarding technical models chosen. A centralised solution needs more financial capital initially but is the most economical solution in the long run. On the other hand, a decentralised solution is more scalable (many-to-many principle) as it is the members themselves that are responsible of deploying the technical capabilities provided by the ecosystem. A model where the financing is arranged by having a member fees and EU/public financing combination seems like the most logical solution. The member fees can also be funded on Member States' service level by fees from customers using the cross-border service (Graphic 28).

It is worth noting that the option of not doing anything carries a big alternative cost. These costs are indirect but nonetheless substantial. The alternative costs can be seen in manual and non-value adding working in the ecosystems and the costs of the effects of inadequate social rights for workers.

9.2 CIRCLE OF TRUST

A cross-border data space is dependent on trust between the members and in the organisational governance and technical services. In summary, trust is derived from a holistic approach where the data space services are provided as illustrated in the graphic. The components are described in the feasibility chapters and must work integrated to form a Circle of Trust (Graphic 29).

One of the most important questions to safeguard is that data is only used for the intended purpose and in compliance with the standards stipulated. This is especially important since personal data is in the centre of the profiles in this Data Space.

9.3 POTENTIAL INNOVATIVE SOLUTIONS

To complete the feasibility study a summary of the potential innovative solutions was created.

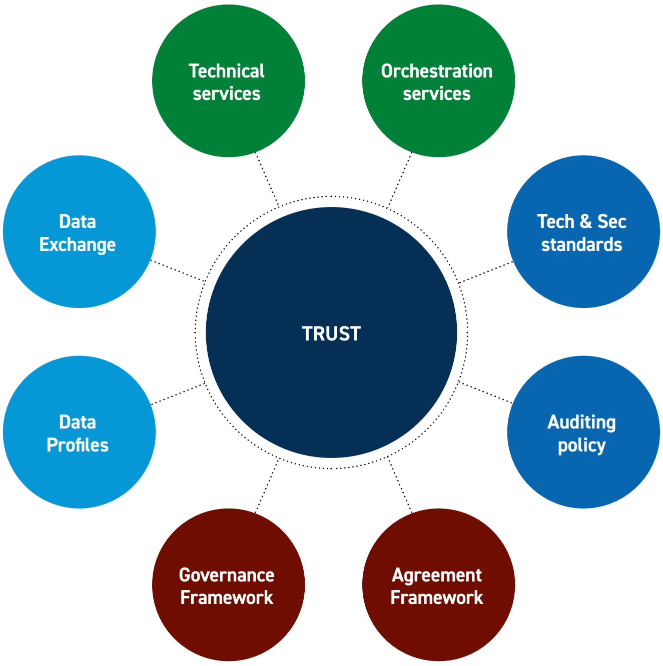
The solutions are shown in Graphic 30.

Some of these solutions were described in the previous chapters. Some novel ideas were also discovered:

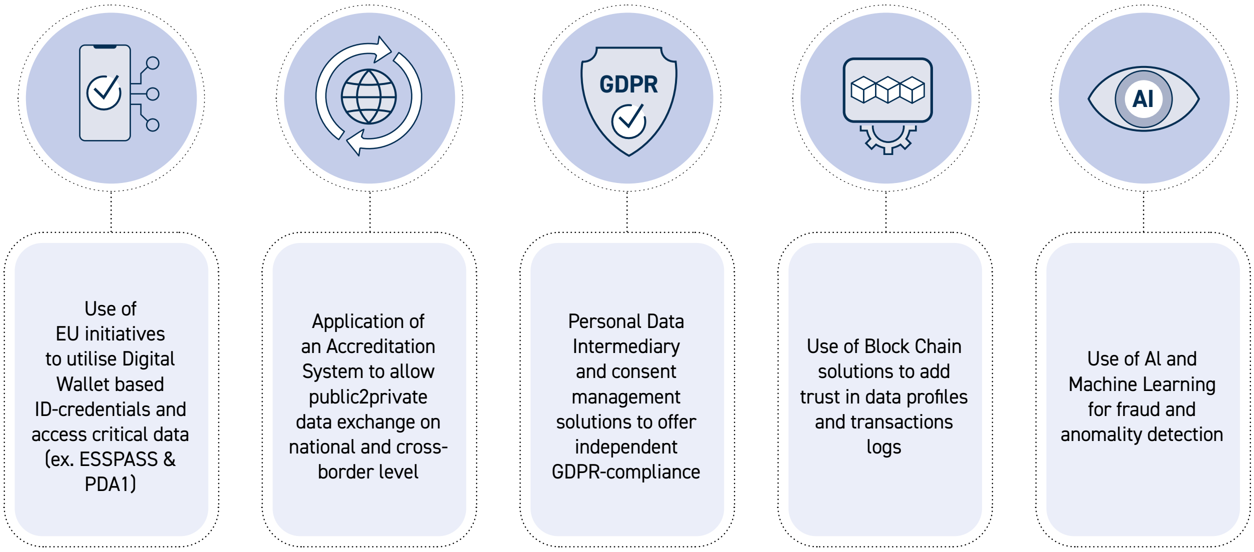
- **Accreditation system**
  The benefit of an accreditation system is that all parties could share information that previously was available only for ex. to authorities. This would enable Social Partner driven or owned Social ID Card services to get access to IMI, eIDAS and other systems described in chapter 2.

- **Block Chain**
  Block Chain could be used to ensure the authenticity of data and documents if needed. The block chain generated key could be cross referenced in an inspection or compliance situation. To use a relatively

Graphic 29 Circle of Trust



Graphic 30 Potential innovative solutions



Use of EU initiatives to utilise Digital Wallet based ID-credentials and access critical data (ex. ESSPASS & PDA1)

Application of an Accreditation System to allow public2private data exchange on national and cross-border level

Personal Data Intermediary and consent management solutions to offer independent GDPR-compliance

Use of Block Chain solutions to add trust in data profiles and transactions logs

Use of AI and Machine Learning for fraud and anomality detection

heavy solution like block chain there would need to be serious doubt of or proven cases of fraud.

- **AI and machine learning anomality detection**
  One of the interesting solutions that could be benchmarked from other industries are fraud detection systems using AI and Machine Learning solutions. In the financial sector anomality detection has been successfully used to detect fraud. The benefit of automated and machine-based solutions is that unknown ways of fraud can be discovered.

10 Obstacles and risk analysis

In this chapter the main obstacles of creating a Social ID Card Data Space are listed and evaluated. In addition, the risks and corresponding mitigation strategies are defined and scored. This section provides and analysis of the outcome scenarios based on the technical mapping, feasibility and recommendation phases.

10.1 OBSTACLES ANALYSIS

Within the scope of the technical analysis, we also evaluated the potential obstacles from a holistic perspective. We did not identify direct roadblocks but more obstacles and challenges that need to be solved to move forward along the pathway between the current and desired state described in section 2.3. The main obstacles and challenges are summarized in the graphic below.

10.1.1 Mandates for founding and funding

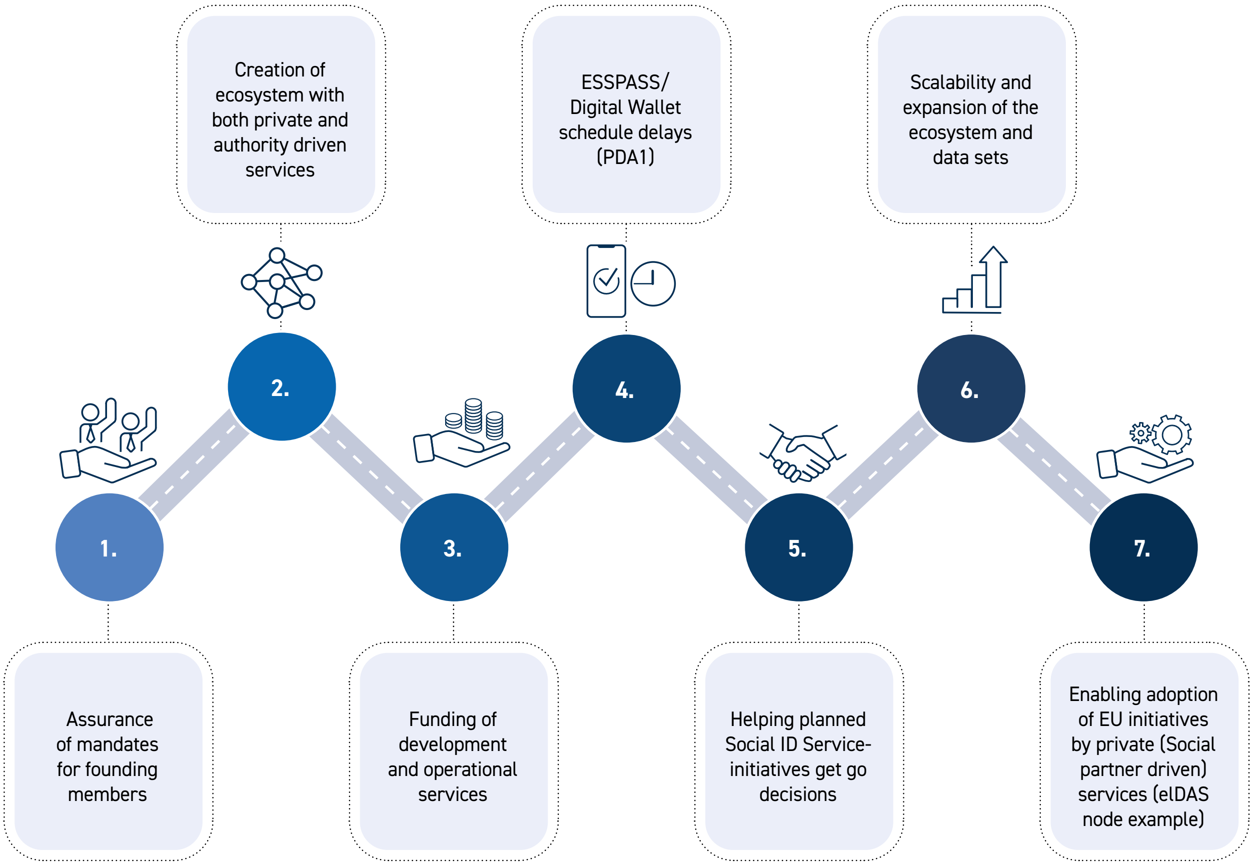
One of the most obvious obstacles (points 1 and 2), is the initial creation of the Data Space and Ecosystem since it requires a mandate and a rather long-term commitment to be part of this kind of co-operation. Since most Social ID Card services are very locally oriented, international co-operation might not be an easy task even though the need for better information regarding workforce from other EU and 3rd countries is duly recognised. Equally acquiring mandate is challenging for Social ID Card services operated by authorities and services that have a statutory mandate i. e. mandate based on legislation. The technical team want to highlight the importance to create a model where founding members can be either data senders or receivers. It is therefore fully up to the individual service to make the choice which profiles they want to use or provide in the ecosystem.

Another mandate related question (point 3) is the question regarding funding of the data space. The members of the data space will have to contribute with some funding to enable the creation and running of common services and capabilities described in section 5.2.

10.1.2 New members and scalability

The second group of obstacles are related to the challenge in some Member States to start a country specific and centralised Social ID Card service. This is the

Graphic 31 Summary of obstacles and challenges


Creation of ecosystem with both private and authority driven services
ESSPASS/ Digital Wallet schedule delays (PDA1)
Scalability and expansion of the ecosystem and data sets
2.
4.
6.
1.
3.
5.
7.
Assurance of mandates for founding members
Funding of development and operational services
Helping planned Social ID Service-initiatives get go decisions
Enabling adoption of EU initiatives by private (Social partner driven) services (eIDAS node example)

situation for the Netherlands, Romania, Iceland and Denmark. It relates to the challenge of expanding the ecosystem from the initial founding members to new members. It is in the interest of all stakeholders that new Member States can adopt Social ID Cards. It is important that the ecosystem gathers key impact information, make illustrative presentations and provide possibility for reference visits to support all Member States' planning a Social ID Card to succeed. In this way the ecosystem grows. Equally, in terms of scalability, it is important the Data Space can grow content wise so that new use cases and added data profiles are constantly introduced. Currently there are no countries that are seen unsuitable to join but there must be a clear accession process and way to show that new members comply to retain trust in the ecosystem. It is important to recognise that the readiness to join varies a lot in EU. This should be alleviated by creating benchmark opportunities and joint standards.

10.1.3 Timeline challenges related to technical availability and data sharing

Some Social ID Card services have stressed the importance of getting access to verified (directly from source) posting data i.e. PDA1 data. The challenge however is that the availability is not clear since it is dependent on Member States' adoption timeline and the progress of the solutions (points 4 and 6). An example of this is the ESSPASS-solution described in multiple sections that finally would make posting information available. In addition, the ESSPASS rollout is dependent on Digital Wallet solutions that must be rolled out in member states for the ESSPASS solution to have mobile credentials. The delay of these initiatives could significantly slow down the progress of this project.

In addition to these points, we have jointly with the legal team identified the importance of proper consent management in relation to cross-border workers data profiles. Since this issue is one of the most common ones in relation to Data Spaces and valid solutions are available, we do not deem this as an obstacle but more a challenge that needs to be solved by practical services.

10.2 RISKS AND MITIGATION STRATEGIES

Based on the studies and the interviews conducted, as well as the discussions and inputs from participants in the workshops and steering group meetings, we have summarised the risk related to the creation of a SIDECIC Data Space. We also made a probability and impact assessment resulting in a risk score. Finally, we made mitigation strategies for all risks.

The potential risks and the respective mitigation strategies are highlighted in the table below.

Table 10 Risk and mitigation table

Stage	Risk	Mitigation
Next phase	Not enough participants (mandates)	Solid plan and feasibility challenges solved
Next phase	Lack of funding	Application only when plan is solid and sufficient parties are secured
Ecosystem creation	Inability to agree on model	Use of existing and proven ecosystem models with support functions available
Formalisation phase	Some willing members do not get mandate to join	Adress of mandate question immediately in the beginning of the next phase so that open questions can be answered in good time
Service deployment	Technical maturity challenges	Common services to ease and support deployment
Service deployment	Non usable (cold) data profiles	Provide assistance for all parties to create and ensure sufficient trust factors
Service deployment	Deployment becomes too expensive	Develop Proof of Concept and pilot versions of services in potential pilot phase › only production scaling needed
Operations and scaling	No or not enough new members joining	Supporting presentations with solid facts and possibilities for reference visits made available

According to our risk assessment there are no risks with critical (9-10) score. The biggest risk foreseen is that some Member States Social ID service providers cannot gain mandate to become a founding member. This would result in a situation where there are not enough founding members to sustain the investments in time and money to create the Data Space for Social ID Data in the construction industry.

Another risk is that the intended Pilot phase is not realised due to funding or political reasons. This is critical since it is important to show for all stakeholders and non-technical persons that interoperability works and that the blueprints and ready models in DSSC.eu and Gaia-x are deployable. A pilot would also enable the evaluation, testing and iteration of governance models and agreement frameworks.

As discussed in the workshop #3 the best model would be an iterative deployment where the solutions can be implemented gradually i.e. in small steps. This would provide a good learning curve for all stakeholders and the necessary time to prepare the mandate process on Member States' service level.

A risk that can have political consequences is a scenario where a national authority driven solution is deployed without consulting the Social Partners. In Estonia, the development was done in close co-operation with the local Trade Union.

11 Benchmark examples

11.1 DS4SKILLS/PROMETHEUS

11.1.1 Background of the data ecosystem

The DS4SKILLS data space is created to enable sharing and accessing of skills data between different parties. It is presented as follows:

“The Data Space for Skills (DS4Skills) is a 1-year project (2022-2023) aiming to prepare the ground for the development of an open and trusted European Data Space for Skills that supports sharing and accessing skills data.

It is funded by the European Commission under the Digital Europe Programme and involves 14 ambitious partners from the industry, education and data ecosystem sectors.

11.1.2 Parties and results

The parties in the ecosystem consists of 10 full Partners and 4 Associated Partners with solid experience in data ecosystem and community building, a wide network of stakeholders from diverse backgrounds, including researchers, training providers, companies as well as associations representing industry and data ecosystems.

The key deliverables in the project were:

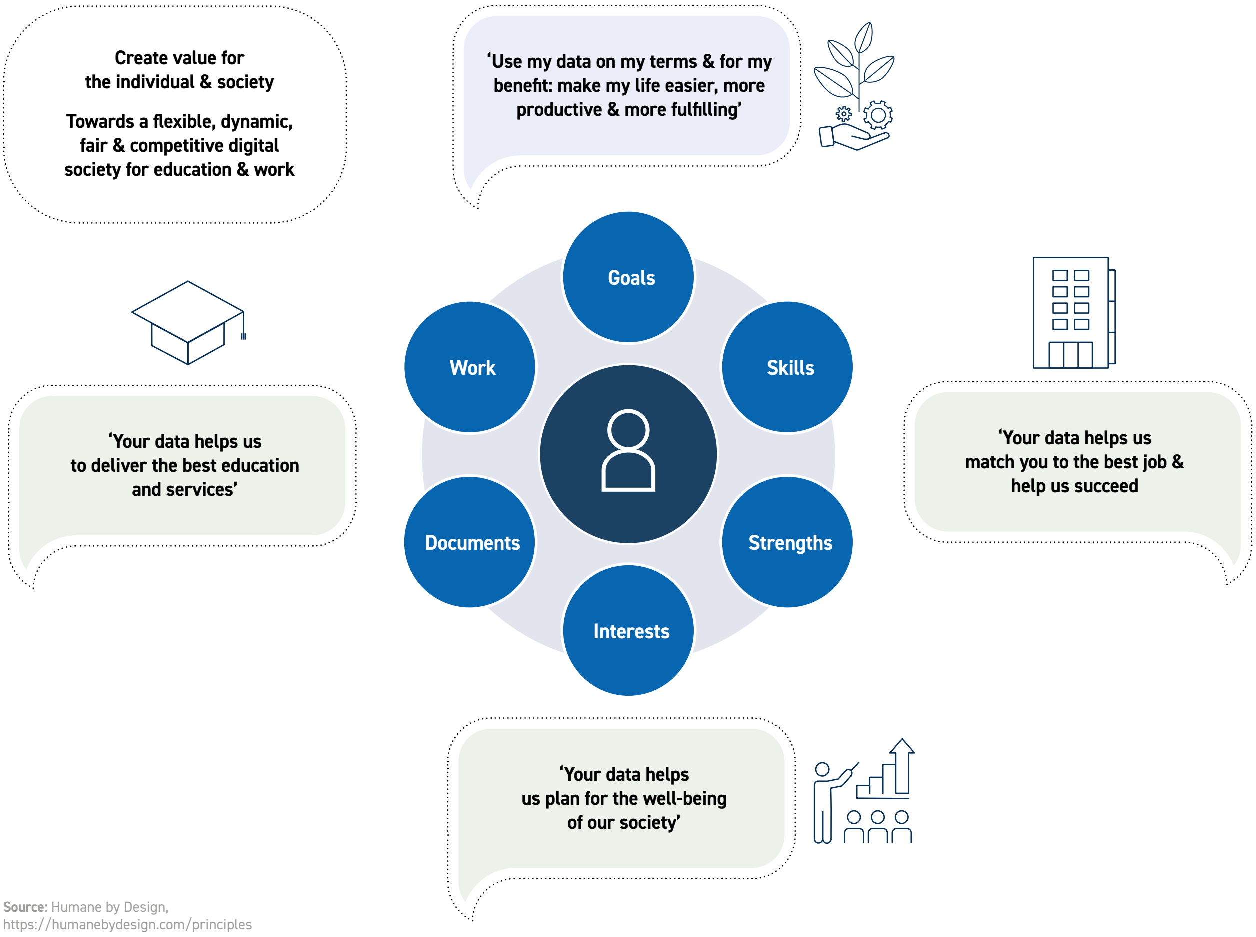
- Technical Building Blocks
- Governance model
- Usage scenarios

All the findings in the project are present in a comprehensive DS4Skills BluePrint (https://skillsdataspace-blueprint.eu/)

11.1.3 Relevance to SIDE-CIC

As a benchmark this is very interesting as it reflects a similar challenge where data is scattered and not working in the interest of the stakeholders involved. The interesting thing about the DS4SKILLS data space is that they have taken a human-centric approach to the skills issue. The figure below explains this clearly.

Graphic 32 Human-centric approach to skill data


Create value for
the individual & society
Towards a flexible, dynamic,
fair & competitive digital
society for education & work
‘Use my data on my terms & for my benefit: make my life easier, more productive & more fulfilling’
Goals
Work
Skills
Documents
Strengths
Interests
‘Your data helps us to deliver the best education and services’
‘Your data helps us match you to the best job & help us succeed
‘Your data helps us plan for the well-being of our society’

Source: Humane by Design, https://humanebydesign.com/principles

Graphic 33 MyData Principles

MyData Principle	For the individual, this means
Human-Centric Control of Personal Data	"I know where my data is and how others may use it. I am able to manage, negotiate and control how it is used: I can give, deny or revoke permissions to use it."
Individual as the Point of Integration	"I have access and the power to allow or disallow others to use my data A & B together for a specific purpose."
Individual Empowerment	"I am the agent of my own data as I have the tools, skills & assistance to transform my data into usable information. This leads to better decisions and improves my life."
Portability: Access and Re-Use	"I can obtain, move and re-use my own data across different services. I can use my data as I want or enable others to use it for my purposes. I do not fear that my data can be locked somewhere where I cannot access it."
Transparency & Accountability	"I can track the use of my data and hold accountable those using it. I understand how my data is used in services: for decisions, transactions or other purposes."
Interoperability	"I experience services seamlessly, regardless if they are from different providers."

Source: MyData, https://mydata.org/participate/declaration/

Equally interesting is that they have used the MyData principles as guidelines to give the person sharing their data full empowerment.

In comparison to SIDE-CIC a worker centric approach is worth investigating in parallel with other angles since it gives another aspect to the challenges we are facing.

11.1.4 Consent management

DS4SKILLS have also resolved the personal data protection issue by introducing 3rd party Personal Data Intermediaries (PDIs) to handle the consent management between the individual user and the stakeholders. The role of the PDI is explained as follows:

"PDIs are a guarantee of trust and neutrality in the network. They don't process or provide services on the data, so they are the best positioned to help people control their data as they have no conflict of interest. A data provider or a service provider is not neutral in the data space use case, a PDI acts as a trusted third party between the players. Moreover, PDIs act as the official representative of the person in the data space. This means request, exertion of rights or consents coming from them are coming from the person which gives the person a great tool to truly control their data. Finally, the PDI will allow people to set their conditions and preferences on the use of their data, to be applied the whole data space."

Link to the consent management descriptions: https://dataspace.prometheus-x.org/building-blocks/consent.

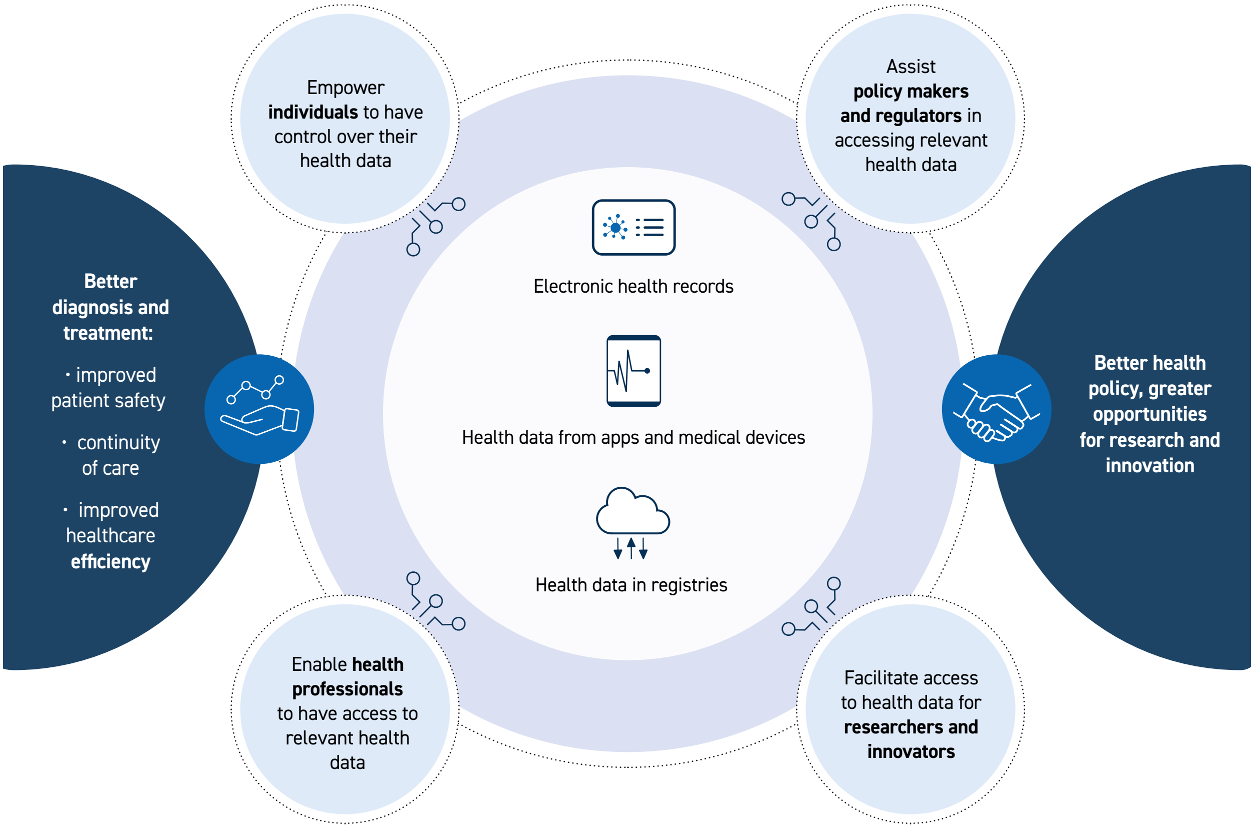
11.2 OTHER APPLICABLE DATA SPACES AND INITIATIVES

11.2.1 The European Health Data Space (EHDS)

The European Health Data Space (EHDS, https://www.european-health-data-space.com/) is a Data Space that aims at providing sharing of personal health data to the needed stakeholders to be able to better deal with health issues both in preventive and care aspects. The description on the site is as follows.

The European Health Data Space is a health specific ecosystem comprised of rules, common standards and practices, infrastructures and a governance framework that aims at:

Graphic 34 EHDS functions and benefits


Empower **individuals** to have control over their health data
Assist **policy makers and regulators** in accessing relevant health data
Better diagnosis and treatment:
· improved patient safety
· continuity of care
· improved healthcare efficiency
Electronic health records
Health data from apps and medical devices
Health data in registries
Better health policy, greater opportunities for research and innovation
Enable **health professionals** to have access to relevant health data
Facilitate access to health data for **researchers and innovators**

Source: EHDS, https://www.european-health-data-space.com/

1. Empowering individuals through increased digital access to and control of their electronic personal health data, at national level and EU-wide.

2. Fostering a single market for electronic health record systems, relevant medical devices and high-risk AI systems.

3. Providing a trustworthy and efficient set-up for the use of health data for research, innovation, policy-making and regulatory activities (secondary use of data).

The European Health Data Space is a key pillar of the European Health Union. It builds further on the General Data Protection Regulation (GDPR) and the NIS 2 Directive.

The European Union is building a strong European Health Union, in which all EU countries prepare and respond to health crises, have available, affordable, innovative and adequate medical supplies and member countries work together to improve prevention, treatment and aftercare for diseases.

The COVID-19 pandemic shows the importance of coordination among European countries to protect health, both during a crisis and in normal times. The European Health Union improves EU-level protection, prevention, preparedness and response against human health hazards.

To enable the EHDS a legislation was passed: (https://data.consilium.europa.eu/doc/document/PE-76-2024-INIT/en/pdf)

11.2.2 EONA-X (Tourism, Mobility and logistics Data Space)

EONA-X (https://eona-x.eu) is a French Aerospace initiative to create a cross-sector data space to provide better services and value to travellers. It is defined as follows:

At EONA-X we have decided to adopt a cross-sector approach, for we find this is a key condition to foster collaboration. We believe this should go beyond local initiatives and EONA-X thrives to operate at the European level, focusing on three interconnected fields:

- Mobility
- Transport & Logistics
- Tourism

This scope allows us to create an ecosystem that can answer to the specific challenges of these sectors, without being limited by a specific type of data, thus facilitating value creation for better efficiency or the creation of new services.

By promoting a governance at European level and interconnections with other data-sharing ecosystems, EONA-X actively contributes to the creation of Europe's Data Economy, serving mobility and tourism across Europe.

11.2.3 The Data Spaces Support Centre Blueprint 1.0

The Blueprint (https://dssc.eu/page/blueprint) provides a comprehensive package how to start, govern and provide the necessary technical components to the Data Space (Graphic 35).

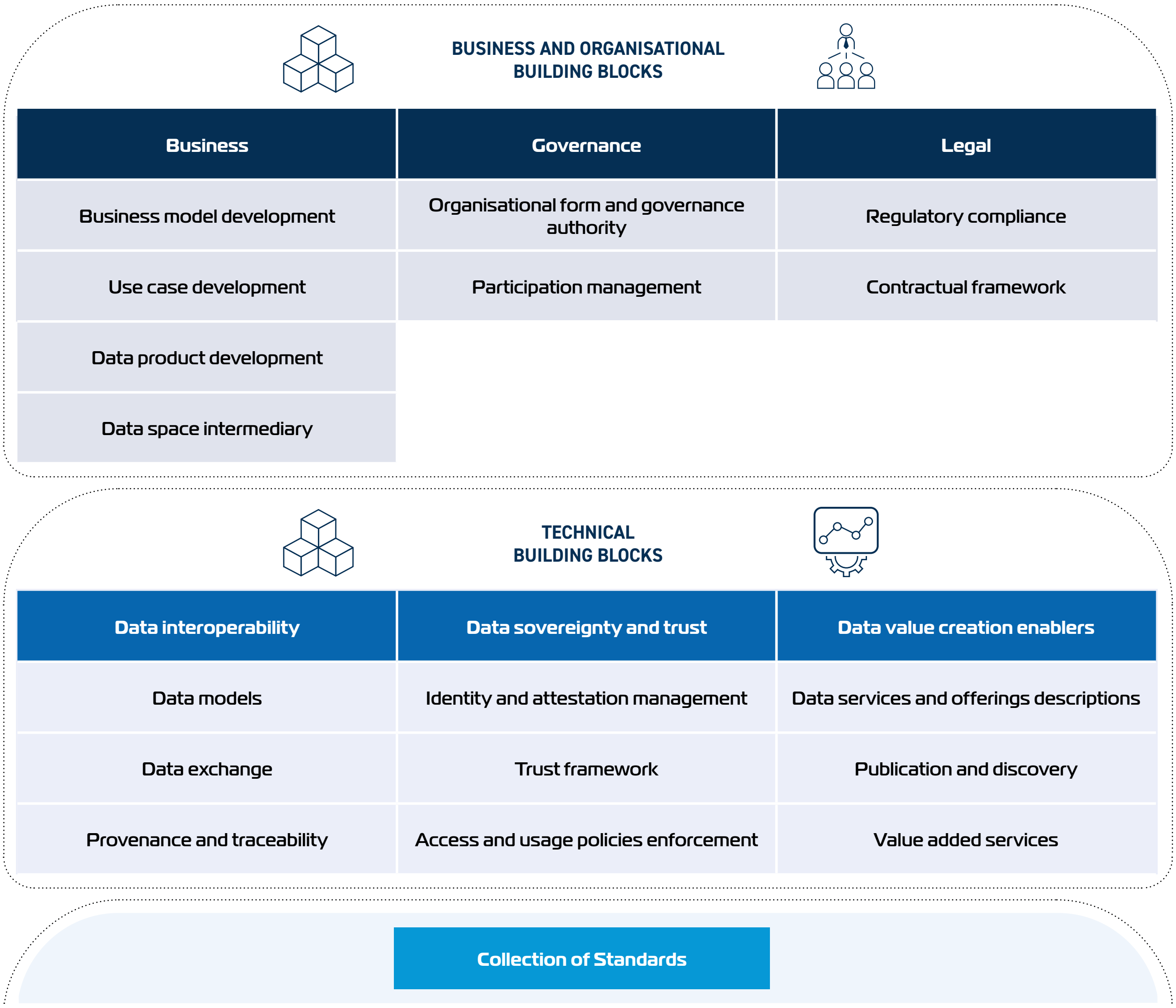
11.2.4 Data Space Protocol

The Dataspace Protocol (https://docs.internationaldataspaces.org/ids-knowledgebase/dataspace-protocol) is used in the context of Dataspaces as described and defined in the subsequent sections with the purpose to support interoperability (Graphic 36).

11.2.5 The SIMPL programme

Simpl (https://simpl-programme.ec.europa.eu/) is an open source, secure middleware that supports data access and interoperability in European data initiatives. It provides multiple compatible components, free to use, that adhere to a common standard of data quality and data sharing. A future where reliable, updated data are available across industries is possible with Simpl.

Graphic 35 DSSC blueprint building blocks



BUSINESS AND ORGANISATIONAL BUILDING BLOCKS

Business	Governance	Legal
Business model development	Organisational form and governance authority	Regulatory compliance
Use case development	Participation management	Contractual framework
Data product development		
Data space intermediary		

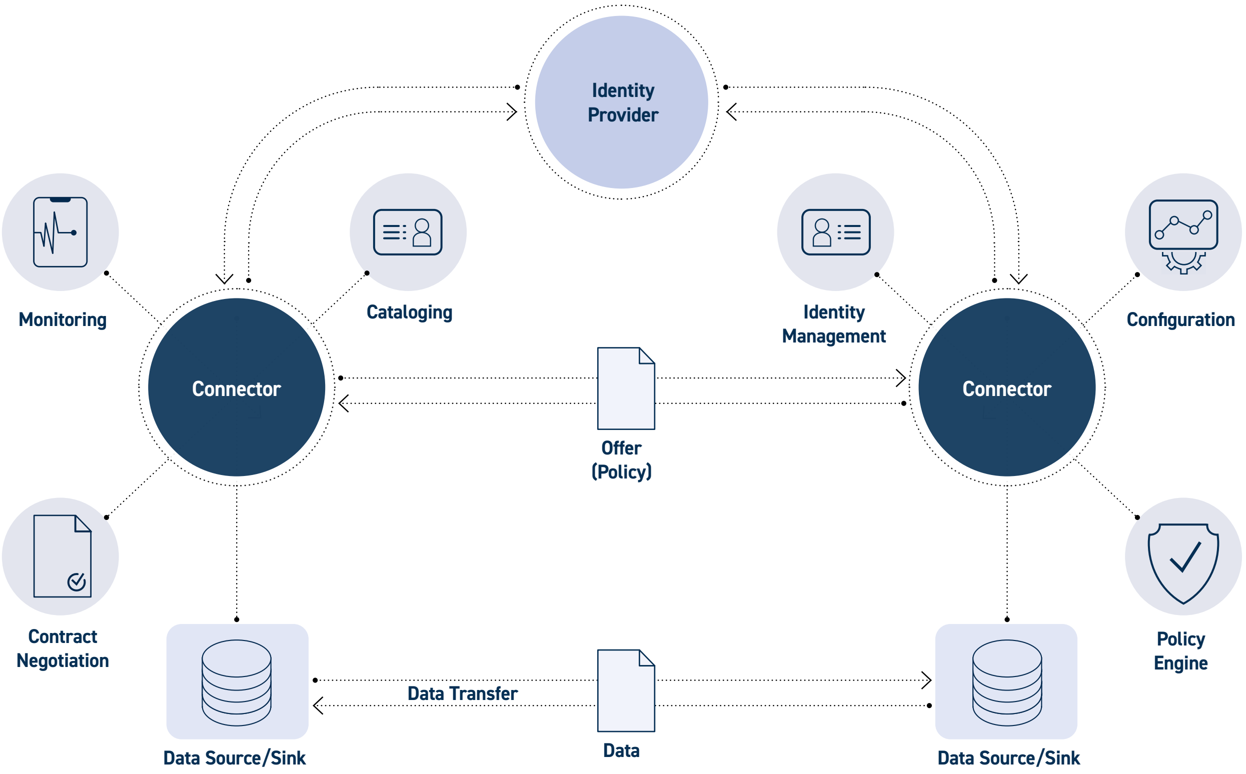
TECHNICAL BUILDING BLOCKS

Data interoperability	Data sovereignty and trust	Data value creation enablers
Data models	Identity and attestation management	Data services and offerings descriptions
Data exchange	Trust framework	Publication and discovery
Provenance and traceability	Access and usage policies enforcement	Value added services

Collection of Standards

Source: Data Space Support Centre, dssc.eu

Graphic 36 Overview of Data Space Protocol

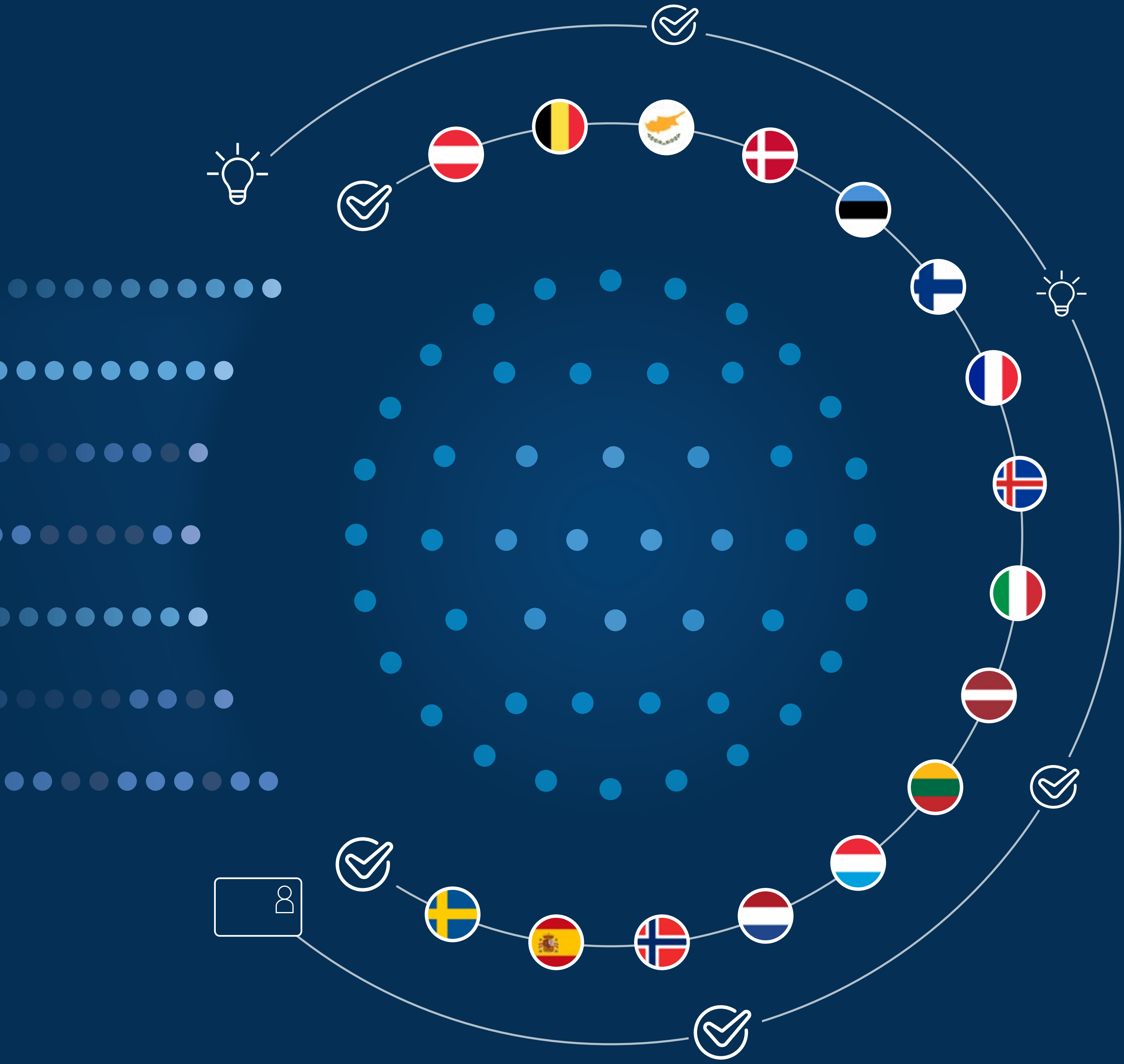


Source: IDSA, https://docs.internationaldataspaces.org/ids-knowledgebase/dataspace-protocol

11.2.6 UNFCCC's Data Exchange Standard

The UNFCCC's Data Exchange Standard (DES) sets the communication protocols—including message formats, security layers (like VPN encryption and digital signatures), reconciliation routines, and audit logging—for standardized, reliable exchange of Kyoto Protocol registry transactions (issuance, transfer, cancellation, retirement) among national and CDM registries, the Independent Transaction Log, and supplementary logs. For more information please see: https://unfccc.int/sites/default/files/data_exchange_standards_for_registry_systems_under_the_kyoto_protocol.pdf.

12 Conclusions



The conclusions by the technical team of the mapping, feasibility and recommendation phases in the SIDE-CIC project can be summarised as follows.

There is an ever-increasing need to find effective solutions for managing Social ID-related information, particularly concerning the mobile workforce originating from other EU Member States or third countries. Currently, the industry and its associated stakeholders operate in a fragmented and siloed manner, which significantly hampers the efficient use of essential information. To address this, cooperation among stakeholders, both in terms of data exchange and the development of joint solutions, is clearly necessary.

A mapping of the existing Social ID services across the Member States reveals notable differences in their mandates, issuing authorities, and technical implementations. While many countries are planning to introduce Social ID cards, they face challenges in generating sufficient momentum due to limited support from local authorities and stakeholders. Despite these hurdles, there is a growing interest among existing and planned Social ID service providers to explore potential cooperation, especially around data exchange and interoperability with relevant authorities within their ecosystems.

From a feasibility perspective, creating individual Social ID card data profiles at the Member State level—which can be both issued and consumed—makes cross-border cooperation possible, even in light of varying data maturity levels and technical infrastructures. Existing data exchange models can be reused for this initiative; the key lies in managing these proposed data profiles and establishing trust levels through appropriate, tailored processes. A central decision will need to be made regarding whether a centralized or decentralized approach should be pursued. Encouragingly, the technical capabilities required to achieve the necessary interoperability are not difficult to develop.

Upon examining all areas of feasibility, it can be concluded that the creation of a dedicated Data Space for the SIDE-CIC initiative is indeed achievable. However, certain legal and organizational challenges remain, particularly in ensuring that Member State Social ID card services are granted the mandate required to participate in the Data Space and contribute to its broader ecosystem. It is also worth noting that the creation of a Data Space carries both a development investment and running costs. The costs of doing nothing is also substantial as it creates indirect costs for all parties involved resulting from administrative burden and effects of fraud.

There are identifiable obstacles and risks associated with the creation of such a Data Space. These challenges can be overcome if stakeholders recognize the mutual benefits of collaboration and data sharing. The most significant initial risk is the potential lack of founding members who are both willing and authorized by their decision-makers to support the formation of the Data Space. A related long-term risk is the absence of mandate for some of the planned Social ID Card solutions, which could hinder the scalability of the Data Space. Furthermore, the successful deployment of key enabling components—such as European Digital Credentials—is critical. If these components are not implemented as planned within the Member States, integrated solutions like ESSPASS may become infeasible.

In terms of benchmarking, Data Spaces are already being adopted across various industries, with substantial EU investment directed at supporting such initiatives. This support includes dedicated centers offering blueprints, governance frameworks, agreement templates, reference architectures, and technical components. A particular challenge within Data Spaces involving personal information is ensuring compliance with GDPR. This is typically addressed through the use of Personal Data Intermediaries and consent management tools. Initiatives like Gaia-X and the EU-funded Data Space Support Center offer a robust platform and network of peers, which can be leveraged to pilot data exchange between SIDE-CIC stakeholders.

Based on the Technical Team study there are no major common technical challenges. The obstacles and challenges noted can be overcome if all stakeholders commit to collaboration and take a practical, step-by-step approach guided by a shared desired state vision.

APPENDIX: List of interviews

Interviews with countries having and operative Social ID Card

- Austria, ISHAP
- Belgium, Constructiv
- Estonia, Estonian Tax and Customs Board
- Finland, Vastuu Group
- France, CIBTP
- Lithuania, STATREG
- Norway, HMS
- Sweden, ID06

Interviews with countries planning a Social ID Card

- Iceland, VMST, Fagfelogin and Rafis
- Italy, CISL
- The Netherlands, FNV
- Romania, FGS

Expert interviews – Ecosystems, Networks and Data Spaces

- Aalto University
- 1001 Lakes Ltd.
- Centre for Knowledge and Innovation Research (Aalto University)
- Ministry of Finance – MiniFinland
- Finnish Tax Administration
- Nordic Data Exchange
- GAIA-X

Expert interviews – EU Commission

- DG EMPL
- ELA
- DC4EU

EUROPEAN
FEDERATION
OF BUILDING AND
WOODWORKERS

FIEC
EUROPEAN CONSTRUCTION
INDUSTRY FEDERATION