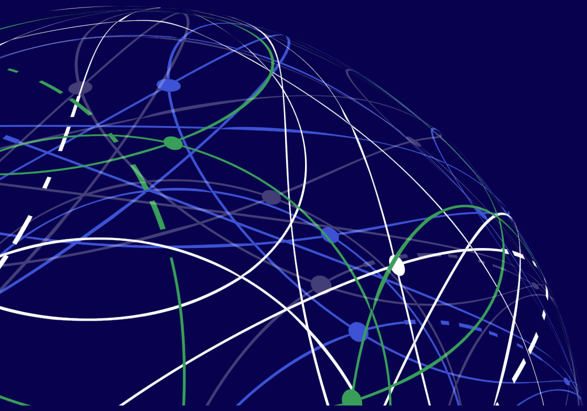
Harmonisation Canvas

DATA SHARING COALITION



Penholder document
INNOPAY

Release
Version 0.1

Date
13 November 2020

Versioning

Version	Date	Comments
Initial v0.1	28 September 2020	Initial version
Version 0.1	13 November 2020	Processed comments on initial version

Table of Contents

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 provider	The actor that offers a Data service to the Data service consumer
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
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
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

Glossary item	Definition
GUIDING PRINCIPLE	A principle that gives direction in the decision-making process of establishing and maintaining the content of the HARMONISATION CANVAS
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	Mitigating risks of threat events through the implementation of technical or organisational information security measures
INITIATIVE	Synonym for DATA SHARING INITIATIVE
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
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

Glossary item	Definition
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

36

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 6 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.

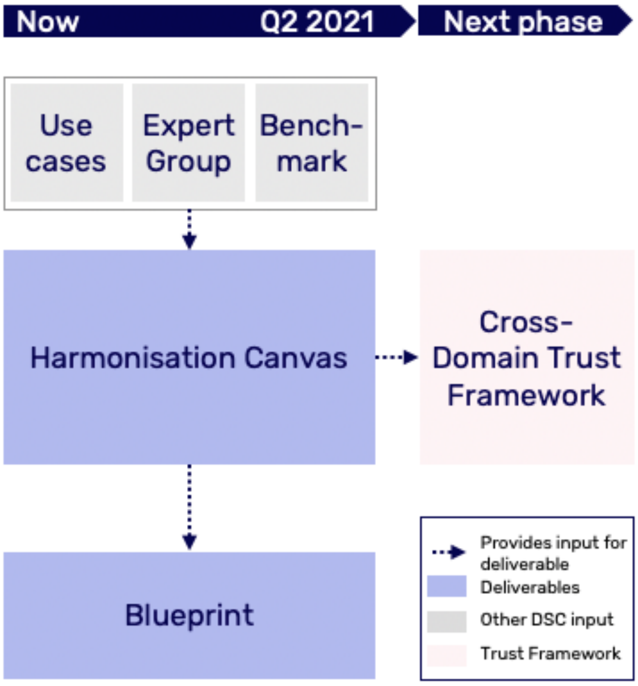


Figure 1: Relationship of the Harmonisation Canvas with other documents

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

Table 2: Overview of documents related to the Harmonisation Canvas

Document	Description	Status
DATA SHARING COALITION *Blueprint*	An overview of elements of DATA SHARING INITIATIVES, corresponding best practices and insights from the HARMONISATION CANVAS. This will inform, inspire and accelerate new and existing DOMAINS and support them in becoming INTEROPERABLE	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

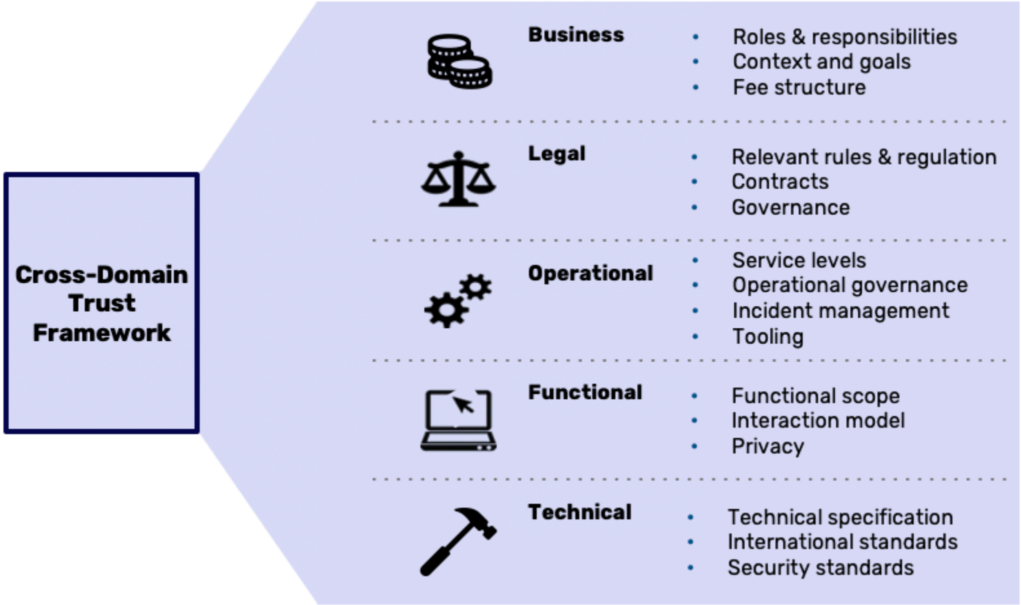
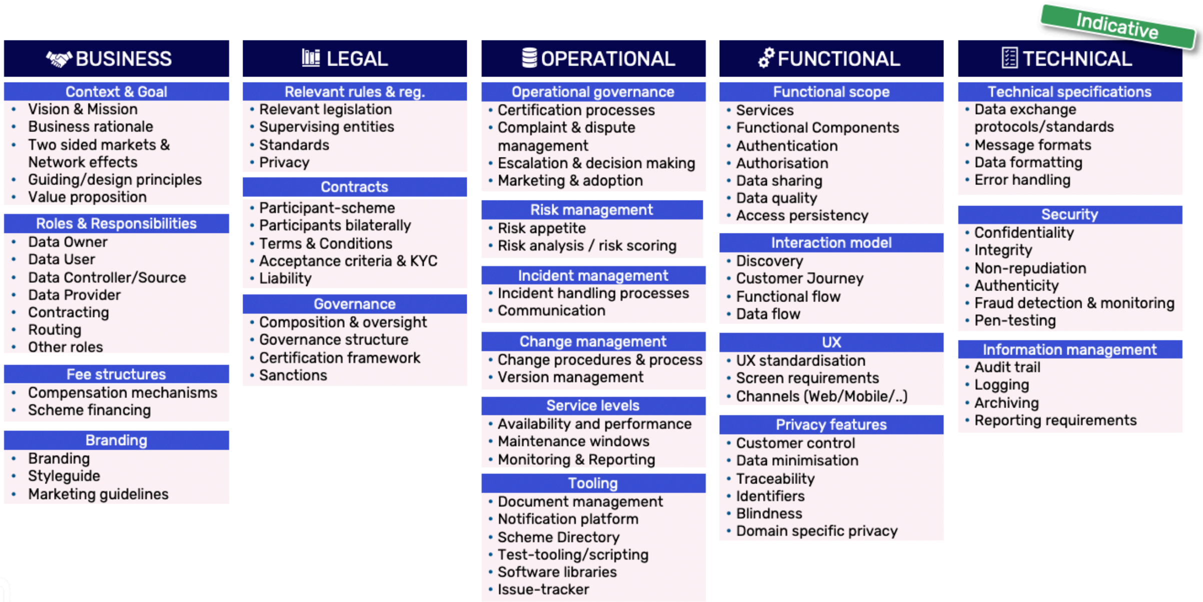


Figure 2: Preliminary content and structure of the future Cross-Domain Trust Framework

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 within the future cross-DOMAIN network through compliance with the TRUST FRAMEWORK. This facilitates a basic reduction of risks between participants to enable a basic level of TRUST.
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 by participants, for example, in terms of value or 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. Strive for the lowest possible 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 share 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[2] (digital waybill) 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 8.1 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

[2] e-CMR stands for e-"Convention relative au Contrat de Transport International de Marchandises par Route"

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.

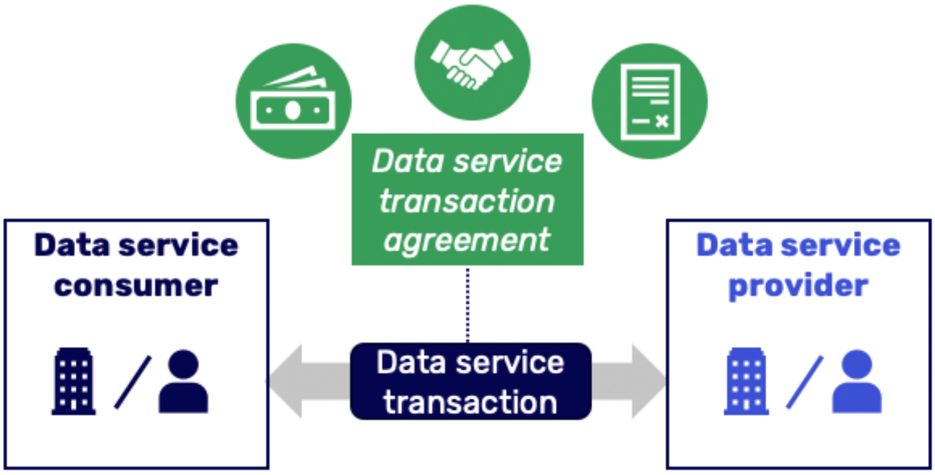


Figure 4: Overview of a Data service, including the DATA SERVICE TRANSACTION AGREEMENT

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 contain reference to all other functionalities and Data services of participants within different Domains in a Cross-Domain Data Service Registry.

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.

The Proxies will be implemented by the individual Domains that adhere to the Cross-Domain Trust Framework. Figure 5 shows a visual representation of the Proxy Model.

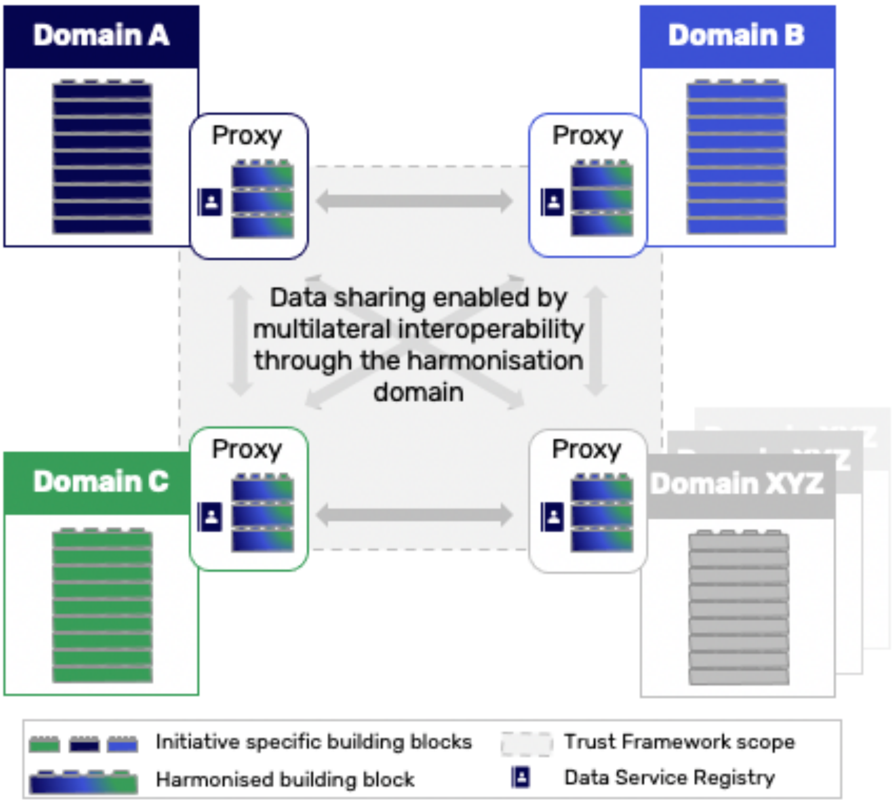

Domain A
Domain B
Proxy
Proxy
Data sharing enabled by multilateral interoperability through the harmonisation domain
Proxy
Proxy
Domain C
Domain XYZ
Initiative specific building blocks
Harmonised building block
Trust Framework scope
Data Service Registry

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.

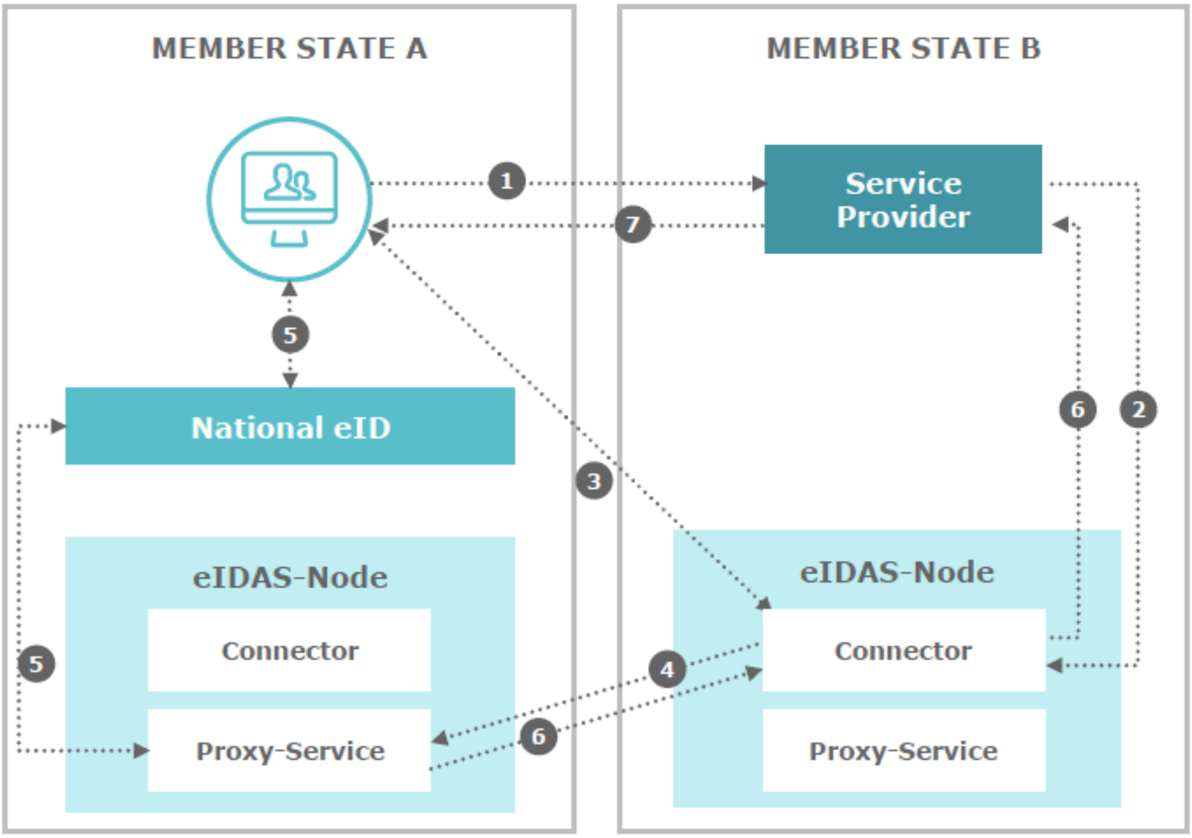


Figure 6: Overview of the eIDAS AUTHENTICATION scheme depicting eIDAS Nodes, Source: https://docs.wso2.com/display/IS570/Electronic+Identification%2C+Authentication+and+Trust+Services+Regulation

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.

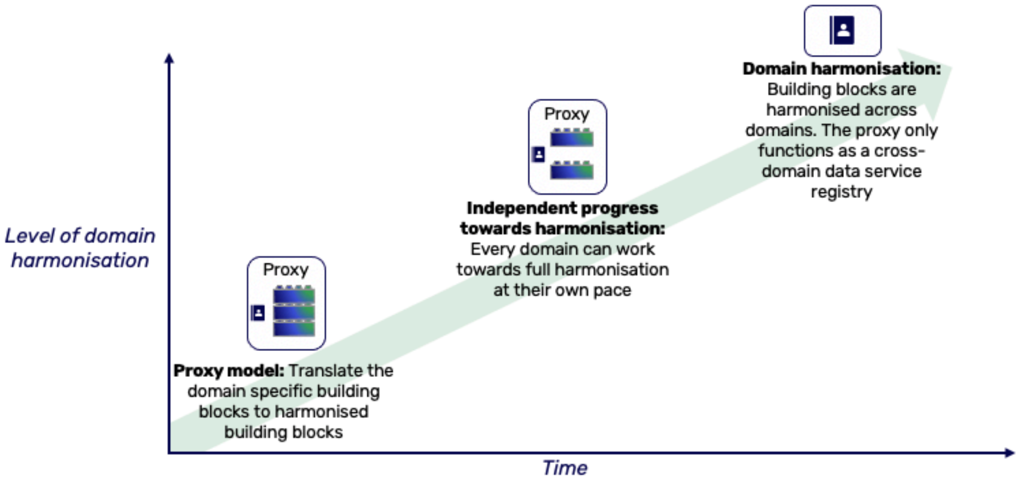

Level of domain harmonisation
Time
Proxy
Proxy model: Translate the domain specific building blocks to harmonised building blocks
Proxy
Independent progress towards harmonisation: Every domain can work towards full harmonisation at their own pace
Domain harmonisation: Building blocks are harmonised across 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.

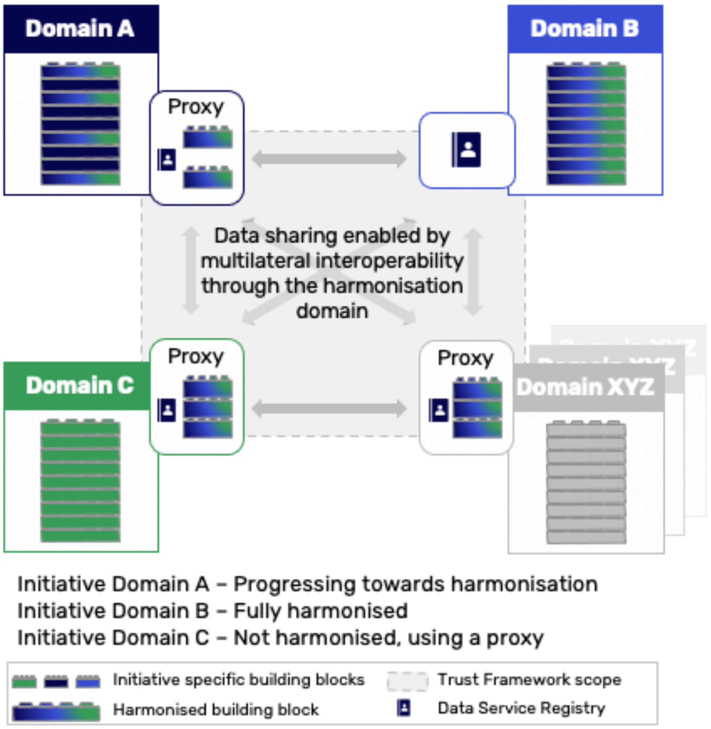

Domain A
Proxy
Domain B
Data sharing enabled by multilateral interoperability through the harmonisation domain
Proxy
Proxy
Domain C
Domain XYZ
Initiative Domain A – Progressing towards harmonisation
Initiative Domain B – Fully harmonised
Initiative Domain C – Not harmonised, using a proxy
Initiative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

Note: More chapters will be added to this section in the coming period, once the DATA SHARING COALITION Expert Group has discussed more topics.

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.

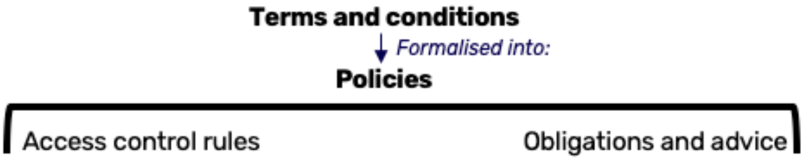


Figure 9: TERMS AND CONDITIONS are formalised in POLICIES, which can be split into ACCESS CONTROL RULES and OBLIGATIONS AND ADVICE

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

Note: This chapter will further explain the topic based on discussions with the experts involved in the Expert Group.

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 9.2 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[3,4] framework.

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.

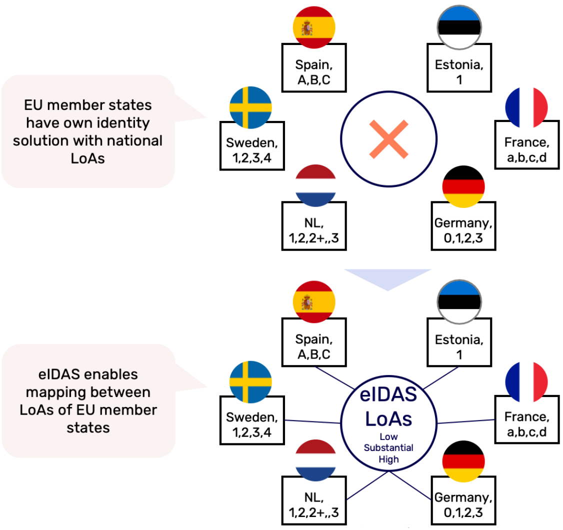
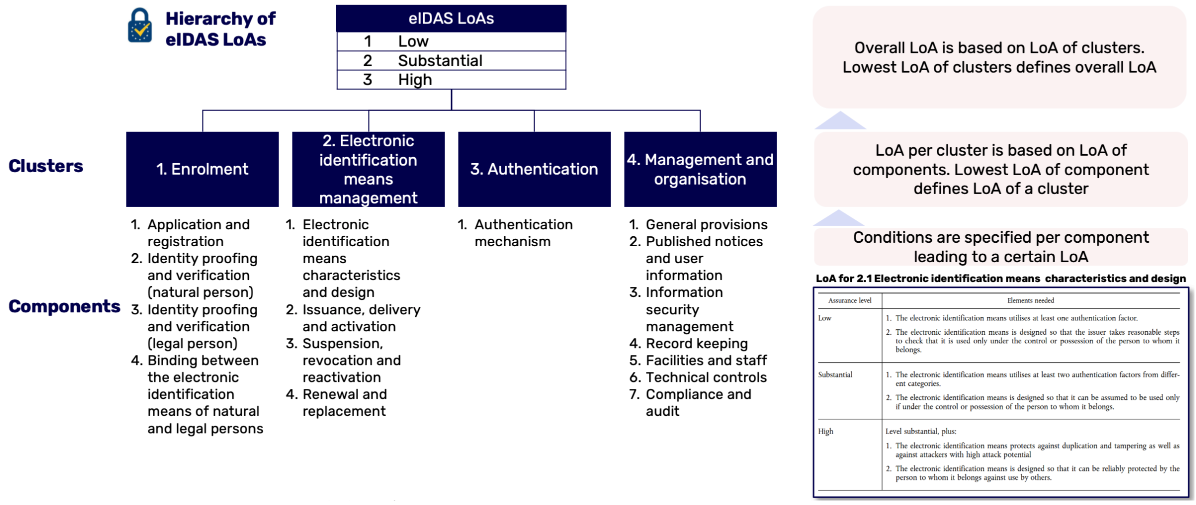


Figure 10: Creation of a mapping between Levels of Assurance in EU member states

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.

[3] **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

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


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. 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 9.1 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.

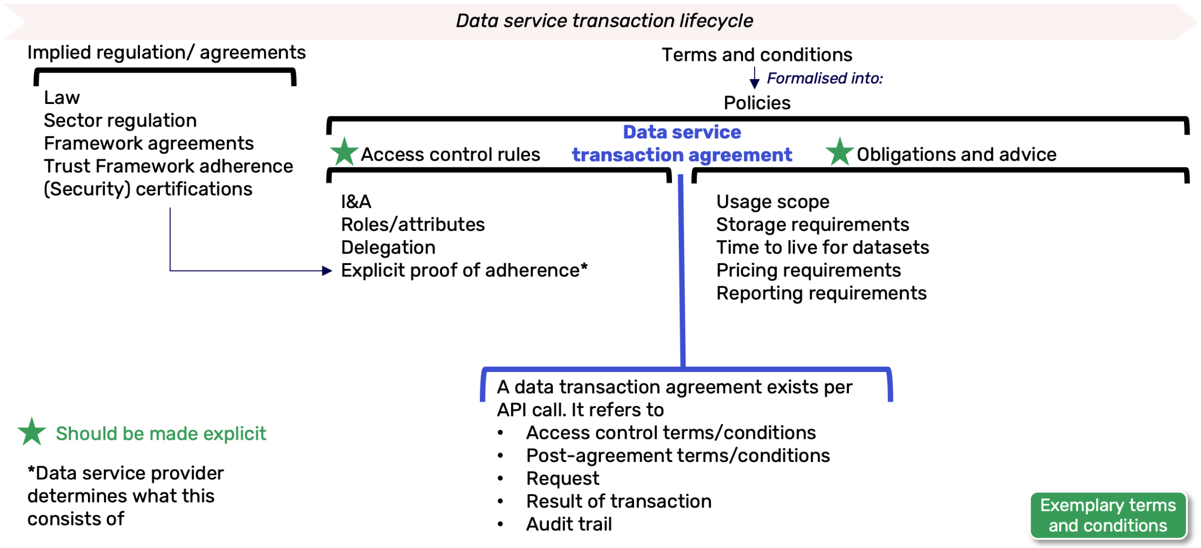

Data service transaction lifecycle
Implied regulation/ agreements
Law
Sector regulation
Framework agreements
Trust Framework adherence
(Security) certifications
Terms and conditions
Formalised into:
Policies
Data service
transaction agreement
Access control rules
Obligations and advice
I&A
Roles/attributes
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-2-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 Authentication 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

Note: This chapter will further explain the topic based on discussions with the experts involved in the expert group.

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 6.3.3 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. Explicit specification can be achieved by including a defining prefix to all identifiers in the INTEROPERABILITY DOMAIN, see Box 3 for a detailed description. The exact method of including the prefix, 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).

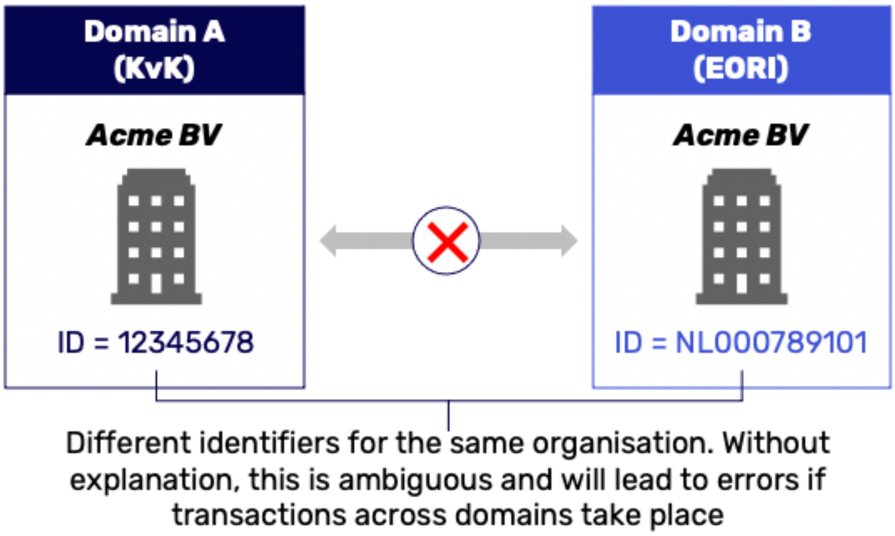

Domain A (KvK)
Acme BV
ID = 12345678
Domain B (EORI)
Acme BV
ID = NL000789101
Different identifiers for the same organisation. Without explanation, this is ambiguous and will lead to errors if transactions across domains take place

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.

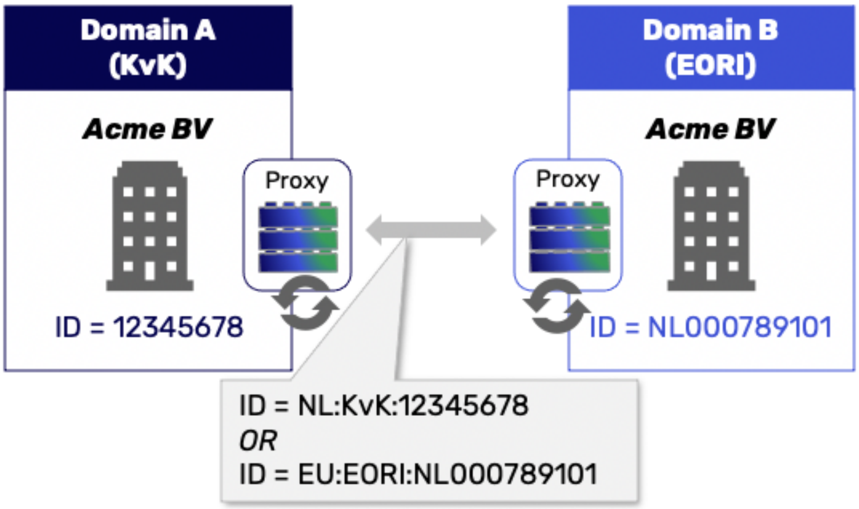


Figure 14: Using prefixes for communication of IDs across domains solves ambiguity

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. Table 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.
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.

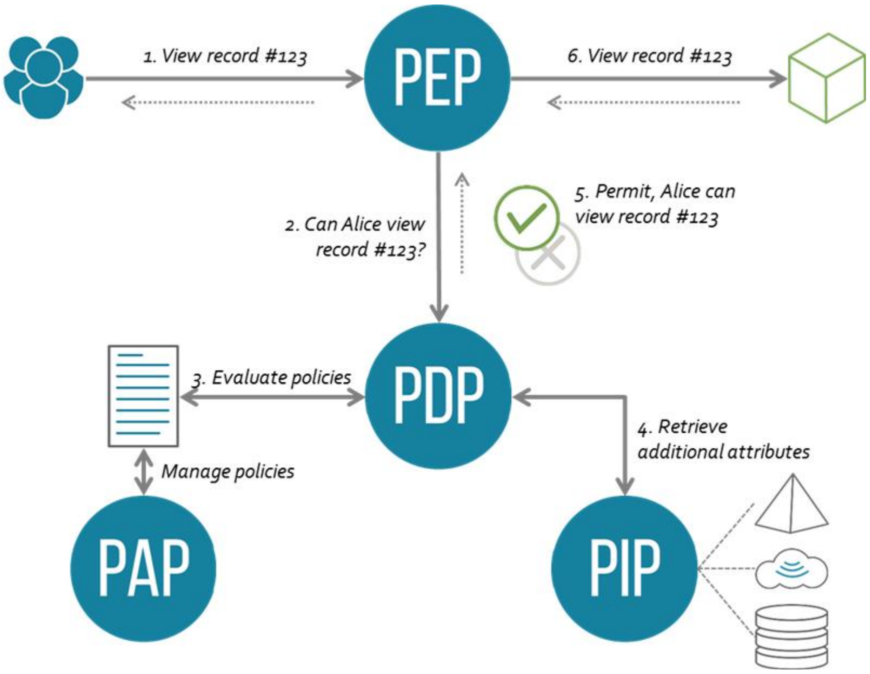

1. View record #123
PEP
6. View record #123
2. Can Alice view record #123?
5. Permit, Alice can view record #123
3. Evaluate policies
PDP
4. Retrieve additional attributes
Manage policies
PAP
PIP

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.

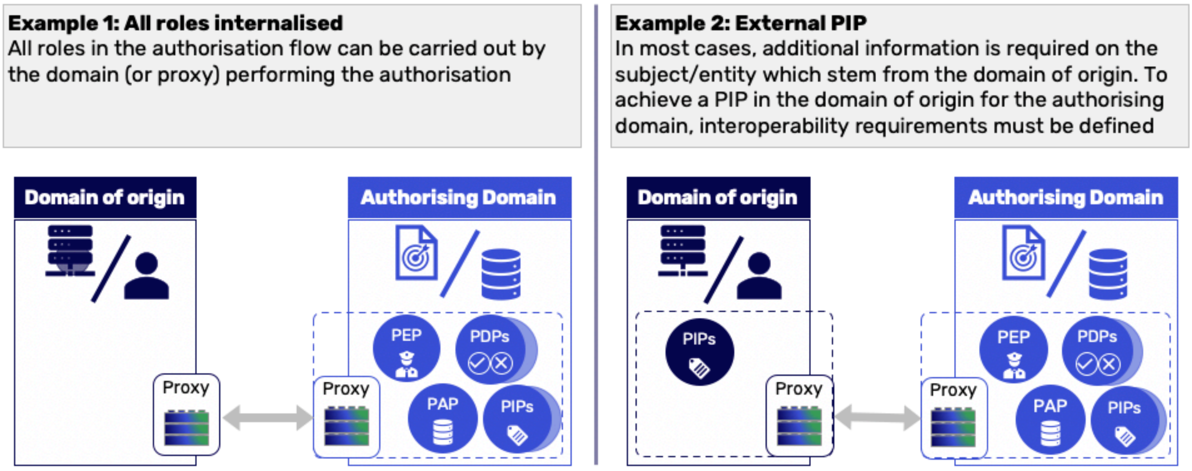
In practice, there is often not just a single implementation of several of the AUTHORISATION roles. For example, there can be multiple PDPs which each take partial AUTHORISATION decisions which collectively can lead to a final AUTHORISATION decision. Furthermore, there are often multiple PIPs, each providing 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.

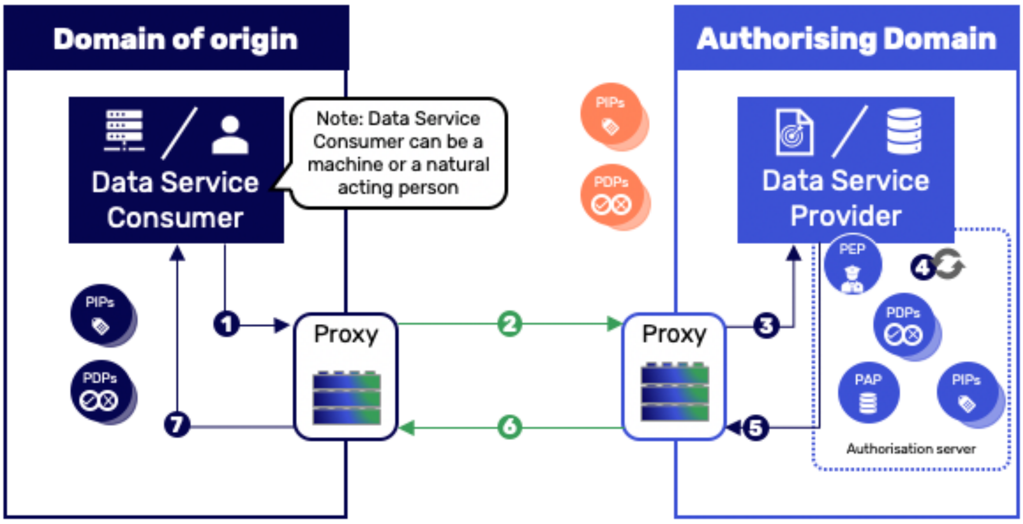


Figure 17: Proxy interaction for a pull authorisation model

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.

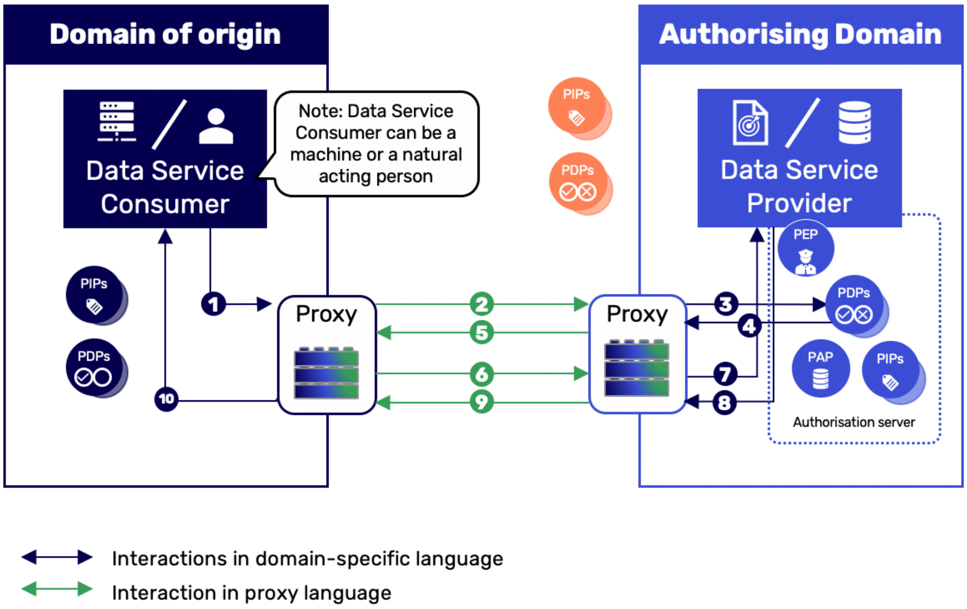

Domain of origin
Authorising Domain
Data Service Consumer
Note: Data Service Consumer can be a machine or a natural acting person
PIPs
PDPs
Data Service Provider
PEP
PAP
Authorisation server
Proxy
Proxy
1
2
3
4
5
6
7
8
9
10
Interactions in domain-specific language
Interaction in proxy language

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 iShare, 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.

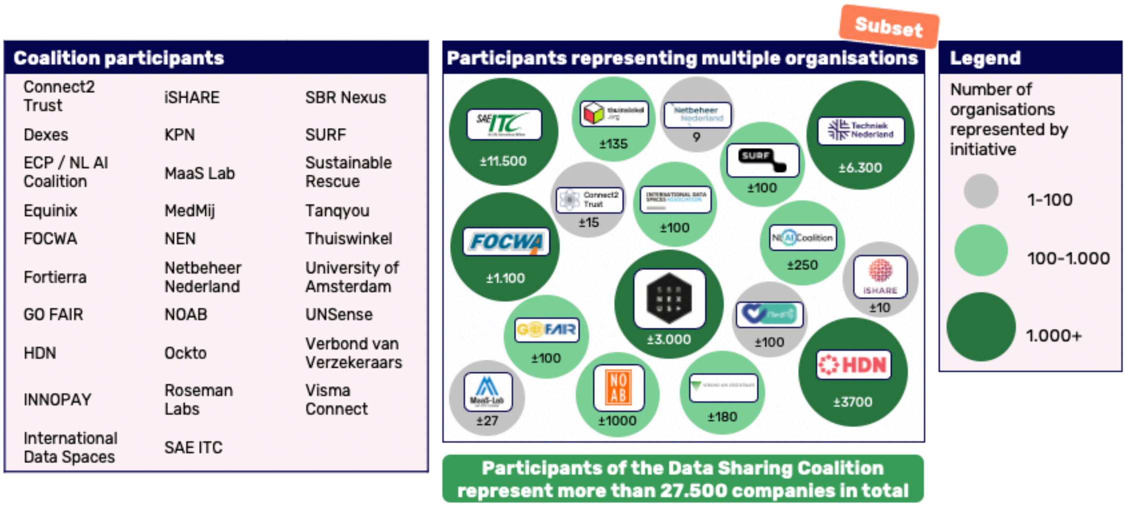
If pre-configured Delegation takes place within the Domain of Origin, this must be communicated to the authorising Domain during a Data service transaction. The Trust Framework must facilitate a method to communicate this Delegation across Domains. Furthermore, a method for the Authorising Domain should 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.

Section C. Appendix

7 Data Sharing Coalition Overview



Coalition participants

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

Subset

Participants representing multiple organisations

Legend

Number of organisations represented by initiative

●	1-100
●	100-1.000
●	1.000+

Participants of the Data Sharing Coalition represent more than 27.500 companies in total

Figure 19: Overview of Data Sharing Initiatives within the DSC

Table 6: 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 / Visma Connect	Marnix Vermaas
MedMij	Johan Hobelman
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
University of Amsterdam	Leon Gommans
University of Amsterdam	Wouter Los
University of Amsterdam	Tom van Engers
Visma Connect	Elsbeth Bodde

Organisation	Name
Visma Connect	Victor den Bak

8 Interoperability and harmonisation

8.1 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 20.

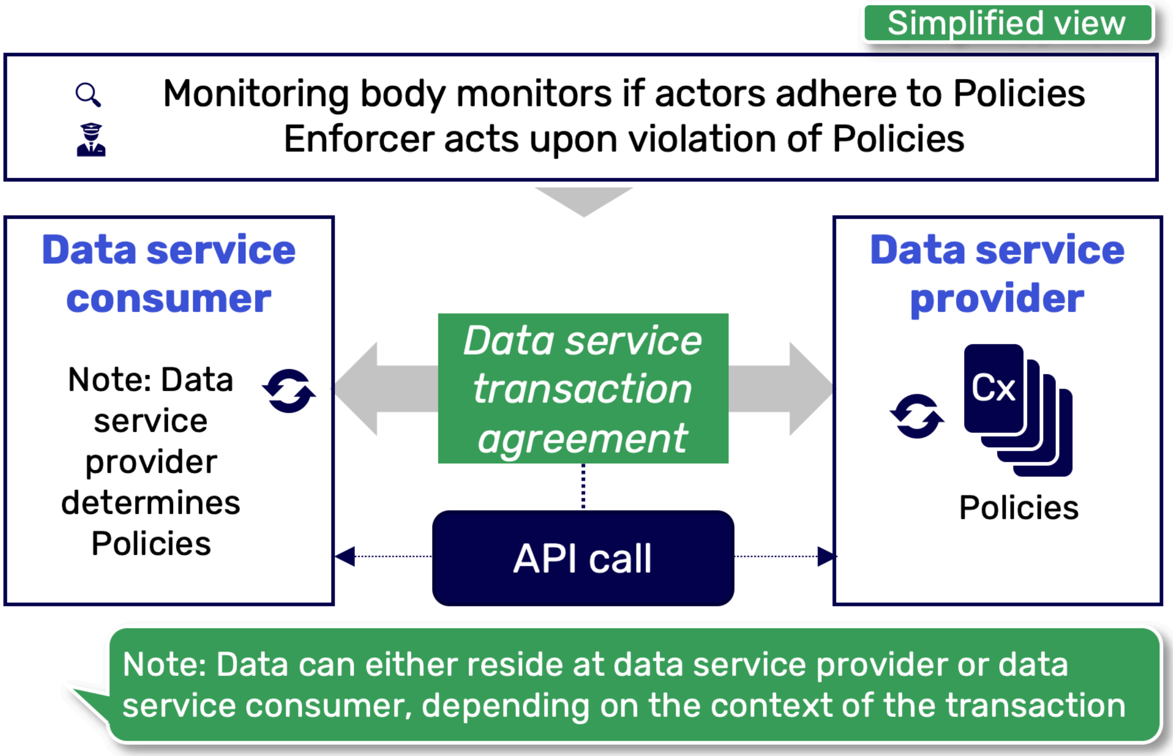

Simplified view
Monitoring body monitors if actors adhere to Policies
Enforcer acts upon violation of Policies
Data service consumer
Note: Data service provider determines Policies
Data service transaction agreement
API call
Data service provider
Cx
Policies
Note: Data can either reside at data service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

Figure 20: 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 8: 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.

9 Terms and Conditions

9.1 Terms and Conditions in DSC use cases

Note: More detail in Box 9 will be included when more use cases have been initiated and current use cases have been developed further.

Box 9: 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

9.2 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 7: 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
Information classification	Data classification scheme	Access Control Rules

Cluster	Policies	Type
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

9.2.1 Longlist of metadata languages for Policies

Note: More detail on the contents of this chapter will be included when the topic metadata has been discussed in more detail. This longlist is not exhaustive.

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.

10 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.

10.1 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.

10.2 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.