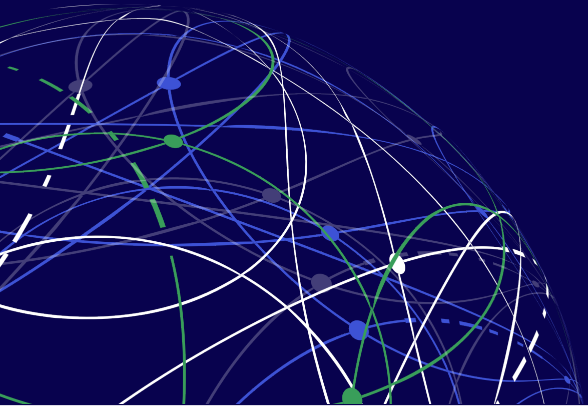
Harmonisation Canvas

DATA SHARING COALITION



DATA SHARING COALITION

Penholder document
INNOPAY

Release
Version 0.5

Date
18 December 2020

Versioning

Version	Date	Comments
Version 0.1	28 September 2020	Initial version
Version 0.3	16 November 2020	Processed feedback of Expert Group on v0.1 Added topics: Legal context & information security
Version 0.5	18 December 2020	Processed feedback of Expert Group on v0.3 Added topics: Data Service Exchange, Operational Agreements, Business Models, Governance, Data Standards & Metadata

Table of Contents

Versioning **2**

Section A. Introduction **6**

1 Reading guide **6**

1.1 About this document 6

1.2 Intended audience 6

1.3 Typography 6

1.4 Glossary 7

2 Context **10**

2.1 About the DSC 10

2.2 About the Harmonisation Canvas 10

2.3 Related documents 11

2.4 About the future Cross-Domain Trust Framework 12

2.5 Next steps 14

3 Guiding principles **15**

3.1 Future proof 15

3.2 Trustworthy 15

3.3 Inclusive 16

3.4 As generic as possible, as specific as needed 16

3.5 Cost-efficient 17

4 Interoperability and harmonisation **18**

4.1 Data sharing 18

4.2 Interoperability and Harmonisation 20

4.3 The Proxy Model 21

Section B: Harmonisation topics **25**

5 Terms and conditions **25**

5.1 Introduction 25

5.2 Relevance 25

5.3 Description 26

6 Identification, Authentication and Authorisation **30**

6.1 Introduction 30

6.2 Relevance 30

6.3 Description 32

7 Legal context 42

7.1 Introduction 42

7.2 Relevance 42

7.3 Description 42

8 Information Security 47

8.1 Introduction 47

8.2 Relevance 48

8.3 Description 48

9 Data Service Exchange 51

9.1 Introduction 51

9.2 Relevance 51

9.3 Description 51

10 Operational Agreements 55

10.1 Introduction 55

10.2 Relevance 55

10.3 Description 55

11 Business Models 58

11.1 Introduction 58

11.2 Relevance 58

11.3 Description 58

12 Governance 61

12.1 Introduction 61

12.2 Relevance 61

12.3 Description 61

13 Data Standards 64

13.1 Introduction 64

13.2 Relevance 64

13.3 Description 65

14 Metadata 66

14.1 Introduction 66

14.2 Relevance 66

14.3 Description 68

15 Manifestation of topics in the Trust Framework 70
15.1 Terms and conditions 70
15.2 Identification, Authentication and Authorisation........ 70
15.3 Legal Context........ 71
15.4 Information Security 71
15.5 Data Service Exchange 71
15.6 Operational Agreements 72
15.7 Business Models........72
15.8 Governance 72
15.9 Data Standards........73
15.10 Metadata 73
Section C. Appendix 74
16 Data Sharing Coalition Overview 74
17 Interoperability and harmonisation 75
17.1 Steps to reach a data service transaction agreement........75
18 Terms and Conditions 76
18.1 Terms and Conditions in DSC use cases 76
18.2 Initial Policy clusters and examples of Policies........77
19 Data Service Discovery........ 79
19.1 Industry standards for Service Discovery........79
19.2 Data service discovery in the proxy model........81

Section A. Introduction

This section provides context on the purpose of the DATA SHARING COALITION and this document, as well as information on how to interpret this document.

1 Reading guide

1.1 About this document

This document is the HARMONISATION CANVAS, which presents the findings of an initial exploration of topics related to enable data sharing across domains. This exploration was conducted as a collaborative effort by participants of the DATA SHARING COALITION (DSC). The main purpose of the HARMONISATION CANVAS is to provide the basis for the development of the future CROSS-DOMAIN TRUST FRAMEWORK. See chapter 2.2 for more details.

1.2 Intended audience

People and organisations that are a stakeholder in the development of the future TRUST FRAMEWORK are the main audience of this document.

However, as a standalone document, the HARMONISATION CANVAS can also provide interesting insights for:

- Participants of and people interested in the DATA SHARING COALITION in general,,
- People interested in what is required to facilitate (cross-sectoral) data sharing
- DATA SHARING DOMAINS that want to learn how to become interoperable with other DATA SHARING DOMAINS.

1.3 Typography

From this paragraph onwards, the typography in this document follows the following rules:

- Regular text appears like this,
- DEFINED TERMS FROM THE GLOSSARY APPEAR LIKE THIS,
- *References to other documents appear like this.*

Additional context given to content written in the document appears like this

Boxes: are used to give examples and extension on certain content

1.4 Glossary

Table 1: Glossary

Glossary item	Definition
Obligations and Advice	Policies that are assessed and enforced after the establishment of a Data Service Agreement, on what must be carried out after a data service is approved. Advice is similar to obligation with the difference that enforcement of the advice is not mandatory
Access Control Rules	Policies that are assessed and enforced prior to the establishment of a Data Service Agreement, which regulate how Data services can be accessed
Authentication	The process where the validity of a claimed identity is verified
Authorisation	The permissions or rights of an actor (humans, machines, proxies, etc.) to perform an action
Data Service	Any service offered by a Data service Provider aimed at exchanging or processing data (for example, this includes basic data services such as data pull, data push, bringing an algorithm to the data as well as complex use cases based on combinations of these basic types)
Data Service consumer	The actor that makes use of a Data service offered by the Data service provider
Data Service Discovery	The mechanism through which a Data Service Consumer and Data Service Provider can find each other across Domains
Data Service provider	The actor that offers a Data service to the Data service consumer
Data Service Transaction	The event of executing a Data Service between Data Service Provider and Data Service Consumer. Depending on the type of Data Service the Data Service Transaction can be a single moment or take place for a length of time.
Data Service Transaction agreement	The agreement (handshake) between a Data service consumer and Data service provider to enable trust and accept the terms on which the Data service transaction can take place
Data Sharing	The act of exchanging data through a Data service Transaction between a Data service provider and a Data service consumer
Data Sharing Coalition (DSC)	A collaborative initiative that aims to enable organisations to easily share data across Domains

Glossary item	Definition
DATA SHARING INITIATIVE	Organisation that enables DATA SHARING in a certain DOMAIN by providing a coherent set of specifications and requirements and by providing supervision
DATA STANDARDS	provide the semantics, structure and formatting of data
DELEGATION	The provision of explicit rights (to perform an action) to a third party
DOMAIN	Flexibly defined as any number organisations collaboratively working together to share data to achieve a shared purpose
DISPUTE	When actors within the TRUST FRAMEWORK cannot settle disagreements between them according to specific service level agreements
DISPUTE MANAGEMENT	The process of managing disputes when they have been reported to the TRUST FRAMEWORK AUTHORITY
GUIDING PRINCIPLE	A principle that gives direction in the decision-making process of establishing and maintaining the content of the HARMONISATION CANVAS
GOVERNANCE	The management and maintenance of the TRUST FRAMEWORK agreements and network
GOVERNING BODY	The entity managing the GOVERNANCE structure of the future TRUST FRAMEWORK
HARMONISATION	Establishing common agreements, standards and requirements between actors to enable DATA SHARING between them
HARMONISATION CANVAS	This document
HARMONISATION DOMAIN	Network of PROXIES
IDENTIFICATION	The process of claiming an identity by a subject or the process of attributing/issuing an identity to a subject by an authority
IMPLIED REGULATION AND AGREEMENTS	Regulation and agreements that hold, but that is not explicitly stated in documentation such as agreement documentation and METADATA
INFORMATION SECURITY	Preservation of the confidentiality, integrity and availability of information though the implementation of technical or organisational information security measures
INITIATIVE	Synonym for DATA SHARING INITIATIVE

Glossary item	Definition
Interoperability	The ability of systems of different actors, adhering to different standards and agreements, to exchange data in a meaningful way that is mutually understandable and satisfactory
Metadata	Describes everything about data, Data Services, and Data Service Transactions in Data Sharing that cannot be assumed to be known
Policies	Define rules for access to and usage of Data Services, can be split into Access control rules and Obligation and Advice. Terms and conditions are formalised into Policies
Proxy model	Solution for multilateral Interoperability across Domains where different Data Sharing Domains implement Proxies. The DSC will initially use this model for implementation of the Cross-Domain Trust Framework
Proxy	A module that translates between specifications and requirements from a data sharing Domain and Harmonised specifications and requirements (and vice versa) in order to achieve Interoperability and trust across Domains
Scheme	Synonym for Trust Framework
Service Registry	Contains necessary Data Service information to perform Data Service Discovery. Can be considered similar to a telephone book
Terms and Conditions	Define the concepts as well as the duties and rights, the powers and liabilities that apply to the actors engaged in data service transactions
Trust	A situation between actors where (perceived) risks are sufficiently reduced in order to enable data sharing. The amount of risk deemed as acceptably low is determined by each actor themselves and therefore varies between actors
Trust Framework	Enables many-to-many data sharing though business, legal, operational, functional and technical agreements, tools and processes which facilitate cross domain data sharing
Trust Framework Governance	Needed to develop, manage and maintain the Trust Framework agreements and network

2 Context

2.1 About the DSC

The Data Sharing Coalition (DSC) is an open and growing, international initiative in which a large variety of organisations collaborate to unlock the value of Cross-domain data sharing. The DSC aims to drive Cross-domain Data sharing, by enabling Interoperability between Domains, thereby strengthening each Domain.

The coalition started in January 2020 and is facilitated by the Dutch Ministry of Economic Affairs and Climate policy. The expected lifespan of the project phase of the coalition is until 2025. By 2025, the Data Sharing Coalition is expected to have transferred its activities to an entity that operates and governs any future frameworks and facilities developed by the DSC. The first and current phase of the Data Sharing Coalition is a feasibility study into the Harmonisation potential to enable Cross-Domain Data sharing. For more information on the Data Sharing Coalition, visit: www.datasharingcoalition.eu

2.2 About the Harmonisation Canvas

The Harmonisation Canvas, this document, provides the foundation for the future *Cross-Domain Trust Framework* and is the main deliverable of the first phase of the Data Sharing Coalition that will run until Q2 2021. This is part of the feasibility study researching the potential for Cross-Domain Data sharing.

The main goal of the Harmonisation Canvas is to serve as a first steppingstone for the further research into and development of common agreements between Domains. The statements and findings presented in this document will provide guidance for future work of the DSC, but do not yet represent any binding agreements or requirements for future frameworks or other deliverables of the DSC. Further, due to the document's goals, the Harmonisation Canvas aims to give an indication of topics and their implication but does not aim to be exhaustive or to complete the detailing of these topics.

The Harmonisation Canvas captures the results of a collaborative exploration of what type of common agreements are required to achieve Interoperability across Domains. This includes determining the topics that require common agreements to achieve interoperability, the extent to which agreements are necessary for these topics and the gathering of best practices with regard to these future agreements.

The content of the Harmonisation Canvas is a product of several activities of (participants of) the Data Sharing Coalition. There are three main sources of input: Use cases, analysis of existing Data Sharing Initiatives and expert input. All three sources of input are combined and discussed in the Expert Group of the Data Sharing Coalition. This varied group of experts from different participants of the DSC meets regularly to discuss the contents of the Harmonisation Canvas. Together, through extensive discussions, collaborative research and knowledge sharing, they deliver input on what should be included in the Harmonisation Canvas.

The three sources of input are:

- Use cases: The DATA SHARING COALITION supports the realisation of five cross-sectoral use cases of DATA SHARING[1]. In these use cases, the aim is to realise INTEROPERABILITY across DOMAINS in a specific context. This provides practical insights into requirements for HARMONISATION across DOMAINS. Although INTEROPERABILITY requirements might be use case specific, the learnings from this use case will be generalised to fit a more generic context, before being included in the HARMONISATION CANVAS.

- Expert input: For each topic, experts that are delegated by DSC participants provide input on their view of what is helpful to include in the Harmonisation Canvas. This can range from a recommendation of a certain market standard to input on the scope of future agreements or input for defining common concepts. See Table 9 for an overview of the experts who contributed to this document.

- Analysis of existing DATA SHARING INITIATIVES: The DSC project team analyses how DATA SHARING INITIATIVES that are participating in the DSC are designed in relation to certain topics (e.g. requirements on identity proofing, standards used for METADATA, etc.). This provides insights into the setup of different DATA SHARING INITIATIVES and therefore what is required for INTEROPERABILITY between these DATA SHARING INITIATIVES and DOMAINS in general.

2.3 Related documents

This HARMONISATION CANVAS is related to a number of other documents within the DATA SHARING COALITION. Figure 1 shows these relationships, and Table 2 gives an overview of the other documents and their status. The HARMONISATION CANVAS will provide input for two future documents, the DATA SHARING COALITION Blueprint and the CROSS-DOMAIN TRUST FRAMEWORK.

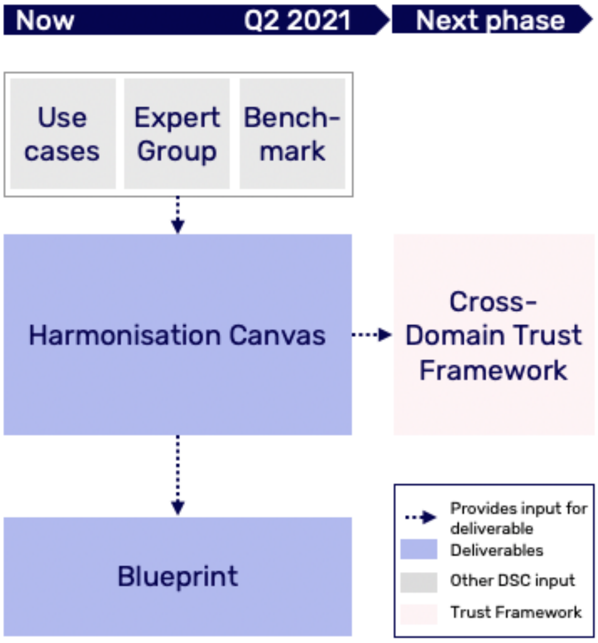


Figure 1: Relationship of the Harmonisation Canvas with other documents

[1] https://datasharingcoalition.eu/use-cases/

Table 2: Overview of documents related to the Harmonisation Canvas

Document	Description	Status
Data Sharing Coalition *Blueprint*	The blueprint is a checklist of BLOFT topics (see Box 1) for data sharing and is based on elements and insights from the Harmonisation Canvas. It will inform, inspire and accelerate new and existing Data Sharing Domains and support them in setting up data sharing activities.	To be included in the first phase of the DSC, to be completed by Q2 2021
(Cross-Domain) Trust Framework	A document that captures all Harmonisation agreements in the Data Sharing Coalition. This set of agreements is to be implemented by Domains in order to achieve Interoperability across Domains	To be developed in the next phase of the DSC (after Q2 2021)

2.4 About the future Cross-Domain Trust Framework

In order to enable Interoperability between Domains, the Data Sharing Coalition will develop common, multilateral agreements on a wide range of relevant topics (e.g. digital identities, legal context, Metadata, etc.). Domains which implement and adhere to these multilateral agreements become Interoperable with each other. This enables Domains to facilitate their participants in sharing data with minimal efforts with actors from other Domains that have also agreed to adhere to these multilateral agreements.

The common agreements that will be made by the Data Sharing Coalition will be captured in one comprehensive document, the future *Cross-Domain Trust Framework*. The document will specify agreements and requirements that Domains should adhere to, divided across five disciplines: Business, Legal, Operational, Functional and Technical (BLOFT), see Box 1 for an overview of the BLOFT model and included topics. An indicative overview of the contents and structure of the future *Cross-Domain Trust Framework* can be found in Figure 2.

Note: More detail on the expected contents of the future Cross-Domain Trust Framework will be included at a later stage, as the development of the Harmonisation Canvas will provide more insights into this

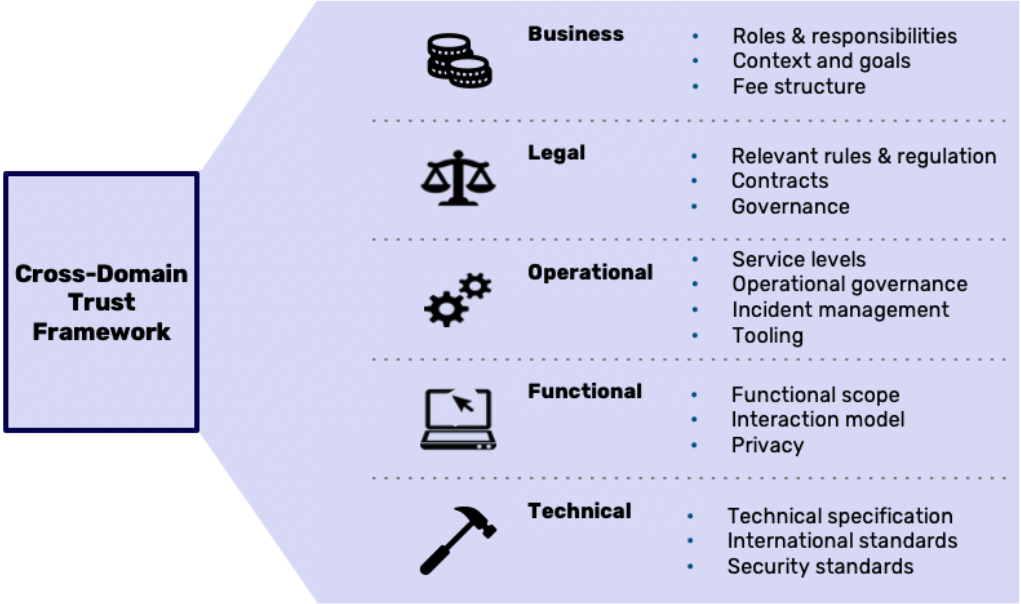
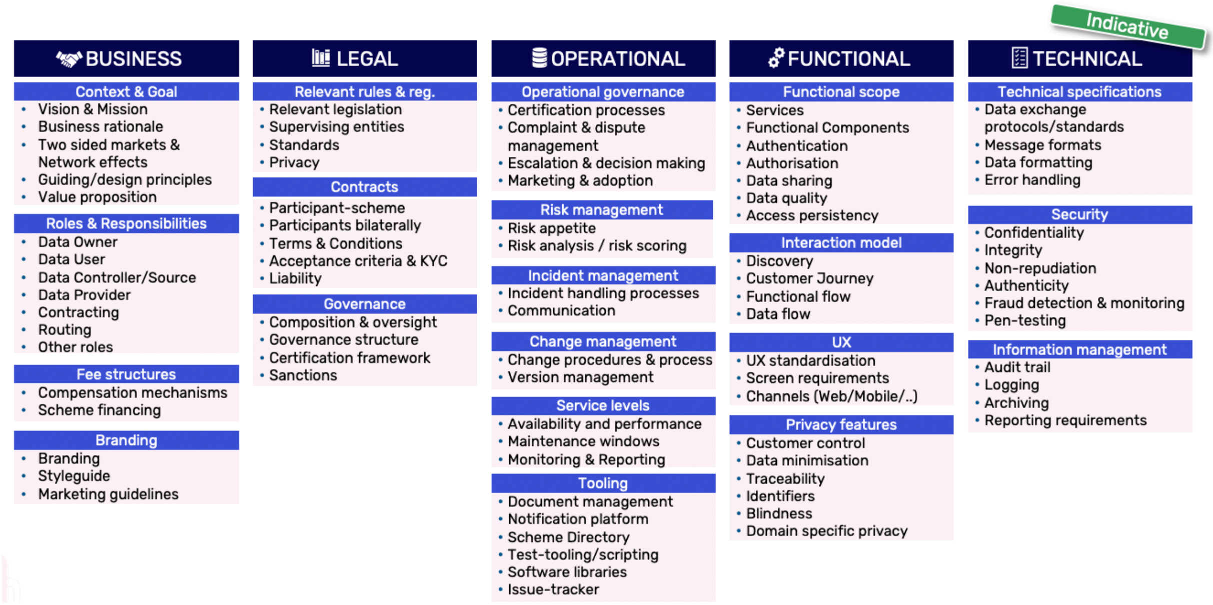


Figure 2: Preliminary content and structure of the future Cross-Domain Trust Framework

Box 1: Complete BLOFT Framework

The BLOFT model has been developed based on experience in the creation of trust frameworks in the past. It contains an extensive list of topics that together form a starting point to create a blueprint for a trust framework. See Figure 3 for a high-level overview of the topics included within the model.



Indicative

BUSINESS

Context & Goal
- Vision & Mission
- Business rationale
- Two sided markets & Network effects
- Guiding/design principles
- Value proposition

Roles & Responsibilities
- Data Owner
- Data User
- Data Controller/Source
- Data Provider
- Contracting
- Routing
- Other roles

Fee structures
- Compensation mechanisms
- Scheme financing

Branding
- Branding
- Styleguide
- Marketing guidelines

LEGAL

Relevant rules & reg.
- Relevant legislation
- Supervising entities
- Standards
- Privacy

Contracts
- Participant-scheme
- Participants bilaterally
- Terms & Conditions
- Acceptance criteria & KYC
- Liability

Governance
- Composition & oversight
- Governance structure
- Certification framework
- Sanctions

OPERATIONAL

Operational governance
- Certification processes
- Complaint & dispute management
- Escalation & decision making
- Marketing & adoption

Risk management
- Risk appetite
- Risk analysis / risk scoring

Incident management
- Incident handling processes
- Communication

Change management
- Change procedures & process
- Version management

Service levels
- Availability and performance
- Maintenance windows
- Monitoring & Reporting

Tooling
- Document management
- Notification platform
- Scheme Directory
- Test-tooling/scripting
- Software libraries
- Issue-tracker

FUNCTIONAL

Functional scope
- Services
- Functional Components
- Authentication
- Authorisation
- Data sharing
- Data quality
- Access persistency

Interaction model
- Discovery
- Customer Journey
- Functional flow
- Data flow

UX
- UX standardisation
- Screen requirements
- Channels (Web/Mobile/..)

Privacy features
- Customer control
- Data minimisation
- Traceability
- Identifiers
- Blindness
- Domain specific privacy

TECHNICAL

Technical specifications
- Data exchange protocols/standards
- Message formats
- Data formatting
- Error handling

Security
- Confidentiality
- Integrity
- Non-repudiation
- Authenticity
- Fraud detection & monitoring
- Pen-testing

Information management
- Audit trail
- Logging
- Archiving
- Reporting requirements

Figure 3: Overview of topics in the BLOFT model

At first glance, this model gives a comprehensive overview. In practice, the separation of topics and elements is not as clear as indicated as there is overlap between topics and topics can be discussed from different perspectives. Therefore, this extensive BLOFT model is used as a starting point to ensure diverse topics are discussed within this phase of the Data Sharing Coalition, but deviations may be implemented as needed.

2.5 Next steps

In the next phase of the DATA SHARING COALITION, this HARMONISATION CANVAS will act as input for the development of the CROSS-DOMAIN TRUST FRAMEWORK. This development process will require an iterative, collaborative approach with a wide range of stakeholders involved. In the future process of co-creating the CROSS-DOMAIN TRUST FRAMEWORK, the common concepts and best practices from this HARMONISATION CANVAS will be used as input and will be detailed further into concrete standards and requirements.

The exact timelines and approach of these next steps will be determined in the run up to the next phase of the DATA SHARING COALITION, which is expected to start in Q3 of 2021.

3 Guiding principles

A number of principles will be used to guide the creation of the HARMONISATION CANVAS and future CROSS-DOMAIN TRUST FRAMEWORK. They provide a basis for decision-making; however, the GUIDING PRINCIPLES are no absolute truth or hard requirements but need to be considered in the context of each decision. In no particular order, the following five principles have been identified:

- Future proof,
- Trustworthy,
- Inclusive,
- As generic as possible, as specific as needed,
- Cost-efficient.

3.1 Future proof

Statement

The CROSS-DOMAIN TRUST FRAMEWORK should be future proof and therefore extensible and non-static.

Rationale

A future proof design entails a TRUST FRAMEWORK which supports different implementations and is, to some extent, able to cater for changes in technology, user behaviour, regulation and for a growing number of DATA SERVICE TRANSACTIONS. An adaptive, extensible and non-static design enables scalability of the TRUST FRAMEWORK.

Objectives

1. Create a cooperative DOMAIN that allows participants to innovate their services.
2. Support scalable and fully INTEROPERABLE participant implementation.

3.2 Trustworthy

Statement

The TRUST FRAMEWORK should be designed and maintained in a way that establishes trust for all participants and organisations, fitting the transaction context.

Rationale

Trust is required on all levels of the Trust Framework in order to achieve wide-reaching adoption. Trust is required across DOMAINS and on a transactional level in order to facilitate CROSS-DOMAIN DATA SERVICE TRANSACTIONS.

Objectives

1. Enable TRUST between actors from different DOMAINS.
2. Ensure that data is used for authorised purposes only, as controlled by the data owner.
3. Define levels of trust dependent on a transaction context to perform a transaction.
4. Facilitate the use of required data security and privacy mechanisms.
5. Be transparent towards participants and related organisations.
6. Be transparent in process and dispute resolution.
7. Install measures/sanctions against participants and related organisations violating trust.

3.3 Inclusive

Statement

The CROSS-DOMAIN TRUST FRAMEWORK should be generic, usable and feasible to all organisations or DOMAINS, regardless of sector and DATA SHARING context.

Rationale

Inclusivity is fundamental to enabling solution independent DATA SHARING across DOMAINS and organisations. It ensures diversity by providing a level playing field and comparable opportunities for incomparable organisations. Inclusivity leads to collaborative advantages across all DOMAINS.

Objectives

1. Neutrality by ensuring a non-discriminatory approach and policies towards all organisations, users and contexts.
2. Cater for different levels of maturity of DOMAINS and their participants.
3. Create a level playing field for participants.

3.4 As generic as possible, as specific as needed

Statement

The CROSS-DOMAIN TRUST FRAMEWORK rules should be as generic as possible and as specific as needed, taking into account different transaction contexts.

Rationale

This principle is needed to keep the TRUST FRAMEWORK as lightweight as possible in order to drive adoption. It ensures that participants are not held back by restricting agreements in order to keep implementation costs low. Furthermore, it ensures a broad reach amongst sectors and types of organisations.

Objectives

1. Maximise the competitive DOMAIN by minimising the collaborative DOMAIN requirements.
2. Keep the TRUST FRAMEWORK as lightweight as possible.
3. Minimise risk of over-engineering.
4. Ensure solutions are generic to enable as many use cases as possible.

3.5 Cost-efficient

Statement

The CROSS-DOMAIN TRUST FRAMEWORK should be cost-efficient.

Rationale

Controlling costs is essential in a collaborative DOMAIN as it enables a fast and effective development. It lowers the threshold for organisations to participate and enables long-term sustainable participation.

Objectives

1. Enable cost savings at an ecosystem level, financially or in terms of effort.
2. Use proven and open standards where possible.
3. Learn from (inter)national best practices.
4. Ensure a transparent cost and benefit structure.
5. Minimise cost of entrance and impact of implementation.
6. Consider impact for participants when changes occur in the future.

4 Interoperability and harmonisation

This section presents the Coalition's initial views on the topics of the common agreements in the future Cross-Domain Trust Framework and how they could be implemented in order to achieve Interoperability across Domains. It is useful to have a preliminary idea of what the final interoperability model will look like so that topics and concepts can be discussed specifically within a practical context to avoid deeply theoretical discussions. The exact manifestation and functionality of this model will be detailed in the future *Trust Framework*

4.1 Data sharing

Data Sharing is the act of exchanging data through a Data service between a Data service provider and a Data service consumer. Data services exist in a variety of different forms. See Table 3 for a non-exhaustive overview of the basic data service types. These basic data services can be combined to realise more complex use cases. For example, a single use case can include multiple data pull services to combine data from a number of different sources. Note that data sharing through these data services can be considered as a transactional data sharing model. Therefore, the act of performing these data services can be called a Data Service Transaction. The alternative of a data publication model, where data should be available at all times for access by a Data Service Consumer, can be captured within this model as a data pull transaction.

Table 3: A non-exhaustive overview of data service types

Data Service	Description
Data Pull	The data service consumer acquires data from the data service provider so that the consumer can make use of the data
Data Push	The data service consumer pushes their data to a data service provider so that the provider can make use of the data
Algorithm Pull / Data visiting	The data service consumer requests an algorithm from the data service provider to be sent so that it can process data. The data service consumer remains in control of the data at all times
Algorithm Push / Data visiting	The data service consumer pushes an algorithm to a data service provider so that the algorithm can process the data. The data service provider remains in control of the data at all times

Table 4 presents some concrete examples of how data sharing is done/can be done in different Domains and explicitly describes who has the roles of Data service consumer and Data service provider.

Table 4: Data sharing examples

Use case		Data service type	Data service consumer	Data service provider
Tax administration	Accountants can push their client's income, VAT and profit tax data towards the tax authority such that the tax authorities, in the role of data service provider, can process tax returns automatically. The accountants push the data to the tax authority	Data Push	Accountants	Tax authority
Green Loans	A house owner wants to share data from his smart energy meter with his loan advisor and prospect loan provider so that he can obtain a loan for energy saving measures (e.g. solar panels). The loan advisor pulls the data from smart meter.	Data Pull	Intermediary (loan advisor)	DSO (Distribution System Operator)
Sharing shipment data for improved risk management	A transport carrier in the logistics sector wants to enable the sharing of actual consignment data using the e-CMR (digital waybill) with an insurer so that the claim handling process runs as smoothly as possible and the insurer is able to assess risk more accurately. The Insurer pulls the data from the e-CMR	Data Pull	Insurer	e-CMR provider
Virus Outbreak Data Network (VODAN)	A researcher in the health domain wants to analyse data owned by other research institutions to discover patterns in the current COVID-19 pandemic and potential future epidemics. The researcher pushes the algorithm to the data repository owned by a research institution	Algorithm Push	Researcher	Research institution

4.1.1 Data Service Transaction

As part of each Data Service Transaction between a Data service consumer and a Data service provider, an agreement between the parties must be established, see Figure 4 (See Appendix 17.1 for the steps to reach a Data service transaction agreement). This Data Service Transaction Agreement is specific to the transaction context and can be considered a handshake between the actors to confirm trust and the mutual acceptance of the specific Terms and Conditions under which the Data Service Transaction takes place. In addition to the characteristics of the Data Service itself, many topics are relevant for the Data Service Transaction Agreement including, but not limited to: Identification, Authentication & Authorisation, Terms and Conditions, legal context, and security aspects. See Section B: Harmonisation topics, for further details about each topic. Coming to an agreement regarding this wide variety of topics is a complex and time-consuming process between organisations.

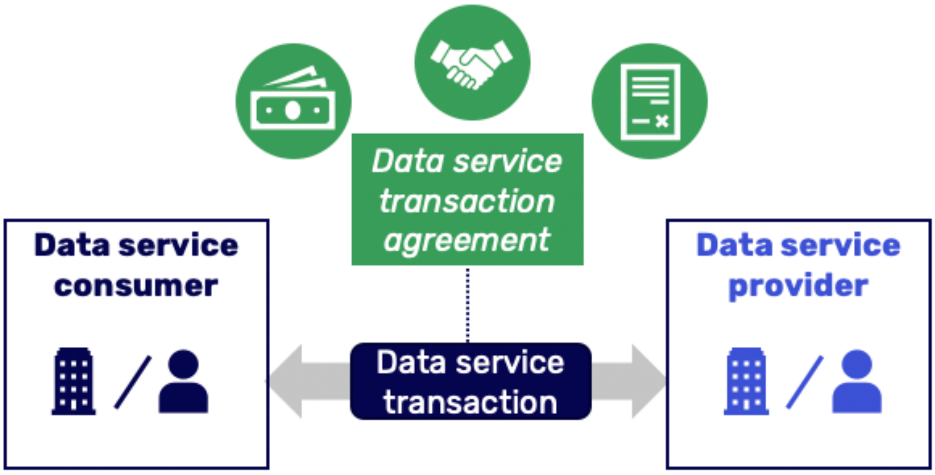


Figure 4: Overview of a Data service, including the DATA SERVICE TRANSACTION AGREEMENT

4.2 Interoperability and Harmonisation

Whenever organisations collaborate, they can make agreements with each other as they see fit to facilitate this collaboration. Within the context of the Data Sharing Coalition, a DOMAIN is flexibly defined as any number of organisations collaboratively working together to share data to achieve a shared purpose. Examples include, but are not limited to:

- An initiative (e.g. a scheme or platform) which facilitates data sharing between 100+ participant organisations,
- Organisations which share data due to legal requirements, (e.g. sharing financial data under PSD2),
- A small number of organisations which bilaterally share data with each other based on proprietary standards.

The DATA SHARING COALITION aims to also enable DATA SERVICE TRANSACTIONS across DOMAINS between actors that are part of different DOMAINS and despite of the fact not all agreements between the Domains have been harmonised. This is enabled by a concept known as INTEROPERABILITY; *"The ability of systems of different actors, adhering to different standards and agreements, to exchange data in a way that is mutually satisfactory".* There are multiple approaches to achieve INTEROPERABILITY.

In theory, full HARMONISATION of DOMAINS is the ideal solution to enable data sharing across DOMAINS. In essence, this forms a new overarching DOMAIN to faciliate DATA SHARING. This means that existing DATA SHARING INITIATIVES adjust their own requirements and implementations to follow a common, cross-DOMAIN design. However, HARMONISATION across INITIATIVES would impact all current INITIATIVE participants as they would need to adjust existing implementations which worked well in the isolated context of their own DOMAIN, requiring significant investments. Given the impact (in effort and cost) it would have on their participants, immediate adoption of fully harmonised agreements by individual INITIATIVES will most likely be limited.

Another option that does not require full HARMONISATION of all DOMAINS, is that individual organisations organise their own CROSS-DOMAIN INTEROPERABILITY for their use cases. For this, they would need bilateral agreements with organisations from another DOMAIN and define and implement their own interoperable requirements. Such bilateral agreements will allow their single use case for CROSS-DOMAIN DATA SHARING but are dependent on individual participants implementing specific harmonised solutions and will therefore limit large scale CROSS-DOMAIN DATA SHARING.

Therefore, the DATA SHARING COALITION initially aims for INTEROPERABILITY between DOMAINS instead of full HARMONISATION. In order to enable CROSS-DOMAIN INTEROPERABILITY, new agreements that hold between DOMAINS should be defined. This will enable a DATA SERVICE PROVIDER in one DOMAIN to provide a DATA SERVICE to a DATA SERVICE CONSUMER in another DOMAIN, while limiting impact for both DATA SERVICE PROVIDER and DATA SERVICE CONSUMER.

In order to enable CROSS-DOMAIN DATA SHARING and reduce the impact on existing INITIATIVES and their participants, the DSC foresees a new role: a PROXY. The role of a PROXY is to absorb the complexity of INTEROPERABILITY for the existing INITIATIVES and participants as much as possible. by implementing all INTEROPERABILITY.

4.3 The Proxy Model

The proxy model is the working hypothesis for a model to solve cross-domain interoperability. Its exact functionalities are not specifically defined yet and are subject to change

A more practical solution to enable many-to-many INTEROPERABILITY across DOMAINS is for each DOMAIN to implement PROXIES. PROXIES are modules which are to be used by every DOMAIN with the function of translating between DOMAIN specific specifications and common, HARMONISED specifications.

The main functionality of the PROXIES is to translate DOMAIN specific transactions to their harmonised equivalents:

- PROXIES will translate DOMAIN specific language to a harmonised language in the HARMONISATION DOMAIN to enable multilateral INTEROPERABILITY,
- PROXIES will facilitate trust across DOMAINS by conforming to the rules and agreements of the future TRUST FRAMEWORK,
- PROXIES will make use of compatible technical standards that enable communication between PROXIES,
- PROXIES will enable the discovery of Data Services across DOMAINS.

The PROXIES implemented by all DOMAINS form a network, the HARMONISATION DOMAIN, which enables each DOMAIN to share data effortlessly with other DOMAINS. The PROXY network will facilitate an INTEROPERABLE transaction capability and a common understanding on concepts like data and trust across DOMAINS. The future CROSS-DOMAIN TRUST FRAMEWORK will define the common agreements on the setup of these PROXIES.

Note that this many-to-many Proxy model solution does not exclude further bilateral agreements and technical implementations between DOMAINS. However, as this is not scalable, it shall not be included within the future TRUST FRAMEWORK.

Individual DOMAINS are responsible for implementation of a PROXY which adheres to the CROSS-DOMAIN TRUST FRAMEWORK. Although DOMAINS remain responsible and liable for the correct operations of their PROXY, they could outsource the development, maintenance and operation of the PROXY to a service provider. Figure 5 shows a visual representation of the PROXY MODEL.

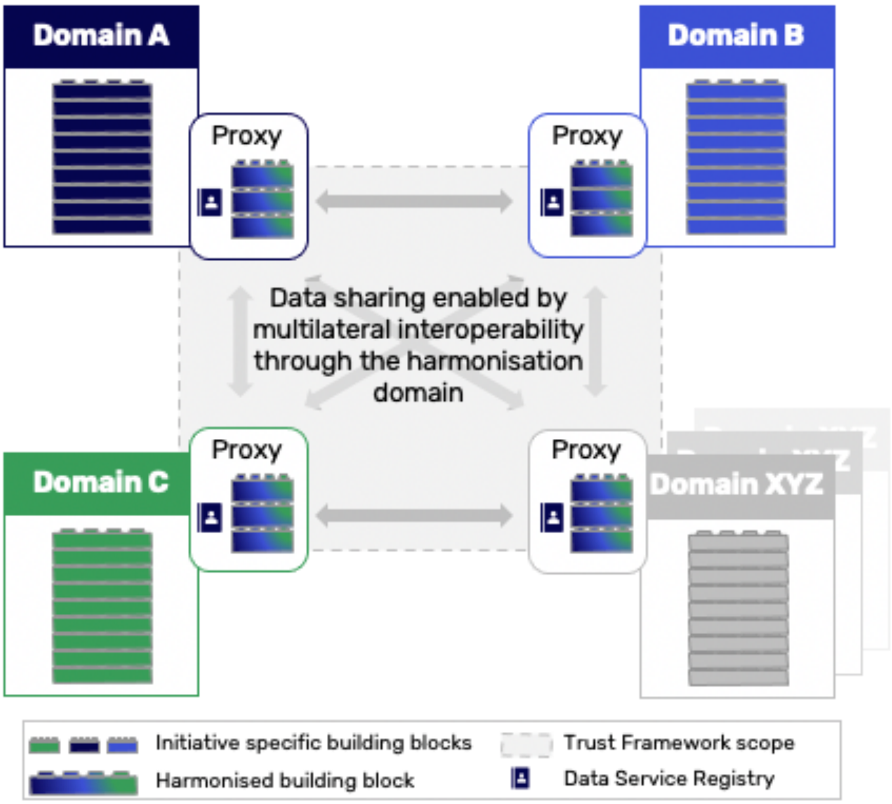

Domain A
Domain B
Proxy
Proxy
Data sharing enabled by multilateral interoperability through the harmonisation domain
Proxy
Proxy
Domain C
Domain XYZ
Initiative specific building blocks
Trust Framework scope
Harmonised building block
Data Service Registry

Figure 5: Visual representation Proxy Model

Similar uses of PROXIES to enable CROSS-DOMAIN INTEROPERABILITY are already applied at scale in multiple contexts, see Box 1 for an example in the use of proxies in eIDAS. However, a PROXY MODEL is no silver bullet. Whether data will be shared across DOMAINS will always depend on case specifics and decisions made by individual participants.

Box 1: Proxying in eIDAS

The eIDAS-nodes, formerly known as 'Pan European Proxy Server' (PEPS) are an implementation of proxies used to enable Interoperability of digital identities across EU member states. Figure 6 shows how eIDAS Nodes are used between two member states.

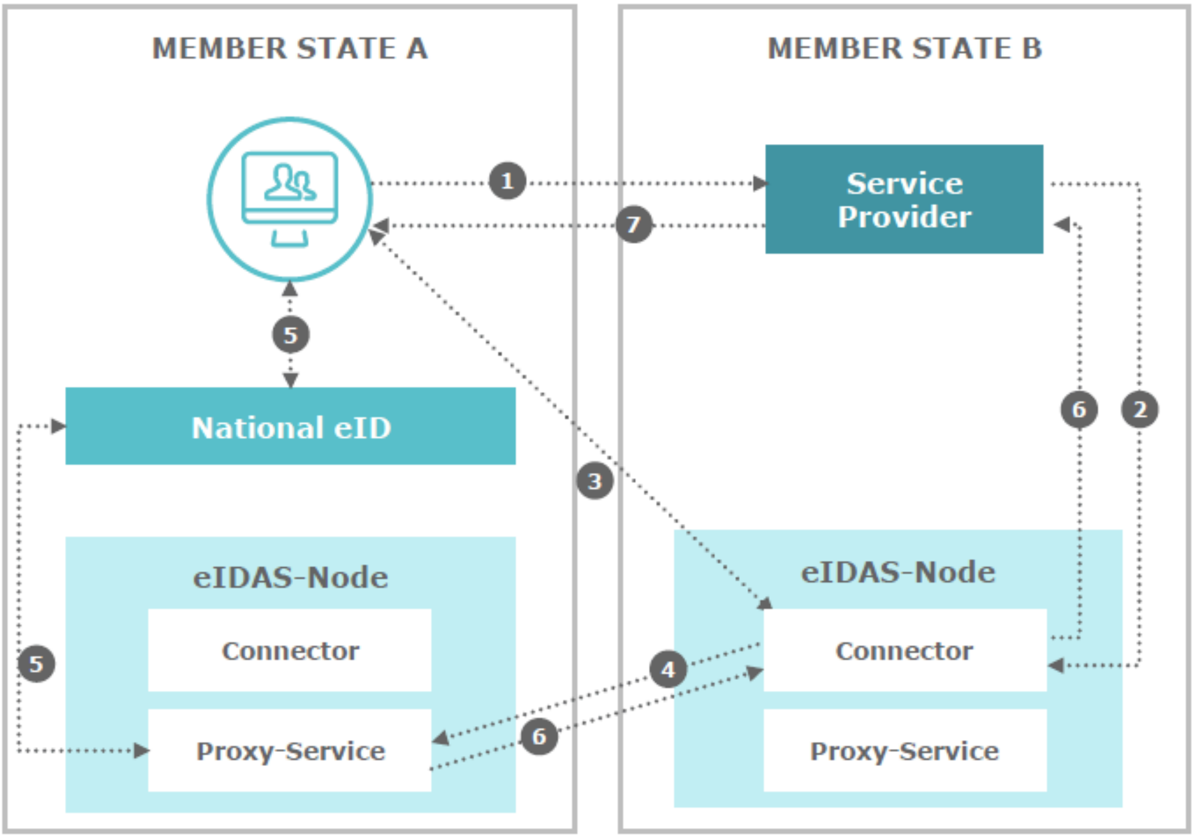


Figure 6: Overview of the eIDAS Authentication scheme depicting eIDAS Nodes, Source: https://docs.wso2.com/display/IS570/Electronic+Identification%2C+Authentication+and+Trust+Services+Regulation

eIDAS is based on well-established standards, such as SAML, to achieve Interoperability and high security between EU member states. EU member states use different national eID solutions, that often involve nation specific implementations. The eIDAS Nodes translate the specific national solutions such that they can be understood across borders.

The Proxy model further serves as a foundation for future developments from Domain Interoperability towards full Domain Harmonisation through a phased approach. Individual Domains can work towards full Harmonisation at their own pace, following their own change management processes. The initial implementation of Proxies will be complex, but in time, the functionality of a Proxy will become lighter, as the Harmonised components are transferred and embedded within the Domain. Eventually, a Proxy only needs to carry out the function of Cross-Domain Data service Registry when all other elements are harmonised within the Domain. See Figure 7 for the possible development of Proxies.

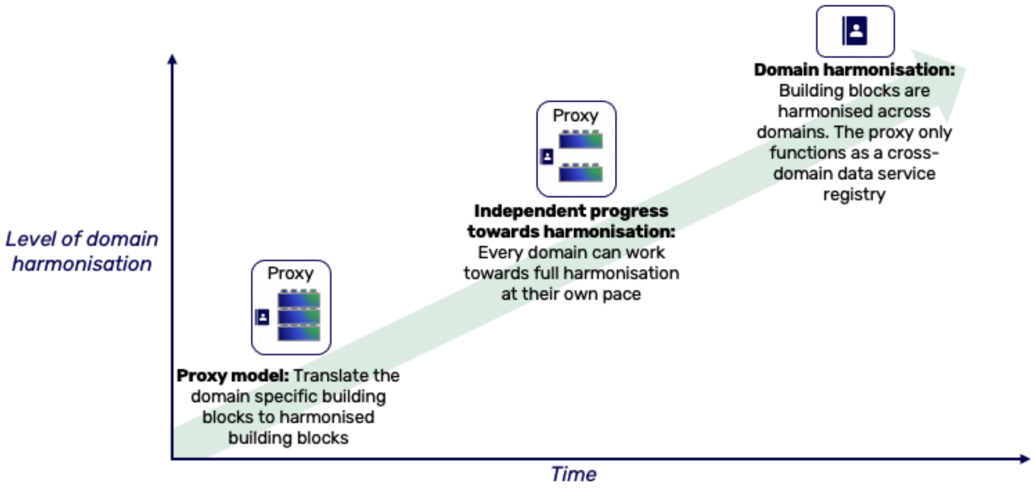

Level of domain harmonisation
Time
Proxy
Proxy model: Translate the domain specific building blocks to harmonised building blocks
Proxy
Independent progress towards harmonisation: Every domain can work towards full harmonisation at their own pace
Domain harmonisation: Building blocks are harmonised across domains. The proxy only functions as a cross-domain data service registry

Figure 7: Development from the PROXY MODEL to full HARMONISATION

It is impossible for DOMAINS to progress towards full HARMONISATION at the same pace, as DOMAINS depend on the implementation pace of their participants. However, the PROXY model enables DOMAINS to remain fully interoperable at different levels of progression towards full HARMONISATION. This is as the rules and agreements which hold for fully HARMONISED DOMAINS are the same as those for DOMAINS with PROXY MODEL implementations. Therefore, data can be shared across DOMAINS irrespective of the pace of progression, Further, these rules and agreements can be easily adopted by new DOMAINS or organisations that are aiming to share data to ease their internal development, meaning they may be fully harmonised from the initial development. See Figure 8 for a visual representation with DOMAINS in different levels of progression towards full HARMONISATION.

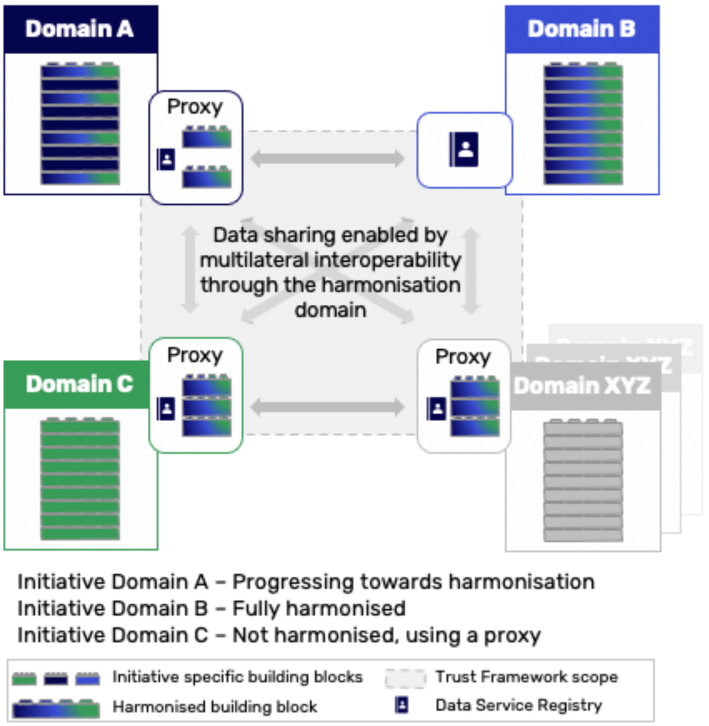

Domain A
Proxy
Domain B
Data sharing enabled by multilateral interoperability through the harmonisation domain
Domain C
Proxy
Proxy
Domain XYZ
Initiative Domain A – Progressing towards harmonisation
Initiative Domain B – Fully harmonised
Initiative Domain C – Not harmonised, using a proxy
Initiative specific building blocks
Harmonised building block
Trust Framework scope
Data Service Registry

Figure 8: Data can be shared across DOMAINS at different levels of progression toward full HARMONISATION

Section B: Harmonisation topics

In this section, topics related to Data sharing are discussed that will need to be included in the future Cross-Domain Trust Framework. Each chapter will describe a specific topic, explain the relevance for cross-domain interoperability and present findings that provide the basis for agreements in the future Cross-Domain Trust Framework.

5 Terms and conditions

5.1 Introduction

Terms and conditions define the concepts, duties, rights, powers and liabilities that apply to the actors on both sides of a Data Service Transaction that are captured in a Data Service Transaction Agreement. Terms and conditions are formalised into policies, which can be split into Access Control Rules, Obligations and Advice (see Figure 9). A Data Service's Terms and Conditions are set by the Data Service Provider directly and/or are (partially) a result of the rules of the Data Sharing Domains the Data Service Provider belongs and adheres to.

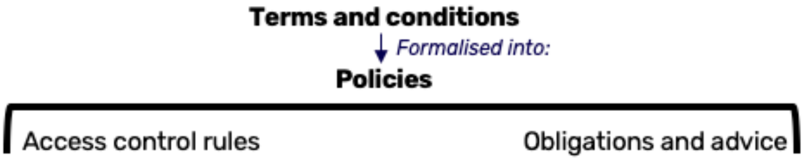


Figure 9: Terms and conditions are formalised in Policies, which can be split into Access control rules and Obligations and Advice

5.2 Relevance

To enable Interoperability, the Data Service Consumer needs to understand the Terms and Conditions of a Data Service in general and a specific Data Service Transaction as specified and communicated by the Data Service Provider, ideally in a machine-readable format. Therefore, it is required that Terms and conditions (formalised into Policies) can be interpreted across Domains, such that individual Policies and the pieces of evidence that demonstrate adherence to these Policies can be mapped to Domain specific Policies and evidence and vice versa. To achieve this, a shared understanding of and language for Policies and evidence is needed.

Within a single Domain, not everything that participants should adhere to is made explicit. Adherence criteria can also be part of rule books, legislation or certifications relevant to the Domain, known as Implied regulation and agreements. In this case, both the Data service provider and Data service consumer operating within the same Domain are aware of these Implied regulation and agreements. Participants in other Domains are not expected to be aware of these Domain specific Implied regulation and agreements. Therefore, to enable Cross-Domain Data Service Transaction Agreements, these implied regulations and agreements may need to be made explicit. Data service providers may decide to make (parts of) the Implied regulation and agreements explicit and require explicit proof of adherence to those Implied regulation and agreements.

5.3 Description

This chapter explains the need for a shared language and understanding on POLICIES in 5.3.1 and the split of POLICIES in 5.3.2.

5.3.1 Creation of a shared language and understanding

A shared language and understanding is needed to enable unambiguous communication on POLICIES and evidence that demonstrates the adherence to these POLICIES. It is not realistic to expect to create a shared language for all individual POLICIES given their variety across DOMAINS. A solution might be to create POLICY clusters and levels of adherence to POLICY clusters (to express an assurance level). These POLICY clusters might make it easier to define a shared language, as the clusters and levels might enable simple comparison across DOMAINS.

POLICY clusters are sets of POLICIES, in which POLICIES belong to the same cluster if they pursue the same objective. See Appendix 18.2 for a first set-up of POLICY clusters. POLICY cluster levels define whether a Domain meets specific criteria within a POLICY cluster, based on underlying POLICIES. POLICY cluster levels are formed differently for each cluster and can be defined along different axes (e.g. nominal, ordinal and interval) based on DATA SERVICE PROVIDER requirements.

POLICY clusters and POLICY levels should be further explored and defined in the next phase of the DSC, once work on the future CROSS-DOMAIN TRUST FRAMEWORK starts.

In the eIDAS Trust Framework, the principle of creating a shared language for POLICIES via clusters and levels for clusters is applied at scale. This is further detailed in Box 2.

Box 2: eIDAS

In the last 15-20 years, most EU member states have developed their own national digital identity solutions for citizen AUTHENTICATION based on member state specific requirements, resulting in member state specific Levels of Assurance (LoAs) for their digital identity.

In line with Europe's ambition to create one Digital Single Market, the European Union strived to enable people and businesses to use their own national electronic IDENTIFICATION schemes (eIDs) to access public services available online in other EU countries. To achieve this, the EU has created the common eIDAS[2,3] framework.

[2] **eIDAS** (**e**lectronic **ID**entification, **A**uthentication and trust **S**ervices) is an EU regulation on electronic identification and trust services for electronic transactions in the European Single Market

[3] **Source**: Commission implementing regulation (EU) 2015/1502, Office journal of the European Union

The variety of POLICIES and LoAs across countries initially made it impossible to create a shared language on individual POLICIES across EU member states. The eIDAS framework allows for mapping of national eID solutions and its member state specific LoAs to generic eIDAS LoAs, enabling INTEROPERABILITY.

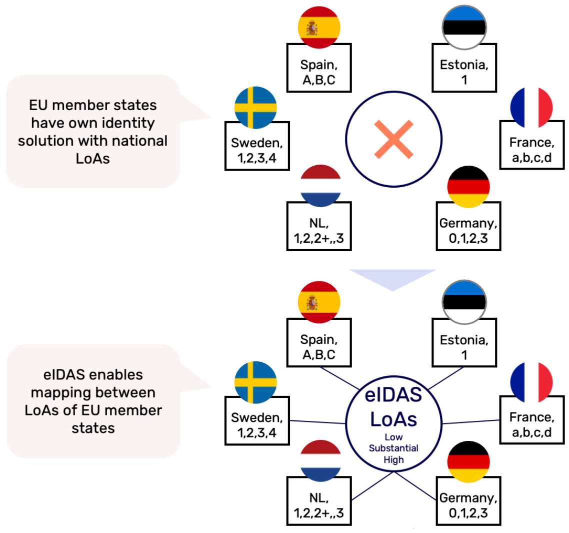
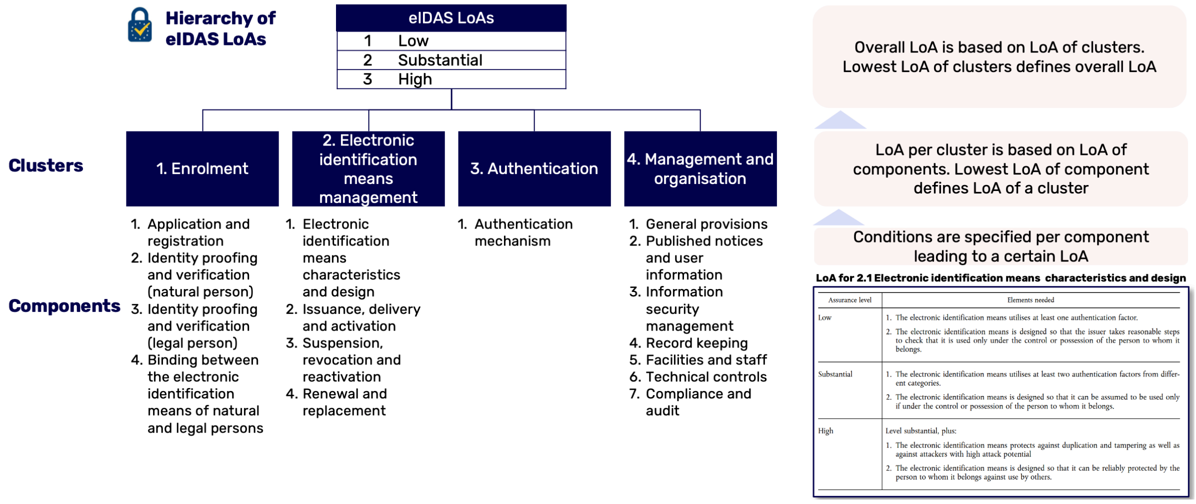


Figure 10: Creation of a mapping between Levels of Assurance in EU member states

eIDAS POLICY clusters consist of multiple components, with underlying POLICIES. The overall LoA of eIDs will be based on the LoA of a number of clusters, where the lowest LoA of the individual clusters will determine the overall LoA. Each cluster contains a number of components, and the LoA of the cluster will be based on the lowest LoA of all the components. Per component, conditions are specified defining how a LoA can be reached.


Hierarchy of eIDAS LoAs
eIDAS LoAs
1 Low
2 Substantial
3 High
Clusters
1. Enrolment
2. Electronic identification means management
3. Authentication
4. Management and organisation
Components
1. Application and registration
2. Identity proofing and verification (natural person)
3. Identity proofing and verification (legal person)
4. Binding between the electronic identification means of natural and legal persons
1. Electronic identification means characteristics and design
2. Issuance, delivery and activation
3. Suspension, revocation and reactivation
4. Renewal and replacement
1. Authentication mechanism
1. General provisions
2. Published notices and user information
3. Information security management
4. Record keeping
5. Facilities and staff
6. Technical controls
7. Compliance and audit
Overall LoA is based on LoA of clusters. Lowest LoA of clusters defines overall LoA
LoA per cluster is based on LoA of components. Lowest LoA of component defines LoA of a cluster
Conditions are specified per component leading to a certain LoA
LoA for 2.1 Electronic identification means characteristics and design

Assurance level	Elements needed
Low	1. The electronic identification means utilises at least one authentication factor. 2. The electronic identification means is designed so that the issuer takes reasonable steps to check that it is used only under the control or possession of the person to whom it belongs.
Substantial	1. The electronic identification means utilises at least two authentication factors from different categories. 2. The electronic identification means is designed so that it can be assumed to be used only if under the control or possession of the person to whom it belongs.
High	Level substantial, plus: 1. The electronic identification means protects against duplication and tampering as well as against attackers with high attack potential 2. The electronic identification means is designed so that it can be reliably protected by the person to whom it belongs against use by others.

Figure 11: Hierarchy of eIDAS LoAs

5.3.2 Policies

TERMS AND CONDITIONS are formalised into POLICIES, which can be split into ACCESS CONTROL RULES and OBLIGATIONS AND ADVICE, depending on whether the POLICIES are enforced before or after the DATA SERVICE AGREEMENT is established.

Access control rules

ACCESS CONTROL RULES are POLICIES that are assessed and enforced prior to establishing the DATA SERVICE AGREEMENT and validated at the moment of a DATA SERVICE TRANSACTION. Some ACCESS CONTROL RULES are in place to assess the likelihood of adherence to IMPLIED REGULATION AND AGREEMENTS (e.g. sector regulation and frameworks and general laws and regulation, through certifications and audit reports).

Examples of ACCESS CONTROL RULES:

- Subject attributes (e.g. LoA of identity, role and age)
- Context/environment attributes (e.g. location and time)
- Proof of security certifications (e.g. ISO 27001)

Obligations and advice

OBLIGATIONS AND ADVICE are POLICIES that are assessed and enforced after the DATA SERVICE AGREEMENT is established. They prescribe future requirements and optional guidance to the DATA SERVICE CONSUMER. It is up to the DATA SERVICE PROVIDER (or the Domain rules to which the DATA SERVICE PROVIDER adheres to) to determine whether a POLICY is OBLIGATION or ADVICE. Policy enforcement may vary (e.g. none, ad-hoc checks or by audit). Examples of OBLIGATIONS AND ADVICE POLICIES:

- Usage scope
- Storage requirements
- Time to live for datasets (deletion of data)
- Pricing and other financial (reporting) requirements
- Operational reporting requirements

See Appendix 18 Terms and Conditions, for an overview of POLICIES split into ACCESS CONTROL RULES and OBLIGATION AND ADVICE within DSC use cases.

Figure 12 provides an overview of the relationship between a DATA SERVICE TRANSACTION AGREEMENT, the associated transaction (the API call) and the TERMS AND CONDITIONS (formalised into POLICIES) within a DATA SERVICE TRANSACTION lifecycle.

The term ‘data transaction lifecycle’ is introduced as a term to distinguish between the sequence in which POLICIES should be adhered to and the actual DATA SERVICE TRANSACTION.

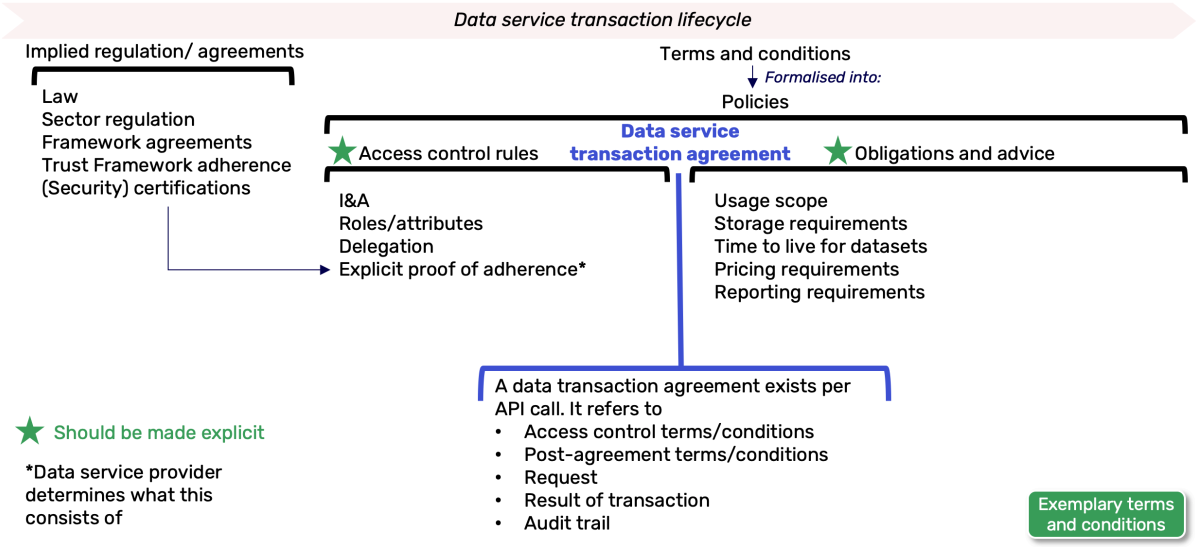

Data service transaction lifecycle
Implied regulation/ agreements
Law
Sector regulation
Framework agreements
Trust Framework adherence
(Security) certifications
Terms and conditions
Formalised into:
Policies
Data service transaction agreement
Access control rules
Obligations and advice
I&A
Roles/attributes
Delegation
Explicit proof of adherence*
Usage scope
Storage requirements
Time to live for datasets
Pricing requirements
Reporting requirements
A data transaction agreement exists per API call. It refers to
Access control terms/conditions
Post-agreement terms/conditions
Request
Result of transaction
Audit trail
Should be made explicit
*Data service provider determines what this consists of
Exemplary terms and conditions

Figure 12: Data service transaction lifecycle with a Data service transaction agreement and Policies

It is expected that only Access control rules and Obligation and Advice Policies will be specified in a Data Service Transaction agreement, as these are relevant for the execution of a single API call.

In the next phase, once work on the future Cross-Domain Trust Framework starts, it should be explored to what detail Implied regulation and agreements should be made explicit.

6 Identification, Authentication and Authorisation

6.1 Introduction

In order for actors to reach a DATA SERVICE TRANSACTION AGREEMENT, they must be able to identify, authenticate and authorise other actors. It is required that actors are able to identify those they are interacting with and assess their assurance level (for IDENTIFICATION and AUTHENTICATION) and know what permissions those other parties have (AUTHORISATION). ACCESS POLICIES define whether an entity should be permitted access to an object (target data, database access, algorithm access, etc.). ACCESS CONTROLS are the mechanisms and methods used to enforce ACCESS POLICIES using AUTHORISATION. Within DOMAINS, various types of IDENTIFICATION, AUTHENTICATION and AUTHORISATION mechanisms are used and while this suffices for activities within a specific DOMAIN, it is not trivial how these mechanisms and the resulting statements and evidence can find their way to another DOMAIN.

6.2 Relevance

When creating a HARMONISATION DOMAIN, PROXIES in different DOMAINS should be able to identify, authenticate and authorise one another in order to facilitate trusted, CROSS DOMAIN DATA SHARING. This will be part of the future creation of the Trust Framework.

In order to facilitate end-to-end CROSS-DOMAIN INTEROPERABILITY, IDENTIFICATION, AUTHENTICATION and AUTHORISATION from one DOMAIN needs to be transportable to another DOMAIN in a trustworthy manner. To enable this, a shared, mutually understandable language needs to be created.

6.2.1 Identification

Actors must be able to establish the identity of actor(s) from other DOMAIN(s) in order to determine the actor with whom a transaction is initiated. Currently, various INITIATIVES have different working implementations of IDENTIFICATION and AUTHENTICATION mechanisms. Table 5 gives a non-exhaustive overview of the various IDENTIFICATION and AUTHENTICATION solutions implemented by INITIATIVES.

Table 5: Overview of how identification and A*UTHENTICATION are organised within initiatives*

	SBR NEXUS	MedMij	SIVI	iSHARE	HDN
Identifier	- *Natural person:* not applicable - *Legal person:* Chamber of Commerce number	- *Natural person:* BSN - *Legal person:* Organisation identification number (OIN)	- *Natural person:* Name, address, date of birth and client number* - *Legal person:* Chamber of Commerce number	- *Natural person:* Proprietary - *Legal person:* Chamber of Commerce number (to be transferred towards EORI for European compatibility)	- *Natural person:* not applicable - *Legal person:* Chamber of Commerce number
Authentication methods	- *Natural person:* not applicable - *Legal person:* PKI Overheid certificate & eHerkenning	- *Natural person:* DigiD via "Toegangsverlenings-service" - *Legal person:* PKI Overheid certificate	- *Natural person*: e.g. IRMA, iDIN (maybe eHerkenning in future) - *Legal Person:* 2-Factor Authentication methods - following eHerkenning - *M2M:* ABZ certificaat*	- *Natural person*: depends on level of identity proof - *Legal person:* PKI Overheid certificate	- *Natural person:* not applicable - *Legal person:* HDN-specific certificate
Requirements	- *Natural person:* not applicable - *Legal person:* eHerkenning niveau 2+	- *Natural person:* eIDAS High (DigiD sub or High) - *Legal person:* eIDAS High	- *Natural person*: Face-to-face - *Legal person*: eHerkenning - *Both*: (Trend towards) 2-Factor Authentication	- *Natural person*: not applicable - *Legal person*: Highest level of identity proofing (proprietary)	- *Natural person:* not applicable - *Legal person:* copy ID, agreement with moneylender (moneylender has a "Wft-vergunning")
Frameworks of identity assurance	- eHerkenning as a derivative of eIDAS	- eIDAS - DigiD	- eHerkenning as a derivative of eIDAS	- eHerkenning as a derivative of eIDAS	- Not applicable

* Indicate initiative specific implementations

Table 5 shows that the INITIATIVES use different identifiers. In order to enable CROSS-DOMAIN DATA SHARING, there must be a mutual understanding of identifiers between DOMAINS such that DATA SERVICE TRANSACTION AGREEMENTS can be made. If the DOMAINS can understand each other's identities, a challenge remains in trusting the identities from another DOMAIN. Therefore, a mechanism should be in place that allows the DOMAINS to validate the authenticity of identities received from other DOMAINS for different types of actors which could initiate a DATA SERVICE TRANSACTION.

6.2.2 Authentication

DATA SERVICE PROVIDERS can set requirements for the level of assurance of AUTHENTICATION required from their DATA SERVICE CONSUMERS. When those consumers reside in other DOMAINS, the AUTHENTICATION information (including LoA) must be communicated and mapped to the DATA SERVICE PROVIDER'S LoA definitions.

6.2.3 Authorisation

For DATA SERVICE PROVIDERS to be able to make proper AUTHORISATION decisions regarding DATA SERVICE CONSUMERS residing in another DOMAIN, the information required for those decisions (attributes, roles, DELEGATION information and/or other information and decisions) must be communicated and mapped to the DATA SERVICE PROVIDER'S language and definitions.

6.3 Description

This chapter explains the need for a shared language and understanding in the topics of Identification, Authentication and Authorisation. This includes discussions on identifiers in 6.3.1, assessing identity levels of assurance in 6.3.2, types of Authentication in 0 roles in Authorisation in 6.3.4, Authorisation sequences in 6.3.5 and delegated authority in 6.3.6.

6.3.1 Identifying actors

The use of different types of identifiers for the same types of actors could lead to situations where one organisation has two different identifiers across Domains, or where identifiers that look exactly the same refer to different organisations. When interacting across Domains, this leads to ambiguity which will lead to errors, see Box 3 for an example.

Ambiguity between identifiers across Domains can be solved by explicitly specifying the type of identifier used in all Cross-Domain communication. Explicitly specifying the identifier used is possible through various mechanisms, including an attribute or prefix (see Box 3). The exact method of specifying the identifier used, and the standardisation of the sharing of this data should be detailed in the Trust Framework.

Box 3: Ambiguous identifiers

See Figure 13 for an example situation. Acme BV is participant in both Domain A and Domain B. Domain A uses the KvK number (Chamber of Commerce number in the Netherlands) as identifier, Domain B uses the EORI number (Identification number for business in the European Union).

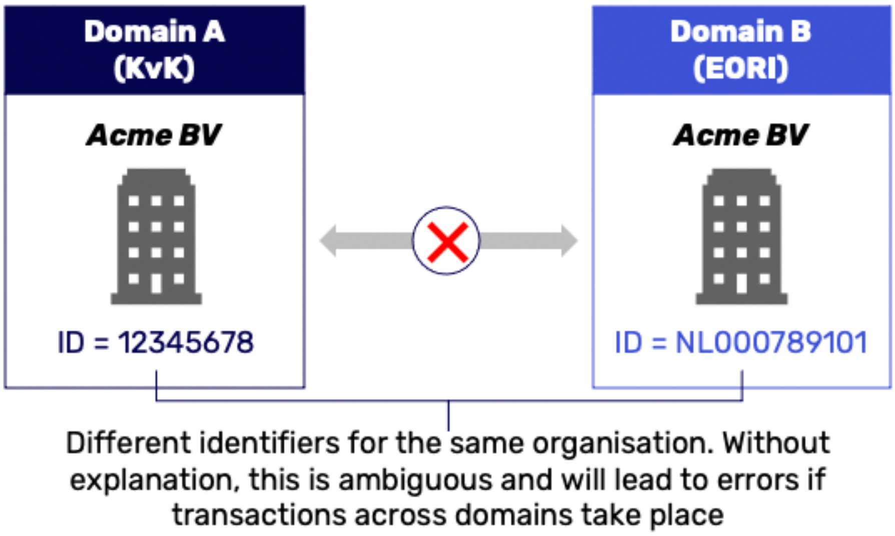

Domain A
(KvK)
Acme BV
ID = 12345678
Domain B
(EORI)
Acme BV
ID = NL000789101
Different identifiers for the same organisation. Without explanation, this is ambiguous and will lead to errors if transactions across domains take place

Figure 13: Ambiguity in identifiers should be resolved

This ambiguity in used identifiers across domains can be resolved through the use of an identifier pre-fix as shown in Figure 14.

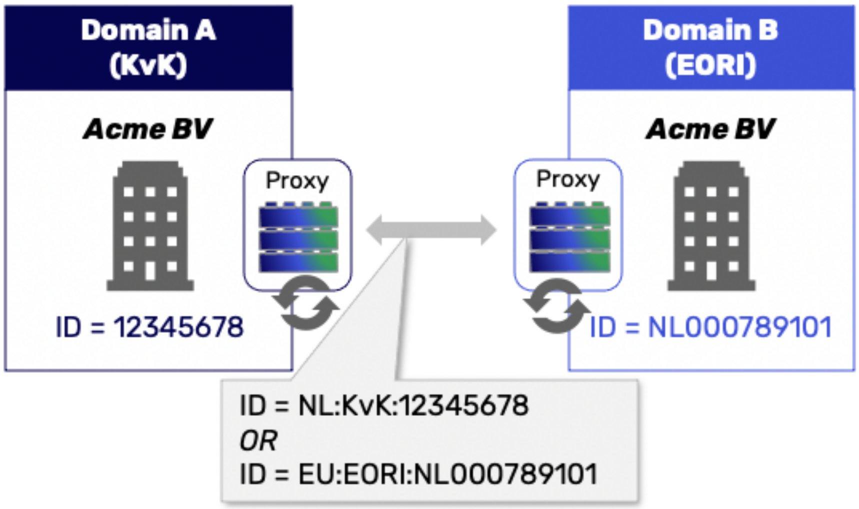


Figure 14: Using prefixes for communication of IDs across domains solves ambiguity

In addition to adding a prefix, proxies could map identifiers from their DOMAIN to identifiers of other DOMAINS. Mapping of identifiers can be done in order to establish the identity of an organisation with a different identifier in another DOMAIN or to distinguish the identities of organisations with a similar identifier in another DOMAIN to open services for them. As of now, it is unsure whether there will be use cases that require the mapping of identifiers. If these use cases are identified, the mapping of identifiers will be included in the future CROSS-DOMAIN TRUST FRAMEWORK.

The future CROSS-DOMAIN TRUST FRAMEWORK shall contain a number of best practices for INTEROPERABILITY solutions regarding identifiers. These best practices will be further detailed in the CROSS-DOMAIN TRUST FRAMEWORK

6.3.2 Assessing identity assurance

Actors must be able to understand the level of assurance that is associated with an identity received from another DOMAIN in order to determine whether the requested action can be performed.

For digital identity solutions, eIDAS has solved the INTEROPERABILITY of Levels of Assurance (LoA) at an EU member state level, see Box 2 for a detailed description. eIDAS allows EU member states with member state specific identity solutions with specific LoAs to be mapped to generic eIDAS LoAs in order to enable INTEROPERABILITY.

The eIDAS framework with 3 LoAs (low, substantial, high) shall be used as a basis for interoperable LoAs in the TRUST FRAMEWORK. This is because the eIDAS framework is widely adopted already and has become the de facto standard for electronic IDENTIFICATION for eGovernment purposes in Europe.

6.3.3 Authentication

Actors must be able to exchange identity information with each other. Depending on the type of actors involved, there are two different types of Authentication: Machine-to-machine Authentication and Human-to-machine Authentication. Machine-to-machine Authentication can be further specified to proxy-to-proxy Authentication and Authentication between a Data Service Consumer (machine) and a Data Service Provider.

Machine-to-machine Authentication

An Authentication mechanism is required between machines (machine-to-machine, M2M) in order to autonomously authenticate each other's identity. This Authentication should take place for each transaction context and without a need for human interaction.

An example of machine-to-machine authentication is in the usage of an IoT device service where the device must authenticate to the service servers. In the Trust Framework, machine-to-machine authentication occurs when proxies communicate with each other and must authenticate themselves.

In order to facilitate Interoperability, the Trust Framework should define a common machine-to-machine Authentication method that all proxies can make use of. eIDAS Qualified Trust Services are anchored in EU law and widely used in Europe. Specifically, the Qualified Website Authentication Certificates (QWAC) and Qualified Seal are relevant to facilitate M2M Authentication methods. These eIDAS Qualified Trust Services could be used as a basis in the Trust Framework.

A Qualified Website Authentication Certificate is a digital certificate which ensures the authenticity and data integrity of a connection and can be used to authenticate Proxies before a connection is made. A Qualified Seal is a signature which ensures the sender's non-repudiation and integrity of messages.

To ensure a correct usage of Qualified Trust Services, cybersecurity experts will be asked to provide insights and design principles so that these are implemented correctly for M2M Authentication within the Trust Framework.

Human-to-machine Authentication

An Authentication mechanism (human-to-machine, H2M) is in place between natural acting persons and the Domain that they are a part of. However, when transacting across Domains, it may be necessary for natural acting persons to authenticate themselves in Domains other than the one they are located in. Domains should facilitate a customer journey to enable this. Natural acting persons in various Domains should therefore be able to be redirected to perform Authentication in other Domains within a single customer journey.

An example of human-to-machine Authentication is a log-in to an online service by using a Facebook account (via OAuth). In the Trust Framework, human-to-machine authentication occurs when a natural acting person has to log in to a service to perform an action. The person logs in a single time, requiring interaction, to set up a session during which they can perform the action, possibly consisting of multiple interactions, without having to authenticate themselves at every step.

Authentication is always performed within a specific domain and therefore, there is no need to organise H2M Authentication across Domains. However, it will occur that a natural acting person (human) must authenticate themselves in a domain they are not present in, while initiating the transaction. In order to facilitate the transaction, the natural acting person needs to be redirected to the authorising Domain to authenticate. The proxies should facilitate this redirect. To ensure a consistent user experience, User Experience (UX) Requirements should be defined for H2M Authentication. The requirements for this redirect functionality by proxies and the UX-requirements for Identification and Authentication (and also Authorisation) should be included in the Trust Framework.

Forwarding Authentication to another Domain

For both H2M and M2M Authentication, it may be required to transfer Authentication attributes across Domains. For example, this may be needed in order to prove actor roles within another Domain. This insight has yet to be discussed within the Expert Group but will be picked up before development of the future Trust Framework.

6.3.4 Roles in Authorisation

Once the identity of the Data Service Consumer has been determined with a sufficient level of assurance, the Data Service Provider must determine what actions they allow the consumer to perform. This is what Authorisation the Data Service Consumer has. For the Data Service Provider to determine Authorisation, a number of different functional roles are established, each with their own responsibilities. provides an overview of these roles and responsibilities and Box 4 provides an illustration of an Authorisation flow.

Table 5: Overview of Authorisation roles and responsibilities

Roles	Responsibilities
PAP (Policy Administration Point)	The Policy Administration Point is where administrators, developers and business users can create and manage Authorisation policies in order to be used by the PDP.
PEP (Policy Enforcement Point)	The Policy Enforcement Point is responsible for protecting the object by executing the access control decision. It intercepts API requests and forwards them on to the PDP.
PDP (Policy Decision Point)	The Policy Decision Point evaluates received Authorisation requests against Authorisation policies using extra information if needed. All decisions reached are returned to the PEP.

Roles	Responsibilities
PIP (Policy Information Point)	The Policy Information Point is any underlying information source of (meta)data such as databases, user directories and Authentication details relevant for the Authorisation. If PEP provides insufficient data to PDP, additional information can be retrieved via the PIP

Box 4: Illustration of Authorisation roles functionality

The following example Authorisation flow model can be applied to most Authorisation methods and provides a usable framework as basis for describing Authorisation concepts.

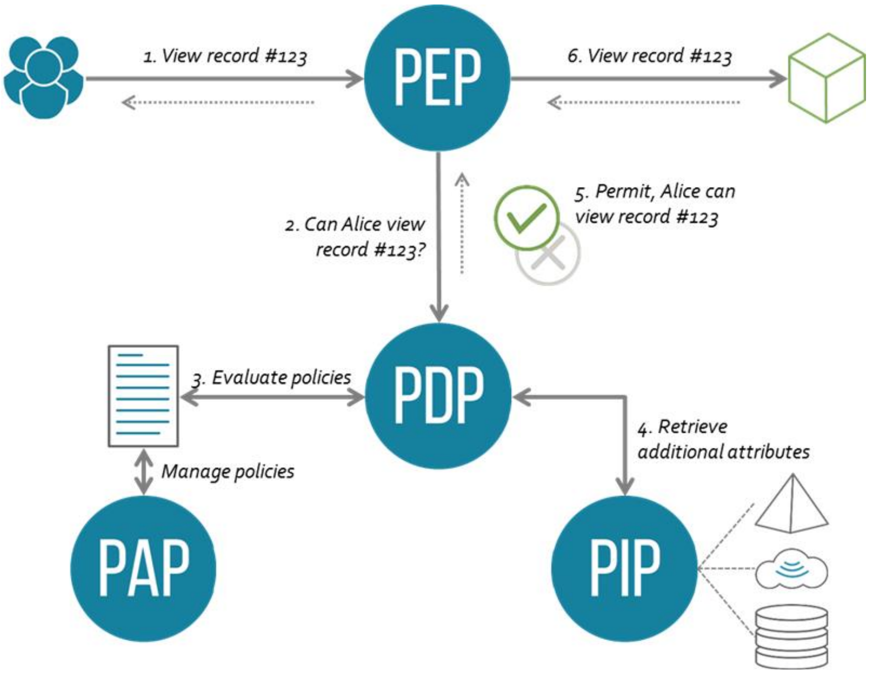

1. View record #123
PEP
6. View record #123
2. Can Alice view record #123?
5. Permit, Alice can view record #123
3. Evaluate policies
PDP
Manage policies
4. Retrieve additional attributes
PAP
PIP

Figure 15: Example Authorisation flow as defined in the XACML standards
Source: https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=xacml

1. A user sends a request which is intercepted by the Policy Enforcement Point (PEP).
2. The PEP converts the API request into an Authorisation request.
3. The PEP forwards the Authorisation request to the Policy Decision Point (PDP).
4. The PDP evaluates the Authorisation request against the loaded policies. The policies are managed by the Policy Administration Point (PAP). If needed, it also retrieves attribute values from underlying Policy Information Points (PIP).
5. The PDP reaches a decision (Permit / Deny / NotApplicable / Indeterminate) and returns it to the PEP.
6. The PEP enforces the decision and processes the request; in the case of a Permit, access is granted.

Note: This is a simplified model, and other Authorisation flows exist. See chapter 6.3.5 for more examples.

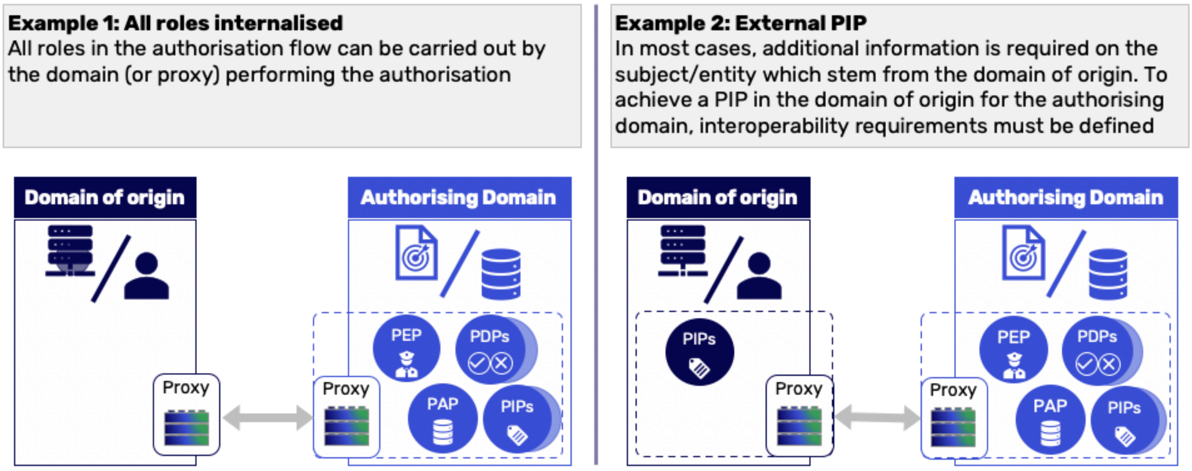
In practice, there is often not just a single implementation of several of the Authorisation roles. For example, there can be multiple PDPs which each take partial Authorisation decisions which collectively can lead to a final Authorisation decision. Furthermore, there are often multiple PIPs, each providing different sets of information to the PDPs as needed. For Cross-Domain Authorisation, these roles (PIPS and PDPs) can even be implemented in different domains. Depending on the choice of possible distribution of the roles across domains, Interoperability requirements are needed to facilitate the implementation of the roles.

Requirements needed to facilitate the distribution of Authorisation roles across domains

The roles required for Authorisation could be distributed across different Domains to enable Cross-Domain use cases. It is to be expected that the enforcement and administration of policies will be located within the same Domain, which in turn makes it likely that the decision will also be made in the same Domain. In the context of Authorisation, it therefore makes sense to refer to Domains as administrative Domains, defined as the Domain where policies are administrated and enforced.

How an Authorisation decision is reached within a Domain can be the result of many (partial) decisions reached by different components within the Domain, However, the PDP combines all partial decisions to a final decision. The details of how this is achieved is out of scope for the future Cross-Domain Trust Framework as it is the responsibility of a single Domain.

If use cases arise where it is necessary to out-source any of these Authorisation roles to other Domains, this will be further investigated to be included in the future Cross-Domain Trust Framework. For now, this means the two most likely role distributions are as shown in Figure 16.



Example 1: All roles internalised
All roles in the authorisation flow can be carried out by the domain (or proxy) performing the authorisation

Example 2: External PIP
In most cases, additional information is required on the subject/entity which stem from the domain of origin. To achieve a PIP in the domain of origin for the authorising domain, interoperability requirements must be defined

Figure 16: Most use cases can be captured in two different Authorisation role distributions

When all the roles for Authorisation can be realised within a Domain (example 1 in Figure 16), there is no need for additional Interoperability requirements. However, in the case of example 2 in Figure 16 where a role is located in another Domain, or even outside of either Domain, Interoperability requirements are needed to enable this. Therefore, further investigation must be done into the following elements to be included in the Trust Framework:

- Language must be created to exchange Authorisation data and attributes in order to transact,
- Trust is needed between domains regarding the sharing of Authorisation attributes,
- Technical standards are needed to enable communication of attributes.

6.3.5 Authorisation flows

There are two possibilities for the Authorisation flow which are most likely to be needed to enable Data sharing: the Pull and Push Authorisation sequence, as identified in RFC 2904 (source: https://tools.ietf.org/html/rfc2904). Both Authorisation sequences can be used for any type of Data service model. Therefore, they can be considered independently from each other.

Pull Authorisation sequence

In a pull Authorisation sequence, the PEP pulls the Authorisation decision from the PDP in the authorising Domain. See Box 5 for more information on the pull Authorisation sequence.

Box 5: Illustration of Pull Authorisation sequences in the proxy model

Figure 17 shows the Proxy interaction for a push Authorisation sequence.

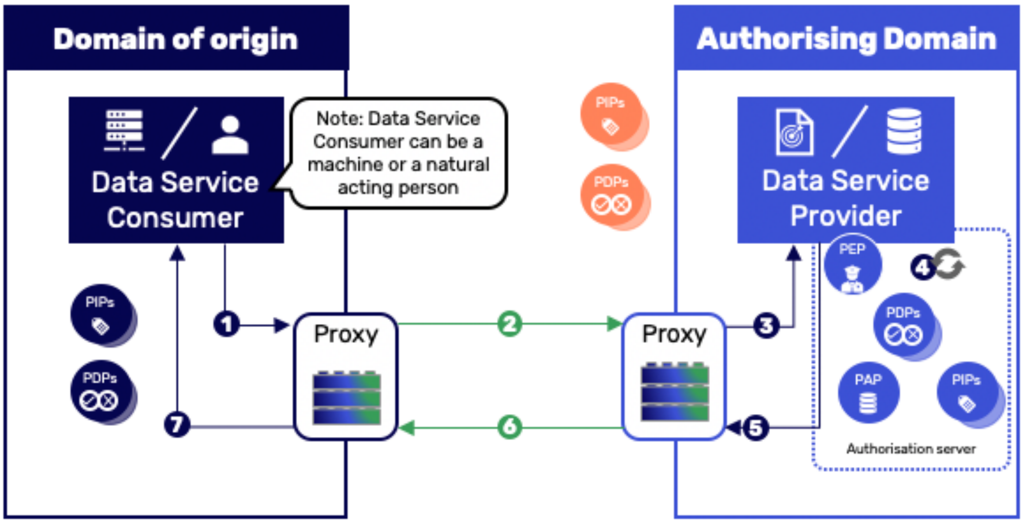


Figure 17: Proxy interaction for a pull authorisation model

1. The Data Service Consumer sends a request for a Data service to the Domain of Origin Proxy (including Data Service Consumer information for Authorisation)
2. The Domain of Origin Proxy translates the request and forwards it to the Authorising Domain Proxy
3. The Authorising Domain Proxy translates the request and forwards it to the Authorising Domain

4. Authorising Domain receives the request, processes it and the PDP takes the appropriate decision. The decision can be based on information and (sub) decisions received from outside of the Authorising Domain.
5. The Data Service Provider PEP provides access and Data Service Provider directly performs the action and sends back the result to the Authorising Domain Proxy
6. The Authorising Domain Proxy translates the results and forwards the result of the action to the Domain of Origin Proxy
7. The Domain of Origin Proxy translates the results and forwards the result of the action to the Data Service Consumer

Note: RFC 2904 additionally identifies the agent Authorisation sequence. From an Interoperability perspective, this can be considered the same as the pull sequence, as this only impacts how the decision is made in step 4.

An example of an Authorisation pull is when a Dutch citizen authorises a family member to perform their tax declaration using the NL mandate registry for citizens, DigID Machtigen. The citizen has to authorise the family member in advance at DigiD Machtigen, where this information is stored. The family member can then log in at the tax authority using their DigiD. The tax authority determines that they can perform the tax declaration based on an Authorisation pull from DigD Machtigen.

Push Authorisation sequence

In a push Authorisation sequence, the PEP gets pushed an Authorisation decision that the Domain of Origin has received from the PDP. See Box 6 for more information on the push Authorisation sequence.

Box 6: Illustration of Push Authorisation sequences in the proxy model

Figure 18 shows the Proxy interaction for a push Authorisation sequence.

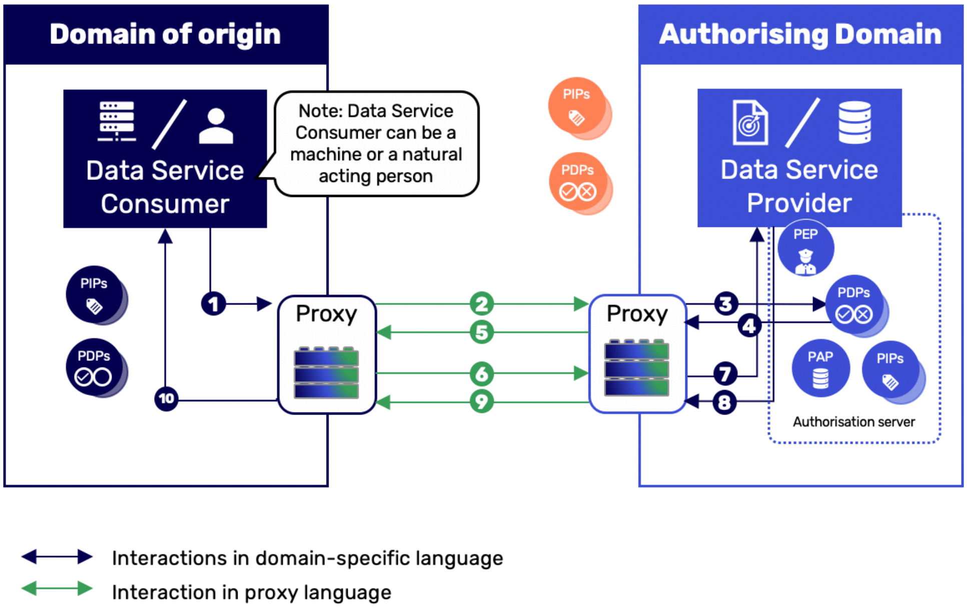


Figure 18: Proxy interaction for a push authorisation sequence

1. The DATA SERVICE Consumer sends an AUTHORISATION request for a DATA SERVICE action to the DOMAIN of Origin proxy (including DATA SERVICE CONSUMER information for AUTHORISATION and user redirect for consent, if necessary)
2. The DOMAIN of Origin PROXY translates the AUTHORISATION request and forwards it to the Authorising DOMAIN PROXY (including information and redirect)
3. The Authorising DOMAIN PROXY translates the AUTHORISATION request and forwards it to the PDP in the Authorising DOMAIN (including information and redirect
4. PDP takes the appropriate decision and responds with the decision to the Authorising DOMAIN PROXY. The decision can be based on information and (sub) decisions received from outside of the authorising DOMAIN.
5. The Authorising DOMAIN PROXY sends the decision to the DOMAIN of Origin PROXY
6. The DOMAIN of Origin PROXY sends a DATA SERVICE request (including decision) to the Authorising DOMAIN PROXY
7. The Authorising DOMAIN PROXY forwards the request to the DATA SERVICES PROVIDER (including decision) where the PEP validates the decision and provides access
8. The DATA SERVICE PROVIDER performs the action and sends the result to the Authorising DOMAIN PROXY
9. The Authorising DOMAIN PROXY translates the results and forwards the result to the DOMAIN of Origin PROXY
10. The DOMAIN of Origin PROXY translates the results and forwards the result of the action to the DATA SERVICE CONSUMER

An example of an AUTHORISATION push is the OAuth 2.0 protocol in which users are redirected to provide consent for requests to access. This results in a long-term access token which can be used for the DATA SERVICE TRANSACTIONS. The DATA SERVICE request includes the token and therefore, the AUTHORISATION is pushed. These mechanisms are common to IoT setups and can be found in access control for home smart meters for electricity. The energy provider receives access to the home smart meter, based on a one-time consent of the user, on which the network operator (the owner of the metering infrastructure) issues an access token that can be used for all future requests for data.

6.3.6 Delegated Authority

DELEGATION is the provision of explicit rights (to perform an action) to a third party. There are a number of different cases where DELEGATION of authority is required, such as:

- Companies cannot perform actions themselves and a service/employee must perform this on their behalf.
    - Natural persons, on behalf of companies, interact with other companies, such as non-standardised interactions using a web browser.
    - Machines, on behalf of companies, interact with other companies, such as PKI Overheid (this is implicit DELEGATION of the machine, allowing machines to act for the company).
- Companies may delegate rights to other companies so that the other company can perform actions on their behalf in another DOMAIN.
- Natural persons may give consent to another natural person to perform an action on their behalf, such as a colleague performing an action for you.

Therefore, DELEGATION of authority must be specified within the TRUST FRAMEWORK. Two types of DELEGATION have been identified: pre-configured, and ad-hoc DELEGATION.

1. **Pre-configured Delegation**
    - Pre-configured DELEGATION occurs well before the DATA SERVICE action takes place and is usually long lasting.
    - Examples of pre-configured DELEGATION can be seen in some iSHARE use cases, where delegation policies can be managed/stored in authorisation registries which can be consulted at any time during data requests to provide authorisation. Another example is in the "Sharing e-CMR data with insurers" use case, in which an insurer can be mandated by a shipper to retrieve data from the e-CMR on their behalf.
2. **Ad-hoc Delegation**
    - Ad-hoc DELEGATION occurs as the DATA SERVICE action is being performed and lasts for that single context.
    - An example of ad-hoc DELEGATION can be seen in the "Green Loans" use case in which mortgages can be provided based on energy usage data. The mortgage intermediary can be granted access to the energy usage of a consumer to prepare a quotation for a mortgage.

Communication required to validate pre-configured delegation

In pre-configured DELEGATION, the delegator gives consent for the delegatee in a single DOMAIN. The delegatee can be given consent for generic rights, or rights to perform a specific action. The delegator does not know if the delegatee made use of the delegated rights and when or how they were used. Once the DELEGATION is performed, this must be stored within the DOMAIN where this occurred and the delegatee is free to perform the action they were given consent for.

The process of pre-configured DELEGATION all takes place within a single DOMAIN and therefore, there is no need for INTEROPERABILITY requirements regarding the act of DELEGATION. Furthermore, if pre-configured DELEGATION takes place within the Authorising DOMAIN, there is no need for additional INTEROPERABILITY requirements as there is no need to communicate AUTHORISATION data across DOMAINS.

If pre-configured DELEGATION takes place within the DOMAIN of Origin, this must be communicated to the authorising DOMAIN during a DATA SERVICE TRANSACTION. The TRUST FRAMEWORK must facilitate a method to communicate this DELEGATION across DOMAINS. Furthermore, a method for the Authorising DOMAIN should be defined to validate the DELEGATION performed.

User experience requirements facilitate Ad-hoc Delegation

In Ad-hoc DELEGATION, the delegatee is given specific rights to perform a DATA SERVICE action only during the transaction. The delegator knows that the delegatee made use of the delegated rights during only that transaction context. In this case, AUTHORISATION must take place within the Authorising DOMAIN. In order to facilitate this, proxies should include UX requirements for H2M interaction to facilitate an actor delegating consent across DOMAINS.

7 Legal context

7.1 Introduction

There is a hierarchy of applicable rules, laws and legislation that must be considered in order to enable Cross-Domain Data Sharing. See Figure 19 for an overview of the hierarchy of applicable rules, laws and legislation and some examples. As described in Chapter 5, the most specific legal context are the Terms and Conditions which are agreed upon in a Data Service Transaction Agreement. In the complete legal context, it can be seen that the Data Service Transaction Agreement adds additional rules to the other levels present in the hierarchy.

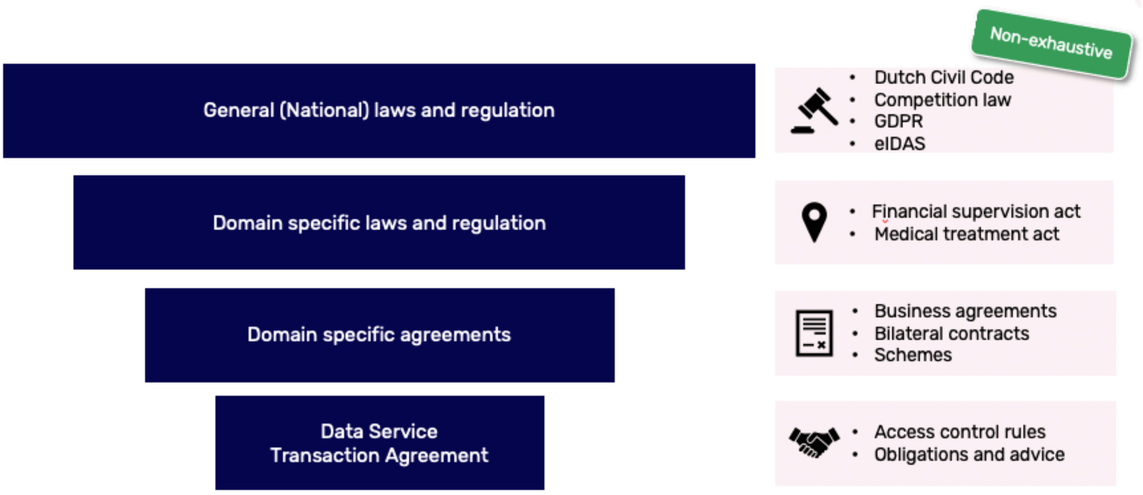


Figure 19: Hierarchy of rules, laws and regulations that must be considered for data sharing

7.2 Relevance

In general, agreements facilitate Trust between organisations as a prerequisite for most actions between them, including data sharing. When actors come to an agreement to be able to share data, they form a Domain. These Domain specific agreements facilitate Trust by creating clarity about the legally binding rules under which data sharing takes place. As indicated in Figure 19, these Domain specific agreements are a further specification of what is allowed additional to applicable rules, laws and regulation. In order to enable cross-Domain agreements, a solution to facilitate cross-Domain agreements must be included in the Trust Framework.

7.3 Description

7.3.1 Contracts

Any pair of organisations may have set up bilateral agreements with each other and may have implemented specific technology to enable data sharing between them. These bilateral contracts need to be set up and maintained for all organisations in order to allow for data sharing between them. In a future where an increasing number of organisations is expected to share data, the multitude of needed bilateral contracts is not efficient. Within some Domains, this has been resolved through the creation of a Domain Scheme to facilitate data sharing between organisations within the Domain, see Figure 20 Domain participants have one contract with the Domain Scheme to enable data sharing with all other Domain participants. This Domain Scheme is often managed collaboratively by actors in the Domain.

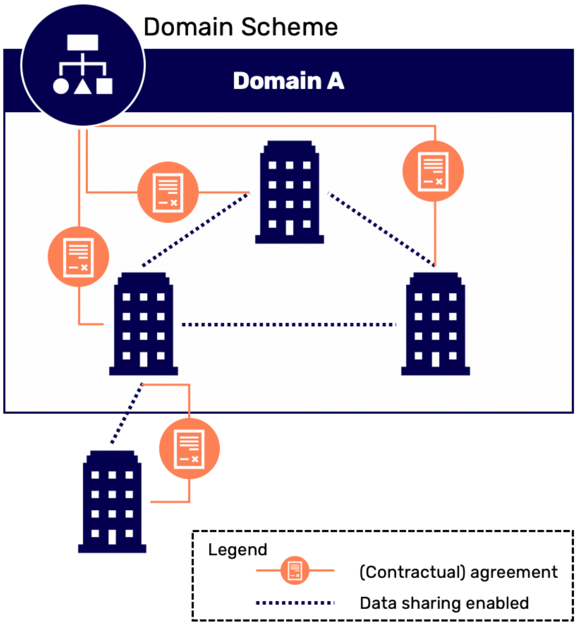


Figure 20: Some Domains have implemented Domain Schemes to enable data sharing within the Domain

Domain Schemes facilitate multilateral Trust through contractual agreements to enable bilateral Data Sharing between Domain participants. Scheme agreements lower barriers for data sharing by defining common technical standards and legal agreements, including Domain specific laws and regulation. Beside these Domain Scheme agreements, organisations are free to make additional bilateral agreements with organisations outside of the Domain to enable cross-Domain data sharing. Where Domain Schemes have solved this need for bilateral agreements within a domain, bilateral agreements remain relevant for Cross-Domain Data Sharing, see Figure 21.

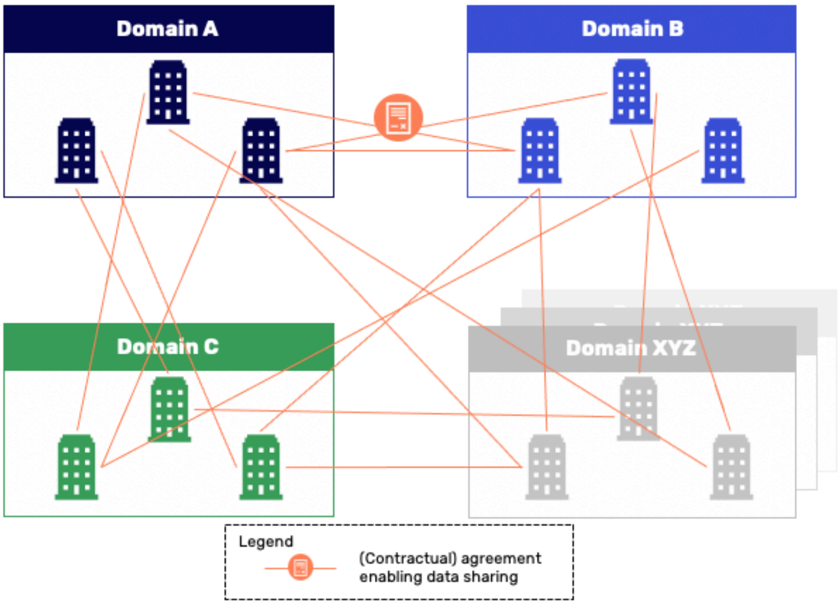


Figure 21: Closing bilateral contracts with every single organisation in cross-Domain data sharing is not scalable

As a multitude of bilateral agreements between organisations from a multitude of Domains is not scalable, the future TRUST Framework should facilitate a scalable solution to legally bind all organisations across DOMAINS. A solution to enable scalability is possible through multilateral agreements, which can be achieved via a chain of bilateral contracts as shown in Figure 22.

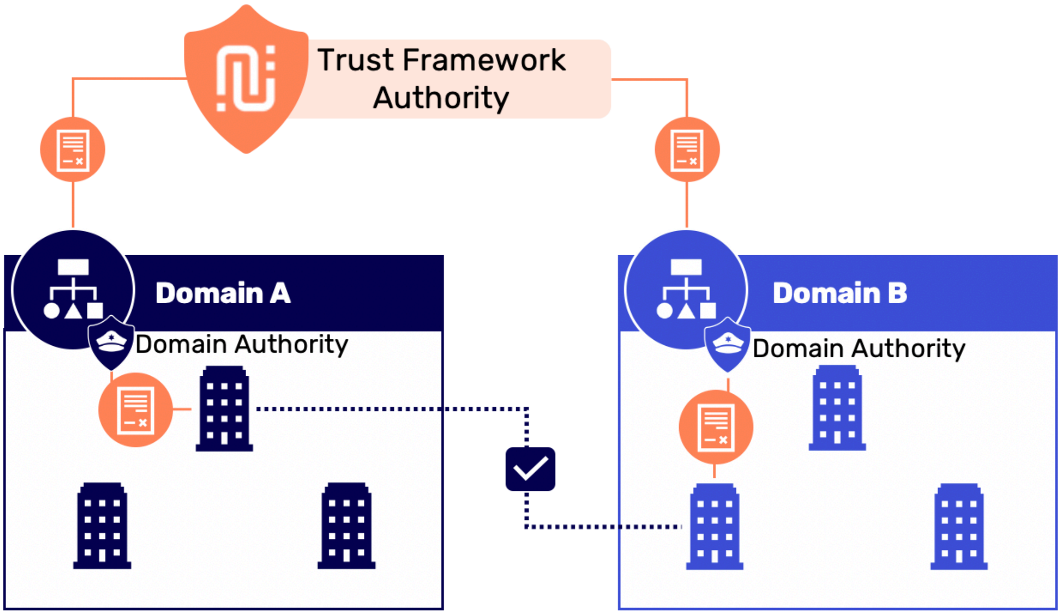


Figure 22: Enabling multilateral agreements via a chain of bilateral agreements

When each DOMAIN scheme has a single bilateral contract with the overarching TRUST FRAMEWORK AUTHORITY and this bilateral contract enables a third-party effect, a chain of contracts is created which legally binds all organisations across all DOMAINS. An example of where this solution has a proven implementation can be seen in Box 7. As all organisations are connected across domains via the chain of multilateral contracts, there is no need for bilateral contracts between organisations in other DOMAINS, however organisations are free to create bespoke agreements on top of the scheme agreements.

Box 7: A chain of bilateral contracts in the Mastercard ecosystem

Within the Mastercard ecosystem, a chain of bilateral contracts binds all actors to enable payments between actors, see Figure 23.

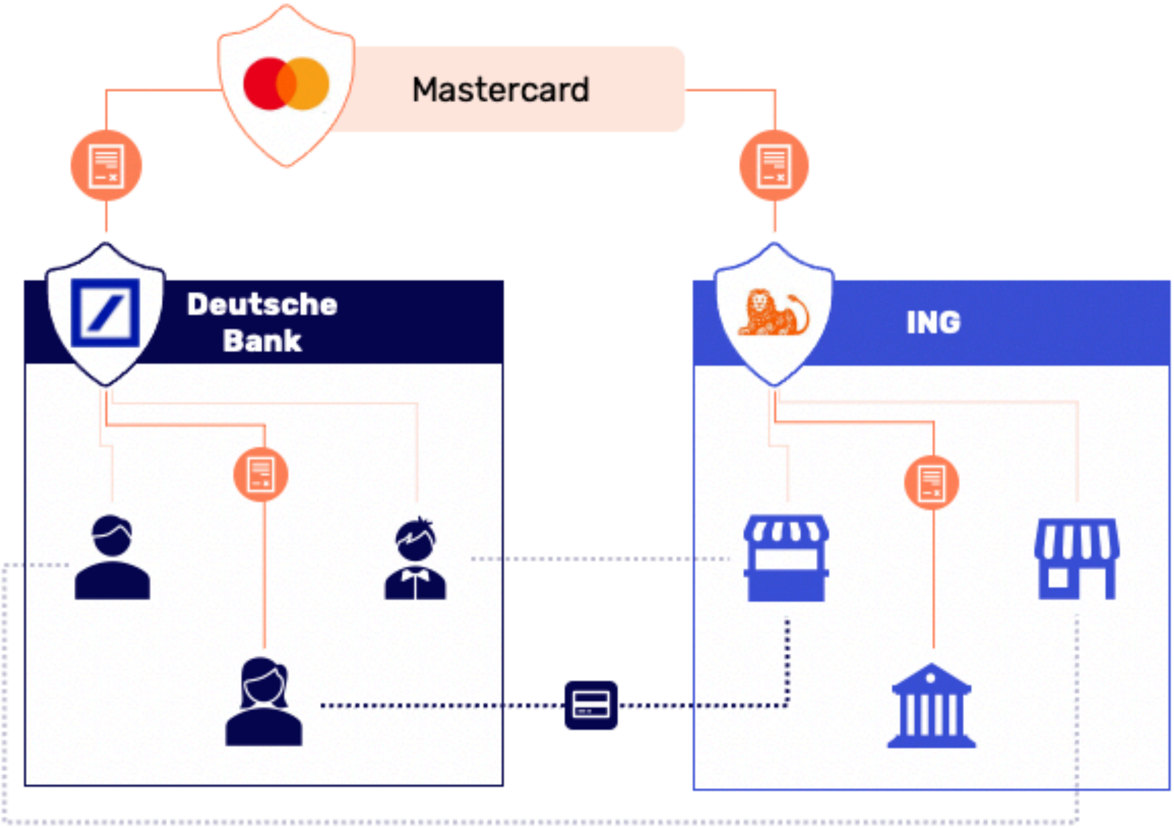


Figure 23: Example of a chain of contracts in the Mastercard ecosystem

- Deutsche Bank has a contract with Mastercard to enable them to issue Mastercard branded credit cards
- Deutsche bank issues Mastercard branded credit cards to their customers, who all have a contract with Deutsche Bank
- ING has a contract with Mastercard to enable them to facilitate accepting Mastercard payments at their merchants
- ING functions as an acquiring bank for their merchants, who all have a contract with ING
- Payments are facilitated between all Deutsche Bank customers and ING merchants

The TRUST FRAMEWORK Authority is a role which is introduced to manage the contracts and ensure adherence to them. This includes the function of a monitoring body, which verifies that DOMAIN SCHEMES adhere to the TRUST FRAMEWORK contract, and the function of an enforcement body which acts when contracts are violated. DOMAIN Authorities are needed to aggregate the chain of contracts to connect all organisations in each DOMAIN. Additionally, the DOMAIN Authority functions as monitoring and enforcement body within the DOMAIN (concerning the Domain specific agreements).

7.3.2 Legal topics

A number of legal topics have been identified which are relevant and should be covered in the future Trust Framework to lower barriers for Cross-Domain Data Sharing. These are categorised according to the Trias Politica separation of powers as shown in Table 6. The Trias Politica separation of powers is a governance structure which prevents the concentration of power at a single entity such that no single entity can abuse its power. A rule making power will establish and maintain the rules in the future Trust Framework for its participants to adhere to, the executive power will administer, monitor and enforce the established rules, and the judicial power will settle disputes. In practice, it is not always practical to fully separate the three powers, and the division of these roles may change with the maturity and scale of the scheme. For example, in iSHARE various executive responsibilities have shifted from the Scheme Owner role to the Scheme Administrator. The future Trust Framework will need sufficient checks and balances so that it is clear to participants that no single entity has disproportionate power it can abuse.

The governance structure of the future Trust Framework will be detailed in a separate chapter. This is will be included in the next version of the Harmonisation Canvas

Table 6: Legal topics categorised in the Trias Politica

Non-exhaustive

Rule Making power	Executive power	Judicial power
Relevant legislation	Supervising entities	Liability
Privacy	Acceptance criteria & KYC	Sanctions
Competition law	Governance structure oversight	Complaint & dispute management
Participant-scheme	Certification framework	Incident handling processes
Bilateral relations	Certification process	Escalation & decision making
Terms & Conditions	Change procedures & process	…
Governance Composition	Version management	
…	Monitoring and reporting	
	…	

8 Information Security

8.1 Introduction

When sharing data, organisations expose themselves to information security risks that need to be managed. Information Security management involves the implementation of sufficient measures to balance the risks of possible threat events. A widely used model to discuss Information Security is the CIA triad, see Box 8 for an overview. Examples of threat events include unauthorised access to data or deletion of data. Examples of Information Security measures include the encryption of communication or contracts defining restrictions. A balance between the risks and implemented measures must be found to reduce risks to an acceptable level while still providing a usable solution, see Figure 24.

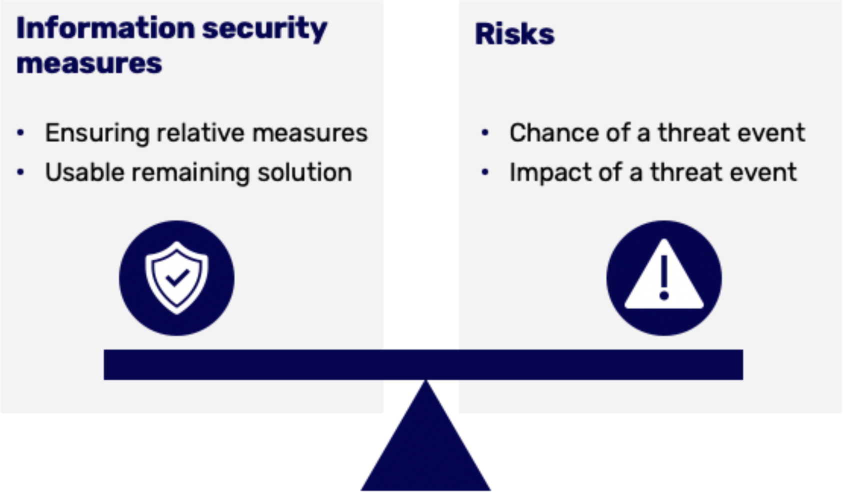
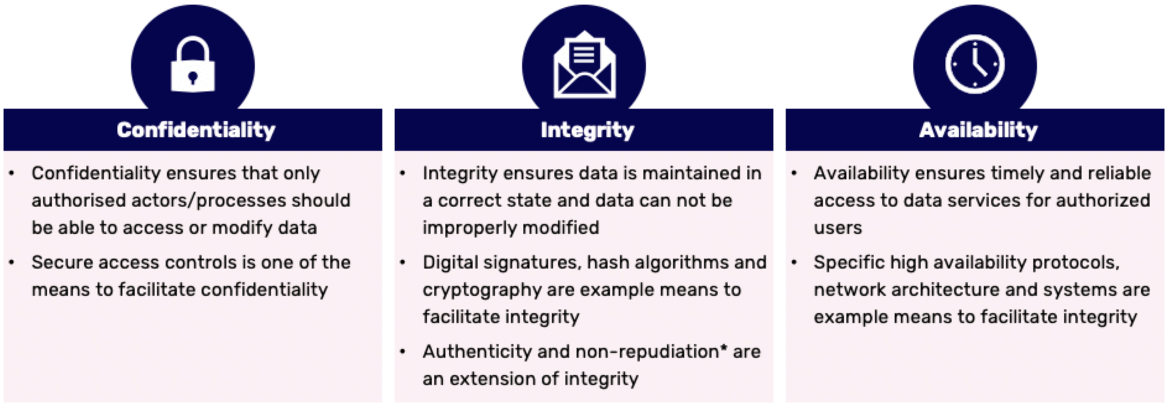

Information security measures
Ensuring relative measures
Usable remaining solution
Risks
Chance of a threat event
Impact of a threat event

Figure 24: Information Security management is the balance between security risks and measures

Box 8: The CIA Triad

The CIA (Confidentiality, Integrity and Availability) triad of Information Security is an Information Security model which can be used as a starting point for discussing Information Security topics and categorising security measures. Figure 25 gives an overview of the concepts within the CIA triad.



Confidentiality

- Confidentiality ensures that only authorised actors/processes should be able to access or modify data
- Secure access controls is one of the means to facilitate confidentiality

Integrity

- Integrity ensures data is maintained in a correct state and data can not be improperly modified
- Digital signatures, hash algorithms and cryptography are example means to facilitate integrity
- Authenticity and non-repudiation* are an extension of integrity

Availability

- Availability ensures timely and reliable access to data services for authorized users
- Specific high availability protocols, network architecture and systems are example means to facilitate integrity

*Authenticity and non-repudiation are part of the CIAAN-model as extensions to the CIA triad

Figure 25: The CIA Triad: Confidentiality, Integrity, Availability

8.2 Relevance

In the context of Cross-Domain Data Sharing, Information Security concerns the risks and measures related to the end-to-end data sharing transaction between actors from different domains. This includes not only what happens when sharing data, but also what happens to the data itself. See Figure 26 for a non-exhaustive view on topics related to data sharing across domains.

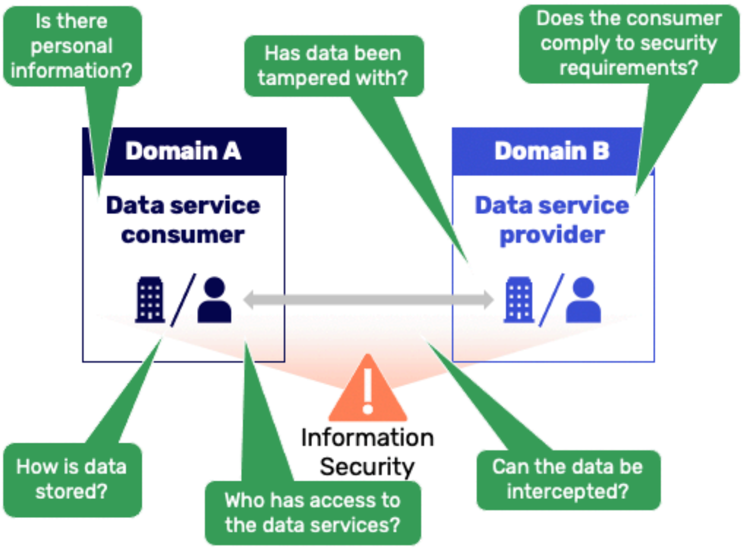

Is there personal information?
Has data been tampered with?
Does the consumer comply to security requirements?
Domain A
Data service consumer
Domain B
Data service provider
Information Security
How is data stored?
Who has access to the data services?
Can the data be intercepted?

Figure 26: Examples of questions related to INFORMATION SECURITY *in cross-domain data sharing*

Therefore, Information Security includes measures implemented within the Data service Consumer Domain (e.g. secure storage of data) and the Data Service Provider Domain (e.g. validating implemented security measures), as well as the Harmonisation Domain (e.g. secure exchange infrastructure). Information Security is a basic prerequisite to enable trust, as it contributes to reducing risks to sufficiently low levels required to share data.

8.3 Description

To facilitate Information Security across domains, Domain A and B need to be able to communicate with each other on applicable Information Security concepts via a shared language and understanding. A shared language and understanding should allow for unambiguous communication on Information Security concepts and evidence to demonstrate compliance.

The main challenge for creating a shared language on Information Security is the large amount of variance in applicable security concepts between Domains. The Information Security risks, and risk appetite of Domains differ from one another, which in turn leads to a difference in implemented Information Security measures. In many cases these various measures aim to mitigate similar risks, and therefore achieve similar goals, but go about it in different ways. This hinders the understanding of implemented measures and levels of risks across Domains. In order to make communication about Information Security measures manageable and to lower barriers to interoperability, the clustering of security measures is a practical solution.

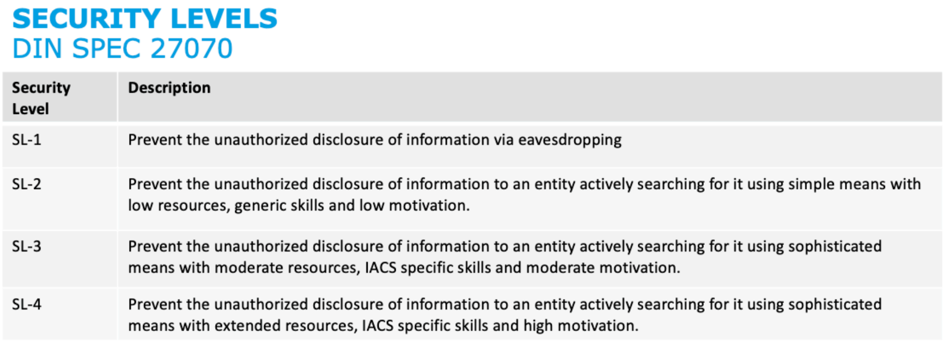
8.3.1 Information security clusters and levels

A security cluster can be defined as a set of Information Security measures which pursue the same objective. Clusters make it easier to communicate and understand the implemented security measures across Domains.

Depending on the use case, transactions may have higher or lower risk. For example, low-risk transactions, such as the sharing of personal preferences like shoe size, do not require the use of high amounts of Information Security. On the other hand, high-risk transactions, such as the sharing of personal medical data, require a very high amount of Information Security. The future Trust Framework should facilitate all types of use cases and therefore enable both high-risk and low-risk transactions. In order to reduce barriers for use, low-risk transactions should be facilitated though use of low Information Security levels and not be mandated to use high levels of Information Security measures. At the same time, the future Trust Framework should allow high security where needed to enable high-risk transactions. Security levels are a practical solution to facilitate this as these can be defined such that the security level is based on the security cluster requirements. See Box 9 for example of security levels used in data sharing.

Box 9: Security levels within DIN SPEC 27070

An example of security levels for data sharing can be seen in the DIN SPEC 27070 "Requirements and reference architecture of a security gateway for the exchange of industry data and services" which specifies the requirements to be met by a security gateway for data exchange across company and sector boundaries. See Figure 27 for an overview of the defined security levels.



SECURITY LEVELS
DIN SPEC 27070

Security Level	Description
SL-1	Prevent the unauthorized disclosure of information via eavesdropping
SL-2	Prevent the unauthorized disclosure of information to an entity actively searching for it using simple means with low resources, generic skills and low motivation.
SL-3	Prevent the unauthorized disclosure of information to an entity actively searching for it using sophisticated means with moderate resources, IACS specific skills and moderate motivation.
SL-4	Prevent the unauthorized disclosure of information to an entity actively searching for it using sophisticated means with extended resources, IACS specific skills and high motivation.

Figure 27: Example of security levels in the DIN SPEC 27070

The DIN SPEC 27070 defines an IDS connector as a security gateway for sending and receiving data, The IDS connector allows three different levels of security: Base, Trust, Trust+.

- The "base" profile meets basic security requirements for communication across company boundaries,
- The "trust" profile provides additional security features such as strict isolation of the service containers and mutual verification of integrity,
- The "trust+" profile provides additional protection against manipulation by malicious administrators.

(Source: https://www.internationaldataspaces.org/ids-is-officially-a-standard-din-spec-27070-is-published/)

Security levels based on requirements of security clusters facilitate different types of transactions. Security levels allow clear communication of various security requirements and support various implementations of INFORMATION SECURITY measures. Further, security levels reduce impact on DOMAIN participants which may have different security implementations as implementations can be easier understood, reducing analysis required of implementations. Further, participant implementations do not need to be adjusted in order to conform to specific standards.

In order to define security levels, INFORMATION SECURITY clusters should be defined. INFORMATION SECURITY clusters can be defined based on the Confidentiality and Integrity parts of the CIA triad can be used. The CIA topic of Availability can be considered as an operational agreement, and therefore is not applicable to TRUST FRAMEWORK security levels. For example: Public data used for many business processes should be readily available (high availability) and has low security requirements (low confidentiality). This example shows that the CIA principles are not all correlated, making the combination of clusters to a single usable security level impossible, unlike eIDAS LoAs. Therefore, Availability will not be included as a cluster to be combined to a single security level is not practical.

The number of security levels, and the definition of security clusters will be detailed in the next phase of the Data Sharing Coalition, once work on the future Cross-Domain Trust Framework starts.

8.3.2 Information security principles

A number of security principles have been identified which can be applied to the Harmonisation Canvas and future Cross-DOMAIN TRUST FRAMEWORK to guide all INFORMATION SECURITY discussions and decisions.

1. **Use of existing standards and consideration of best practices**
   This is a generic design principle for the Harmonisation Canvas but is especially important for the complex topic of INFORMATION SECURITY as standards provide a solid foundation of managing security.
2. **Fit-for-purpose security levels**
   This principle means facilitating low-risk transactions to use low information security measures to reduce barriers for use but allowing high security where needed to enable high-risk transactions.
3. **Organisational and technical security measures go hand-in-hand**
   INFORMATION SECURITY relies on technical and organisational measures which complement each other to enable a best solution to facilitate trust.
4. **Enable trust through security and privacy by design**
   Security and privacy are not only defensives mechanisms, but also enables trust. Therefore, Information Security must be rigorously included in the design of the future TRUST FRAMEWORK.

9 Data Service Exchange

9.1 Introduction

To achieve interoperable data sharing across domains, a technical communication standard (a so-called exchange protocol) should be defined in the future TRUST FRAMEWORK. Therefore, the functional DATA SERVICE exchange requirements should be determined before standardisation and implementation decisions of an exchange protocol are made. This chapter explores some of the functional data service exchange requirements.

9.2 Relevance

The complete DATA SERVICE exchange can be split into two distinct steps: DATA SERVICE DISCOVERY, and DATA SERVICE TRANSACTION, as shown in Figure 28. These steps should be carried out sequentially and, where possible automatically, without human interaction. In order for a DATA SERVICE CONSUMER to perform a DATA SERVICE TRANSACTION with a DATA SERVICE PROVIDER, they must first know that the service exists, meets their needs and if so, where to find the service. A DATA SERVICE PROVIDER must be discoverable to allow a DATA SERVICE CONSUMER to find the DATA SERVICE PROVIDER and its service(s). Once the DATA SERVICE CONSUMER has discovered the DATA SERVICE PROVIDER, they are able to perform a DATA SERVICE TRANSACTION without the need for re-discovery for subsequent transactions.

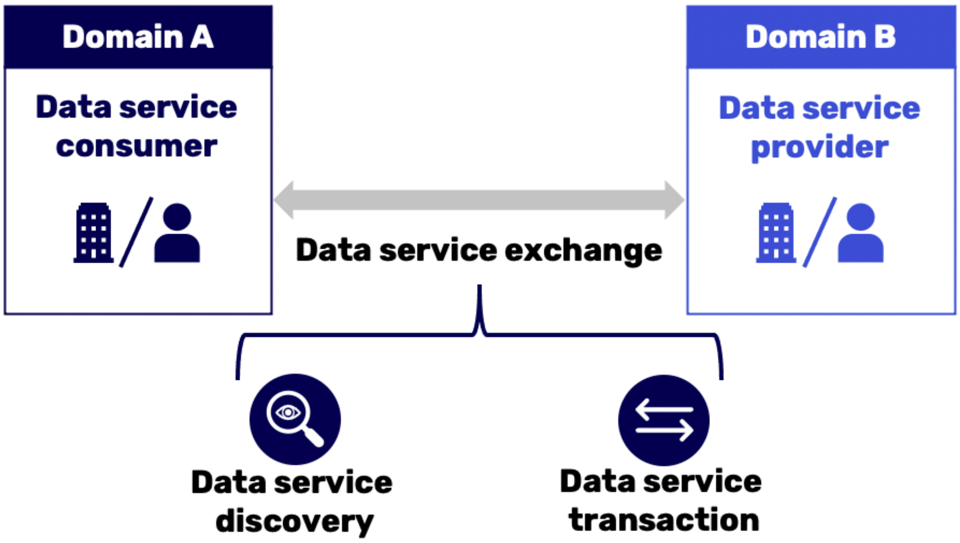


Figure 28: Data service consumers must discover services before they can make use of them.

9.3 Description

9.3.1 Data Service discovery

A DATA SERVICE DISCOVERY mechanism should be facilitated in the future TRUST FRAMEWORK and give answers to a number of different questions from the DATA SERVICE CONSUMER perspective, such as:

- What DATA SHARING DOMAINS are part of the TRUST FRAMEWORK?
- What data service providers are available?
- What data services do the DATA SERVICE PROVIDERS offer?
- Do DATA SERVICE PROVIDERS have data that is relevant for me?

A DATA SERVICE DISCOVERY mechanism facilitates the answering of these questions and should at least have the following characteristics:

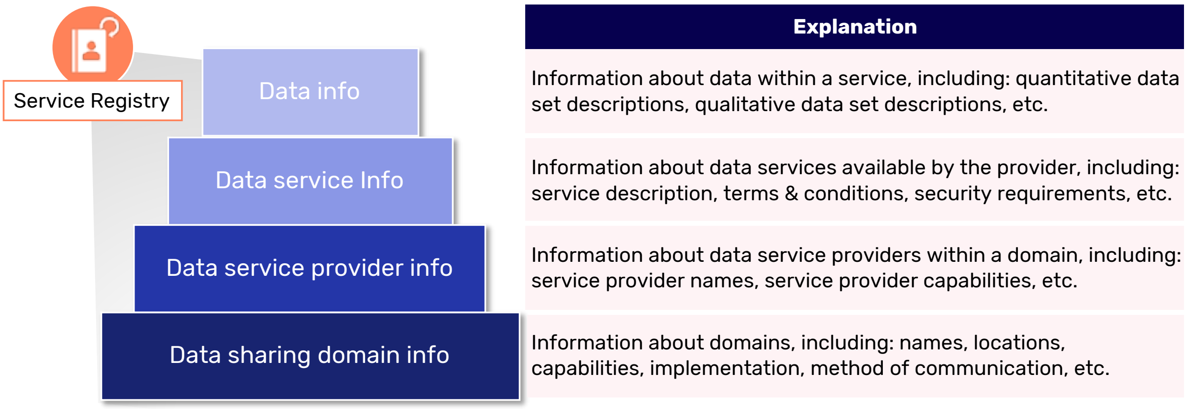
- Allows services to connect without manual intervention,
- Allows DATA SERVICE CONSUMERS to have access to all information needed to make a decision on whether to use the DATA SERVICE,
- Provides a clear communication from the DATA SERVICE PROVIDER to the DATA SERVICE CONSUMER through a common language (METADATA).

A solution to enable DATA SERVICE DISCOVERY is to maintain a SERVICE REGISTRY that contains service information for the purpose of discovery information. A SERVICE REGISTRY contains all the necessary information about all data services available and can be considered similar to a telephone book. Since the TRUST FRAMEWORK network is dynamic by nature, as domains and actors will change over time. Therefore, the SERVICE REGISTRY should be dynamic to facilitate this changing TRUST FRAMEWORK network.

At minimum, the SERVICE REGISTRY should include information about the DATA SHARING DOMAINS which are participating in the TRUST FRAMEWORK. This allows DATA SERVICE CONSUMERS to discover domains, after which they still need to find answers to the rest of their questions elsewhere to be able to determine if they can and want to make use of the specific DATA SERVICE. However, this is not a practical solution, and does not allow services to connect without manual intervention. Therefore, additional information should be included in the SERVICE REGISTRY to simplify the process of discovering DATA SERVICES by the DATA SERVICE CONSUMERS. The exact implementation choice of the SERVICE REGISTRY content will be made in designing the future TRUST FRAMEWORK, but one can imagine the TRUST FRAMEWORK SERVICE REGISTRY will contain information about (see Figure 29):

- DATA Information,
- DATA SERVICE Information,
- DATA SERVICE PROVIDER Information,
- DATA SHARING DOMAIN information.

Initial discussions in the Expert Group suggest that, practically, the SERVICE REGISTRY should contain at least DATA SHARING DOMAIN information and DATA SERVICE PROVIDER information. For DATA SERVICE CONSUMERS, this is the information needed for them to consider making use of the DATA SERVICE. If this information is included in the SERVICE REGISTRY, it relieves the DATA SERVICE CONSUMER of implementing complex discovery logic before making their consideration. In the next phase of the DATA SHARING COALITION an implementation choice needs to be made for the contents of the SERVICE REGISTRY.



	Explanation
Data info	Information about data within a service, including: quantitative data set descriptions, qualitative data set descriptions, etc.
Data service Info	Information about data services available by the provider, including: service description, terms & conditions, security requirements, etc.
Data service provider info	Information about data service providers within a domain, including: service provider names, service provider capabilities, etc.
Data sharing domain info	Information about domains, including: names, locations, capabilities, implementation, method of communication, etc.

Figure 29: The Service Registry can contain information about domains, service providers, services, and specific data

Data Service Providers require a mechanism to register their services in the Service Registry. It may not be desirable for all Data Service Providers to provide the same level of information in the Service Registry. Further, not all Data Service Providers may be able to or want to deliver all specified levels of information in the Service Registry as this may include sensitive data. In the future Trust Framework Data Service Providers should be able to register their services and be free to add information relevant to their services.

Based on industry standards a number of roles and functions have been identified that can facilitate Service Discovery. Two models are applicable for different perspectives in the Trust Framework. See Appendix 19 Data Service Discovery, for more information. In 'Client' side discovery the client is responsible for discovering services and performing transaction requests. For every request for discovery of a data service, the client will check a service registry to find relevant services. An alternative is 'Server' side discovery in which the client makes a discovery request towards a discovery server. The server is responsible for discovering services and returns the discovery response to the client. An implementation choice based on a detailed analysis should be made for the type of implementation of the Service Registry and implementation mechanism. This analysis should include the assessment of the desired location and distribution of the Service Registry. This could be a single central implementation, or a decentralised distribution.

It is likely that the desired implementation of the Data Service Discovery mechanism and the Service Registry will change over time given the maturity and development of the future Trust Framework. A basic implementation is likely sufficient initially, and this could be further developed to support additional services in the future. This should be taken into account in when making implementation choices for Data Service Discovery in the next phase of the Data Sharing Coalition.

9.3.2 Data Service Transaction

Functional Data Service exchange requirements for the future Trust Framework must be determined based on the data transfer characteristics of desired use cases. Data transfer characteristics influence the Data Service exchange, for example, transferring a small amount of data can be realised through sending the data in APIs, whereas transferring a large amount of data is not possible through APIs. For large amounts of data an FTP server could be used for example. Given the goal of the future Trust Framework to support a wide variety data sharing use cases possible within the possible Data Services, a number of identified data transfer characteristics should be supported. The following have been identified and will be taken into account in the further development of the future Trust Framework:

- Sharing of time-dependent data,
- One-time sharing of data,
- Continuous sharing of data,
- Sharing large amounts of data,
- Sharing small amounts of data,
- Sharing of live data,
- Sharing of static data.

10 Operational Agreements

10.1 Introduction

Within the future TRUST FRAMEWORK operational agreements help to facilitate the trust between actors that is needed for them to share data. Operational Agreements includes topics such as Service Level Agreements (SLAs), end user support, and DISPUTE MANAGEMENT. Within the Expert Group it was concluded that SLAs and end user support do not need to be harmonised between DOMAINS as these topics are part of domain-specific implementations without a cross-DOMAIN component. They come as part of the DATA SERVICE that needs to be accepted by the DATA SERVICE CONSUMER. However, the operating of a DISPUTE MANAGEMENT process has a cross-DOMAIN component as DISPUTE MANAGEMENT involves actors from different domains. Therefore, DISPUTE MANAGEMENT is a key topic which should be harmonised in the future TRUST FRAMEWORK to enable TRUST.

10.2 Relevance

A core component to create TRUST is setting clear expectations for all actors involved in the complete data sharing process, and subsequently meeting these expectations. This includes creating transparency in all phases of Data Sharing:

- before sharing data through TRUST FRAMEWORK agreements,
- during data sharing through DATA SERVICE TRANSACTION AGREEMENTS,
- after data sharing through DISPUTE MANAGEMENT.

A transparent DISPUTE MANAGEMENT process contributes to TRUST between actors.

10.3 Description

A DISPUTE arises when actors have a disagreement in which the actors cannot settle this between themselves. Three types of disputes have been identified which may occur within the future TRUST FRAMEWORK. Therefore, the processing and management of these should be supported in THE CROSS-DOMAIN TRUST FRAMEWORK.

1. A DATA SERVICE PROVIDER disputes an action from the DATA SERVICE CONSUMER. For example: The DATA SERVICE CONSUMER sells data obtained via a DATA SERVICE and this commercial use of the data goes against the terms and conditions of the agreement.
2. A DATA SERVICE CONSUMER disputes an action from the DATA SERVICE PROVIDER. For example: The data provided to the DATA SERVICE CONSUMER by the DATA SERVICE PROVIDER is not according to the DATA SERVICE CONSUMERS expectations (e.g. data quality is below what was advertised in the service description).
3. A DISPUTE between actors/domains and the CROSS-DOMAIN TRUST FRAMEWORK. For example: The TRUST FRAMEWORK AUTHORITY believes a DOMAIN no longer adheres to certain TRUST FRAMEWORK rules, and the DOMAIN disagrees.

The settlement of disputes should be facilitated by a neutral party to ensure that neither actors involved in a dispute gains an unfair advantage. For the first two types of disputes, the TRUST FRAMEWORK AUTHORITY can act as a neutral party to facilitate disputes between participants. When actors have a dispute with the TRUST FRAMEWORK AUTHORITY, the TRUST FRAMEWORK AUTHORITY is no longer neutral, and should not facilitate the DISPUTE management process itself.

10.3.1 Dispute management process

The complete Dispute Management process can be split into three high-level steps as shown in Figure 30.

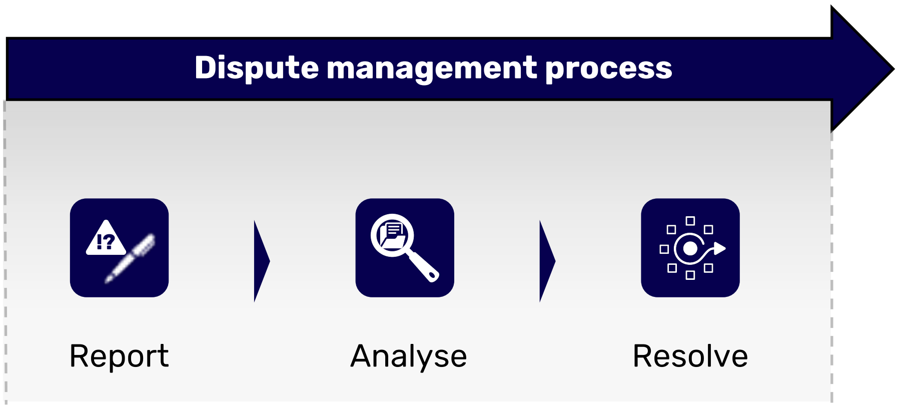


Figure 30: The three steps in managing a dispute in the Trust Framework

Report

A Dispute is reported only when actors within the Trust Framework cannot settle disagreements between themselves. Actors involved in disagreements should attempt to resolve these between themselves via bilateral communication. The Trust Framework should define service level agreements for the process of solving disagreements in order to clearly define when a disagreement becomes a dispute. If the actors cannot reach an agreement according to these service level agreements, they can report a dispute. When a dispute is reported to the Trust Framework Authority, a Dispute Case Manager should be assigned to facilitate the dispute management process for the actors involved in the dispute.

Analyse

In the next step of the Dispute Management process, a reported dispute is managed by the Dispute Case Manager based on input provided by the actors. This is an iterative process which shall be managed by the Dispute Case Manager. Actors in the dispute will provide input for the analysis and can provide evidence (e.g. audit trails, contracts, etc) and clarification on their position. The exact analysis process will probably not be defined in detail in the future Trust Framework as this is dependent on the dispute. Although the process is not fixed, the Trust Framework should define service level agreements for this process. This manages expectations of the actors involved and guides the process.

Resolve

The analysis leads to a decision on how to resolve the Dispute. The context of the Dispute influences the method of resolving Disputes. Dispute characteristics which impact the resolving of the Dispute include:

- Type of Dispute,
- Number of actors involved,
- Financial impact,
- Reputational impact.

The decision further includes the method to resolve the DISPUTE. A number of possibilities for the resolving of DISPUTES have been identified. This could be (any combination of):

- Repair, the DISPUTE was caused by an issue by an actor or the Trust Framework. The relevant party must update implementation accordingly,
- Fines, the party is fined based on the impact of the DISPUTE,
- Warning, (temporary) suspension or removal of actor from the TRUST FRAMEWORK.

If one of the actors involved in the DISPUTE does not agree with the DISPUTE resolution, they should be able to appeal the decision. The facilitation of an appeal process in the future TRUST FRAMEWORK further adds towards building trust required for DATA SHARING. This appealing process must be further developed in the future TRUST FRAMEWORK.

The need for a detailed and operational appeal process will depend on the scale and maturity of the future Trust Framework network. Therefore, when developing the Trust Framework possible solutions should be balanced against the need and costs of solutions implemented. In the Expert Group possible solutions have been identified through the instantiation of a neutral party or arbitration committee, which can be considered a starting point for determining a solution.

11 Business Models

11.1 Introduction

Business models describe how organisations create and capture value, in the context of the DATA SHARING COALITION, specifically through providing DATA SERVICES. Business models in the TRUST FRAMEWORK describe how the value of a DATA SERVICE is compensated for between actors. As the future TRUST FRAMEWORK should facilitate a wide variety of use cases, multiple business models for CROSS-DOMAIN DATA SHARING should be facilitated in the future TRUST FRAMEWORK agreements.

11.2 Relevance

Actors in a DATA SERVICE should agree to a business model before performing a DATA SERVICE TRANSACTION. To this end, the Data Service Provider should communicate the relevant business model information to all potential Data Service Consumers during Data Service Discovery (see chapter 9.3.1). Further, once the financial compensation is agreed, a mechanism to settle this across domains is needed. Therefore, agreements to enable the communication of business models and facilitate financial clearing and settlement are required in the future Trust Framework.

11.3 Description

A compensation mechanism is needed to facilitate the financial compensation between actors involved in the DATA SERVICE TRANSACTION. Examples of compensation mechanisms include, but are not limited to:

- Fees per transaction,
- Recurring fees,
- Flat fees,
- Fee per record of data,
- Fees dependent on data usage.

The compensation mechanism of a use case, is dependent on its characteristics, and could include factors such as:

- Actors involved,
- Data service type,
- Value of the data service.

In practice, many of these compensation mechanisms seem realistic for CROSS-DOMAIN DATA SHARING use cases, and therefore these should be investigated for inclusion in the future Trust Framework. Note that it is likely that there will be plenty of use cases that explicitly do not have business models or compensation mechanism implemented, and this possibility should also be included. See Table 7 for examples of compensation mechanisms used in DATA SHARING COALITION use cases.

In general, in Data Services, there should be value for both DATA SERVICE CONSUMER and DATA SERVICE PROVIDER in every DATA SERVICE TRANSACTION. Based on the specific CROSS-DOMAIN DATA SERVICE and what actors aim to achieve through the DATA SERVICE, the value each actor perceives is not always obvious. In vase of an imbalance of perceived value, one actor may need to compensate the other for the DATA SERVICE, as it could be expected that the actor who experiences the most value should financially compensate the other actor. Examples of the value experienced by actors in the Data Sharing Coalition use cases are shown in Table 7.

Table 7: Examples of value and compensation mechanisms used in Data Sharing Coalition use cases

Use case	Value for Data Service Consumer	Value for Data Service Provider	Compensation mechanism
Weed Robot	Famers have guaranteed removal of weeds from land with minimal pesticide usage and damage to crops	Scanned data can be used by weed whacking party to further train algorithms and provide better services	To be decided
Benchmarking for industry associations	Industry associations members can make strategic decisions based on benchmarks performed by the industry association	Industry association gains insights in and for the whole sector and can provide additional benchmarking services to its members	Annual membership fee paid by members to the industry association or a fee per benchmark
Green Loans	Financial domain obtains insights in customer energy usage to deliver advice and loans for sustainable measures to customers, driving new business	Energy system operators allow consumer to use energy data in new contexts; fulfil their societal obligation of facilitating the use of energy data	None
VODAN	Research institution realises Societal value; data is being used for effectively battling COVID-19	Researchers ability to analyse larger datasets, allowing algorithms to discover meaningful patterns in COVID-19 infections	None
Sharing shipment data with insurers	Insurer receives structured and machine-readable data that can be used in their services to enable improved processes and risk management	Logistics organisations can share their trade documentation in one click with control over their data and without the administrative burden of paper-based documents	To be decided, as it is not clear what actor experiences the most value

To enable trust needed for a DATA SERVICE the DATA SERVICE CONSUMER must be aware of the business model of a DATA SERVICE before choosing to make use of it. To this end the business model and compensation mechanism should be clear and transparent upfront and DATA SERVICE PROVIDERS should include the business model in DATA SERVICE information, as introduced in chapter 9.3.1 Data Service discovery. How this will be accomplished should be detailed in the future Trust Framework.

Once the DATA SERVICE CONSUMER is aware of the business model of a DATA SERVICE, they can choose to accept that business model. After acceptance of the Data Service with accompanying business model in the DATA SERVICE TRANSACTION AGREEMENT, the DATA SERVICE can be consumed. Therefore, acceptance of the business model is conditional to making use of the DATA SERVICE.

Dependent on the business model, the financial compensation for consuming a DATA SERVICE should be settled between actors. The settlement of the financial compensation could be based on the actual usage. To enable financial compensation based on usage, transactions should be captured in METADATA which can be used in settlement calculations, see 14 METADATA for more information.

The process for clearing and settlement of the agreed financial compensation could still pose a hurdle for INTEROPERABILITY and scale. If all DOMAINS organise their payments in a non-standardised way this is not scalable as each DOMAIN would need bilateral implementations to compensate each other. Therefore, a clearing and settlement mechanism can be considered in the future TRUST FRAMEWORK. The need and costs of clearing and settlement services are dependent on the scale and maturity of the TRUST FRAMEWORK. This dependency of costs of clearing and settlement services on TRUST FRAMEWORK should be taken into account in the decision towards the use of a centralised or decentralised clearing and settlement mechanism within the TRUST FRAMEWORK.

Possible solutions for financial clearing and settlement have been identified in the Expert Group and shall be further investigated in the next phase of the DATA SHARING COALITION. One possibility includes that clearing and settlement is facilitated by a separate decentralised broker. The context broker[4] as defined by CEF Digital is an example of a decentralised broker. Within the future TRUST FRAMEWORK, a decentralised broker role could be fulfilled by the TRUST FRAMEWORK AUTHORITY, or a separate service provider.

It could be that the PROXY will have a role in clearing and settlement, to reduce the impact on DATA SERVICE CONSUMERS and DATA SERVICE PROVIDERS. The exact mechanism for clearing and settlement and the role of the Proxy in this will be determined in the future TRUST FRAMEWORK.

[4] Source: https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/Context+Broker

12 Governance

12.1 Introduction

The future Trust Framework agreements and network should be continuously managed and maintained to ensure alignment with future wishes and requirements of participants. In order to achieve the management and maintenance of the TRUST FRAMEWORK agreements and network a TRUST FRAMEWORK GOVERNANCE is needed.

12.2 Relevance

GOVERNANCE is needed for the development and subsequent management of the TRUST FRAMEWORK. These two phases can be considered separately:

1. **Trust Framework development**
   The initial development of the TRUST FRAMEWORK agreements is planned in the next phase of the DATA SHARING COALITION, when the first version of the Trust Framework agreements are co-created in a project setting by participants delegated by members of a so-called "coalition of the willing". This project has a typical co-creation governance, in which the delegates of the coalition of the willing will decide on all the content of the TRUST FRAMEWORK.
2. **Trust Framework management**
   Once the first version of the TRUST FRAMEWORK has been developed and implemented, its agreements and network of participants should be managed. Participants want to influence the future developments of the TRUST FRAMEWORK to ensure alignment with their future wishes and requirements, in order to protect their investment during the development phase. This continuous management requires a neutral governing body which should be described in the TRUST FRAMEWORK agreements and thus be shaped and determined in the initial development phase.

12.3 Description

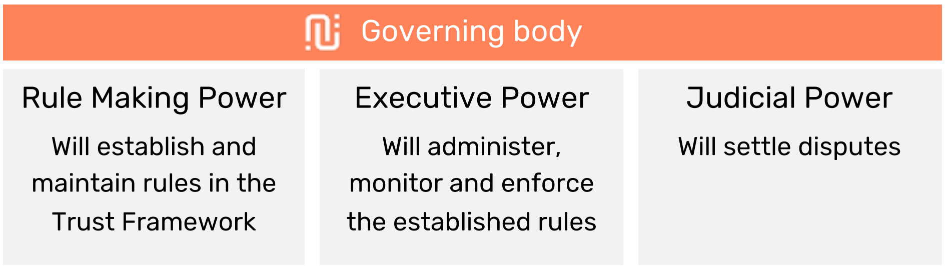
12.3.1 Trust Framework Development

Through a co-creation project the coalition of the willing shall develop the TRUST FRAMEWORK agreements in the next phase of the DATA SHARING COALITION.

A project GOVERNANCE structure will be instantiated for the initial development of the TRUST FRAMEWORK agreements. This project governance structure will be determined before starting the next phase of the DATA SHARING COALITION. The TRUST FRAMEWORK agreements should include a description of the GOVERNING BODY required for phase 2: TRUST FRAMEWORK management and maintenance.

12.3.2 Trust Framework Management

The TRUST FRAMEWORK agreements will contain a description of the TRUST FRAMEWORK GOVERNING BODY structure, roles and responsibility. The roles and responsibility will be described based on the so-called Trias Politica separation of powers, see Figure 31. This separation of powers is useful in describing and categorising the TRUST FRAMEWORK GOVERNANCE functionality and structure. However, it is likely not practical to realise a pure separate governance entity from the start, because financing separate entities is costly, as each power requires similar resources and capabilities. Further, it is expected that there will not be many disputes in the Trust Framework, and therefore the judicial power will not have a large role. Further, the implementation of the Governance is based on the level of maturity and size of the ecosystem, and therefore is subject to change over time. The exact realisation of the Governing Body will be determined in the Trust Framework development phase.



Governing body

Rule Making Power

Will establish and maintain rules in the Trust Framework

Executive Power

Will administer, monitor and enforce the established rules

Judicial Power

Will settle disputes

Figure 31: The separation of powers in the Trust Framework Governing Body

Rule Making Power

The Rule Making Power establishes and maintains the Trust Framework agreements. The Trust Framework agreements need to be continuously maintained and updated to ensure alignment with future wishes and requirements of participants. To facilitate this, the functionality of Trust Framework agreement management has been identified.

Executive Power

The Executive Power administers, monitors and enforces the established Trust Framework agreements and contains all necessary functions to run and manage the Trust Framework. The future Trust Framework network needs to be actively managed to enable Cross-Domain Data Services for participants and the enrolment of new participants. Further, The Trust Framework network should be monitored to ensure participants meet the set rules and agreements. Additional roles may be needed to realise efficiencies within the Trust Framework network, such as providing standardised test tools. All of these functionalities can be considered elements of the Executive Power. A number of functionalities have been identified which will be detailed further in the next phase of the Data Sharing Coalition:

- Enforcement body,
- Monitoring body,
- Marketing,
- Service Registry management,
- Participant enrolment,
- Facilitating test tooling,
- Change and release management,
- Knowledge management.

Judicial Power

The Judicial Power plays a role in settling disputes. This includes the role of Dispute Case Manager, as described in 10.3.1 Dispute management process.

12.3.3 Trust Framework Governance representation and financing

The Governing Body of the Trust Framework must be financed so that it has the resources to achieve its goals of developing and managing the future Trust Framework. Financing is possible through various means such as:

- Subsidy,
- Recurring fees for participants,
- Fees based on Trust Framework usage.

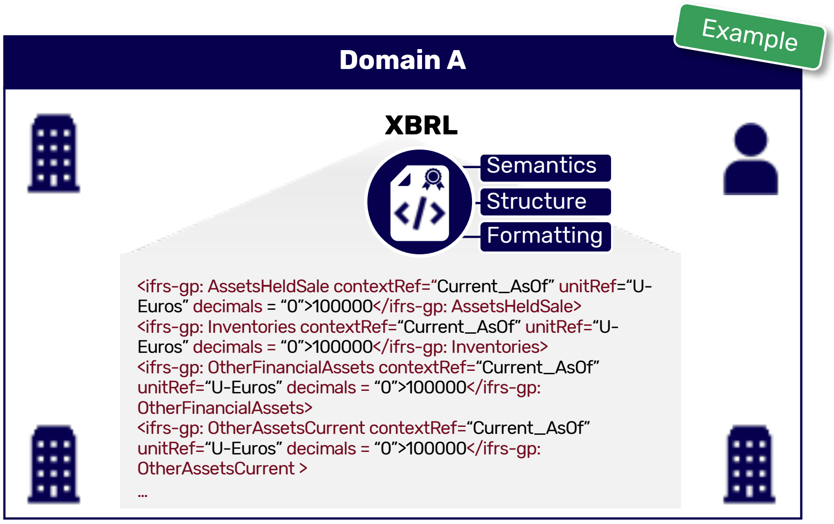
The financing model of the Governing Body is dependent on the value and maturity of the complete Trust Framework ecosystem which impacts the willingness-to-pay of participants. Initially, when the value of the Trust Framework is not clear to participants, the willingness-to-pay may be low. However, once the Trust Framework has proven its value, the willingness-to-pay of participants may increase. Therefore, the financing model of the Trust Framework Governance is subject to change over time and this should be taken into account in the Trust Framework.

In governance structures the participant representation often has an impact on their influence. In practice, participant representation is often closely linked to the financing of the Trust Framework and participant contribution. In existing Data Sharing Domains the link between financing and influence has been identified as an issue, as participants who have the most influence may not act in the best interest of the complete ecosystem. Therefore, this issue should be addressed, and lessons learned by other Domains should be taken into account when determining the Governance of the future Trust Framework. The financing of the Trust Framework Governance and participant representation in the Governing Body will be determined in the Trust Framework development phase.

13 Data Standards

13.1 Introduction

DATA STANDARDS are standards that provide the semantics, structure and formatting of data. DATA STANDARDS are used to ease communication and create a mutual understanding between actors sharing data. See Figure 32 for an example of the use of a DATA STANDARD within a single DOMAIN.



```
<ifrs-gp: AssetsHeldSale contextRef="Current_AsOf" unitRef="U-
Euros" decimals = "0">100000</ifrs-gp: AssetsHeldSale>
<ifrs-gp: Inventories contextRef="Current_AsOf" unitRef="U-
Euros" decimals = "0">100000</ifrs-gp: Inventories>
<ifrs-gp: OtherFinancialAssets contextRef="Current_AsOf"
unitRef="U-Euros" decimals = "0">100000</ifrs-gp:
OtherFinancialAssets>
<ifrs-gp: OtherAssetsCurrent contextRef="Current_AsOf"
unitRef="U-Euros" decimals = "0">100000</ifrs-gp:
OtherAssetsCurrent >
...
```

Figure 32: Example of XBRL used as a DATA STANDARD within a Domain

13.2 Relevance

DATA STANDARDS are used to create a mutual understanding on the semantics, structure and formatting of data used in data pull and data push DATA SERVICES, as well as the data exchange towards algorithms. See Box 10 for a description of the differences between Data Standards and algorithm standards. For data transfer in DATA SERVICES, DATA STANDARDS can be used to ensure a mutual understanding of the data used.

Box 10: Algorithms

Algorithms differ greatly from data when considering the standards used. Data in a specific DATA STANDARD often can be mapped to another DATA STANDARD and be useable. For example, an XBRL data set can be easily converted to be represented in an XLSX file. This is not the case for algorithms. Algorithms are a sequence of instructions to perform a specific computation. Algorithms in computation are written in a certain software to perform their intended task. The algorithm cannot function within other software, and therefore the mapping of algorithms to other standards is not always possible without human interaction. For example, if an algorithm is written in Java, it cannot be easily converted to work in Python.

In the context of the DATA SHARING COALITION, an algorithm requires data for it to function. This data will be in a specific format and should be transferred to the algorithm for it to function. For this data transfer the mutual understanding of DATA STANDARDS applies.

DOMAINS within the future TRUST FRAMEWORK all make use of different DATA STANDARDS. Even within DOMAINS there is a variety of DATA STANDARDS used for a variety of specific use cases. Within a DOMAIN, the DATA SERVICE PROVIDER and DATA SERVICE CONSUMER are familiar with each other and can communicate about the DATA STANDARDS used for specific DATA SERVICES offered. For DATA SERVICES that operate across DOMAINS, the data used within DOMAINS needs to be understandable to other DOMAINS. To this end, the DATA STANDARD used should be communicated across DOMAINS to facilitate understanding of the data by the DATA SERVICE CONSUMER.

13.3 Description

The DATA STANDARD used in DATA SERVICES is dependent on a number of different factors such as actors involved, DOMAINS involved and service offered, etc. For example, in some cases, the DATA SERVICE PROVIDER determines the DATA STANDARD used in their service. If the service is used by many different DATA SERVICE CONSUMERS, they will likely not alter their standards used for a single DATA SERVICE CONSUMER. However, in some cases a single DATA SERVICE CONSUMER has sufficient power and influence that a DATA SERVICE PROVIDER is willing to alter the DATA STANDARDS used in their service to accommodate their specific needs. Additionally, there are instances where a single DATA SERVICE supports the use of multiple DATA STANDARDS.

As there is a wide variety of DATA STANDARDS used across DATA SERVICES, every DATA SERVICE should explicitly communicate what DATA STANDARD they make use of before a DATA SERVICE TRANSACTION can take place. To achieve this a common language should be created to enable communication of the used DATA STANDARD across domains.

In order to realise efficiencies and enable scalability within the future TRUST FRAMEWORK, the communication of the used DATA STANDARD should be implemented in a machine-readable way. Therefore, DATA STANDARDS should be communicated in METADATA, see Chapter 14 METADATA for more information. To enable all possible DATA STANDARDS to be used within DATA SERVICES in the future TRUST FRAMEWORK, the TRUST FRAMEWORK should be DATA STANDARD agnostic to support all DATA STANDARDS used in different DOMAINS.

An alternative to describing used DATA STANDARDS in METADATA is to define a single DATA STANDARD to be used by all DOMAINS. The Expert Group has identified that it is not always possible to describe a single DATA STANDARD that covers all requirements. Even within DOMAINS it is often difficult to define a single DATA STANDARD to be used. Due to the effort it would take to align all DOMAINS on a single DATA STANDARD, it is not feasible to create a DATA STANDARD for the TRUST FRAMEWORK. Therefore, the standardisation of DATA STANDARDS is left out of scope for the future TRUST FRAMEWORK. However, the HARMONISATION of data standards through bilateral agreements should remain possible to TRUST FRAMEWORK participants.

14 Metadata

14.1 Introduction

Metadata describes everything about data, Data Services, and Data Service Transactions in Data Sharing that cannot be assumed to be known by actors involved in Data Service Transactions. Metadata provides a common language through which actors can communicate with each other across domains in a machine-readable way, to create a shared understanding. Within the future Trust Framework, Metadata is needed to achieve a number of different goals:

- Enable scalability and efficiencies by providing machine-readable information,
- Facilitate the discovery of Data Services,
- Provide input on the Data Service for post-transactional processes.
- Enable future developments of the Trust Framework, by being extensible by default.

Within the context of the Data Sharing Coalition, Metadata concerns the Data Service Transaction itself and does not include the logging that takes place afterwards.

Note: The Expert Group has identified that the logging of actions after a Data Service Transaction has taken place, should also be considered as part of Metadata as this is required for audit trails. In a future Expert Group session we will determine the minimal logging requirements for dispute resolution and this chapter will be updated accordingly.

14.2 Relevance

In a Cross-Domain Data Service, Metadata is created at two distinct phases in time in order to achieve the goals described above. Metadata is created before a Data Service Transaction and at the moment of a Data Service Transaction, as shown in Figure 33. Before a Data Service Transaction, Metadata provides a Data Service description, which allows services to be discovered and actors to decide whether or not to engage in a Data Service Transaction Agreement. At the moment of a Data Service Transaction, Metadata is created to describe the Data Service Transaction and the Data Service Transaction Agreement. See 9.3.2 Data Service Transaction, for an overview of the characteristics of Data Service Transactions.

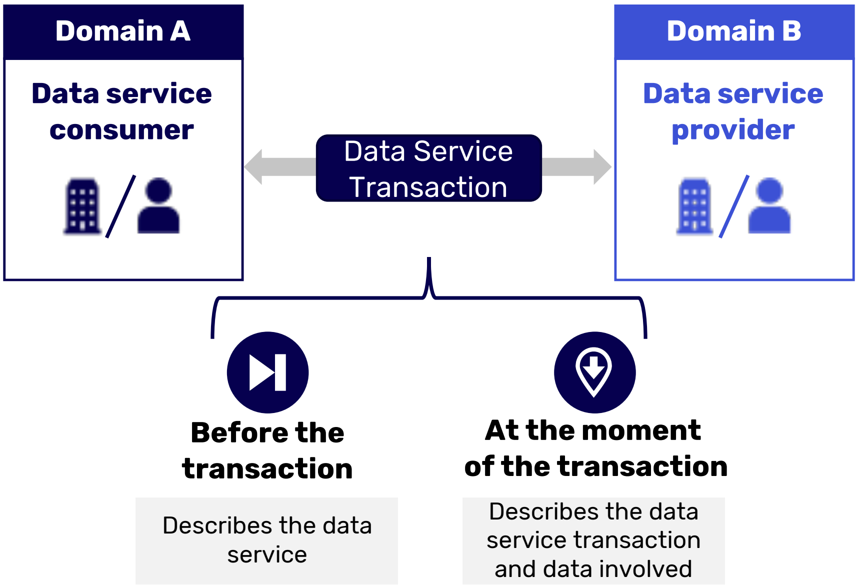

Domain A
Data service consumer
Data Service Transaction
Domain B
Data service provider
Before the transaction
Describes the data service
At the moment of the transaction
Describes the data service transaction and data involved

Figure 33: METADATA is created before and at the moment of a DATA SERVICE TRANSACTION

One of the participants of the DATA SHARING COALITION, GO FAIR, have described a number of guiding principles for the reuse of digital assets for scientific data. METADATA plays a large role in fulfilling the FAIR principles, which can also be generically applied to CROSS-DOMAIN DATA SHARING beyond the scientific DOMAIN. See Box 11 for a description of the FAIR guiding principles.

Box 11: FAIR Data Principles

The FAIR Data Principles provide guidelines for DOMAINS and organisations to improve the findability, accessibility, interoperability, and reuse of digital assets. The principles are an extensive list that emphasises the need to make data machine-actionable to deal with its increased volume, complexity, and speed of data creation. The FAIR Data Principles indicate that data needs to be:

Findable

The first step in (re)using data is to find them. METADATA and data should be easy to find for both humans and computers. Machine-readable METADATA are essential for automatic discovery of data and data services.

F1. (Meta)data are assigned a globally unique and persistent identifier,
F2. Data are described with rich METADATA (defined by R1 below),
F3. METADATA clearly and explicitly include the identifier of the data they describe,
F4. (Meta)data are registered or indexed in a searchable resource.

Accessible

Once the user finds the required data, they need to know how they can be accessed, possibly including authentication and authorisation.

A1. (Meta)data are retrievable by their identifier using a standardised communications protocol,

A1.1 The protocol is open, free, and universally implementable,

A1.2 The protocol allows for an authentication and authorisation procedure, where necessary,

A2. METADATA are accessible, even when the data are no longer available.

Interoperable

The data usually need to be integrated with other data. In addition, the data need to interoperate with applications or workflows for analysis, storage, and processing.

I1. (Meta)data use a formal, accessible, shared, and broadly applicable language for knowledge representation.

I2. (Meta)data use vocabularies that follow FAIR principles

I3. (Meta)data include qualified references to other (meta)data

Reusable

The ultimate goal of FAIR is to optimise the reuse of data. To achieve this, METADATA and data should be well-described so that they can be replicated and/or combined in different settings.

R1. Meta(data) are richly described with a plurality of accurate and relevant attributes,

R1.1. (Meta)data are released with a clear and accessible data usage license,

R1.2. (Meta)data are associated with detailed provenance,

R1.3. (Meta)data meet domain-relevant community standards.

Source: https://www.go-fair.org/fair-principles/

14.3 Description

14.3.1 Before the Data Service Transaction

Before data can be shared, relevant DATA SERVICE information needs to be clear to all actors involved in the DATA SERVICE TRANSACTION. To this end, the potential DATA SERVICE CONSUMER first needs to discover the data service, as described in 9.3.1 DATA SERVICE DISCOVERY. After the data service discovery, the potential DATA SERVICE CONSUMER should have access to all DATA SERVICE information needed to come to a decision on whether or not to make use of the DATA SERVICE. Throughout the previous chapters of this document, a number of topics have been identified (see Table 8) which should be described in METADATA before the DATA SERVICE TRANSACTION.

Table 8: Overview of categorised identified Metadata topics

	Before the transaction	At the moment of the transaction
Actor information	• Domain information • Data service provider information • Role information	• Data service provider information • Data service consumer information • Role information
Data Service information	• Terms and conditions • Business model	• Negotiated Terms and conditions • Negotiated Business model
Data Service Transaction information	• Security level requirements	• Data service transaction agreement • Security level • Consent • Transaction actions (for audit trails
Data information	• Data description • Data standards • Data quality	• Data standards • Data quality

The identified topics actively contribute towards fulfilling the FAIR guiding principles (see Box 11) and can be categorised as shown in the left column of Table 8.

14.3.2 At the moment of the Data Service Transaction

At the moment of a Data Service Transaction, Metadata is created to be used in processes after the Data Service Transaction. Specific actions during the Data Service Transaction should be captured in Metadata to be used for a number of different purposes, including:

- Register the accepted Data Service,
- Data analysis,
- Auditing,
- Clearing and settlement.

As shown in Table 8, topics have been identified which should be captured in Metadata at the moment of the Data Service Transaction. The topics can be categorised as shown in the right column of Table 8, and actively contribute towards fulfilling the FAIR guiding principles (see Box 11).

14.3.3 Metadata in the future Trust Framework

In the next phase of the Data Sharing Coalition, the Metadata implementation of the future Trust Framework will be specified, based on the high-level business requirements described here. An investigation into existing Metadata implementations in Domains and by other Data Sharing Initiatives will be done to analyse where existing Metadata standards can be used in the future Trust Framework.

15 Manifestation of topics in the Trust Framework

The common agreements that will be made by the DATA SHARING COALITION will be captured in one comprehensive document, the future Cross-Domain Trust Framework. The document will specify agreements and requirements that DATA SHARING DOMAINS should adhere to. Every topic that has been discussed in this HARMONISATION CANVAS will become part of the future TRUST FRAMEWORK and will be analysed across five disciplines: Business, Legal, Operational, Functional and Technical (BLOFT).

Note: More detail on the contents of this chapter will be included when more topics have been discussed, to enable uniformity on the manifestation in Trust Framework across different topics.

15.1 Terms and conditions

The topic TERMS AND CONDITIONS will be discussed in all BLOFT dimensions (Business, Legal, Operational, Functional and Technical) as it is connected to multiple different topics (e.g. IAA, metadata, business model). The general outline of the topic will be discussed in the Functional part of the BLOFT dimensions of the future CROSS-DOMAIN TRUST FRAMEWORK, as how organisations have to deal with, and handle conditions is a functional aspect.

Steps to take in the next phase to come to agreements for the future CROSS-DOMAIN TRUST FRAMEWORK are/can be:

- Make implicit TERMS AND CONDITIONS more explicit,
- Finalise TERMS AND CONDITIONS clusters,
- Create levels for TERMS AND CONDITIONS clusters,
- Decide on metadata language for TERMS AND CONDITIONS.

15.2 Identification, Authentication and Authorisation

The general outline of the topic will be discussed in mainly the Functional and Technical part of the BLOFT dimensions of the TRUST FRAMEWORK, as these are the most important topics regarding how organisations have to deal with and handle IDENTIFICATION, AUTHENTICATION and AUTHORISATION.

Steps to take in the next phase for the TRUST FRAMEWORK in working towards agreements are/can be:

- Include explicit definitions for identifier prefixes,
- Define standard LoAs based on eIDAS,
- Further investigate and define usage of Qualified Trust Services,
- Define interoperable UX standards,
- Define requirements needed to facilitate the distribution of AUTHORISATION roles across DOMAINS,
- Investigate and define a method of validating Pre-configured DELEGATION,
- Discuss and define the redirects and user interface requirements needed for interoperable human to machine AUTHENTICATION.

15.3 Legal Context

Legal context is of vital importance to establish trust required to share data. The general outline of the topic will be discussed in the Legal and functional parts of the BLOFT dimensions of the TRUST FRAMEWORK.

Steps to take in the next phase for the TRUST FRAMEWORK in working towards agreements are/can be:

- Specify the functionality of a chain of bilateral agreements,
- Investigate the role of a Trust Framework Authority with functions of monitoring and enforcement body,
- Investigate a number of open legal topics to ensure they are covered within the Trust Framework.

15.4 Information Security

Managing Information Security risk is essential to establish trust required to share data. The general outline of the topic will be discussed in mainly the Organisational and Technical part of the BLOFT dimensions of the TRUST FRAMEWORK, as these are the most important topics regarding how organisations implement Information Security.

Steps to take in the next phase for the TRUST FRAMEWORK in working towards agreements are/can be:

- Define INFORMATION SECURITY clusters
- Define security levels and requirements based on security clusters
- Specify how security levels can be communicated within metadata

15.5 Data Service Exchange

The functional data service exchange requirements should be determined before implementation decisions of an exchange protocol are made as these have an impact on the functionality of the future TRUST FRAMEWORK. The general outline of the topic will be discussed in mainly the Business and Technical part of the BLOFT dimensions of the TRUST FRAMEWORK, as these are the most important topics regarding how data service exchange can be realised.

Steps to take in the next phase for the TRUST FRAMEWORK in working towards agreements are/can be:

- Determining the contents of the SERVICE DIRECTORY,
- Defining the DATA SERVICE DISCOVERY mechanisms,
- Specifying Functional DATA SERVICE exchange requirements based.

15.6 Operational Agreements

Within the topic of Operational Agreements, Dispute Management is a key topic which should be harmonised in the future Trust Framework to enable Trust. The general outline of the topic will be discussed in mainly the Operational part of the BLOFT dimensions of the Trust Framework, as this is the most important topic regarding a Dispute Management Process.

Steps to take in the next phase for the Trust Framework in working towards agreements are/can be:

- Describe a Dispute Management Process,
- Define SLAs for the process of solving disputes,
- Define SLAs for the analyse of reported disputes,
- Determine the need and extent of an appeal process.

15.7 Business Models

The future Trust Framework should support a wide variety of use cases with a variety in business models, therefore all possible business models should be facilitated. The general outline of the topic will be discussed in mainly the Business and Technical parts of the BLOFT dimensions of the Trust Framework, as these are the most important topics regarding use case business models and implementation of these.

Steps to take in the next phase for the Trust Framework in working towards agreements are/can be:

- Investigate the need to support all possible compensation mechanisms in the future Trust Framework,
- Define a method to communicate use case business model across Domains,
- Investigate the need for a financial clearing and settlement function in the future Trust Framework,
- Determine the role of the Proxies in Clearing and Settlement.

15.8 Governance

Governance is needed to develop and subsequently manage the Trust Framework agreements and network. The general outline of the topic will be discussed in mainly the Legal and Operational part of the BLOFT dimensions of the Trust Framework, as these are the most important topics regarding use case business models and implementation of these.

Steps to take in the next phase for the Trust Framework in working towards agreements are/can be:

- Determine a coalition of the willing who will decide on the content of the Trust Framework,
- Define a description of the Governing Body in the initial Trust Framework agreements,
- Describe Governance functionality split by the Trias Politica separation of powers,
- Determine a Governance representation and financing model.

15.9 Data Standards

DATA STANDARDS are standards that provide the semantics, structure and formatting of data, and are used in the Trust Framework to create a mutual understanding between actors sharing data. The general outline of the topic will be discussed in mainly the Technical part of the BLOFT dimensions of the TRUST FRAMEWORK.

Steps to take in the next phase for the TRUST FRAMEWORK in working towards agreements are/can be:

- Ensure the TRUST FRAMEWORK is data standard agnostic,
- Enable the communication of data standards within METADATA.

15.10 Metadata

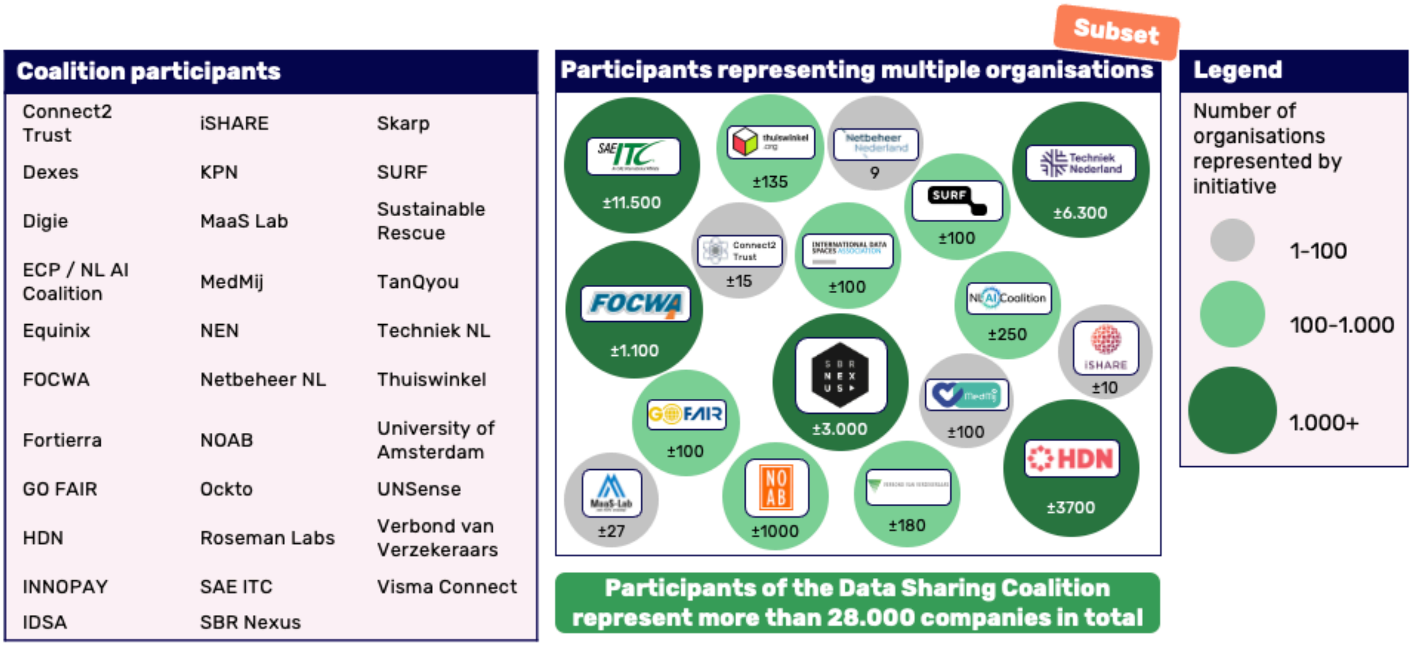
METADATA is needed in the TRUST FRAMEWORK to enable scalability and efficiencies by providing machine-readable information before and after DATA SERVICE TRANSACTIONS. METADATA concerns all dimensions of the BLOFT framework, but the general outline of the topic will be discussed in mainly the Technical part of the BLOFT dimensions of the TRUST FRAMEWORK.

Steps to take in the next phase for the TRUST FRAMEWORK in working towards agreements are/can be:

- Determine existing METADATA languages which can be used to describe all topics identified to be part of METADATA,
- Decide on the METADATA language used in the TRUST FRAMEWORK,
- Define a shared data ontology that defines different levels for different data constructs,
- Describe the technical implementation of METADATA.

Section C. Appendix

16 Data Sharing Coalition Overview



Coalition participants

- Connect2 Trust
- Dexes
- Digie
- ECP / NL AI Coalition
- Equinix
- FOCWA
- Fortierra
- GO FAIR
- HDN
- INNOPAY
- IDSA
- iSHARE
- KPN
- MaaS Lab
- MedMij
- NEN
- Netbeheer NL
- NOAB
- Ockto
- Roseman Labs
- SAE ITC
- SBR Nexus
- Skarp
- SURF
- Sustainable Rescue
- TanQyou
- Techniek NL
- Thuiswinkel
- University of Amsterdam
- UNSense
- Verbond van Verzekeraars
- Visma Connect

Participants of the Data Sharing Coalition represent more than 28.000 companies in total

Figure 34: Overview of Data Sharing Initiatives within the DSC

Table 9: Overview of Expert Group participants and their organisations

Organisation	Name
Dexes	Hayo Schreijer
Dexes	Joep Meindertsma
Dexes	Willem ter Berg
GO FAIR	Bert Meerman
HDN	Arjen de Bake
HDN	Jan Schrama
INNOPAY	Vincent Jansen
International Data Spaces Association	Sebastian Steinbuss
iSHARE	Gerard van der Hoeven
iSHARE / Visma Connect	Marnix Vermaas
MedMij	Johan Hobelman
MedMij	Casper van der Harst
NEN	Jolien van Zetten
Netbeheer Nederland	Edwin Edelenbos
SAE ITC	Lisa Spellman
SBR Nexus	Gerard Huis in 't Veld
SIVI	Robin Oostrum
SURF	Erik Kentie
SURF	Michiel Schok
SURF	Freek Dijkstra

Organisation	Name
University of Amsterdam	Leon Gommans
University of Amsterdam	Wouter Los
University of Amsterdam	Tom van Engers
Visma Connect	Elsbeth Bodde
Visma Connect	Victor den Bak

17 Interoperability and harmonisation

17.1 Steps to reach a data service transaction agreement

In a DATA SERVICE TRANSACTION AGREEMENT between a DATA SERVICE CONSUMER and a DATA SERVICE PROVIDER, POLICIES apply. See Figure 35.

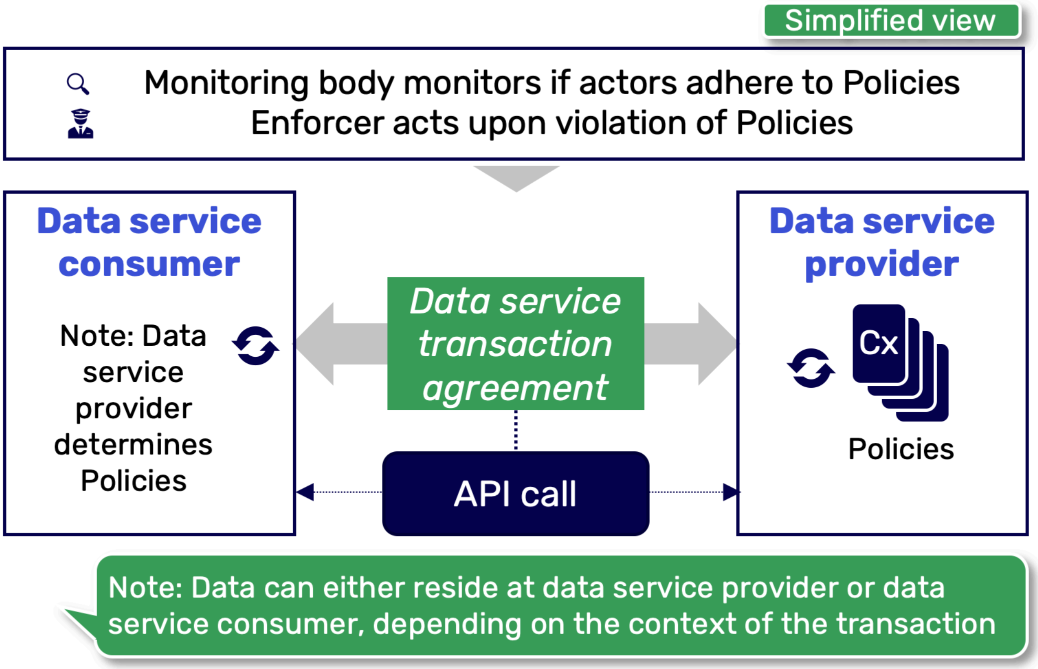

Simplified view
Monitoring body monitors if actors adhere to Policies
Enforcer acts upon violation of Policies
Data service consumer
Note: Data service provider determines Policies
Data service transaction agreement
API call
Data service provider
Cx
Policies
Note: Data can either reside at data service provider or data service consumer, depending on the context of the transaction

Figure 35: Terms and Conditions in a DATA SERVICE TRANSACTION agreement.

A DATA SERVICE TRANSACTION AGREEMENT is an agreement (handshake) between a DATA SERVICE CONSUMER and PROVIDER on the terms and conditions associated with a specific data transaction. An agreement is achieved through the following five steps:

1. A DATA SERVICE PROVIDER publishes its DATA SERVICE including all POLICIES.
2. A DATA SERVICE CONSUMER requests a DATA SERVICE (API call) and provides evidence of adherence to ACCESS CONTROL RULES.
3. The DATA SERVICE PROVIDER evaluates the evidence and executes the requested DATA SERVICE based on the result of this evaluation.
4. The DATA SERVICE PROVIDER confirms the DATA SERVICE TRANSACTION AGREEMENT.
5. The DATA SERVICE PROVIDER executes the DATA SERVICE while both DATA SERVICE PROVIDER and DATA SERVICE CONSUMER provide evidence of adherence OBLIGATION AND ADVICE POLICIES.

These steps hold for all types of DATA SERVICES (e.g. data pull/push, bring algorithm to data, see Table 3).

Box 12: Steps to reach a DATA SERVICE TRANSACTION agreement in the energy domain

Within the energy DOMAIN, the energy provider (DATA SERVICE CONSUMER) wants to make use of energy consumer data (e.g. on energy usage), which is currently in possession of the DSOs (DATA SERVICE PROVIDER). DSOs enable energy providers to access consumer data through publishing their DATA SERVICE, including all POLICIES that the energy provider should adhere to. Only with consent of the consumer can the energy provider access the consumer's energy data. The energy provider needs to identify the energy producer and the DSO authenticates the identity of the energy producer. In addition, the DSO evaluates the evidence of adherence to other POLICIES of the energy provider, before providing energy provider access to the consumer data. Both the energy provider and the DSO have agreed on the POLICIES both should adhere to and access will be provided.

18 Terms and Conditions

18.1 Terms and Conditions in DSC use cases

Note: More detail in Box 13 will be included when more use cases have been initiated and current use cases have been developed further.

Box 13: Terms and conditions in DSC use cases

Different TERMS AND CONDITIONS are relevant in the use cases in which the DSC is involved. Below, indicative and non-exhaustive lists of TERMS AND CONDITIONS (formalised into POLICIES) within these use cases are shown.

Example Policies in 'Green Loans' use case (HDN – Netbeheer NL)

ACCESS CONTROL RULES:

- Identity of consumer must be verified at the appropriate Level of Assurance that matches the risk-context of the transaction
- There must be reasonable certainty that the EAN-code (smart meter identifier) for which data is requested belongs to the consumer's smart meter
- Identity Intermediary must be certain
- Intermediary must have unique identifier
- DSO must be able to verify that intermediary is "Trustworthy"
- Consumer AUTHORISATION must be linked to identifier of intermediary
- Purpose of data requested must match the operations of the intermediary

ADVICE AND OBLIGATION:

- Scope of usage is the "bemiddelingsproces", which includes sending (subset of) data to banks
- Data may not be altered and must maintain "seal of validity"
- Time to live is maximum of 24 months

Example Policies in 'Sharing e-CMR data with insurers' use case (iSHARE – Verbond van Verzekeraars)

ACCESS CONTROL RULES:

- Access rights of the insurer must be registered by the claim issuer in an Authorisation Registry
- Authorisation is granted based on Delegation evidence provided by claim issuer to the e-CMR provider
- Parties must either be an organisation with delegated data access or the owner of the data
- Parties must provide a qualified eIDAS (or PKIOverheid) certificate for Authentication

Advice and Obligation:

- Scope of usage is the claims handling process
- Licenses indicate for which purposes the (subset of) shipment data may be used (e.g. no limitations, non-commercial use only, for own use only)
- Time to live of shipment data points at insurer can be set to a maximum by the claim issuer

18.2 Initial Policy clusters and examples of Policies

Policy clusters are sets of Policies. The overview below shows preliminary Policy clusters. This overview is based on the input that is provided by the Data sharing initiatives in the DSC and input provided in Expert Group discussions. This overview of clusters is not exhaustive but serves as an example to be used as a starting point for the next phase of the DSC. These clusters may be subject to change in the next phase. This first set-up distinguishes clusters on its type of Policies: Access control rules and Advice and Obligation (both usage and other).

Table 10: Overview of clusters and types of Policies

Cluster	Policies	Type
Scope	Time to live	Obligations and Advice: Usage
	Usage scope	Obligations and Advice: Usage
	Propagation restrictions	Obligations and Advice: Usage
	Third party use of data	Obligations and Advice: Usage
	Usage based on geography	Obligations and Advice: Usage
	Target binding	Obligations and Advice
Authorisation	Access management	Access Control Rules
	Delegated rights	Access Control Rules
Authentication	Multi-factor Authentication	Access Control Rules
	Supported e-ID means	Access Control Rules
	Identity confirmation mechanism	Access Control Rules
Liabilities	Indemnification	Obligations and Advice
Privacy (pre)	Privacy Impact Assessments	Access Control Rules
	Risk analysis	Access Control Rules
Privacy (post)	Anonymisation	Obligations and Advice
	Right to be forgotten	Obligations and Advice

Cluster	Policies	Type
Information classification	Data classification scheme	Access Control Rules
Information access	Access management protocol	Access Control Rules
	Separation of functions	Access Control Rules
	User access rights audit	Access Control Rules
Operational conditions	Data minimalisation	Obligations and advice
	Testing requirement	Obligations and advice
	Data breach notification(s)	Obligations and advice
Provenance	Obligated provenance	Obligations and advice
Data storage	Data retention period	Obligations and advice
	Data deletion evidence	Obligations and advice
	Encryption of stored data	Obligations and advice
	Back-up retention period	Obligations and advice
	Cryptographic key storage	Obligations and advice
Non-repudiation	Digital signature requirement	Obligations and advice
Laws and regulations	Declaration of adherence to law	Access Control Rules
	Applicable law	Access Control Rules
	GDPR compliance	Access Control Rules
Information security	Confidentiality	Obligations and advice
	Integrity	Obligations and advice
	Authenticity	Obligations and advice
Geographical information	Data processing outside of EU	Obligations and advice
Employee qualifications	IT officer assignment	Access Control Rules
	Employee competency declaration	Access Control Rules
	Employee screenings	Access Control Rules
Supervision	Monitoring	*All*
	Enforcement	*All*
	Arbitrage and dispute settlement	Obligations and advice

18.2.1 Longlist of metadata languages for Policies

Different Metadata languages exist of which some are specifically developed for Terms and conditions. These Metadata languages enable coherent communication across sectors on TERMS AND CONDITIONS and hence, examples (see below) are discussed in this chapter.

DCAT/ODRL

DCAT is a worldwide W3C METADATA standard, applied by the Dutch government among others. In the newest version of DCAT, datasets can be enriched with conditions for DATA SHARING. ODRL is the standard for the description of these conditions.

eFlint

eFlint is a standard meant to make the structure and meaning of legal documents “machine readable”.

Akomo Ntoso

Akomo Ntoso is an open standard meant to make the structure and meaning of legal documents “machine readable”.

RDF

RDF (Resource Description Framework) is a standard for data exchange, developed by W3C.

19 Data Service Discovery

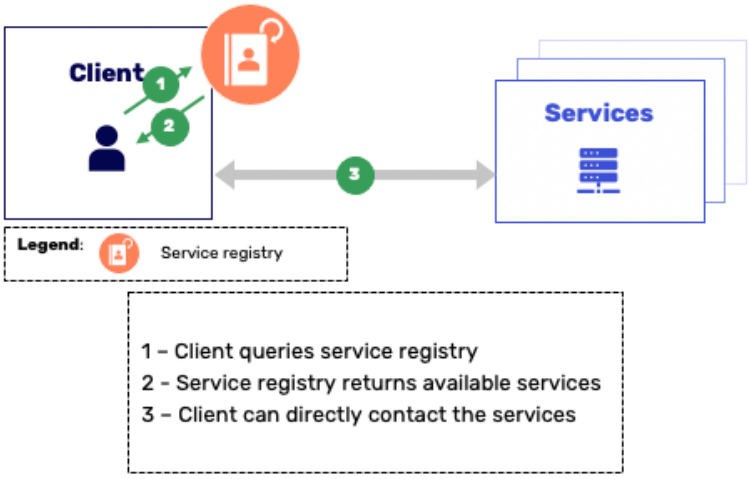
19.1 Industry standards for Service Discovery

‘Client’ and ‘Server’ side discovery are industry standards for discovery through the use of a service registry. From the perspective of CROSS-DOMAIN DATA SHARING, the Client can be considered either a DATA SERVICE CONSUMER or their PROXY. In this context, the services being discovered can be either the DATA SERVICE PROVIDER or their PROXY.

19.1.1 CLIENT SIDE DISCOVERY

In client side discovery, the client is responsible for discovering data services. For every discovery request, the client will check a SERVICE REGISTRY, see Figure 36. Main characteristics of client side discovery include:

- Straightforward interactions which do not require additional parties (i.e. discovery broker),
- Client implementation must contain intelligent logic and a coupling with the SERVICE REGISTRY.



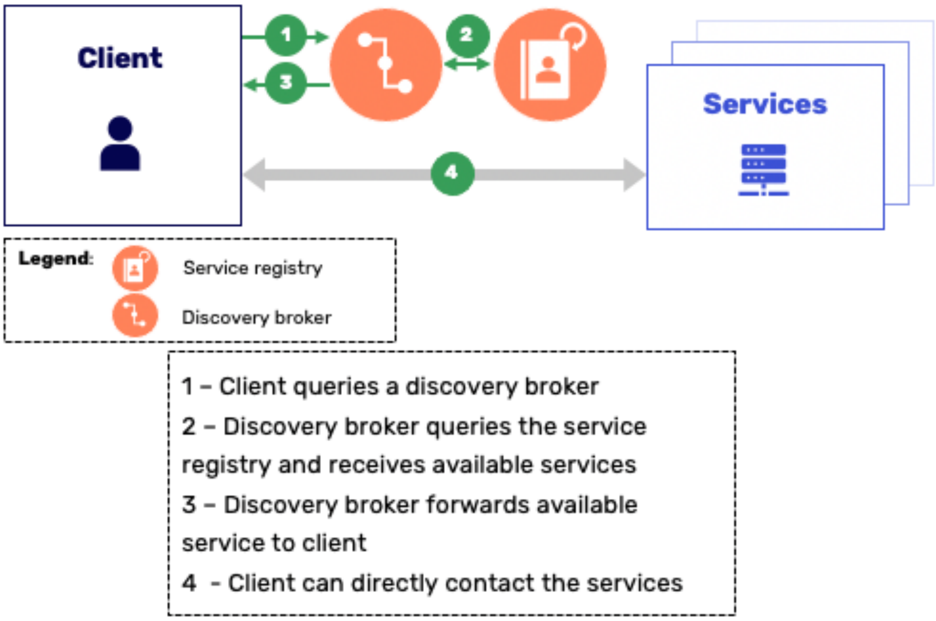
1 – Client queries service registry
2 - Service registry returns available services
3 – Client can directly contact the services

Figure 36: Schematic overview of client side discovery

19.1.2 Server side discovery

In server side discovery, the client makes a transaction request towards a discovery broker. The discovery broker is responsible for discovering data services, see Figure 37. For every discovery request, the discovery broker will check a SERVICE REGISTRY and may perform additional services. Main characteristics of server side discovery include:

- Simple client implementation as discovery logic is handled by a broker,
- A discovery broker can deliver additional services,
- The role of discovery broker must be implemented and maintained, which comes with costs.



1 – Client queries a discovery broker
2 – Discovery broker queries the service registry and receives available services
3 – Discovery broker forwards available service to client
4 - Client can directly contact the services

Figure 37: Schematic overview of server side discovery

19.2 Data service discovery in the proxy model

DATA SERVICE DISCOVERY applies to the complete end-to-end process of DATA SERVICE EXCHANGE. In the PROXY model, DATA SERVICE discovery can be seen from a number of different perspectives. Once DOMAINS are fully HARMONISED, discovery can take place directly between DATA SERVICE CONSUMERS and DATA SERVICE PROVIDERS. Before full HARMONISATION is reached, each perspective of DATA SERVICE discovery must be considered separately, see Figure 38.

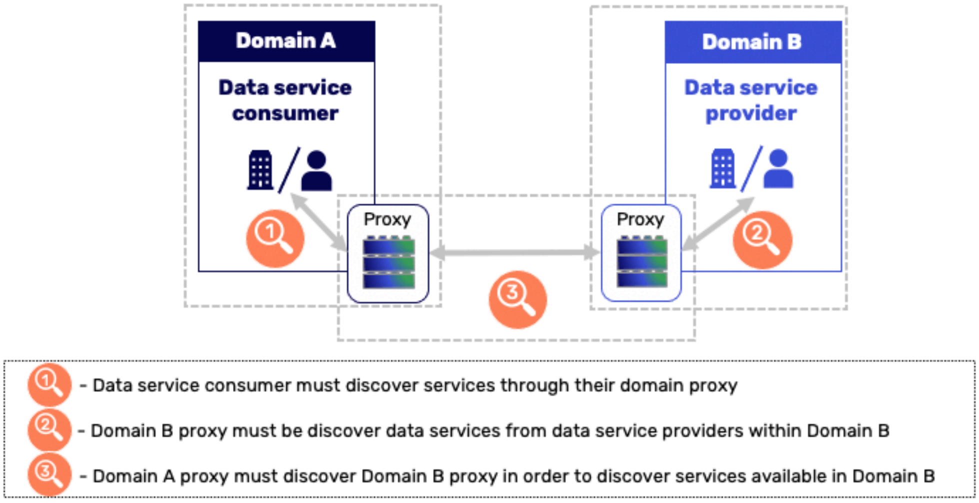

Domain A
Data service consumer
Proxy
Domain B
Data service provider
Proxy
1
2
3
1 - Data service consumer must discover services through their domain proxy
2 - Domain B proxy must be discover data services from data service providers within Domain B
3 - Domain A proxy must discover Domain B proxy in order to discover services available in Domain B

Figure 38: Various data service discovery perspectives within the proxy model

From a DATA SERVICE CONSUMER perspective, server side discovery reduces impact on the DATA SERVICE CONSUMERS, (Discovery perspective 1 in Figure 38). A DATA SERVICE CONSUMER must discover the services that they want to make use of. In order to reduce impact on DATA SERVICE CONSUMER, the PROXY can perform this DISCOVERY request for them. From the DATA SERVICE CONSUMER perspective, the PROXY has the role of discovery broker and this can be considered server side discovery.

The DATA SERVICE PROVIDER'S PROXY must be able to discover available DATA SERVICES within its DOMAIN (DISCOVERY perspective 2 in Figure 38). Depending on DOMAIN implementations, both client and server side discovery solutions are viable as both solutions do not impact the DATA SERVICE PROVIDER.

The DATA SERVICE CONSUMER'S DOMAIN proxy must be able to discover DATA SERVICE providers within another DOMAIN via their PROXY (Discovery perspective 3 in Figure 38). Client side discovery can be implemented in order for the PROXY to be able to perform its own discovery. Server side discovery can be implemented in order to facilitate discovery brokers to implement the discovery server. The design choices made will be applicable to DATA SERVICE CONSUMERS and DATA SERVICE PROVIDERS once DOMAINS reach full HARMONISATION.